UNIVERSITY OF NAIROBI

ON APPLICATION OF OPERATOR AND GROUP-THEORETIC CONCEPTS IN SIGNAL PROCESSING AND CRYPTOGRAPHY

BY:

NJAGI LOYFORD

REGISTRATION NUMBER: I80/98391/2015

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN PURE MATHEMATICS OF THE UNIVERSITY OF NAIROBI

SCHOOL OF MATHEMATICS, UNIVERSITY OF NAIROBI
P. O. BOX 30197, NAIROBI, KENYA

JUNE, 2019

DECLARATION

I declare that this thesis is my original work and has not been presented for a degree award in any other University.

SIGNATURE:....................................DATE:...............................

We decalare that this thesis has been submitted with our approval as University supervisors.

Prof. Bernard M. Nzimbi
School of Mathematics
University of Nairobi

SIGNATURE:....................................DATE:...............................

Prof. Ganesh P. Pokhariyal
School of Mathematics
University of Nairobi

SIGNATURE:....................................DATE:...............................

Prof. Stephen K. Moindi
School of Mathematics
University of Nairobi

SIGNATURE:....................................DATE:...............................

ACKNOWLEDGEMENT

Glory and Honor to the Almighty God for His providence, sustenance and his unmerited grace and mercy that He accorded me during the entire period of my research on this thesis.

I am greatly indebted to my main supervisor Prof. B. M. Nzimbi, who has inspired me on research in this topic, which was very challenging yet very interesting. His timely encouragement, guidance and support have not only made the completion of this thesis possible but have also left an impression which will continue to influence my research work in future.

My sincere gratitude goes to my other supervisors Prof. G. P. Pokhariyal and Prof. S. K. Moindi for their big encouragement and support.

A big thank you to the Director of the School of Mathematics Prof. P.G.O. Weke who was always there for me when I needed assistance from his office.

I am also very grateful to my family: my dear wife, Mary and my children, Fred and family, Emmies and spouse, Dennis and Dave for their moral support, co-operation and prayers throughout the entire period of my research.

May the Almighty God Bless you all.

DEDICATION

I dedicate this work to my dear wife Mary, for her continued support, prayers, patience during the entire period of my study.

ABSTRACT

In this thesis we have studied how operator theory is applied in signal processing and how some concepts in group theory are crucial in the design of cryptosystems and their use in hiding information. A frame is a redundant (i.e. not linearly independent) coordinate system for a vector space that satisfies a certain Parseval-type norm inequality. Frames provide a means for transmitting data and, when a certain loss is anticipated, their redundancy allows for better signal reconstruction. We have started with the basics of frame theory and given examples of frames and applications that illustrate how this redundancy can be exploited to achieve better signal reconstruction. The key idea is that in order to protect against a noise, we should encode the message by adding some redundant information to the message. In such a case, even if the message is corrupted by noise, there will be enough redundancy in the encoded message to recover, or to decode the message completely
Cryptography is the science of information security, it is the practice of defending information from unauthorized access, use, disclosure,disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take(electronic, physical, etc). We have explored and demonstrated how simple concepts like divisibility of integers, primes and other concepts in number theory come in handy in cryptography. We have demonstrated how to use group theory concepts to send messages(plaintext) in disguised form so that only the intended recipients can remove the disguise and read the message(ciphertext). To be able to achieve all this, we have spent a bit of time developing the notion of Hilbert space frames, some groups, number systems and their their properties. We have chosen the most optimal frames(tight frames) and groups(cyclic) for use in sending signal and also reconstructing the sent signal and enciphering and deciphering a message.

STRUCTURE OF THE THESIS

This research thesis consists of six chapters.

Chapter I begins with an introduction, background of the problem, definitions, key terminologies, notations and continues to focus on some basic results and examples that seem to be of greatest relevance to signal processing and cryptography.

In Chapter II we present the literature review, which in essence forms a basis to the research problem. It also gives an overview of what has been done in this research area. We identify the research or knowledge gap and identify a strategy on how to fill it. We formally state the research problem, objectives and significance of the study.

In chapter III, we look at the mathematical underpinnings of this research. We develop the mathematics required for signal processing and cryptography. We study vector spaces, metric spaces, normed spaces, Hilbert spaces and some group theory/number theory and the public-key RSA cryptosystem.

In chapter IV we present results on frames in both finite and infinite dimensional Hilbert spaces.

In chapter V, we provide applications of these concepts in cryptography and signal processing.

In chapter VI we give a summary of the main results and conclusion. We have also given direction for further research.

Contents

Chapter 1

PRELIMINARIES

1.1 Background of Signal Processing and Cryptography

Signal processing is a subfield of mathematics, information and electrical engineering that concerns the analysis, synthesis, and modification of signals, which are broadly defined as functions conveying information about the behavior or attributes of some phenomenon, such as sound, images, etc. In signal processing, each vector is interpreted as a signal. In this interpretation, a vector expressed as a linear combination of the frame vectors is a redundant signal. Redundancy can be used to mitigate noise, which is relevant to the restoration, enhancement, and reconstruction of signals.

Cryptography is the science of disguising data so that only the sender and recipient can read the data. Cryptographers call the data they want to send plaintext, usually converted into a string as a vector in a vector space. The process of disguising the data is encryption. Encryption is a one-to-one mathematical function that requires a key (a unique number or set of numbers) and a plaintext as input to produce the encrypted text or ciphertext. The ciphertext, a new string (or vector) of integers between 0 and 255, can be converted back to the same medium as the plaintext and sent through the mail, internet, or any other mode of data decryption. Decryption is the inverse mathematical function of encryption which takes a key and a ciphertext as input to reproduce the plaintext.

The domains of the plaintext and ciphertext along with the keys, encryption function, and decryption function make up a cryptosystem. A good cryptosystem is one that is computationally efficient and requires little storage space. Cryptographers are encouraged to develop systems that have a small key size, so that the keys are easy to share through covert channels; for example, short verbal communication, an encrypted email or disguised postal letter. The cryptostem must be secure against attack.

1.2 Notations, Terminologies, Definitions and Basic Results

In thesis, $\mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, \mathcal{K}, \mathcal{K}_1, \mathcal{K}_2$, etc will denote Hilbert spaces and $\mathcal{H}^N$ will denote an N-dimensional Hilbert space. By $B(\mathcal{H})$, we denote the Banach algebra of bounded linear operators on a Hilbert space $\mathcal{H}$. We denote by $B(\mathcal{H}_1, \mathcal{H}_2)$ the Banach space of all bounded linear operators from a Hilbert space $\mathcal{H}_1$ into a Hilbert space $\mathcal{H}_2$.

T, T_1, T_2: etc denote bounded linear operators.

T^*: denotes the adjoint of an operator T.

$\langle x, y\rangle$: Inner product of two vectors x and y.

$\|x\|$: norm of a vector x.

$\|T\|$: norm of a bounded linear operator T.

$\mathcal{M}$: a closed subspace or closed linear manifold of a Hilbert space $\mathcal{H}$.

$\overline{\mathcal{M}}$: closure of a subspace $\mathcal{M}$.

$\mathcal{M}^\perp = \{y \in \mathcal{H} : \langle x, y\rangle = 0,\ x \in \mathcal{M}\}$: the orthogonal complement or annihilator of a subspace $\mathcal{M}$.

$Ran(T) = \{y : Tx = y\}$: the range of T, where x belongs to the domain of T.

$Ker(T) = \{x : Tx = 0\}$: the kernel of T.

$\mathcal{M} \oplus \mathcal{N}$: the orthogonal direct sum of subspaces $\mathcal{M}$ and $\mathcal{N}$.

$\mathbb{F}$: any field.

$\mathbb{C}$: field of complex numbers

$M_n(\mathbb{C})$: the algebra of $n \times n$ matrices over the field of complex numbers.

$\sigma(T)$: the spectrum of a bounded linear operator T.

$A \approx B$: similar bounded linear operators A and B.

$A \cong B$: unitarily equivalent bounded linear operators A and B.

$\ell^2(\mathbb{Z}) = \{x = (x_1, x_2, ...) : \sum_{n=1}^{\infty} |x_n|^2 < \infty\}$ with the inner product $\langle x, y\rangle = \sum_{n=1}^{\infty} x_n \overline{y_n}$.

$L^2(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{C} : \int_{\mathbb{R}} |f(t)|^2 dt < \infty\}$(in the sense of Lebesgue) with the inner product $\langle f, g\rangle = \int_{\mathbb{R}} f(t)\overline{g(t)}dt$, where the "bar" denotes complex conjugation. This inner product induced norm $\|f\| = \langle f, f\rangle^{1/2}$.

Definition 1.2.1. Two operators $A \in B(\mathcal{H})$ and $B \in B(\mathcal{K})$ are said to be *similar* (denoted $A \cong B$) if there exists an invertible operator $N \in B(\mathcal{H}, \mathcal{K})$ such that $NA = BN$ or equivalently $A = N^{-1}BN$, and are *unitarily equivalent* (denoted by $A \cong B$) if there exists a unitary operator $U \in B_+(\mathcal{H}, \mathcal{K})$ (Banach algebra of all invertible operators in $B(\mathcal{H})$) such that $UA = BU$ (i.e. $A = U^*BU$, equivalently, $A = U^{-1}BU$).

Definition 1.2.2. Two operators $A \in B(\mathcal{H})$ and $B \in B(\mathcal{K})$ are said to be *metrically equivalent* (denoted by $A \sim_m B$) if $\|Ax\| = \|Bx\|$, (equivalently, $|\langle Ax, Ax\rangle|^{\frac{1}{2}} = |\langle Bx, Bx\rangle|^{\frac{1}{2}}$ for all $x \in \mathcal{H}$, [22]). Two operators S and T are said to be nearly equivalent if there exists an invertible operator V such that $S^*S = V^{-1}T^*TV$.

Clearly similarity, unitary equivalence, near-equivalence and metric equivalence are equivalence relations on $B(\mathcal{H})$.

Definition 1.2.3. An operator $T \in B(\mathcal{H})$ is said to be:

self-adjoint if $T = T^*$,

normal if $T^*T = TT^*$,

unitary if $T^*T = TT^* = I$, where I denotes the identity operator,

a projection if $T = T^*$ and $T^2 = T$,

an isometry if $T^*T = I$,

a co-isometry if $TT^* = I$,

a partial isometry if $T * TT^* = T^*$ or $TT^*T = T$,

a scalar if $T = \alpha I$, where $\alpha \in \mathbb{C}$.

Definition 1.2.4. An operator $T \in B(\mathcal{H})$ is said to be positive if it is self-adjoint and that $\langle Tx, x\rangle \geq 0$, for all $x \in \mathcal{H}$.

Definition 1.2.5. A field $\mathbb{F}$ is said to be algebraically closed if the only irreducible polynomials in the polynomial ring $\mathbb{F}[x]$ are those of degree one, or every polynomial over $\mathbb{F}$ factors completely into linear factors.

Definition 1.2.6. Let $T \in B(\mathcal{H})$. If there exists an operator $T^D \in B(\mathcal{H})$ satisfying the following three operator equations

$$TT^D = T^DT,\ T^DTT^D = T^D,\ T^{k+1}T^D = T^k,$$

where $k = ind(T)$, the index of T, which is the smallest non-negative integer for which $Ran(T^{k+1}) = Ran(T^k)$ and $Ker(T^{k+1}) = Ker(T^k)$, then T^D is called the Drazin inverse of T.

The Drazin inverse of an operator T is a generalized inverse and if T is invertible, then its inverse is equal to its Drazin inverse. That is, $T^{-1} = T^D$.

Definition 1.2.7. A group is a set G, together with a binary operation $*$ that is closed, associative under $*$ and has an identity element and an inverse element for every element in G.

Remark. The group of operators $\mathcal{U} = \{U_{n\times n} : U^*U = UU^* = I\}$ is called the unitary group, and is denoted by $SU(n)$.

Definition 1.2.8. A plaintext is a message to be communicated. A ciphertext is a disguised version of a plaintext message.

Definition 1.2.9. The process of creating a ciphertext from a plaintext is called encryption. The process of turning a ciphertext back into plaintext is called decryption.

Definition 1.2.10. The process of changing plaintext to bits(usually numbers) is called encoding. Decoding turns bits or numbers back into plaintext.

Definition 1.2.11. A signal is a formal description of a physical phenomenon evolving over time or space.

Signal is a physical phenomenon that carries information. This physical phenomenon is described by mathematical functions, and usually the signal and its mathematical function are used for one another, i.e., synonymous. For instance, when we talk about a sinusoidal signal, we use the sinusoidal function, a mathematical function, to characterize the signal, and the name sinusoidal is used for the signal. Signals are usually depicted in graphs to observe their behavior and analyze them. Sinusoidal signals are the main signals and all the other signals can be considered as being made up of sinusoidal signals with different frequencies and amplitudes.

Definition 1.2.12 ([24])**.** Signal processing generally is any manual or electronical/mechnical operation that involves a prescribed manipulation(modification, analysis or otherwise, of information contained in a signal) of signals in order to achieve some useful goal such as communication, compression, information extraction, information enhancing, and storage.

Digital signals are obtained from continuous time signals via sampling operation. Digital signals are represented as mathematical sequences, and the elements of these sequences are nothing but the amplitude values taken from continuous time signals at every multiple of the sampling period.

Definition 1.2.13. A frame is a sequence of vectors $\{f_i\}$ for a Hilbert space $\mathcal{H}$ for which there exist constants $0 < \alpha \leq \beta < \infty$ such that for all vectors $f \in \mathcal{H}$

$$\alpha \|f\|^2 \leq \sum_i |\langle f, f_i \rangle|^2 \leq \beta \|f\|^2.$$

Remark. The constants α and β are called the lower and upper frame bounds, respectively. They are, respectively, the smallest and largest eigenvalues of the frame operator S. The numbers $(\langle f, f_i \rangle)$ are called the frame coefficients. A frame is a redundant or over-complete(i.e. not linearly independent) coordinate system for a vector space that satisfies the Parseval-type norm inequality. A set of vectors in a finite dimensional Hilbert space is a frame if and only if it is (just) a spanning set.

Definition 1.2.14. Let $\{f_i\}_{i=1}^m$ be a frame for $\mathcal{H}^N$. Then a frame $\{g_i\}_{i=1}^m$ is called a dual frame for $\{f_i\}_{i=1}^m$ if

$$f = \sum_{i=1}^m \langle f, f_i \rangle g_i, \qquad \forall f \in \mathcal{H}^N.$$

Remark. Frames are similar to a basis for a Hilbert space but have a special feature: they contain redundancy that could be used to hide data. Any vector in a Hilbert space can be reconstructed using a frame and its dual.

We define some special operators associated with a frame in Hilbert space.

Definition 1.2.15. Let $\{f_i\}_{i=1}^m$ be a frame for a Hilbert space $\mathcal{H}^N$. The operator $T : \mathcal{H}^N \to \ell_2^m$ defined by $Tf = (\langle f, f_i\rangle)_{i=1}^m$, for all $f \in \mathcal{H}^N$ is called the analysis operator of the frame. The adjoint $T^* : \ell_2^m \longrightarrow \mathcal{H}^N$ of the analysis operator T defined by $T^*(a_i)_{i=1}^m = \sum_{i=1}^m a_i f_i$ is called the synthesis operator of the frame.

The following results give some basic properties of the analysis and synthesis operators of a frame which are necessary in the rest of the thesis.

Lemma 1.2.16. *Let $\{f_i\}_{i=1}^m$ be a frame for $\mathcal{H}^N$ with associated analysis operator T. Then*
(i). $\|Tf\|^2 = \sum_{i=1}^m |\langle f, f_i\rangle|^2, \quad \forall f \in \mathcal{H}^N$.
(ii). $\{f_i\}_{i=1}^m$ is a frame if and only if T is injective.
(iii). $T^*(a_i)_{i=1}^m = \sum_{i=1}^m a_i f_i$.

Proof. (i) and (ii) are immediate consequences of the definition of T and that of a frame.
To prove (iii), suppose that $f, g \in \mathcal{H}^N$. Then

$$\langle T^* f, g\rangle = \langle f, Tg\rangle = \langle \sum_{i=1}^m a_i f_i, (\langle g, f_i\rangle)_{i=1}^m\rangle = \sum_{i=1}^m a_i \overline{\langle g, f_i\rangle} = \langle \sum_{i=1}^m a_i f_i, g\rangle.$$

This proves the claim.

The next result summarizes some basic, yet useful properties of the synthesis operator of a frame.

Lemma 1.2.17. *Let $\{f_i\}_{i=1}^m$ be a frame for $\mathcal{H}^N$ with associated analysis operator T and let $\{e_i\}_{i=1}^m$ be the standard basis for ℓ_2^m. Then*
(i). $T^* e_i = T^* P e_i = f_i$, where $P : \ell_2^m \longrightarrow \ell_2^m$ denotes the orthogonal projection onto $Ran(T)$.
(ii). $\{f_i\}_{i=1}^m$ is a frame if and only if T^* is surjective.

Proof. The proof of (i) follows from Lemma 1.2.16 and the fact that $Ker(T^*) = Ran(T)^\perp$.
(ii). is a consequence of the fact that $Ran(T^*) = Ker(T)^\perp$ and Lemma 1.2.11 (i) and (ii).

Remark. The analysis and synthesis operators of a frame play a central role in the analysis, reconstruction and recovery of any function or signal $f \in \mathcal{H}^N$. The analysis operator, as the name suggests- analyzes a signal $f \in \mathcal{H}^N$ in terms of the frame by computing its frame coefficients $(\langle f, f_i\rangle)_{i=1}^m$.

Often frames are modified by the application of an invertible operator, which multiplies all its frame vectors. The next result shows not only the impact on the associated analysis operator, but also the fact that the new sequence again forms a frame.

Proposition 1.2.18 (Njagi et al[18], Proposition 3). *Let $\Phi = \{f_i\}_{i=1}^m$ be a sequence of vectors in $\mathcal{H}^N$ with associated analysis operator T_Φ and let $F : \mathcal{H}^N \longrightarrow \mathcal{H}^N$ be a bounded linear operator. Then the analysis operator of the sequence $F\Phi = \{Ff_i\}_{i=1}^m$ is given by $T_{F\Phi} = T_\Phi F^*$. Moreover, if Φ is a frame for $\mathcal{H}^N$ and F is invertible, then $F\Phi$ is also a frame for $\mathcal{H}^N$.*

Proof. For any $f \in \mathcal{H}^N$ we have

$$TF_\Phi f = (\langle f, Ff_i\rangle) = \langle F^* f, f_i\rangle_{i=1}^m = T_\Phi F^* f.$$

This proves that $TF_\Phi = T_\Phi F^*$. The second claim follows easily from Lemma 1.2.17(ii).

Next, we analyze the structure of the matrix representation of the synthesis operator. This matrix is of fundamental importance, since this is what frame re-constructions focusses on. The next result provides the form of this matrix along with its stability properties.

Lemma 1.2.19 (Njagi et al [18], Lemma 4). *Let $\{f_i\}_{i=1}^m$ be a frame for $\mathcal{H}^N$ with analysis operator T. Then a matrix representation of the synthesis operator T^* is the $N \times m$ matrix whose columns are the frame vectors given by*

$$T^* = \begin{bmatrix} | & | & \cdots & | \\ f_1 & f_2 & \cdots & f_m \\ | & | & \cdots & | \end{bmatrix}.$$

Moreover, the Riesz bounds of the row vectors of this matrix equal the frame bounds of the column vectors.

Proof. The form of the matrix representation is obvious. To prove the moreover part, let $\{e_j\}_{j=1}^N$ be the corresponding orthonormal basis of $\mathcal{H}^N$. Let

$$\psi_j = [\langle f_1, e_j\rangle, \langle f_2, e_j\rangle, \cdots, \langle f_m, e_j\rangle]$$

be the row vectors of the matrix. Then for $f = \sum_{j=1}^N a_j e_j$ we obtain

$$\sum_{i=1}^m |\langle f, f_i\rangle|^2 = \sum_{i=1}^m \sum_{j=N}^m a_j \langle e_j, f_i\rangle = \sum_{j,k=1}^N a_j \overline{a_k} \sum_{i=1}^m \langle e_j, f_i\rangle\langle f_i, e_k\rangle = \sum_{j,k=1}^N a_j \overline{a_k} \langle \psi_k, \psi_j\rangle = \|\sum_{j=1}^N \overline{a_j}\psi_j\|^2.$$

This proves the claim.

