2006

Extension of Shor's period-finding algorithm to infinite dimensional Hilbert spaces

Jeremy James Becnel
Louisiana State University and Agricultural and Mechanical College

EXTENSION OF SHOR'S PERIOD–FINDING ALGORITHM
TO INFINITE DIMENSIONAL HILBERT SPACES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Jeremy James Becnel
B.S. in Mathematics, Nicholls State University, 2001
B.S. in Computer Science, Nicholls State University, 2001
M.S. in Mathematics, Louisiana State University, 2002
August 2006

Dedication

This dissertation is dedicated to my daughter, Alyssa ... may all your dreams come true.

Acknowledgments

This dissertation would not have been possible without several contributions. First and foremost, it is a pleasure to thank my advising professor, Dr. Ambar Sengupta. Throughout my time at LSU, Professor Sengupta has been extremely generous with his insight and knowledge. Despite the many demands on his time, he was always willing to discuss my work and offer his suggestions. He also had a unique and important ability to address and solve any concerns I had during some of my more stressful times here.

I would also like to thank the members of my committee, Drs. Kuo, Morales, Smolinsky, and Sundar. A special thanks to Dr. Kuo for his help and for writing a very useful book on White Noise Distribution Theory.

I am also very grateful for the generous financial support given to me by the university and mathematics department throughout my time at LSU.

I am also pleased to thank the good friends I made here at LSU: Tim, Bill, Deb, Troels, Misi, and Pietro. We shared many good times and had a lot of fun. I wish the best for you all, and hope to always maintain the friendships we have formed.

Finally, I would like give a special thanks to my wife, Kesha. Her support and sacrifice allowed my dream of obtaining a doctorate in mathematics to become a reality.

Table of Contents

Abstract

Over the last decade quantum computing has become a very popular field in various disciplines, such as physics, engineering, and mathematics. Most of the attraction stemmed from the famous Shor period–finding algorithm, which leads to an efficient algorithm for factoring positive integers. Many adaptations and generalizations of this algorithm have been developed through the years, some of which have not been ripened with full mathematical rigor. In this dissertation we use concepts from white noise analysis to rigorously develop a Shor algorithm adapted to find a hidden subspace of a function with domain a real Hilbert space. After reviewing the framework of quantum mechanics, we demonstrate how these principles can be used to develop algorithms which operate on a quantum computing device. We present a self-contained account of white noise analysis, including the main relevant results. Inspired by a generalized function in the algorithm, we develop a new distribution, the delta function for a subspace of an infinite dimensional Hilbert space. We then use this distribution to rigorously prove one of the main identities needed for the algorithm. Finally we provide a rigorous formulation of the hidden subspace algorithm in infinite dimensions.

Chapter 1

Introduction

The field of quantum computing gained much fame with the development of Shor's quantum factoring algorithm in 1995. Using the fundamental ideas from the factoring algorithm and a few new concepts many new quantum algorithms have been constructed. At first most quantum algorithms were designed to run on a finite dimensional state space. However, in recent years many researchers have turned their attention to developing quantum algorithms which operate on state spaces of infinite dimension.

The present work began as an attempt to develop a quantum algorithm on an infinite dimensional state space which computes the famous Jones polynomial, a principal concept in knot theory. Such an algorithm is conjectured possible in the work by Lomonaco and Kauffman [21]. In order to do this, we began by examining a baby version of such an algorithm, the quantum hidden subspace algorithm. This algorithm takes a function ϕ on a Hilbert space and attempts to find a subspace V such that $\phi(x+v) = \phi(x)$ for all $v \in V$. This algorithm is also presented in [21], but only at a very formal level. It is based on being able to do computation in the spirit of Feynman path integrals.

When trying to derive a rigorous mathematical formulation of this algorithm many interesting results presented themselves. Many of these centered around trying to make sense of the formal distributional identity

$$\int_V \delta(x-v)\, Dv = \int_{V^\perp} e^{2\pi i \langle x,u \rangle}\, Du$$

where Dv and Du are Lebesgue type measures on the subspaces V and $V^\perp$ of a real Hilbert space E. In order to formalize such notions we turned to the theory of White Noise Analysis, which is the theory of distributions in infinite dimensions. The background material needed for White Noise Analysis and a summary of the subject are presented in chapters 4 and 5, respectively.

With the tools of White Noise Analysis we develop the concept of a delta function of a subspace V. This is presented in chapter 6. We also formulate and prove a mathematically rigorous formulation of the above equation in chapter 7.

Finally, we apply the theory of White Noise Analysis in chapter 8 to present a complete mathematically rigorous quantum algorithm for finding a hidden subspace.

Chapter 2

Quantum Mechanics

At the turn of the twentieth century Einstein developed the general theory of relativity. This theory is successful in describing the geometric structure of the universe and in showing how matter affects and is affected by this structure. However, it does not provide an answer to a question that puzzled physicists at the time (and to an extent still does today): What exactly is matter? Physicists developed quantum theory in an attempt to provide an answer to this question.

The first step toward quantum theory stemmed from a puzzle created by Maxwell's electromagnetic theory. Maxwell's enigma was that the total energy generated in an enclosed "black oven" (sealed, lightproof metal box with heated walls) should be infinite according to his theory. He reasoned that the walls would emit electromagnetic radiation of all possible frequencies—of which there are infinitely many.

In 1900, Max Planck offered a solution. He suggested that energy comes in discrete "clumps" which he called quanta, and these quanta cannot be subdivided. He even calculated the proportion between the energy and the frequency of a wave—what is now known as Planck's constant. However, Planck was not able to answer the most obvious question: Why should energy comes in "clumps"?

Einstein answered this riddle in 1905 when he proposed that a light wave is made of discrete packets of energy called photons. He reasoned that Planck's quanta are the photons that make up the wave. Now, what does it mean to say that particles constitute a wave? Even today no one really knows. So, in the realm of quantum mechanics physicists have to abandon their intuitions and rely on mathematics—in particular, the theory of Hilbert spaces.

2.1 Framework of Quantum Mechanics

Quantum Mechanics can be thought of as a means for the development of physical theories. The subject does not tell you what laws a physical system obeys; it provides a framework for deducing such laws. Here we will briefly describe the postulates of quantum mechanics. These postulates were derived from a long process of trial and error. Also, the motivation for these postulates is not always clear—even to the expert.

2.1.1 State Space

The first postulate tells us about the structure of a physical system.

Postulate 1. Associated to an isolated physical system is a Hilbert space known as the *state space* of the system. The system is completely described by its *state vectors*, which are unit vectors in the state space of the system.

Notation. State vectors in a state space are usually denoted by $|\phi\rangle$. The condition that $|\phi\rangle$ is a unit vector is usually expressed in inner–product notation as $\langle\phi|\phi\rangle = 1$, where $\langle\phi|$ denotes the linear functional in the dual of the state space given by the inner–product of a vector with $|\phi\rangle$. Also, the orthogonal projection onto a unit vector $|\phi\rangle$ is written as $|\phi\rangle\langle\phi|$. This is the Dirac notational convention.

Unfortunately, this postulate does not tell us what the state space is for a physical system; it only tells us that one exists. Finding the exact state space for a physical system can be a difficult problem.

Example 2.1. The simplest quantum mechanical system, and the one most common in quantum computing, is the *qubit.* The state space of the qubit is $\mathbb{C}^2$. It can be represented physically by two electronic levels in an atom. In this model, an electron can exist in a ground state or an excited state. By shining light of a particular intensity on the atom for an appropriate amount of time, it is possible to the move the electron from a ground state to an excited state and vice versa. What is perhaps more interesting is that by reducing the the amount of time we shine the light, an electron initially in a ground state will move into a state "between" the excited and ground states.

The standard orthonormal basis elements for $\mathbb{C}^2$ are denoted by $|0\rangle$ and $|1\rangle$. (These correspond to our ground and excited states in the atom model.) Hence an arbitrary state vector in this system can be expressed as

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. The vector $|\phi\rangle$ is called a *superposition* of the states $|0\rangle$ and $|1\rangle$. Also, the state $|\phi\rangle$ is said to be a *pure state* when either $\alpha = 0$ or $\beta = 0$; otherwise, it is called a *mixed state.*

Example 2.2. Another classical example of a state space is $L^2(\mathbb{R}^3)$, used in the study of wave functions.

2.1.2 Evolution

The next postulate tells us how the quantum system changes with time.

Postulate 2 (Discrete Version)**.** A unitary operator on the state space relates the state of a closed quantum system at different times.

This postulate tells us that $|\phi_1\rangle$, the state of the system at time t_1, is related to $|\phi_2\rangle$, the state of the system at time t_2, by a unitary operator U depending only on t_1 and t_2. That is,

$$|\phi_2\rangle = U|\phi_1\rangle$$

Let us note that just as the framework of quantum mechanics does not tell us the state space or state of a particular quantum system, it also does not tell us which unitary operator U describes the evolution between states at two different times; it only assures us that such a U exists.

Example 2.3. Let us now return to the qubit of Example 2.1 and look at some common unitary transformations on this space. The unitary transformations

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

along with the identity, make up what are known as the *Pauli matrices*. These are often used in the study of quantum computation. In particular, the matrix X is sometimes called the *bit flip* matrix, since it takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.

Another useful unitary operator in quantum computing is the *Hadamard gate* given by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Postulate 2 describes how the quantum states of a closed system at two different times are related. This postulate can be refined to describe the evolution of a quantum system in continuous time.

Postulate 2 (Continuous Version)**.** In a closed quantum system, the time evolution of the system's state is described by the *Schrödinger equation*,

$$i\hbar \frac{d|\phi\rangle}{dt} = H|\phi\rangle$$

where $\hbar$ is *Planck's constant* and H is a fixed Hermitian operator known as the *Hamiltonian* of the system.

To see that the discrete version of Postulate 2 agrees with with the continuous version, observe that when H is constant with respect to t, the Schrödinger equation yields the solution

$$U_t = e^{-itH/\hbar}$$

It is easy to check that U_t is the unitary operator guaranteed by the discrete version of Postulate 2. That is, if $|\phi_1\rangle$ is the state of the system at time t_1, and $|\phi_2\rangle$ is the state of the system at time t_2, then

$$|\phi_2\rangle = U_{t_2 - t_1}|\phi_1\rangle$$

When H depends on t, the solution to the Schrödinger equation is a bit more complicated, but in the special case when H_s and H_t commute for all s, t a little differential equations can offer the formal solution

$$|\phi_t\rangle = \exp\left(\frac{-i}{\hbar}\int_0^t H_s\, ds\right)|\phi_0\rangle$$

2.1.3 Measurement

Now that we know the structure of a quantum system and how this structure evolves, we must develop a means by which to observe the system. This action of observing no longer leaves the system closed, and thus does not require the use of unitary operators. The next postulate describes the effects of measurement on a quantum system.

Postulate 3. Quantum measurements are described by a collection of operators $\{M_m\}$ on the state space of the system. These operators must satisfy the *completeness relation*

$$\sum_m M_m^* M_m = I$$

Each M_m is called a *measurement operator* and the index m refers to a measurement outcome that may occur in the experiment. If the quantum system is in the state $|\phi\rangle$ before a measurement takes place, then the probability that the result m occurs is given by

$$p(m) = \langle\phi|M_m^* M_m|\phi\rangle$$

Moreover, the state of the system after the measurement is

$$\frac{M_m|\phi\rangle}{\sqrt{p(m)}}$$

Postulate 3 is a bit discouraging in that we cannot directly observe the state of a quantum system—as the mere act of doing so destroys the current state and places the system in another state. However, we will see that people have devised clever methods of getting around this.

Note that the completeness relation assures us that the probabilities of each possible outcome sum to 1. Observe

$$\sum_m p(m) = \sum_m \langle\phi|M_m^* M_m|\phi\rangle = \langle\phi|\Big(\sum_m M_m^* M_m\Big)|\phi\rangle = \langle\phi|I|\phi\rangle = \langle\phi|\phi\rangle = 1$$

Also, as a consequence of Postulate 3, we can make no distinction between the states $|\phi\rangle$ and $e^{i\theta}|\phi\rangle$ since $\langle\phi|e^{-i\theta}M_m^* M_m e^{i\theta}|\phi\rangle = \langle\phi|M_m^* M_m|\phi\rangle$. In the state $e^{i\theta}|\phi\rangle$, we call $e^{i\theta}$ the *phase factor* and we say $e^{i\theta}|\phi\rangle$ is equal to $|\phi\rangle$ up to a *global phase factor*.

Projective Measurements

An important special case of Postulate 3 is projective measurements. They are used in many applications of quantum computation.

Postulate 3 (Projective Measurements)**.** A Hermitian operator, M, on the state space of the system describes a projective measurement. The operator M is called an *observable* and has spectral decomposition given by

$$M = \sum_m m P_m$$

where P_m is the orthogonal projection onto the eigenspace of M with eigenvalue m. Each eigenvalue m of the observable corresponds to a possible outcome of the experiment. If the system is in state $|\phi\rangle$ before the measurement, then the probability of obtaining the result m is given by

$$p(m) = \langle\phi|P_m|\phi\rangle$$

and upon the outcome m occurring, the state of the system immediately after the measurement is

$$\frac{P_m|\phi\rangle}{\sqrt{p(m)}}$$

Remark 2.4. Often a set of projections $\{P_m\}$ is provided satisfying $\sum_m P_m = I$ and $P_m P_n = \delta_{mn} P_m$. The observable is understood to be $M = \sum_m m P_m$.

Another common practice is to *measure in the basis* $|m\rangle$ where $\{|m\rangle\}$ forms an orthonormal basis for the state space. In this case the observable is given by $M = \sum_m m|m\rangle\langle m|$.

Remark 2.5. Projective measurements are equivalent to the first version of Postulate 3, when the projective measurements are given the ability to perform unitary transformation, as described in the discrete version of Postulate 2.

Example 2.6. Let us again consider the state space of the qubit with standard orthonormal basis $|0\rangle$ and $|1\rangle$. Suppose the state space is in that state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

where $\alpha, \beta \in \mathbb{C}$. It is important to note that when performing a measurement on $|\phi\rangle$, what is actually being observed is j, where $j = 0$ signifies the state $|0\rangle$ and $j = 1$ signifies the state $|1\rangle$. Now measuring $|\phi\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ we see that

$$p(0) = \langle 0|\phi\rangle\langle\phi|0\rangle = |\alpha|^2 \qquad \text{and} \qquad p(1) = \langle 1|\phi\rangle\langle\phi|1\rangle = |\beta|^2$$

gives us the probability of observing the state $|0\rangle$ and $|1\rangle$, respectively. Also, the state of the system after the measurement is $|0\rangle$ if measurement outcome 0 occurred and $|1\rangle$ if measurement outcome 1 occurred.

2.1.4 Composite Systems

The next postulate describes how the state space of a quantum system can be built from the state spaces of many distinct quantum systems. It gives us a canonical way of describing composite systems in quantum mechanics.

Postulate 4. Suppose we have n physical systems with state spaces $H_1, H_2, \cdots, H_n$, respectively. Then the state space of the composite physical system is given by $H_1 \otimes H_2 \otimes \cdots \otimes H_n$, the tensor product of the state spaces of the component physical systems. Moreover, if system number i is in state $|\phi_i\rangle$, then the state of the composite system is given by $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$.

Notation. The composite state $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$ is often written $|\phi_1\rangle|\phi_2\rangle \cdots |\phi_n\rangle$ or $|\phi_1\phi_2\cdots\phi_n\rangle$

Example 2.7. In Example 2.1, we said that the state space of different polarizations of n photons is given by $\mathbb{C}^{2^n}$. When considering only 1 photon we have the qubit state space $\mathbb{C}^2$. So, as per Postulate 4, the state space for the composite system of n photons is given by $\bigotimes_1^n \mathbb{C}^2$, which is canonically isomorphic to the space $\mathbb{C}^{2^n}$ in Example 2.1.

Entangled States

Perhaps the most intriguing notion arising from Postulate 4 is that of *entanglement* in composite quantum systems. A state $|\phi\rangle \in H_1 \otimes H_2$ is said to be *entangled* if it cannot be written as $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ where $|\phi_1\rangle$ and $|\phi_2\rangle$ are state vectors in H_1 and H_2, respectively. A simple example of an entangled state occurs when $H_1 = H_2 = \mathbb{C}^2$, where H_1 and H_2 are both given the standard orthonormal basis $\{|0\rangle, |1\rangle\}$. The state

$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

is an entangled state. This can be easily verified with a wee bit of algebra.

Chapter 3

Quantum Algorithms

Quantum Computation is the study of information processing tasks that can be carried out on a quantum mechanical system. Such a system can be considered a quantum computer. In this chapter we explore some of the more important algorithms that have been developed to run on a quantum mechanical system. We begin by examining what is considered the most important tool in the development of quantum algorithms, the quantum Fourier transform.

3.1 Fourier Transform

Suppose we are working in the vector space $\mathbb{C}^N$ with orthonormal basis given by $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. We define the *quantum Fourier transform* to be the linear operator $\mathcal{F}$ with the following effect on the orthonormal basis:

$$\mathcal{F}|l\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ilk/N}|k\rangle$$

To see that the quantum Fourier transform is a unitary linear operator, it suffices to show that $\langle l|\mathcal{F}^*\mathcal{F}|m\rangle = \delta_{lm}$ for any $|l\rangle, |m\rangle$ in the orthonormal basis. Observe

$$\langle m|\mathcal{F}^*\mathcal{F}|l\rangle = \frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi imk/N} e^{2\pi ilk/N} \langle k|k\rangle = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i(l-m)k/N} \tag{3.1}$$

Now if $l = m$, then the above sum is 1. If $l \neq m$, then using the algebraic identity $1 + x + x^2 + \cdots + x^{N-1} = \frac{1-x^N}{1-x}$ the above becomes

$$\frac{1 - e^{2\pi i(l-m)}}{1 - e^{2\pi i(l-m)/N}} = 0 \tag{3.2}$$

3.1.1 Product Representation

We now focus on the n qubit state space $\mathbb{C}^{2^n}$ with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$. In this space, the Fourier transform has a useful representation. Before we derive this, we adopt some notational conventions. It will be convenient to write the state $|l\rangle$ using the binary representation $l = l_1 l_2 \ldots l_n$, where $l = l_1 2^{n-1} + l_2 2^{n-2} + \ldots l_n 2^0$. We also adopt the binary fraction notation for $0.l_m l_{m+1} \ldots l_p$. That is

$$0.l_m l_{m+1} \ldots l_p = \frac{l_m}{2} + \frac{l_{m+1}}{4} + \cdots \frac{l_p}{2^{p-m+1}}$$

Now we can derive the *product representation* for the quantum Fourier transform on the n qubit space.

$$\begin{aligned}
\mathcal{F}|l\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i l k/2^n} |k\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i l \sum_{j=1}^{n} k_j 2^{-j}} |k_1 \cdots k_n\rangle \text{ changing to binary notation} \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{j=1}^{n} e^{2\pi i l k_j 2^{-j}} |k_j\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{j=1}^{n} \sum_{k_j=0}^{1} e^{2\pi i l k_j 2^{-j}} |k_j\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{j=1}^{n} \left[|0\rangle + e^{2\pi i l 2^{-j}} |1\rangle \right]
\end{aligned}$$

(3.3)

$$\begin{aligned}
&= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.l_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0.l_{n-1} l_n} |1\rangle \right) \cdots \left(|0\rangle + e^{2\pi i 0.l_1 l_2 \cdots l_n} |1\rangle \right) \\
&\qquad \text{since } e^{2\pi i l 2^{-j}} = \exp(2\pi i l_1 \cdots l_{n-j}.l_{n-j+1} \cdots l_n) = \exp(2\pi i 0.l_{n-j+1} \cdots l_n)
\end{aligned}$$

The product representation (3.3) for the quantum Fourier transform is very useful in a number of quantum algorithms. In particular, it makes up the crux of the Phase Estimation algorithm, which is discussed in the next section.

3.2 Phase Estimation

The phase estimation algorithm is the fountainhead of many other quantum algorithms and relies heavily on the quantum Fourier transform. In a state space, suppose we have an unitary operator U with eigenvector $|\phi\rangle$ and eigenvalue $e^{2\pi i u}$, where u has an unknown value between 0 and 1. The phase estimation procedure finds an approximation for u.

3.2.1 Procedure

The phase estimation procedure requires two registers. The first register is an n qubit state vector initialized to $|0\rangle$. The second register is initialized to the state $|\phi\rangle$. We begin by applying the Hadamard $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ gate to each of the n qubits initialized to 0 to create a superposition of all the orthonormal basis states in the state space $\mathbb{C}^{2^n}$. At the end of this step the first register is in the state

$$\frac{1}{\sqrt{2^n}} \bigotimes_{k=0}^{2^n-1} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \cdots (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \tag{3.4}$$

For the next step we must assume we have available a *black box* that can perform the controlled–U^j on the vector $|\phi\rangle$. That is, upon reading a $|1\rangle$ in the k^{th} qubit, the controlled–$U^{2^{n-k}}$ operator would apply $U^{2^{n-k}}$ to $|\phi\rangle$ and would do nothing when a $|0\rangle$ is read. Black boxes such as these are often referred to as *oracles*. Applying such an oracle places the first register in the state:

$$\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 2^{n-1} u}|1\rangle\right) \left(|0\rangle + e^{2\pi i 2^{n-2} u}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 2^{0} u}|1\rangle\right) \tag{3.5}$$

Observe that (3.5) above looks strikingly similar to the product representation of the quantum Fourier transform given in (3.3). In fact, by applying the inverse quantum Fourier transform, $\mathcal{F}$, to the above state we get an approximation for u. To see why this is so, suppose that that u can be written using exactly n bits. That is, $u = 0.u_1 u_2 \dots u_n$. Then (3.5) becomes

$$\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.u_n}|1\rangle\right) \left(|0\rangle + e^{2\pi i 0.u_{n-1}u_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.u_1 u_2 \dots u_n}|1\rangle\right) \tag{3.6}$$

Now (3.6) is exactly equal to the product representation for $\mathcal{F}|u_1 \dots u_n\rangle$. Therefore applying the inverse quantum Fourier transform will give put us in the state $|u_1 \dots u_n\rangle$, which when measuring in the basis yields the state $|u_1 \dots u_n\rangle$. From this we can compute $u = 0.u_1 u_2 \dots u_n$.

In many cases we will not be able to express the eigenvalue u using a fixed number of bits. For an arbitrary $u = 0.u_1 u_2 \dots u_n u_{n+1} \dots$ we can obtain an approximation $\tilde{u}$ for u. In fact, it can be shown that it requires

$$n = m + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$$

qubits to obtain an m–bit approximation, $\tilde{u}$, to u with a probability of success at least $1 - \varepsilon$ (see pages 223 and 224 in [24]).

Many interesting quantum algorithms rely heavily upon the quantum phase estimation algorithm. The most famous of which is Shor's Factoring Algorithm.

Below we provide a summary of the the Quantum Phase Estimation algorithm.

Algorithm: Quantum Phase Estimation

Inputs: $n = m + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$ qubits initialized to 0; an eigenstate $|\phi\rangle$ of U with eigenvalue $e^{2\pi iu}$; a black box that performs the controlled–U^k operation

Outputs: An m–bit approximation $\tilde{u}$ to u, with probability of success at least $1 - \varepsilon$

Procedure:

1. Start in the initial state: $|0\rangle|\phi\rangle$
2. Apply $H^{\otimes n} \otimes I$ to create superposition:
$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|\phi\rangle$$
3. Apply the black box:
$$\begin{aligned} &\rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle U^k|\phi\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi iku}|k\rangle|\phi\rangle \end{aligned}$$
4. Apply $\mathcal{F}^{-1} \otimes I$:
$$\rightarrow |\tilde{u}\rangle|\phi\rangle$$
5. Measure the first register with respect to the basis $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$:
$$\rightarrow |\tilde{u}\rangle$$

3.3 Shor's Factoring Algorithm

Shor's Factoring Algorithm is responsible for much of the interest surrounding the subject of quantum computing in the past decade. This algorithm simply takes a positive composite integer N and returns a non–trivial factor of N. What is so remarkable is that it can accomplish this task *efficiently*, whereas there is no known *efficient* algorithm that performs this task on a classical computer. By efficient, we mean the algorithm runs and completes in polynomial time in the number of bits it takes to represent the problem.

The algorithm relies on being able to find the order p of an integer a modulo N. That is, $p > 0$ is the smallest integer such that $a^p \equiv 1 \pmod{N}$.

3.3.1 Order–Finding

Essentially, the quantum algorithm for order–finding boils down to applying the phase estimation algorithm to the unitary operator defined by

$$U|b\rangle = |ab \mod N\rangle$$

where a and N are coprime with $a < N$. However, in order to apply the phase estimation algorithm to U, we must know an eigenstate of U. This is the subject of the next proposition.

Proposition 3.1. *If a has order p with respect to N, then the state*

$$|u_s\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} |a^k \mod N\rangle$$

is an eigenvector of U with eigenvalue $e^{2\pi is/p}$ for all integers s with $0 \leq s \leq r-1$.

Proof. Observe

$$\begin{aligned}
U|u_s\rangle &= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} U|a^k \mod N\rangle \\
&= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} |a^{k+1} \mod N\rangle \\
&= \frac{1}{\sqrt{p}} \sum_{k=1}^{p} e^{-2\pi i(k-1)s/p} |a^k \mod N\rangle \\
&= e^{2\pi is/p} \frac{1}{\sqrt{p}} \sum_{k=1}^{p} e^{-2\pi iks/p} |a^k \mod N\rangle \\
&= e^{2\pi is/p} \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} |a^k \mod N\rangle, \\
&\qquad\qquad \text{since } a^p \equiv a^0 \ (\bmod N) \text{ and } e^{-2\pi ikp/p} = e^{-2\pi ik0/p} = 1 \\
&= e^{2\pi is/p} |u_s\rangle
\end{aligned}$$

Since $U|u_s\rangle = e^{2\pi is/p}|u_s\rangle$ we have that u_s is an eigenvector or U with eigenvalue $e^{2\pi is/p}$. □

The next object of concern is that preparing the eigenstate

$$|u_s\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} |a^k \mod N\rangle$$

requires that we know the value of p, which defeats the purpose of the algorithm. To circumvent this dilemma, we use the identity

$$\sum_{s=0}^{p-1} e^{2\pi iks/p} = p\delta_{k0} \qquad \text{for } k \in \{0, 1, \ldots, p-1\}, \tag{3.7}$$

which we saw in (3.1) and (3.2), to observe that

$$\frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} e^{2\pi isk/p} |u_s\rangle = |a^k \mod N\rangle \tag{3.8}$$

In particular, for $k = 0$

$$\frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} |u_s\rangle = |1\rangle \tag{3.9}$$

The final problem to deal with is that running the phase estimation procedure with U and $|u_s\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi iks/p} |a^k \bmod N\rangle$ will return an approximation to s/p, where we are only interested in p. The way to overcome this is to use continued fractions.

3.3.2 Continued Fractions Algorithm

The continued fractions algorithm provides us with a means of describing positive real numbers using expressions of the form

$$[a_0, a_1, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_k}}}}$$

where $a_0, a_1, \ldots, a_k$ are positive integers. It allows us to express a real number in terms of integers alone. The continued fractions algorithm determines the continued fraction expansion for a given positive real number. To see how it works, it is best to consider an example:

Example 3.2. To find the expansion for the rational number $41/18$ we break up $41/18$ into integer and fractional parts

$$\frac{41}{18} = 2 + \frac{5}{18}$$

Next we take the fractional part, $5/18$, invert it and break it up

$$\frac{41}{18} = 2 + \frac{5}{18} = 2 + \frac{1}{\frac{18}{5}} = 2 + \frac{1}{3 + \frac{3}{5}}$$

Continuing in this manner, we find that 41/18 has the following continued fraction expansion:

$$\frac{41}{18} = 2 + \frac{1}{3 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}}$$

Thus we can write 41/18 as $[2, 3, 1, 1, 2]$.

It is not hard to verify that the continued fraction algorithm converges after a finite number of steps for any rational number. In fact, it can be shown that the expansion converges fast enough that the algorithm can be performed efficiently on a quantum or classical computer (see [33],[19], [10]).

3.3.3 Algorithm

Before we give the full procedure for the factoring algorithm, we outline the steps of the quantum order–finding algorithm. In the following suppose N is a positive integer that can be represented using m bits. Also suppose $a < N$ is a positive integer coprime to N. Below we outline the steps for the order–finding algorithm which finds the order of a with respect to N.

Algorithm: Quantum Order–Finding

Inputs: $n = 2m + 1 + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$ qubits initialized to 0; m qubits initialized to the state $|1\rangle$; a black box U_a which has the effect $U_a|k\rangle|j\rangle = |k\rangle|a^k j \bmod N\rangle$

Outputs: The least integer $p > 0$ such that $a^p \equiv 1 \pmod N$.

Procedure:

1. Start in the initial state: $|0\rangle|1\rangle$
2. Apply $H^{\otimes n} \otimes I$ to create superposition:

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|1\rangle$$

3. Apply the black box:

$$\begin{aligned}
\rightarrow & \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} U_a|k\rangle|1\rangle \\
= & \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|a^k \mod N\rangle \\
\approx & \frac{1}{\sqrt{p2^n}} \sum_{s=0}^{p-1} \sum_{k=0}^{2^n-1} e^{2\pi iks/p}|k\rangle|u_s\rangle \qquad \text{by (3.8)}
\end{aligned}$$

4. Apply $\mathcal{F}^{-1} \otimes I$:

$$\to \sum_{s=0}^{p-1} |\widetilde{s/p}\rangle |u_s\rangle$$

5. Measure the first register with respect to the basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$:

$$\to |\widetilde{s/p}\rangle$$

6. Apply the continued fractions algorithm:

$$\to p$$

The reason for the approximate equality in step 3, is that 2^n may not be an integer multiple of p. This situation is taken into account by the bounds of the phase estimation algorithm.

However, there are still a couple of ways this algorithm can fail. First, it inherits a possibility of failure from the phase estimation algorithm. However, we saw that this occurs with probability at most ε. The more serious situation occurs when s and p have a factor in common. In this scenario, the number returned by the algorithm is a factor of p and not p itself. To see how this is overcome, suppose the algorithm returns p_1, a factor of p. In the algorithm, we replace a by $a_1 \equiv a^{p_1} \pmod{N}$. Note that the order of a_1 is p/p_1. We then complete the algorithm with a_1 and compute p by multiplying p_1 and p/p_1, the results from each run. Of course, after running the algorithm with a_1 we could also produce a factor p_2 of p/p_1. If this happens, we simply repeat the algorithm with $a_2 \equiv a_1^{p_2} \pmod{N}$. Since each iteration of the algorithm divides p_i by a least 2, after at most $\lceil \log(p) \rceil \leq \lceil \log(N) \rceil$ iterations we will be able to find p.

With the quantum order–finding algorithm in hand, we can now provide the steps necessary for Shor's factoring algorithm

Algorithm: Shor's Factoring Algorithm

Inputs: A composite integer $N > 0$.

Outputs: A non-trivial factor of N.

Procedure:

1. If N is an even integer, return 2.

2. If $N = a^b$ for some integers $a \geq 1$ and $b \geq 2$, return a.

3. Choose a random a where $1 \leq a \leq N-1$. If $\gcd(a, N) > 1$, then return the factor $\gcd(a, N)$.

4. Call the quantum order–finding algorithm to find the order p of a with respect to N.

5. If p is odd, then go to step 1 and start over. If p is even go to step 6.

6. If $a^{p/2} \equiv -1(\bmod N)$, then go to step 1 and start over. Otherwise, compute $\gcd(a^{p/2}-1, N)$ and $\gcd(a^{p/2}+1, N)$, test to see which one of these is a nontrivial factor, and return the factor.

The first step guarantees that N is an odd integer. For the second step, there is an efficient classical algorithm which determines if $N = a^b$ (see page 234 in [24]). At the end of the third step, we either have a factor or we have to use the quantum order–finding algorithm in the fourth step. In the fifth step, the probability that p is odd is only $(\frac{1}{2})^k$ where k is the number of distinct prime factors of N. (see [19] and [33]).

To see why we get a nontrivial factor in step 6 note that since $a^p \equiv 1 \pmod N$, N must divide $a^p - 1 = (a^{p/2} - 1)(a^{p/2} + 1)$, using that p is even from step 5. Therefore N must have a common factor with either $(a^{p/2} - 1)$ or $(a^{p/2} + 1)$. To see that this factor is nontrivial observe that since p is the order of a and p is even, a cannot be 1. Thus either $\gcd(a^{p/2} - 1, N)$ or $\gcd(a^{p/2} + 1, N)$ is not equal to 1. Also, since p is the least integer such that $a^p \equiv 1 \pmod N$, we cannot have $a^{p/2} - 1 \equiv 0 \pmod N$. And step 6 checks to make sure that we do not have $a^{p/2} \equiv -1(\bmod N)$. Thus the $\gcd(a^{p/2} - 1, N)$ and $\gcd(a^{p/2} + 1, N)$ cannot be N.

3.4 Quantum Period Finding Algorithm

Looking back at the quantum order–finding algorithm, we see that what truly takes place is that the algorithm finds the period of the integer function $f(r) = a^r \mod N$. Not surprisingly this algorithm can be generalized to an algorithm that finds the period p of a function $f : \mathbb{N} \to \{0, 1\}$ where $0 < p < 2^m$ for some integer m. All we need for such an algorithm is an oracle U_f that performs the unitary transformation $U|k\rangle|j\rangle = |k\rangle|j \oplus f(k)\rangle$ where $\oplus$ denotes addition modulo 2. Below we outline the steps of the quantum period–finding algorithm:

Algorithm: Quantum Period–Finding

Inputs: $n = O(m+\log(1/\varepsilon))$ qubits initialized to 0; 1 qubit initialized to the state $|0\rangle$ for the function evaluation; a black box U_f which performs the operation $U|k\rangle|j\rangle = |k\rangle|j \oplus f(k)\rangle$

Outputs: The least integer $p > 0$ such that $f(k + p) = f(k)$.

Procedure:

1. Start in the initial state: $|0\rangle|0\rangle$

2. Apply $H^{\otimes n} \otimes I$ to create superposition:

$$\to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$$

3. Apply the black box U_f:

$$\begin{aligned} \to & \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} U_f|k\rangle|0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle \\ &\approx \frac{1}{\sqrt{p2^n}} \sum_{s=0}^{p-1} \sum_{k=0}^{2^n-1} e^{2\pi iks/p}|k\rangle|\tilde{f}(s)\rangle \end{aligned}$$

4. Apply $\mathcal{F}^{-1} \otimes I$:

$$\to \sum_{s=0}^{p-1} |\widetilde{s/p}\rangle|\tilde{f}(s)\rangle$$

5. Measure the first register with respect to the basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$:

$$\to |\widetilde{s/p}\rangle$$

6. Apply the continued fractions algorithm:

$$\to p$$

The only difference between this algorithm and the quantum order–finding algorithm is in step 3 when we introduced the state $|\tilde{f}(s)\rangle$ which we now define as

$$|\tilde{f}(s)\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{2\pi isk/p}|f(k)\rangle$$

This is simply the Fourier transform of $|f(k)\rangle$. The identity in step 3 comes from

$$|f(k)\rangle = \frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} e^{2\pi isk/p}|\tilde{f}(s)\rangle$$

This is easy to verify by observing that $\sum_{s=0}^{p-1} e^{2\pi isk/p} = p$ if k is an integer multiple of p and zero otherwise.

3.5 Continuous Variable Order Finding Algorithm

Up to this point, we have been primarily focused on algorithms involving finite dimensional state spaces. In this section we begin to explore quantum algorithms designed to operate on a state space of infinite dimension. In particular, we will describe a continuous variable version of Shor's order finding algorithm. This algorithm is due to Lomonaco and Kauffman [20]. We will not provide a mathematically rigorous construction and implementation of the algorithm, as this will take us too far off course. However, we do provide an overview of the algorithm at a formal level with some examples and descriptions of how to make it rigorous.

3.5.1 Description

Recall that the original quantum Order Finding algorithm found the period p of an integer function

$$\phi : \mathbb{Z} \to \mathbb{Z} \mod N$$

In particular, for Shor's factoring algorithm, ϕ was taken to be $\phi(r) = a^r \mod N$ for some positive integer a.

With the continuous variable ordering finding algorithm, we would like to develop a quantum algorithm to find the period p of a function $\phi : \mathbb{R} \to \mathbb{C}$.