Definition 1.2.20. Let $\{f_i\}_{i=1}^m$ be a sequence of vectors in $\mathcal{H}^N$ with associated analysis operator

T. Then the operator $S : \mathcal{H}^N \longrightarrow \mathcal{H}^N$ is defined by

$$Sf = T^*Tf = \sum_{i=1}^{m} \langle f, f_i \rangle f_i, \quad \forall f \in \mathcal{H}^N,$$

is called the frame operator of the sequence.

From the definition, we deduce that the frame operator $S = T^*T$, where T is the analysis operator of the sequence. A first observation concerning the close relationship of the frame operator to frame properties is the following lemma.

Lemma 1.2.21 (Njagi et al[18], Njagi et al[21]). *Let $\{f_i\}_{i=1}^m$ be a sequence of vectors in $\mathcal{H}^N$ with associated frame operator S. Then for $f \in \mathcal{H}^N$,*

$$\langle Sf, f \rangle = \sum_{i=1}^{m} |\langle f, f_i \rangle|^2.$$

Proof. The proof follows directly from the fact that

$$\langle Sf, f \rangle = \langle T^*Tf, f \rangle = \langle Tf, Tf \rangle = \|Tf\|^2 = \sum_{i=1}^{m} \langle f, f_i \rangle \langle f_i, f \rangle = \sum_{i=1}^{m} \langle f, f_i \rangle \overline{\langle f, f_i \rangle} = \sum_{i=1}^{m} |\langle f, f_i \rangle|^2.$$

Clearly, the frame operator $S = T^*T$ is positive and invertible if the underlying sequence of vectors form a frame.

Theorem 1.2.22. *If a bounded linear operator S is a frame operator, then S is invertible.*

Proof. Suppose S is the frame operator of a frame $\{f_k\}_{k=1}^n$ for a Hilbert space $\mathcal{H}$. Since $S = A^*A$ is self-adjoint, where A is the analysis operator of $\{f_k\}_{k=1}^n$, it is enough to prove that if $f \in \mathcal{H}$ and $Sf = 0$ then $f = 0$. Suppose that $Sf = 0$. Then by definition

$$\begin{aligned} 0 = \langle Sf, f \rangle &= \langle \textstyle\sum_{k=1}^n \langle f, f_k \rangle, f \rangle \\ &= \textstyle\sum_{k=1}^n \langle f, f_k \rangle \langle f_k, f \rangle \\ &= \textstyle\sum_{k=1}^n \langle f, f_k \rangle \overline{\langle f, f_k \rangle} \\ &= \textstyle\sum_{k=1}^n |\langle f, f_k \rangle|^2 \end{aligned}$$

This implies that $\langle f, f_k \rangle = 0$ for all $k = 1, 2, \cdots, n$, which means that $f = 0$. This shows that S is injective. Since $\{f_k\}_{k=1}^n$ is a frame, by Lemma 1.2.17 A^* is surjective. Therefore $Ran(S) = Ran(A^*A) = Ran(A^*) = \mathcal{H}$. This proves that S is surjective. This proves the claim.

Remark. The invertibility of S and that of its inverse S^{-1} is crucial for the reconstruction formula.

Proposition 1.2.23 (Frame Reconstruction/Reproducing Formula, Njagi et al[21], Proposition 3.8)**.** *Let $\{f_i\}$ be a frame for a Hilbert space $\mathcal{H}$ with analysis operator T and frame operator $S = T^*T$. Then*

$$f = \sum_i \langle S^{-1}f, f_i\rangle = \sum_i \langle f, S^{-1}f_i\rangle f_i = \sum_i \langle f, f_i\rangle S^{-1}f_i, \quad \forall f \in \mathcal{H}.$$

Proof. Let $f \in \mathcal{H}$. By definition and self-adjointness of the frame operator S, we have

$$f = SS^{-1}f = \sum_k \langle S^{-1}f, f_i\rangle f_i = \sum_i \langle f, S^{-1}f_i\rangle f_i.$$

Similarly,

$$f = S^{-1}Sf = S^{-1}\sum_i \langle f, f_i\rangle f_i = \sum_i \langle f, f_i\rangle S^{-1}f_i.$$

This proves the claim.

Theorem 1.2.24 (Njagi et al[18], Theorem 6)**.** *The frame operator S of a frame $\{f_i\}_{i=1}^{M}$ for $\mathcal{H}^N$ with frame bounds is invertible and satisfies*

$$\alpha I \leq S \leq \beta I.$$

Proof. By Lemma 1.2.21 we have

$$\langle \alpha f, f\rangle = \alpha\|f\|^2 \leq \sum_{i=1}^{m} |\langle f, f_i\rangle|^2 = \langle Sf, f\rangle \leq \beta\|f\|^2, \;\; \forall f \in \mathcal{H}^N.$$

This implies the claimed inequality.

Chapter 2

LITERATURE REVIEW

The Fourier transform has been a major tool in signal processing for over 100 years. However, it solely provides frequency information, hides(in its phases) information concerning the moment of emission and duration of a signal.

In 1946, Gabor[11] resolved this problem by introducing a fundamentally new approach to signal decomposition. Gabor's approach quickly became the paradigm for this area because it provided resilience to additive noise, quantization, and transmission losses as well as ability to capture signal characteristics.

In 1952, Duffin and Schaeffer[10] were studying some deep problems in non-harmonic Fourier series for which they required a formal structure for working with highly over-complete families of exponential functions in the Hilbert space $L^2[0,1]$. For this, they introduced the notion of a Hilbert space frame in which Gabor's approach is now a special case, falling into the area of time-frequency analysis.

Much later, in 1986, Daubechies et al[9] revived the fundamental concept of frames and resolved its importance in data processing. In 2004, Miotke and Rebollo-Neira[17] published a theoretical private key encryption scheme using infinite frames and over-sampling of Fourier coefficients.

Cryptography is the art or science of hiding data and it relies heavily on invertible mathematical functions or operators. Mathematicians have explored a plethora of mathematical concepts in their quest to develop an unbreakable system. In 1977, Rivest, Shamir, and Adleman proposed a trapdoor function which resulted in a public-key cryptosystem, called RSA. The function was

$$RSA(n,e,x) = x^e \ mod \ n,$$

where n is the product of two large primes p and q and $gcd(e, \varphi(n)) = 1$, where $\varphi(n)$ denotes Euler's (totient) function defined by $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.
In 2005, Harkins et al[12] published a set of private key encryption schemes using finite frames and Hadamard arrays. Both of these schemes use the same frame theory structure. It is always important that once a cryptosystem is developed, it be tested for vulnerable attack.

In 2005, Harkins et all[12] showed that their system was vulnerable to a chosen ciphertext attack. Later, in 2006, Osvik et al[23] published paper showing that the general cryptosystem used by Mioke and Rebello-Neira[17] was vulnerable to a known plaintext attack.

In this thesis, we have used the redundancy of finite frames in an N-dimensional Hilbert space and some techniques in number theory and group theory to show how to send and reconstruct signals and how to hide information.

2.1 Statement of the Problem

We investigated some application of operator theory and group theory concepts in signal processing and cryptography. First, we have developed some finite frame theory and investigated properties of some frames. We have investigated and demonstrated how notions of divisibility, non-divisibility and modular arithmetic can be utilized to hide data or information.

2.2 Objectives of the Study

The main objective is to develop the abstract theory of finite frames and group theory and demonstrate some of the applications in signal processing and cryptography.

The specific objectives of this study are

(i). Given a frame, determine the analysis, synthesis and the frame operator, a dual frame, canonical dual.

(ii). To explore and further develop the abstract theory of finite Hilbert space frames, their properties.

(iii). To explore prime numbers, divisibility and modular arithmetic and how they can be used to design cryptosystems. Our focus will be to demonstrate how these concepts work. We focus on the working of the RSA.

(iv). Demonstrate how we can still reconstruct, encode and decode information securely, even after dropping some vectors in an over-complete frame.

(v). Demonstrate some applications of frame theory and group theory in signal processing and cryptography.

2.3 Significance of the Study

This study will generalize some existing results on Hilbert space frames and cryptography and will contribute significantly to a better understanding of how to send, reconstruct, encrypt and decrypt messages or signals.

The results obtained in this research will broaden the scope of understanding of frame theory and positively contribute to the mathematics and the scientific community.

Chapter 3

VECTOR SPACE THEORY AND GROUP THEORY CONCEPTS

In this chapter we explore some basic vector space and group theory concepts of importance in the rest of the chapters of this thesis.

3.1 Elementary Vector Space theory

In this section, we study vector spaces and their properties. The following definitions and results will be useful in the sequel.

Definition 3.1.1. A vector over a field $\mathbb{F}$ is a set V with two operations, $+$ addition of vectors $(x, y) \longrightarrow x + y$ and . multiplication by scalar function $(\lambda, x) \longrightarrow \lambda x$ from $\mathbb{F} \times V$ to V defined on it and satisfying some axioms.

The elements of a vector space are called vectors.

Definition 3.1.2. Let V be a vector space over $\mathbb{F}$. A subset U of V is called a subspace of V if it is a vector space itself over $\mathbb{F}$ under the same operations that make V a vector space over $\mathbb{F}$.

Definition 3.1.3. Let V be a vector space over a scalar field $\mathbb{F}$ and let $f_1, f_2, \cdots, f_n$ vectors in V. The finite sum

$$\sum_{k=1}^{n} a_k f_k$$

for some scalars $a_1, a_2, \cdots, a_n$ is called a linear combination of the vectors $f_1, f_2, \cdots, f_n$.

Definition 3.1.4. Let V be a vector space over a scalar field $\mathbb{F}$ and $\mathcal{M}$ be a subset of V. The span of $\mathcal{M}$ is the set

$$span(\mathcal{M}) = \Big\{ \sum_{k=1}^{n} a_k f_k : n \in \mathbb{N}, a_i \in \mathbb{C} \; and \; f_i \in \mathcal{M} \Big\}.$$

Definition 3.1.5. Let V be a vector space over a scalar field $\mathbb{F}$. We say that vectors $f_1, f_2, \cdots, f_n$ be vectors in V are linearly independent if from

$$\sum_{k=1}^{n} a_k f_k = 0$$

one can conclude that $a_1 = a_2 = \cdots = a_n = 0$.

Remark. Clearly, vectors $f_1, f_2, \cdots, f_n$ are linearly independent if no vector f_k is a linear combination of the other vectors. We call an infinite number of vectors$\{f_k\}_{k=1}^{\infty}$ linearly independent if every finite subset $\{f_k\}_{k=1}^{n}$, where $n < \infty$ of those vectors is linearly independent.

Definition 3.1.6. Let V be a vector space over a scalar field $\mathbb{F}$. We say that vectors $f_1, f_2, \cdots, f_n$ in V are linearly dependent if there exists scalars $a_1, a_2, \cdots, a_n$ not all equal to zero such that the linear combination

$$\sum_{k=1}^{n} a_k f_k = 0.$$

Remark. Trivially, any list of vectors that includes the zero vector in a vector space V is linearly dependent.

Definition 3.1.7. Let X be a non-empty set. A metric on X is a distance function $d : X \times X \longrightarrow \mathbb{R}^+$, that satisfies the following properties
(i). $d(x, y) \geq 0$.
(ii). $d(x, y) = 0$ if and only if $x = y$.
(iii). $d(x, y) = d(y, x)$.
(iv). $d(x, z) \leq d(x, y) + d(y, z)$, for every $x, y, z \in X$.

The set X, when equipped with a metric d, and denoted by (X, d) is called a metric space. A distance function ρ satisfying properties (i), (iii) and (iv) of a metric and that $\rho(x, y) = 0$ for some $x \neq y$ is called a pseudo-metric. Clearly every metric is a pseudo-metric.

Definition 3.1.8. Let V be a complex vector space. A function $\|.\| : V \longrightarrow \mathbb{R}^2$ satisfying the following properties
(i). $\|f\| \geq 0$
(ii). $\|f\| = 0$ if and only if $f = 0$.

(iii). $\|\alpha f\| = |\alpha|\|f\|, \forall f \in V,\ \forall \alpha \in \mathbb{C}$.
(iv). $\|f+g\| \leq \|f\| + \|g\|, \forall f, g \in V$
is called a norm. A vector space V with a norm is called a normed space. A complete normed space is called a Banach space.

Definition 3.1.9. Let V be a complex vector space. A complex bilinear function $\langle ., . \rangle : V \times V \longrightarrow \mathbb{C}$ is called an inner product if for any $f, f_1, f_2, g, g_1, g_2 \in V$ and $\alpha_1, \alpha_2 \in \mathbb{C}$, the following conditions are satisfied.
(i). $\langle f, f \rangle \geq 0$.
(ii). $\langle f, f \rangle = 0$ if and only if $f = 0$.
(iii). $\langle \alpha_1 f_1 + \alpha_2 f_2, g \rangle = \alpha_1 \langle f_1, g \rangle + \alpha_2 \langle f_2, g \rangle$.
(iv). $\langle f, g \rangle = \overline{\langle g, f \rangle}$ and $\langle f, \alpha_1 g_1 + \alpha_2 g_2 \rangle = \overline{\alpha_1} \langle f, g_1 \rangle + \overline{\alpha_2} \langle f, g_2 \rangle$. A vector space V endowed with an inner product is called an inner product space. A complete inner product space is called a Hilbert space.

Given an inner product $\langle ., . \rangle$ in a vector space V, induce norm is defined as

$$\|f\| = \langle f, f \rangle^{1/2}, \qquad \forall f \in V.$$

Theorem 3.1.10 (Cauchy-Schwarz Inequality)**.** *For any two vectors f, g in an inner product space $\mathcal{H}$, we have*

$$|\langle f, g \rangle| \leq \|f\|\|g\|.$$

Definition 3.1.11. Two vectors $f, g \in \mathcal{H}$ are said to be orthogonal if $\langle f, g \rangle = 0$. If in addition they have the additional property $\|f\| = \|g\| = 1$, then they are called orthonormal vectors. A subset X of non-zero vectors in a Hilbert space $\mathcal{H}$ is called an orthonormal set if

$$\langle f_i, f_j \rangle = \begin{cases} 1, & if\ i = j \\ 0, & otherwise \end{cases}, \quad f_i \in X.$$

Remark. In Definition 3.1.11, the subset X can be finite, countably infinite or even uncountably infinite. When X is countably infinite, then it can be arranged in a sequence and we now refine the definition using the Kronecker delta function

$$\delta_{n,m} = \begin{cases} 1, & when\ m = n \\ 0, & otherwise \end{cases}.$$

This leads to the following definition of an orthonormal sequence.

Definition 3.1.12. A sequence of non-zero vectors $\{f_n\}_{n=1}^{\infty}$ in a Hilbert space $\mathcal{H}$ is called an orthonormal sequence if $\langle f_m, f_n \rangle = \delta_{n,m}$, for all $m, n \in \mathbb{N}$.

3.2 Group Theory and the RSA Encryption System

In this section we discuss one of the main methods of encrypting data, the RSA encryption system. This system has an algebraic structure of a group. The RSA encryption system was invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman[25], and is one of the most common methods of encrypting data used today.

First we introduce the notion of prime numbers, divisibility, congruence calculus and modular arithmetic.

Definition 3.2.1. An integer $x \geq 2$ with only trivial factors ± 1 and $\pm x$ is called a prime number. If an integer $y \geq 2$ is not a prime, it is called composite.

Definition 3.2.2 (Congruences)**.** Given three numbers a, b and m, we say that "a is congruent to b modulo m" and write $a \equiv b \ mod \ m$ if the difference $a - b$ is divisible by m. Here, m is called the modulus of the congruence.

Clearly, for a fixed modulus m, the congruence modulo m is an equivalence relation. For fixed m, each equivalence class with respect to congruence modulo m has one and only one representative between 0 and $m - 1$. This is equivalent to saying that any integer is congruent modulo m to one and only one integer between 0 and $m - 1$. We will denote the set of equivalence classes or residue classes by $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$. Clearly, congruences with the same modulus can be added, subtracted and multiplies: If $a \equiv b \ mod \ m$ and $c \equiv d \ mod \ m$, then $a \pm c \equiv b \pm d \ mod \ m$ and $ac \equiv bd \ mod \ m$ Clearly, $\mathbb{Z}_m$ is a commutative ring. In fact, $\mathbb{Z}_m$ is a field.

Theorem 3.2.3. *(a).([15]) If $a \equiv b \ mod \ m$, then $a \equiv b \ mod \ d$ for any divisor d of m.*
(b). If $a \equiv b \ mod \ m$ and $a \equiv b \ mod \ n$, and m and n are relatively prime(i.e. $gcd(m, n) = 1$), then $a \equiv b \ mod \ mn$.

Remark. The idea of congruence calculus is that computation is only done with the remainders of integers using a fixed divisor or modulus $m \geq 1$.

Definition 3.2.4. A function f which is easy to compute but for which f^{-1} is hard to compute without having some auxiliary information beyond what is necessary to compute f is called a *trapdoor function.*

We note that for a trapdoor function, the inverse f^{-1} is easy to compute, however, for someone who has the decrypting key. The RSA uses a trap-door function.

Definition 3.2.5. A function f which is easy to compute but for which f^{-1} is hard and cannot be made easy to compute even by acquiring some additional information is called a *one-way function.*

There exist a one-way cipher, where it is possible for a computer to verify passwords without storing information that could be used by an intruder to impersonate a legitimate user. This uses the principle of a one-way function.

To describe the RSA system, we start with the following data:

-distinct prime numbers p and q.
-an integer e relatively prime to $(p-1)(q-1)$.

The trap-door function is

$$RSA(n, e, x) = x^e \; mod \; n,$$

where n is a product of two large primes p and q and $gcd(e, \varphi(n)) = 1$, where $\varphi(n)$ is Euler's (totient) function defined by $\varphi(n) = \varphi(pq) = (p-1)(q-1)$

From this data we build an encryption system. Let $n = pq$. For convenience and without loss of generality, we restrict our attention to encrypting numbers. This is satisfactory since any text message can be converted to numbers by replacing each letter with an appropriate number. Let M be an integer, considered to be a message we wish to encrypt. We then calculate $M^e \; mod \; n$, the remainder after dividing n into M^e. This remainder is our encrypted message.

Example 3.2.6.

Let $p = 3486784409, q = 282429536483$ and $e = 19$. Then $n = pq = 984770904450021093547$. Also, $(p-1)(q-1) = 984770904164104772656$. To encrypt the message 12345, we calculate $12345^{19} \; mod \; n$, to get 123355218486796132288. Therefore, if we wish to transmit the number 12345, we would instead transmit 123355218486796132288. For the person receiving 123355218486796132288, the question is how to know that it represents 12345. First, our assumption that e is relatively prime to $(p-1)(q-1)$, we know that e has an inverse modulo $(p-1)(q-1)$. That is, there is an integer d with

$$ed \equiv 1 \; mod \; (p-1)(q-1).$$

If an encrypted number N is received, then one calculates $N^d \; mod \; n$ and the result returns the original message. In this example, Maple computation gives $d = 207320190350337846875$. Thus to recover the original message 12345, we compute

$$123355218486796132288^{207320190350337846875} \; mod \; 984770904450021093547 = 12345.$$

Remark. While this calculation looks formidable, Maple can do it virtually instantaneously. In

fact, on an average personal computer, Maple can calculate M^d *mod* n in a couple of seconds even if d and n are 400 digit numbers, so the calculations in RSA system are easy to do even with very large numbers.
To summarize, the RSA encryption system starts with two prime numbers p and q an an integer e satisfying $gcd(e, (p-1)(q-1)) = 1$. We then calculate a positive integer d satisfying $ed \equiv 1 \ mod \ (p-1)(q-1)$. We then encrypt an integer M by replacing it by $N = M^e \ mod \ n$. To decrypt N, we see that $M = N^d \ mod \ n$.

The reason why this method works will be addressed in our study of group theory. The theoretical fact that the inventors of the RSA system needed was Euler's theorem, which is a special case of Lagrange's theorem.