3.5.2 Rigged Hilbert Spaces

In order to develop such an algorithm, we will have to momentarily abandon the structure of a Hilbert space and work with a *rigged Hilbert Space*, also known as a *Gel'fand triple*. In particular, we will use the rigged Hilbert Space $(\mathcal{S}(\mathbb{R}), L^2(\mathbb{R}), \mathcal{S}'(\mathbb{R}))$, where $\mathcal{S}(\mathbb{R})$ is the space of *test functions* and $\mathcal{S}'(\mathbb{R})$ is the space of *generalized functions* or *distributions*. For a treatment of test functions and distributions see Rudin [31].

The most common generalized function, and the one we will be most concerned with is the Dirac delta function, $\delta(x)$, which has the following effect

$$\int_{\mathbb{R}} \delta(x) f(x)\, dx = f(0)$$

for suitable f (bounded, continuous functions, for instance).

We will use the notation $H_{\mathbb{R}}$ for our rigged Hilbert space. This space has *orthonormal basis*

$$\{|x\rangle; x \in \mathbb{R}\}$$

where by orthonormal we mean that

$$\langle x|y\rangle = \delta(x - y)$$

For a function f in $L^2(\mathbb{R})$ or $\mathcal{S}'(\mathbb{R})$, we have the element in $H_{\mathbb{R}}$ given by the formal integral

$$\int_{\mathbb{R}} dx\, f(x)|x\rangle$$

(In this sense, $|y\rangle$ can be thought of as the delta function at y, $\delta(x-y)$.)

For a particular x_0, we define

$$|x_0\rangle = \int_{\mathbb{R}} dx\, \langle x_0|x\rangle |x\rangle = \int_{\mathbb{R}} dx\, \delta(x-x_0)|x\rangle$$

which gives us the following:

$$\langle x_0|y_0\rangle = \delta(x_0 - y_0)$$

We will also make use of the rigged Hilbert space $H_{\mathbb{C}}$ which is defined in an analogous manner.

3.5.3 Generalized Fourier Transform

In the continuous variable ordering finding algorithm, the periodic function ϕ is taken to be Lebesgue integrable on every closed subinterval of $\mathbb{R}$. We call such a function *admissible*.

Remark 3.3. We have chosen one suitable definition of admissible functions. However, there are many definitions for which the algorithm will still provide a solution. In this sense, admissible can be taken to mean any such function for which the algorithm can provide a solution.

Since ϕ is not assumed to be in $L^2(\mathbb{R})$ or $L^1(\mathbb{R})$, the usual definition of the Fourier transform cannot be applied. We will define the Fourier transform on an periodic admissible function as follows:

Definition 3.4. Let $\phi : \mathbb{R} \to \mathbb{C}$ be a periodic admissible function with minimum period p. The *Fourier transform* of ϕ is given by

$$(\mathcal{F}\phi)(y) = \delta_p(y) \int_0^p dx\, e^{-2\pi i x y} \phi(x)$$

where

$$\delta_p(y) = \frac{1}{|p|} \sum_{n=-\infty}^{\infty} \delta\big(y - \tfrac{n}{p}\big)$$

This definition of the Fourier transform is motivated by the following calculation:

$$\begin{aligned}
\int_{\mathbb{R}} dx\, e^{-2\pi ixy}\phi(x) &= \sum_{n=-\infty}^{\infty} \int_{np}^{(n+1)p} dx\, e^{-2\pi ixy}\phi(x) \\
&= \sum_{n=-\infty}^{\infty} \int_0^p dx\, e^{-2\pi i(x+np)y}\phi(x+np) \qquad \text{by a change of variables} \\
&= \sum_{n=-\infty}^{\infty} e^{-2\pi inpy} \int_0^p dx\, e^{-2\pi ixy}\phi(x) \qquad \text{by the periodicity of } \phi \\
&= \sum_{n=-\infty}^{\infty} \frac{1}{|p|}\delta\big(y - \tfrac{n}{p}\big) \int_0^p dx\, e^{-2\pi ixy}\phi(x) \qquad \text{by Lemma 3.5 below} \\
&= \delta_p(y) \int_0^p dx\, e^{-2\pi ixy}\phi(x)
\end{aligned}$$

The calculation above relies heavily on the distribution equality

$$\sum_{n=-\infty}^{\infty} e^{-2\pi inpy} = \sum_{n=-\infty}^{\infty} \frac{1}{|p|}\delta\big(y - \tfrac{n}{p}\big)$$

Since it is not very intuitive, we provide a rigorous proof.

Lemma 3.5. *As distributions we have the equality*

$$\sum_{n=-\infty}^{\infty} e^{-2\pi inpy} = \sum_{n=-\infty}^{\infty} \frac{1}{|p|}\delta\big(y - \tfrac{n}{p}\big) \tag{3.10}$$

This is a form of the Poisson summation formula.

Proof. Let $f \in C^\infty(\mathbb{R})$ be a rapidly decreasing function. That is,

$$\sup_n \sup_{x\in\mathbb{R}} (1+x^2)^n |f^{(n)}(x)| < \infty$$

We first show:

$$\sum_{m=-\infty}^{\infty} f\big(x + \tfrac{m}{p}\big) = p \sum_{m=-\infty}^{\infty} \hat{f}(mp) e^{-2\pi impx} \tag{3.11}$$

where $\hat{f}$ denotes the usual Fourier transform of the function f and $p > 0$.

Let $F(x) = \sum_{n=-\infty}^{\infty} f(x + \frac{n}{p})$. Observe that the sum is absolutely and uniformly convergent. Also F is periodic with period $\frac{1}{p}$. Thus F has Fourier expansion $F(x) =$

$\sum_{m=-\infty}^{\infty} a_m e^{-2\pi i m p x}$ where

$$\begin{aligned}
a_m &= p \int_0^{1/p} F(x) e^{-2\pi i m p x}\, dx \\
&= p \int_0^{1/p} \sum_{n=-\infty}^{\infty} f\big(x + \tfrac{n}{p}\big) e^{-2\pi i m p x}\, dx \\
&= p \int_{\mathbb{R}} f(x) e^{-2\pi i m p x}\, dx \qquad \text{by the Fubini Theorem} \\
&= p \hat{f}(mp)
\end{aligned}$$

Therefore

$$\sum_{n=-\infty}^{\infty} f(x + \tfrac{n}{p}) = F(x) = \sum_{m=-\infty}^{\infty} a_m e^{-2\pi i m p x} = p \sum_{m=-\infty}^{\infty} \hat{f}(mp) e^{-2\pi i m p x}$$

which establishes (3.11).

Now for any such function f we have

$$\begin{aligned}
\int_{\mathbb{R}} \sum_{n=-\infty}^{\infty} e^{-2\pi i n p y} f(y)\, dy &= \sum_{n=-\infty}^{\infty} \int_{\mathbb{R}} e^{-2\pi i n p y} f(y)\, dy \qquad \text{again by Fubini} \\
&= \sum_{n=-\infty}^{\infty} \hat{f}(np) \\
&= \frac{1}{p} \sum_{n=-\infty}^{\infty} f\big(\tfrac{n}{p}\big) \qquad \text{by (3.11)} \\
&= \int_{\mathbb{R}} \frac{1}{p} \sum_{n=-\infty}^{\infty} \delta\big(y - \tfrac{n}{p}\big) f(y)\, dy \\
&\qquad \text{by the definition of the right side in (3.10).}
\end{aligned}$$

This proves the equality we are after. □

3.5.4 Algorithm

With our Fourier transform in hand we can construct an algorithm for finding the minimum period p of

$$\phi : \mathbb{R} \to \mathbb{C}$$

where ϕ is a periodic admissible function. For clarity, we begin by assuming that p is an integer. This algorithm follows the same general procedure as the quantum order finding algorithm which was discussed in section 3.3.1.

For the algorithm we will work in the state space $H_{\mathbb{R}} \otimes H_{\mathbb{C}}$. We will use an element in $H_{\mathbb{R}}$ to hold arguments of the function ϕ and another element in $H_{\mathbb{C}}$ to hold the values of ϕ. We will also make use of a black box

$$U_\phi : H_{\mathbb{R}} \otimes H_{\mathbb{C}} \to H_{\mathbb{R}} \otimes H_{\mathbb{C}}$$

which performs the operation

$$U_\phi |x\rangle|y\rangle = |x\rangle|y + \phi(x)\rangle$$

We now outline the algorithm:

Algorithm: Continuous Variable Order–Finding

Inputs: an element in $H_{\mathbb{R}}$ initialized to $|0\rangle$; an element in $H_{\mathbb{C}}$ initialized to $|0\rangle$ for function evaluation; a black box U_ϕ which has the effect $U_\phi|x\rangle|y\rangle = |x\rangle|y+\phi(x)\rangle$; a positive integer q such that $q \geq 2p^2$.

Outputs: The least integer $p > 0$ such that $\phi(x + p) = \phi(x)$.

Procedure:

1. Start in the initial state: $|0\rangle|0\rangle$
2. Apply $\mathcal{F}^{-1} \otimes I$ to create superposition:
$$\to \int_{\mathbb{R}} dx\, e^{2\pi i x \cdot 0}|x\rangle|0\rangle = \int_{\mathbb{R}} dx\, |x\rangle|0\rangle$$
3. Apply the black box U_ϕ:
$$\to \int_{\mathbb{R}} dx\, |x\rangle|\phi(x)\rangle$$
4. Apply $\mathcal{F} \otimes I$:
$$\begin{aligned}
\to \int_{\mathbb{R}} dy \int_{\mathbb{R}} dx\, e^{-2\pi i x y}|y\rangle|\phi(x)\rangle &= \int_{\mathbb{R}} dy\, |y\rangle \sum_{n=-\infty}^{\infty} \int_{np}^{(n+1)p} dx\, e^{-2\pi i x y}|\phi(x)\rangle \\
&= \int_{\mathbb{R}} dy\, |y\rangle \sum_{n=-\infty}^{\infty} \int_{0}^{p} dx\, e^{-2\pi i (x+np)y}|\phi(x + np)\rangle \\
&= \int_{\mathbb{R}} dy\, |y\rangle \sum_{n=-\infty}^{\infty} e^{-2\pi i n p y} \int_{0}^{p} dx\, e^{-2\pi i x y}|\phi(x + np)\rangle \\
&= \int_{\mathbb{R}} dy\, |y\rangle \delta_p(y) \int_{0}^{p} dx\, e^{-2\pi i x y}|\phi(x)\rangle \\
&= \sum_{n=-\infty}^{\infty} |n/p\rangle \left(\frac{1}{|p|} \int_{0}^{p} dx\, e^{-2\pi i x \frac{n}{p}}|\phi(x)\rangle \right) \\
&= \sum_{n=-\infty}^{\infty} |n/p\rangle|\Omega(n/p)\rangle
\end{aligned}$$

where

$$|\Omega(n/p)\rangle = \frac{1}{|p|}\int_0^p dx\, e^{-2\pi i x \frac{n}{p}}|\phi(x)\rangle$$

5. Measure the first register with respect to the observable

$$M = \int_{\mathbb{R}} dy\, \frac{\lfloor qy \rfloor}{q}|y\rangle\langle y|$$

where $\lfloor qy \rfloor$ denotes the greatest integer less than qy.
Measuring produces an eigenvalue

$$\frac{m}{q}$$

6. Use continued fraction recursion to find p.

Let us examine the final two steps of the algorithm in greater detail. Note that the spectral decomposition of the observable M is given by

$$M = \int_{\mathbb{R}} dy\, \frac{\lfloor qy \rfloor}{q}|y\rangle\langle y| = \sum_{m=-\infty}^{\infty} P_m$$

where P_m is the project operator given by

$$P_m = \int_{\frac{m}{q}}^{\frac{m+1}{q}} dy\, |y\rangle\langle y|$$

Measuring the state $\sum_{n=-\infty}^{\infty}|n/p\rangle|\Omega(n/p)\rangle$ will produce an eigenvalue $\frac{m}{q}$ where there exist some integer n for which we have

$$\frac{m}{q} \leq \frac{n}{p} \leq \frac{m+1}{q}$$

Using this we must determine the value of p.

It turns out that by selecting $q \geq 2p^2$, the fraction $\frac{n}{p}$ is a convergent of the continued fraction expansion of the eigenvalue $\frac{m}{q}$. Thus, after determining $\frac{n}{p}$, we can use the continued fraction algorithm (see subsection 3.3.2) to find the value of p.

For more on the continuous variable ordering finding algorithm refer to the original paper by Lomonaco and Kauffman [20]. In the paper, they describe how to extend the algorithm to find the period p of ϕ when p is a rational or irrational number.

3.6 Hidden Subspace Algorithm

Let E be a Hilbert space with inner–product $\langle \cdot, \cdot \rangle$. Further suppose we have a functional $\phi : E \to \mathbb{R}^n$ with a hidden subspace $V \subset E$ such that

$$\phi(x+v) = \phi(x) \qquad \text{for all } v \in V$$

The Hidden Subspace Algorithm attempts to find the hidden subspace V. The algorithm we present is based on the work of Lomonaco and Kauffman [21]. We will follow the same general procedure found in the continuous variable order finding algorithm.

Remark 3.6. As the authors admit, the algorithm is "highly speculative". It is based on functional integrals, and uses a Lebesgue type measure, Dx on E, which does not exist. The algorithm calculations are all done at a very formal level.

We will need two rigged Hilbert spaces. The first we denote by H_E. It is the rigged Hilbert space with orthonormal basis

$$\{|x\rangle ; x \in E\}$$

where we have the bracket product defined as

$$\langle x|y\rangle = \delta(x-y)$$

We will also need the rigged Hilbert space $H_{\mathbb{R}^n}$, which can be defined in an analogous manner to the rigged Hilbert space $H_{\mathbb{R}}$ found in section 3.5.2.

For the algorithm we will need an element in H_E to hold arguments of the function ϕ and another element in $H_{\mathbb{R}^n}$ to hold the values of ϕ. We will also make use of a black box

$$U_\phi : H_E \otimes H_{\mathbb{R}^n} \to H_E \otimes H_{\mathbb{R}^n}$$

which performs the operation

$$U_\phi |x\rangle|z\rangle = |x\rangle|z + \phi(x)\rangle$$

Remark 3.7. The algorithm also relies heavily on the following identity:

$$\int_{V^\perp} \delta(y-u)\, Du = \int_V e^{-2\pi i \langle v,y\rangle}\, Dv \tag{3.12}$$

This identity is not obvious and is studied in great detail in chapter 6.

We now outline the algorithm:

Algorithm: Hidden Subspace

Inputs: the elements $|0\rangle \in H_E$ and $|0\rangle \in H_{\mathbb{R}^n}$; a black box U_ϕ which has the effect $U_\phi|x\rangle|z\rangle = |x\rangle|z + \phi(x)\rangle$;

Outputs: a vector $u \in V^{\perp}$

Procedure:

1. Start in the initial state: $|0\rangle|0\rangle \in H_E \otimes H_{\mathbb{R}^n}$
2. Apply $\mathcal{F}^{-1} \otimes I$ to create superposition:

$$\to \int_E Dx\, e^{2\pi i\langle x,0\rangle}|x\rangle|0\rangle = \int_{\mathbb{R}} Dx\,|x\rangle|0\rangle$$

3. Apply the black box U_ϕ:

$$\to \int_E Dx\,|x\rangle|\phi(x)\rangle$$

4. Apply $\mathcal{F} \otimes I$:

$$\begin{aligned}
\to \int_E Dy \int_E Dx\, e^{-2\pi i\langle x,y\rangle}|y\rangle|\phi(x)\rangle &= \int_E Dy\,|y\rangle \int_E Dx\, e^{-2\pi i\langle x,y\rangle}|\phi(x)\rangle \\
&= \int_E Dy\,|y\rangle \int_V Dv \int_{v+V^{\perp}} Dx\, e^{-2\pi i\langle x,y\rangle}|\phi(x)\rangle \qquad \text{using that } E = \bigcup_{v\in V}(v+V^{\perp}) \\
&= \int_E Dy\,|y\rangle \int_V Dv \int_{V^{\perp}} Dx\, e^{-2\pi i\langle x+v,y\rangle}|\phi(x+v)\rangle \qquad \text{by a change of variables} \\
&= \int_E Dy\,|y\rangle \int_V Dv\, e^{-2\pi i\langle v,y\rangle} \int_{V^{\perp}} Dx\, e^{-2\pi i\langle x,y\rangle}|\phi(x)\rangle \qquad \text{since } \phi(x+v)=\phi(x) \\
&= \int_E Dy\,|y\rangle \int_{V^{\perp}} Du\,\delta(y-u) \int_{V^{\perp}} Dx\, e^{-2\pi i\langle x,y\rangle}|\phi(x)\rangle \qquad \text{by equation (3.12)} \\
&= \int_{V^{\perp}} Du\,|u\rangle \int_{V^{\perp}} Dx\, e^{-2\pi i\langle x,u\rangle}|\phi(x)\rangle \\
&= \int_{V^{\perp}} Du\,|u\rangle|\Omega(u)\rangle
\end{aligned}$$

where

$$|\Omega(u)\rangle = \int_{V^{\perp}} Dx\, e^{-2\pi i\langle x,u\rangle}|\phi(x)\rangle$$

5. Measure the first register with respect to the observable

$$M = \int_E Dw\,|w\rangle\langle w|$$

to produce a random vector $u \in V^{\perp}$

Remark 3.8. In the original algorithm by Lomonaco and Kauffman [21], E was taken to be the space *Paths* of all functions (paths) $x : [0,1] \to \mathbb{R}^n$ which are L^2 with respect to the inner–product

$$x \cdot y = \int_0^1 dt\, x(t)y(t)$$

and the measure Dx, was taken in line with Feynman path integrals.

This algorithm provides much of the motivation for the work to follow in chapters 6, 7, and 8. We focus on making the notions introduced by this algorithm mathematically rigorous. To do this we will need the mathematical machinery of *White Noise Analysis* or *Infinite Dimensional Distribution Theory.* The next chapters introduce the concepts necessary for working in this subject.

Chapter 4

Topological Vector Spaces

In this chapter we study the weak, strong, and inductive topologies on the dual of a countably–normed space. We see that under certain conditions the strong and inductive topologies coincide (and are also equivalent with the Mackey topology, which is introduced later). We also examine and compare the σ–fields generated by these topologies to see that under reasonable conditions all the σ–fields are in fact equivalent. This σ–field will serve as the Borel σ–field.

4.1 Basic Notions of Topological Vector Spaces

In this section we review the basic notions of topological vector spaces along and provide proofs a few useful results.

4.1.1 Topological Preliminaries

Let E be a real vector space.

A *vector topology* τ on E is a topology such that addition $E \times E \to E : (x, y) \mapsto x + y$ and scalar multiplication $\mathbb{R} \times E \to E : (t, x) \mapsto tx$ are continuous. If E is a complex vector space we require that $\mathbb{C} \times E \to E : (\alpha, x) \mapsto \alpha x$ be continuous.

It is useful to observe that when E is equipped with a vector topology, the translation maps

$$t_x : E \to E : y \mapsto y + x$$

are continuous, for every $x \in E$, and are hence also homeomorphisms since $t_x^{-1} = t_{-x}$.

A *topological vector space* is a vector space equipped with a vector topology.

Recall that a *local base* of a vector topology τ is a family of open sets $\{U_\alpha\}_{\alpha \in I}$ containing 0 such that if W is any open set containing 0 then W contains some U_α. A set W that contains an open set containing x is called a *neighborhood* of x. If U is any open set and x any point in U then $U - x$ is an open neighborhood of 0 and hence contains some U_α, and so U itself contains a neighborhood $x + U_\alpha$ of x:

$$\text{(4.1)} \qquad \textit{If } U \textit{ is open and } x \in U \textit{ then } x + U_\alpha \subset U, \textit{ for some } \alpha \in I$$

Doing this for each point x of U, we see that each open set is the union of translates of the local base sets U_α.

If $\mathcal{U}_x$ denotes the set of all neighborhoods of a point x in a topological space X, then $\mathcal{U}_x$ has the following properties:

(1) $x \in U$ for all $U \in \mathcal{U}_x$
(2) if $U \in \mathcal{U}_x$ and $V \in \mathcal{U}_x$, then $U \cap V \in \mathcal{U}_x$
(3) if $U \in \mathcal{U}_x$ and $U \subset V$, then $V \in \mathcal{U}_x$.
(4) if $U \in \mathcal{U}_x$, then there is some $V \in \mathcal{U}_x$ with $U \in \mathcal{U}_y$ for all $y \in V$. (taking V to be the interior of U is sufficient).

Conversely if X is any set and a non-empty collection of subsets $\mathcal{U}_x$ is given for each $x \in X$, then when the conditions above are satisfied by the $\mathcal{U}_x$, exactly one topology can be defined on X in such a way to make $\mathcal{U}_x$ the set of neighborhoods of x for each $x \in X$. A set $V \subset X$ is called open if for each $x \in V$, there is a $U \in \mathcal{U}_x$ with $U \subset V$. [29]

In most cases of interest a topological vector space has a local base consisting of convex sets. We call such spaces *locally convex topological vector spaces*.

In a topological vector space there is the notion of bounded sets. A set D in a topological vector space is said to be *bounded*, if for every neighborhood U of 0 there is some $\lambda > 0$ such that $D \subset \lambda U$. If $\{U_\alpha\}_{\alpha \in I}$ is a local base, then it is easily seen that D is bounded if and only if to each U_α there corresponds $\lambda_\alpha > 0$ with $D \subset \lambda_\alpha U_\alpha$. [29]

A set A in a vector space E is said to be *absorbing* if given any $x \in E$ there is an η such that $x \in \lambda A$ for all $|\lambda| \geq \eta$. The set A is called *balanced* if, for all $x \in A$, $\lambda x \in A$ whenever $|\lambda| \leq 1$. Also, a set A in a vector space E is call *symmetric* if $-A = A$. Finally, although the next concept is very common, the term we use for it is not, so we make a formal definition:

Definition 4.1. A subset A of a topological space X is *limit point compact* if every infinite subset of A has a limit point.

Remark 4.2. The term *limit point compact* is not the standard term for spaces with the above property. In fact, I do not believe there is a standard term. I have seen it called "Fréchet compactness", "relative sequential compactness", and the "Bolzano-Weierstrass property". The term *limit point compact* was taken directly from Munkres [23]. It is my personal favorite term; at the very least it is descriptive.

4.1.2 Bases in Topological Vector Spaces

Here we take the time to prove some general, but very useful, results about local bases for topological vector spaces. Most of the results in this subsection are taken from Robertson [29].

Lemma 4.3. *Every topological vector space E has a base of balanced neighborhoods.*

Proof. Let U be a neighborhood of 0 in E. Consider the function $h : \mathbb{C} \times E \to E$ given by $h(\lambda, x) = \lambda x$. Since E is a topological vector space, h is continuous at $\lambda = 0, x = 0$. So there is a neighborhood V and $\varepsilon > 0$ with $\lambda x \in U$ for $|\lambda| \leq \varepsilon$ and $x \in V$. Hence $\lambda V \subset U$ for $|\lambda| \leq \varepsilon$. Therefore $\frac{\varepsilon}{\alpha} V \subset U$ for all α with $|\alpha| \geq 1$. Thus $\varepsilon V \subset U' = \bigcap_{|\alpha| \geq 1} \alpha U \subset U$. Now since V is a neighborhood of 0 so is εV. Hence U' is a neighborhood of 0. If $x \in U'$ and $0 \leq |\lambda| \leq 1$, then for $|\alpha| \geq 1$, we have $x \in \frac{\alpha}{\lambda} U$ (since $\left|\frac{\alpha}{\lambda}\right| \geq 1$). So $\lambda x \in \alpha U$ for $|\lambda| \leq 1$. Hence $\lambda x \in U'$. Therefore U' is balanced. $\square$

Lemma 4.4. *Let E be a vector space. Let $\mathcal{B}$ be a collection of subsets of E satisfying:*

(i) *if $U, V \in \mathcal{B}$, then there exist $W \in \mathcal{B}$ with $W \subset U \cap V$.*

(ii) *if $U \in \mathcal{B}$ and $\lambda \neq 0$, then $\lambda U \in \mathcal{B}$.*

(iii) *if $U \in \mathcal{B}$, then U is balanced, convex, and absorbing.*

Then there is a topology making E a locally convex topological vector space with $\mathcal{B}$ the base of neighborhoods of 0.

Proof. Let $\mathcal{A}$ be the set of all subsets of E that contain a set of $\mathcal{B}$. For each x take $x + \mathcal{A}$ to be the set of neighborhoods of x. We need to see that (1)-(4) are satisfied from subsection 4.1.1.

For (1), we have to show $x \in A$ for all $A \in x + \mathcal{A}$. Note that since each $U \in \mathcal{B}$ is absorbent, there exists a non-zero λ such that $0 \in \lambda U$. But then $0 \in \lambda^{-1}\lambda U = U$. So each $U \in \mathcal{B}$ contains 0. So $x \in A$ for all $A \in x + \mathcal{A}$.

For (2), we have to show that if $A, B \in \mathcal{A}$, then $(x + A) \cap (x + B) \in x + \mathcal{A}$ for each $x \in E$. Recall $U \subset A$ and $V \subset B$ for some $U, V \in \mathcal{B}$. So $U \cap V \subset A \cap B$. By the first hypothesis, there is a $W \in \mathcal{B}$ with $W \subset U \cap V \subset A \cap B$. Thus $A \cap B \in \mathcal{A}$ and hence $(x + A) \cap (x + B) \in x + \mathcal{A}$ for each $x \in E$.

Next (3) is clear from the definition of $\mathcal{A}$, since if $A \in \mathcal{A}$ and $A \subset B$ then $B \in \mathcal{A}$.

Finally for (4), we must show that if $x + A \in x + \mathcal{A}$, then there is an $V \in x + \mathcal{A}$ with $x + A \in y + \mathcal{A}$ for all $y \in V$. If $A \in \mathcal{A}$ take a $U \in \mathcal{B}$ with $U \subset A$. Now we see that $x + A$ is a neighborhood of each point $y \in x + \frac{1}{2}U$. Since $y \in x + \frac{1}{2}U$ we have $y - x \in \frac{1}{2}U$. Thus $y - x + \frac{1}{2}U \subset \frac{1}{2}U + \frac{1}{2}U \subset A$. Hence $y + \frac{1}{2}U \subset x + A$. Thus $x - y + A \supset \frac{1}{2}U$. So $x - y + A \in \mathcal{A}$. Therefore $y + x - y + A = x + A \in y + \mathcal{A}$.

To prove continuity of addition, let $U \in \mathcal{B}$. Then if $x \in a + \frac{1}{2}U$ and $y \in b + \frac{1}{2}U$, we have $x + y \in a + b + U$.

Finally, to see that scalar multiplication, λx, is continuous at $x = a, \lambda = \alpha$, we should find δ_1 and δ_2 such that $\lambda x - \alpha a \in U$ whenever $|\lambda - \alpha| < \delta_1$ and $x \in a + \delta_2 U$. Since U is absorbing, there is a η with $a \in \eta U$. Take δ_1 so that $0 < \delta_1 < \frac{1}{2\eta}$ and take

δ_2 so that $0 < \delta_2 < \frac{1}{2(|\alpha|+\delta_1)}$. Now observe

$$\begin{aligned}\lambda x - \alpha a &= \lambda(x-a) + (\lambda - \alpha)a \\ &\in (|\alpha| + \delta_1)\delta_2 U + \delta_1 \eta U \\ &\subset \frac{1}{2}U + \frac{1}{2}U \subset U\end{aligned}$$

Thus we are done. $\square$

4.1.3 Topologies Generated by Families of Topologies

Let $\{\tau_\alpha\}_{\alpha\in I}$ be a collection of topologies on a space. It is natural and useful to consider the the least upper bound topology τ, i.e. the coarsest topology containing all sets of $\cup_{\alpha\in I}\tau_\alpha$. In our setting, we work with each τ_α a vector topology on a vector space E.

Theorem 4.5. *The least upper bound topology τ of a collection $\{\tau_\alpha\}_{\alpha\in I}$ of vector topologies is again a vector topology. If $\{W_{\alpha,i}\}_{i\in I_\alpha}$ is a local base for τ_α then a local base for τ is obtained by taking all finite intersections of the form $W_{\alpha_1,i_1} \cap \cdots \cap W_{\alpha_n,i_n}$.*

Proof. Let $\mathcal{B}$ be the collection of all sets which are of the form $W_{\alpha_1,i_1} \cap \cdots \cap W_{\alpha_n,i_n}$.

Let τ' be the collection of all sets which are unions of translates of sets in $\mathcal{B}$ (including the empty union). Our first objective is to show that τ' is a topology on E. It is clear that τ' is closed under unions and contains the empty set. We have to show that the intersection of two sets in τ' is in τ'. To this end, it will suffice to prove the following:

$$\begin{gathered}\text{If } C_1 \text{ and } C_2 \text{ are sets in } \mathcal{B}, \text{ and } x \text{ is a point in} \\ \text{the intersection of the translates } a + C_1 \text{ and } b + C_2, \\ \text{then } x + C \subset (a + C_1) \cap (b + C_2) \text{ for some } C \text{ in } \mathcal{B}.\end{gathered} \tag{4.2}$$

Clearly, it suffices to consider finitely many topologies τ_α. Thus, consider vector topologies $\tau_1, ..., \tau_n$ on E.

Let $\mathcal{B}_n$ be the collection of all sets of the form $B_1 \cap \cdots \cap B_n$ with B_i in a local base for τ_i, for each $i \in \{1, ..., n\}$. We can check that if $D, D' \in \mathcal{B}_n$ then there is an $G \in \mathcal{B}_n$ with $G \subset D \cap D'$.

Working with B_i drawn from a given local base for τ_i, let z be a point in the intersection $B_1 \cap \cdots \cap B_n$. Then there exist sets B_i', with each B_i' being in the local base for τ_i, such that $z + B_i' \subset B_i$ (this follows from our earlier observation (4.1)). Consequently,

$$z + \cap_{i=1}^n B_i' \subset \cap_{i=1}^n B_i$$

Now consider sets C_1 an C_2, both in $\mathcal{B}_n$. Consider $a, b \in E$ and suppose $x \in (a+C_1)\cap(b+C_2)$. Then since $x - a \in C_1$ there is a set $C_1' \in \mathcal{B}_n$ with $x - a + C_1' \subset C_1$; similarly, there is a $C_2' \in \mathcal{B}_n$ with $x - b + C_2' \subset C_2$. So $x + C_1' \subset a + C_1$ and $x + C_2' \subset b + C_2$. So

$$x + C \subset (a + C_1) \cap (b + C_2),$$

where $C \in \mathcal{B}_n$ satisfies $C \subset C_1 \cap C_2$.

This establishes (4.2), and shows that the intersection of two sets in τ' is in τ'.

Thus τ' is a topology. The definition of τ' makes it clear that τ' contains each τ_α. Furthermore, if any topology σ contains each τ_α then all the sets of τ' are also open relative to σ. Thus

$$\tau' = \tau,$$

the topology generated by the topologies τ_α.

Observe that we have shown that if $W \in \tau$ contains 0 then $W \supset B$ for some $B \in \mathcal{B}$.

Next we have to show that τ is a vector topology. The definition of τ shows that τ is translation invariant, i.e. translations are homeomorphisms. So, for addition, it will suffice to show that addition $E \times E \to E : (x, y) \mapsto x + y$ is continuous at $(0, 0)$. Let $W \in \tau$ contain 0. Then there is a $B \in \mathcal{B}$ with $0 \in B \subset W$. Suppose $B = B_1 \cap \cdots \cap B_n$, where each B_i is in the given local base for τ_i. Since τ_i is a vector topology, there are open sets $D_i, D_i' \in \tau_i$, both containing 0, with

$$D_i + D_i' \subset B_i$$

Then choose C_i, C_i' in the local base for τ_i with $C_i \subset D_i$ and $C_i' \subset D_i'$. Then

$$C_i + C_i' \subset B_i$$

Now let $C = C_1 \cap \cdots \cap C_n$, and $C' = C_1' \cap \cdots \cap C_n'$. Then $C, C' \in \mathcal{B}$ and $C + C' \subset B$. Thus, addition is continuous at $(0, 0)$.

Now consider the multiplication map $\mathbb{R} \times E \to E : (t, x) \mapsto tx$. Let $(s, y), (t, x) \in \mathbb{R} \times E$. Then

$$sy - tx = (s - t)x + t(y - x) + (s - t)(y - x)$$

Suppose $F \in \tau$ contains tx. Then

$$F \supset tx + W',$$

for some $W' \in \mathcal{B}$. Using continuity of the addition map

$$E \times E \times E \to E : (a, b, c) \mapsto a + b + c$$

at $(0, 0, 0)$, we can choose $W_1, W_2, W_3 \in \mathcal{B}$ with $W_1 + W_2 + W_3 \subset W'$. Then we can choose $W \in \mathcal{B}$, such that

$$W \subset W_1 \cap W_2 \cap W_3$$

Then $W \in \mathcal{B}$ and

$$W + W + W \subset W'$$

Suppose $W = B_1 \cap \cdots \cap B_n$, where each B_i is in the given local base for the vector topology τ_i. Then for s close enough to t, we have $(s-t)x \in B_i$ for each i, and hence $(s-t)x \in W$. Similarly, if y is τ–close enough to x then $t(y-x) \in W$. Lastly, if $s-t$ is close enough to 0 and y is close enough to x then $(s-t)(y-x) \in W$. So $sy - tx \in W'$, and so $sy \in F$, when s is close enough to t and y is τ–close enough to x. $\square$

The above result makes it clear that if each τ_α has a convex local base then so does τ. Note also that if at least one τ_α is Hausdorff then so is τ.

A family of topologies $\{\tau_\alpha\}_{\alpha \in I}$ is *directed* if for any $\alpha, \beta \in I$ there is a $\gamma \in I$ such that

$$\tau_\alpha \cup \tau_\beta \subset \tau_\gamma$$

In this case every open neighborhood of 0 in the generated topology contains an open neighborhood in one of the topologies τ_γ.

4.2 Countably–Normed Spaces

We begin with the basic definition of a *countably–normed space* and a *countably–Hilbert space.*

Definition 4.6. Let V be a topological vector space over $\mathbb{C}$ with topology given by a family of norms $\{|\cdot|_n; n = 1, 2, \ldots\}$. Then V is a *countably–normed space.* The space V is called a *countably–Hilbert space* if each $|\cdot|_n$ is an inner product norm and V is complete with respect to its topology.

Remark 4.7. By considering the new norms $\|v\|_n = (\sum_{k=1}^n |v|_k{}^2)^{\frac{1}{2}}$ we may assume that the family of norms $\{|\cdot|_n; n = 1, 2, \ldots\}$ is increasing, i.e.

$$|v|_1 \le |v|_2 \le \cdots \le |v|_n \le \cdots, \forall v \in V$$

If V is a countably–normed space, we denote the completion of V in the norm $|\cdot|_n$ by V_n. Then V_n is by definition a Banach space. Also in light of Remark 4.7 we can assume that

$$V \subset \cdots \subset V_{n+1} \subset V_n \subset \cdots \subset V_1$$

Lemma 4.8. *The inclusion map from V_{n+1} into V_n is continuous.*

Proof. Consider an open neighborhood of 0 in V_n given by

$$B_n(0, \epsilon) = \{v \in V_n; |v|_n < \epsilon\}$$

Let $i_{n+1,n} : V_{n+1} \to V_n$ be the inclusion map. Now

$$i_{n+1,n}^{-1}(B_n(0,\epsilon)) = \{v \in V_{n+1}; |v|_n < \epsilon\} \supset B_{n+1}(0,\epsilon) \text{ since } |v|_n \le |v|_{n+1}$$

Therefore $i_{n+1,n}$ is continuous. $\square$

Proposition 4.9. *Let V be a countably–normed space. Then V is complete if and only if $V = \bigcap_{n=1}^{\infty} V_n$.*

Proof. Suppose $V = \bigcap_{n=1}^{\infty} V_n$ and $\{v_k\}_{k=1}^{\infty}$ is Cauchy in V. By definition $\{v_k\}_{k=1}^{\infty}$ is Cauchy in V_n for all n. Since V_n is complete, a limit $v^{(n)}$ exist in V_n. Using that the inclusion map $i_{n+1,n} : V_{n+1} \to V_n$ is continuous (by Lemma 4.8) and that

$$V \subset \cdots \subset V_{n+1} \subset V_n \subset \cdots \subset V_1$$

we have that all the $v^{(n)}$ are the same and belong to each V_n. Thus they are in $V = \bigcap_{n=1}^{\infty} V_n$. Let us call this element $v \in V$.

Since $|v_k - v^{(n)}|_m \to 0$ for all m we have that $|v_k - v|_m \to 0$ for all m. Hence $v = \lim_{k\to\infty} v_k$ in V. Thus V is complete.

Conversely, let V be complete and take $v \in \bigcap_{n=1}^{\infty} V_n$. We need to show v is in V. For each n we can find $v_n \in V$ such that $|v - v_n|_n < \frac{1}{n}$ (using that V is dense in V_n). Now for any $k < n$ we have $|v - v_n|_k \leq |v - v_n|_n < \frac{1}{n}$. Thus $\lim_{n\to\infty} |v - v_n|_k = 0$. This gives us that $\{v_n\}$ is Cauchy with respect to all norms $|\cdot|_k$ where $k = 1, 2, \ldots$

Let $\overline{v} = \lim_{n\to\infty} v_n$ in V. Since for all k we have $\overline{v}, v \in V_k$ and $\lim_{n\to\infty} |\overline{v} - v_n|_k = 0$, we see that $v = \overline{v}$. Thus $v \in V$ and we have $V \supset \bigcap_{n=1}^{\infty} V_n$. That $V \subset \bigcap_{n=1}^{\infty} V_n$ is obvious, since $V \subset V_n$ for all n. □

4.2.1 Open Sets in V

In light of Theorem 4.5, we see that a local base for V is given by sets of the form:

$$B = B_{n_1}(\varepsilon_1) \cap B_{n_2}(\varepsilon_2) \cap \cdots \cap B_{n_k}(\varepsilon_k)$$

where $B_{n_i}(\varepsilon_i) = \{v \in V; |v|_{n_i} < \varepsilon_i\}$ is the $|\cdot|_{n_i}$ unit ball of radius ε_i in V.

Proposition 4.10. *Let V be a countably–normed space. For every element B of the local base for V there exist n and $\varepsilon > 0$ such that $B_n(\varepsilon) \subset B$.*

Proof. Let $B = B_{n_1}(\varepsilon_1) \cap B_{n_2}(\varepsilon_2) \cap \cdots \cap B_{n_k}(\varepsilon_k)$ be an element of the local base for V. Then take $n = \max_{1\leq j\leq k} n_j$ and $\varepsilon = \min_{1\leq j\leq k} \varepsilon_j$. Observe $B_n(\varepsilon) \subset B$ since for $v \in B_n(\varepsilon)$ we have $|v|_{n_j} \leq |v|_n < \varepsilon \leq \varepsilon_j$ for any $j \in \{1, 2, \ldots, k\}$. Thus $v \in B$. □

Corollary 4.11. *Let V be a countably–normed space. Then a local base for V is given by the collection $\{B_n(\frac{1}{k})\}_{n,k=1}^{\infty}$.*

Corollary 4.12. *Let V be a countably–normed space. Then a local base for V is given by the collection $\{B_k(\frac{1}{k})\}_{k=1}^{\infty}$. Moreover we have that $B_1(1) \supset B_2(\frac{1}{2}) \supset \cdots$*

Proof. Let U be a neighborhood of 0. By Corollary 4.11 there are positive integers n and k such that $B_n(\frac{1}{k}) \subset U$. If $n \geq k$, we have that $B_n(\frac{1}{n}) \subset B_n(\frac{1}{k})$ since $\frac{1}{n} \leq \frac{1}{k}$. If $n \leq k$, then $B_k(\frac{1}{k}) \subset B_n(\frac{1}{k})$ since $|v|_k < \frac{1}{k}$ gives us that $|v|_n \leq |v|_k < \frac{1}{k}$.

For $m \geq k$ we have that $B_m(\frac{1}{m}) \subset B_k(\frac{1}{k})$ since $|v|_k \leq |v|_m$ and $\frac{1}{m} < \frac{1}{k}$. □

4.2.2 Bounded Sets in V

Recall that a subset D of a countably–normed space V is said to be *bounded* if for any neighborhood U of zero in V there is a positive number λ such that $D \subset \lambda U$ (see subsection 4.1.1). This leads us to the following useful proposition:

Proposition 4.13. *A set D in a countably–normed space V is bounded if and only if $\sup_{v \in D} |v|_n < \infty$ for all $n \in \{1, 2, \ldots\}$.*

Proof. ($\Rightarrow$) Suppose D is a bounded set in V. Take the open neighborhood $B_n(1) = \{v \in V; |v|_n < 1\}$ in V. Since D is bounded in V there is an $\lambda > 0$ such that $D \subset \lambda B_n(1)$. Thus $\sup_{v \in D} |v|_n \leq \lambda$.

($\Leftarrow$) Suppose U is a neighborhood of 0 in V. Then by Proposition 4.10 there is an $B_n(\varepsilon) \subset U$. Let $\sup_{v \in D} |v|_n = M < \infty$. Then $D \subset \frac{M+1}{\varepsilon} B_n(\varepsilon) \subset \frac{M+1}{\varepsilon} U$. So D is bounded. □

4.2.3 The Dual

Again take V to be a countably–normed space associated with an increasing sequence of norms $\{|\cdot|_n\}_{n=1}^{\infty}$ and let V_n be the completion of V with respect to the norm $|\cdot|_n$. We denote the dual space of V by V'. Let $\langle \cdot, \cdot \rangle$ denote the bilinear pairing of V' and V.

Of course, each Banach space V_n also has a dual, which we denote by V'_n. We use the notation to $|\cdot|_{-n}$ to denote the operator norm on the Banach space V'_n. The relationship between V' and each V'_n is discussed in the next proposition.

Proposition 4.14. *The dual of a countably–normed space V is given by $V' = \bigcup_{n=1}^{\infty} V'_n$ and we have the inclusions*

$$V'_1 \subset \cdots \subset V'_n \subset V'_{n+1} \subset \cdots V'$$

Moreover, for $f \in V'_n$ we have $|f|_{-n} \geq |f|_{-n-1}$.

Proof. ($\supset$) Take $v' \in V'_n$. Then v' is continuous on V_n with topology coming from the norm $|\cdot|_n$. Thus v' is continuous on V, since $V \subset V_n$ and the norm $|\cdot|_n$ is one of the norms generating the topology on V.

($\subset$) Take $v' \in V'$. Since v' is continuous on V the set

$$v'^{-1}(-1, 1) = \{v \in V \; ; \; |\langle v', v \rangle| < 1\}$$

is open in V. So we can find a member B of the local base for V such that $B \subset v'^{-1}(-1, 1)$. By the corollary to Proposition 4.10 we have that $B_n(\varepsilon) \subset v'^{-1}(-1, 1)$ for some positive integer n and some $\varepsilon > 0$.

Thus for all $v \in V$ with $|v|_n < \varepsilon$ we have that $|\langle v', v \rangle| < 1$. Since V is dense in V_n, if $v \in V_n$ and $|v|_n \leq \varepsilon$ then $|\langle v', v \rangle| \leq 1$. Thus $v' \in V'_n$.

To see that $V'_n \subset V'_{n+1}$ take $f \in V'_n$. Then for all $v \in V_n$ we have that

$$|f(v)| \leq |f|_{-n}|v|_n \leq |f|_{-n}|v|_{n+1}$$

Since $V_{n+1} \subset V_n$, the above holds for all $v \in V_{n+1}$. Thus $f \in V'_{n+1}$ and $|f|_{-n-1} \leq |f|_{-n}$. □

Proposition 4.15. *A linear functional f on V is continuous if and only if f is bounded on bounded sets of V.*

Proof. ($\Rightarrow$) Let f be a continuous linear functional on V. Then f is in V'. So $f = \langle v', \cdot \rangle$ for some $v' \in V'$. Now by Proposition 4.14, $v' \in V'_n$ for some n. Let $D \subset V$ be bounded. By Proposition 4.13 we have that $\sup_{v \in D} |v|_n = M < \infty$. Using this we see that $\sup_{v \in D} |\langle v', v \rangle| \leq M|v'|_{-n} < \infty$. Thus $f = \langle v', \cdot \rangle$ is bounded on bounded sets.

($\Leftarrow$) Suppose f is bounded on bounded sets. Consider the local base sets $B_1(1) \supset B_2\left(\frac{1}{2}\right) \supset \cdots$ in V as in Corollary 4.12. By contradiction we assume that f is not in V'. Then f is not in V'_k for any k. So f is not continuous on V_k and hence not bounded on $B_k\left(\frac{1}{k}\right)$. Hence we can find a v_k in $B_k\left(\frac{1}{k}\right)$ such that $|f(v_k)| > k$. The sequence $\{v_k\}_{k=1}^{\infty}$ goes to 0 in V. Thus $\{v_k\}_{k=1}^{\infty}$ must be bounded. But then by hypothesis, $\{f(v_k)\}_{k=1}^{\infty}$ should be bounded. But by construction it is not, a contradiction. □

Corollary 4.16. *A linear functional f on V is continuous if and only if f is bounded on some neighborhood of* 0 *in V.*

Proof. Suppose f is bounded on some neighborhood U of 0 in V. Then for any $\alpha > 0$, f is bounded on αU. Let D be a bounded set in V. Then $D \subset \lambda U$ for some $\lambda > 0$. So f is bounded on D and hence continuous by Proposition 4.15 □

There are several topologies one can put on the dual space V'. The three most common are the weak, strong, and inductive topologies. In the following sections we discuss the properties of these three topologies and compare them against one another. Throughout this discussion, the topology on V'_n is taken to be the usual strong topology (i.e. the topology induced by the operator norm on V'_n as the dual of the Banach space V_n).

4.2.4 Bounded Sets of V Revisited

Let V be a countably–normed space. With the notion of the dual V' of V behind us (see subsection 4.2.3), we can formulate a better understanding of bounded sets in V. We begin with the following simple definition:

Definition 4.17. A set $D \subset V$ is said to be weakly bounded if given a set $N(v'; \varepsilon) = \{v \in V; |\langle v', v \rangle| < \varepsilon\}$ there is a $\lambda > 0$ such that $D \subset \lambda N(v'; \varepsilon)$.

Theorem 4.18. *Suppose V is a countably–normed space with dual V'. Let $D \subset V$. Then the following are equivalent*

(1) *D is bounded.*

(2) *D is weakly bounded.*

(3) *The values of each $v' \in V'$ are bounded on D.*

(4) *For all n, we have $\sup_{v \in D} |v|_n < \infty$.*

Proof. We have already shown that (1) and (4) are equivalent in Proposition 4.13.

((1) $\Rightarrow$ (2)) Suppose D is bounded in V. Take a $v' \in V'$. Then $v' \in V_n'$ for some n. For $v \in D$ we have $|\langle v', v\rangle| \le |v'|_{-n}|v|_n \le |v'|_{-n}M_n$ where $M_n = \sup_{v \in D} |v|_n$. Thus we have $D \subset \frac{2|v'|_{-n}M_n}{\varepsilon}N(v';\varepsilon)$. So D is weakly bounded.

((2) $\Rightarrow$ (3)) Suppose D is weakly bounded in V. Take $v' \in V'$. By assumption $D \subset \lambda N(v';\varepsilon)$ for some $\lambda > 0$. So for $v \in D$ we have $|\langle v', v\rangle| \le \lambda\varepsilon$.

((3) $\Rightarrow$ (4)) Consider $D \subset V \subset V_n$. By hypothesis all $v' \in V'$ are bounded on D. In particular all $v' \in V_n' \subset V'$ are bounded on D. This means the linear functionals $\{\langle \cdot, v\rangle; v \in D\}$ are pointwise bounded on V_n'. Thus we can apply the uniform boundedness principle to see that $\sup_{v \in D} |v|_n < \infty$. □

4.2.5 The Metric on V

Let V be a countably–normed space. Define the function $\rho : V \times V \to [0, \infty)$ by

$$\rho(v, u) = \sum_{n=1}^{\infty} \frac{1}{2^n} \frac{|v-u|_n}{1+|v-u|_n} \tag{4.3}$$

First observe that ρ is a metric on V. From the above definition it is obvious that $\rho(v, v) = 0$ and $\rho(v, u) > 0$ for all $u \ne v$. It is also clear that $\rho(v, u) = \rho(u, v)$. We have left to check the triangle inequality. To verify the triangle inequality it is sufficient to show that

$$\frac{|v+u|_n}{1+|v+u|_n} \le \frac{|v|_n}{1+|v|_n} + \frac{|u|_n}{1+|u|_n}$$

To show this, we first note that the function $f : [0, \infty) \to [0, 1)$ given by $f(t) = \frac{t}{1+t}$ is increasing. Thus

$$\begin{aligned} \frac{|v+u|_n}{1+|v+u|_n} &\le \frac{|v|_n + |u|_n}{1+|v|_n+|u|_n} \\ &= \frac{|v|_n}{1+|v|_n+|u|_n} + \frac{|u|_n}{1+|v|_n+|u|_n} \\ &\le \frac{|v|_n}{1+|v|_n} + \frac{|u|_n}{1+|u|_n} \end{aligned}$$

Proposition 4.19. *The metric ρ on V has the following properties:*

(1) $\rho(v,u) = \rho(v-u,0)$

(2) *If $v_k \to 0$ in V, then $\rho(v_k,0) \to 0$.*

Proof. That $\rho(v,u) = \rho(v-u,0)$ for all $u,v \in V$ is obvious from the definition.

For (2), let $v_k \to 0$ in V. Then $\lim_{k\to\infty} |v_k|_n \to 0$ for each n. So, for a given $\varepsilon > 0$, take N so that $\frac{1}{2^N} < \frac{\varepsilon}{2}$. Take K such that for any $k > K$ we have $|v_k|_n < \frac{\varepsilon}{2}$ for all $1 \leq n \leq N$. Then for $k > K$ we have

$$\sum_{n=1}^{\infty} \frac{1}{2^n} \frac{|v_k|_n}{1+|v_k|_n} = \sum_{n=1}^{N} \frac{1}{2^n} \frac{|v_k|_n}{1+|v_k|_n} + \sum_{n=N+1}^{\infty} \frac{1}{2^n} \frac{|v_k|_n}{1+|v_k|_n} < \frac{\varepsilon}{2} + \frac{1}{2^N} < \varepsilon$$

Therefore $\rho(v_k,0) \to 0$ as $k \to \infty$. □

As you may have guessed, we would not take the time to talk about this metric unless it proved useful in some way. Well, it turns out that the topology induced by this metric is identical to the original topology on V.

Theorem 4.20. *The topology on the countably–normed space V induced by the metric ρ is equivalent to the original topology on V (i.e. the topology induced by the family of norms $\{|\cdot|_n\}_{n=1}^{\infty}$).*

Proof. By Proposition 4.19, it is sufficient to consider the sets $\{v \in V \,;\, \rho(v,0) < \varepsilon\}$ and the neighborhoods $\{v \in V \,;\, |v|_n < \delta\}$ of 0 in V for $\varepsilon, \delta > 0$ and $n \in \{1,2,\ldots\}$. We have to show that every $\{v \in V \,;\, |v|_n < \delta\}$ contains some $\{v \in V \,;\, \rho(v,0) < \varepsilon\}$ and conversely.

Consider a neighborhood $\{v \in V \,;\, |v|_n < \delta\}$ in V. If $v \in V$ satisfies $\rho(v,0) < \varepsilon$, then $\frac{1}{2^n}\frac{|v|_n}{1+|v|_n} < \varepsilon$ and thus

$$|v|_n < \frac{2^n \varepsilon}{1-2^n\varepsilon} = \frac{2^n}{\frac{1}{\varepsilon} - 2^n}$$

So, take $\varepsilon > 0$ such that

$$0 < \frac{2^n}{\frac{1}{\varepsilon} - 2^n} < \delta$$

and we have $\{v \in V \,;\, \rho(v,0) < \varepsilon\} \subset \{v \in V \,;\, |v|_n < \delta\}$.

Now consider a set $\{v \in V \,;\, \rho(v,0) < \varepsilon\}$. Assume, by contradiction, there is no n and $\delta > 0$ such that $\{v \in V \,;\, |v|_n < \delta\} \subset \{v \in V \,;\, \rho(v,0) < \varepsilon\}$. Then for each k we can find $v_k \in \left\{v \in V \,;\, |v|_k < \frac{1}{k}\right\}$ such that v_k is not in $\{v \in V \,;\, \rho(v,0) < \varepsilon\}$. This gives us a sequence $\{v_k\}_{k=1}^{\infty}$ that tends to 0 in V but not with respect to the metric ρ. This contradicts Proposition 4.19. □

From this it follows that V is a complete countably–normed space if and only (V,ρ) is a complete metric space. The following is a result which proves useful in a few theorems to come:

Lemma 4.21. *Given a closed convex symmetric absorbing set C in a complete countably–normed space V we can find a neighborhood U of 0 contained in C.*

Proof. Since C is absorbing we have that $V \subset \bigcup_{n=1}^{\infty} nC$. Knowing that V is a complete metric space we can apply the Baire category theorem to see that the closed set C is not nowhere dense. Thus the interior of C, C°, is not empty. Take v in C° and let U be a symmetric open set around 0 such that $v + U \subset C^{\circ}$ (e.g. take U to be one of the $B_k(\frac{1}{k})$ described in Corollary 4.12).

Because C is symmetric we have that $-v - U = -v + U$ is in C. Since C is convex it contains the convex hull of $v + U$ and $-v + U$. But this convex hull contains U; observe for any $w \in U$ we have that

$$w = \frac{(v + w) + (-v + w)}{2}$$

Thus we are done. □

4.3 Weak Topology

The weak topology is the simplest topology placed on the dual of a countably–normed space. It is defined as follows:

Definition 4.22. The *weak topology* on the dual V' of a countably–normed space V is the coarsest vector topology on V' such that the functional $\langle \cdot, v\rangle$ is continuous for any $v \in V$.

In the following propositions, we prove some commonly used properties of the weak topology.

Proposition 4.23. *The weak topology on V' has a local base of neighborhoods given by sets of the form:*

$$N(v_1, v_2, \ldots, v_k; \varepsilon) = \{v' \in V';\ |\langle v', v_j\rangle| < \varepsilon,\ 1 \leq j \leq k\}$$

Proof. In order for $\langle \cdot, v\rangle$ to be continuous for all $v \in V$ we need $\langle \cdot, v\rangle$ to be continuous at 0. Or equivalently, we require that $\langle \cdot, v\rangle^{-1}(-\varepsilon, \varepsilon) = N(v; \varepsilon)$ be open for each $\varepsilon \in \mathbb{R}$. Hence for each $v \in V$ we form the topology τ_v on V given by the local base $\{N(v; \varepsilon)\}_{\varepsilon > 0}$ The weak topology is the least upper bound topology for the family $\{\tau_v\}_{v \in V}$ (see subsection 4.1.3). Thus, by Theorem 4.5, a local base for the weak topology is given by sets of the form

$$N(v_1, v_2, \ldots, v_k; \varepsilon) = N(v_1; \varepsilon) \cap N(v_2; \varepsilon) \cap \cdots \cap N(v_k; \varepsilon)$$

where $v_1, v_2, \ldots, v_k \in V$. □

Proposition 4.24. *The inclusion map $i'_n : V'_n \to V'$ is continuous when V' is given the weak topology.*

Proof. Consider the weak base neighborhood $N(v_1 \dots v_k; \varepsilon)$ where $v \in V$. Observe that

$$i'^{-1}_n (N(v_1 \dots v_k; \varepsilon)) = \{v' \in V'_n;\ |\langle v', v_j \rangle| < \varepsilon,\ 1 \leq j \leq k\}$$

Since for each j, $v_j \in V \subset V_n$ we have that the functional $\langle \cdot, v_j \rangle$ is continuous on V'_n. (Since V_n is a Banach space, $V_n \subset V''_n$.) Thus $\{v' \in V'_n;\ |\langle v', v_j \rangle| < \varepsilon,\ 1 \leq j \leq k\}$, is open in V'_n, being the finite intersection of open sets. $\square$

Proposition 4.25. *Let V be a countably–Hilbert space. Then the space V'_n is dense in V' when V' is endowed with the weak topology.*

Proof. Consider $v' \in V'$. An arbitrary neighborhood U of v' contains a set of the form $v' + N$ where $N = N(v_1, \dots, v_k; \varepsilon) = \{v' \in V';\ |\langle v', v_j \rangle| < \varepsilon,\ 1 \leq j \leq k\}$. We must find a $v'_n \in V_n$ such that $v'_n \in v' + N$. That is $|\langle v'_n - v', v_j \rangle| < \varepsilon$ for all $1 \leq j \leq k$.

Now $v' \in V_l$ for some l since $V' = \bigcup_{n=1}^{\infty} V'_n$. If $l \leq n$ we are done, since $V'_l \subset V'_n$ by Proposition 4.14. If $l > n$ a little more work needs to be done, but it is still very straightforward.

For clarity, we assume $k = 2$ and v_1, v_2 are independent unit vectors in V_n. (There is no harm in assuming this. We can just shrink ε suitably by dividing by the maximum of $|v_1|_n$ and $|v_2|_n$.) Suppose $\langle v', v_1 \rangle = \lambda_1$ and $\langle v', v_2 \rangle = \lambda_2$. Write v_2 as $v_2 = \alpha v_1 + \beta v_1^{\perp}$ where $v_1^{\perp}$ is a unit vector in the orthogonal complement of $\{v_1\}$ in V_n. Then $\lambda_2 = \langle v', v_2 \rangle = \lambda_1 \alpha + \beta \langle v', v_1^{\perp} \rangle$ or equivalently $\langle v', v_1^{\perp} \rangle = \frac{\lambda_2 - \lambda_1 \alpha}{\beta}$. Consider $w = \lambda_1 v_1 + \frac{\lambda_2 - \lambda_1 \alpha}{\beta} v_1^{\perp}$. Now $w \in V_n$. Thus $\langle w, \cdot \rangle_n$ is in V'_n, where $\langle \cdot, \cdot \rangle_n$ is the inner-product on V_n. We now observe that $\langle w, v_1 \rangle_n = \lambda_1$ and $\langle w, v_2 \rangle_n = \langle w, \alpha v_1 + \beta v_1^{\perp} \rangle_n = \lambda_1 \alpha + \lambda_2 - \lambda_1 \alpha = \lambda_2$. Hence $\langle w, \cdot \rangle_n$ agrees with v' on v_1 and v_2. Therefore $w \in v' + N$ and we have that V'_n is dense in V. $\square$

4.4 Strong Topology

Recall the notion of bounded sets in a countably–normed space V (as in subsections 4.2.2 and 4.2.4). Using bounded sets in V we can define the *strong topology* on V'.

Definition 4.26. The *strong topology* on the dual V' of a countably–normed space V is defined to be the topology with a local base given by sets of the form

$$N(D; \varepsilon) = \{v' \in V';\ \sup_{v \in D} |\langle v', v \rangle| < \varepsilon\}$$

where D is any bounded subset of V and $\varepsilon > 0$.

Taking D to be a finite set such as $\{v_1, v_2, \dots, v_k\}$, it is clear that the strong topology is finer than the weak topology.

Proposition 4.27. *The inclusion map $i'_n : V'_n \to V'$ is continuous when V' is given the strong topology.*

Proof. Consider the neighborhood $N(D;\varepsilon) = \{v' \in V';\ \sup_{v\in D} |\langle v', v\rangle| < \varepsilon\}$ where D is a bounded set in V and $\varepsilon > 0$. Now

$$i'^{-1}_n(N(D;\varepsilon)) = \left\{v' \in V'_n;\ \sup_{v\in D} |\langle v', v\rangle| < \varepsilon\right\}$$

Let $\sup_{v\in D} |v|_n = M$. Take v'_0 in $i'^{-1}_n(N(D;\varepsilon))$ and let $c_0 = \sup_{v\in D} |\langle v'_0, v\rangle| < \varepsilon$. Consider the open set $B(v'_0, \frac{\varepsilon - c_0}{M+1}) = \{v' \in V'_n;\ |v' - v'_0|_{-n} < \frac{\varepsilon - c_o}{M+1}\}$. We assert that $B(v'_0, \frac{\varepsilon-c_0}{M+1}) \subset i'^{-1}_n(N(D;\varepsilon))$.

Take $v' \in B(v'_0, \frac{\varepsilon-c_0}{M+1})$. Then $|v' - v'_0|_{-n} < \frac{\varepsilon-c_0}{M+1}$. This gives us the following

$$\sup_{v\in D} \left|\langle v' - v'_0, \tfrac{v}{|v|_n}\rangle\right| < \frac{\varepsilon - c_0}{M+1}$$

Thus $\sup_{v\in D} |\langle v' - v'_0, v\rangle| < \varepsilon - c_0$, since $|v|_n \leq M$ when $v \in D$. From this we see that $\sup_{v\in D} |\langle v', v\rangle| < \varepsilon$. Therefore $v' \in i'^{-1}_n(N(D;\varepsilon))$. □

4.4.1 Strongly Bounded Sets of V'

When V' is endowed with the strong topology, a bounded set $B \subset V'$ is called *strongly bounded.* (Likewise when V' has the weak topology, B is said to be *weakly bounded*). Strongly bounded sets have many nice properties, which we will prove in this section. First let us begin with the following definition:

Definition 4.28. A set $B \subset V'$ is said to be *bounded on the set* $A \subset V$ if

$$\sup_{v'\in B, v\in A} |\langle v', v\rangle| < \infty$$

Lemma 4.29. *A set $B \subset V'$ is strongly bounded if and only if it is bounded on each bounded set $D \subset V$.*

Proof. ($\Rightarrow$) Let $B \subset V'$ be strongly bounded and let D be a bounded set of V. Consider the neighborhood of V' given by

$$N(D;1) = \left\{v' \in V';\ \sup_{v\in D} |\langle v', v\rangle| < 1\right\}$$

Since B is bounded there exists an $\lambda > 0$ such that $B \subset \lambda N(D;1)$ or equivalently $\frac{1}{\lambda}B \subset N(D;1)$. Then for $v' \in B$ we have $\frac{v'}{\lambda} \in N(D;1)$. Thus $|\langle v, v'\rangle| \leq \lambda$ for any $v \in D$. Therefore B is bounded on the set D.

($\Leftarrow$) Suppose B is bounded on each bounded set $D \subset V$. Consider a neighborhood $N(D;\varepsilon)$ of 0 in V'. By hypothesis, $\sup_{v'\in B, v\in D} |\langle v', v\rangle| = M < \infty$. So for any $v' \in B$ we have that $|\langle \frac{\varepsilon v'}{M+1}, v\rangle| < \varepsilon$ when $v \in D$. Thus $\frac{\varepsilon}{M+1}B \subset N(D;\varepsilon)$ or equivalently $B \subset \frac{M+1}{\varepsilon}N(D;\varepsilon)$. Hence B is bounded. □

Lemma 4.30. *A set $B \subset V'$ is strongly bounded if an only if there exists k such that B is bounded on $B_k(\frac{1}{k})$.*

Proof. ($\Rightarrow$) As per Corollary 4.12, consider the local base sets $B_1(1) \supset B_2(\frac{1}{2}) \supset \cdots$ of V. By contradiction suppose that B is not bounded on $B_k(\frac{1}{k})$ for any k. Then for every k there exist a $v_k \in B_k(\frac{1}{k})$ and a $v'_k \in B$ such that $|\langle v'_k, v_k\rangle| > k$. The sequence $\{v_k\}$ goes to 0, thus it must be bounded. So by Lemma 4.29 there must exist a positive number M such that $|\langle v', v_k\rangle| \leq M$ for all $v' \in B$ and all $k \in \{1, 2, \ldots\}$. This contradicts the way v'_k and v_k were chosen.

($\Leftarrow$) Conversely, let $B \subset V'$ be bounded on some $B_k(\frac{1}{k}) \subset V$. Take a bounded set D in V. Then $D \subset \lambda B_k\big(\frac{1}{k}\big)$ for some $\lambda > 0$. Thus B is bounded on D, since B is bounded on $\lambda B_k\big(\frac{1}{k}\big)$. Thus by Lemma 4.29, B is bounded. $\square$

Theorem 4.31. *A set $B \subset V'$ is strongly bounded if and only if $B \subset V'_k$ for some k and B is bounded in the norm $|\cdot|_{-k}$ of V'_k.*

Proof. ($\Leftarrow$) Let $B \subset V'_k$ be bounded in the norm $|\cdot|_{-k}$ by some $M > 0$ (i.e. $\sup_{v' \in B} |v'|_{-k} < M$). Consider the set $B_k(1) = \{v \in V; |v|_k < 1\}$. Then for $v' \in B$ and $v \in B_k(1)$ we have that $|\langle v', v\rangle| \leq M$. Thus B is bounded on $B_k(1)$ and hence on $B_k(\frac{1}{k})$. Therefore B is strongly bounded by Lemma 4.30.

($\Rightarrow$) Conversely suppose B is a strongly bounded set in V'. Then by Lemma 4.30 there is a k such that B is bounded on the set $B_k(\frac{1}{k}) = \{v \in V; |v|_k < \frac{1}{k}\}$. That is there is an $M < \infty$ such that $|\langle v', v\rangle| \leq M$ for all $v' \in B$ and all $v \in B_k\big(\frac{1}{k}\big)$.

Let $N_k \subset V_k$ be given by $N_k = \{v \in V_k; |v|_k < \frac{1}{k}\}$. Since V is dense in V_k we have that

$$\sup_{v' \in B, v \in N_k} |\langle v', v\rangle| \leq M$$

From the above we see for any $v' \in B$ and unit vector $v \in V_k$ we have that $|\langle v', \frac{v}{(k+1)}\rangle| < M$. Hence $|v'|_{-k} \leq (k+1)\, M$. Thus for any $v' \in B$ we have that $v' \in V'_k$ and $|v'|_{-k} \leq (k+1)\, M$. $\square$

4.4.2 Reflexivity

Just as we can discuss the dual V' of V, we can also talk about the dual of V'. Of course, this depends on the topology we put on V'. As we will see it turns out that $V'' = V$ as sets if V' is given the weak or strong topology (and V is a countably–Hilbert space). We can also put a topology on V''. We construct this topology from the strongly bounded sets in V'. For each set B in V' that is strongly bounded and each $\varepsilon > 0$ form the neighborhood

$$N(B; \varepsilon) = \Big\{\hat{v} \in V''; \sup_{v' \in B} |\langle \hat{v}, v'\rangle| < \varepsilon\Big\}$$

Take the collection of all sets $N(B; \varepsilon)$ as our local base in V''. We call this topology the *strong topology on V''*. Given this topology we will also see that V'' is homeomorphic to V.

Proposition 4.32. *Let V be a countably–Hilbert space. Then $V = V''$ when V' is given the weak or strong topology.*

Proof. Consider $v \in V$ and the corresponding linear functional $\hat{v}$ on V' given by

$$\langle \hat{v}, v' \rangle = \langle v', v \rangle \qquad \text{where } v' \in V'$$

Observe that $\langle \hat{v}, \cdot \rangle$ is continuous since $\langle \hat{v}, \cdot \rangle^{-1}(-\varepsilon, \varepsilon) = \{v' \in V'; |\langle v', v \rangle| < \varepsilon\}$ which is open in the weak (and hence the strong) topology on V'.

Also note that if $\hat{u} = \hat{v}$, then $\langle v', v \rangle = \langle v', u \rangle$ for all $v' \in V'$. Thus $v = u$. Therefore the correspondence $v \to \hat{v}$ is injective.

We now show that the correspondence $v \to \hat{v}$ is surjective. Take $v'' \in V''$. Then v'' is continuous on V'. Since, by Proposition 4.14, $V' = \bigcup_{n=1}^{\infty} V_n'$ we have that $v'' \in V_n''$ for all n. But $V_n = V_n''$ since V_n is a Hilbert space. Thus v'' can be considered as an element of V_n for all n. Since V is a countably–Hilbert space we have that $\cap_{n=1}^{\infty} V_n = V$ by Proposition 4.9. Thus $v'' \in V$ and we have that $v \to \hat{v}$ is surjective. □

Theorem 4.33. *If V is a countably–Hilbert space, then V'' is homeomorphic to V when V'' is given the strong topology.*

Proof. From Proposition 4.32 we already see that $V = V''$. We now need to see that the correspondences $\hat{v} \to v$ and $v \to \hat{v}$ are continuous.

First we consider the continuity of $v \to \hat{v}$. Let $N(B; \varepsilon)$ be a neighborhood of 0 in V''. So we have that B is a strongly bounded set in V'. By Theorem 4.31 we know that $B \subset V_k'$ for some k and is bounded in the norm $|\cdot|_{-k}$. Let us call $\sup_{v' \in B} |v'|_{-k} = M < \infty$. Consider the neighborhood $B_k(\frac{\varepsilon}{M}) \subset V$ given by $B_k(\frac{\varepsilon}{M}) = \{v \in V \,;\, |v|_k < \frac{\varepsilon}{M}\}$. Take a $v \in B_k(\frac{\varepsilon}{M})$. We need to see that $\hat{v} \in N(B; \varepsilon)$. For any $v' \in B$ we have that

$$|\langle \hat{v}, v' \rangle| = |\langle v', v \rangle| \leq |v'|_{-k} |v|_k < M \frac{\varepsilon}{M} = \varepsilon$$

So $\hat{v} \in N(B; \varepsilon)$. Thus $v \to \hat{v}$ is continuous.

Now consider $\hat{v} \to v$. Let $0 < \varepsilon < 1$ and take $B_k(\varepsilon) = \{v \in V; |v|_k < \varepsilon\}$, a member of the local base for V (see subsection 4.2.1). Let $B \subset V'$ be given by

$$B = \{v' \in V'; |\langle v', v \rangle| \leq 1 \text{ for all } v \in V_k \text{ with } |v|_k < \varepsilon\}$$

Note that B is strongly bounded by Theorem 4.31. So we can form the local base element $N(B; \varepsilon)$ of V'' given by

$$N(B; \varepsilon) = \left\{ \hat{v} \in V''; \sup_{v' \in B} |\langle \hat{v}, v' \rangle| < \varepsilon \right\}$$

Take a $\hat{v} \in N(B; \varepsilon)$. Note that $\langle \frac{v}{|v|_k}, \cdot \rangle_k \in B$ since $\langle \frac{v}{|v|_k}, u \rangle_k \leq |u|_k$ for $u \in V_k$. Since $\hat{v} \in N(B; \varepsilon)$ and $\langle \frac{v}{|v|_k}, \cdot \rangle_k \in B$, we must have $|\langle \frac{v}{|v|_k}, v \rangle_k| = |v|_k < \varepsilon$. Therefore $v \in B_k(\varepsilon)$. This proves the continuity of the map $\hat{v} \to v$.

□

4.4.3 Completeness in V'

Suppose V' is given the strong topology. The convergence of a sequence of functionals $\{v'_k\}_{k=1}^{\infty}$ in V' to an element $v' \in V'$ is called *strong convergence* and $\{v'_k\}_{k=1}^{\infty}$ is said to *converge strongly* to v'. Obviously $\{v'_k\}_{k=1}^{\infty}$ converging strongly to v' is equivalent to $\{v'_k - v'\}_{k=1}^{\infty}$ converging strongly to 0. Thus a sequence $\{v'_k\}_{k=1}^{\infty}$ converges strongly to v' if and only if for any bounded set $D \subset V$ and any number $\varepsilon > 0$ there exist a $K > 0$ such that $v'_k - v' \in N(D;\varepsilon) = \{v' \in V';\ \sup_{v\in D} |\langle v', v\rangle| < \varepsilon\}$ for all $k \geq K$. Hence a sequence $\{v'_k\}_{k=1}^{\infty}$ converges strongly to v' if and only if $\{\langle v'_k, \cdot\rangle\}_{k=1}^{\infty}$ converges uniformly to $\langle v', \cdot\rangle$ on each bounded set $D \subset V$. We say that a sequence $\{v'_k\}_{k=1}^{\infty}$ is *strongly Cauchy* (or *strongly fundamental*) if the sequence of numbers $\{\langle v'_k, v\rangle\}_{k=1}^{\infty}$ converges for each element $v \in V$ and the convergence is uniform on each bounded set $D \subset V$.

Theorem 4.34. *Let V be a countably–normed space. The dual V' of V is complete under the strong topology.*

Proof. Let $\{v'_k\}_{k=1}^{\infty}$ be a strongly Cauchy sequence in V'. Then for $v \in V$ we have that the sequence of numbers $\{\langle v'_k, v\rangle\}_{k=1}^{\infty}$ converges. We conveniently denote this limit by $\langle v', v\rangle$. For for each $v \in V$ we have

$$\langle v', v\rangle = \lim_{k\to\infty} \langle v'_k, v\rangle$$

This functional $\langle v', \cdot\rangle$ is clearly linear on V. We have to check that it is continuous. For this it is sufficient to see that $\langle v', \cdot\rangle$ is bounded on bounded sets (see Proposition 4.15). Let D be a bounded set in V. Observe the functions $\{\langle v'_k, \cdot\rangle\}_{k=1}^{\infty}$ are bounded on D. Moreover they converge uniformly to $\langle v', \cdot\rangle$ on D. Hence there is a $K > 0$ such that $|\langle v' - v'_K, v\rangle| < 1$ for all v in D. Thus we have that

$$\sup_{v\in D} |\langle v', v\rangle| \leq \sup_{v\in D} |\langle v'_K, v\rangle| + 1 < \infty$$

Therefore $\langle v', \cdot\rangle$ is bounded on bounded sets and hence continuous. So $v' \in V'$ and V' is complete with respect to the strong topology. $\square$

4.4.4 Comparing the Weak and Strong Topology

When a countably–normed space V is complete, many properties of the strong and weak topologies coincide. We will see that weakly and strongly bounded sets are one in the same. Also under suitable conditions, weak and strong convergence coincide.