Definition 3.2.7. A group is a nonempty set G together with a binary operation $*$ on it that makes it closed, associative, there is an identity element such that every element in G has an inverse in G.

Proposition 3.2.8. *If $a \equiv b \ (mod \ m)$, then $an \equiv bn \ (mod \ m)$ for any positive integer n.*

Proof. Since $a \equiv b \ (mod \ m)$, we can multiply the congruence by itself to get $a^2 \equiv b^2 \ (mod \ m)$. Continuing to multiply, we get $an \equiv bn \ (mod \ m)$ for any positive integer n.

Remark. Being able to compute $a^n \ (mod \ m)$ for large values of n is extremely important in cryptographic applications. This process is known as modular exponentiation.

To encrypt a message using the RSA cryptosystem, we first convert the plaintext into a list of nonnegative integers. In this chapter, we will again assume that all messages are written using only the characters in the alphabet $L = \{A, B, C, ..., Z\}$, and associate each of these characters with their corresponding elements in the ring $R = \mathbb{Z}_{26}$ under the bijection $\psi : L \longrightarrow R$ given by

$$A \longmapsto 0, B \longmapsto 1, C \longmapsto 2, \cdots, Z \longmapsto 25.$$

We then choose distinct primes p and q and let $n = pq$ and $m = (p-1)(q-1)$(Here $\varphi(n) := m$, where φ is Euler's function?). Next, we choose $a \in \mathbb{Z}_m$ with $gcd(a, m) = 1$, and find $b \in \mathbb{Z}_m$ that satisfies $ab = 1 \ mod \ m$). To encrypt a numerical plaintext message, we raise the plaintext integers to the power a and reduce modulo n.

We note that the RSA is based on the tremendous difficulty of factoring. One chooses two extremely large prime numbers p, q(say of 100 digits each) and lets $n = pq$. Knowing the factorization of n, it is easy to compute $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$. Next, one randomly[using a random number generator or computer program, of course] chooses a number e between 1 and $\varphi(n)$ which is relatively prime to $\varphi(n)$

We state the next case as a lemma.

Lemma 3.2.9. *Let p and q be distinct primes. Then $\varphi(pq) = (p-1)(q-1)$.*

Proof. Set $n = pq$. To count $\varphi(n)$, we first count the number of integers between 1 and n and not relatively prime to n. If $1 \leq a \leq n$, then $gcd(a, n) > 1$ only if p divides a or q divides a. The multiples of p between 1 and and n are then

$$p, 2p, \cdots, (q-1)p, qp = n,$$

so that there are q multiples of p between 1 and n. The multiples of q in this range are

$$q, 2q, \cdots, (p-1)q, pq = n,$$

so that there are p multiples of q in this range. The only number on both lists is n. This follows from unique factorization. Therefore, there are $p + q - 1$ integers between 1 and n that are not relatively prime to n. Since there are $n = pq$ numbers in this range, we see that

$$\varphi(n) = pq - (p + q - 1) = pq - p - q + 1 = p(q-1) - (q-1) = (p-1)(q-1),$$

as desired.

To summarize, the group $\mathbb{Z}_n^*$ has $\varphi(n)$ elements, and if $n = pq$ is the product of two Disney primes, then $\mathbb{Z}_{pq}^*$ has $(p-1)(q-1)$ elements. The significance of this result and its application to the RSA encryption system will become clear when we prove Lagrange's theorem. To do this, we first discuss subgroups.

Definition 3.2.10. Let G be a group. A nonempty subset H of G is said to be a subgroup of G if the operation on G restricts to an operation on H, and if H is a group with respect to this restricted operation.

Lemma 3.2.11. *A nonempty set H of a group G is a subgroup if and only if it is closed under the operation inherited from G and the inverse of every element in H is also in H.*

Remark. If G is a group and $a \in G$, then the cyclic subgroup generated by a is the set

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

To formally define a^n, we first define $a^0 = e$, the identity of G. If n is a positive integer, then we define, inductively, $a^{n+1} = a^n.a$. For negative exponents, if $n > 0$, we set $a^{-n} = (a^n)^{-1}$. Clearly,

$\langle a \rangle$ is a subgroup of G by Lemma 3.2.11.

Lemma 3.2.12. *Let G be a finite group and let $a \in G$. If $n = \min\{m : m > 0, a^m = e\}$, then $n = |\langle a \rangle|$, the number of elements in the cyclic subgroup generated by a.*

Proof. We prove the claim by showing that $\langle a \rangle = \{a^r : 0 \leq r < n\}$ and that these elements are all distinct. First, any element of $\langle a \rangle$ is of the form a^s for some integer s. By the division algorithm, we may write $s = qn + r$, with $0 \leq r < n$. Then

$$a^s = a^{qn+r} = a^{qr} a^r = (a^n)^q a^r = a^r,$$

since $a^n = e$, so $(a^n)^q = e$. Therefore, a^s can be written as a power a^r of a with $0 \leq r < n$. This proves the first claim. For the second claim, suppose that $a^r = a^t$ with $0 \leq r, t < n$. Suppose that $r \leq t$. Then, by the laws of exponents, $e = a^t a^{-r} = a^{t-r}$. Since n is the smallest positive integer satisfying $a^m = e$, and since $0 \leq r, t < n$, we must have $t - r = 0$. Thus, $t = r$. So the elements $a^0, a^1, \cdots, a^{n-1}$ are all distinct. Since these elements form $\langle a \rangle$, we conclude that $|\langle a \rangle| = n$.

We now consider Lagrange's theorem. First, we note that if H is a subgroup of a group $(G, *)$ and if $a \in G$, then the coset of H generated by a is the set

$$Ha = \{ha : h \in H\}.$$

Remark. Cosets are equivalence classes for the following equivalence relation: for $a, b \in G$, define $a \sim b$ if $ab^{-1} \in H$. Clearly, $\sim$ is an equivalence relation and the equivalence class of a is the coset Ha. This means that the cosets of H form a partition for the group G.

Theorem 3.2.13 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. Then $|H|$ divides $|G|$.*

Proof. It suffices to show that each coset has $|H|$ elements, which means that $|G|$ is equal to $|H|$ times the number of cosets. To do this, let $a \in G$. We wish to prove that $|Ha| = |H|$. One way to prove that two sets have the same size is to produce a one-to-one correspondence(one-to-one and onto map) between them. We define a function $f : H \longrightarrow Ha$ by $f(h) = ha$. Clearly f is one-to-one since if $f(h) = f(k)$, then $ha = ka$. Multiplying both sides on the right by a^{-1} yields $h = k$. The function f is also onto since if $x \in Ha$, then $x = ha$ for some $h \in H$, and so $x = f(h)$. Since f is a one-to-one correspondence(on-to-one and onto map) from H onto Ha, we conclude that $|Ha| = |H|$, as desired.

Remark. Combining Lemma 3.2.12 and Theorem 3.2.13[Lagrange], we get a result in the RSA encryption system.

Corollary 3.2.14. *Let G be a finite group with $n = |G|$. If $a \in G$, then $a^n = e$.*

Proof. Let $m = |\langle a \rangle|$. By Theorem 3.2.13(Lagrange's Theorem), m divides n, so $n = mt$ for some integer t. By Lemma 3.2.12, $a^m = e$. Therefore, $a^n = a^{mt} = (a^m)^t = e^t = e$, as desired.

A special consequence of Corollary 3.2.14 is Euler's theorem. Recall that Euler's (totient) function $\varphi(m)$ gives the count of those integers x in the intervals $1 \leq x \leq m$ for which $gcd(x, m) = 1$. That is

$$\varphi(m) = |\{x : 1 \leq x \leq m \ \ and \ \ gcd(x, m) = 1\}| = |\mathbb{Z}_m^*|.$$

This is the number of reduced residue classes modulo m in the multiplicative group $\mathbb{Z}_m^* = \{1, 2, ..., m - 1\}$ (called the group of units) of $\mathbb{Z}_m$. It is a convention that $\varphi(1) = 1$. Note that all elements $\alpha \in \mathbb{Z}_m^*$ have the property that $gcd(\alpha, m) = 1$. This means we can find α^{-1} mod m, their inverses modulo m. Euler's (totient) function will be needed in the RSA cryptosystem.

Theorem 3.2.15. *(a). If p is a prime and $k \geq 1$, then $\varphi(p^k) = p^{k-1}(p - 1)$. In particular, $\varphi(p) = p - 1$.*
(b). If $gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

The following results prove useful in the sequel(For more literature on prime numbers and modular arithmetic see Kraft and Washington[16]).

Theorem 3.2.16 (Euler's Theorem). *Let n be a positive integer. If a is an integer with $gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1$ mod n.*

Proof. If $gcd(a, n) = 1$, then $\bar{a} \in \mathbb{Z}_n^* = \{1, 2, ..., n - 1\}$, a group of order $\varphi(n)$. By Corollary 3.2.14, we have $\bar{a}^{\varphi(n)} = \bar{1}$. By definition of coset multiplication, we have $\bar{a}^{\varphi(n)} = \overline{a^{\varphi(n)}}$. The equation $\overline{a^{\varphi(n)}} = \bar{1}$ is equivalent to the relation $a^{\varphi(n)} \equiv 1$ mod n.

Euler's Theorem is often useful when we compute powers modulo n. A consequence of Euler's Theorem is the following result.

Theorem 3.2.17 (Fermat's Little Theorem). *If p is a prime and x is not divisible by p, then $x^{p-1} \equiv 1$ mod p.*

Note that when $n = p$ is prime, Euler's Theorem is the same as Fermat's Little Theorem. If the factors of the modulus m are known, that is if we can write $m = m_1m_2...m_k$, the congruences $x \equiv y$ mod m_i $(i = 1, 2, ..., k)$ naturally follow from $x \equiv y$ mod m. If the modulus is a large number, it may often be easier to compute these smaller moduli. We note that this becomes even easier if the factors are pairwise co-prime, that is, if $gcd(m_i, m_j) = 1$, when $i \neq j$.

The above remark leads to the Chinese Remainder Theorem.

Theorem 3.2.18 (Chinese Remainder Theorem). *If the numbers $y_1, y_2, ..., y_k$ are given and the moduli $m_1, m_2, ..., m_k$ are pairwise co-prime, then there is a unique integer x modulo $m_1 m_2 ... m_k$ that satisfies the k congruences $x \equiv y_i \ mod \ m_i \quad (i = 1, 2, ..., k)$.*

Remark. We have laid the foundation and are now in a position to see how group theory will tell us that the method of decrypting in the RSA system recovers the original message.

Let $G = \mathbb{Z}_n^*$, where $n = pq$ is the product of two distinct (large) prime numbers. Using the Euler (totient) function, $|G| = \varphi(n) = (p-1)(q-1)$. We have an integer e (the decrypting exponent) satisfying $gcd(e, \varphi(n)) = gcd(e, (p-1)(q-1)) = 1$. RSA's secret key k_s consists of n and e). The public key k_p is formed of the number $n = pq$ (multiplied out) and the integer d (called the encrypting exponent) satisfying

$$ed \equiv 1 \ mod \ \varphi(n).$$

We may write $1 = ed + s\varphi(n)$, for some integer s. The claim of the RSA system is that, for any message M, we have $(M^e)^d \ mod \ n = 1$. Written another way, it claims that $(\overline{M}^e)^d = \overline{M}$. Assuming that M is not divisible by p or q, we have $M \in \mathbb{Z}_n^*$. Therefore

$$\overline{M} = \overline{M}^{ed+s\varphi(n)} = \overline{M}^{ed}\overline{M}^{s\varphi(n)} = \overline{M}^{ed}(\overline{M}^{\varphi(n)})^s = \overline{M}^{ed}(\overline{1})^s = \overline{M}^{ed},$$

since $\overline{M}^{\varphi(n)} = 1$ by Corollary 3.2.14. Thus, $(\overline{M}^e)^d = \overline{M}$, and so the decryption RSA recovers the original message.

From the above argument, we have two very important functions of the RSA. The encrypting function is

$$E_{k_p}(M) = (M^d, mod \ n),$$

and the decrypting function is

$$D_{k_s}(C) = (C^e, mod \ n).$$

We note that in our argument, we assume that M was not divisible by either p or q in order to conclude that decryption would recover M. This is not a necessary assumption, but it makes the argument a little simpler.

3.2.1 Secure Signatures with RSA

One issue in data transmission is the ability to verify a person's identity. If a client sends a request to a bank to transfer money out of an account, then the bank would want to know if the client is the owner of the account. If the client makes the request over the internet, how can the bank check his or her identity? The RSA system encryption gives a method for checking identities.

Suppose that person A transmits data to person B, and that person B wants a method to check the identity of person A. To do this, both person A and B get sets of RSA data: person A has a modulus n_A and an encryption exponent e_A, which are publicly available. That person also has a decryption exponent d_A that remains private. Person B similarly has data n_B, e_B and d_B. In addition, Person A has a signature, a publicly available number. To convince person B of his identity, person A first calculates $T = S^{d_A}\ modn_A$ and then $R = T^{e_B}\ modn_B$. Person A then transmits R to person B. Person B then decrypts R with with her data, recovering $T = R^{d_B}\ mod\ n_B$. Finally, she encrypts T with person A's data, obtaining $T^{e_A}\ mod\ n_A = S$. By seeing that this result is the signature of person A, the identity has been validated.

We demonstrate this in an example. We used Maple calling sequence `x mod m` to carry out the heavy modular computation. Of course, this example is not secure, since the numbers are so small that it would be easy for Eve to factor the modulus N. Secure implementations of RSA use moduli N with hundreds of digits.

Example 3.2.19.

Suppose that the data for person A is

$$n_A = 2673157, \quad e_A = 23, \quad d_A = 2437607, \quad S = 837361$$

and person B has

$$n_B = 721864639, \quad e_B = 19823, \quad d_B = 700322447.$$

Person A then calculates

$$837361^{2437606}\ mod\ 2673157 = 1216606,$$

and then

$$1216606^{19823}\ mod\ 721864639 = 241279367.$$

Person A then transmits 241279367 to person B. When person B receives this number, he goes ahead and calculates

$$241279367^{700322447}\ mod\ 721864639 = 1216606,$$

and finally recovers S as

$$S = 1216606^{23} \; mod \; 2673157 = 837361.$$

To explain why this works, we denote by $encrypt_A(M)$ and $dencrypt_A(M)$ the integers $M^{e_A} \; mod \; n_A$ and $M^{d_A} \; mod \; n_A$, respectively. We similarly have $encrypt_B(M)$ and $dencrypt_B(M)$. The validity of the RSA system says that

$$decrypt_A(encrypt_A(M)) = M,$$

$$ecrypt_A(dencrypt_A(M)) = M.$$

Similar equations hold for B. With this notation, Person A calculates

$$R = encrypt_B(decrypt_A)(S)$$

and then Person B calculates

$$S = encrypt_A(decrypt_B(R)).$$

Therefore, person B will calculate

$$encrypt_A(decrypt_B(decrypt_B(decrypt_A(S)))) = encrypt_A(decrypt_A(S)) = S.$$

Therefore, person B does recover the signature of person A.

The reason that this method validates the identity of person A is because only person A can calculate $dencrypt_A(S)$. If another person tries to claim he is person A, or tries to substitute a number F in place of $dencrypt_A(S)$, he will transmit $encrypt_B(F)$ to person B. Person B will then calculate

$$encrypt_A(decrypt_B(encrypt_B(F))) = encrypt_A(F).$$

However, in order to have $encrypt_A(F) = S$, we must have

$$decrypt_A(S) = decrypt_A(encrypt_A(F)) = F,$$

which means that this person has to have the correct decrypted number $decrypt_A(S)$. This means that he cannot send any other number without person B realizing it is a fake number.

We note that all the computation in this section can be implemented on a computer running

Maple 18. The random numbers can be generated using the RandomTools[MersenneTwister] package or library in Maple 18 with the following calling sequence

```
>With(RandomTools[MersenneTwister]):
```

```
>GenerateInteger();
```

A Marsenne number is a number of the form $M_n = 2^n - 1$. For M_n to be prime, n must be prime.

If the number is even, we add 1(to get an odd integer). Then Primality Test is carried out from this odd integer to generate a prime number from the randomly generated number.

One of our main contributions in this chapter is how to use Maple 18 to test whether a given number is prime:

```
> isprime(n);
```

```
> p := nextprime(4000433442120074580000);
```

```
> q := nextprime(5000300663662690012000);
```

```
> n := p * q;
```

```
> m := (p - 1) * (q - 1);
```

```
> a := 10098768900987679000910003;
```

To verify that the preceding value of a is a valid RSA encryption exponent given our value of m, we will use the Maple igcd function, which is designed to calculate the greatest common divisor of a pair of integer inputs. The following command returns the greatest common divisor of the integers a and m. Note that, as required, $gcd(a, m) = 1$.

```
> igcd(a, m);
```

Theorem 3.2.20. *The trapdoor function $RSA_{n,e}$ is a permutation over the cyclic commutative group $\mathbb{Z}_n^*$.*

Proof. Let $n = pq$ for some large prime numbers, e is a number such that $gcd(e, \varphi(n)) = 1$, where $\varphi(n)$ is Euler's (totient) function. Then by Theorem 3.2.16 (Euler's Theorem), there exists a number d such that

$$ed \equiv 1 \ mod \ \varphi(n).$$

Given $x \in \mathbb{Z}_n^*$, consider the element $x^d \in \mathbb{Z}_n^*$. Then

$$RSA_{n,e}(x^d) \equiv (x^d)^e \ mod \ n \equiv x^{ed} \ mod \ n \equiv x \ mod \ n.$$

This shows that the function

$$RSA_{n,e} : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$$

is onto and since $\varphi(n) = |\mathbb{Z}_n^*|$ if finite, we conclude that $RSA_{n,e}$ is a permutation over $\mathbb{Z}_n^*$.

Remark. From Theorem 3.2.20, it clear that the $RSA_{n,e}$ has a unique inverse. Using the fact that $gcd(e, \varphi(n)) = 1$, we can find a $d \in \mathbb{Z}_n^*$ such that

$$RSA_{n,e}^{-1}(x) = (x^e \ mod \ n)^d \ mod \ n = (x^e)^d \ mod \ n = x \ mod \ n.$$

Once we find a d such that $ed \equiv 1 \ mod \ \varphi(n)$, then we can invert $RSA_{n,e}$ efficiently because then

$$RSA_{n,e}(x^d) = (x^e)^d \equiv x \ mod \ \varphi(n).$$

Remark An encrypting function must be injective, so that it won't encrypt two different plaintexts to the same ciphertext. Encryption can still be random, and an encrypting function can encrypt the same plaintext to several different ciphertext, so an encrypting function is not actually a mathematical function, but an injective relation.

Chapter 4

HILBERT SPACE FRAMES

Hilbert space frames were introduced in 1952 by Duffin and Schaeffer[10] to address some deep questions in non-harmonic Fourier series. In 1986, Daubechies, Grossman and Meyer[9] reintroduced the notion of frames and observed that frames can be used to find series expansions of functions in the Hilbert space $L^2(\mathbb{R})$. Frames are generalizations of orthonormal bases in Hilbert spaces. The main property of frames which makes them so useful is their redundancy. In this chapter we further develop the theory and Hilbert space frames and present new results.

4.1 Pseudo-inverses and the Singular Value Decomposition

Definition 4.1.1 ([6], Definition 1.7). A `singular value decomposition` (SVD) of an $M \times N$ matrix A is a factorization $A = U\Sigma V^*$, where $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_p, 0..., 0)$ is an $M \times N$ real matrix, $p = \min\{M, N\}$ and $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_p \geq 0$ are the singular values of A, $U = [u_1, u_2, ..., u_M]$ is an $M \times M$ unitary matrix, $V = [v_1, v_2, ..., v_n]$ is an $N \times N$ unitary matrix.