Theorem 4.35. *Let V be a complete countably–normed space with dual V'. Every weakly bounded set in V' is strongly bounded.*

Proof. By Lemma 4.30 and Corollary 4.12 it is sufficient to show that a weakly bounded set B is bounded on some neighborhood of zero in V.

Let us define a set $C \subset V$ as follows:

$$C = \{v \in V; |\langle v', v\rangle| \leq 1 \text{ for all } v' \in B\} = \bigcap_{v' \in B} \{v \in V; |\langle v', v\rangle| \leq 1\}$$

Observe that C is closed, being the intersection of closed sets, C is convex, being the intersection of convex sets, and C is symmetric, being the intersection of symmetric sets. Finally note that C is absorbent: Take $v \in V$. Since B is weakly bounded we must have $B \subset \lambda N(v; 1)$ where $N(v; 1) = \{v' \in V';\ |\langle v', v\rangle| < 1\}$ for some $\lambda > 0$. Thus $|\langle v', v\rangle| \leq \lambda$ for all $v' \in B$. Hence $\frac{v}{\lambda} \in C$ or equivalently $v \in \lambda C$.

So we can apply Lemma 4.21 to see that there is a neighborhood U of 0 in V such that $U \subset C$. Therefore the elements of B are uniformly bounded on U (by 1). Thus B is bounded on U and hence strongly bounded. □

Corollary 4.36. *Let V be a complete countably–normed space with dual V'. If a sequence $\{v'_k\}_{k=1}^{\infty}$ in V' converges pointwise (on each $v \in V$), then $\{v'_k\}_{k=1}^{\infty}$ is strongly bounded.*

Proof. Since $\{v'_k\}_{k=1}^{\infty}$ converges pointwise, it is weakly bounded. □

Corollary 4.37. *Let V be a complete countably–normed space with dual V'. Then V' is complete with respect to the weak topology.*

Proof. Take a Cauchy sequence $\{v'_k\}_{k=1}^{\infty} \subset V'$. Then by Corollary 4.36, we have that $\{v'_k\}_{k=1}^{\infty}$ is strongly bounded. Thus by Lemma 4.30, $\{v'_k\}_{k=1}^{\infty}$ is bounded on some neighborhood U of 0 in V. That is, there exist an $M > 0$ such that $|\langle v'_k, v\rangle| \leq M$ for all $v \in U$ and all $k \in \{1, 2, \ldots\}$.

Define v' by $\langle v', v\rangle = \lim_{k\to\infty}\langle v'_k, v\rangle$. Obviously, v' is linear. Observe that for all $v \in U$ we have

$$|\langle v', v\rangle| = \lim_{k\to\infty} |\langle v'_k, v\rangle| \leq M$$

So v' is bounded on U and hence continuous (by Corollary 4.16). □

Of particular interest are countably–normed spaces such with the property that bounded sets are limit point compact. These spaces have many wonderful properties, that do not hold in general for infinite-dimensional normed spaces. We make the following definition (the terminology comes from Gel'fand [8]):

Definition 4.38. A complete countably–normed space V in which all bounded sets are limit point compact is called *perfect*.

Remark 4.39. Since Theorem 4.20 gives us that V is metrizable, limit point compact can be replaced with compact or sequentially compact in the above definition. Therefore if V is perfect, the strong topology on V' is nothing more than the well known *compact–open topology* [23].

Theorem 4.40. *Let V be a perfect space with dual V'. Then a sequence $\{v'_k\}_{k=1}^{\infty}$ in V' converges strongly if and only if it converges weakly. i.e. weak and strong converge coincide on the dual space V'*

Proof. Obviously strong convergence implies weak convergence. So take a a sequence $\{v'_k\}_{k=1}^{\infty}$ in V' which converges weakly to $v' \in V'$. Without loss of generality we can take $v' = 0$ (replace v'_k with $v'_k - v'$). The sequence $\{v'_k\}_{k=1}^{\infty}$ is weakly bounded, being weakly convergent. Thus by Theorem 4.35 we have that $\{v'_k\}_{k=1}^{\infty}$ is strongly bounded.

To show $\{v'_k\}_{k=1}^{\infty}$ converges strongly we must show $\langle v'_k, \cdot\rangle$ goes to 0 uniformly on each bounded set $D \subset V$. Suppose, by contradiction, that there exist a bounded set D in V where $\langle v'_k, \cdot\rangle$ does not go to 0 uniformly. So for some $\varepsilon > 0$, there is a $k_1 \geq 1$ such that $\left|\langle v'_{k_1}, v\rangle\right| \geq \varepsilon$ for some $v \in D$. Name this v as v_{k_1}. Likewise there an $k_2 > k_1$ and $v_{k_2} \in V$ such that $\left|\langle v'_{k_2}, v_{k_2}\rangle\right| \geq \varepsilon$. Continuing in this manner we form a sequence $\{v_{k_j}\}_{j=1}^{\infty}$ in V. This sequence is bounded, being taken from the bounded set D.

Knowing that V is a perfect space we have a subsequence of $\{v_{k_j}\}_{j=1}^{\infty}$ that converges to some v in V. Renumbering if necessary we will just take this subsequence to be $\{v_{k_j}\}_{j=1}^{\infty}$. Since $\{v_{k_j}\}_{j=1}^{\infty}$ goes to v in V then the sequence given by $w_{k_j} = v_{k_j} - v$ goes to 0 in V.

Now for any strongly bounded set $B \subset V'$, Theorem 4.31 guarantees that $\langle v', w_{k_j}\rangle$ goes to 0 uniformly for all $v' \in B$. So take B to be the set $\{v'_{k_j}\}_{j=1}^{\infty}$. Then $\langle v'_{k_j}, w_{k_j}\rangle$ goes to 0 and by weak convergence we have that $\langle v_{k_j}, v\rangle$ goes to 0. Thus

$$\lim_{j\to\infty} \langle v'_{k_j}, v_{k_j}\rangle = \lim_{j\to\infty} \langle v'_{k_j}, w_{k_j}\rangle + \langle v'_{k_j}, v\rangle = 0$$

This contradicts the construction of the v_{k_j} and v'_{k_j}. □

4.5 Inductive Limit Topology

Given a sequence of normed spaces $\{(W_n, |\cdot|_n); n \geq 1\}$ with W_n continuously imbedded in W_{n+1} for all n, we form the space $W = \bigcup_{n=1}^{\infty} W_n$ and endow W with the finest locally convex vector topology such that for each n the inclusion map $i_n : W_n \to W$ is continuous. This topology is call the *inductive limit topology* on W and W is said to be the *inductive limit* of the sequence $\{(W_n, |\cdot|_n); n \geq 1\}$

4.5.1 Local Base

As always, when discussing a vector topology, we should try to discover what a useful local base for the topology would be.

Theorem 4.41. *Suppose W is the inductive limit of the normed spaces $\{(W_n, |\cdot|_n); n \geq 1\}$. A local base for W is given by the set $\mathcal{B}$ of all balanced convex subsets U of W such that $i_n^{-1}(U)$ is a neighborhood of 0 in W_n for all n.*

Proof. We first apply Lemma 4.4 to see the set $\mathcal{B}$ is in fact a local base for W. Take $U, V \in \mathcal{B}$, then clearly $U \cap V \in \mathcal{B}$. Now if $U \in \mathcal{B}$, then it is easy to see that $\alpha U \in \mathcal{B}$ for $\alpha \neq 0$. Finally we show $U \in \mathcal{B}$ is absorbing. Note that $i_n^{-1}(U)$ is absorbing in W_n (since W_n is a normed space and $i_n^{-1}(U)$ is open in W_n). Thus U absorbs all the point of $W_n = i_n(W_n) \subset W$. Since $W = \bigcup_{n=1}^{\infty} W_n$, U absorbs W. Thus by Lemma 4.4 we see that $\mathcal{B}$ is a base of neighborhoods for a locally convex vector topology on W.

It is fairly straightforward to see that $\mathcal{B}$ gives us the finest locally convex vector topology making all the $i_n : W_n \to W$ continuous: Let τ be a locally convex vector topology on W making all the i_n continuous. Take a convex neighborhood (of 0) U in τ. By Lemma 4.3 we can assume U is balanced. Since each i_n is continuous, we have $i_n^{-1}(U)$ is a neighborhood in W_n. Thus $U \in \mathcal{B}$. $\square$

Corollary 4.42. *Suppose W is the inductive limit of the normed spaces $\{(W_n, |\cdot|_n); n \geq 1\}$. A local base for W is given by the balanced convex hulls of sets of the form $\bigcup_{n=1}^{\infty} i_n(B_n(\varepsilon_n))$ (where $B_n(\varepsilon_n) = \{x \in W_n \, ; \, |x|_n < \varepsilon_n\}$).*

Proof. Let U be the balanced convex hull of the set $\bigcup_{n=1}^{\infty} i_n(B_n(\varepsilon_n))$ in W. Then $B_n(\varepsilon_n) \subset i_n^{-1}(U)$. So $i_n^{-1}(U)$ is a neighborhood of 0 in W_n. By Theorem 4.41 such a U is a neighborhood in W.

Now if U is any balanced convex neighborhood of 0 in W, then $i_n^{-1}(U)$ contains a neighborhood $B_n(\varepsilon_n)$. Hence $i_n(B_n(\varepsilon_n)) \subset U$. Since U is convex and balanced, the balanced convex hull of $\bigcup_{n=1}^{\infty} i_n(B_n(\varepsilon_n))$ is contained in U. Thus the sets described form a local base for W. $\square$

4.5.2 Inductive Limit Topology on V'

Let V be a countably–normed space. Then V', the dual of V, can be regarded as the inductive limit of the sequence of normed spaces $\{(V_n', |\cdot|_{-n}); n \geq 1\}$. Thus V' can be given the inductive limit topology. In light of Proposition 4.24 and Proposition 4.27 we see that the inductive limit topology on V' is finer than the strong and weak topology on V'. We also have the following useful result about convergence on V' in the inductive topology:

Theorem 4.43. *Let V be a countably–normed space. Endow V' with the inductive limit topology. A sequence $\{v_k'\}_{k=1}^{\infty}$ converges to v' in V' if and only if there exists some n such that $v_k \in V_n'$ for all k and $\lim_{k\to\infty} |v_k' - v|_{-n} = 0$ (i.e. v_k' converges to v' in V_n').*

Proof. ($\Leftarrow$) Using Corollary 4.42, this direction is obvious.

($\Rightarrow$) Let $\{v_k'\}_{k=1}^{\infty}$ be sequence in V' that converges to $v' \in V'$. Replacing v_k' with $v_k' - v'$, if necessary, we assume that $v' = 0$. Since $\{v_k'\}_{k=1}^{\infty}$ converges to 0 in the inductive limit topology, by the above discussion, it converges to 0 in the strong topology on V. Hence $\{v_k'\}_{k=1}^{\infty}$ is strongly bounded. Thus by Theorem 4.31 we have that there is an n such that $\{v_k'\}_{k=1}^{\infty} \subset V_n'$.

Now we must show that $|v'_k|_{-n}$ goes to 0 as k tends to infinity. That is for a given $\varepsilon > 0$ we need to find a $K > 0$ such that for all $k \geq K$ we have $|v'_k|_{-n} < \varepsilon$. Consider the base neighborhood U of V' given by the balanced convex hull of $\bigcup_{l=1}^{\infty} B_l$ where for $l = n$ we take

$$B_n = \{v' \in V'_n\,;\, |v'|_{-n} < \varepsilon\}$$

For $l < n$, $B_l = \{v' \in V'_l\,;\, |v'|_{-l} < \varepsilon_l\}$ where $\varepsilon_l > 0$ is chosen so that B_l is contained in $i'^{-1}_{l,n}(B_n)$. (Such an $\varepsilon_l > 0$ exist by the continuity of the inclusion map $i'_{l,n} : V'_l \to V'_n$.)

And for $l > n$ we first note that the restricted inclusion $\tilde{i}_{n,l} : V'_n \to i_{n,l}(V'_n) = V'_n \subset V'_l$ is a homeomorphism (since V'_n is continuously imbedded into V'_{n+1} for each n). This gives us $i'_{n,l}(B_n) \cap V'_n = W \cap V'_n$ where W is open in V'_l. Thus take $B_l = \{v' \in V'_l\,;\, |v'|_{-l} < \varepsilon_l\}$ where $\varepsilon_l > 0$ is chosen so that $B_l \subset W$.

Now since U is open, there is a K such that for all $k \geq K$ we have that $v'_k \in U$. We will show that $v'_k \in B_n$ for $k \geq K$. Let $k \geq K$ and consider the element v'_k. Since $v'_k \in U$ we can write v'_k as $v'_k = \sum_{j=1}^{m} \lambda_j y_j$ where $\sum_{j=1}^{m} |\lambda_j| \leq 1$ and $y_j \in B_j$. Observe that each y_j with $\lambda_j \neq 0$ is in V'_n. (If there is an y_j not in V'_n with $\lambda_j \neq 0$, then v'_k could not be V'_n.) Thus we have

$$|v'_k|_{-n} \leq \sum_{j=1}^{m} |\lambda||y_j|_{-n} \tag{4.4}$$

Observe for $j \leq n$, $y_j \in B_j \subset i'^{-1}_{j,n}(B_n)$. So $|y_j|_{-n} < \varepsilon$. Also for $j > n$ we have that $y_j \in B_j$. Since $y_j \in V'_n$ we get that $y_j \in B_j \cap V'_n \subset i'_{n,j}(B_n) \cap V'_n$. So $|y_j|_{-n} < \varepsilon$.

Therefore in (4.4) we have that

$$|v'_k|_{-n} \leq \sum_{j=1}^{\infty} |\lambda||y_j|_{-n} < \sum_{j=1}^{\infty} |\lambda_j|\varepsilon \leq \varepsilon$$

Thus v'_k is in B_n for all $k \geq K$ and we are done.

□

4.6 Comparing the Three Topologies

In this section we compare the three topologies on the dual V' of a countably–normed space V. In order to do this efficiently we first introduce a fourth topology on V'. It is the *Mackey topology* on V'.

4.6.1 Mackey Topology

In order to talk about the Mackey topology we need the following notion:

Definition 4.44. Let $\mathcal{D}$ be a set of bounded subsets of a topological vector space E with dual E'. The topology of *uniform convergence on the sets of* $\mathcal{D}$ is the topology with subbasis neighborhoods of 0 given by

$$N(D;\varepsilon) = \Big\{ v' \in E' \, ; \, \sup_{v \in D} |\langle v', v \rangle| < \varepsilon \Big\}$$

where $D \in \mathcal{D}$ and $\varepsilon > 0$. This is also referred to as the topology of $\mathcal{D}$*–convergence* on E'.

From the definition we see that a local base neighborhood for the topology of $\mathcal{D}$–convergence on a vector space E with dual E' looks like

$$N(D_1;\varepsilon_1) \cap N(D_2;\varepsilon_2) \cap \cdots N(D_k;\varepsilon_k)$$

where $D_j \in \mathcal{D}$ and $\varepsilon_j > 0$ for all $1 \le j \le k$. We now state the following theorem without proof:

Theorem 4.45 (Mackey-Arens)**.** *Suppose that under a locally convex vector topology τ, E is a Hausdorff space. Then E has dual E' under τ if and only if τ is a topology of uniform convergence on a set of balanced convex weakly–compact subsets of E'.*

For a proof of this results see [29], [32], or [15]. Using this theorem we can define the Mackey topology as follows:

Definition 4.46. Let E be a topological vector space with dual E'. The *Mackey topology* on E is the topology on uniform convergence on all balanced convex weakly–compact subsets of E'.

Remark 4.47. From this discussion we see that the Mackey topology on V' has a local base given by

$$N(C;\varepsilon) = \Big\{ v' \in V' \, ; \, \sup_{v \in C} |\langle v', v \rangle| < \varepsilon \Big\}$$

where $\varepsilon > 0$ and C is a balanced convex weakly–compact set in V.

Remark 4.48. Although we have not defined the term weakly–compact, it is nothing to fret about. Just as we have defined the weak topology on V', we can define an analogous topology on V. This topology has as its local base sets of the form

$$N(v_1', v_2', \ldots, v_k'; \varepsilon) = \big\{ v \in V; \; |\langle v_j', v \rangle| < \varepsilon, \; 1 \le j \le k \big\}$$

When a set in V is said to be weakly–compact, it simply means that the set is compact with respect to the weak topology on V.

4.6.2 The Topologies on V'

Let us make the following notational convention throughout this section:

Notation. Let V be a countably–normed space with dual V'. The weak topology, strong topology, inductive limit topology, and Mackey topology on V' with be denoted by τ_w, τ_s, τ_i, and τ_m, respectively.

Proposition 4.49. *Let V be a countably–normed space. Suppose $C \subset V$ is weakly–compact, then C is weakly bounded.*

Proof. Let $v' \in V'$ and $\varepsilon > 0$ be given. We have to show there exists a k such that $C \subset kN(v'; \varepsilon)$ (see Definition 4.17). Cover C by the sets $\{kN(v'; \varepsilon)\}_{k=1}^{\infty}$. Since C is weakly–compact, $C \subset kN(v'; \varepsilon)$ for some k. □

Corollary 4.50. *Let V be a countably–normed space with dual V'. Then the strong topology τ_s is finer than the Mackey topology τ_m on V'.*

Proof. The topology τ_s is by definition the topology of uniform convergence on all bounded sets in V. But by Theorem 4.18 every bounded set in V is weakly bounded. And by Proposition 4.49, we have that every weakly–compact set is weakly bounded. Thus $\tau_m \subset \tau_s$. □

Lemma 4.51. *Let V be a countably–normed space with dual V'. Then V' is Hausdorff in the weak topology t_w, and hence in the strong, Mackey, and inductive limit topologies.*

Proof. Take $u' \in V'$. We must find a neighborhood of 0 in τ_w that does not contain u'. Take $v \in V$ such that $|\langle u', v\rangle| \neq 0$. Let $|\langle u', v\rangle| = \lambda \neq 0$. Consider the set $N(v; \frac{\lambda}{2}) = \left\{v' \in V';\ |\langle v', v\rangle| < \frac{\lambda}{2}\right\}$. This set cannot contain u'. Thus V' is Hausdorff in the weak topology (and hence in the finer strong, Mackey, and inductive topologies). □

Lemma 4.52. *Let V be a countably–Hilbert space with dual V'. Then the dual of V' is V when V' is given the weak, strong, Mackey, or inductive limit topology.*

Proof. Consider $v \in V$ and the corresponding linear functional $\hat{v}$ on V' given by

$$\langle \hat{v}, v'\rangle = \langle v', v\rangle \qquad \text{where } v' \in V'$$

Observe that $\langle \hat{v}, \cdot\rangle$ is continuous since $\langle \hat{v}, \cdot\rangle^{-1}(-\varepsilon, \varepsilon) = \{v' \in V'; |\langle v', v\rangle| < \varepsilon\}$ which is open in the weak topology (and hence the strong, Mackey, and inductive limit topologies) on V'.

Also note that if $\hat{u} = \hat{v}$, then $\langle v', v\rangle = \langle v', u\rangle$ for all $v' \in V'$. Thus $v = u$. Therefore the correspondence $v \to \hat{v}$ is injective.

We now show that the correspondence $v \to \hat{v}$ is surjective. Take $v'' \in V''$, the dual of V'. Then v'' is continuous on V'. Since $V' = \bigcup_{n=1}^{\infty} V_n'$ by Proposition 4.14, we have that $v'' \in V_n''$ for all n. But $V_n = V_n''$ since V_n is a Hilbert space. Thus v'' can be considered as an element of V_n for all n. Since V is a complete we have that $\bigcap_{n=1}^{\infty} V_n = V$ by Proposition 4.9. Thus $v'' \in V$ and we have that $v \to \hat{v}$ is surjective. □

Theorem 4.53. *Let V be a countably–Hilbert space with dual V'. Then the inductive, strong, and Mackey topologies on V' are equivalent (i.e. $\tau_s = \tau_i = \tau_m$).*

Proof. By Lemma 4.51 and Lemma 4.52 we have that V' is Hausdorff and has dual V under the topologies t_s, t_i, and t_m. Thus we can apply Theorem 4.45 to V'. (In the theorem we are taking V' as E and V as E'.) This gives us that t_i and t_s are topologies of uniform convergence on a set of balanced convex weakly–compact subsets of V. However, by definition, the Mackey topology, τ_m, is the finest such topology. Thus $\tau_s \subset \tau_m$ and $\tau_i \subset \tau_m$. However, by Corollary 4.50 we have $\tau_m \subset \tau_s$. Thus $\tau_s = \tau_m$. Likewise, we have $\tau_i \subset \tau_m = \tau_s$; and, by Proposition 4.27 and the definition of the inductive limit topology on V' we have $\tau_s \subset \tau_i$. Therefore $\tau_s = \tau_m = \tau_i$. □

4.7 Borel Field

In this section our aim is to discuss the σ–field on V' generated by the three topologies (strong, weak, and inductive). We will see that under certain conditions the three σ–fields coincide. The standing assumption throughout this section is that V is a countably–Hilbert space with a countable dense subset Q_o. On each $V'_n \subset V'$ define the sets $F_n\big(\frac{1}{k}\big)$ for all k as:

$$F_n\big(\tfrac{1}{k}\big) = \Big\{ v' \in V'_n\,;\ \sup_{v\in Q} |\langle v', \tfrac{v}{|v|_n}\rangle| < \tfrac{1}{k} \Big\}$$

where $Q = Q_o - \{0\}$.

Recall that the local base for the topology of V'_n is given by the sets

$$N_n(\varepsilon) = \{ v' \in V'_n\,;\ |v'|_n < \varepsilon \}$$

where $\varepsilon > 0$.

Lemma 4.54. *In V'_n we have that $F_n\big(\frac{1}{k}\big) = N_n\big(\frac{1}{k}\big)$ for all k.*

Proof. Recall that $|v'|_{-n} = \sup_{v\in V_n-\{0\}} |\langle v', \frac{v}{|v|_n}\rangle|$. It is enough to show that for any $v' \in V'_n$ we have $|v'|_{-n} = \sup_{v\in Q} |\langle v', \frac{v}{|v|_n}\rangle|$. This is quite easy to see: for any non-zero $v \in V_n$ we have a sequence $\{v_l\}_{l=1}^{\infty}$ in Q that converges to v (since Q is dense in V and V is dense in V_n). Thus $\langle v', v\rangle = \lim_{l\to\infty}\langle v', v_l\rangle$. □

Proposition 4.55. *The collection $\{F_n\big(\frac{1}{k}\big)\}_{k=1}^{\infty}$ forms a local base in V'_n. That is, V'_n is first countable.*

Proof. Take an open set $U \subset V'_n$ containing 0. Then $N_n(\varepsilon) \subset U$ for some $\varepsilon > 0$. Choose k so that $\frac{1}{k} < \varepsilon$. Then by Lemma 4.54 we have $F_n\big(\frac{1}{k}\big) = N_n\big(\frac{1}{k}\big) \subset N_n(\varepsilon)$. □

Since each V_n is a separable Hilbert space, so is its dual V'_n. Let Q'_n be a countable dense subset in V'_n.

Proposition 4.56. *The collection* $\{x' + F_n(\frac{1}{k}) \mid x' \in Q'_n\,,\, 1 \le k < \infty\}$ *is a basis for* V'_n. *That is,* V'_n *is second countable.*

Proof. Consider an open set $U \subset V'_n$ and an element v' in U. By Proposition 4.55 there is a k such that $v' + F_n(\frac{1}{k}) \subset U$. Take $x' \in Q'_n$ such that $|x' - v'|_{-n} < \frac{1}{2k}$.

Observe that $x' + F_n(\frac{1}{2k}) \subset v' + F_n(\frac{1}{k})$: Take any $w' \in F_n(\frac{1}{2k})$ and we have

$$\begin{aligned}\sup_{v\in Q} |\langle x' - v' + w', \tfrac{v}{|v|_n}\rangle| &\le |x' - v'|_{-n} + \sup_{v\in Q} |\langle w', \tfrac{v}{|v|_n}\rangle| \\ &< \frac{1}{2k} + \frac{1}{2k} = \frac{1}{k}\end{aligned}$$

This gives us that $x' - v' + F_n(\frac{1}{2k}) \subset F_n(\frac{1}{k})$ or equivalently $x' + F_n(\frac{1}{2k}) \subset v' + F_n(\frac{1}{k})$. Also $v' \in x' + F_n(\frac{1}{2k})$ since $|x' - v'|_{-n} < \frac{1}{2k}$.

In summary we have that $v' \in x' + F_n(\frac{1}{2k}) \subset v' + F_n(\frac{1}{k}) \subset U$. Therefore the collection $\{x' + F_n(\frac{1}{k}) \mid x' \in Q'_n\,,\, 1 \le k < \infty\}$ is basis for V'_n □

Lemma 4.57. *Let* $\sigma(\tau_w)$ *be the Borel* σ*–field on* V' *induced by the weak topology. Then* $F_n(\frac{1}{k})$ *is in* $\sigma(\tau_w)$ *for all positive integers* k *and* n.

Proof. Observe $F_n(\frac{1}{k}) = \{v' \in V'_n\,;\, |v'|_n < \frac{1}{k}\} = \{v' \in V'\,;\, |v'|_{-n} < \frac{1}{k}\}$. (If $v' \in V'$ satisfies $\sup_{v\in Q} |\langle v', \frac{v}{|v|_n}\rangle| < \frac{1}{k}$, then $v' \in V'_n$.)

Now note that $F_n(\frac{1}{k})$ can be expressed as

$$F_n(\tfrac{1}{k}) = \bigcup_{r\in S} \bigcap_{v\in Q'_n} N(\tfrac{v}{|v|_n}; r)$$

where $N(\frac{v}{|v|_n}; r) = \{v' \in V';\, |\langle v', \frac{v}{|v|_n}\rangle| < r\}$ and $S = \{r \in \mathbb{Q}\,;\, 0 < r < \frac{1}{k}\}$. Therefore $F_n(\frac{1}{k})$ can be expressed as the countable intersection of the weakly open sets $N(\frac{v}{|v|_n}; r)$. Hence $F_n(\frac{1}{k})$ is in $\sigma(\tau_w)$. □

Theorem 4.58. *Let* V' *be endowed with a topology* τ. *If* τ *is finer than* τ_w *and the inclusion map* $i'_n : V'_n \to V'$ *is continuous for all* n, *then the* σ*–fields generated by* τ *and* τ_w *are equal. (i.e.* $\sigma(\tau_w) = \sigma(\tau)$*)*

Proof. Let U be a set in τ. Then $U_n = i_n'^{-1}(U)$ is open in V'_n. By Proposition 4.56, U_n can be expressed as $U_n = \bigcup_{l\in T} x'_{n_l} + F_n(\frac{1}{k_l})$ where $x'_{n_l} \in Q'_n$ and T is countable. Then

$$\begin{aligned}U \cap V' &= U \cap \Big(\bigcup_{n=1}^{\infty} V'_n\Big) = \bigcup_{n=1}^{\infty} U \cap V'_n \\ &= \bigcup_{n=1}^{\infty} U_n = \bigcup_{n=1}^{\infty} \bigcup_{l\in T} x'_{n_l} + F_n\Big(\tfrac{1}{k_l}\Big)\end{aligned}$$

Thus U can be expressed as a countable union of sets in $\sigma(\tau_w)$. Hence U is in $\sigma(\tau_w)$. Therefore $\sigma(\tau_w) = \sigma(\tau)$.

□

Corollary 4.59. *The σ–fields generated by the inductive, strong, and weak topologies on V' are equivalent.* (*i.e.* $\sigma(\tau_w) = \sigma(\tau_s) = \sigma(\tau_i)$)

Proof. We can apply Theorem 4.58 since i'_n is continuous with respect to τ_i and τ_s and also both τ_i and τ_s are finer than τ_w. $\square$

The σ–field on V' generated by the weak, strong, or inductive topology is referred to as the *Borel field* on V'.

4.8 A Word on Nuclear Spaces

Let V be a countably–Hilbert space associated with an increasing sequence of inner-product norms $\{|\cdot|_n; n \geq 1\}$. Again let V_n be the completion of V with respect to the norm $|\cdot|_n$.

Definition 4.60. The countably–Hilbert space V is called a *nuclear space* if for any n, there exists $m \geq n$ such that the inclusion map from V_m into V_n is a Hilbert-Schmidt operator (i.e. there is an orthonormal basis $\{e_k\}_{k=1}^{\infty}$ for V_m such that $\sum_{k=1}^{\infty} |e_k|_n^2 < \infty$).

Remark 4.61. Note that a trace class operator is also a Hilbert-Schmidt operator and that the product of two Hilbert-Schmidt operators is a trace class operator. Thus V is a nuclear space if and only if for any n, there exists $m \geq n$ such that the inclusion map from V_m into V_n is a trace class operator.

Proposition 4.62. *Let V be a perfect space. Then V has a countable dense subset* (*i.e. V is separable*).

Proof. Recall $V = \bigcap_{n=1}^{\infty} V_n$. We can divide this into two cases: either each V_n is separable or there exists a k such that V_k is not separable.

In the first scenario, since $V \subset V_1$ and V_1 is separable, we can find a countable set $Q_1 \subset V$ such that Q_1 is dense in V in the norm $|\cdot|_1$. Likewise, we can find $Q_2 \subset V$ that is dense in V with respect to the norm $|\cdot|_2$. Continuing in this manner, we form $Q_n \subset V$ for all $n \in \{1, 2, \ldots\}$. Let $Q = \bigcup_{n=1}^{\infty} Q_n$. We will now show Q is dense in V. Let $v \in V$. For each n we can find a $v_n \in Q_n$ such that $|v - v_n|_n < \frac{1}{n}$. Then for any $k < n$ we have that

$$|v - v_n|_k \leq |v - v_n|_n < \frac{1}{n}$$

Therefore, the sequence $\{v_n\}_{n=1}^{\infty}$ will converge to v in the space V.

In the second case, without loss of generality we can take V_1 to be nonseparable. Using the Axiom of Choice we can find an uncountable set S_1 in V of points bounded in the norm $|\cdot|_1$ with the distance between any two points being larger than a positive constant M. (That is, for $x, y \in S_1$, we have $|x - y|_1 \geq M$.) Likewise, since $V = \bigcup_{n=1}^{\infty} \{v \in V\,;\, |v|_2 \leq n\}$, there is an uncountable set $S_2 \subset S_1$, which is bounded in the norm $|\cdot|_2$. Continuing in this manner, for each n we form an uncountable set

$S_n \subset S_{n-1}$ such that S_n is bounded in the norm $|\cdot|_n$. Note that for any $x, y \in S_n$, we have that

$$|x - y|_n \geq |x - y|_1 \geq M$$

From each S_k take an arbitrary point v_k and form the set $\{v_k\}_{k=1}^{\infty}$. Note that $\{v_k\}_{k=1}^{\infty}$ is bounded in V. However, by construction $\{v_k\}_{k=1}^{\infty}$ cannot contain a Cauchy sequence. Therefore, V cannot be perfect, a contradiction. □

Proposition 4.63. *If V is a nuclear space, then V is perfect.*

Proof. Let B be a bounded set in V. Denote the set B considered as a subset of V_n by B_n. Since B is bounded, each B_n is bounded in V_n. For $m < n$, let $i_{n,m} : V_n \to V_m$ be the inclusion map. Note that $i_{n,m}(B_n) = B_m$. Since V is a nuclear space the image of the bounded set B_n has compact closure in V_m. For $m = 1$, taking a sequence of elements $\{v_k\}_{k=1}^{\infty}$ in B, there is a subsequence $\{v_{k_1}\}_{k_1=1}^{\infty}$ that is Cauchy in the norm $|\cdot|_1$. Taking $m = 2$, we can find subsequence $\{v_{k_2}\}_{k_2=1}^{\infty}$ of $\{v_{k_1}\}_{k_1=1}^{\infty}$ that is Cauchy in the norm $|\cdot|_2$. Continuing in this way and forming the diagonal sequence $\{v_{k_j}\}_{j=1}^{\infty}$ we see that $\{v_{k_j}\}_{j=1}^{\infty}$ is Cauchy in every norm $|\cdot|_k$. Thus $\{v_{k_j}\}_{j=1}^{\infty}$ is Cauchy in V. Since V is complete, this sequence has a limit in V. Thus B is limit point compact. □

Combining the last two propositions, we see that all the results proved throughout this article apply to nuclear spaces. Most importantly, for a nuclear space, the strong and inductive topologies on the dual coincide and the σ–fields generated by the inductive, strong, and weak topologies are equal.

Chapter 5

White Noise Analysis

In this chapter we present an overview of the subject of White Noise Analysis or Infinite Dimensional Distribution Theory. We begin by constructing the infinite dimensional Gaussian measure and formalizing the concepts of test functions and generalized functions. We then highlight some of the major results of the subject.

5.1 Gaussian Measure on the Dual of a Nuclear Space

Let E be a real separable Hilbert space with norm $|\cdot|_0$, and let A be a operator on E. Suppose further that there is an orthonormal basis $\{e_n\}_{n=1}^{\infty}$ on E of eigenvectors of A satisfying

(1) $Ae_n = \lambda_n e_n$

(2) $1 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n \leq \cdots$

(3) $\sum_{n=1}^{\infty} \lambda_n^{-2} < \infty$

Remark 5.1. In the sections to come the reason for having the condition $1 < \lambda_1$ will not be immediately clear. However, let us mention that this condition is important in ensuring that the test functions we develop are continuous (or at least have a continuous version almost everywhere).

Applying conditions (1) and (2) we see that A^{-1} is a bounded operator with operator norm $\|A^{-1}\| = \frac{1}{\lambda_1}$. By condition (3), we see that A^{-1} is also Hilbert–Schmidt on E with

$$\|A^{-1}\|_{HS}^2 = \sum_{n=1}^{\infty} \lambda_n^{-2} < \infty \tag{5.1}$$

From this operator A and the Hilbert space E we proceed to construct a nuclear space.

Using the notation $W = \{0, 1, 2, ...\}$, we have the coordinate map

$$I : E \mapsto \mathbb{R}^W : f \mapsto \big(\langle f, e_n\rangle\big)_{n\in W}$$

Let

$$F_0 = I(E) = \Big\{(x_n)_{n\in W} : \sum_{n\in W} x_n^2 < \infty\Big\} \tag{5.2}$$

Now, for each $p \in W$, let

$$F_p = \Big\{(x_n)_{n\in W} : \sum_{n\in W} \lambda_n^{2p} x_n^2 < \infty\Big\} \tag{5.3}$$

On F_p we have the inner–product $\langle\cdot,\cdot\rangle_p$ given by

$$\langle a, b\rangle_p = \sum_{n\in W} \lambda_n^{2p} a_n b_n$$

This makes F_p a real Hilbert space, unitarily isomorphic to $L^2(W, \nu_p)$ where ν_p is the measure on W specified by $\nu_p(\{n\}) = \lambda_n^{2p}$. Moreover, we have

$$F \stackrel{\text{def}}{=} \cap_{p\in W} F_p \subset \cdots F_2 \subset F_1 \subset F_0 = L^2(W, \nu_0) \tag{5.4}$$

and each inclusion $F_{p+1} \hookrightarrow F_p$ is Hilbert–Schmidt.

Now we pull this back to E. First set

$$\mathcal{E}_p = I^{-1}(F_p) = \Big\{x \in E : \sum_{n\geq 0} \lambda_n^{2p} |\langle x, e_n\rangle|^2 < \infty\Big\} \tag{5.5}$$

It is readily checked that

$$\mathcal{E}_p = A^{-p}(E) \tag{5.6}$$

On $\mathcal{E}_p$ we have the pull back inner-product $\langle\cdot,\cdot\rangle_p$, which works out to be

$$\langle f, g\rangle_p = \langle A^p f, A^p g\rangle \tag{5.7}$$

and that induces a norm $|f|_p = |A^p f|_0$. Then we have the chain

$$\mathcal{E} \stackrel{\text{def}}{=} \cap_{p\in W} \mathcal{E}_p \subset \cdots \mathcal{E}_2 \subset \mathcal{E}_1 \subset E, \tag{5.8}$$

with each inclusion $\mathcal{E}_{p+1} \hookrightarrow \mathcal{E}_p$ being Hilbert–Schmidt.

Equip $\mathcal{E}$ with the topology generated by the norms $\{|\cdot|_p\}_{p=0}^{\infty}$. Then $\mathcal{E}$ is, by definition, a nuclear space. The vectors e_n all lie in $\mathcal{E}$ and the set of all rational–linear combinations of these vectors produces a countable dense subspace of $\mathcal{E}$. Since

$\mathcal{E}$ is a nuclear space, the topological dual $\mathcal{E}'$ is the union of the duals $\mathcal{E}'_p$. In fact, we have:

$$\mathcal{E}' = \cup_{p\in W}\mathcal{E}'_p \supset \cdots \mathcal{E}'_2 \supset \mathcal{E}'_1 \supset E' \simeq E, \tag{5.9}$$

where in the last step we used the usual Hilbert space isomorphism between E and its dual E'.

Going over to the sequence space, $\mathcal{E}'_p$ corresponds to

$$F_{-p} \stackrel{\text{def}}{=} \{(x_n)_{n\in W} : \sum_{n\in W} \lambda_n^{-2p} x_n^2 < \infty\} \tag{5.10}$$

The element $y \in F_{-p}$ corresponds to the linear functional on F_p given by

$$x \mapsto \sum_{n\in W} x_n y_n$$

which, by Cauchy–Schwartz, is well–defined and does define an element of the dual F'_p with norm equal to the square root of $\sum_{n\in W} \lambda_n^{-2p} y_n^2 < \infty$. This gives us the pull back inner–product $\langle\cdot,\cdot\rangle_{-p}$, which works out to

$$\langle f, g\rangle_{-p} = \langle A^{-p} f, A^{-p} g\rangle \tag{5.11}$$

and that induces a norm $|f|_{-p} = |A^{-p} f|_0$.

Combining (5.8) and (5.9) we can get the triple

$$\mathcal{E} \subset E \subset \mathcal{E}'$$

where $\mathcal{E}$ is a nuclear space dense in E relative to the norm $|\cdot|_0$. Such a triple is called a *Gel'fand triple*.

Consider now the product space $\mathbb{R}^W$, along with the coordinate projection maps

$$\hat{X}_j : \mathbb{R}^W \to \mathbb{R} : x \mapsto x_j$$

for each $j \in W$. Equip $\mathbb{R}^W$ with the product σ–algebra, i.e. the smallest σ–algebra with respect to which each projection map $\hat{X}_j$ is measurable. A fundamental result in probability measure theory (a special case of Kolmogorov's theorem, for instance) says that for a given $\sigma > 0$ there is a unique probability measure ν on the product σ–algebra such that each function $\hat{X}_j$, viewed as a random variable, has Gaussian distribution with variance σ. Thus,

$$\int_{\mathbb{R}^W} e^{it\hat{X}_j}\, d\nu = e^{-t^2\sigma^2/2}$$

for $t \in \mathbb{R}$, and every $j \in W$. The measure ν is the product of the Gaussian measure $e^{-x^2/2\sigma^2}(2\pi\sigma^2)^{-1/2}dx$ on each component $\mathbb{R}$ of the product space $\mathbb{R}^W$.

Since, for any $p \geq 1$, we have

$$\int_{\mathbb{R}^W} \sum_{j \in W} \lambda_j^{-2p} x_j^2 \, d\nu(x) = \sum_{j \in W} \lambda_j^{-2p} < \infty,$$

it follows that

$$\nu(F_{-p}) = 1$$

for all $p \geq 1$. Thus $\nu(F') = 1$.

We can, therefore, transfer the measure ν back to $\mathcal{E}'$, obtaining a probability measure μ_σ on the σ–algebra of subsets of $\mathcal{E}'$ generated by the maps

$$\hat{e}_j : \mathcal{E}' \to \mathbb{R} : f \mapsto f(e_j),$$

where $\{e_j\}_{j \in W}$ is the orthonormal basis of E we started with (note that each e_j lies in $\mathcal{E} = \bigcap_{p \geq 0} \mathcal{E}_p$). This is clearly the σ–algebra generated by the weak topology on $\mathcal{E}'$, which, by Corollary 4.59, is equal to the σ–algebras generated by the strong or inductive–limit topologies.

The above discussion gives a simple direct description of the measure μ_σ.

To summarize, we are at the starting point of much of infinite–dimensional distribution theory (white noise analysis): Given a real, separable Hilbert space E and an operator A on E, we have constructed a nuclear space $\mathcal{E}$ and a unique probability measure μ_σ on the Borel σ–algebra of the dual $\mathcal{E}'$ such that there is a linear map

$$E \to L^2(\mathcal{E}', \mu) : \xi \mapsto \hat{\xi},$$

satisfying

$$\int_{\mathcal{E}'} e^{it\hat{\xi}(x)} \, d\mu_\sigma(x) = e^{-t^2\sigma^2|\xi|_0^2/2}$$

for every real t and $\xi \in E$. The measure $\mu = \mu_1$ is often called the (*standard*) *Gaussian measure* or the *white noise measure* and is the principal measure used white–noise analysis. Also the probability space $(\mathcal{E}', \mu)$ is called the *white–noise space*.

Remark 5.2. The existence of the Gaussian measure μ_σ is also obtainable by applying the Minlos Theorem (see Theorem 7.1). In this setting, we have

$$\int_{\mathcal{E}'} e^{i\langle x, \xi \rangle} \, d\mu_\sigma(x) = \int_{\mathcal{E}'} e^{i\hat{\xi}(x)} \, d\mu_\sigma(x) = e^{-|\xi|_0^2\sigma^2/2}$$

for any $\xi \in \mathcal{E}$.

5.1.1 Properties of the Gaussian Measure

Here we present some standard results about the Gaussian measure μ defined on the dual of a nuclear space.

Notation. For a real vector space V, we denote the complexification of V by V_c, where as usual $V_c = \{v_1 + iv_2\,;\, v_1, v_2 \in V\}$. In particular, the complexification of the nuclear space $\mathcal{E}$ and its dual $\mathcal{E}'$ is denoted by $\mathcal{E}_c$ and $\mathcal{E}'_c$, respectively. Moreover, the bilinear pairing $\langle\cdot,\cdot\rangle$ between $\mathcal{E}$ and $\mathcal{E}'$ extends to a bilinear pairing $\langle\cdot,\cdot\rangle_c$ between $\mathcal{E}_c$ and $\mathcal{E}'_c$ where

$$\langle x_1 + ix_2, \xi_1 + i\xi_2\rangle_c = \langle x_1, \xi_1\rangle - \langle x_2, \xi_2\rangle + i(\langle x_1, \xi_2\rangle + \langle x_2, \xi_1\rangle)$$

for $x_1, x_2 \in \mathcal{E}'$ and $\xi_1, \xi_2 \in \mathcal{E}$. Also, for $\xi = \xi_1 + i\xi_2 \in E_c$ we have the norm $|\cdot|_0$ on E extends to E_c by

$$|\xi|_0^2 = |\xi_1|_0^2 + |\xi_2|_0^2$$

Lemma 5.3. *Let $\xi_1, \xi_2, \ldots, \xi_n \in \mathcal{E}$ be an orthonormal system for E. Then the image of the Gaussian measure μ under the map*

$$x \mapsto (\langle x, \xi_1\rangle, \cdots, \langle x, \xi_n\rangle) \in \mathbb{R}^n, \qquad x \in \mathcal{E}'$$

is the standard Gaussian measure on $\mathbb{R}^n$ (i.e. the probability measure with distribution function $(2\pi)^{-n/2}e^{-|t|^2/2}$). That is $\hat{\xi_1}, \hat{\xi_2}, \ldots, \hat{\xi_n}$ are independent identically distributed standard Gaussian random variables.

Proof. Let ν denote the image of μ under the above map. So ν is a probability measure on $\mathbb{R}^n$. Computing the characteristic function of ν we see

$$\begin{aligned}
\hat{\nu}(s) = \int_{\mathbb{R}^n} e^{i\langle s,t\rangle} d\nu(t) &= \int_{\mathcal{E}'} \exp\Big(i\sum_{k=1}^n s_k\langle x, \xi_k\rangle\Big) d\mu(x) \\
&= \exp\Big(-\tfrac{1}{2}\Big|\sum_{k=1}^n s_k\xi_k\Big|_0^2\Big) \\
&= \exp\Big(-\tfrac{1}{2}\sum_{i,j=1}^n s_i s_j\langle \xi_i, \xi_j\rangle\Big) \\
&= \exp\big(-\tfrac{1}{2}|s|^2\big)
\end{aligned}$$

which is the characteristic function of the standard Gaussian measure on $\mathbb{R}^n$. $\square$

Lemma 5.4. *Let $\xi_1, \xi_2, \ldots, \xi_n \in \mathcal{E}$ be an orthonormal system for E. For any Gaussian integrable functions $f_1, f_2, \ldots, f_n$ on $\mathbb{R}$ we have*

$$\int_{\mathcal{E}'} f_1(\langle x, \xi_1\rangle) \ldots f_n(\langle x, \xi_n\rangle)\, d\mu(x) = \prod_{k=1}^n \int_{\mathcal{E}'} f_k(\langle x, \xi_k\rangle)\, d\mu(x)$$

Proof. Apply Lemma 5.3. $\square$

Lemma 5.5. *For any $\xi \in \mathcal{E}_c$ and $n = 0, 1, 2, \ldots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}'} |\langle x, \xi\rangle_c|^2\, d\mu(x) = |\xi|_0^2$

(b) $\displaystyle\int_{\mathcal{E}'} \langle x, \xi\rangle_c^{2n}\, d\mu(x) = \frac{(2n)!}{2^n n!}\langle \xi, \xi\rangle_c^n$

(c) $\displaystyle\int_{\mathcal{E}'} \langle x, \xi\rangle_c^{2n+1}\, d\mu(x) = 0$

(d) $\displaystyle\int_{\mathcal{E}'} e^{\langle x, \xi\rangle_c}\, d\mu(x) = e^{\langle \xi, \xi\rangle_c/2}$

Proof. The identities obviously hold when $\xi = 0$. So we take $\xi \in \mathcal{E}$ with $\xi \neq 0$. By Lemma 5.3 we have that

$$\int_{\mathcal{E}'} |\langle x, \xi\rangle|^2\, d\mu(x) = |\xi|_0^2 \int_{\mathcal{E}'} \Big|\Big\langle x, \frac{\xi}{|\xi|_0}\Big\rangle\Big|^2 d\mu(x) = \frac{|\xi|_0^2}{\sqrt{2\pi}} \int_{\mathbb{R}} t^2 e^{-\frac{t^2}{2}} dt = |\xi|_0^2$$

Thus we have the first identity for $\xi \in \mathcal{E}$. Using this, we take $\xi = \xi_1 + i\xi_2 \in \mathcal{E}_c$ and observe that

$$\int_{\mathcal{E}'} |\langle x, \xi\rangle_c|^2\, d\mu(x) = \int_{\mathcal{E}'} \left(\langle x, \xi_1\rangle^2 + \langle x, \xi_2\rangle^2\right)\, d\mu(x) = |\xi_1|_0^2 + |\xi_2|_0^2 = |\xi|_0^2$$

which proves the first identity. The second and third identity can be proved by a similar argument.

For the last identity we again write $\xi = \xi_1 + i\xi_2$ where $\xi_1, \xi_2 \in \mathcal{E}$. Now use the orthogonal decomposition $\xi_2 = \xi_2' + \langle \xi_2, \frac{\xi_1}{|\xi_1|_0^2}\rangle \xi_1$ along with Lemma 5.4 to see that

$$\int_{\mathcal{E}'} e^{\langle x, \xi_1 + i\xi_2\rangle_c}\, d\mu(x) = e^{\langle \xi_1 + i\xi_2, \xi_1 + i\xi_2\rangle_c/2}$$

To prove identities (b) and (c) one can use an argument similar to that which we used to prove (a). We can also use the indentity in (d) to prove (b) and (c). Let t be a real number. Substituting $t\xi$ for ξ in (d) we have $\int_{\mathcal{E}'} e^{\langle x, t\xi\rangle_c}\, d\mu(x) = e^{\langle t\xi, t\xi\rangle_c/2}$. We can expand $e^{\langle t\xi, t\xi\rangle_c/2}$ and $e^{\langle x, t\xi\rangle_c}$ as follows:

$$e^{\langle x, t\xi\rangle_c} = \sum_{k=0}^{\infty} \frac{t^k}{k!}\langle x, \xi\rangle_c^k \qquad\qquad e^{\langle t\xi, t\xi\rangle_c/2} = \sum_{n=0}^{\infty} \frac{t^{2n}}{2^n n!}\langle \xi, \xi\rangle_c^n$$

Thus (d) becomes

$$\int_{\mathcal{E}'} \sum_{k=0}^{\infty} \frac{t^k}{k!}\langle x, \xi\rangle_c^k\, d\mu(x) = \sum_{n=0}^{\infty} \frac{t^{2n}}{2^n n!}\langle \xi, \xi\rangle_c^n$$

and after interchanging the integral with the sum we get

$$\sum_{k=0}^{\infty} \frac{t^k}{k!} \int_{\mathcal{E}'} \langle x, \xi\rangle_c^k\, d\mu(x) = \sum_{n=0}^{\infty} \frac{t^{2n}}{2^n n!}\langle \xi, \xi\rangle_c^n$$

Taking $t = 1$ and comparing terms in the power series expansions we see that for $k = 2n$ we get

$$\frac{1}{(2n)!}\int_{\mathcal{E}'} \langle x, \xi\rangle^k \, d\mu(x) = \frac{1}{2^n n!}\langle \xi, \xi\rangle_c^n$$

and for $k = 2n + 1$ we get

$$\frac{1}{(2n)!}\int_{\mathcal{E}'} \langle x, \xi\rangle^k \, d\mu(x) = 0$$

which proves (b) and (c). □

We can now define $\langle \cdot, \xi\rangle_c$ for any $\xi \in E_c$ as a μ–almost everywhere defined function of $x \in \mathcal{E}'$ in $L^2(\mathcal{E}', \mu)$, the space of all functions $f : \mathcal{E}' \to \mathbb{C}$ which are L^2 integrable with respect to μ. Take a sequence $\{\xi_n\}_{n=1}^{\infty}$ in $\mathcal{E}_c$ such that $\lim_{n\to\infty} |\xi - \xi_n|_0 = 0$. Using Lemma 5.5 we can see that the functions $\{\langle \cdot, \xi_n\rangle_c\}_{n=1}^{\infty}$ form a Cauchy sequence in $L^2(\mathcal{E}', \mu)$. Thus there exists a $\phi \in L^2(\mathcal{E}', \mu)$ such that $\lim_{n\to\infty}\langle \cdot, \xi_n\rangle_c = \phi$. We denote such a ϕ by $\langle \cdot, \xi\rangle_c$.

Proposition 5.6. *For any $\xi \in E_c$ and $n = 0, 1, 2, \ldots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}'} |\langle x, \xi\rangle_c|^2 \, d\mu(x) = |\xi|_0^2$

(b) $\displaystyle\int_{\mathcal{E}'} \langle x, \xi\rangle_c^{2n} \, d\mu(x) = \frac{(2n)!}{2^n n!}\langle \xi, \xi\rangle_c^n$

(c) $\displaystyle\int_{\mathcal{E}'} \langle x, \xi\rangle_c^{2n+1} \, d\mu(x) = 0$

(d) $\displaystyle\int_{\mathcal{E}'} e^{\langle x,\xi\rangle_c} \, d\mu(x) = e^{\langle \xi,\xi\rangle_c/2}$

Proof. It is easily shown that Lemmas 5.3 and 5.4 are true when $\xi_1, \xi_2, \ldots, \xi_n$ are in E. Using this, we can mimic the proof of Lemma 5.5 to get the identities. □

Proposition 5.7. *Let $\xi, \eta \in E_c$, Then*

$$\int_{\mathcal{E}'} \langle x, \xi\rangle_c \langle x, \eta\rangle_c \, d\mu(x) = \langle \xi, \eta\rangle_c$$

Proof. First take $\xi, \eta \in E$. If $\xi = 0$, the identity holds trivially, so assume $\xi \neq 0$ and let $\eta_\xi = \langle \eta, \frac{\xi}{|\xi|_0^2}\rangle \xi$ be the orthogonal projection of η onto ξ. Then

$$\begin{aligned}\int_{\mathcal{E}'} \langle x, \xi\rangle \langle x, \eta\rangle \, d\mu(x) &= \int_{\mathcal{E}'} \langle x, \xi\rangle \langle x, \eta - \eta_\xi + \eta_\xi\rangle \, d\mu(x) \\ &= \int_{\mathcal{E}'} \langle x, \xi\rangle \langle x, \eta - \eta_\xi\rangle \, d\mu(x) + \int_{\mathcal{E}'} \langle x, \xi\rangle \langle x, \eta_\xi\rangle \, d\mu(x)\end{aligned}$$

Since ξ and $\eta - \eta_\xi$ are orthogonal we can apply Lemma 5.4 and Proposition 5.6 to see that $\int_{\mathcal{E}'} \langle x, \xi\rangle\langle x, \eta - \eta_\xi\rangle \, d\mu(x) = 0$. Using that $\eta_\xi = \langle \eta, \frac{\xi}{|\xi|_0^2}\rangle \xi$ we have

$$\int_{\mathcal{E}'} \langle x, \xi\rangle\langle x, \eta_\xi\rangle \, d\mu(x) = \frac{\langle \eta, \xi\rangle}{|\xi|_0^2} \int_{\mathcal{E}'} \langle x, \xi\rangle\langle x, \xi\rangle \, d\mu(x) = \langle \eta, \xi\rangle$$

where the last equality was derived using Proposition 5.6.

To get the identity for $\xi, \eta \in E_c$ simply write $\xi = \xi_1 + i\xi_2$ and $\eta = \eta_1 + i\eta_2$ where $\xi_1, \xi_2, \eta_1, \eta_2 \in E$. Then expand and multiply $\langle x, \xi\rangle_c \langle x, \eta\rangle_c$ accordingly. □

5.2 Construction of Test Functions and Generalized Functions

5.2.1 Terminology and Notation

Let X be a nuclear space or a Hilbert space. For $\xi_1, \xi_2, \ldots, \xi_n \in X$ we define the *symmetrization* of $\xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n$ to be

$$\xi_1 \widehat{\otimes} \xi_2 \widehat{\otimes} \cdots \widehat{\otimes} \xi_n = \frac{1}{n!} \sum_{\sigma \in S_n} \xi_{\sigma(1)} \otimes \xi_{\sigma(2)} \otimes \cdots \otimes \xi_{\sigma(n)} \tag{5.12}$$

where S_n is the group of permutations of $\{1, 2, \ldots, n\}$. We define the set $X^{\widehat{\otimes} n}$ to be the closed subspace of $X^{\otimes n}$ spanned by $\xi_1 \widehat{\otimes} \xi_2 \widehat{\otimes} \cdots \widehat{\otimes} \xi_n$ where $\xi_1, \xi_2, \ldots, \xi_n$ run over X.

For an $F \in (X^{\otimes n})'$ and $\sigma \in S_n$ we define F^σ to be the element in $(X^{\otimes n})'$ uniquely determined by

$$\langle F^\sigma, \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n\rangle = \langle F, \xi_{\sigma(1)} \otimes \xi_{\sigma(2)} \otimes \cdots \otimes \xi_{\sigma(n)}\rangle, \qquad \xi_1, \cdots, \xi_n \in X$$

For $F \in (X^{\otimes n})'$ we define the *symmetrization* $\widehat{F}$ of F by

$$\widehat{F} = \frac{1}{n!} \sum_{\sigma \in S_n} F^\sigma \tag{5.13}$$

If $F = \widehat{F}$, we say that F is *symmetric*. Let $(X^{\otimes n})'_\sigma$ denote the subspace of $(X^{\otimes n})'$ consisting of symmetric elements. Since

$$(f_1 \otimes \cdots \otimes f_n)\widehat{\ } = f_1 \widehat{\otimes} \cdots \widehat{\otimes} f_n, \qquad f_1, \cdots, f_n \in X'$$

the defintions in equations (5.12) and (5.13) are consistent. For $F \in (X^{\otimes m})'$ and $G \in (X^{\otimes n})'$ we denote the symmetrization of $F \otimes G$ by $F \widehat{\otimes} G$. Also note that $(X^{\otimes n})' \cong X'^{\otimes n}$. This is clear when X is a Hilbert space and it is also true when X is a nuclear space (see Theorem 1.3.10 in [25]). Therefore, we have $(X^{\otimes n})'_\sigma \cong X'^{\widehat{\otimes} n}$, and this is the notation we will use throughout this work.

5.2.2 Construction

We denote the space of all sequences $\mathbf{f} = (f_n)_{n=0}^{\infty}$ with $f_n \in E^{\widehat{\otimes} n}$ and $\sum_{n=0}^{\infty} n!|f_n|_0^2 < \infty$ by $\Gamma(E)$. (Here $|\cdot|_0$ denotes the norm on $E^{\widehat{\otimes} n}$ induced by the norm on E.) Then $\Gamma(E)$ is a Hilbert space with norm

$$\|\mathbf{f}\|_{\Gamma(E)}^2 = \sum_{n=0}^{\infty} n!|f_n|_0^2 < \infty$$

and inner–product

$$\langle\langle \mathbf{f}, \mathbf{g} \rangle\rangle_{\Gamma(E)} = \sum_{n=0}^{\infty} n!\langle f, g \rangle_0$$

It is typically called the *Fock space* or *symmetric Hilbert space* over E. The Fock space $\Gamma(E_c)$ can be defined similarly.

Having developed the Gaussian measure μ on the space $\mathcal{E}'$, we form the real Hilbert space $L^2(\mathcal{E}', \mu)$. We denote the norm on $L^2(\mathcal{E}', \mu)$ by $\|\cdot\|_0$. It turns out that by using the multiple Wiener–Itô integral

$$I_n : E_c^{\widehat{\otimes} n} \to L^2(\mathcal{E}', \mu),$$

$L^2(\mathcal{E}', \mu)$ is canonically ismorphic to $\Gamma(E_c)$.

Theorem 5.8 (Wiener–Itô)**.** *Each $\phi \in L^2(\mathcal{E}', \mu)$ can be uniquely expressed as*

$$\phi = \sum_{n=0}^{\infty} I_n(f_n) \tag{5.14}$$

where $(f_n)_{n=0}^{\infty} \in \Gamma(E_c)$. Conversely, for any $(f_n)_{n=0}^{\infty} \in \Gamma(E_c)$ we have that (5.14) *defines a function in $L^2(\mathcal{E}', \mu)$. Moreover,*

$$\|\phi\|_0^2 = \sum_{n=0}^{\infty} n!|f_n|_0^2$$

For a proof refer to Obata's book [25]. The map which identifies $\phi \in L^2(\mathcal{E}', \mu)$ with its corresponding $(f_n)_{n=0}^{\infty} \in \Gamma(E_c)$ is call the Wiener–Itô isomorphism and is uniquely specified by

$$I : L^2(\mathcal{E}', \mu) \to \Gamma(E_c) : \sum_{n=0}^{\infty} \frac{x^{\otimes n}}{n!} \mapsto e^{\hat{x} - \frac{1}{2}|x|_0^2}$$

Remark 5.9. We will not delve too deeply into the theory of Wiener integrals, as much of this theory will not be needed for our later work. We just mention that the multiple Wiener integral I_n can be defined as the linear functional on $E_c^{\widehat{\otimes} n}$ such that for any $n_1 + n_2 + \cdots = n$, we have

$$\boxed{I_n(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots) = H_{n_1}(\langle \cdot, e_1 \rangle) H_{n_2}(\langle \cdot, e_2 \rangle) \cdots ,} \tag{5.15}$$

where $H_n = (-1)e^{x^2/2} D_x^n e^{-x^2/2}$ is the Hermite polynomial of degree n.

Using the operator A on E we form a densely defined operator $\Gamma(A)$ on $L^2(\mathcal{E}', \mu)$. If $\phi = \sum_{n=0}^{\infty} I_n(f_n)$, then

$$\Gamma(A)\phi = \sum_{n=0}^{\infty} I_n(A^{\otimes n} f_n)$$

The operator $\Gamma(A)$ has the same properties as A. To see this let

$$\phi_{n_1,n_2,\ldots} \equiv \frac{1}{\sqrt{n_1! n_2! \ldots}} I_n(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots), \qquad n_1 + n_2 + \cdots = n \tag{5.16}$$

Then the collection $\{\phi_{n_1,n_2,\ldots}\,;\, n_1+n_2+\cdots = n,\ n = 0, 1, 2 \ldots\}$ forms an orthonormal basis for $L^2(\mathcal{E}', \mu)$ and

$$\Gamma(A)\phi_{n_1,n_2,\ldots} = (\lambda_1^{n_1} \lambda_2^{n_2} \cdots)\phi_{n_1,n_2,\ldots}$$

Therefore conditions (2) and (3) from Section 5.1 can be checked to hold for the operator $\Gamma(A)$ on $L^2(\mathcal{E}', \mu)$. In fact $\Gamma(A)^{-1}$ is a Hilbert–Schmidt operator with

$$\|\Gamma(A)^{-1}\|_{HS}^2 = \Big(\prod_{n=1}^{\infty}(1 - \lambda_j^{-2})\Big)^{-1}$$

Now we can apply the same method used in Section 5.1 to construct a Gel'fand triple with $\Gamma(A)$ and $L^2(\mathcal{E}', \mu)$. For each integer $p \geq 0$, define

$$\|\phi\|_p = \|\Gamma(A)^p \phi\|_0$$

and let

$$(\mathcal{E}_p) = \{\phi \in L^2(\mathcal{E}', \mu)\,;\, \|\phi\|_p < \infty\}$$

With this definition it is clear that $(\mathcal{E}_q) \subset (\mathcal{E}_p)$ when $q \leq p$ and the inclusion map from $(\mathcal{E}_{p+1})$ to $(\mathcal{E}_p)$ is a Hilbert–Schmidt operator. Now we can form the nuclear space

$$(\mathcal{E}) = \bigcap_{p=0}^{\infty} (\mathcal{E}_p)$$

with topology given by the norms $\{\|\cdot\|_p\}_{p=0}^{\infty}$. Likewise, we form the dual $(\mathcal{E})'$ of $(\mathcal{E})$, which is equal to $\bigcup_{p=1}^{\infty} (\mathcal{E}'_p)$, where the norm on $(\mathcal{E}'_p)$ is easily checked to be

$$\|\phi\|_{-p} = \|\Gamma(A)^{-p}\phi\|_0$$

Therefore, we have formed the Gel'fand triple

$$(\mathcal{E}) \subset L^2(\mathcal{E}', \mu) \subset (\mathcal{E})'$$

where $(\mathcal{E})$ is called the space of *test function* and $(\mathcal{E})'$ is called the space of *generalized functions* (or *Hida distributions*). Also, we denote the natural bilinear pairing between $(\mathcal{E})$ and $(\mathcal{E})'$ by $\langle\langle \cdot, \cdot \rangle\rangle$.

5.3 Wick Tensors

The *trace operator* τ plays a very important role in White Noise Analysis. The trace operator is in $(\mathcal{E}_c')^{\widehat{\otimes}2}$ and is defined by

$$\langle \tau, \xi \otimes \eta \rangle_c = \langle \xi, \eta \rangle_c \qquad \xi, \eta \in \mathcal{E}_c$$

It can be represented by

$$\sum_{k=1}^{\infty} e_k \otimes e_k$$

where $\{e_k\}_{k=1}^{\infty}$ are the eigenvectors of the operator A and form an orthonormal basis for E. To see that τ is in $(\mathcal{E}_c')^{\widehat{\otimes}2}$, observe that for any integer $p > 0$ we have:

$$\begin{aligned} |\tau|_{-p}^2 &= \sum_{k=1}^{\infty} |(A^{-p})^{\otimes 2}(e_k \otimes e_k)|_0^2 \\ &= \sum_{k=1}^{\infty} |A^{-p} e_k|_0^4 \\ &= \sum_{k=1}^{\infty} \lambda_k^{-4p} \\ &\leq \sum_{k=1}^{\infty} \lambda_k^{-2} \end{aligned}$$

and the last sum is finite by (5.1).

5.3.1 Hermite Polynomials

We now review some concepts and properties concerning Hermite polynomials. The function defined by

$$:x^n:_{\sigma^2} \equiv H_n^{\sigma}(x) = (-\sigma^2)^n e^{\frac{x^2}{2\sigma^2}} D_x^n e^{-\frac{x^2}{2\sigma^2}}$$

is the *Hermite polynomial* of degree n with parameter σ^2. They can also be defined by the generating function:

$$e^{tx - \frac{1}{2}\sigma^2 t^2} = \sum_{n=0}^{\infty} \frac{t^n}{n!} :x^n:_{\sigma^2} \tag{5.17}$$

Using this one can derive that

$$\frac{1}{\sqrt{2\pi\sigma^2}} \int_{\mathbb{R}} H_n^{\sigma}(x)\, H_m^{\sigma}(x)\, e^{-x^2/2\sigma^2} dx = (\sigma^{2n}) n! \delta_{mn} \tag{5.18}$$

where δ_{mn} is 1 if $m = n$ and 0 otherwise.

We have the following formulas for Hermite polynomials

$$:x^n:_{\sigma^2} = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-\sigma^2)^k x^{n-2k} \tag{5.19}$$

$$x^n = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!\,\sigma^{2k} :x^{n-2k}:_{\sigma^2} \tag{5.20}$$

5.3.2 Definition

The formula given in (5.19) provides the motivation for the following definition:

Definition 5.10. Given an element $x \in \mathcal{E}'$, we define the *Wick tensor for x of order n* to be

$$:x^{\otimes n}: = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-1)^k x^{\otimes(n-2k)} \widehat{\otimes} \tau^{\otimes k}$$

For example, if $x \in \mathcal{E}_{-p}$, then $:x^{\otimes n}:$ is in $\mathcal{E}_{-p}$.

Remark 5.11. For an element $x \in \mathcal{E}'$, we can also define $:x^{\otimes n}:$ inductively as follows:

$$\begin{cases} :x^{\otimes 0}: = 1 \\ :x^{\otimes 1}: = x \\ :x^{\otimes n}: = x \widehat{\otimes} :x^{\otimes(n-1)}: -(n-1)\tau \widehat{\otimes} :x^{\otimes(n-2)}: \qquad \text{for } n \geq 2 \end{cases}$$

Similar to the formula in (5.20) for the Hermite polynomials, we have the following formula for Wick tensors:

$$x^{\otimes n} = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!! :x^{\otimes(n-2k)}: \widehat{\otimes} \tau^{\otimes k}$$

Proposition 5.12. *For any $x \in \mathcal{E}'$ and $\xi \in \mathcal{E}$ we have*

$$\langle :x^{\otimes n}:, \xi^{\otimes n} \rangle = :\langle x, \xi \rangle^n:_{|\xi|_0^2} \qquad \textit{and} \qquad \| \langle :x^{\otimes n}:, \xi^{\otimes n} \rangle \|_0 = \sqrt{n!}|\xi|_0^n$$

Remark 5.13. In the second equality, $\langle :x^{\otimes n}:, \xi^{\otimes n} \rangle$ is viewed as a function of $x \in \mathcal{E}'$ and norm $\| \cdot \|_0$ is from $L^2(\mathcal{E}', \mu)$

Proof. First we use the definition $:x^{\otimes n}:$ to see that

$$\langle :x^{\otimes n}:, \xi^{\otimes n} \rangle = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-|\xi|_0^2)^k \langle x, \xi \rangle^{n-2k} \tag{5.21}$$

Comparing this with (5.19) we have $\langle :x^{\otimes n}:, \xi^{\otimes n}\rangle =: \langle x, \xi\rangle^n :_{|\xi|_0^2}$

For the second equality, we use equation (5.19) and observe that for $\xi \neq 0$

$$\begin{aligned}
:\langle x, \xi\rangle^n:_{|\xi|_0^2} &= \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-|\xi|_0^2)^k \langle x, \xi\rangle^{n-2k} \\
&= |\xi|_0^n \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-1)^k \langle x, \tfrac{\xi}{|\xi|_0}\rangle^{n-2k} \\
&= |\xi|_0^n :\langle x, \tfrac{\xi}{|\xi|_0}\rangle^n:
\end{aligned}$$

Now we can apply Lemma 5.3 and (5.18) to see that

$$\|\langle :x^{\otimes n}:, \xi^{\otimes n}\rangle\|_0^2 = \frac{|\xi|_0^{2n}}{\sqrt{2\pi}} \int_{\mathbb{R}} :x^n:_1 :x^n:_1 \, e^{-x^2/2}\, dx = n!|\xi|_0^{2n}$$

which gives us the desired equality. $\square$

Corollary 5.14. *Let $\xi_1, \xi_2, \cdots \in \mathcal{E}$ be orthogonal vectors in E. Then for any $x \in \mathcal{E}'$ we have*

$$\langle :x^{\otimes n}:, \xi_1^{\otimes n_1} \widehat{\otimes}\, \xi_2^{\otimes n_2} \widehat{\otimes} \cdots\rangle =: \langle x, \xi_1\rangle^{n_1}:_{|\xi_1|_0^2} : \langle x, \xi_2\rangle^{n_2}:_{|\xi_2|_0^2} \cdots$$

where $n_1 + n_2 + \cdots = n$. Moreover, the following holds

$$\|\langle :\cdot^{\otimes n}:, \xi_1^{\otimes n_1} \widehat{\otimes}\, \xi_2^{\otimes n_1} \widehat{\otimes} \cdots\rangle\|_0 = \sqrt{n_1!n_2!\cdots}|\xi_1|_0^{n_1}|\xi_2|_0^{n_2}\cdots$$

Proof. The first identity can be derived from the defintion of Wick tensor, much like as in Proposition 5.12. For the second identity we can combine the first identity with Lemma 5.4 to get

$$\|\langle :\cdot^{\otimes n}:, \xi_1^{\otimes n_1} \widehat{\otimes}\, \xi_2^{\otimes n_1} \widehat{\otimes} \cdots\rangle\|_0^2 = \| :\langle x, \xi_1\rangle^{n_1}:_{|\xi_1|_0^2} \|_0^2 \cdot \| :\langle x, \xi_2\rangle^{n_2}:_{|\xi_2|_0^2} \|_0^2 \cdots$$

We can now use Proposition 5.12 to arrive at

$$\|\langle :\cdot^{\otimes n}:, \xi_1^{\otimes n_1} \widehat{\otimes}\, \xi_2^{\otimes n_1} \widehat{\otimes} \cdots\rangle\|_0 = \sqrt{n_1!n_2!\cdots}|\xi_1|_0^{n_1}|\xi_2|_0^{n_2}\cdots$$

$\square$

By Corollary 5.14 one can see that if $g \in \mathcal{E}^{\widehat{\otimes} n}$, then

$$\|\langle :\cdot^{\otimes n}:, g\rangle\|_0 = \sqrt{n!}|g|_0$$

Using this, we take a function $f \in E^{\widehat{\otimes} n}$ and a sequence $\{g_k\}$ in $\mathcal{E}^{\widehat{\otimes} n}$ with $g_k \to f$ in $E^{\widehat{\otimes} n}$. Then, by the equality above, $\{\langle :\cdot^{\otimes n}:, g_k\rangle\}$ is Cauchy in $L^2(\mathcal{E}', \mu)$. Therefore we can define the function $\langle :\cdot^{\otimes n}:, f\rangle$ μ–almost everywhere as the limit in $L^2(\mathcal{E}', \mu)$ of the functions $\{\langle :\cdot^{\otimes n}:, g_k\rangle\}$. Defined in this way we have

$$\|\langle :\cdot^{\otimes n}:, f\rangle\|_0 = \sqrt{n!}|f|_0 \tag{5.22}$$

Of course, for $f = f_1 + if_2 \in E_c^{\widehat{\otimes} n}$ we can define for almost every $x \in \mathcal{E}'$,

$$\langle : \cdot^{\otimes n} :, f \rangle_c = \langle : \cdot^{\otimes n} :, f_1 \rangle + i \langle : \cdot^{\otimes n} :, f_2 \rangle$$

and equation (5.22) still holds.

Corollary 5.15. *Let $\xi_1, \xi_2, \cdots \in E$ be orthogonal vectors in E. Then for almost every $x \in \mathcal{E}'$ we have*

$$\langle : x^{\otimes n} :, \xi_1^{\otimes n_1} \widehat{\otimes} \xi_2^{\otimes n_2} \widehat{\otimes} \cdots \rangle =: \langle x, \xi_1 \rangle^{n_1} :_{|\xi_1|_0^2} : \langle x, \xi_2 \rangle^{n_2} :_{|\xi_2|_0^2} \cdots$$

where $n_1 + n_2 + \cdots = n$.