Theorem 4.1.2 (Singular Value Decomposition, SVD). *Let A be an $M \times N$ matrix with $M \geq N$. Then there exists a unitary $M \times M$ matrix U, a unitary $N \times N$ matrix V and a diagonal $M \times N$ real matrix $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_N)$ with $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_N \geq 0$ such that $A = U\Sigma V^*$ holds. Moreover, the column vectors of V are the eigenvectors of A^*A associated with the eigenvalues σ_i^2, $i = 1, 2, ..., N$. The columns of u are the eigenvectors of the matrix AA^*.*

Proof. The existence claim is trivial. We prove the second claim. First note that $A^*A = (U\Sigma V^*)(U\Sigma V^*)^* = VDV^*$, where $D = \Sigma^*\Sigma = diag(\sigma_1^2, \sigma_2^2, ..., \sigma_N^2)$ is $N \times N$. Thus $A^*AV = VD$. This shows that σ_i^2 is an eigenvalue of A^*A. Similarly, $AA^* = U\Sigma V^*(U\Sigma V^*)^* = U\Sigma\Sigma^*U^*$, where $\Sigma\Sigma^* = diag(\sigma_1^2, \sigma_2^2, ..., \sigma_N^2, 0, ..., 0)$ is $M \times M$. Clearly if $U\Sigma V^*$ is a singular value decomposition, then $V\Sigma^*U^*$ is a singular value decomposition of A^*. The non-zero singular values of A are the square roots of the non-zero eigenvalues of A^*A or AA^*.

Definition 4.1.3. A `Moore-Penrose pseudo-inverse` of an $M \times N$ matrix A is an $N \times M$ matrix $A^\dagger$ that satisfies the four Penrose conditions:

$$AA^\dagger A = A; \quad A^\dagger AA^\dagger = A^\dagger; \quad (AA^\dagger)^* = AA^\dagger; \quad (A^\dagger A)^* = A^\dagger A.$$

Theorem 4.1.4 ([6], Theorem 1.2). *If A an $M \times N$ matrix has SVD given by $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where $\Sigma^\dagger = diag(\frac{1}{\sigma_1}, \frac{1}{\sigma_2}, ..., \frac{1}{\sigma_p}, 0, ..., 0)$ is $N \times M$.*

The notion of pseudo-inverse can be extended to any bounded linear operators. Let $A \in B(\mathcal{H}, \mathcal{K})$. If AA^* is invertible, then $B = A^*(AA^*)^{-1}$ is the pseudo-inverse of A. Equivalently, if A^*A is invertible, then $B = (A^*A)^{-1}A^*$ is the pseudo-inverse of A. From this definition, it is succinctly clear that the pseudo-inverse of a bounded linear operator need not be unique. That is, bounded linear operator may admit infinitely many pseudo-inverses. In fact, if an operator has more than one pseudo-inverse, then it has infinitely many(see [13]).

4.2 Frames and their Associated Operators

Theorem 4.2.1. *(Parseval Identity) Let $\{f_k\}_{k=1}^n$ be an orthonormal basis for an n-dimensional Hilbert space $\mathcal{H}$. Then for any $f \in \mathcal{H}$,*

$$\sum_{k=1}^{n} |\langle f, f_k \rangle|^2 = \|f\|^2.$$

We note that the Parseval Identity also holds in infinite dimensional Hilbert spaces.

A subset $\{f_k\}_{k \in J}$ of a Hilbert space $\mathcal{H}$ is said to be *complete* if every element $f \in \mathcal{H}$ can be represented arbitrarily well in norm by linear combinations of the elements in $\{f_k\}_{k \in J}$. A complete set $\{f_k\}_{k \in J}$ is said to be *over-complete* or *redundant* if removal of an element f_j from the set results in a complete set or system. That is, if $\{f_k\}_{k \in J \setminus \{j\}}$ is still complete.

Definition 4.2.2. A sequence of vectors $\{f_k\}$ in a Hilbert space $\mathcal{H}$ is a *frame* for $\mathcal{H}$ if there exists real numbers $0 < \alpha \leq \beta < \infty$ called `frame bounds` such that for all $f \in \mathcal{H}$

$$\alpha \|f\|^2 \leq \sum_{k} |\langle f, f_k \rangle|^2 \leq \beta \|f\|^2.$$

The numbers α and β are called the *lower bound and upper bound* of the frame, respectively. They are, respectively, the smallest and largest eigenvalues of the frame operator. The numbers $(\langle f, f_k \rangle)$ are called the `frame coefficients`. A frame is a redundant or over-complete (i.e. not linearly independent) coordinate system for a vector space that satisfies a Parseval-type norm inequality. A set of vectors in a finite dimensional Hilbert space is a frame if and only if it is (just) a spanning set.

Let J be an indexing set. If $\alpha = \beta$, then the frame $\{f_k\}_{k \in J}$ is called *tight* and if $\alpha = \beta = 1$, the frame is called a *normalized tight frame* or *Parseval.* If $\|f_i\| = \|f_j\|$, for all $i, j \in J$, then $\{f_k\}_{k \in J}$ is called an *equal-norm* or *uniform norm frame*, and if in addition $\alpha = \beta = 1$, we have a *uniform normalized tight frame* (UNTF). If a frame is equal-norm and if there exists a $c \geq 0$ such that $|\langle f_j, f_k \rangle| = c$, for all j, k with $j \neq k$, then the frame is said to be *equiangular.* A frame $\{f_k\}$ that ceases to be a frame when an arbitrary element $\{f_j\}$ is removed is called an `exact frame`. For more exposition about these classes of frames(see,[8],[9],[10]).

Definition 4.2.3. Let $\{f_k\}$ be a frame for a Hilbert space $\mathcal{H}$. The operator $A : \mathcal{H} \to \ell^2(\mathbb{Z})$ defined by
$Af = \{\langle f, f_k \rangle\}$, for all $f \in \mathcal{H}$ and $k \in \mathbb{Z}$ is called the `analysis operator` of the frame $\{f_k\}$.

Definition 4.2.4. Let $\{f_k\}$ be a frame for a Hilbert space $\mathcal{H}$ with analysis operator A. The Hilbert space adjoint of the analysis operator $A^* : \ell^2(\mathbb{Z}) \to \mathcal{H}$ defined by $A^*(\{\langle f, f_k \rangle\}) = \sum_k \langle f, f_k \rangle f_k$ is called the `synthesis operator` of the frame $\{f_k\}$.

Remark. The analysis and synthesis operators of a frame play a central role in the analysis, reconstruction and recovery of any function or signal $f \in \mathcal{H}$. The analysis operator analyzes a signal in terms of the frame by computing its frame coefficients.

Definition 4.2.5. Given a frame $\{f_k\}$ in a Hilbert space $\mathcal{H}$ with analysis operator A, another frame $\{g_k\}$ with analysis operator B is said to be a `dual frame` of $\{f_k\}$ if the following reproducing formula or frame decomposition formula holds

$$f = \sum_k \langle f, f_k \rangle g_k, \qquad \forall f \in \mathcal{H}. \tag{4.2.1}$$

We call $\{f_k\}$ and $\{g_k\}$ a `pair of dual frames` or a `dual frame pair`.

Remark. Equation (4.2.1) says that $B^*A = I$, where I denotes the identity operator in $\mathcal{H}$. This means that a frame $\{g_k\}$ with analysis operator B is dual to a frame $\{f_k\}$ with analysis operator A if and only if $B^*A = I$ or equivalently $(B^*A)^* = A^*B = I$. Therefore all the duals of $\{f_k\}$ are left inverses B^* to A (or equivalently, right inverses to A^*). Dual frames are not unique. However, it has been shown that if the frame is exact, then the dual is unique(see [6]).

Definition 4.2.6. Let $\{f_k\}$ be a frame in a Hilbert space $\mathcal{H}$ with analysis operator A. The operators $S = A^*A$ and $G = AA^*$ are called the `frame operator` and `Grammian`, respectively.

The frame operator $S : \mathcal{H} \to \mathcal{H}$ is positive and invertible, while the Grammian $G : \ell^2(\mathbb{Z}) \to \ell^2(\mathbb{Z})$ need not be invertible, since its range need not be all of $\ell^2(\mathbb{Z})$. The Grammian operator and its pseudo-inverse $G^\dagger$ play a crucial role in the process of recovery of $f \in \mathcal{H}$ from frame representation.

Proposition 4.2.7. *Suppose that $\{f_k\}$ is a frame for the Hilbert space $\mathcal{H}$ with analysis operator A and Grammian $G = AA^*$ and frame bounds α and β.*

(i). If the set $\{f_k\}$ is an orthonormal basis for $\mathcal{H}$, then the Grammian operator G is the identity.

(ii). The frame $\{f_k\}$ is a Parseval frame if and only if the Grammian operator G is an orthogonal projection.

Proof.
(i). Since $\{f_k\}$ is an orthonormal basis for $\mathcal{H}$, we have that $A = A^* = I$. Therefore $G = AA^* = I$.

(ii). Clearly $\{f_k\}$ is Parseval if and only if the frame operator $S = A^*A = I$. It is easily verified that Grammian $G = AA^*$ is self-adjoint and that

$$G^2 = (AA^*)(AA^*) = A(A^*A)A^* = A(I)A^* = AA^* = G.$$

Proposition 4.2.8 (Frame Reconstruction/Reproducing Formula)**.** *Let $\{f_k\}$ be a frame in a Hilbert space $\mathcal{H}$ with analysis operator A and frame operator $S = A^*A$. Then*

$$f = \sum_k \langle S^{-1}f, f_k\rangle f_k = \sum_k \langle f, S^{-1}f_k\rangle f_k = \sum_k \langle f, f_k\rangle S^{-1}f_k = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k, \qquad f \in \mathcal{H}.$$

Proof. Let $f \in \mathcal{H}$. By definition and self-adjointness of the frame operator S, we have

$$f = SS^{-1}f = \sum_k \langle S^{-1}f, f_k\rangle f_k = \sum_k \langle f, S^{-1}f_k\rangle f_k.$$

Similarly,

$$f = S^{-1}Sf = S^{-1}\sum_k \langle f, f_k\rangle f_k = \sum_k \langle f, f_k\rangle S^{-1}f_k = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k.$$

Finally, using the fact that $I = S^{-1/2}SS^{-1/2}$, we have

$$f = S^{-1/2}SS^{-1/2}f = S^{-1/2}\sum_k \langle S^{-1/2}f, f_k\rangle f_k = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k.$$

Remark. The reconstruction formula shows that all information about a given vector or signal $f \in \mathcal{H}$ is contained in the sequence $\{\langle f, S^{-1}f_k\rangle\}$. We note that the choice of coefficients in Proposition 4.2.8 is not unique, in general. If the frame $\{f_k\}$ is linearly dependent(redundant or over-complete), a typical phenomenon in applications, then there exist infinitely many choices of coefficients $c_k = \langle f, S^{-1}f_k\rangle$ in the expansion of $f \in \mathcal{H}$ as $f = \sum_k c_k f_k$. This possibility ensures resilience to erasures or noise in a signal $f \in \mathcal{H}$. A new approach (see [5]) has emerged recently, and has received increasing attention, namely choose the coefficient sequence to be sparse in the sense of having only few non-zero entries, thereby allowing data compression while preserving perfect reconstruction or recoverability.

The sequence $\{S^{-1}f_k\}$ is called the `canonical dual` of $\{f_k\}$. Bijectivity of S clearly implies that the canonical dual $\{S^{-1}f_k\}$ is also a frame in $\mathcal{H}$ with frame bounds $\frac{1}{\beta}$ and $\frac{1}{\alpha}$ and frame operator S^{-1}.
The sequence $\{S^{-1/2}f_k\}$ is also frame(by the bijectivity of $S^{-1/2}$), called the `canonical tight frame` associated with the frame $\{f_k\}$(see [2], [6]). By Definition 4.2.5, we note that the canonical dual frame is the pseudo-inverse of A, which we write $(A^*)^\dagger = (A^*A)^{-1}A^* = S^{-1}A^*$.(see also [2]).

Proposition 4.2.9. *Let $\{f_k\}$ be a frame in a Hilbert space $\mathcal{H}$ with analysis operator A and a frame operator $S = A^*A$. Then the frame operator provides a stable reconstruction process*

$$Sf = \sum_k \langle f, f_k\rangle f_k, \qquad f \in \mathcal{H}.$$

Proof. Follows immediately from the definition of S and Proposition 4.2.8.

Remark. Notice from Proposition 4.2.9 that

$$\langle Sf, f\rangle = \langle A^*Af, f\rangle = \langle Af, Af\rangle = \|Af\|^2 = \sum_k \langle f, f_k\rangle\langle f_k, f\rangle = \sum_k \langle f, f_k\rangle\overline{\langle f, f_k\rangle} = \sum_k |\langle f, f_k\rangle|^2, \forall f \in \mathcal{H}.$$

Therefore if α and β are the frame bounds, we have

$$\langle \alpha f, f\rangle = \alpha\|f\|^2 \leq \sum_k |\langle f, f_k\rangle|^2 = \langle Sf, f\rangle \leq \beta\|f\|^2 = \beta\langle f, f\rangle, \ \ \forall f \in \mathcal{H}.$$

This says that

$$\alpha I \leq S \leq \beta I.$$

It has been shown in ([2], Theorem 2.2) that if $\{f_k\}$ is a frame for a Hilbert space $\mathcal{H}$ with frame operator S and $T \in B(\mathcal{H})$, then the frame operator for $\{Tf_k\}$ equals TST^*. Using this result, we conclude that the canonical tight frame has frame operator $S^{-1/2}SS^{-1/2} = I$. This means that $\{S^{-1/2}f_k\}$ is a Parseval frame.

Theorem 4.2.10. *Let $\{f_k\}$ be a tight frame in a Hilbert space $\mathcal{H}$. Then the canonical dual frame $\{S^{-1}f_k\} = \{\frac{1}{\alpha}f_k\}$. Moreover, $f = \frac{1}{\alpha}\sum_k \langle f, f_k\rangle f_k$ and α is the tight frame bound.*

Proof. Suppose that $\{f_k\}$ is a tight frame with frame bound α and frame operator S. Then by definition of S and the reconstrution formula in Proposition 4.2.9, we have

$$\langle Sf, f\rangle = \sum_k |\langle f, f_k\rangle|^2 = \alpha\|f\|^2 = \langle \alpha f, f\rangle.$$

Since S is self-adjoint, this implies that $S = \alpha I$. Thus S^{-1} is the multiplication by $\frac{1}{\alpha}$ operator. The rest of the proof follows from application of Proposition 4.2.8 and definition of a frame.

4.3 The Singular Value Decomposition, Pseudo-inverses and Dual Frames

When designing frames with prescribed properties, it is important to check the behavior of the canonical dual frame $\{S^{-1/2}f_k\}$. In some cases, especially in high dimensional settings, however, the complicated structure of the frame operator and its inverse make this a difficult task. For instance, if $\{f_k\}$ is a frame in the Hilbert space $L^2(\mathbb{R})$ consisting of functions with exponential decay, there is no guarantee that the functions in the canonical dual frame $\{S^{-1}f_k\}$ have exponential decay.

Some frames have advantages over others. For tight frames, by Proposition 4.2.8, Proposition 4.2.9 and Theorem 4.2.10, the canonical dual frame automatically has the same structure as the frame itself. If the frame has a wavelet structure or a Gabor structure, the same is the case for the canonical dual frame. In contrast, there are non-tight wavelet frames which lack this special property. We use the singular value decomposition to avoid inverting the frame operator S.

Theorem 4.3.1 (The dual frame of a tight frame)**.** *$\{f_i\}$ is a tight frame for a Hilbert space $\mathcal{H}$ with analysis operator A and frame bound α if and only if its dual is given by $\widetilde{\Phi} = \{\frac{1}{\alpha}f_i\}$.*

Proof. Suppose that $\Phi = \{f_i\}$ is an α-tight frame. Then for any $f \in \mathcal{H}$, we have

$$\|Af\|^2 = \langle Af, Af\rangle = \langle A^*Af, f\rangle = \alpha\|f\|^2 = \alpha\langle f, f\rangle,$$

and thus $A^*A = \alpha I$, where I denotes the identity operator on $\mathcal{H}$. It follows that $(A^*A)^{-1} = \frac{1}{\alpha} I$, and so $\widetilde{\Phi}_i = \frac{1}{\alpha} f_i$. Conversely, suppose we know that the dual frame satisfies $\widetilde{\Phi}_i = \frac{1}{\alpha} f_i$. Then the associated analysis operator $\widetilde{A}$ satisfies

$$\widetilde{A}f = \langle \widetilde{\Phi}_i, f\rangle = \frac{1}{\alpha}(Af)_i.$$

This is equivalent to $A = \alpha \widetilde{A}$. Therefore

$$A^*A = \alpha \widetilde{A}^* A = \alpha I.$$

So, for any $f \in \mathcal{H}$, we have

$$\langle A^*Af, f\rangle = \langle Af, Af\rangle = \|Af\|^2 = \alpha\langle f, f\rangle = \alpha\|f\|^2,$$

which proves that $\{f_i\}$ is a tight frame with frame bound α.

Example 4.3.2.

In $\mathbb{R}^2$, any set of three vectors that are equally distributed(i.e. equiangular, with angle between them as 120°) on the unit circle is a tight frame. A special case is the Mercedes-Benz frame

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{pmatrix} \right\}$$

is a tight frame.

Example 4.3.3.

For an example on how to construct a frame for $\mathbb{C}^2$ consisting of three vectors that satisfies $\alpha = \beta = 1$ (see [19], Example 8).

Proposition 4.3.4. *Let $\{f_k\}$ be a frame in a Hilbert space $\mathcal{H}$ and suppose that $\{g_k\}$ is its dual frame. Then*

$$f = \sum_k \langle f, g_k\rangle f_k = \sum_k \langle f, f_k\rangle g_k, \qquad \forall f \in \mathcal{H}.$$

It is clear that if $\{g_k\}$ is a dual frame for $\{f_k\}$, then $\{f_k\}$ is also a dual of $\{g_k\}$.(see [6]). If the frame $\{f_k\}_{k=1}^M$ for a Hilbert space of dimension N and $M > N$(that is the frame contains more vectors than is needed for the spanning property-that is, it is over-complete or redundant), there exists infinitely many dual frames(no rigidity as is the case of bases or when $M = N$)(see [2]).

We find the $SVD(A)$ as $A = U\Sigma V^*$, where A is any $M \times N$ matrix of real numbers with rank k, U is a matrix whose columns are the M orthonormal eigenvectors associated with the non-zero eigenvalues of the self-adjoint matrix $G = AA^*$. On the other hand, matrix V is formed with the orthonormal eigenvectors associated with the non-zero eigenvalues of the self-adjoint operators $S = A^*A$. In a frame, S is invertible, and hence has no zero eigenvalues(see [13]).

Remark. For computational purposes, it is important to notice that the pseudo-inverse of an operator T can be found by the singular value decomposition of T.

We will explore the use of MAPLE software to find the duals of frames and avoid finding the inverse of the frame operator S.

Example 4.3.5 ([21], Example 4.2)**.** For the frame $\{f_k\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ for $\mathcal{H} = \mathbb{R}^2$,

$$G = (\langle f_m, f_n \rangle)_{1 \le m,n \le 3} = \begin{bmatrix} \langle f_1, f_1 \rangle & \langle f_1, f_2 \rangle & \langle f_1, f_3 \rangle \\ \langle f_2, f_1 \rangle & \langle f_2, f_2 \rangle & \langle f_2, f_3 \rangle \\ \langle f_3, f_1 \rangle & \langle f_3, f_2 \rangle & \langle f_3, f_3 \rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

A simple calculation shows that G is not invertible. A simple computation shows that $S = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, and S is invertible. It is easy to show that $\sigma(G) = \{0, 1, 3\}$ and $\sigma(S) = \{1, 3\}$.