Proof. It suffices to show that for any $\xi \in E$ we have

$$\langle : x^{\otimes n} :, \xi^{\otimes n} \rangle =: \langle x, \xi \rangle^n :_{|\xi|_0^2}$$

for almost all $x \in \mathcal{E}'$. Take a sequence $\{\xi_k\}$ in $\mathcal{E}$ of non–zero elements such that $\xi_k \to \xi$ in E. Replacing $\{\xi_k\}$ with $\{|\xi|_0 \frac{\xi_k}{|\xi_k|_0}\}$, we can assume that $|\xi_k|_0 = |\xi|_0$ for all k. Then by Proposition 5.12 we have that

$$\begin{aligned} \langle : x^{\otimes n} :, \xi^{\otimes n} \rangle &= \lim_{k \to \infty} \langle : x^{\otimes n} :, \xi_k^{\otimes n} \rangle \\ &= \lim_{k \to \infty} : \langle x, \xi_k \rangle^n :_{|\xi|_0^2} \\ &= \lim_{k \to \infty} : \langle x, \xi \rangle^n :_{|\xi|_0^2} \end{aligned}$$

□

5.3.3 Relationship to Multiple Wiener Integrals

The next theorem gives an explicit relationship between the multiple Wiener integrals I_n introduced in section 5.2 and the Wick tensors of elements in $\mathcal{E}'$.

Theorem 5.16. *For any $f \in E_c^{\widehat{\otimes} n}$ we have that*

$$I_n(f)(x) = \langle : x^{\otimes n} :, f \rangle_c$$

holds for almost all $x \in \mathcal{E}'$

Proof. Recalling that $H_n^1(x) =: x^n :_1$, we can use equation (5.15) and Corollary 5.14 to see that

$$I_n(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots)(x) = \langle : x^{\otimes n} :, e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots \rangle$$

holds for the orthonormal basis elements $\{e_k\}$. Therefore the equality holds for any $f \in \mathcal{E}_c^{\widehat{\otimes} n}$. Using that $\mathcal{E}_c^{\widehat{\otimes} n}$ is dense in $E_c^{\widehat{\otimes} n}$, we have that $I_n(f)(x) = \langle : x^{\otimes n} :, f \rangle$ for any $f \in E_c^{\widehat{\otimes} n}$. □

Combining Theorems 5.8 and 5.16 we have that any element $\phi \in L^2(\mathcal{E}', \mu)$ can expressed in terms of Wick tensors as

$$\phi(x) = \sum_{n=0}^{\infty} I_n(f_n)(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, f_n \rangle_c, \qquad \mu\text{–a.e. for } x \in \mathcal{E}' \tag{5.23}$$

where $f_n \in E_c^{\widehat{\otimes} n}$. Moreover, for any positive integer p we have

$$\|\phi\|_p^2 = \|\Gamma(A)^p \phi\|_0^2 = \sum_{n=0}^{\infty} n! |f_n|_p^2 \tag{5.24}$$

where $|f_n|_p = |(A^p)^{\otimes n} f_n|_0$ for $f_n \in E_c^{\widehat{\otimes} n}$. This implies that if $\phi \in (\mathcal{E}_p)$, then $f_n \in \mathcal{E}_{p,c}^{\widehat{\otimes} n}$ for all n.

Conversely, it is easy to see that given any $\mathbf{f} = (f_n)_{n=0}^{\infty} \in \Gamma(\mathcal{E}_{p,c})$, we have that equation (5.23) defines a unique function ϕ in $(\mathcal{E}_p)$.

The expression in (5.23) is called the *Wiener–Itô expansion* for ϕ. This type of representation can be extended to functions Φ in $(\mathcal{E})'$.

Theorem 5.17. *Given a $\Phi \in (\mathcal{E}_p')$, there exists a unique element $\mathbf{F} = (F_n)_{n=0}^{\infty} \in \Gamma(\mathcal{E}_{p,c}')$ such that*

$$\langle\langle \Phi, \phi \rangle\rangle = \sum_{n=0}^{\infty} n! \langle F_n, f_n \rangle_c \qquad \text{for all } \phi \in (\mathcal{E}_p) \tag{5.25}$$

where $\phi(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, f_n \rangle$ μ–a.e. Conversely, given a sequence $\mathbf{F} = (F_n)_{n=0}^{\infty} \in \Gamma(\mathcal{E}_{p,c}')$ we can define a $\Phi \in (\mathcal{E}_p')$ by (5.25). Moreover, we have that

$$\|\Phi\|_{-p}^2 = \|\Gamma(A)^{-p} \Phi\|_0^2 = \sum_{n=0}^{\infty} n! |F_n|_{-p}^2 = \|\mathbf{F}\|_{\Gamma(\mathcal{E}_{p,c}')}^2 \tag{5.26}$$

Proof. Take an arbitrary $f \in \mathcal{E}_{p,c}^{\otimes n}$ and let S_n denote the group of permutations of the set $\{1, 2, \cdots, n\}$. For each $\sigma \in S_n$ let f^σ be the element in $\mathcal{E}_{p,c}^{\otimes n}$ uniquely determined by

$$\langle f^\sigma, \xi_1 \otimes \cdots \otimes \xi_n \rangle_c = \langle f, \xi_{\sigma^{-1}(1)} \otimes \cdots \otimes \xi_{\sigma^{-1}(n)} \rangle_c$$

and define the symmetrization of f by

$$\hat{f} = \frac{1}{n!} \sum_{\sigma \in S_n} f^\sigma$$

Obviously, $\hat{f}$ is in $\mathcal{E}_{p,c}^{\widehat{\otimes} n}$. Therefore, by Theorem 5.16 and the discussion that follows, we have $\langle :x^{\otimes n}:, \hat{f} \rangle_c \in (\mathcal{E}_p)$. So we let

$$\phi_f(x) = \langle :x^{\otimes n}:, \hat{f} \rangle_c$$

The linear functional given by

$$f \mapsto \langle\langle \Phi, \phi_f \rangle\rangle \qquad f \in \mathcal{E}_{p,c}^{\otimes n}$$

is continuous since

$$|\langle\langle \Phi, \phi_f \rangle\rangle| \leq \|\Phi\|_{-p} \|\phi_f\|_p = \sqrt{n!}\|\Phi\|_{-p} |\hat{f}|_p \leq \sqrt{n!}\|\Phi\|_{-p} |f|_p$$

Thus, there exists $F_n \in \mathcal{E}_{p,c}^{\prime \otimes n}$ such that

$$\langle\langle \Phi, \phi_f \rangle\rangle = n! \langle F_n, f \rangle_c$$

Observe that since $\phi_f = \phi_{\hat{f}}$, we have $\langle F_n, f \rangle_c = \langle F_n, \hat{f} \rangle_c$ for all $f \in \mathcal{E}_{p,c}^{\otimes n}$. Therefore $F_n \in \mathcal{E}_{p,c}^{\prime \widehat{\otimes} n}$. Doing this for all $n = 0, 1, 2 \ldots$ gives us a $\mathbf{F} \in \Gamma(\mathcal{E}'_{p,c})$ such that (5.25) holds. The converse is easily verified.

To prove (5.26) we let $\mathbf{n} = (n_1, n_2, \cdots)$ with $|\mathbf{n}| = n_1 + n_2 + \cdots = n$ and consider the functions given by

$$\phi_{\mathbf{n}}(x) = \frac{1}{\sqrt{n_1! n_2! \cdots}} \langle :x^{\otimes n}:, e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots \rangle$$

These functions form a complete orthonormal basis of $L^2(\mathcal{E}', \mu)$ by (5.16) and Theorem 5.16. Therefore

$$\begin{aligned} \|\Phi\|_{-p}^2 &= \|\Gamma(A)^{-p}\Phi\|_0^2 \\ &= \sum_{n=1}^{\infty} \sum_{|\mathbf{n}|=n} \langle\langle \Gamma(A)^{-p}\Phi, \phi_n \rangle\rangle^2 \\ &= \sum_{n=1}^{\infty} \sum_{|\mathbf{n}|=n} \langle\langle \Phi, \Gamma(A)^{-p}\phi_n \rangle\rangle^2 \end{aligned}$$

Now observe that

$$\Gamma(A)^{-p}\phi_{\mathbf{n}}(x) = \frac{1}{\sqrt{n_1! n_2! \cdots}} \langle :x^{\otimes n}:, (A^{\otimes n})^{-p}(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots) \rangle_c$$

So we can apply (5.25) to see that

$$\langle\langle \Phi, \Gamma(A)^{-p}\phi_{\mathbf{n}} \rangle\rangle = \frac{n!}{\sqrt{n_1! n_2! \cdots}} \langle F_n, (A^{\otimes n})^{-p}(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots) \rangle_c$$

Therefore we have that

$$\begin{aligned}
\|\Phi\|_{-p}^2 &= \sum_{n=1}^{\infty} n! \sum_{|\mathbf{n}|=n} \frac{n!}{\sqrt{n_1! n_2! \cdots}} \left|\langle F_n, (A^{\otimes n})^{-p}(e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots)\rangle_c\right|^2 \\
&= \sum_{n=1}^{\infty} n! \sum_{|\mathbf{n}|=n} \left|\langle (A^{\otimes n})^{-p} F_n, \sqrt{\tfrac{n!}{n_1! n_2! \cdots}} (e_1^{\otimes n_1} \widehat{\otimes} e_2^{\otimes n_2} \widehat{\otimes} \cdots)\rangle_c\right|^2 \\
&= \sum_{n=1}^{\infty} n! |(A^{\otimes n})^{-p} F_n|_0^2 \\
&= \sum_{n=1}^{\infty} n! |F_n|_{-p}^2
\end{aligned}$$

which gives us (5.26). □

Using the previous theorem we can adopt a formal expression for $\Phi \in (\mathcal{E})'$ as follows:

$$\Phi(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, F_n\rangle_c \tag{5.27}$$

Here $\langle :x^{\otimes n}:, F_n\rangle_c$ is not a functions of $x \in \mathcal{E}'$, but a generalized function. It can only be understood through the pairing with a test function in $(\mathcal{E})$. The expression given by (5.27) is called the *Wiener–Itô expansion* of Φ.

5.4 S–transform

In this section we introduce a fundamental tool in White Noise Analysis. We begin by defining a special type of exponential function in $L^2(\mathcal{E}', \mu)$.

Definition 5.18. For any $\xi \in E_c$ we define the function $:e^{\langle \cdot, \xi\rangle_c}:$ in $L^2(\mathcal{E}', \mu)$ by the Wiener–Itô expansion

$$:e^{\langle \cdot, \xi\rangle_c}: = \sum_{n=0}^{\infty} \frac{1}{n!} \langle :x^{\otimes n}:, \xi^{\otimes n}\rangle_c$$

The following verifies that the right side is convergent in $L^2(\mathcal{E}', \mu)$.

Lemma 5.19. *For $\xi, \eta \in E_c$ we have that*

$$\langle\langle :e^{\langle \cdot, \xi\rangle_c}:, :e^{\langle \cdot, \eta\rangle_c}:\rangle\rangle = e^{\langle \xi, \eta\rangle_c} \qquad \text{and} \qquad \|:e^{\langle \cdot, \xi\rangle_c}:\|_0 = e^{|\xi|_0^2/2}$$

(i.e. $:e^{\langle \cdot, \xi\rangle_c}: \in L^2(\mathcal{E}', \mu)$ whenever $\xi \in E_c$)

Proof. Using the definition given above we have

$$\langle\langle :e^{\langle\cdot,\xi\rangle_c}:, :e^{\langle\cdot,\eta\rangle_c}:\rangle\rangle = \sum_{n=0}^{\infty} \frac{n!}{(n!)^2}\langle \xi^{\otimes n}, \eta^{\otimes n}\rangle_c = \sum_{n=0}^{\infty} \frac{1}{n!}\langle \xi, \eta\rangle_c^n = e^{\langle \xi,\eta\rangle_c}$$

This gives us the first identity. Using $\overline{:e^{\langle\cdot,\xi\rangle_c}:} = :e^{\langle\cdot,\bar{\xi}\rangle_c}:$ we can get the second identity. □

Lemma 5.20. *The function* $:e^{\langle\cdot,\xi\rangle_c}:$ *is in* $(\mathcal{E}_p)$ *if and only if* $\xi \in (\mathcal{E}_p)$*. For such a function we have*

$$\| :e^{\langle\cdot,\xi\rangle_c}: \|_p = \exp(\tfrac{1}{2}|\xi|_p^2)$$

Proof. For the given p we have

$$\| :e^{\langle\cdot,\xi\rangle_c}: \|_p^2 = \sum_{n=0}^{\infty} \frac{n!}{(n!)^2}|\xi^{\otimes n}|_p^2 = \sum_{n=0}^{\infty} \frac{1}{n!}|\xi|_p^{2n} = e^{|\xi|_p^2}$$

□

Corollary 5.21. *The function* $:e^{\langle\cdot,\xi\rangle_c}:$ *is in* $(\mathcal{E})$ *if and only if* $\xi \in \mathcal{E}_c$*.*

Proposition 5.22. *For any* $\xi \in E$ *we have* $:e^{\langle x,\xi\rangle}:= e^{\langle x,\xi\rangle - \langle \xi,\xi\rangle/2}$*.*

Proof. For $\xi = 0$ the assertion is obvious. So we take $\xi \neq 0$ and apply Corollary 5.15 to see that

$$:e^{\langle x,\xi\rangle}: = \sum_{n=0}^{\infty} \frac{1}{n!}\langle :x^{\otimes n}:, \xi^{\otimes n}\rangle = \sum_{n=0}^{\infty} \frac{1}{n!} :\langle x,\xi\rangle^n:_{|\xi|_0^2}$$

The last sum is the generating series for the Hermite polynomials with parameter $|\xi|_0^2$ (see equation (5.17)). Therefore $:e^{\langle x,\xi\rangle_c}:= e^{\langle x,\xi\rangle - \langle \xi,\xi\rangle/2}$. □

Definition 5.23. The *S–transform* of a function $\Phi \in (\mathcal{E})'$ is defined to be the function on $\mathcal{E}_c$ given by

$$S\Phi(\xi) = \langle\langle \Phi, :e^{\langle\cdot,\xi\rangle_c}:\rangle\rangle, \qquad \xi \in \mathcal{E}_c$$

Proposition 5.24. *If* $\Phi \in (\mathcal{E})'$ *has Wiener–Itô expansion given by* $\Phi = \sum_{n=0}^{\infty}\langle :x^{\otimes n}:, F_n\rangle_c$*, then the S–transform of* Φ *is given by*

$$S\Phi(\xi) = \sum_{n=0}^{\infty}\langle F_n, \xi^{\otimes n}\rangle_c \qquad \textit{for all } \xi \in \mathcal{E}_c$$

Proof. Apply Definition 5.23 and Theorem 5.17. □

The S–transform is one of the most important tools used in the study of White Noise Analysis. As we will see, many properties of a generalized function can be deduced from its S–transform. The next theorem justifies the importance of this map.

Theorem 5.25. *Let Φ, Ψ be arbitrary functions in $(\mathcal{E})'$. If $S\Phi = S\Psi$, then $\Phi = \Psi$.*

Proof. It is sufficient to show that $S\Phi = 0$ implies $\Phi = 0$. Suppose Φ has Wiener–Itô expansion given by $\Phi = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, F_n \rangle_c$. Then by Proposition 5.24 the S–transform of Φ is given by

$$S\Phi(\xi) = \sum_{n=0}^{\infty} \langle F_n, \xi^{\otimes n} \rangle_c, \qquad \xi \in \mathcal{E}$$

Since $S\Phi = 0$, we have for any real t

$$S\Phi(t\xi) = \sum_{n=0}^{\infty} t^n \langle F_n, \xi^{\otimes n} \rangle_c = 0$$

Therefore $F_0 = 0$ and $\langle F_n, \xi^{\otimes n} \rangle_c = 0$ for all $\xi \in \mathcal{E}$. Since F_n is a symmetric n–linear map we can apply the polarization identity to see that

$$\langle F, \xi_1 \widehat{\otimes} \cdots \widehat{\otimes} \xi_n \rangle_c = \frac{1}{n!} \sum_{k=1}^{n} (-1)^{n-k} \sum_{j_1 < \cdots < j_k} \langle F_n, (\xi_{j_1} + \cdots \xi_{j_k})^{\otimes n} \rangle_c = 0$$

So $F_n = 0$ for all $n \geq 0$. Hence $\Phi = 0$. $\square$

In the course of proving the above theorem we have shown:

Corollary 5.26. *The linear span of the set $\{:e^{\langle \cdot, \xi \rangle}: ; \xi \in \mathcal{E}\}$ (or $\{:e^{\langle \cdot, \xi \rangle_c}: ; \xi \in \mathcal{E}_c\}$) is dense in $(\mathcal{E})$.*

Proof. For any $\phi \in (\mathcal{E}_p)$, if $\langle\langle \phi, :e^{\langle \cdot, \xi \rangle}: \rangle\rangle = 0$ for all $\xi \in \mathcal{E}$, then $\phi = 0$ by Theorem 5.25. Hence the orthogonal complement of the closed linear space of $\{:e^{\langle \cdot, \xi \rangle}: ; \xi \in \mathcal{E}\}$ is $\{0\}$ in $(\mathcal{E}_p)$. Since p is arbitrary, $\{:e^{\langle \cdot, \xi \rangle}: ; \xi \in \mathcal{E}\}$ is dense in $(\mathcal{E}_p)$ for all p. Recall that the topology on $(\mathcal{E})$ is induced by the topologies on each $(\mathcal{E}_p)$. Hence $\{ :e^{\langle \cdot, \xi \rangle}: ; \xi \in \mathcal{E}\}$ is dense in $(\mathcal{E})$. $\square$

We can now extend Proposition 5.22 to the case where $\xi \in E_c$.

Proposition 5.27. *For any $\xi \in E_c$ we have $:e^{\langle x, \xi \rangle_c}: = e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle_c / 2}$.*

Proof. Let $\xi \in E_c$. It follows from Lemma 5.19 that

$$S(:e^{\langle \cdot, \xi \rangle_c}:)(\eta) = e^{\langle \xi, \eta \rangle_c}$$

Now consider the $L^2(\mathcal{E}', \mu)$ function $e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle_c / 2}$. Taking the S–transform with $\eta \in E$ we have

$$\begin{aligned} S(e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle_c / 2})(\eta) &= \langle\langle e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle_c / 2}, :e^{\langle \cdot, \eta \rangle_c}: \rangle\rangle \\ &= \int_{\mathcal{E}'} e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle_c / 2} e^{\langle x, \eta \rangle - \langle \eta, \eta \rangle / 2} \, d\mu(x) \qquad \text{by Proposition 5.22} \\ &= e^{-\langle \xi, \xi \rangle_c / 2 - \langle \eta, \eta \rangle_c / 2} e^{\langle \xi + \eta, \xi + \eta \rangle_c / 2} \qquad \text{by Lemma 5.5} \\ &= e^{\langle \xi, \eta \rangle_c} \end{aligned}$$

So we have shown that

$$\langle\langle e^{\langle x,\xi\rangle_c - \langle \xi,\xi\rangle_c/2}, :e^{\langle\cdot,\eta\rangle_c}:\rangle\rangle = S(e^{\langle x,\xi\rangle_c - \langle \xi,\xi\rangle_c/2})(\eta) = S(:e^{\langle\cdot,\xi\rangle_c}:)(\eta) = \langle\langle :e^{\langle\cdot,\xi\rangle_c}:, :e^{\langle\cdot,\eta\rangle_c}:\rangle\rangle$$

for all $\eta \in \mathcal{E}$. Therefore by Corollary 5.26 we have that $:e^{\langle\cdot,\xi\rangle_c}:= e^{\langle x,\xi\rangle_c - \langle \xi,\xi\rangle_c/2}$. $\square$

5.4.1 Renormalized Exponential Functions

Using the S–transform we can extend Definition 5.18 slightly to include vectors $y \in \mathcal{E}'_c$.

Definition 5.28. For any $y \in \mathcal{E}'_c$ we define the function $:e^{\langle\cdot,y\rangle_c}:$ in $(\mathcal{E})'$ by the Wiener–Itô expansion

$$:e^{\langle\cdot,y\rangle_c}:= \sum_{n=0}^{\infty} \frac{1}{n!} \langle :x^{\otimes n}:, y^{\otimes n}\rangle_c$$

This definition coincides with that of Definition 5.18 if $y \in E_c$. We now show that $:e^{\langle\cdot,y\rangle_c}:$ is indeed a generalized function.

Theorem 5.29. *For $y \in \mathcal{E}'_c$ we have $:e^{\langle\cdot,y\rangle_c}: \in (\mathcal{E})'$ with S–transform given by*

$$S(:e^{\langle\cdot,y\rangle_c}:)(\xi) = e^{\langle y,\xi\rangle_c}, \qquad \xi \in \mathcal{E}'_c$$

Moreover, if $y \in \mathcal{E}'_{p,c}$, then $:e^{\langle\cdot,y\rangle_c}: \in (\mathcal{E}'_p)$ with

$$\| :e^{\langle\cdot,y\rangle_c}: \|_{-p} = e^{|y|^2_{-p}/2}$$

Proof. Since $\mathcal{E}'_c = \bigcup_{p=0}^{\infty} \mathcal{E}'_{p,c}$, there exist some $p \geq 0$ for which $|y|_{-p} < \infty$. For such a p, we have

$$\| :e^{\langle\cdot,y\rangle_c}: \|^2_{-p} = \sum_{n=0}^{\infty} n! \frac{1}{(n!)^2} |y^{\otimes n}|^2_{-p} = \sum_{n=0}^{\infty} \frac{1}{n!} |y|^{2n}_{-p} = e^{|y|^2_{-p}}$$

Hence we have $:e^{\langle\cdot,y\rangle_c}: \in (\mathcal{E}'_p)$.

To compute the S–transform we use Definition 5.28 and Proposition 5.24 to see that

$$S(:e^{\langle\cdot,y\rangle_c}:)(\xi) = \sum_{n=0}^{\infty} n! \frac{1}{(n!)^2} \langle y^{\otimes n}, \xi^{\otimes n}\rangle_c = \sum_{n=0}^{\infty} \frac{1}{n!} \langle y,\xi\rangle^n_c = e^{\langle y,\xi\rangle_c}$$

$\square$

5.4.2 Characterization and Convergence Theorems

One of the most important applications of the S–transform is the ability to characterize test and generalized functions through their respective S–transforms. These characterizations are summarized in the following two theorems, which we present without proof.

Theorem 5.30. *Let F be a complex valued function on $\mathcal{E}_c$. Then $F = S\Phi$ for some $\Phi \in (\mathcal{E})'$ if and only if*

(a) *for fixed $\xi, \eta \in \mathcal{E}_c$, the function $F(z\xi + \eta)$ is an entire function of $z \in \mathbb{C}$*

(b) *there exists nonnegative constants K, a, and p such that*

$$|F(\xi)| \leq K \exp[a|\xi|_p^2], \qquad \text{for all } \xi \in \mathcal{E}_c$$

Moreover, for any q satisfying $2ae^2\|A^{-(q-p)}\|_{HS} < 1$ we have the following

$$\|\Phi\|_{-q} \leq K(1 - 2ae^2\|A^{-(q-p)}\|_{HS})^{-1/2}$$

For a proof see page 65, Theorem 3.6.1 in [25] or page 79, Theorem 8.2 in [17].

Theorem 5.31. *Let F be a complex valued function on $\mathcal{E}_c$. Then $F = S\Phi$ for some $\Phi \in (\mathcal{E})$ if and only if*

(a) *for fixed $\xi, \eta \in \mathcal{E}_c$, the function $F(z\xi + \eta)$ is an entire function of $z \in \mathbb{C}$*

(b) *for any constants $a > 0$ and $p \geq 0$, there exists a $K > 0$ such that*

$$|F(\xi)| \leq K \exp[a|\xi|_p^2], \qquad \text{for all } \xi \in \mathcal{E}_c$$

For a proof see page 65, Theorem 3.6.2 in [25] or page 89, Theorem 8.9 in [17].

Having that generalized (and test) functions can be characterized by their S–transform, we observe that convergence of generalized functions can also be deduced in terms of the S–transform.

Theorem 5.32. *Let $\{\Phi_n\}_{n=0}^{\infty}$ be a sequence in $(\mathcal{E})'$ and let $F_n = S\Phi_n$. Then Φ_n converges strongly to Φ in $(\mathcal{E})'$ if and only if*

(a) *For each $\xi \in \mathcal{E}_c$, $\lim_{n\to\infty} F_n(\xi) = F(\xi)$, where $F(\xi) = S(\Phi)(\xi)$.*

(b) *There exists nonnegative constants K, a, and p (independent of n) such that*

$$|F_n(\xi)| \leq K \exp[a|\xi|_p^2], \qquad \text{for all } \xi \in \mathcal{E}_c \text{ and } n \in \mathbb{N}$$

Proof. Suppose Φ_n converges strongly to Φ in $(\mathcal{E})'$. Then for any $\xi \in \mathcal{E}_c$,

$$\begin{aligned}
\lim_{n\to\infty} F_n(\xi) &= \lim_{n\to\infty} \langle\langle \Phi_n, :e^{\langle \cdot, \xi\rangle_c}: \rangle\rangle \\
&= \langle\langle \Phi, :e^{\langle \cdot, \xi\rangle_c}: \rangle\rangle \\
&= F(\xi)
\end{aligned}$$

Also, since Φ_n converges strongly to Φ, the sequence $\{\Phi_n\}_{n=0}^{\infty}$ is strongly bounded in $(\mathcal{E})'$. Therefore, by Theorem 4.31, there is a positive integer p and a constant $K > 0$ such that $\sup_n \|\Phi_n\|_{-p} < K$. Hence

$$|F_n(\xi)| = |\langle\langle \Phi_n, :e^{\langle \cdot, \xi\rangle_c}: \rangle\rangle| \leq \|\Phi_n\|_{-p} \| :e^{\langle \cdot, \xi\rangle_c}: \|_p \leq K \exp\left(\tfrac{1}{2}|\xi|_p^2\right)$$

Therefore condition (b) is satisfied.

To see that the converse holds, let $\Phi_n \in (\mathcal{E})'$ and assume that $F_n = S\Phi_n$ satisfies conditions (a) and (b). By condition (a) we have that

$$\lim_{n\to\infty} F_n(\xi) = F(\xi)$$

exist for each $\xi \in \mathcal{E}_c$. We would like to apply Theorem 5.30 to see F is the S–transform of a generalized function. To show that $F(z\xi + \eta)$ is entire for any $\xi, \eta \in \mathcal{E}_c$, we can use conditions (a) and (b) to and observe that for any closed contour C in $\mathbb{C}$

$$\int_C F(z\xi+\eta)\,dz = \int_C \lim_{n\to\infty} F_n(z\xi+\eta)\,dz = \lim_{n\to\infty}\int_C F_n(z\xi+\eta)\,dz = 0$$

where the last equality uses Morera's theorem (since $F_n(z\xi+\eta)$ is entire). Thus we can apply Morera's theorem to $F(z\xi+\eta)$ to say that it is entire. Moreover, using conditions (a) and (b) it is easy to see that

$$|F(\xi)| \leq K \exp[a|\xi|_p^2]$$

for all $\xi \in \mathcal{E}_c$. Thus, we can apply Theorem 5.30 to show that there exists a unique $\Phi \in (\mathcal{E})'$ such that $F = S\Phi$.

Now we have left to show that Φ_n converges strongly to Φ. First of all, condition (a) gives us that

$$\langle\langle \Phi, :e^{\langle\cdot,\xi\rangle_c}:\rangle\rangle = \lim_{n\to\infty}\langle\langle \Phi_n, :e^{\langle\cdot,\xi\rangle_c}:\rangle\rangle$$

for all $\xi \in \mathcal{E}_c$. So for any ϕ in the linear span of $\{:e^{\langle\cdot,\xi\rangle_c}:;\, \xi \in \mathcal{E}_c\}$ we have

$$\langle\langle \Phi, \phi\rangle\rangle = \lim_{n\to\infty}\langle\langle \Phi_n, \phi\rangle\rangle$$

Thus for any $\phi \in (\mathcal{E})$ we apply Corollary 5.26 to find a sequence $\{\phi_k\}_{k=0}^{\infty}$ in the linear span of $\{:e^{\langle\cdot,\xi\rangle_c}:;\, \xi \in \mathcal{E}_c\}$ with $\phi_k \to \phi$ in $(\mathcal{E})$. We then write $\langle\langle \Phi, \phi\rangle\rangle - \langle\langle \Phi_n, \phi\rangle\rangle$ as

$$\begin{aligned}&\langle\langle \Phi, \phi\rangle\rangle - \langle\langle \Phi_n, \phi\rangle\rangle = \\ &\qquad (\langle\langle \Phi, \phi\rangle\rangle - \langle\langle \Phi, \phi_k\rangle\rangle) + (\langle\langle \Phi, \phi_k\rangle\rangle - \langle\langle \Phi_n, \phi_k\rangle\rangle) + (\langle\langle \Phi_n, \phi_k\rangle\rangle - \langle\langle \Phi_n, \phi\rangle\rangle)\end{aligned}$$

to see that

$$\langle\langle \Phi, \phi\rangle\rangle = \lim_{n\to\infty}\langle\langle \Phi_n, \phi\rangle\rangle$$

for all $\phi \in (\mathcal{E})$. Hence Φ_n converges weakly to Φ. Therefore, by Theorem 4.40, we have ϕ_n converges strongly to Φ in $(\mathcal{E})'$. $\square$

5.4.3 Fourier Transform

The S–transform can also be used to define a Fourier transform on the space of generalized functions $(\mathcal{E})'$. In the finite dimensional setting the Fourier transform can be written as

$$\begin{aligned}\mathcal{F}(f)(y) &= (2\pi)^{-n/2}\int_{\mathbb{R}^n} e^{-i\langle x,y\rangle+|x|^2/2} f(x)e^{-|x|^2/2}\,dx\\ &= \int_{\mathbb{R}^n} e^{-i\langle x,y\rangle+|x|^2/2} f(x)\,d\mu_n(x)\end{aligned}$$

where μ_n is the standard Gaussian measure on $\mathbb{R}^n$. We would like to define the Fourier transform of a generalized function $\Phi \in (\mathcal{E})'$ in an analogous manner. Namely as,

$$\mathcal{F}\Phi(y) = \int_{\mathcal{E}'} :e^{-i\langle x,y\rangle}: \Phi(x)\,d\mu(x)$$

However, this is a purely symbolic integral. But, if we informally take the S–transform of $\mathcal{F}\Phi$ we get

$$S(\mathcal{F}\Phi)(\xi) = \int_{\mathcal{E}'} e^{-i\langle x,\xi\rangle_c}\Phi(x)\,d\mu(x) = \langle\langle \Phi, e^{-i\langle x,\xi\rangle_c}\rangle\rangle$$

for $\xi \in \mathcal{E}_c$. It is easily verified that

$$\langle\langle \Phi, e^{-i\langle \cdot,\xi\rangle_c}\rangle\rangle = S(\Phi)(-i\xi)e^{-\langle\xi,\xi\rangle_c/2} \tag{5.28}$$

For a generalized function $\Phi \in (\mathcal{E})'$, the function given by (5.28) satisfies conditions (a) and (b) of Theorem 5.30. Therefore there is a unique element $\Psi \in (\mathcal{E})'$ with S–transform given by (5.28). With this in mind we define the Fourier transform of generalized function as follows:

Definition 5.33. The *Fourier transform* of a generalized function $\Phi \in (\mathcal{E})'$ is the unique element $\mathcal{F}\Phi$ in $(\mathcal{E})'$ with S–transform given by

$$S(\mathcal{F}\Phi)(\xi) = \langle\langle \Phi, e^{-i\langle \cdot,\xi\rangle_c}\rangle\rangle = S(\Phi)(-i\xi)e^{-\langle\xi,\xi\rangle_c/2}$$

It turns out that defined in this way the Fourier transform is a continuous linear operator from $(\mathcal{E})'$ into itself. (For a proof, see page 141 in [25] or page 152 in [17].)

5.5 Delta Functions

The White Noise analogue of the finite dimensional Dirac's delta function is the Kubo–Yokoi delta function, $\tilde{\delta}_x$. We would like $\tilde{\delta}_x$ to have the following effect on a test function $\phi \in (\mathcal{E})$:

$$\langle\langle \tilde{\delta}_x, \phi\rangle\rangle = \phi(x)$$

However, in order to do this we need $\phi(x)$ to be continuous. Luckily we have the following theorem:

Theorem 5.34. *For every test function $\phi \in (\mathcal{E})$ there exist a unique continuous function $\widehat{\phi}$ such that $\phi(x) = \widehat{\phi}(x)$ for μ–almost every $x \in \mathcal{E}'$. Moreover, $\widehat{\phi}$ is given by*

$$\widehat{\phi}(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, f_n \rangle,$$

the Wiener–Itô expansion for ϕ.

For a proof of this theorem refer to page 38 in [25] or page 52 in [17].

Remark 5.35. By assuming continuous versions of test functions we can pointwise multiply two functions $\phi, \psi \in (\mathcal{E})$. It turns out this operation is continuous (see Theorem 8.18 on page 98 in [17]).

Thanks to the previous theorem we can now define $\tilde{\delta}_x$ as follows:

Definition 5.36. The *Kubo–Yokoi delta function at* x is defined to be the generalized function $\tilde{\delta}_x$ such that

$$\langle\langle \tilde{\delta}_x, \phi \rangle\rangle = \phi(x)$$

for each $\phi \in (\mathcal{E})$.

To see that Kubo–Yokoi delta function at x is in $(\mathcal{E})'$ we take the S–transform of $\tilde{\delta}_x$

$$S(\tilde{\delta}_x)(\xi) = \langle\langle \tilde{\delta}_x, :e^{\langle \cdot, \xi \rangle_c}: \rangle\rangle = e^{\langle x, \xi \rangle_c - \langle \xi, \xi \rangle / 2} \tag{5.29}$$

Clearly, this function satisfies conditions (a) and (b) of Theorem 5.30. So $\tilde{\delta}_x$ is in fact a generalized function. We now derive the Wiener–Itô expansion of $\tilde{\delta}_x$.

Theorem 5.37. *The Wiener–Itô expansion of the Kubo–Yokoi delta function at x is given by*

$$\tilde{\delta}_x = \sum_{n=0}^{\infty} \frac{1}{n!} \langle :\cdot^{\otimes n}:, :x^{\otimes n}: \rangle$$

Proof. By Theorem 5.17, $\tilde{\delta}_x$ has Wiener–Itô expansion given by

$$\tilde{\delta}_x = \sum_{n=0}^{\infty} \langle :\cdot^{\otimes n}:, F_n \rangle_c \tag{5.30}$$

where $F_n \in \mathcal{E}'^{\otimes n}_{p,c}$. For each n consider the function given by $\phi_f = \langle :\cdot^{\otimes n}:, f \rangle_c$ where $f \in \mathcal{E}_c^{\widehat{\otimes} n}$. By the definition of $\tilde{\delta}_x$ we have that

$$\langle\langle \tilde{\delta}_x, \phi_f \rangle\rangle = \phi_f(x) = \langle :x^{\otimes n}:, f \rangle_c \tag{5.31}$$

But, by using (5.30), we have

$$\langle\langle \tilde{\delta}_x, \phi_f \rangle\rangle = n! \langle F_n, f \rangle_c \tag{5.32}$$

Combining equations (5.31) and (5.32) we see that $n!\langle F_n, f \rangle_c = \langle :x^{\otimes n}:, f \rangle_c$ for all $f \in \mathcal{E}_c^{\widehat{\otimes} n}$. Therefore $F_n = \frac{1}{n!} :x^{\otimes n}:$ and we have the Wiener–Itô expansion for $\tilde{\delta}_x$ promised by the theorem. □

5.5.1 Donsker's Delta Function

Another delta function often used in White Noise Analysis is Donsker's delta function. It is defined using the specific Gel'fand triple $\mathcal{S}(\mathbb{R}) \subset L^2(\mathbb{R}) \subset \mathcal{S}'(\mathbb{R})$. Let δ_a be the Dirac delta function at a and note that

$$t \mapsto B(t) \stackrel{\text{def}}{=} \langle \cdot, 1_{[0,t]} \rangle$$

is a Brownian motion. The generalized function $\delta_a(B(t))$ is *Donsker's delta function.* To see that it is in fact an element of $(S)'$ we need the following theorem:

Theorem 5.38. *Let $F \in S_c'(\mathbb{R})$ and $f \in L^2(\mathbb{R})$ with $f \neq 0$. Then $F(\langle \cdot, f \rangle)$ is a generalized function and has S–transform given by*

$$SF(\langle \cdot, f \rangle)(\xi) = \frac{1}{\sqrt{2\pi}|f|_0} \int_{\mathbb{R}} F(y) \exp\left[-\frac{1}{2|f|_0^2} (y - \langle f, \xi \rangle)^2 \right] dy, \qquad \xi \in S_c(\mathbb{R})$$

where the integral is understood to be the bilinear pairing of $S_c'(\mathbb{R})$ and $S_c(\mathbb{R})$.

For a proof refer to [16] or page 63 in [17].

Using this theorem, we can see that $\delta_a(B(t))$ is in fact a generalized function. Moreover, we have the S–transform of $\delta_a(B(t))$ is given by

$$\begin{aligned} S[\delta_a(B(t))](\xi) &= \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} \delta_a(y) e^{-\frac{1}{2t}(y - \langle B(t), \xi \rangle_c)^2} \, dy \\ &= \frac{1}{\sqrt{2\pi t}} \exp\Big[-\frac{1}{2t}\Big(a - \int_0^t \xi(u)\, du \Big)^2 \Big] \end{aligned}$$

Chapter 6

The Delta Function of a Subspace

Let E be a real Hilbert space with V a subspace of E. We want to make sense of the identities

$$\delta_V(x) = \int_V \delta(x-v)\, Dv = \int_{V^\perp} e^{2\pi i \langle x,u\rangle}\, Du \tag{6.1}$$

where Dv and Du are the (nonexistent) Lebesgue measure on the subspace V and $V^\perp$ of E. This identity was first introduced in equation (3.12)—it is a fundamental component of the Hidden Subspace Algorithm. The finite dimensional verison of this equality can be found in [13]. (It is in the proof of Theorem 7.1.25.)

6.1 Motivation

To motivate our definition of the delta function of a subspace we formally demonstrate that the the equalities in (6.1) hold in the distributional sense. We also formally show that the S–transform of each of the terms agree.

6.1.1 Formal Calculations

Let f be a function on E. We will show that when any of the terms in (6.1) are integrated against f, we arrive at the same result. Thus we say the equalities in (6.1) hold in the distributional sense. Observe:

(1) Essentially by the "definition" of δ_V we have

$$\int_E \delta_V(x) f(x) Dx = \int_V f(v) Dv$$

(2) Now for $\int_V \delta(x-v)Dv$ we calculate

$$\int_E \int_V \delta(x-v)Dv\, f(x)\, Dx = \int_V \int_E \delta(x-v) f(x) Dx\, Dv = \int_V f(v) Dv$$

This formally verifies the first equation in (6.1).

(3) For $\int_{V^\perp} e^{2\pi i\langle x,u\rangle} Du$ we mimic the finite dimensional case and give meaning to this integral through "regularization":

$$\begin{aligned}\int_{V^\perp} e^{2\pi i\langle x,u\rangle} Du &= \lim_{\sigma\to\infty} \int_{V^\perp} e^{2\pi i\langle x,u\rangle - \frac{|u|_0^2}{2\sigma^2}} Du \\ &= \lim_{\sigma\to\infty} (2\pi\sigma^2)^{\dim V^\perp/2} e^{\frac{-4\pi^2\sigma^2}{2}|x_{V^\perp}|_0^2}\end{aligned}$$

where $x_{V^\perp}$ is the projection of x onto $V^\perp$. Momentarily ignoring the possibility that $V^\perp$ is infinite dimensional, we see that this last limit is ∞ if $x_{V^\perp} = 0$ and 0 otherwise. So we have

$$\begin{aligned}&\int_E \int_{V^\perp} e^{2\pi i\langle x,u\rangle}\, Du\, f(x)\, Dx \\ &\quad= \lim_{\sigma\to\infty} \int_E f(x_V + x_{V^\perp})(2\pi\sigma^2)^{\dim V^\perp/2} e^{\frac{-4\pi^2\sigma^2}{2}|x_{V^\perp}|_0^2}\, D(x_V + x_{V^\perp}) \\ &\quad= \lim_{\sigma\to\infty} \int_V \int_{V^\perp} f(x_V + x_{V^\perp})(2\pi\sigma^2)^{\dim V^\perp/2} e^{\frac{-4\pi^2\sigma^2}{2}|x_{V^\perp}|_0^2}\, Dx_{V^\perp} Dx_V\end{aligned}$$

Here we use a change of variables with $u = 2\pi\sigma x_{V^\perp}$ and $Du = (2\pi\sigma)^{\dim V^\perp} Dx_{V^\perp}$ to get

$$\begin{aligned}&= \lim_{\sigma\to\infty} \int_V \int_{V^\perp} f\left(x_V + \tfrac{u}{2\pi\sigma}\right) e^{\frac{-|u|_0^2}{2}} \frac{Du}{(2\pi)^{\dim V/2}}\, Dx_V \\ &= \int_V f(x_V)\, Dx_V \\ &= \int_V f(v)\, Dv\end{aligned}$$

Thus the equalities in (6.1) hold in the distributional sense.

6.1.2 *S*–transform

Next we formally take the S–transform of each term to see that the common factor is

$$(2\pi)^{-\dim V^\perp/2} e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c^2} \tag{6.2}$$

where $\xi \in \mathcal{E}_c$ and $\xi_{V^\perp}$ is the orthogonal projection of ξ onto $V_c^\perp$. That is, if $\xi = \xi_1 + i\xi_2$ with $\xi_1, \xi_2 \in \mathcal{E}$, then $\xi_{V^\perp} = \xi_{1V^\perp} + \xi_{2V^\perp}$, where $\xi_{1V^\perp}, \xi_{2V^\perp}$ are the orthogonal projections onto $V^\perp$. Observe

(1) For δ_V we have, working formally,

$$\begin{aligned}
S(\delta_V)(\xi) &= \langle\langle \delta_V, :e^{\langle \cdot,\xi\rangle_c}:\rangle\rangle \\
&= \int_{\mathcal{E}'} \delta_V(x) :e^{\langle x,\xi\rangle_c}: d\mu(x) \\
&= \int_E \delta_V(x) e^{\langle x,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c^2 - \frac{1}{2}|x|_0^2} \frac{Dx}{(2\pi)^{\dim E/2}} \\
&= \int_V e^{\langle v,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c^2 - \frac{1}{2}|v|_0^2} \frac{Dv}{(2\pi)^{\dim E/2}} \\
&= (2\pi)^{-\dim V^\perp/2} \int_V e^{\langle v,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c^2 - \frac{1}{2}|v|_0^2} \frac{Dv}{(2\pi)^{\dim V/2}} \\
&= (2\pi)^{-\dim V^\perp/2} e^{\frac{1}{2}\langle \xi_V,\xi_V\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c} \\
&= (2\pi)^{-\dim V^\perp/2} e^{-\frac{1}{2}\langle \xi_{V^\perp},\xi_{V^\perp}\rangle_c}
\end{aligned}$$

(2) For $\int_V \delta(x-v)Dv$ we see that

$$\begin{aligned}
S\Big(\int_V \delta(x-v)Dv\Big)(\xi) &= \int_{\mathcal{E}'}\int_V \delta(x-v)Dv :e^{\langle x,\xi\rangle_c}: d\mu(x) \\
&= \int_V\int_{\mathcal{E}'} \delta(x-v) :e^{\langle x,\xi\rangle_c}: d\mu(x)Dv \\
&= \int_V\int_E \delta(x-v) e^{\langle x,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c^2 - \frac{1}{2}|x|_0^2} \frac{Dx}{(2\pi)^{\dim E/2}} Dv \\
&= (2\pi)^{-\dim V^\perp/2} \int_V e^{\langle v,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c^2 - \frac{1}{2}|v|_0^2} \frac{Dv}{(2\pi)^{\dim V/2}} \\
&= (2\pi)^{-\dim V^\perp/2} e^{\frac{1}{2}\langle \xi_V,\xi_V\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c} \\
&= (2\pi)^{-\dim V^\perp/2} e^{-\frac{1}{2}\langle \xi_{V^\perp},\xi_{V^\perp}\rangle_c}
\end{aligned}$$

(3) And for $\int_{V^\perp} e^{2\pi i\langle x,u\rangle} Du$ we get

$$\begin{aligned}
S\Big(\int_{V^\perp} e^{2\pi i\langle x,u\rangle} Du\Big)(\xi) &= \int_{\mathcal{E}'}\int_{V^\perp} e^{2\pi i\langle x,u\rangle}\ Du :e^{\langle x,\xi\rangle_c}:\ d\mu(x) \\
&= \int_{V^\perp}\int_{\mathcal{E}'} e^{2\pi i\langle x,u\rangle} e^{\langle x,\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c}\ d\mu(x)Du \\
&= \int_{V^\perp}\int_{\mathcal{E}'} e^{\langle x,2\pi iu+\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c} d\mu(x)Du \\
&= \int_{V^\perp} e^{\frac{1}{2}\langle 2\pi iu+\xi,2\pi iu+\xi\rangle_c - \frac{1}{2}\langle \xi,\xi\rangle_c} Du \\
&= \int_{V^\perp} e^{\langle 2\pi iu,\xi\rangle_c - 4\pi^2\frac{|u|_0}{2}} Du
\end{aligned}$$

Letting $w = 2\pi u$ we have

$$\begin{aligned}
&= \int_{V^\perp} e^{i\langle w,\xi\rangle_c - \frac{1}{2}|w|_0} \frac{Dw}{(2\pi)^{\dim V^\perp}} \\
&= (2\pi)^{-\dim V^\perp/2} \int_{V^\perp} e^{i\langle w,\xi\rangle_c - \frac{1}{2}|w|_0} \frac{Dw}{(2\pi)^{\dim V^\perp/2}} \\
&= (2\pi)^{-\dim V^\perp/2} e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c}
\end{aligned}$$

6.2 Definition of Delta Function of a Subspace

Consider the function

(6.3) $$F_V(\xi) = e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c} \qquad \xi \in \mathcal{E}_c$$

We would like to see that F_V is the S–transform of some generalized function in $(\mathcal{E})'$. To do this we show that F_V satisfies the conditions in Theorem 5.30. Letting $\xi = \xi_1 + i\xi_2$ where $\xi_1, \xi_2 \in \mathcal{E}$ we observe that

(6.4) $$\begin{aligned}
|F_V(\xi)| &= |e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c}| = |\exp(-\tfrac{1}{2}\langle P_\perp(\xi_1 + i\xi_2), P_\perp(\xi_1 + i\xi_2)\rangle_c)| \\
&\qquad \text{where } P_\perp \text{ is the orthogonal projection onto } V^\perp \\
&= |\exp(-\tfrac{1}{2}|P_\perp\xi_1|_0^2 + \tfrac{1}{2}|P_\perp\xi_2|_0^2 - i\langle P_\perp\xi_1, P_\perp\xi_2\rangle)| \\
&= \exp(-\tfrac{1}{2}|P_\perp\xi_1|_0^2 + \tfrac{1}{2}|P_\perp\xi_2|_0^2) \\
&\le \exp(\tfrac{1}{2}|P_\perp\xi_1|_0^2 + \tfrac{1}{2}|P_\perp\xi_2|_0^2) \\
&\le e^{\frac{1}{2}|\xi|_0^2}
\end{aligned}$$

Also for $z \in \mathbb{C}$ and $\xi, \eta \in \mathcal{E}_c$ we have

$$F_V(z\xi + \eta) = e^{-\frac{1}{2}\langle z\xi_{V^\perp} + \eta_{V^\perp}, z\xi_{V^\perp} + \eta_{V^\perp}\rangle_c} = e^{-\frac{z^2}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c - z\langle \xi_{V^\perp}, \eta_{V^\perp}\rangle_c - \frac{1}{2}\langle \eta_{V^\perp}, \eta_{V^\perp}\rangle_c}$$

Therefore $F_V(z\xi + \eta)$ is entire.

Hence by Theorem 5.30 there is a generalized function $\Phi \in (\mathcal{E})'$ whose S–transform is given by $F_V(\xi)$ in (6.3). This leads us to the following definition:

Definition 6.1. Let V be a closed subspace of a real Hilbert space E. The *delta function of the subspace* V is defined to be the generalized function in $(\mathcal{E})'$ whose S–transform is given by $e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c}$ where $\xi \in \mathcal{E}_c$. This generalized function will be denoted by $\tilde{\delta}_V$.

In order to account for the possibility that the codimension of V is infinite, we have defined $\tilde{\delta}_V$ to be essentially $(2\pi)^{\dim V^\perp/2}\delta_V$ from equation (6.1).

6.2.1 Relationship with the Kubo–Yokoi Delta Function

As the notation indicates, the delta function of a subspace, $\tilde{\delta}_V$, is related to the Kubo–Yokoi delta function from Section 5.5. If we interpret the Kubo–Yokoi delta function at 0, $\tilde{\delta}_0$, as the delta function of the subspace $V = 0$, then observing that $V^\perp = E$, we see from the definition above that the S–transform of $\tilde{\delta}_V$ is given by $e^{-\frac{1}{2}\langle\xi,\xi\rangle_c}$, which is the S–transform of $\tilde{\delta}_0$ (see equation (5.29)).

6.2.2 Relationship with Donsker's Delta Function

What is not so apparent is that the delta function of a subspace, $\tilde{\delta}_V$, is related to Donsker's delta function. We saw in Section 5.5.1 that Donsker's delta function is defined for the Gel'fand triple $\mathcal{S}(\mathbb{R}) \subset L^2(\mathbb{R}) \subset \mathcal{S}'(\mathbb{R})$ and is usually given by $\delta_a(B(t))$ where $B(t) = \langle\cdot, 1_{[0,t]}\rangle$ and δ_a is the Dirac delta function at a. However, this definition can be extended slightly. In fact, by Theorem 5.38, we have for any $f \in L^2(\mathbb{R})$, $\delta_a(\langle\cdot, f\rangle)$ is in $\mathcal{S}'(\mathbb{R})$.

Now given a unit vector $f \in L^2(\mathbb{R})$ consider the generalized function $\delta_0(\langle\cdot, f\rangle)$. Intuitively, this is a function that gives enormous weight to vectors $g \in L^2(\mathbb{R})$ with $\langle f, g\rangle = 0$ (i.e. vectors $g \in \{f\}^\perp$). So taking $V = \{f\}^\perp$, the distribution $\delta_0(\langle\cdot, f\rangle)$ should be related to $\tilde{\delta}_V$.

Using Theorem 5.38 to find the S–transform of $\delta_0(\langle\cdot, f\rangle)$ we see that

$$S[\delta_0(\langle\cdot, f\rangle)](\xi) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} \delta_0(y) e^{-\frac{1}{2}(y-\langle f,\xi\rangle_c)^2} dy = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}\langle f,\xi\rangle_c^2}$$

Now since $V = \{f\}^\perp$, we have $V^\perp = \{\mathbb{R}f\}$. Thus the $V^\perp$ component of ξ, $\xi_{V^\perp}$, is given by $\langle f, \xi\rangle_c f$. Observe

$$\langle f, \xi\rangle_c^2 = \langle\langle f, \xi\rangle_c f, \langle f, \xi\rangle_c f\rangle_c = \langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c$$

Also since the $\dim V^\perp = 1$, we have

$$S(\delta_0(\langle\cdot, f\rangle))(\xi) = (2\pi)^{-\dim V^\perp/2} e^{-\frac{1}{2}\langle\xi_{V^\perp},\xi_{V^\perp}\rangle_c^2}$$

Thus, Theorem 5.25 tells us that $\sqrt{2\pi}\,\delta_0(\langle\cdot, f\rangle) = \tilde{\delta}_V$.

6.3 The Wiener–Itô Decomposition of $\tilde{\delta}_V$

In this section we find the Wiener–Itô decomposition of $\tilde{\delta}_V$. We begin by generalizing the definition of the trace operator and Wick tensor found in Section 5.3

6.3.1 Subspace Trace Operator

As usual, let V be a closed subspace of our Hilbert space E.

Definition 6.2. The V*–trace operator*, which we denote by τ_V is the element in $(\mathcal{E}_c')^{\widehat{\otimes}2}$ given by

$$\langle \tau_V, \xi \otimes \eta \rangle_c = \langle \xi_V, \eta_V \rangle_c \qquad \xi, \eta \in \mathcal{E}_c$$

The V–trace operator can be represented as

$$\tau_V = \sum_{k=1}^{\infty} e_k \otimes P_V e_k$$

where P_V is the orthogonal projection onto the subspace V. Observe

$$\begin{aligned}
\langle \tau_V, \xi \otimes \eta \rangle_c &= \Big\langle \sum_{k=1}^{\infty} e_k \otimes P_V e_k, \xi \otimes \eta \Big\rangle_c \\
&= \sum_{k=1}^{\infty} \langle e_k, \xi \rangle_c \langle P_V e_k, \eta \rangle_c \\
&= \sum_{k=1}^{\infty} \langle e_k, \xi \rangle_c \langle e_k, \eta_V \rangle_c \qquad \text{where } \eta_V = P_V \eta \\
&= \Big\langle \sum_{k=1}^{\infty} \langle e_k, \xi \rangle_c e_k, \sum_{k=1}^{\infty} \langle e_k, \eta_V \rangle_c e_k \Big\rangle_c \\
&= \langle \xi, \eta_V \rangle_c = \langle \xi_V, \eta_V \rangle_c
\end{aligned}$$

Remark 6.3. We can also represent τ_V as $\sum_{k=1}^{\infty} P_V e_k \otimes P_V e_k$ or $\sum_{k=1}^{\dim V} v_k \otimes v_k$ where $\{v_k\}_1^{\dim V}$ is an orthonormal basis for V. However, we find that the representation of τ_V given above is more suitable for our computations.

Now note that τ_V is in fact in $(\mathcal{E}_c')^{\widehat{\otimes}2}$

$$|\tau_V|_{-p}^2 = \sum_{k=1}^{\infty} |(A^{-p})^{\otimes 2}(e_k \otimes P_V e_k)|_0^2 = \sum_{k=1}^{\infty} |A^{-p} e_k|_0^2 |A^{-p} P_V e_k|_0^2$$

Here we use that $|A^{-p} P_V e_k|_0^2 \leq \|A^{-1}\|^p |P_V e_k|_0^2 \leq \frac{1}{\lambda_1^p} |e_k|_0^2 \leq \frac{1}{\lambda_1^p}$ in the above to see that

$$|\tau_V|_{-p}^2 \leq \lambda_1^{-p} \sum_{k=1}^{\infty} |A^{-p} e_k|_0^2 \leq \lambda_1^{-p} \sum_{k=1}^{\infty} \lambda_k^{-2p}$$

where λ_k is the eigenvalue corresponding to e_k. We know that $\sum_{k=1}^{\infty} \lambda_k^{-2} < \infty$ by (5.1). So for any $p > 0$ we have

$$|\tau_V|_{-p}^2 \leq \lambda_1^{-p} \sum_{k=1}^{\infty} \lambda_k^{-2p} < \infty \tag{6.5}$$

and hence τ_V is in $(\mathcal{E}_c')^{\widehat{\otimes}2}$.

6.3.2 Subspace Wick Tensor

With the notion of a subspace trace operator securely behind us, we can now define the subspace Wick tensor. Again we let V be a closed subspace of our Hilbert space E

Definition 6.4. For $x \in \mathcal{E}'$ the $V-$*Wick tensor for* x *of order* n is defined to be

$$:x_V^{\otimes n}:= \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-1)^k x^{\otimes(n-2k)} \widehat{\otimes} \tau_V^{\otimes k}$$

Proposition 6.5. *For any* $x \in \mathcal{E}'$ *and* $\xi \in \mathcal{E}$ *we have*

$$\langle :x_V^{\otimes n}:, \xi^{\otimes n} \rangle =: \langle x, \xi \rangle^n :_{|\xi_V|_0^2}$$

Proof. From the definition we have

$$\langle :x_V^{\otimes n}:, \xi^{\otimes n} \rangle = \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!(-|\xi_V|_0^2)^k \langle x, \xi \rangle^{n-2k}$$

Comparing this with (5.19) we see that $\langle :x_V^{\otimes n}:, \xi^{\otimes n} \rangle =: \langle x, \xi \rangle^n :_{|\xi_V|_0^2}$ □

6.3.3 Wiener–Itô Expansion

Consider the following function

$$\Phi_x^V = \sum_{n=0}^{\infty} \frac{1}{n!} \langle :\cdot^{\otimes n}:, :x_V^{\otimes n}: \rangle$$

We would like to see that Φ_x^V is in $(\mathcal{E})'$.

Lemma 6.6. *If* $a, b \in \mathcal{E}_{-p}$ *for any integer* $p > 0$, *then*

$$|a^{\otimes k} \widehat{\otimes} b^{\otimes l}|_{-p} \leq |a|_{-p}^k |b|_{-p}^l$$

Proof. Recall

$$a^{\otimes k} \widehat{\otimes} b^{\otimes l} = \frac{1}{2} \left(a^{\otimes k} \otimes b^{\otimes l} + b^{\otimes l} \otimes a^{\otimes k} \right)$$

Hence

$$\begin{aligned} |a^{\otimes k} \widehat{\otimes} b^{\otimes l}|_{-p} &\leq \frac{1}{2} \left(|a^{\otimes k} \otimes b^{\otimes l}|_{-p} + |b^{\otimes l} \otimes a^{\otimes k}|_{-p} \right) \\ &\leq \frac{1}{2} \left(|a^{\otimes k}|_{-p} |b^{\otimes l}|_{-p} + |b^{\otimes l}|_{-p} |a^{\otimes k}|_{-p} \right) \\ &\leq |a^{\otimes k}|_{-p} |b^{\otimes l}|_{-p} \end{aligned}$$

which proves the inequality. □

Lemma 6.7. *For any $n \geq 1$ and $x \in \mathcal{E}'_p$ we have*

$$|{:}x_V^{\otimes n}{:}|_{-p} \leq \sqrt{n!}(|x|_{-p} + |\tau_V|_{-p}^{1/2})^n$$

Proof. From the definition of ${:}x_V^{\otimes n}{:}$ and Lemma 6.6 we see that

$$|{:}x_V^{\otimes n}{:}|_{-p} \leq \sum_{k=0}^{[n/2]} \binom{n}{2k} (2k-1)!!\, |x|_{-p}^{n-2k} |\tau_V|_{-p}^k$$

Now for $k \leq [n/2]$ we use that $(2k-1)!! \leq (n-1)!! \leq \sqrt{n!}$ to get

$$\begin{aligned}
|{:}x_V^{\otimes n}{:}|_{-p} &\leq \sqrt{n!} \sum_{k=0}^{[n/2]} \binom{n}{2k} |x|_{-p}^{n-2k} (|\tau_V|_{-p}^{1/2})^{2k} \\
&\leq \sqrt{n!} \sum_{k=0}^{n} \binom{n}{k} |x|_{-p}^{n-k} (|\tau_V|_{-p}^{1/2})^{k} \\
&\leq \sqrt{n!}(|x|_{-p} + |\tau_V|_{-p}^{1/2})^n
\end{aligned}$$

□

Proposition 6.8. *For $x \in \mathcal{E}'$, $\Phi_x^V = \sum_{n=0}^{\infty} \frac{1}{n!} \langle {:}\cdot^{\otimes n}{:}, {:}x_V^{\otimes n}{:} \rangle$ is a generalized function (i.e. Φ_x^V is in $(\mathcal{E})'$)*

Proof. Since $x \in \mathcal{E}'$, x is in $\mathcal{E}'_q$ for $q \geq 0$. Thus for any $p \geq q$ we have

$$\begin{aligned}
\|\Phi_x^V\|_{-p}^2 &= \sum_{n=0}^{\infty} n! \frac{1}{(n!)^2} |{:}x_V^{\otimes n}{:}|_{-p}^2 \\
&\leq \sum_{n=0}^{\infty} \frac{1}{n!} (\sqrt{n!})^2 (|x|_{-p} + |\tau_V|_{-p}^{1/2})^{2n} \qquad \text{by Lemma 6.7} \\
&= \sum_{n=0}^{\infty} (|x|_{-p} + |\tau_V|_{-p}^{1/2})^{2n} \qquad (6.6)
\end{aligned}$$

From (6.5) we have that $|\tau_V|_{-p}^2 \leq \lambda_1^{-p} \sum_{k=1}^{\infty} \lambda_k^{-2}$. Thus $|\tau_V|_{-p} \to 0$ as $p \to \infty$. Also for $x \in \mathcal{E}'$, we have $|x|_{-p} \to 0$ as $p \to \infty$. Therefore we can take p so that $|x|_{-p} + |\tau_V|_{-p}^{1/2} < 1$. From (6.6) above this gives us

$$\|\Phi_x^V\|_{-p}^2 \leq \frac{1}{1 - \left(|x|_{-p} + |\tau_V|_{-p}^{1/2}\right)^2}$$

Thus $\Phi_x^V \in (\mathcal{E})'$. □

Theorem 6.9. *The Wiener–Itô decomposition of $\tilde{\delta}_V$ is given by $\sum_{n=0}^{\infty} \frac{1}{n!} \langle {:}\cdot^{\otimes n}{:}, {:}0_{V^\perp}^{\otimes n}{:} \rangle$*

Proof. From Proposition 6.8 we know that $\Phi_0^{V^\perp} = \sum_{n=0}^{\infty} \frac{1}{n!}\langle :\cdot^{\otimes n}:, :0_{V^\perp}^{\otimes n}:\rangle$ is in $(\mathcal{E})'$. Taking the S–transform of $\Phi_0^{V^\perp}$ with $\xi \in \mathcal{E}$ we get

$$\begin{aligned}
S(\Phi_0^{V^\perp})(\xi) &= \sum_{n=0}^{\infty} n! \frac{1}{(n!)^2} \langle :0_{V^\perp}^{\otimes n}:, \xi^{\otimes n}\rangle \\
&= \sum_{n=0}^{\infty} \frac{1}{n!} :0:_{|\xi_{V^\perp}|_0^2} \qquad \text{by Proposition 6.5} \\
&= \sum_{n=0}^{\infty} \frac{(2n-1)!!}{(2n)!} (-1)^n |\xi_{V^\perp}|_0^{2n} \qquad \text{by (5.19)} \\
&= \sum_{n=0}^{\infty} \frac{1}{n!} \frac{(-1)^n}{2^n} |\xi_{V^\perp}|_0^{2n} \qquad \text{since } (2n-1)!! = \frac{(2n)!}{2^n n!} \\
&= e^{-\frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle}
\end{aligned}$$

Comparing this with the S–transform of $\tilde{\delta}_V$ in Definition 6.1 we see that

$$\langle\langle \Phi_0^{V^\perp}, :e^{\langle \cdot, \xi\rangle}:\rangle\rangle = S(\Phi_0^{V^\perp})(\xi) S(\tilde{\delta}_V)(\xi) = \langle\langle \tilde{\delta}_V, :e^{\langle \cdot, \xi\rangle}:\rangle\rangle$$

for all $\xi \in \mathcal{E}$. Thus by Corollary 5.26 we have $\tilde{\delta}_V = \Phi_0^{V^\perp}$ μ–almost everywhere. Therefore $\tilde{\delta}_V = \sum_{n=0}^{\infty} \frac{1}{n!}\langle :\cdot^{\otimes n}:, :0_{V^\perp}^{\otimes n}:\rangle$. □

Note that if we take $V = 0$, and hence $V^\perp = E$, we get

$$\tilde{\delta}_V = \sum_{n=0}^{\infty} \langle :\cdot^{\otimes n}:, :0^{\otimes n}:\rangle$$

which, as expected, is identical to the Wiener–Itô decompostion for the Kubo–Yokoi delta function at 0 (see Theorem 5.37).

Chapter 7

The Measure on a Subspace

Here we define the Gaussian measure on a closed subspace V of E. Recall the Minlos theorem:

Theorem 7.1 (Minlos). *Let $\mathcal{E}$ be a nuclear space with dual $\mathcal{E}'$. If ν is a probability measure on $\mathcal{E}'$, then the Fourier transform of ν*

$$\mathcal{F}\nu(\xi) = \int_{\mathcal{E}'} e^{i\langle x,\xi\rangle}\, d\nu(x), \qquad \xi \in \mathcal{E}$$

is a characteristic function. That is, $\mathcal{F}\nu(\cdot)$ is continuous, positive definite, and $\mathcal{F}\nu(0) = 1$. Conversely, given a characteristic function C on $\mathcal{E}$, there exists a unique probability measure ν on $\mathcal{E}'$ such that $\mathcal{F}\nu = C$.

Consider the function C_V^σ on $\mathcal{E}$ given by

$$C_V^\sigma(\xi) = \exp(-\tfrac{\sigma^2}{2}|\xi_V|_0^2) \qquad \xi \in \mathcal{E}$$

where $\sigma \geq 0$ and ξ_V represents the orthogonal projection of ξ onto V. The next lemma shows that C_V^σ is a characteristic function. That is, C_V^σ is continuous, positive definite, and $C_V^\sigma(0) = 1$.

Lemma 7.2. *For $\sigma \geq 0$, C_V^σ is a characteristic function.*

Proof. Obviously C_V^σ is continuous on $\mathcal{E}$ and $C_V^\sigma(0) = 1$. To see that C_V^σ is positive definite, let $\xi_1, \xi_2, \ldots, \xi_n \in \mathcal{E}$ and $z_1, z_2, \ldots, z_n \in \mathbb{C}$. Now let W be the subspace of $\mathcal{E}$ spanned by $\{P\xi_1, P\xi_2, \ldots, P\xi_n\}$, where P is the orthogonal projection onto V. Let μ_W be the gaussian measure on W with mean 0 and variance σ^2. Then for any $w \in W$ we have

$$\int_W e^{i\langle w,y\rangle}\, d\mu_W(y) = \exp(-\tfrac{\sigma^2}{2}|w|_0^2)$$

Therefore

$$\begin{aligned}\sum_{j,k=1}^{n} z_j C_V^{\sigma}(\xi_j - \xi_k)\overline{z_k} &= \sum_{j,k=1}^{n} \int_W z_j e^{i\langle P\xi_j - P\xi_k, y\rangle}\overline{z_k}\, d\mu_W(y) \\ &= \int_W \sum_{j,k=1}^{n} z_j e^{i\langle P\xi_j - P\xi_k, y\rangle}\overline{z_k}\, d\mu_W(y) \\ &= \int_W \Big| \sum_{j,k=1}^{n} z_j e^{i\langle P\xi_j, y\rangle}\Big|^2 d\mu_W(y) \geq 0\end{aligned}$$

□

Applying the Minlos theorem leads to the following definition:

Definition 7.3. The probability measure on $\mathcal{E}'$ corresponding to the characteristic function $C_V^{\sigma}(\cdot)$ for $\sigma \geq 0$ is called the *Gaussian measure on the subspace* V with variance σ^2 and is denoted by μ_V^{σ}. If $\sigma = 1$, we denote it by μ_V and call it the *standard Gaussian measure on the subspace* V.

Thus μ_V^{σ} is the Borel measure on $\mathcal{E}'$ which satisfies

$$\int_{\mathcal{E}'} e^{i\langle x,\xi\rangle}\, d\mu_V^{\sigma}(x) = e^{-\frac{\sigma^2}{2}|\xi_V|_0^2} \qquad \text{for all } \xi \in \mathcal{E}$$

where ξ_V is the orthogonal projection of ξ onto V.

Remark 7.4. Another formulation of the Gaussian measure on a subspace of a real Hilbert space can be found in [22].

7.1 Basic Properties of the Measure μ_V

Here we will list a few properties of the measure μ_V. Most of these results follow from the next Lemma:

Lemma 7.5. *Let $\xi_1, \xi_2, \ldots, \xi_n \in \mathcal{E}$ and V be a closed subspace of E, with P the orthogonal projection onto V. Then the image of the Gaussian measure μ_V under the map*

$$x \mapsto (\langle x, \xi_1\rangle, \cdots, \langle x, \xi_n\rangle) \in \mathbb{R}^n, \qquad x \in \mathcal{E}'$$

is the Gaussian measure on $\mathbb{R}^n$ with covariance matrix $\Sigma = (\langle P\xi_j, P\xi_k\rangle)_{j,k}$. (i.e. the probability measure on $\mathbb{R}^n$ with characteristic function $e^{-\frac{1}{2}\langle t, \Sigma t\rangle}$)

Proof. Let ν denote the image of μ_V. So ν is a probability measure on $\mathbb{R}^n$. Computing the characteristic function of ν we see

$$\begin{aligned}\hat{\nu}(s) &= \int_{\mathbb{R}^n} e^{i\langle s,t\rangle} dv(t) = \int_{\mathcal{E}'} \exp\Big(i\sum_{k=1}^n s_k\langle x,\xi_k\rangle\Big) d\mu_V(x) \\ &= \exp\Big(-\tfrac{1}{2}\Big|P\sum_{k=1}^n s_k\xi_k\Big|_0^2\Big) = \exp\Big(-\tfrac{1}{2}\Big|\sum_{k=1}^n s_k P\xi_k\Big|_0^2\Big) \\ &= \exp\Big(-\tfrac{1}{2}\sum_{i,j=1}^n s_i s_j\langle P\xi_i, P\xi_j\rangle\Big) = \exp\big(-\tfrac{1}{2}\langle s,\Sigma s\rangle\big)\end{aligned}$$

□

Corollary 7.6. *Let V be a closed subspace of E. Suppose $\xi_1,\xi_2,\ldots,\xi_n \in \mathcal{E}$ have orthonormal projections in V, then the Gaussian measure in the previous lemma becomes the standard Gaussian measure on $\mathbb{R}^n$.*

Lemma 7.7. *Let V be a closed subspace of E, with P the orthogonal projection onto V. Let $\xi_1,\xi_2,\ldots,\xi_n \in \mathcal{E}$ be such that $P\xi_1, P\xi_2,\ldots,P\xi_n$ is an orthogonal system in E. For any Gaussian integrable functions $f_1,f_2,\ldots,f_n$ on $\mathbb{R}$ we have*

$$\int_{\mathcal{E}'} f_1(\langle x,\xi_1\rangle)\ldots f_n(\langle x,\xi_n\rangle)\, d\mu_V(x) = \prod_{k=1}^n \int_{\mathcal{E}'} f_k(\langle x,\xi_k\rangle)\, d\mu_V(x)$$

Proof. Apply Lemma 7.5. □

Lemma 7.8. *For any $\xi \in \mathcal{E}_c$ and $n = 0,1,2,\ldots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}'} |\langle x,\xi\rangle_c|^2\, d\mu_V(x) = |\xi_V|_0^2$

(b) $\displaystyle\int_{\mathcal{E}'} \langle x,\xi\rangle_c^{2n}\, d\mu_V(x) = \frac{(2n)!}{2^n n!}\langle\xi_V,\xi_V\rangle_c^n$

(c) $\displaystyle\int_{\mathcal{E}'} \langle x,\xi\rangle_c^{2n+1}\, d\mu_V(x) = 0$

Proof. The identities obviously hold when $\xi = 0$. So we take $\xi \in \mathcal{E}$ with $\xi \neq 0$. By Corollary 7.6 we have that

$$\int_{\mathcal{E}'} |\langle x,\xi\rangle|^2\, d\mu_V(x) = |\xi_V|_0^2 \int_{\mathcal{E}'} \Big|\Big\langle x, \frac{\xi}{|\xi_V|_0}\Big\rangle\Big|^2 d\mu_V(x) = \frac{|\xi_V|_0^2}{\sqrt{2\pi}} \int_{\mathbb{R}} t^2 e^{-\frac{t^2}{2}} dt = |\xi_V|_0^2$$

Thus we have the first identity for $\xi \in \mathcal{E}$. Using this, we take $\xi = \xi_1 + i\xi_2 \in \mathcal{E}_c$ and observe that

$$\int_{\mathcal{E}'} |\langle x,\xi\rangle|^2\, d\mu_V(x) = \int_{\mathcal{E}'} \big(\langle x,\xi_1\rangle^2 + \langle x,\xi_2\rangle^2\big)\, d\mu_V(x) = |\xi_{1V}|_0^2 + |\xi_{2V}|_0^2 = |\xi_V|_0^2$$

which proves the first identity. The second and third identity can be proved by a similar argument. □

As done in Section 5.1.1, we can define $\langle\cdot,\xi\rangle_c$ for any $\xi \in E_c$ as a μ–almost everywhere defined function of $x \in \mathcal{E}'$ in $L^2(\mathcal{E}',\mu_V)$, the space of all functions $f : \mathcal{E}' \to \mathbb{C}$ which are L^2 integrable with respect to μ_V. Take a sequence $\{\xi_n\}_{n=1}^{\infty}$ in $\mathcal{E}_c$ such that $\lim_{n\to\infty} |\xi - \xi_n|_0 = 0$. Using Lemma 7.8 we can see that the functions $\{\langle\cdot,\xi_n\rangle_c\}_{n=1}^{\infty}$ form a Cauchy sequence in $L^2(\mathcal{E}',\mu_V)$. Thus there exists a $\phi \in L^2(\mathcal{E}',\mu_V)$ such that $\lim_{n\to\infty}\langle\cdot,\xi_n\rangle_c = \phi$. We denote such a ϕ by $\langle\cdot,\xi\rangle_c$.