Theorem 4.3.6 ([21], Theorem 4.3)**.** *Let $\{f_n\}$ be a frame for a Hilbert space $\mathcal{H}$ with analysis operator A and frame operator S and Grammian G. Let the associated canonical dual frame be $\{\widetilde{f_n}\}$, where $\widetilde{f_n} = S^{-1}f_n$ with an associated analysis operator $\widetilde{A}$. Then $\widetilde{A} = (G|_{Ran(A)})^{-1}A$.*

Proof. We first note that $\widetilde{A}f = (\langle f, \widetilde{f_n} \rangle) = (\langle f, S^{-1}f_n \rangle)$. Thus $Ran(A) = Ran(\widetilde{A})$, since S is invertible. Thus

$$A^*\widetilde{A} = \widetilde{A}^*A = I_{\mathcal{H}},$$

where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$. On $Ran(A), A, \widetilde{A}$, and hence the Gramian G for$\{f_n\}$ are invertible and we have that $A^{-1} = \widetilde{A}^*$ and $\widetilde{A}^{-1} = A^*$. Thus the relation between the analysis operator A and its dual $\widetilde{A}$ is

$$\widetilde{A} = (G|_{Ran(A)})^{-1}G\widetilde{A} = (G|_{Ran(A)})^{-1}AA^*\widetilde{A} = (G|_{Ran(A)})^{-1}A.$$

Proposition 4.3.7 ([6], Corollary 1.10)**.** *A frame $\{f_n\}_{n=1}^{M}$ for an N-dimensional Hilbert space $\mathcal{H}$ has a unique dual frame if and only if $M = N$.*

Proposition 4.3.8. *Let $\{f_n\}_{n=1}^M$ be a frame for an N-dimensional Hilbert space $\mathcal{H}$ with frame bounds α and β. Let P be an orthogonal projection of $\mathcal{H}$ onto a subspace $\mathcal{M}$. Then $\{g_n\} = \{Pf_n\}_{n=1}^M$ is a frame for $\mathcal{M}$ with frame bounds α and β. In particular, if $\{f_n\}_{n=1}^M$ is a Parseval frame, then $\{Pf_n\}_{n=1}^M$ is a Parseval frame.*

Proof. For any $f \in \mathcal{M}$, we have that $f = P_{\mathcal{M}}f$ and so

$$\alpha\|f\|^2 = \alpha\|Pf\|^2 \leq \sum_{n=1}^{M} |\langle Pf, f_n\rangle|^2 = \sum_{n=1}^{M} |\langle f, Pf_n\rangle|^2 \leq \beta\|Pf\|^2 = \beta\|f\|^2.$$

If $\{f_n\}_{n=1}^M$ is Parseval, then we have

$$\|f\|^2 = \|Pf\|^2 = \sum_{n=1}^{M} |\langle Pf, f_n\rangle|^2 = \sum_{n=1}^{M} |\langle f, Pf_n\rangle|^2 = \sum_{n=1}^{M} |\langle f, g_n\rangle|^2.$$

The canonical coefficients from the frame expansion arise naturally by considering the pseudo-inverse of the analysis operator. The pseudo-inverse can be given by the singular value decomposition of A.

Theorem 4.3.9 ([20], Theorem 3.11). *If $\{f_k\}_{k=1}^n$ is a frame for an N-dimensional Hilbert space $\mathcal{H}$ with frame operator S and T is an operator on $\mathcal{H}$, then the frame operator for $\{Tf_k\}_{k=1}^n$ equals TST^*.*

Proof. The proof follows from the fact that the frame operator for $\{Tf_k\}_{k=1}^n$ is given by

$$\sum_{k=1}^{n}\langle f, Tf_k\rangle Tf_k = T(\sum_{k=1}^{n}\langle T^*f, f_k\rangle f_k) = TST^*.$$

Alternatively, from Lemma 8.20, the frame operator of $\{Tf_k\}_{k=1}^n$ is given by

$$B^*B = (AT^*)^*(AT^*) = TA^*AT^* = T(A^*A)T^* = TST^*.$$

Clearly

$$TST^*f = T(\sum_{k=1}^{n}\langle T^*f, f_k\rangle f_k) = \sum_{k=1}^{n}\langle f, Tf_k\rangle Tf_k.$$

This leads to the following consequences.

Corollary 4.3.10. *If $\{f_k\}_{k=1}^n$ is a tight frame for an N-dimensional Hilbert space $\mathcal{H}$ with frame operator S and T is an operator on $\mathcal{H}$, then the frame operator for $\{Tf_k\}_{k=1}^n$ is a scalar multiple of TT^*. Moreover, if $\{f_k\}_{k=1}^n$ is Parseval/normalized and tight, then the frame operator for $\{Tf_k\}_{k=1}^n$ is TT^*.*

The canonical tight frame $\{S^{-\frac{1}{2}}f_n\}_{n=1}^M$ inherits properties of the original frame $\{f_n\}_{n=1}^M$.

Proposition 4.3.11. *If $\{f_n\}_{n=1}^M$ is a frame for a Hilbert space $\mathcal{H}$ with frame operator S and frame bounds α and β, then $\{S^{-\frac{1}{2}}f_n\}_{n=1}^M$ is a tight frame with frame bound 1(i.e. it is Parseval) and $f = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k$ for all $f \in \mathcal{H}$.*

Proof. We need to show that $\{S^{-\frac{1}{2}}f_n\}_{n=1}^M$ satisfies the reconstruction formula $f = \sum_{k=1}^n \langle f, f_k\rangle f_k$ for all $f \in \mathcal{H}$. Clearly, the operator $S^{-1/2}$ is well defined and commutes with S^{-1}. Therefore by Proposition 4.2.8, every $f \in \mathcal{H}$ can be reconstructed as

$$f = S^{-1/2}SS^{-1/2}f = S^{-1/2}\sum_k \langle S^{-1/2}f, f_k\rangle f_k = S^{-1/2}\sum_k \langle f, S^{-1/2}f_k\rangle f_k = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k.$$

This proves the Parseval reconstruction formula for f.
Taking the inner product with f we have

$$\|f\|^2 = \langle f, f\rangle = \sum_k \langle f, S^{-1/2}f_k\rangle\langle S^{-1/2}f_k, f\rangle = \sum_k \langle f, S^{-1/2}f_k\rangle\overline{\langle f, S^{-1/2}f_k\rangle} = \sum_k |\langle f, S^{-1/2}f_k\rangle|^2.$$

This shows that $\{S^{-\frac{1}{2}}f_n\}_{n=1}^M$ is a tight frame with frame bound 1.
We note that the first claim can be proved easily using Theorem 4.3.9 by showing that the frame operator of the canonical tight frame is $S^{can} = S^{-1/2}SS^{-1/2} = I$. This is equivalent the statement that for every $f \in \mathcal{H}$, we have

$$S^{can}f = \sum_k \langle f, \widetilde{f_k}\rangle\widetilde{f_k} = \sum_k \langle f, S^{-1/2}f_k\rangle S^{-1/2}f_k = S^{-1/2}\sum_k \langle S^{-1/2}f, \widetilde{f_k}\rangle f_k = S^{-1/2}SS^{-1/2}f = f.$$

Therefore $S^{can} = I$.

Theorem 4.3.12. *Let $\Phi = \{f_k\}$ be a frame for a Hilbert space $\mathcal{H}$ with frame operator S and frame bounds α and β. The canonical dual frame $\widetilde{\Phi} = \{S^{-1}f_k\}$ has frame operator S^{-1}.*

Proof. The synthesis operator of $\widetilde{\Phi}$ is given by $B^* = S^{-1}A^*$(see [2]), where A is the analysis operator of Φ. Thus the frame operator for $\widetilde{\Phi}$ is given by

$$\widetilde{S} = B^*B = S^{-1}A^*(AS^{-1}) = S^{-1}(A^*A)S^{-1} = S^{-1}SS^{-1} = S^{-1}.$$

Alternatively, by ([2], Theorem 2.2), the frame operator of $\{S^{-1}f_k\}$ is

$$\widetilde{S} = S^{-1}S(S^{-1})^* = S^{-1}SS^{-1} = S^{-1}.$$

This result can also be proved as follows:
For every $f \in \mathcal{H}$, we have

$$\widetilde{S}f = \sum_k \langle f, \widetilde{f_k}\rangle\widetilde{f_k} = \sum_k \langle f, S^{-1}f_k\rangle S^{-1}f_k = S^{-1}\sum_k \langle S^{-1}f, \widetilde{f_k}\rangle f_k = S^{-1}SS^{-1}f = S^{-1}f.$$

Therefore $\widetilde{S} = S^{-1}$.

We note the claim can be proved easily using ([21], Theorem 4.6) by showing that the frame operator of the canonical dual frame is $\widehat{S} = S^{-1}SS^{-1} = S^{-1}$. This is equivalent the statement that for every $f \in \mathcal{H}$, we have

$$\widetilde{S}f = \sum_k \langle f, \widetilde{f_k}\rangle \widetilde{f_k} = \sum_k \langle f, S^{-1}f_k\rangle S^{-}f_k = S^{-1}\sum_k \langle S^{-1}f, \widetilde{f_k}\rangle f_k = S^{-1}SS^{-1}f = S^{-1}f.$$

Therefore $\widetilde{S} = S^{-1}$.

Since S is the frame operator, we have that $\langle \alpha f, f\rangle \le \langle Sf, f\rangle \le \langle \beta f, f\rangle$ for all $f \in \mathcal{H}$. This is equivalent to the statement that $\alpha I \le S \le \beta I$. We conclude that $\frac{1}{\beta}I \le S^{-1} \le \frac{1}{\alpha}I$.

We have seen that the problem of finding duals to a frame $\Phi = \{f_k\}_{k=1}^m$ with analysis operator A boils down the problem of finding the set of matrices or operators B such that $B^*A = I$ or $A^*B = I$. Equivalently, this is the set of all left-inverses or pseudo-inverses B to A or the adjoints of all right inverses to A. Since $m > N$, the frame is redundant(consists of more vectors than needed to span $\mathcal{H}$), Gauss-Jordan elimination shows that there are infinitely many dual frames.

We give examples for the cases $m = 3, 4$ and $\mathcal{H} = \mathbb{R}^2$.

Example 4.3.13 ([21], Example 5.1)**.**

Consider the sequence $\{f_k\}_{k=1}^3 := \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$. Clearly the analysis operator is $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ and the synthesis operator $A^* = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. A simple calculation shows that the frame operator $S := A^*A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and the Gram matrix $G := AA^* = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}$. Clearly $S^{-1} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$ and hence the canonical dual frame

$$\{S^{-1}f_k\} = \left\{\begin{pmatrix} \frac{2}{3} \\ -\frac{1}{3} \end{pmatrix}, \begin{pmatrix} -\frac{1}{3} \\ \frac{2}{3} \end{pmatrix}, \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \end{pmatrix}\right\}.$$

The pseudo inverse of A^* computed by singular value decomposition is $B = (A^*)^\dagger = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \end{pmatrix}$ and its columns give the dual frame vectors. Notice that $BA^* = I$, and so the columns of B represent the alternate dual frame. Notice that in this case the alternate dual coincides with the canonical frame $\{S^{-1}f_k\}$. Notice also that the above result can be obtained from $B = S^{-1}A^*$.

However, the frame has infinitely many duals. For instance the matrix $\begin{pmatrix} 2 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}$ is another pseudo-inverse for A. This frame has a redundancy $\frac{3}{2}$.

Example 4.3.14 ([21], Example 5.2)**.**

The frame $\{f_k\}_{k=1}^4 := \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ is a tight frame for $\mathbb{R}^2$ since $S = 2I$ and hence $S^{-1} = \frac{1}{2}I$. The normalized frame is $\Psi = \{\frac{1}{\sqrt{2}}f_k\}$. A simple computation shows that Ψ is a normalized tight frame for $\mathbb{R}^2$, with Grammian $G_\Psi = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}$, which is an orthogonal projection. More calculations show that the alternate dual frame consists of the columns of $\widetilde{A}^* = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}$. Since $\widetilde{S} = \widetilde{A}^*\widetilde{A} = \frac{1}{2}I$, we conclude that the dual frame is also tight. This frame has redundancy 2. Another computation shows that $\widetilde{G} = G^\dagger = \frac{1}{4}G$ and $G = \widetilde{G}^\dagger$. This says that $G\widetilde{G} = G\widetilde{G} = I$.

From this example, we deduce two results.

Lemma 4.3.15. *Let $\Phi = \{f_k\}_{k=1}^m$ be a frame for an N-dimensional Hilbert space $\mathcal{H}$. If Φ has a redundancy greater or equal to 2, then it has a tight dual frame.*

Theorem 4.3.16. *The Grammian of a frame Φ and its dual $\widetilde{\Phi}$ are pseudo-inverses. That is, $Gram(\widetilde{\Phi}) = Gram(\Phi)^\dagger$.*

Proposition 4.3.4 and Theorem 4.3.16 leads us to a new relation, which we call `duality of finite frames`. We denote this new relation by $\Phi \overset{dual}{\sim} \Psi$ if and only if $f = \sum_{k=1}^n \langle f, g_k\rangle f_k$ for all $f \in \mathcal{H}$

Theorem 4.3.17 ([21])**.** *Duality of frames $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ for a Hilbert space $\mathcal{H}$ is an equivalence relation.*

Proof. Recall that $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ are a dual pair if $f = \sum_{k=1}^n \langle f, g_k\rangle f_k$ for all $f \in \mathcal{H}$. Clearly $\Phi \overset{dual}{\sim} \Phi$, since $f = \sum_{k=1}^n \langle f, f_k\rangle f_k$. This shows that $\overset{dual}{\sim}$ is reflexive.
Suppose $\Phi \overset{dual}{\sim} \Psi$. Then $f = \sum_{k=1}^n \langle f, g_k\rangle f_k = \sum_{k=1}^n \langle f, f_k\rangle g_k$ for all $f \in \mathcal{H}$. This shows that $\Psi \overset{dual}{\sim} \Phi$ and therefore $\overset{dual}{\sim}$ is symmetric. Now, suppose $\Omega = \{h_k\}_{k=1}^n$ be a frame for $\mathcal{H}$. Suppose that $\Phi \overset{dual}{\sim} \Psi$ and $\Psi \overset{dual}{\sim} \Omega$. Then $f = \sum_{k=1}^n \langle f, g_k\rangle f_k = \sum_{k=1}^n \langle f, f_k\rangle g_k$ and $f = \sum_{k=1}^n \langle f, g_k\rangle h_k = \sum_{k=1}^n \langle f, h_k\rangle g_k$. This implies that $f = \sum_{k=1}^n \langle f, f_k\rangle g_k = \sum_{k=1}^n \langle f, h_k\rangle g_k$. Equating the coefficients we have that $\langle f, f_k\rangle = \langle f, h_k\rangle$ and therefore $f = \sum_{k=1}^n \langle f, h_k\rangle f_k$, which proves that $\Phi \overset{dual}{\sim} \Omega$. Therefore $\overset{dual}{\sim}$ is transitive. Thus $\overset{dual}{\sim}$ is an equivalence relation.

Example 4.3.18 ([21], Example 5.6)**.**

Consider the frame in Example 4.3.13. It can be shown that the frame bounds are $\sigma_1 = 1, \sigma_2 = \sqrt{3}$ and so

$$\|f\|^2 \leq \|Af\|^2 \leq 3\|f\|^2.$$

and that the dual analysis operator is $B^* = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$. Notice that in this case the alternate dual coincides with the canonical dual frame.

Suppose we want to reconstruct $f = \begin{pmatrix} -5 \\ 2 \end{pmatrix}$ in terms of the frame $\{f_k\}$ and in terms of the dual. Then

$$B^*f = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} -5 \\ 2 \end{pmatrix} = \begin{pmatrix} -4 \\ 3 \\ -1 \end{pmatrix}.$$

Therefore

$$f = \begin{pmatrix} -5 \\ 2 \end{pmatrix} = -4f_1 + 3f_2 - f_3.$$

To find the expansion of f in terms of the dual frame we compute the coefficients as

$$Af = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -5 \\ 2 \end{pmatrix} = \begin{pmatrix} -5 \\ 2 \\ -3 \end{pmatrix},$$

and so

$$f = \begin{pmatrix} -5 \\ 2 \end{pmatrix} = -5\widetilde{f_1} + 2\widetilde{f_2} - 3\widetilde{f_3}.$$

To find the canonical tight frame, we compute $S^{-1/2}$. To achieve this, we orthogonally diagonalize $S^{-1/2}$. Let $T = S^{-1}$. We find an orthogonal matrix U such that $UTU^{-1} = D = R^2$, where D is a diagonal matrix with diagonal entries the eigenvalues of T and R is any of the four square roots of D. We ortho-normalize the eigenvectors of $S^{-1/2}$ and let U be the matrix whose columns are the normalized vectors. A simple computation gives $\lambda_1 = 1, \lambda_2 = \frac{1}{3}$ as the eigenvalues of T with corresponding eigenvectors $[-1, 1]^t$ and $[1, 1]^t$. The vectors are already orthogonal and we only need to divide each by its length. Thus $U = \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$. Without loss of generality we let

$R = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{3}} \end{pmatrix}$. Then

$$S^{-1/2} = T^{1/2} = U^*R^*U = \begin{pmatrix} \frac{1}{2} + \frac{1}{\sqrt{12}} & -\frac{1}{2} + \frac{1}{\sqrt{12}} \\ -\frac{1}{2} + \frac{1}{\sqrt{12}} & \frac{1}{2} + \frac{1}{\sqrt{12}} \end{pmatrix}.$$

This means that

$$B^* = S^{-1/2}A^* = \begin{pmatrix} \frac{1}{2} + \frac{1}{\sqrt{12}} & -\frac{1}{2} + \frac{1}{\sqrt{12}} & \frac{2}{\sqrt{12}} \\ -\frac{1}{2} + \frac{1}{\sqrt{12}} & \frac{1}{2} + \frac{1}{\sqrt{12}} & \frac{2}{\sqrt{12}} \end{pmatrix}$$

is the synthesis operator for the canonical tight frame. Hence

$$\Phi^{can} = \left\{ \begin{pmatrix} \frac{1}{2} + \frac{1}{\sqrt{12}} \\ -\frac{1}{2} + \frac{1}{\sqrt{12}} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} + \frac{1}{\sqrt{12}} \\ \frac{1}{2} + \frac{1}{\sqrt{12}} \end{pmatrix}, \begin{pmatrix} \frac{2}{\sqrt{12}} \\ \frac{2}{\sqrt{12}} \end{pmatrix} \right\}$$

, is the canonical tight frame for Φ.
A simple calculation shows that

$$\langle f_k, \widehat{f_k} \rangle = \langle f_k, \widetilde{f_k} \rangle = \|f_k^{can}\|^2, \forall k,$$

where $\widehat{f_k}$ denotes a canonical dual vector and $\widetilde{f_k}$ denotes an alternate dual vector. This implies that

$$\sum_{k=1}^{3} \langle f_k, \widetilde{f_k} \rangle = 2 = dim(\mathcal{H}).$$

MAPLE 18 software reveals that $B^*BB^* = B^*$, which proves that B^* is a partial isometry. This agrees with an earlier remark. Further computation using MAPLE 18 approximates

$$S^{can} = \begin{pmatrix} 1 & -1.899 \times 10^{-16} \\ -1.899 \times 10^{-16} & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

and

$$Gram(\Phi^{can}) = \begin{pmatrix} 0.3333 & -7.269 \times 10^{-17} & 0.4714 \\ -7.269 \times 10^{-17} & 1 & -1.813 \times 10^{-16} \\ 0.4714 & -1.813 \times 10^{-16} & 0.6666 \end{pmatrix} \approx \begin{pmatrix} 0.3333 & 0 & 0.4714 \\ 0 & 1 & 0 \\ 0.4714 & 0 & 0.6666 \end{pmatrix}.$$

Since $S^{can} = I$, we conclude that the canonical tight frame $\{S^{-1/2}f_k\}$ is a Parseval frame, which agrees with Proposition 4.3.11.

Theorem 4.3.19 ([21], Theorem 5.7)**.** *If $\Phi = \{f_k\}_{k=1}^n$ is a normalized tight frame for a Hilbert space $\mathcal{H}$ and $T : \mathcal{H} \longrightarrow \mathcal{H}$ is an invertible operator, then the frames $\{T^*f_k\}$ and $\{T^{-1}f_k\}$ are* *dual to each other.*

Proof. Since $\Phi = \{f_k\}_{k=1}^n$ is a normalized tight frame, its frame operator $S = I$. Using this fact together with Proposition 4.2.9, we have that $\{f_k\}_{k=1}^n$ is normalized tight frame if and only if $f = \sum_k \langle f, f_k\rangle f_k$, for all $f \in \mathcal{H}$. Let $\{g_k\} = \{T^* f_k\}$ and $\{h_k\} = \{T^{-1} f_k\}$. We need to show that $f = \sum_k \langle f, g_k\rangle h_k = \sum_k \langle f, h_k\rangle g_k$. Using the definition, we have

$$\begin{aligned} f \;=\; \textstyle\sum_k \langle f, f_k\rangle f_k &= \textstyle\sum_k \langle f, TT^{-1} f_k\rangle f_k \\ &= \textstyle\sum_k \langle T^* f, T^{-1} f_k\rangle f_k \\ &= T^* \textstyle\sum_k \langle f, T^{-1} f_k\rangle f_k \\ &= \textstyle\sum_k \langle f, T^{-1} f_k\rangle T^* f_k \\ &= \textstyle\sum_k \langle f, h_k\rangle g_k. \end{aligned}$$

Similarly,

$$\begin{aligned} f \;=\; \textstyle\sum_k \langle f, f_k\rangle f_k &= \textstyle\sum_k \langle f, (T^*)^{-1} T^* f_k\rangle f_k \\ &= \textstyle\sum_k \langle f, (T^{-1})^* T^* f_k\rangle f_k \\ &= \textstyle\sum_k \langle T^{-1} f, T^* f_k\rangle f_k \\ &= T^{-1} \textstyle\sum_k \langle f, T^* f_k\rangle f_k \\ &= \textstyle\sum_k \langle f, T^* f_k\rangle T^{-1} f_k \\ &= \textstyle\sum_k \langle f, g_k\rangle h_k. \end{aligned}$$

This proves the claim.

Theorem 4.3.20. *If $\Phi = \{f_k\}_{k=1}^n$ is a frame for a Hilbert space $\mathcal{H}$ and $Q : \mathcal{H} \longrightarrow \mathcal{H}$ is an invertible operator, then the frames $\Psi = \{Qf_k\}$ is a frame for $\mathcal{H}$, and $\Psi^{can} = U\Phi^{can}$, where U is a unitary operator.*

Proof. The claim that $\Psi = \{Qf_k\}$ is a frame for $\mathcal{H}$ follows easily from the fact that Q is invertible. To prove the second claim, we let

$$g_k = Qf_k = QS^{1/2}S^{-1/2}f_k = (QS^{1/2})S^{-1/2}f_k = TS^{-1/2}f_k = Tf_k^{can} = T\Phi^{can},$$

where $T = QS^{1/2}$ is invertible. Thus the synthesis operator for Ψ is $T[f_k^{can}]$. But any canonical tight frame is Parseval by Proposition 4.3.11. Thus $\Psi = \{Tf_k^{can}\}$ is Parseval if and only if its frame operator $S_\Psi^{can} = I$. That is if and only if $S_\Psi^{can} = T[f_k^{can}](T[f_k^{can}])^* = T[f_k^{can}][f_k^{can}]^*T^* = TT^* = I$. This means that T is an co-isometry. Since T is invertible, it must be a unitary operator. So we let $T = U$, where U is unitary. Therefore $\Psi^{can} = U\Phi^{can}$.

Remark. Let $\Phi = \{f_k\}_{k=1}^n$ be a finite frame for a Hilbert space $\mathcal{H}$ with analysis operator A and frame operator S. The Grammian of the canonical tight frame is an orthogonal projection, by ([2], Theorem 2.2), we have $P = Gram(\Phi^{can}) = AS^{-1}A^* : \ell^2(\mathbb{Z}) \longrightarrow \ell^2(\mathbb{Z})$ which gives the coefficients c_k with $f = \sum_k c_k f_k$ of minimal ℓ^2-norm. This means that the canonical tight frame gives a more precise and better reconstruction than the alternate dual frame. This means that the canonical tight frame $\{S^{-1/2}f_k\}$ inherits many of the properties of the original frame $\{f_k\}$. The only problem is that it is not easy to find $\{S^{-1/2}f_k\}$ and that some nice properties of $\{f_k\}$ may not be necessarily inherited.

Lemma 4.3.21. *If $\{f_k\}_{k=1}^n$ is a frame for a finite dimensional Hilbert space $\mathcal{H}$ with analysis operator A and frame operator S and T is an operator on $\mathcal{H}$, then the analysis operator for $\{Tf_k\}_{k=1}^n$ equals AT^*.*

Proof. Let B be the analysis operator of $\{Tf_k\}_{k=1}^n$. Then

$$Bf = \sum_{k=1}^n \langle f, Tf_k\rangle f_k = \sum_{k=1}^n \langle T^*f, f_k\rangle f_k = AT^*f, \quad \forall f \in \mathcal{H}.$$

That is, $B = AT^*$.

APPENDIX

Maple 18 Code for Example 4.3.13

```
>with(MTM):
>A:=matrix([[1,0],[0,1],[1,1]]);     Enters matrix A
>svd:=svd(A);     Gives the singular values of A
>U,S,V:=svd(A);    Gives the full svd(A) and returns matrices U,S,V in that order
>PseudoInv:=MatrixInverse(A,method=pseudo);    Returns the Pseudo-inverse of A
```

The output is

$$\mathtt{A} := \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\mathtt{svd} := \begin{bmatrix} 0 \\ \sqrt{3} \\ 1 \end{bmatrix}$$

$$\mathtt{U,S,V} := \begin{bmatrix} 0.4082 & -0.7071 & -0.5774 \\ 0.4082 & 0.7071 & 0.5774 \\ 0.8165 & -5.5511\ 10^{-17} & 0.5774 \end{bmatrix}, \begin{bmatrix} 1.7321 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0.7071 & -0.7071 \\ 0.7071 & 0.7071 \end{bmatrix}$$

$$\mathtt{PseudoInv} := \begin{bmatrix} \frac{2}{3} & -\frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \end{bmatrix}$$

The following result gives the relationship between analysis operator of a frame and that of any of its infinitely many duals.

Theorem 4.3.22. *If $\Phi = \{f_i\}$ is a frame for $\mathcal{H}$ with analysis operator A and Ψ is a dual frame with analysis operator B, then $B^*A = A^*B = I$.*

The following result shows the optimality of the pseudo-inverse of a pseudo-inverse of the analysis operator of a frame $\{f_i\}$.

Theorem 4.3.23. *If $\{f_i\}$ is a frame for a Hilbert space $\mathcal{H}$ with analysis operator A and let B be the dual analysis operator. Then $B^* = A^\dagger$ is the left inverse of A with minimum induced norm. That is, if $B^*A = TA = I$, then $\|B\| \leq \|T\|$.*

4.4 Isomorphy and Unitary Isomorphy of Hilbert Space Frames

There are several commonly used notions of equivalence among frames. There are frames which, although they are technically different, are considered to be the "same" in some sense. First we explore the more general notions of isomorphy and unitary isomorphy of frames, associated operators and their properties.

Definition 4.4.1. Two frames $\Phi = \{f_n\}_{n=1}^M$ and $\Psi = \{g_n\}_{n=1}^M$ for an N-dimensional Hilbert space $\mathcal{H}$ are said to be `isomorphic`, denoted $\Phi \sim \Psi$ if there is an invertible operator $F : \mathcal{H} \to \mathcal{H}$ such that $Ff_n = g_n$ for all $n = 1, 2, ..., M$.

Definition 4.4.2. Two frames $\{f_n\}_{n=1}^M$ and $\{g_n\}_{n=1}^M$ for an N-dimensional Hilbert space $\mathcal{H}$ are said to be `unitarily isomorphic`, denoted $\{f_n\}_{n=1}^M \cong \{g_n\}_{n=1}^M$ if there is a unitary operator $U : \mathcal{H} \to \mathcal{H}$ such that $Uf_n = g_n$ for all $n = 1, 2, ..., M$.

Remark Balan in [1] has used the term F-`equivalent` to mean isomorphic. We note also that in the literature the terms similarity and unitary equivalence have been used in place of isomorphy and unitary isomorphy, respectively. In this thesis we adopt the latter and reserve the terms similar and unitary equivalence to operators.

Isomorphy and unitary isomorphy of frames are equivalence relations. We also note that isomorphy of frames is order-dependent. This means that the order in which the vectors are arranged in a frame matters.

Example 4.4.3.

Note that if $\{e_n\}$ is an orthonormal basis for an n-dimensional Hilbert space $\mathcal{H}$, then the sets $\{0, e_1, e_2, ..., e_n\}$ and $\{e_1, 0, e_2, ..., e_n\}$ are two non-similar frames for H, although they are the same set.

Definition 4.4.4. Let $\Phi = \{f_n\}_{n=1}^{M}$ be a frame for a Hilbert space $\mathcal{H}$ with frame operator S. The sequence $\Phi^{can} = \{S^{-\frac{1}{2}} f_n\}_{n=1}^{M}$ is a frame, called the `canonical tight frame`.

The canonical tight frame $\{S^{-\frac{1}{2}} f_n\}_{n=1}^{M}$ is a Parseval frame that inherits properties of the original frame $\{f_n\}_{n=1}^{M}$.

Remark. An interesting result in the context of frame isomorphy is that any Parseval frame derived from a frame is in fact isomorphic to it.

Theorem 4.4.5 ([20], Theorem 4.5)**.** *Let $\{f_n\}_{n=1}^{M}$ be a frame for an N-dimensional Hilbert space $\mathcal{H}$ with frame operator S. Then the Parseval frame $\{S^{-\frac{1}{2}} f_n\}_{n=1}^{M}$ is isomorphic to $\{f_n\}_{n=1}^{M}$.*

Proof. The proof follows by letting $Q = S^{-1/2}$.

Theorem 4.4.6 ([20], Theorem 4.6)**.** *Let $\{f_n\}_{n=1}^{M}$ be a frame for an N-dimensional Hilbert space $\mathcal{H}$ with frame operator S. Then the canonical dual frame $\{S^{-1} f_n\}_{n=1}^{M}$ is isomorphic to $\{f_n\}_{n=1}^{M}$.*

Proof. The proof follows by letting $Q = S^{-1}$.

Lemma 4.4.7 ([20], Lemma 4.7)**.** *Let $\{f_n\}_{n=1}^{M}$ and $\{\phi_n\}_{n=1}^{M}$ be isomorphic Parseval frames for an N-dimensional Hilbert space $\mathcal{H}$. Then they are unitarily isomorphic.*

The above lemma says that the notions of isomorphy and unitary isomorphy coincide for Parseval frames.

Theorem 4.4.8 ([20], Theorem 4.8)**.** *Every tight frame $\{f_k\}$ for a Hilbert space $\mathcal{H}$ with frame bound $\alpha \neq 1$ can be re-scaled to a Parseval frame.*

Proof. Suppose that $\{f_k\}$ is a tight frame with frame bound $\alpha \neq 1$. Then

$$\sum_k |\langle f, f_k \rangle|^2 = \alpha \|f\|^2, \quad \forall f \in \mathcal{H}.$$

Thus

$$\frac{1}{\alpha} \sum_k |\langle f, f_k \rangle|^2 = \|f\|^2, \quad \forall f \in \mathcal{H}.$$

Pulling $\frac{1}{\alpha}$ into the sum, we have

$$\sum_k |\langle \frac{1}{\sqrt{\alpha}} f, f_k \rangle|^2 = \sum_k |\langle f, \frac{1}{\sqrt{\alpha}} f_k \rangle|^2 = \|f\|^2.$$

Theorem 4.4.8 says that given a frame, it is always possible to find a frame isomorphic to it.

Theorem 4.4.9. *Every Riesz sequence $\{f_k\}$ for a Hilbert space $\mathcal{H}$ is isomorphic to an orthonormal basis.*

Theorem 4.4.10. *Two frames for a Hilbert space $\mathcal{H}$ are unitarily isomorphic if and only if their Grammians are equal.*

Proof. Suppose $\Phi = \{f_k\}$ and $\Psi = \{g_k\}$ are unitarily isomorphic. Then $g_k = U f_k$, for some unitary operator $U \in B(\mathcal{H})$. By definition, the Grammian

$$G_\Psi = (\langle g_j, g_k \rangle) = (\langle U f_j, U f_k \rangle) = (\langle f_j, f_k \rangle) = G_\Phi.$$

Conversely, suppose that $G_\Psi = G_\Phi$. Then $\langle g_j, g_k \rangle = \langle f_j, f_k \rangle = \langle U f_j, U f_k \rangle$ for some unitary operator $U \in B(\mathcal{H})$. Therefore $g_k = U f_k$. This proves that the frames are unitarily isomorphic.

The theorem above says that unitary isomorphism preserves the Grammian of an operator. In fact the Grammian characterizes the equivalence class of a frame.

Corollary 4.4.11. *Let $\Phi = \{f_n\}_{n=1}^M$ and $\Psi = \{g_n\}_{n=1}^M$ be frames for an N-dimensional Hilbert space $\mathcal{H}$ with analysis operators A and B, respectively. Then the following conditions are equivalent.*

(a). Φ and Ψ are unitarily isomorphic .

(b). $Ran(A) = Ran(B)$.

(c). $Ker(A^*) = Ker(B^*)$.

Proof.(a)$\Longrightarrow$(b): By ([20] Theorem 5.1), $AA^* = BB^*$. Therefore
$Ran(A) = Ran(AA^*) = Ran(BB^*) = Ran(B)$.
(b)$\Longrightarrow$(c): We use the fact that $Ker(T^*) = Ran(T)^\perp$ for any $T \in B(\mathcal{H})$. So if
$Ran(A) = Ran(B)$, then $Ker(A^*)^\perp = Ker(B^*)^\perp$ which implies that $Ker(A^*) = Ker(B^*)$.
(c)$\Longrightarrow$(a): We prove by contradiction. Suppose that $Ker(A^*) = Ker(B^*)$ but Φ and Ψ are not unitarily isomorphic frames. Then $G_\Psi \neq G_\Phi$. This implies that $Ker(B^*B) \neq Kernel(AA^*)$. Since $Ker(AA^*) = Ker(A^*)$ and $Ker(BB^*) = Ker(B^*)$, we have that
$Ker(G_\Phi) = Ker(AA^*) = Ker(A^*) \neq Ker(B^*) = Ker(BB^*) = Ker(G_\Psi)$. This implies that $Ker(A^*) \neq Ker(B^*)$, which is a contradiction to the assumption that $Ker(A^*) = Ker(B^*)$. This proves the claim.

We note that unitary isomorphy need not preserve frame operators.

The next result characterizes the unitary somorphy of two frames in terms of their analysis operators.

Corollary 4.4.12 ([20], Corollary 5.3)**.** *Unitarily isomorphic frames have unitarily equivalent frame operators.*

Proof. Suppose $\Phi = \{f_k\}_{k=1}^n$ $\Psi = \{g_k\}_{k=1}^n$ are unitarily equivalent and suppose $\Phi = \{f_k\}_{k=1}^n$ has frame operator S. Then by $g_k = Uf_k$ for some unitary operator $U \in B(\mathcal{H})$. by Theorem 4.3.9, the frame operator of Ψ is USU^*, which is unitarily equivalent to S.

The following result gives a condition when unitarily isomorphic frames have the same frame operator.

Corollary 4.4.13 ([20], Corollary 5.4)**.** *Unitarily isomorphic tight frames for a Hilbert space $\mathcal{H}$ have same frame operators.*

Proof. Suppose $\Phi = \{f_k\}$ and $\Psi = \{g_k\}$ are unitarily isomorphic tight frames with frame operators S_Φ and S_Ψ, respectively. Tightness implies that $S_\Phi = \alpha_1 I$ and $S_\Psi = \alpha_2 I$ for some $0 < \alpha_1, \alpha_2 < \infty$. Unitary isomorphy of the frames implies unitary equivalence of the frame operators, which means $\sigma(S) = \sigma(USU^*)$. Finally strict positivity of α_1 and α_2 implies that $\alpha_1 = \alpha_2$. Therefore $S_\Phi = S_\Psi$. This proves the claim.

Recall that the Grammian of a tight frame $\Phi = \{f_k\}$ is an orthogonal projection $G = AA^* = P = P_\Phi$. The columns of P_Φ give a canonical copy of Φ and so the kernel of P_Φ is the space of linear dependence $dep(\Phi)$ between vectors in Φ. This leads to the following result.

Proposition 4.4.14. *Let $\Phi = \{f_k\}_{k=1}^m$ be a tight frame for an n-dimensional Hilbert space with Grammian $G = P_\Phi$. Then $dep(\Phi) = Ker(P_\Phi)$.*

Proof. Since the Grammian of a tight frame $\Phi = \{f_k\}$ is an orthogonal projection, we have

$$Ker(P_\Phi) = \{a = (a_1, a_2, ..., a_n) \in \mathbb{F}^n : Pa = \sum_k a_k Pe_k = 0\} = \{a \in \mathbb{F}^n : Pa = \sum_k a_k f_k = 0\} =: dep(\Phi).$$

Proposition 4.4.14 says that for a tight frame the Grammian is determined by its kernel. It also says that P is the orthogonal projection onto $dep(\Phi)^\perp$. We also note from the definition that if Φ is a basis of $\mathcal{H}$, then $dep(\Phi) = \{0\}$.

Theorem 4.4.15. *Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ unitarily isomorphic for a Hilbert space $\mathcal{H}$. Then $dep(\Phi) = dep(\Psi)$.*

Proof. The proof follows easily from Theorem 4.4.10 and the definition of the notion of dependence.
This result can be relaxed as follows.

Theorem 4.4.16. *Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ finite frames for a Hilbert space $\mathcal{H}$ with frame operators A_Φ and A_Ψ, respectively. Then the following are equivalent.*
(a). Φ and Ψ are isomorphic.
(b). $dep(\Phi) = dep(\Psi)$.

Proof. (a)$\Longrightarrow$ (b): Suppose that Φ and Ψ are isomorphic. Then there exists an invertible operator $Q \in B(\mathcal{H})$ such that $g_k = Qf_k$ for all $k = 1, 2, ..., n$. Thus the synthesis operator for Ψ is $A_\Psi^* = [g_k] = [Qf_k] = Q[f_k]$. Note first that the Grammian of Ψ is a projection $P = P_\Psi$. Using the fact that $Ker(AA^*) = Ker(A^*)$ for any operator A and the definition we have

$$dep(\Psi) = Ker(A_\Psi^*) = Ker(Q[f_k]) = Ker([f_k]) = Ker(A_\Phi^*) = Ker(P_\Phi) = dep(\Phi).$$

(b)$\Longrightarrow$ (a): Suppose that $dep(\Phi) = dep(\Psi)$. Note that since $A_\Phi^* = A_\Phi^* P_\Phi$ and $Ran(P_\Phi) = Ker(A_\Phi^*)^\perp$, we have that $A_\Phi^* : Ran(P_\Phi) \longrightarrow \mathcal{H}$ is invertible. Similarly $A_\Psi^*|_{Ran(P_\Psi)} = A_\Psi^*|_{Ran(P_\Phi)}$ is invertible. This means that $Q := (A_\Psi^*|_{Ran(P_\Phi)})(A_\Phi^*|_{Ran(P_\Phi)})^{-1} : \mathcal{H} \longrightarrow \mathcal{H}$ is invertible. Using the fact that $f_k = A_\Phi^* e_k = A_\Phi^* P_\Phi e_k$, where $\{e_k\}$ is an orthonormal basis of $\ell^2(J)$, $J = \{1, 2, ..., n\}$ for $\mathcal{H}$, have

$$Qf_k = QA_\Phi^*(P_\Phi e_k) = A_\Psi^* P_\Phi e_k = A_\Psi^* P_\Psi e_k = A_\Psi^* e_k = g_k.$$

This shows that $g_k = Qf_k$, and hence the frames are isomorphic.

Theorem 4.4.17 ([21], Theorem 5.9)**.** *Unitarily isomorphic frames have the same frame bounds.*

Proof. Suppose that $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ are unitarily isomorphic frames for a Hilbert space $\mathcal{H}$. Suppose that $\Phi = \{f_k\}_{k=1}^n$ has S as its frame operator. By Corollary 4.3.9, $\Psi = \{g_k\}_{k=1}^n$ has frame operator USU^*. Corollary 4.4.12 shows that the frame operators are unitarily equivalent and hence have the same spectrum. That is $\sigma(S) = \sigma(USU^*)$ and therefore the lower and upper frame bounds are the same.

Remark. We note that Theorem 4.4.17 need not be true if we replace unitary isomorphy with isomorphy. This is because isomorphism of frames need not imply similarity of frame operators. To see this, consider the following example.

Example 4.4.18 ([21], Example 5.10)**.**

Consider the frame $\Phi = \{f_k\}_{k=1}^3 = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ for $\mathcal{H} = \mathbb{R}^2$. Let $U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $Q = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. Clearly both U and Q are invertible and in addition U is unitary. So the sequences $\Psi = \{Uf_k\}_{k=1}^3$ and $\Omega = \{Qf_k\}_{k=1}^3$ are frames for $\mathcal{H} = \mathbb{R}^2$. A simple computation gives the corresponding frame vectors as $S_\Phi = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $S_\Psi = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $S_\Omega = \begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$.

We note that the frame bounds for Φ are $\alpha = 1$ and $\beta = 2$ are the same for Ψ, but the frame bounds for S_Ω are $\alpha = 4$ and $\beta = 8$. This shows that unlike frame unitary isomorphy, frame isomorphy need not preserve the frame bounds, and as can be seen in this example, frame isomorphy need not preserve tightness.

Remark. For frames which are not tight, isomorphy of frames is weaker than unitary isomorphy of frames. Thus

$$Unitary\ Isomorphy \Longrightarrow Isomorphy.$$

but the converse is not true, in general.

Theorem 4.4.19. *A frame $\Phi = \{f_k\}_{k=1}^n$ for a Hilbert space $\mathcal{H}$ with a frame operator S, its canonical dual $\widetilde{\Phi} = \{S^{-1}f_k\}_{k=1}^n$ and its canonical tight frame $\Phi^{can} = \{S^{-1/2}f_k\}$ are isomorphic frames. Moreover, they are unitarily isomorphic if and only if $\Phi = \{f_k\}_{k=1}^n$ is Parseval.*

Proof. The proof of the first claim follows from ([20], Theorem 5.8 and Theorem 5.9). The proof of the second claim follows from Lemma 4.4.7.

Corollary 4.4.20. *Two Parseval frames $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ for a Hilbert space $\mathcal{H}$ are unitarily isomorphic if and only if they are isomorphic.*

Proof. We prove the converse. The other direction is clear from the definition. Isomorphy of $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ implies existence of an invertible operator T such that $g_k = Tf_k$, for all k. By ([2], Theorem 2.2) and Corollary 3.11 and the fact that the frames are Parseval implies that the frame operator for $\Psi = \{g_k\}_{k=1}^n$ is $T(I)T^* = TT^* = I$. This implies that T is an isometry. Invertibility of the frame then implies that $T = U$, where U is a unitary operator. Therefore $g_k = Uf_k$. Therefore the frames are unitarily isomorphic.

Remark. The above proof is equivalent to the following direct one: Let $f \in \mathcal{H}$. Then

$$\|T^*f\|^2 = \sum_k |\langle T^*f, f_k\rangle|^2 = \sum_k |\langle f, Tf_k\rangle|^2 = \sum_k |\langle f, g_k\rangle|^2 = \|f\|^2.$$

This proves that T^* is an isometry. That is, $TT^* = I$. Invertibility of T then implies that $T^* = T^{-1}$, which proves that T is unitary. The result now follows by letting $T = U$, for some unitary operator on $\mathcal{H}$.

Remark. We note that if a frame is unitarily isomorphic to a Parseval frame, then it is also a Parseval frame. We note also that every Riesz basis is isomorphic to an orthonormal basis for a Hilbert space $\mathcal{H}$.

The following result characterizes isomorphic frames in terms of the Grammians of their canonical tight frames.

Proposition 4.4.21. *Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ be finite frames for a Hilbert space $\mathcal{H}$ with analysis operators A and B, respectively. Then the following are equivalent:*
(a). Φ and Ψ are isomorphic.
(b). $Gram(\Phi^{can}) = Gram(\Psi^{can})$.
(c). $Ran(A) = Ran(B)$. Equivalently $Ker(A^*) = Ker(B^*)$.

Proof. (a)$\Longrightarrow$(b): Suppose $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ are isomorphic and that the frame operator of $\Phi = \{f_k\}_{k=1}^n$ is S. Then there exists an invertible operator Q such that $g_k = Qf_k$ for all k. Then

$$g_k = Qf_k = QS^{1/2}S^{-1/2}f_k = (QS^{1/2})S^{-1/2}f_k = Tf_k^{can}, \quad \forall k,$$

where $T = QS^{1/2}$ is invertible, since Q and $S^{1/2}$ are. Hence $\Psi = \{Tf_k^{can}\}$. Let us denote the frame operator of $\Psi = \{g_k\}_{k=1}^n$ by S_Ψ. Let the synthesis operator be denoted by C^{can}. Then $S_\Psi = T(C^{can})^*(C^{can})T^* = TT^* = I$. Using the fact that $\Psi = \{Tf_k^{can}\}$ is tight if and only if $S_\Psi = c^2I$ for some $c > 0$, we conclude that T is a unitary operator. Thus Ψ is unitarily equivalent to Φ^{can}. Therefore $Gram(\Phi^{can}) = Gram(\Psi^{can})$.

(b)$\Longrightarrow$(c): Since $P_{\Phi}^{can} := Gram(\Phi^{can})$ and $P_{\Psi}^{can} := Gram(\Psi^{can})$are orthogonal projections, they are determined by their ranges, then $P_{\Phi}^{can} = P_{\Psi}^{can}$ if and only if $Ran(A) = Ran(B)$.

(c)$\Longrightarrow$(a): Follows immediately from the equality of the Grammians. This means that the two frames are unitarily isomorphic and hence isomorphic. Alternatively, first note that

$$Bf = \sum_k \langle f, g_k \rangle f_k = \sum_k \langle f, Tf_k \rangle f_k = \sum_k \langle T^* f, f_k \rangle f_k = AT^* f.$$

This shows that $Ran(B) = Ran(AT^*) = Ran(A)$. That is, $Ran(B) = Ran(A)$. We now let $Ran(A) = Ran(B) = \mathcal{M}$, where $\mathcal{M}$ is a closed subspace of $\ell^2(\mathbb{Z})$. Since A^* and B^* are invertible when restricted to $\mathcal{M}$, the operator $T = B^*(AA^*)^{-1}A : \mathcal{H} \longrightarrow \mathcal{M}$ is onto and invertible on $\mathcal{M}$. Therefore

$$A^*(\mathcal{M}^{\perp}) = B^*(\mathcal{M}^{\perp}) = \{0\}.$$

Thus $f_k = A^* e_k = A^* P e_k$ and $g_k = B^* e_k = B^* P e_k$, where $\{e_k\}$ is the standard basis for $\ell^2(\mathbb{Z})$. Therefore

$$Tf_k = TA^* P e_k = B^*(AA^*|_M)^{-1}(AA^*|_M) P e_k = B^* P e_k = g_k.$$

That is, $g_k = Tf_k$, which implies that the frames are isomorphic.

Remark. Proposition 4.4.21 shows that finite frames are isomorphic if and only if their canonical Gramians are equal. It also says that finite frames are isomorphic if and only if their analysis operators have the same range.

We define the traditional notion of redundancy $Red(\Phi)$ of a frame $\Phi = \{f_k\}_{k=1}^N$ for an n-dimensional Hilbert space $\mathcal{H}$ as the quotient $\frac{N}{n}$. This however, is a customary and crude quantitative notion of redundancy. For literature on other quantitative notions of redundancy (see [5],[6]). In any case, it is known that the redundancy of an over-complete frame is greater than 1.

Remark. We note that unitary isomorphy of frames preserves redundancy of frames. However, equality of redundancy does not, in general translate to unitary isomorphy.

Example 4.4.22 ([21], Example 5.14)**.**

Consider the frames $\Phi = \{e_1, e_1, e_2\}$ and $\Psi = \{e_1, e_2, e_2\}$ where $\{e_k\}$ denotes the orthonormal basis of $\mathbb{R}^2$. Then $Red(\Phi) = Red(\Psi) = \frac{3}{2}$. However the frames are not unitarily isomorphic, since

$$Gram(\Phi) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = Gram(\Psi).$$

Define $\mathfrak{F} := \{\Phi : \Phi \; is \; a \; frame\}$ be the set of frames in a finite dimensional Hilbert space $\mathcal{H}$.

Theorem 4.4.23. *Define a relation $\overset{red}{\sim}$ on $\mathfrak{F}$ by $\Phi \overset{red}{\sim} \Psi$ if and only if $Red(\Phi) = Red(\Psi)$. Then $\overset{red}{\sim}$ is an equivalence relation on $\mathfrak{F}$.*

Let Φ, Ψ, and Ω be in $\mathfrak{F}$. Trivially, $\Phi \overset{red}{\sim} \Phi$, since $Red(\Phi) = Red(\Phi)$. This shows that $\overset{red}{\sim}$ is reflexive. Now suppose $\Phi \overset{red}{\sim} \Psi$. Then $Red(\Phi) = Red(\Psi)$. This is same as $Red(\Psi) = Red(\Phi)$ which implies that $\Psi \overset{red}{\sim} \Phi$. Thus $\overset{red}{\sim}$ is symmetric. Finally, suppose that $\Phi \overset{red}{\sim} \Psi$ and $\Psi \overset{red}{\sim} \Omega$. Then $Red(\Phi) = Red(\Psi)$ and $Red(\Psi) = Red(\Omega)$. Thus $Red(\Phi) = Red(\Psi) = Red(\Omega)$. Thus $\overset{red}{\sim}$ is transitive. This proves the claim.

Remark. Theorem 4.4.23 says that searching for a frame which possesses a predetermined redundancy function is equivalent to searching for the equivalence class.

Corollary 4.4.24 ([4])**.** *Let Φ and Ψ be frames for a finite dimensional Hilbert space $\mathcal{H}$. Let $\widehat{S}_\Phi$ and $\widehat{S}_\Psi$ denote the frame operators of their normalized versions. Then following conditions are equivalent.*
(a). $Red(\Phi) = Red(\Psi)$.
(b). $\widehat{S}_\Phi = \widehat{S}_\Psi$.

Corollary 4.4.24 says that $\overset{red}{\sim}$-equivalent frames must have the same number of non-zero frame vectors.

Theorem 4.4.25. *Unitarily isomorphic and isomorphic frames are $\overset{red}{\sim}$-equivalent.*

In particular, orthonormal bases and Riesz bases/frames are $\overset{red}{\sim}$-equivalent.

Definition 4.4.26. Let $\mathcal{H}$ be a Hilbert space with dimension n and let $\Phi = \{f_k\}$ be a collection of (unit) vectors from $\mathcal{H}$. The `frame potential` of Φ is the number $\mathbb{P}_\Phi = \sum_{i=1}^{k} \sum_{j=1}^{k} |\langle f_i, f_j \rangle|^2$.

The frame potential gives an intuitive idea of the configurations of the vectors which come from tight frames. This notion can be extended to any collection of vectors with varied norms. The inner product between vectors gives a quantity describing the orthogonality of the vectors. For more in the literature about frame potential (see [26]).

Theorem 4.4.27. *Every tight finite frame $\{f_i\}_{i=1}^n$ in a finite dimensional Hilbert space $\mathcal{H}$ has the same frame potential.*

Lemma 4.4.28. *If $\Phi = \{f_i\}_{i=1}^k$ is a tight frame of unit vectors in $\mathbb{R}^n$, then the frame potential of Φ is $\mathbb{P}_\Phi = \frac{k^2}{n}$.*

Proof. Since Φ is a tight frame of unit vectors, the frame bound is $\alpha = \frac{k}{n}$. By definition of a tight frame, we then have

$$\sum_{i=1}^k (\sum_{j=1}^k |\langle f_i, f_j\rangle|^2) = \sum_{i=1}^k \alpha \|f_i\|^2 = \sum_{i=1}^k \alpha = \frac{k^2}{n}.$$

Remark. Frame potential of a frame $\Phi = \{f_i\}_{i=1}^k$ can be described in terms of the trace and the Grammian matrix G. First, recall that $tr(S) = tr(G)$, where $S = A^*A$ and $G = AA^*$. The frame potential can also be given by

$$\mathbb{P}_\Phi = \sum_{i=1}^k \sum_{j=1}^k |\langle f_i, f_j\rangle|^2 = \sum_{i=1}^k \sum_{j=1}^k |G_{i,j}|^2 = tr(G^2) = \sum_{i=1}^k \lambda_i^2,$$

where λ_i are the eigenvalues of G.

The frame potential is minimized when the vectors are as orthogonal as possible. The next result shows that unitary isomorphy preserves frame potential.

Lemma 4.4.29. *If two frames are unitarily isomorphic, then they have equal frame potential.*

Proof. Suppose that $\Phi = \{f_i\}_{i=1}^k$ is a frame for a Hilbert space $\mathcal{H}$. Let $\Psi = \{g_k\}_{k=1}^n$, where $g_k = Uf_k$ for some unitary operator $U \in B(\mathcal{H})$. Then

$$\mathbb{P}_\Psi = \sum_{i=1}^k \sum_{j=1}^k |\langle Uf_i, Uf_j\rangle|^2 = \sum_{i=1}^k \sum_{j=1}^k |\langle f_i, f_j\rangle|^2 = \mathbb{P}_\Phi.$$

Given two $M \times N$ matrices A and B, we define the *Hilbert-Schimdt trace inner product* as $\langle A, B\rangle_{H.S} = tr(AB^*)$. This inner product induces the *Hilbert-Schmidt norm* $\|.\|_{H.S}$ or the *Frobenius norm* on the vector space of all $M \times N$ matrices. Using this distance notion we define a distance function on the space of frames $\mathfrak{F} = \{\Phi : \Phi \ is \ a \ frame\}$.

Definition 4.4.30. Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ be finite frames for an m-dim Hilbert space $\mathcal{H}$. The `frame distance` between them is $d_{\mathfrak{F}}(\Phi, \Psi) = \|\Phi - \Psi\|_{H.S}$.

Clearly the frame distance is a metric on $\mathfrak{F}$.

Definition 4.4.31. Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ be finite frames for an m-dim Hilbert space $\mathcal{H}$. The `Grammian distance` between them is $d_G(\Phi, \Psi) = \|Gram(\Phi) - Gram(\Psi)\|_{H.S}$, where $Gram(\Phi) = AA^*$ and $Gram(\Psi) = BB^*$, where A and B are the analysis operators of Φ and Ψ, respectively.

Clearly the Gram distance is a pseudo-metric, because unitary isomorphism of Φ and Ψ implies $Gram(\Phi) = Gram(\Psi)$, which means that $d_G(\Phi, \Psi) = 0$.

We also define a distance in terms of unitary isomorphy of frames.

Definition 4.4.32. Let $\Phi = \{f_k\}_{k=1}^n$ and $\Psi = \{g_k\}_{k=1}^n$ be finite frames for an m-dim Hilbert space $\mathcal{H}$. The `isomorphy distance` between them is $d_I(\Phi, \Psi) = \inf_{\Phi' \cong \Phi, \Psi' \cong \Psi} \|\Phi' - \Psi'\|_{H.S}$.

Clearly the isomorphy distance is a pseudo-metric, since $d_I(\Phi, \Psi) = 0$ whenever Φ and Ψ are unitarily isomorphic.

Definition 4.4.33. Two frames $\Phi = \{f_n\}_{n=1}^M$ and $\Psi = \{g_n\}_{n=1}^M$ for an N-dimensional Hilbert space $\mathcal{H}$ are said to be `switching equivalent` , denoted $\Phi \overset{s.e}{\cong} \Psi$ if there is a unitary operator $U : \mathcal{H} \to \mathcal{H}$ and a permutation π of the set $J = \{1, 2, ..., M\}$ such that $f_j = Ug_{\pi(j)}$, for all $j \in J$.

We note that switching equivalent frames contain the same vectors but given in a different order.

Theorem 4.4.34. *Two Parseval frames $\Phi = \{f_n\}_{n=1}^M$ and $\Psi = \{g_n\}_{n=1}^M$ for an N-dimensional Hilbert space $\mathcal{H}$ are switching equivalent if and only if there exists a permutation π of the index set $J = \{1, 2, ..., M\}$ such that $Gram(\Phi)_{i,j} = Gram(\Psi)_{\pi(i),\pi(j)}$.*

Proof. Define a matrix

$$P = P_{i,j} = \begin{cases} 1, & if\ \pi(i) = j \\ 0, & otherwise \end{cases}.$$

Let A and B be the analysis operators of the frames Φ and Ψ, respectively. Suppose that $\Phi \overset{s.e}{\cong} \Psi$. Then there is a unitary operator $U : \mathcal{H} \to \mathcal{H}$ and a permutation π of the set $J = \{1, 2, ..., M\}$ such that $f_j = Ug_{\pi(j)}$, for all $j \in J$. Thus $A^* = UB^*P^*$, where U is a unitary operator. This is equivalent to

$$Gram(\Phi) = AA^* = PBU^*UB^*P^* = PBB^*P^* = P(Gram(\Psi))P^*.$$

Thus the Grammians are identical up to conjugation by a permutation matrix. Therefore $Gram(\Phi)_{i,j} = Gram(\Psi)_{\pi(i),\pi(j)}$. Conversely, suppose that $Gram(\Phi)_{i,j} = Gram(\Psi)_{\pi(i),\pi(j)}$. Then $\langle f_i, f_j \rangle = \langle g_{\pi(i)}, g_{\pi(j)} \rangle = \langle Ug_{\pi(i)}, Ug_{\pi(j)} \rangle$. Therefore $f_j = Ug_{\pi(j)}$, for all $j \in J$. That is the frames are switching equivalent.

Remark. Note that if $P = I$ in the proof of Theorem 4.4.34, then the Grammians of the frames Φ and Ψ are equal, which means they are unitarily isomorphic by Theorem 4.4.10. This shows that switching equivalence is weaker than unitary isomorphism.

Theorem 4.4.35. *If two tight frames $\Phi = \{f_n\}_{n=1}^M$ and $\Psi = \{g_n\}_{n=1}^M$ for an N-dimensional Hilbert space $\mathcal{H}$ are unitarily isomorphic then they have the same tightness.*

Proof. Suppose $\{f_k\}$ is α-tight. Then $f = \frac{1}{\alpha}\sum_{k=1}^n \langle f, f_k\rangle f_k, \quad \forall f \in \mathcal{H}$. Taking inner product with f we get

$$\|f\|^2 = \langle f, f\rangle = \frac{1}{\alpha}\sum_{k=1}^n \langle f, f_k\rangle\overline{\langle f, f_k\rangle} = \frac{1}{\alpha}\sum_{k=1}^n |\langle f, f_k\rangle|^2.$$

Now suppose $g_k = Uf_k$, for some unitary operator $U \in B(\mathcal{H})$. Then using the fact that $U^* = U^{-1}$ we get

$$\begin{aligned} f &= \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle f, f_k\rangle f_k = \tfrac{1}{\alpha}\sum_{k=1}^n \langle f, U^{-1}Uf_k\rangle f_k \\ &= \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle (U^{-1})^* f, Uf_k\rangle f_k \\ &= (U^{-1})^* \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle f, Uf_k\rangle f_k \\ &= \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle f, Uf_k\rangle (U^{-1})^* f_k \\ &= \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle f, Uf_k\rangle Uf_k \\ &= \tfrac{1}{\alpha}\textstyle\sum_{k=1}^n \langle f, g_k\rangle g_k \end{aligned}$$

Taking inner product with f gives

$$\|f\|^2 = \frac{1}{\alpha}\sum_{k=1}^n \langle f, g_k\rangle\langle g_k, f\rangle = \frac{1}{\alpha}\sum_{k=1}^n \langle f, g_k\rangle\overline{\langle f, g_k\rangle} = \frac{1}{\alpha}\sum_{k=1}^n |\langle f, g_k\rangle|^2.$$

This shows that $\Psi = \{g_k\}_{k=1}^n$ is also α-tight.

Remark. Theorem 4.4.35 can easily be proved as follows using the Corollary 3.11 and the fact that unitary equivalence of operators preserves norm:

$$\|S_\Psi f\| = \|USU^* f\| = \|Sf\| = \alpha\|f\|^2.$$

Frame isomorphy and unitary isomorphy can be used to uniquely determine equivalence classes of some Hilbert space frames. There are at most finitely many frame equivalence classes, which means that the problem of determining, for instance, tight frames reduces to the problem of finding representatives for each equivalence class and determining which of these equivalence classes is optimal in application. Some classes of frames are enticing to frame theorists and experts because their properties make calculations easier. Knowledge about the frame operators and synthesis operators is also crucial in classifying frames.

4.5 Gabor Frames

Frames having Gabor structure or wavelet structure involve translations and modulations of a fixed function $g \in L^2(\mathbb{R})$, called the window function. A Gabor frame is a sequence for $L^2(\mathbb{R})$ of the form $\{M_{mb}T_{na}g\}_{n,m\in\mathbb{Z}}$, where $M_{mb}T_{na}g(x) = e^{2\pi imbx}g(x-na), \quad a, b > 0$, $T_a, M_b : L^2(\mathbb{R}) \longrightarrow L^2(\mathbb{R})$ are the *translation by a* and *modulation by b operators* defined by $(T_af)(x) = f(x-a)$ and $(M_bf)(x) = e^{2\pi bx}f(x)$, respectively, where $x \in \mathbb{R}$ and $f \in L^2(\mathbb{R})$. Gabor frames are overcomplete frames for $L^2(\mathbb{R})$. A wavelet system takes the form $\{2^{j/2}\psi(2^jx-k)\}_{j,k\in\mathbb{Z}}$, where D is the *dilation operator* $D : L^2(\mathbb{R}) \longrightarrow L^2(\mathbb{R})$ defined by $(Df)(x) = 2^{j/2}f(2x)$, which are orthonormal bases for $L^2(\mathbb{R})$. Wavelet frames are used to obtain Fourier expansion for $f \in L^2(\mathbb{R})$. It is known (see [14], [3] and [6]) that most Gabor frames are overcomplete and that if $ab > 1$, then any Gabor system is incomplete, if $ab = 1$, then a Gabor frame is a Riesz basis, and if $ab < 1$, then a Gabor frame is overcomplete.

Over-complete Gabor frames and wavelet frames have been used in signal detection, image representation, object recognition, noise reduction, sampling theory, wireless communications, filter banks and quantum computing(see [7]).

Chapter 5

SOME APPLICATIONS OF OPERATORS, FRAMES AND GROUP THEORY TO SIGNAL PROCESSING AND CRYPTOGRAPHY

5.1 APPLICATION OF GROUP-THEORETIC CONCEPTS TO CRYPTOGRAPHY

We have seen in Chapter 3 that the most basic primitive for a cryptographic system like the RSA is a trap-door one-way function f which is easy to compute but hard to invert, but f^{-1} is easy to compute when a trapdoor or a secret string of information associated with the function becomes available. The function $g : (p, q) \longrightarrow pq$ for large prime numbers is conjectured to be a one-way and also a trapdoor function, in the sense that given the product $n = pq$, it is extremely hard to know the prime factors p and q or to factor n. The function

$$f(x) = x^e \; mod \; n,$$

where e is relatively prime to $\varphi(n) = (p - 1)(q - 1)$ is a trap-door function. The trapdoor are the large primes p and q, knowledge of which allows one to invert f efficiently. The trapdoor functions help in the design of protocols that allow for entities who have never met or exchanged information to establish a shared secret key by exchanging messages over an unsecured communication channel.

The main task in public-key cryptography like the RSA is to find a suitable trap-door one-way function, so that both encryption and decryption are easy to perform for authorized users, whereas decryption, the inverse of the encryption, should be computationally infeasible for an unauthorized user (the adversary, eavesdropper or the enemy). One of the major advantages of public-key cryptography is that it can be used not only for encryption bust also for digital signatures, a feature which is useful for Internet security and which is not provided by the traditional secret-key cryptography.

Sensitive data exchanged between a user and a Web site needs to be encrypted to prevent it from being disclosed to or modified by unauthorized parties. The encryption must be done in such a way that decryption is only possible with knowledge of a secret decryption key. The decryption key should only be known by authorized parties.

The simple notion of the trapdoor function in RSA finds application in the design of pin numbers and passwords in the telephony, email communication and electronic banking industry(bank transaction, bank account security, Personal Identification Numbers(PINs), passwords, credit card transactions).

We have given examples in Chapter 3, on the encryption and decryption schemes for the RSA. We have shown that for $n = pq$, where p and q are two large integers and e a positive integer, most encryption and decryption protocols utilize a trapdoor function $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ defined by $f(x) = x^e \ mod \ n$. We have shown that if $gcd(e, \phi(n)) = 1$, then this function is the RSA encryption function $RSA_{n,e} : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$ given by $RSA_{n,e}(x) = x^e \ mod \ n$. To decrypt a message securely, there is need for trapdoor, which consists of secret information that permits easy inversion of the encryption key. We have shown in Theorem 3.2.20 that the inverse f^{-1} has a similar form: $f^{-1}(x) = x^d \ mod \ n$ for an appropriate value of d. These trapdoor functions are designed using Euler's theorem. This is where group theory comes into play. Since $ed \equiv 1 \ mod \ \phi(n)$, it follows that $ed = t\phi(n) + 1$, for some integer $t \geq 1$. For $x \in \mathbb{Z}_n^*$, it follows by Euler's Theorem and Fermat's Little Theorem that

$$(x^e)^d \equiv x^{t\phi(n)+1} \ mod \ n \equiv (x^{\phi(n)})^t x \ mod \ n \equiv 1^t x \ mod \ n \equiv x \ mod \ n.$$

The values (n, e) comprise the public key and the values p, q and d form the private key. The security of a public-key cryptosystem like the RSA is based on the belief that the encryption function $f(x) = x^e \ mod \ n$ is a one-way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext. The trapdoor that allows the legitimate receiver to decrypt a ciphertext is the knowledge of the factorization $n = pq$. Since this factorization is known, the receiver can compute $\phi(n) = (p-1)(q-1)$ and then compute the decryption exponent d using the Extended Euclidean algorithm. To be on the safe side, the numbers p and q are chosen(or randomly generated) to be 1024-bit primes, making n a 2048-bit modulus. Factoring a number of this size is beyond the capability of the best current factoring algorithms.

Another application of group-theoretic concepts is in the design of certified or digital signatures for public-key encryption, whose signing, authentication, identification and verification algorithms uses the same concept of the RSA protocol, which is a product of Euler's Theorem. Certified signatures as demonstrated in Chapter 3, can be attached to the public-key encryption messages in such a manner as to bind an entity to its identity to a piece of information (or its signature), hence removing any doubt about the sender of a digital message. With the spread of the internet and electronic banking, data security and guaranteed signatures have taken on a wholly new dimension. These signatures are important in protecting computer systems against illicit entry and manipulation, and safeguarding data files from unauthorised parties, falsification and destruction. Certified signatures help mitigate against entities reneging(disowning a transaction), forgery, alteration of a transaction, and impersonation.

5.2 APPLICATION OF FRAMES AND OPERATORS TO SIGNAL PROCESSING

Hilbert space frames and operators have been effectively used for the reconstruction of bandlimited signals(those with compact support and their Fourier transforms vanish off a compact set) from irregularly spaced sampling points in communication systems(see [10]). The analysis and synthesis operators of frames have been used for signal reconstruction in signal processing. The advantage of frames over bases is that frames can be considered as redundant while they provide stable reconstructions.

The notion of filter or cryptosystem is a linear system. Subjecting a signal through a filter or cryptosystem can be viewed as a multiplication operator

$$\mathcal{F}ilter.Signal = Signal$$

The analysis of a signal $f \in \mathcal{H}$ is typically performed by merely considering its frame coefficients $\langle f, f_i \rangle$. However, if the task is transmission of a signal, the ability to reconstruct the signal from its frame coefficients and also to do so efficiently becomes crucial. However, reconstruction from coefficients with respect to a redundant system is much more delicate and requires the utilization of a dual frame.

Let $\{f_i\}_{i=1}^m$ be a frame for $\mathcal{H}$ with frame operator S. Then for every $f \in \mathcal{H}$ we have

$$f = \sum_i \langle S^{-1}f, f_i\rangle f_i = \sum_i \langle f, S^{-1}f_i\rangle f_i.$$

as the reconstruction formula for f. This formula shows that every vector(or signal)$f \in \mathcal{H}$ can be uniquely reconstructed from a set of measurements $\{\langle f, f_i\rangle\}$ and that this reconstruction is stable.

This has been clearly demonstrated in Examples 4.3.13 and 4.3.18. A MAPLE 18 code has been provided on how to compute the alternate dual frame using the notion of SVD and the pseudo-inverse.

In real life application, a message spoken into a cellphone can be thought of as a vector. The voice message is broken down into a series of coefficients which are digitized, transmitted, and read by a receiver which knows how to transform the coefficients back into an audible sentence. During the transmission, however, some of those coefficients may be scrambled up or lost(This is what happens with payTV,e.g GoTV, DSTV, MTN, Verizon, etc when subscription expires and is not renewed on time!-they erase all coefficients except for some local basic channels like KBC, etc.). If there were extra coefficients used, we have a better chance of understanding the message on the other end, even if it is not perfectly identical to the message that was sent.

Another advantage to redundancy is the variety of frames that exist. Frames are used in a wide variety of applications, each having unique constraints. Orthonormal bases are very restrictive. The elements in an orthonormal basis must all be orthogonal, there can only be exactly as many elements as the dimension of the space, and they must all have unit norm.

Frames can be structured to adjust the weight on each component by having vectors with varying norms. Frames exist which pay special attention to some parts of a signal by grouping more vectors in these areas. This is accomplished by constructing a frame with varied spacing (measured by the inner products). between vectors.

Phase retrieval is the problem of recovering a signal from the absolute values of linear measurement coefficients (frame coefficients) called intensity measurements. Note that multiplying a signal by a unimodular constant does not affect these coefficients, so we seek signal recovery modulo a unimodular constant. In [8], they determine what kind of reconstruction is possible if we only have knowledge of the absolute values of the frame coefficients.

Compared to orthonormal bases, frame bases are generally over-complete. It turns out that this property is very advantageous for many applications. It makes frame bases a very flexible tool for analysis and syntheses of signals in many branches of information theory.

During transmission of a signal through a channel(telephone, atmosphere, etc) there is possibility of noise, which may be caused by several factors including lightning, radio disturbance, electromagnetic waves. To protect a message or signal against noise we should encode it by adding some redundant information to it. This is the essence of the notion of redundancy associated with over-complete frames.
In such a case, even if the message is corrupted by a noise, there will be enough redundancy in the encoded message to recover or decode the message completely.

A good example is given in Example 4.3.18, where the signal $f = \begin{pmatrix} -5 \\ 2 \end{pmatrix}$ in the Hilbert space $\mathbb{R}^2$ has been expanded as a linear combination of the frame vectors. Since the frame $\{f_i\}_1^3$ in this example is over-complete, the signal can still be expanded as a linear combination of two of the frame vectors in case one frame vector is lost during the transmission. It is also demonstrated how the original signal can be reconstructed from the alternate dual frame of the original frame.

The analysis operator $A : \mathcal{H} \longrightarrow \ell^2(\mathbb{Z})$ denined by $f \longmapsto \{\langle f, f_i \rangle\}$ is the main tool used for discretization of a signal $f \in \mathcal{H}$ using a frame $\{f_i\}$ for a Hilbert space $\mathcal{H}$. Any signal $f \in \mathcal{H}$ can be fully represented by the discrete vector Af. This means that the original signal can be recovere from the discrete representation Af. In other words, f and Af contain the same information.

The Grassmannian operator $G = AA^*$, where A is the analysis operator of a frame and its pseudo-inverse $G^\dagger$ play a crucial role in the process of digital reconstruction from frame representation. The fact that G operates on $\ell^2(\mathbb{Z})$, a Hilbert space of countable sequences(digital sequences) immediately suggests that it is possible to implement G on a digital machine. The size of the kernel of G is directly related to the robsutness to noise in the representation.

Chapter 6

CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER RESEARCH

6.1 SUMMARY

In this thesis we have shown major results:

In Chap 1, we have given notations, definitions and very important results that we have used in the rest of the chapters in this thesis.

In Chapter 2, we have given literature review to the study and stated the statement of the problem. We have also stated the main objective, the specific objectives and the significance of the study.

In Chapter 3, we have successfully identified the trap-door function in the RSA cryptosystem as

$$RSA_{n,e}(x) = x^e \; mod \; n,$$

where n is a product of two large primes p and q and $gcd(e, \varphi) = 1$, where $\varphi(n)$ is the Euler (totient) function defined by $\varphi(n) = \varphi(pq) = (p-1)(q-1)$. We have shown that the trapdoor information is a number d such that

$$d.e \equiv 1 \; mod \; \varphi(n).$$

We have demonstrated that as a collective, the RSA can be viewed as

$$RSA = \Big\{ RSA_{n,e} : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*,\ where\ RSA_{n,e}(x) = x^e\ mod\ n,\ n = pq,\ gcd(e, \varphi(n)) = 1 \Big\}$$

We have used Theorem 3.2.13(Lgrange) and Theorem 3.2.16(Euler's Theorem) and Fermat's Little Theorem and examples, we have demonstrated how the public key cryptosystme RSA works. We have used Maple to carry out most of the modular arithmetic involving large prime integers and were able to randomly generate large positive integers and test their primality.

In Theorem 3.2.20, we have also shown that the trapdoor function $RSA_{n,e}$ is a permutation over the cyclic multiplicative group $\mathbb{Z}_n^*$.

We have also shown that it is hard to break or hack the RSA because the factors of n cannot be computed in any easy way. We have also shown that for encryption to work, a message block must be coded as an integer in the interval $0 \leq M \leq n-1$.
We have also shown that RSA signature key consists of a pair (k_s, k_p), where $k_s = (n, e)$ is the secret signing key and $k_p = (n, d)$ is the public verifying key and that faking this signature is akin to breaking the RSA.

In Chapter 4, we have shown the many major results. We have demonstrated how to determine the analysis, synthesis and frame operator for a given frame in a Hilbert space. We have demonstrated how to use the singular value decomposition(svd) and the notion of a pseudo-inverse to find a dual to a frame, the canonical dual and the canonical tight frame. This has been shown in Examples 4.3.5, 4.3.13, 4.3.14 and 4.3.18.

In Theorem 4.3.9, we have shown that if $\{f_k\}_{k=1}^n$ is a frame for a Hilbert space $\mathcal{H}$ with a frame operator S and $T : \mathcal{H} \longrightarrow \mathcal{H}$ is an operator on $\mathcal{H}$, then the sequence $\{Tf_k\}_{k=1}^n$ is a frame with frame operator TST^*.

In Theorem 4.3.17, we have shown that duality of frames for the same Hilbert space $\mathcal{H}$ is an equivalence relation.

In Theorem 4.3.19, we have shown that if $\{f_k\}$ is a normalized tight frame for a Hilbert space $\mathcal{H}$ and $T \in B(\mathcal{H})$ is invertible, then the frames $\{T^* f_k\}$ and $\{T^{-1} f_k\}$ are dual to each other.

In Corollary 4.4.12, we have shown that unitarily isomorphic finite frames have unitarily equivalent operators. We have also shown in Corollary 4.4.13 that unitarily isomorphic finite frames have the same frame operators. In Theorem 4.4.17, we have shown that unitarily isomorphic frames have the same frame bounds.

In Chapter 5, we have have given some of the applications of Hilbert space frame operators and group theory in signal processing and cryptography. We have also discussed some applications of cryptography.

6.2 FURTHER RESEARCH

Part of this thesis has focussed on results involving finite frames for finite dimensional Hilbert spaces and their applications to signal processing. Further research could be carried out involving infinite dimensional Hilbert spaces and their applications. More work can also be done on Gabor frames and wavelets in signal processing. We also suggest a new direction on the use of group transforms, especially those that are 'fast', for coding and pattern recognition purposes, and group filters, for signal estimation.

In this thesis, we have focussed on RSA and how it works. Further research can be carried out in other public key cryptosystems.

Almost all widely used encryption procedures are based on results in group theory(especially, number theory) and involve computations of large integers. In is interesting to investigate whether frames can also be used in the design of cryptosystems.

References

[1] R. Balan, *Equivalence relations and distances between Hilbert frames*, Proc. Amer. Math. Soc. **128, No.8** (1999), 2353–2366.

[2] P. Balazs, *Frames and finite dimensionality:Frame transformation, classification and algorithms*, Applied Mathematical Sciences **2, No. 43** (2008), 2131–2144.

[3] J. J. Benedeto and D. Colella, *Wavelet analysis of spectrogram seizure chirps*, Proc. SPIE Wavelet Appl. in Signal and Image Proc. III **2569, San Diego, CA** (July 1995), 512–521.

[4] B.G. Bodmann, P.G. Casazza, and G. Kutyniok, *A quantitative notion of redundancy for finite frames*, Applied and Computational Harmonic Analysis **30, Issue 3** (2011), 348–362.

[5] A. M. Bruckstein, D. L. Donoho, and M. Elad, *From sparse solutions of systems of equations to sparse modeling of signals and images*, SIAM Review **51** (2009), 34–81.

[6] P. G. Casazza and G. Kutyniok, *Finite Frames: Theory and Applications, Applied and Numerical Harmonic Analysis*, Birkhauser, New York, 2013.

[7] O. Christensen, *Introduction to Frames and Riesz Bases*, Birkhauser, Boston, MA, 2003.

[8] I. Daubechies, *Ten lectures on wavelets*, CBMS-NSF, SIAM, Philadelphia, 1992.

[9] I. Daubechies, A. Grossman, and Y. Meyer, *Painless nonorthogonal expansions*, J. Math. Phys. **27(5)** (May, 1986), 1271–1283.

[10] R.J. Duffin and A.C. Schaeffer, *A class of nonharmonic Fourier series*, Trans. Amer. Math. Soc. **72** (1952), 341–366.

[11] G. Gabor, *Theory of communication*, J. Inst. Electr. Eng.(London) **93** (1946), 429–457.

[12] R. Harkins, E. Weber, and A. Westmeyer, *Encryption schemes using finite frames and Hadamard arrays*, Experimental Math. **14** (2005), 423–433.

[13] L. Hogben, *Handbook of Linear Algebra*, CRC Press Taylor & Francis, 2014.

[14] A. J. E. M. Janssen, *Duality and biorthogonality fof weyl-heiseberg frames*, J. Fourier Anal. Appl. **1, No. 4** (1995), 403–436.

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

[16] J.S. Kraft and L.C. Washington, *An Introduction to Number Theory with Cryptography*, CRC Press, Florida, 2018.

[17] J.R. Miotke and Rebollo-Neira, *Oversampling of Fourier coefficients for hiding message*, Applied and Computational Harmonic Analy. **16** (2004), 203–207.

[18] L. Njagi, B. M. Nzimbi, and S. K. Moindi, *On analysis and synthesis operators and characterization of the synthesis matrix of a frame in terms of the frame operator*, Journal of Advance Research in Mathematics and Statistics **5, Issue 12** (2018), 1–10.

[19] ______, *On finite dimensional Hilbert space frames, dual and normalized frames and pseudo-inverse of the frame operator*, Journal of Advance Research in Mathematics and Statistics **5, Issue 11** (2018), 1–14.

[20] ______, *A note on isomorphy and unitary isomorphy of Hilbert space frames*, International Journal of Mathematica Trends and Technology(IJMTT) **65, Issue 1** (2019), 15–30.

[21] ______, *On pseudo-inverses and duality of frames in Hilbert spaces*, International Journal of Mathematics and its Applications(IJMAA) **7, Issue 2** (2019), 75–88.

[22] B.M. Nzimbi, G.P. Pokhariyal, and S.K. Moindi, *A note on metric equivalence of some operators*, Far East J. of Math. Sci.(FJMS) **75, No.2** (2013), 301–318.

[23] D. A. Osvik, A. Shamir, and E. Tromer, *Cache attacks and countermeasures:the case of aes*, Springer, 2006.

[24] P. Prandoni and M. Vetterli, *Signal Processing for Communications*, CRC Press, Boca Raton, Florida, 2008.

[25] R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key crypstosystems*, Commun. of the ACM **21** (1978), 120–126.

[26] S.F.P. Waldron, *An Introduction to Finite Tight Frames*, Birkhauser, 2018.