Proposition 7.9. *For any $\xi \in E_c$ and $n = 0, 1, 2, \ldots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}'} |\langle x,\xi\rangle_c|^2 \, d\mu_V(x) = |\xi_V|_0^2$

(b) $\displaystyle\int_{\mathcal{E}'} \langle x,\xi\rangle_c^{2n} \, d\mu_V(x) = \frac{(2n)!}{2^n n!}\langle\xi_V,\xi_V\rangle_c^n$

(c) $\displaystyle\int_{\mathcal{E}'} \langle x,\xi\rangle_c^{2n+1} \, d\mu_V(x) = 0$

Proof. It is easily shown that Lemmas 7.5 and 7.7 are true when $\xi_1, \xi_2, \ldots, \xi_n$ are in E. Using this, we can mimic the proof of Lemma 7.8 to get the identities. □

Next we present what is probably the most important identity involving the measure μ_V.

Proposition 7.10. *For any $\xi \in E_c$ we have the following:*

$$\int_{\mathcal{E}'} e^{\langle x,\xi\rangle_c} \, d\mu_V(x) = e^{\langle\xi_V,\xi_V\rangle_c/2}$$

where ξ_V is the orthogonal projection of ξ onto V

Proof. Take $\xi, \eta \in E$ and then $\xi + i\eta \in E_c$. In light of Proposition 7.9 and the definition of μ_V we can assume that $\xi, \eta \in V$. Write η as $\eta = \xi_\eta + \eta - \xi_\eta$ where $\xi_\eta = \langle \eta, \frac{\xi}{|\xi|_0}\rangle \frac{\xi}{|\xi|_0}$ is the projection of η onto the subspace spanned by ξ. Note that ξ and $\eta - \xi_\eta$ are orthogonal. Now

$$\int_{\mathcal{E}'} e^{\langle x,\xi+i\eta\rangle_c} \, d\mu_V(x) = \int_{\mathcal{E}'} e^{\langle x,\xi+i(\xi_\eta+\eta-\xi_\eta)\rangle_c} \, d\mu_V(x)$$

Applying Lemma 7.7 we get

$$\begin{aligned}
&= \int_{\mathcal{E}'} e^{\langle x,\xi+i\xi_\eta\rangle_c} \, d\mu_V(x) \int_{\mathcal{E}'} e^{i\langle x,\eta-\xi_\eta\rangle} \, d\mu_V(x) \\
&= e^{-\langle \eta-\xi_\eta,\eta-\xi_\eta\rangle/2} \int_{\mathcal{E}'} \exp\left[\left\langle x, (|\xi|_0 + i|\xi_\eta|_0)\frac{\xi}{|\xi|_0}\right\rangle_c\right] d\mu_V(x) \\
&= e^{-\langle \eta-\xi_\eta,\eta-\xi_\eta\rangle/2} \exp\left[\tfrac{1}{2}(|\xi|_0 + i|\xi_\eta|_0)^2\right] \\
&= \exp\tfrac{1}{2}\Big[-|\eta|_0^2 + 2\langle\eta,\xi_\eta\rangle - |\xi_\eta|_0^2 + |\xi|_0^2 + 2i|\xi|_0|\xi_\eta|_0 - |\xi_\eta|_0^2\Big]
\end{aligned}$$

Note that $\langle \eta, \xi_\eta \rangle = |\xi_\eta|_0^2$ and $|\xi|_0 |\xi_\eta|_0 = \langle \eta, \xi \rangle$ to see that the above gives us

$$= \varepsilon^{-\langle \xi + i\eta, \xi + i\eta \rangle /2}$$

This gives us the identity when $\xi \neq 0$. If $\xi = 0$ we can immediately apply Lemma 7.7 to see the conclusion. □

7.2 Equivalence of $\tilde{\delta}_V$ and μ_V

In this section we demonstrate that $\tilde{\delta}_V$ and μ_V are equal when considered as elements of $(\mathcal{E})'$.

7.2.1 Hida Measure

Recall the definition of a Hida Measure:

Definition 7.11. A measure ν on $\mathcal{E}'$ is called a *Hida measure* if $\phi \in L^1(\nu)$ for all $\phi \in (\mathcal{E})$ and the linear functional

$$\phi \mapsto \int_{\mathcal{E}'} \phi(x)\, d\nu(x)$$

is continuous on $(\mathcal{E})$.

We say that a generalized function $\Phi \in (\mathcal{E})'$ is *induced* by a Hida measure ν if for any $\phi \in (\mathcal{E})$ we have

$$\langle\langle \Phi, \phi \rangle\rangle = \int_{\mathcal{E}'} \phi(x)\, d\nu(x)$$

The following Theorem characterizes those generalized functions which are induced by a Hida measure.

Theorem 7.12. *Let $\Phi \in (\mathcal{E})'$. Then the following are equivalent:*

(a) *For any nonnegative $\phi \in (\mathcal{E})$, $\langle\langle \Phi, \phi \rangle\rangle \geq 0$*

(b) *$\mathcal{T}(\Phi)(\xi) = \langle\langle \Phi, e^{i\langle \cdot, \xi \rangle} \rangle\rangle$ is positive definite on $\mathcal{E}$*

(c) *Φ is induced by a Hida measure*

Proof. That (c) implies (a) is obvious. To see that (a) $\Rightarrow$ (b), for $k = 1, 2, \ldots, n$, let $\xi_k \in \mathcal{E}$ and $z_k \in \mathbb{C}$. Then

$$\begin{aligned}
\sum_{j,k=1}^{n} z_j \mathcal{T}(\Phi)(\xi_j - \xi_k) \overline{z_k} &= \sum_{j,k=1}^{n} z_j \langle\langle \Phi, e^{i\langle \cdot, \xi_j - \xi_k \rangle} \rangle\rangle \overline{z_k} \\
&= \left\langle\left\langle \Phi, \sum_{j,k=1}^{n} z_j e^{i\langle \cdot, \xi_j - \xi_k \rangle} \overline{z_k} \right\rangle\right\rangle \\
&= \left\langle\left\langle \Phi, \Big| \sum_{k=1}^{n} z_k e^{i\langle \cdot, \xi_k \rangle} \Big|^2 \right\rangle\right\rangle
\end{aligned}$$

Since

$$\Big|\sum_{k=1}^{n} z_k e^{i\langle\cdot,\xi_k\rangle}\Big|^2 = \sum_{j,k=1}^{n} z_j\overline{z_k}e^{i\langle\cdot,\xi_j-\xi_k\rangle}$$

is a nonnegative test function in $(\mathcal{E})$, we have that

$$\sum_{j,k=1}^{n} z_j\mathcal{T}(\Phi)(\xi_j-\xi_k)\overline{z_k}\geq 0$$

by the positivity of Φ. Thus $T(\Phi)$ is positive definite on $\mathcal{E}$.

For (b) $\Rightarrow$ (c), let $\mathcal{T}(\Phi)$ be positive definite on $\mathcal{E}$. Note that if $\xi_n\to\xi$ in $\mathcal{E}$, then $e^{i\langle\cdot,\xi_n\rangle}\to e^{i\langle\cdot,\xi\rangle}$ in $(\mathcal{E})$. Thus

$$\lim_{n\to\infty}\mathcal{T}(\Phi)(\xi_n)=\lim_{n\to\infty}\langle\langle\Phi, e^{i\langle\cdot,\xi_n\rangle}\rangle\rangle=\langle\langle\Phi, e^{i\langle\cdot,\xi\rangle}\rangle\rangle=\mathcal{T}(\Phi)(\xi)$$

Thus $\mathcal{T}(\Phi)$ is continuous on $\mathcal{E}$. Hence by the Minlos Theorem (see Theorem 7.1) there exists a finite measure ν with

$$\langle\langle\Phi, e^{i\langle\cdot,\xi\rangle}\rangle\rangle=\int_{\mathcal{E}'} e^{i\langle x,\xi\rangle}\,d\nu(x)\qquad\text{for all }\xi\in\mathcal{E}\tag{7.1}$$

We need to show that $(\mathcal{E})\subset L^1(\mathcal{E}',\nu)$ and

$$\langle\langle\Phi,\phi\rangle\rangle=\int_{\mathcal{E}'}\phi(x)\,d\nu(x)\qquad\text{for all }\phi\in(\mathcal{E})$$

Let L be the subspace of $(\mathcal{E})$ consisting of the linear span of $\{e^{i\langle\cdot,\xi\rangle}\,;\,\xi\in\mathcal{E}\}$. From (7.1) we see that

$$\langle\langle\Phi,\phi\rangle\rangle=\int_{\mathcal{E}'}\phi(x)\,d\nu(x)\qquad\text{for all }\phi\in L$$

Observe that if $\phi,\psi\in L$, then $\phi\psi\in L$. Most importantly, if $\phi\in L$, then $\overline{\phi}$ is in L and thus $|\phi|^2\in L$. By equation (7.1) above we have

$$\int_{\mathcal{E}'}|\phi(x)|^2\,d\nu(x)=\langle\langle\Phi,|\phi|^2\rangle\rangle<\infty$$

Thus $L\subset L^2(\mathcal{E}',\nu)$.

Now take an arbitrary $\phi\in(\mathcal{E})$. Since L is dense in $(\mathcal{E})$, we can take a sequence $\{\phi_n\}_{n=0}^{\infty}$ with ϕ_n converging to ϕ in $(\mathcal{E})$. Since pointwise multiplication is continuous on $(\mathcal{E})$ (see Remark 5.35) we have that $|\phi_n-\phi|^2\to 0$ in $(\mathcal{E})$ as $n\to\infty$. Therefore $|\phi_n-\phi_m|^2\to 0$ in $(\mathcal{E})$ as $n,m\to\infty$. This gives us

$$\lim_{n,m\to\infty}\langle\langle\Phi,|\phi_n-\phi_m|^2\rangle\rangle=0$$

So we can apply equation (7.1) above to see that

$$\lim_{n,m\to\infty} \int_{\mathcal{E}'} |\phi_n - \phi_m|^2 \, d\nu(x) = \lim_{n,m\to\infty} \langle\langle \Phi, |\phi_n - \phi_m|^2 \rangle\rangle = 0$$

Hence $\{\phi_n\}_{n=0}^{\infty}$ forms a sequence in $L^2(\mathcal{E}', \nu)$. Let ψ be the $L^2(\mathcal{E}', \nu)$ limit of this sequence. That is,

$$\psi = \lim_{n\to\infty} \phi_n \qquad \text{in } L^2(\mathcal{E}', \nu)$$

Since $\phi_n \to \psi$ in $L^2(\mathcal{E}', \nu)$, there exists a subsequence $\{\phi_{n'}\}_{n'=0}^{\infty}$ of $\{\phi_n\}_{n=0}^{\infty}$ such that $\phi_{n'} \to \psi$, ν–almost everywhere.

Now since $\tilde{\delta}_x$ is in $(\mathcal{E})'$ for all $x \in \mathcal{E}'$ (see Section 5.5), we have

$$\lim_{n\to\infty} \phi(x) - \phi_n(x) = \lim_{n\to\infty} \langle\langle \tilde{\delta}_x, \phi - \phi_n \rangle\rangle = 0 \qquad \text{for all } x \in \mathcal{E}'$$

Therefore $\phi_{n'}(x) \to \phi(x)$ for all $x \in \mathcal{E}'$. Thus $\phi = \psi$, ν–almost everywhere. We have shown that $\phi \in L^2(\mathcal{E}', \nu)$ which implies $(\mathcal{E}) \subset L^2(\mathcal{E}', \nu)$. We also have

$$\begin{aligned}
\langle\langle \Phi, \phi \rangle\rangle = \lim_{n'\to\infty} \langle\langle \Phi, \phi_{n'} \rangle\rangle &= \lim_{n'\to\infty} \int_{\mathcal{E}'} \phi_{n'}(x) \, d\nu(x) \\
&= \int_{\mathcal{E}'} \psi(x) \, d\nu(x) \\
&= \int_{\mathcal{E}'} \phi(x) \, d\nu(x)
\end{aligned}$$

Therefore Φ is induced by ν and the proof is complete. □

Corollary 7.13. *Let ν be a finite measure on $\mathcal{E}'$ such that*

$$\langle\langle \Phi, e^{i\langle \cdot, \xi \rangle} \rangle\rangle = \int_{\mathcal{E}'} e^{i\langle x, \xi \rangle} \, d\nu(x)$$

for some $\Phi \in (\mathcal{E})'$. Then Φ is induced by ν, i.e.

$$\langle\langle \Phi, \phi \rangle\rangle = \int_{\mathcal{E}'} \phi \, d\nu$$

for all $\phi \in (\mathcal{E})$.

Proof. Since $\langle\langle \Phi, e^{i\langle \cdot, \xi \rangle} \rangle\rangle = \int_{\mathcal{E}'} e^{i\langle x, \xi \rangle} \, d\nu(x)$ it is clear that $\langle\langle \Phi, e^{i\langle \cdot, \xi \rangle} \rangle\rangle$ is positive definite. So we can apply Theorem 7.12 to get a finite measure m which is induced by Φ. Hence for all $\phi \in (\mathcal{E})$,

$$\langle\langle \Phi, \phi \rangle\rangle = \int_{\mathcal{E}'} \phi \, dm$$

Letting $\phi = e^{i\langle \cdot, \xi \rangle}$ in the above equation, we see that the characteristic functions for m and ν are identical. Therefore $m = \nu$ and we have that Φ is induced by ν. □

The next Theorem demonstrates the relationship between $\tilde{\delta}_V$ and μ_V.

Theorem 7.14. *The delta function of a subspace V is induced by the Gaussian measure on the subspace V, i.e. $(\mathcal{E}) \subset L^1(\mu_V)$ and*

$$\langle\langle \tilde{\delta}_V, \phi \rangle\rangle = \int_{\mathcal{E}'} \phi(x)\, d\mu_V(x) \qquad \textit{for all } \phi \in (\mathcal{E})$$

Proof. We can use the S–transform for $\tilde{\delta}_V$ to see that

$$\langle\langle \tilde{\delta}_V, e^{i\langle \cdot, \xi\rangle_c} \rangle\rangle = e^{-\frac{1}{2}\langle \xi, \xi\rangle_c} S(\tilde{\delta}_V)(i\xi) = e^{-\frac{1}{2}\langle \xi, \xi\rangle_c + \frac{1}{2}\langle \xi_{V^\perp}, \xi_{V^\perp}\rangle_c} = e^{-\frac{1}{2}\langle \xi_V, \xi_V\rangle_c}$$

Thus for any $\xi \in \mathcal{E}$ we have

$$\langle\langle \tilde{\delta}_V, e^{i\langle \cdot, \xi\rangle_c} \rangle\rangle) = C_V(\xi) = \int_{\mathcal{E}'} e^{i\langle x, \xi\rangle}\, d\mu_V(x)$$

Hence, by Corollary 7.13 we have that $\tilde{\delta}_V$ is induced by a Hida measure μ_V. $\square$

This next example provides some insight for the measure μ_V by comparing it to the finite dimensional setting.

Example 7.15. Suppose $V \subset \mathbb{R}^n$. In this finite dimensional setting we have

$$\int_V \delta(v - y)\, dv = \lim_{\varepsilon \to 0} \int_V \frac{1}{(2\pi\varepsilon^2)^{\dim V/2}} e^{-\frac{|v|^2}{2\varepsilon^2}}\, dv = \lim_{\varepsilon \to 0} \frac{e^{-\frac{|y_{V^\perp}|^2}{2\varepsilon^2}}}{(2\pi\varepsilon^2)^{\dim V^\perp/2}}$$

Observe that for a suitably decaying continuous function f we have

$$\begin{aligned}
\int_{\mathbb{R}^n} \int_V \delta(v - y) f(y)\, dv\, dy &= \lim_{\varepsilon \to 0} \int_{\mathbb{R}^n} f(y) \frac{e^{-\frac{|y_{V^\perp}|^2}{2\varepsilon^2}}}{(2\pi\varepsilon^2)^{\dim V^\perp/2}}\, dx \\
&= \lim_{\varepsilon \to 0} \int_V \int_{V^\perp} f(y_V + y_{V^\perp}) \frac{e^{-\frac{|y_{V^\perp}|^2}{2\varepsilon^2}}}{(2\pi\varepsilon^2)^{\dim V^\perp/2}}\, dy_{V^\perp}\, dy_V
\end{aligned}$$

Letting $y_{V^\perp} = \varepsilon x$ we get

$$= \lim_{\varepsilon \to 0} \int_V \int_{V^\perp} f(y_V + \varepsilon x) \frac{e^{-|x|^2/2}}{(2\pi)^{\dim V^\perp/2}}\, dx\, dy_V$$

Using the dominated convergence theorem we obtain

$$\begin{aligned}
&= \int_V \int_{V^\perp} f(y_V) \frac{e^{-|x|^2/2}}{(2\pi)^{\dim V^\perp/2}}\, dx\, dy_V \\
&= \int_V f(y_V)\, dy_V
\end{aligned}$$

For the Gaussian measure on $\mathbb{R}^n$ we replace $f(y)$ in the above with $f(y)e^{-\frac{|y|^2}{2}}(2\pi)^{-n/2}$ to get

$$\int_{\mathbb{R}^n}\int_V (2\pi)^{\dim V^{\perp}/2}\delta(v-y)f(y)\,dv\,d\mu(y) = \int_V f(v)\,d\mu_V(v)$$

where μ and μ_V are the Gaussian measures on $\mathbb{R}^n$ and V, respectively. (See the comment just before section 6.2.1.)

What appears to have happened is that as the variance of the Gaussian measure on $V^{\perp}$ heads to 0, the Gaussian measure on V remains unchanged. With this in mind, we now let V be a possibly infinite dimensional closed subspace of E and consider the characteristic function

$$C_t^{\perp}(\xi) = \exp(-\tfrac{1}{2}|\xi_V|_0^2 - \tfrac{t^2}{2}|\xi_{V^{\perp}}|_0^2) \qquad \xi \in \mathcal{E}$$

Let ρ_t be the measure on $\mathcal{E}'$ corresponding to $C_t^{\perp}$ and $\tilde{\rho}_t$ the corresponding distribution.

Consider the following

$$\begin{aligned} F_t(\xi) = S(\tilde{\rho}_t)(\xi) &= e^{-\frac{1}{2}\langle\xi,\xi\rangle_c}\int_{\mathcal{E}'} e^{\langle y,\xi\rangle_c}d\rho_t(y) \\ &= e^{-\frac{1}{2}\langle\xi,\xi\rangle}e^{\frac{1}{2}\langle\xi_V,\xi_V\rangle_c + \frac{t^2}{2}\langle\xi_{V^{\perp}},\xi_{V^{\perp}}\rangle_c} \\ &= \exp\left[-\tfrac{1}{2}(1-t^2)\langle\xi_{V^{\perp}},\xi_{V^{\perp}}\rangle_c\right] \end{aligned}$$

So we have $\lim_{t\to 0} F_t(\xi) = e^{-\frac{1}{2}\langle\xi_{V^{\perp}},\xi_{V^{\perp}}\rangle} = S(\tilde{\delta}_V)(\xi)$. Also by calculations similar to those in (6.4) we see that for $0 \le t \le 1$,

$$|F_t(\xi)| \le \exp(\tfrac{1}{2}|\xi|_0^2)$$

Therefore we can use Theorem 5.32 to see that $\tilde{\rho}_t \to \tilde{\delta}_V$ in $(\mathcal{E})'$ as $t \to 0$.

7.3 Main Result

In this section we prove the main result of this chapter, which is a rigorous formulation and proof of the identity (6.1) in the infinite dimensional setting. But first we must build upon the notion of S–transform developed in Section 5.4.

7.3.1 S–transform Extension on $(\mathcal{E})$

For $\Phi \in (\mathcal{E})'$ we have the S–transform of Φ given by

$$S\Phi(\xi) = \langle\langle \Phi, :e^{\langle\cdot,\xi\rangle}:\rangle\rangle \qquad \xi \in \mathcal{E}_c$$

If we apply the S–transform to elements $\phi \in (\mathcal{E}) \subset (\mathcal{E})'$, then we can extend the domain of $S\phi(\cdot)$ to include all $x \in \mathcal{E}_c'$. We denote this extension by $\breve{S}\phi$. That is, for $\phi \in (\mathcal{E})$ we define

$$\breve{S}\phi(x) = \langle\langle :e^{\langle\cdot,x\rangle_c}:, \phi\rangle\rangle \qquad x \in \mathcal{E}_c'$$

Remark 7.16. Note that while we are restricting S to $(\mathcal{E})$, for a $\phi \in (\mathcal{E})$ the domain of $\breve{S}\phi$ extends the domain of $S\phi$ from $\mathcal{E}_c$ to $\mathcal{E}_c'$.

Remark 7.17. Let $\phi, \psi \in (\mathcal{E})$. If $\breve{S}(\phi) = \breve{S}(\psi)$, then $\phi = \psi$. This is a consequence of $\breve{S}(\phi) = \breve{S}(\psi)$ implies $S(\phi) = S(\psi)$.

Proposition 7.18. *If $\phi \in (\mathcal{E})$ has Wiener–Itô decomposition given by*

$$\phi = \sum_{n=0}^{\infty} \langle :\cdot^{\otimes n}:, f_n\rangle_c \qquad f_n \in \mathcal{E}_c^{\widehat{\otimes} n}$$

then we have

$$\breve{S}(\phi)(x) = \sum_{n=0}^{\infty} \langle x^{\otimes n}, f_n\rangle_c \qquad x \in \mathcal{E}_c'$$

and the right hand side converges absolutely.

Proof. Using the expansion for ϕ given above and that the Wiener–Itô expansion for $:e^{\langle\cdot,x\rangle_c}:$ is given by $\sum_{n=0}^{\infty} \langle :\cdot^{\otimes n}:, x^{\otimes n}\rangle_c$ (see Definition 5.28), we have that

$$\breve{S}(\phi)(x) = \langle\langle :e^{\langle\cdot,x\rangle_c}:, \phi\rangle\rangle = \sum_{n=0}^{\infty} \langle x^{\otimes n}, f_n\rangle_c$$

So now if $x \in \mathcal{E}_{p,c}'$, then

$$\begin{aligned}
\sum_{n=0}^{\infty} \left|\langle x^{\otimes n}, f_n\rangle_c\right| &\leq \sum_{n=0}^{\infty} |x|_{-p}^n |f_n|_p \\
&\leq \left(\sum_{n=0}^{\infty} \frac{|x|_{-p}^{2n}}{n!}\right)^{\frac{1}{2}} \left(\sum_{n=0}^{\infty} n!|f|_p^{2n}\right)^{\frac{1}{2}} \\
&= \|\phi\|_p \exp(\tfrac{1}{2}|x|_{-p}^2)
\end{aligned}$$

□

In the proof of the above proposition we have established the following:

Corollary 7.19. *Given $\phi \in (\mathcal{E})$, if $x \in \mathcal{E}_{p,c}'$, then*

$$\left|\breve{S}(\phi)(x)\right| \leq \|\phi\|_p \exp(\tfrac{1}{2}|x|_{-p}^2)$$

7.3.2 The Main Identity

Now we would like to show that

$$\int_{\mathcal{E}'} \phi(x)\, d\mu_V(x) = \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\mu_{V^\perp}(y) \tag{7.2}$$

for $\phi \in (\mathcal{E})$, where μ_V and $\mu_{V^\perp}$ are the Gaussian measures on V and $V^\perp$, respectively.

Lemma 7.20. *Equation* (7.2) *holds for* $\phi(x) = :e^{\langle x,\xi\rangle_c}:$, *where* $\xi \in \mathcal{E}_c$.

Proof. For the left–hand side of equation (7.2) we have

$$\int_{\mathcal{E}'} :e^{\langle x,\xi\rangle_c}:\, d\mu_V(x) = e^{-\frac{1}{2}\langle \xi,\xi\rangle_c} e^{\frac{1}{2}\langle \xi_V,\xi_V\rangle_c} = e^{-\frac{1}{2}\langle \xi_{V^\perp},\xi_{V^\perp}\rangle_c} \tag{7.3}$$

Now for the right–hand side of equation (7.2) we first observe that

$$\breve{S}(:e^{\langle \cdot,\xi\rangle_c}:)(-iy) = \langle\langle :e^{\langle \cdot,-iy\rangle_c}:, :e^{\langle \cdot,\xi\rangle_c}:\rangle\rangle = e^{-i\langle y,\xi\rangle_c}$$

by Lemma 5.19. This gives us

$$\int_{\mathcal{E}'} \breve{S}(:e^{\langle \cdot,\xi\rangle_c}:)(-iy)\, d\mu_{V^\perp}(y) = \int_{\mathcal{E}'} e^{-i\langle y,\xi\rangle_c}\, d\mu_{V^\perp}(y) = e^{-\frac{1}{2}\langle \xi_{V^\perp},\xi_{V^\perp}\rangle_c} \tag{7.4}$$

by Proposition 7.9 $\square$

Corollary 7.21. *Equation* (7.2) *holds for functions ϕ in the linear span of* $\{:e^{\langle \cdot,\xi\rangle_c}: ;\ \xi \in \mathcal{E}_c\}$.

We now observe that $\tilde{\delta}_V$ and $\tilde{\delta}_{V^\perp}$ are related through the White Noise version of the Fourier transform (see Section 5.4.3).

Corollary 7.22. *The Fourier transform of $\tilde{\delta}_{V^\perp}$ is $\tilde{\delta}_V$.*

Proof. From Definition 5.33 we have that $S(\mathcal{F}\tilde{\delta}_{V^\perp})(\xi) = \langle\langle \tilde{\delta}_{V^\perp}, e^{-i\langle \cdot,\xi\rangle_c}\rangle\rangle$. Now we apply Theorem 7.14 to get that

$$\begin{aligned}
\langle\langle \tilde{\delta}_{V^\perp}, e^{-i\langle \cdot,\xi\rangle_c}\rangle\rangle &= \int_{\mathcal{E}'} e^{-i\langle x,\xi\rangle_c}\, d\mu_{V^\perp}(x) \\
&= \int_{\mathcal{E}'} :e^{\langle x,\xi\rangle_c}:\, d\mu_V(x) \qquad \text{using (7.3) and (7.4)} \\
&= S(\tilde{\delta}_V)(\xi) \qquad \text{again applying Theorem 7.14}
\end{aligned}$$

Therefore for any $\xi \in \mathcal{E}_c$ we have that $S(\mathcal{F}\tilde{\delta}_{V^\perp})(\xi) = S(\tilde{\delta}_V)(\xi)$, from which we conclude that $\mathcal{F}\tilde{\delta}_{V^\perp} = \tilde{\delta}_V$ $\square$

In order to prove the main result we need the following theorem:

Theorem 7.23. *Let ν be a Hida measure on $\mathcal{E}'$. Then ν is supported in $\mathcal{E}'_p$ for some $p \geq 1$ and*

$$\int_{\mathcal{E}'_p} \exp\left(\tfrac{1}{2}|x|^2_{-p}\right) d\nu(x) < \infty$$

The proof of this theorem can be found on page 332, Theorem 15.15 in [17].

Using this, we can prove the result we are after

Theorem 7.24. *Let $\phi \in (\mathcal{E})$. Then*

$$\int_{\mathcal{E}'} \phi \, d\mu_V = \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\mu_{V^\perp}(y)$$

Proof. Let L be the linear span of $\{: e^{\langle \cdot, \xi \rangle_c} : ; \xi \in \mathcal{E}\}$. Take $\phi_n \in L$ such that ϕ_n converges to ϕ in $(\mathcal{E})$ as $n \to \infty$. Then we have

(7.5)

$$\begin{aligned}
\left| \int_{\mathcal{E}'} \breve{S}(\phi_n)(-iy)\, d\mu_{V^\perp}(y) - \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\mu_{V^\perp}(y) \right| & \\
\leq \int_{\mathcal{E}'} \left| \breve{S}(\phi_n - \phi)(-iy) \right| d\mu_{V^\perp}(y) & \\
\leq \|\phi_n - \phi\|_p \int_{\mathcal{E}'} \exp(\tfrac{1}{2}|y|^2_{-p})\, d\mu_{V^\perp}(y) & \qquad \text{by Corollary 7.19}
\end{aligned}$$

By Theorem 7.23 we can choose p so that $\int_{\mathcal{E}'_p} \exp(\frac{1}{2}|y|^2_{-p})\, d\mu_{V^\perp}(y)$ is finite. With such a p we see that the last term goes to 0 as $n \to \infty$.

Therefore

$$\begin{aligned}
\int_{\mathcal{E}'} \phi(x)\, d\mu_V(x) &= \lim_{n\to\infty} \int_{\mathcal{E}'} \phi_n(x)\, d\mu_V(x) \qquad \text{since } \mu_V \text{ is a Hida measure} \\
&= \lim_{n\to\infty} \int_{\mathcal{E}'} \breve{S}(\phi_n)(-iy)\, d\mu_{V^\perp}(y) \qquad \text{by Corollary 7.21} \\
&= \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\mu_{V^\perp}(y) \qquad \text{by (7.5) above}
\end{aligned}$$

□

7.3.3 A Slight Generalization

Theorem 7.24 can be extended to include all Hida measures. Given a Hida measure ν on $\mathcal{E}'$, we can think of ν as an element in $(\mathcal{E})'$ as follows:

$$\langle\langle \tilde{\nu}, \phi \rangle\rangle = \int_{\mathcal{E}'} \phi \, d\nu(x) \qquad \phi \in (\mathcal{E})$$

Thus we can take the Fourier transform $\mathcal{F}\tilde{\nu}$ of the distribution $\tilde{\nu}$. Motivated by Corollary 7.22 we rewrite the identity in equation (7.2) as follows

$$\langle\langle \mathcal{F}\tilde{\nu}, \phi\rangle\rangle = \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\nu(y) \tag{7.6}$$

Lemma 7.25. *Equation* (7.6) *holds for* $\phi(x) =: e^{\langle x,\xi\rangle_c}:$, *where* $\xi \in \mathcal{E}_c$.

Proof. The left–hand side is

$$\langle\langle \mathcal{F}\tilde{\nu}, \phi\rangle\rangle = S(\mathcal{F}\tilde{\nu})(\xi) = \langle\langle \tilde{\nu}, e^{-i\langle\cdot,\xi\rangle_c}\rangle\rangle$$

by definition of the Fourier transform. The right–hand side gives

$$\int_{\mathcal{E}'} \breve{S}(:e^{\langle\cdot,\xi\rangle_c}:)(-iy)\, d\nu(y) = \int_{\mathcal{E}'} \langle\langle :e^{\langle\cdot,-iy\rangle_c}:, :e^{\langle\cdot,\xi\rangle_c}:\rangle\rangle d\nu(y) = \int_{\mathcal{E}'} e^{-i\langle y,\xi\rangle_c}\, d\nu(y)$$

And we have $\langle\langle \tilde{\nu}, e^{-i\langle\cdot,\xi\rangle_c}\rangle\rangle = \int_{\mathcal{E}'} e^{-i\langle y,\xi\rangle_c}\, d\nu(y)$. Therefore the equation holds. □

Corollary 7.26. *Equation* (7.6) *holds for functions* ϕ *in the linear span of* $\{:e^{\langle\cdot,\xi\rangle_c}: ; \xi \in \mathcal{E}_c\}$.

Now we can prove (7.6) for all test functions

Theorem 7.27. *Let* $\phi \in (\mathcal{E})$. *Then*

$$\langle\langle \mathcal{F}\tilde{\nu}, \phi\rangle\rangle = \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\nu(y)$$

Proof. Let L be the linear span of $\{: e^{\langle\cdot,\xi\rangle_c} : ; \xi \in \mathcal{E}\}$. Take $\phi_n \in L$ such that ϕ_n converges to ϕ in $(\mathcal{E})$ as $n \to \infty$. Then we see that

$$\begin{aligned}
&\left| \int_{\mathcal{E}'} \breve{S}(\phi_n)(-iy)\, d\nu(y) - \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\nu(y) \right| \\
&\qquad\qquad \le \int_{\mathcal{E}'} \left|\breve{S}(\phi_n - \phi)(-iy)\right| d\nu(y) \\
&\qquad\qquad \le \|\phi_n - \phi\|_p \int_{\mathcal{E}'_p} \exp(\tfrac{1}{2}|y|^2_{-p})\, d\nu(y) \qquad \text{by Corollary 7.19}
\end{aligned} \tag{7.7}$$

By Theorem 7.23 we can choose p so that $\int_{\mathcal{E}'_p} \exp(\frac{1}{2}|y|^2_{-p})\, d\nu(y)$ is finite. With such a p the last term goes to 0 as $n \to \infty$

Therefore

$$\begin{aligned}
\langle\langle \mathcal{F}\tilde{\nu}, \phi\rangle\rangle &= \lim_{n\to\infty} \langle\langle \mathcal{F}\tilde{\nu}, \phi_n\rangle\rangle \\
&= \lim_{n\to\infty} \int_{\mathcal{E}'} \breve{S}(\phi_n)(-iy)\, d\nu(y) \quad \text{by Corollary 7.26} \\
&= \int_{\mathcal{E}'} \breve{S}(\phi)(-iy)\, d\nu(y) \quad \text{by (7.7) above}
\end{aligned}$$

□

Chapter 8

Rigorous Hidden Subspace Algorithm

In this chapter we use the theory of white noise analysis to develop a mathematically rigorous formulation of the quantum hidden subspace algorithm which was first described in Section 3.6. In order to do this we must develop yet another Gaussian measure—this time on the space $\mathcal{E}'_c$.

8.1 The Gaussian Measure on $\mathcal{E}'_c$

In Section 5.1 we defined the Hilbert spaces $\mathcal{E}_p$ and used them to form the nuclear space $\mathcal{E}$. Then we were able to construct the Gaussian measure on $\mathcal{E}'$, the dual of $\mathcal{E}$.

Recall that for each Hilbert space $\mathcal{E}_p$ we have the complexification $\mathcal{E}_{p,c}$ and the norm $|\cdot|_p$ on $\mathcal{E}_p$ which induces a norm $|\cdot|_p$ on $\mathcal{E}_{p,c}$ such that

$$|\xi + i\eta|_p^2 = |\xi|_p^2 + |\eta|_p^2 \qquad \xi, \eta \in \mathcal{E}_p$$

Likewise we also have that the inner–product $\langle \cdot, \cdot \rangle_p$ on $\mathcal{E}_p$ induces a real inner–product $\langle \cdot, \cdot \rangle_p$ on $\mathcal{E}_{p,c}$ given by

$$\langle \xi_1 + i\eta_1, \xi_2 + i\eta_2 \rangle_p = \langle \xi_1, \xi_2 \rangle_p + \langle \eta_1, \eta_2 \rangle_p$$

where $\xi_1, \xi_2, \eta_1, \eta_2 \in \mathcal{E}_{p,c}$. Having that the inclusion map $\mathcal{E}_{p+1} \hookrightarrow \mathcal{E}_p$ is Hilbert–Schmidt gives us that each inclusion $\mathcal{E}_{p+1,c} \hookrightarrow \mathcal{E}_{p,c}$ is Hilbert–Schmidt. Therefore, it follows that $\mathcal{E}_c$, is a nuclear space with topology induced by the norms $\{|\cdot|_p\}_{p=0}^{\infty}$. Moreover,

$$\mathcal{E}_c = \bigcap_{p=0}^{\infty} \mathcal{E}_{p,c}$$

We also have the dual $\mathcal{E}'_c$ with

$$\mathcal{E}'_c = \bigcup_{p=0}^{\infty} \mathcal{E}'_{p,c}$$

The bilinear pairing $\langle \cdot, \cdot \rangle$ between $\mathcal{E}$ and $\mathcal{E}'$ extends to a real bilinear pairing between $\mathcal{E}_c$ and $\mathcal{E}'_c$. Letting $z = x + iy$ with $x, y \in \mathcal{E}'$ and $\zeta = \xi + i\eta$ with $\xi, \eta \in \mathcal{E}$ we see that this pairing is given by

$$\langle z, \zeta \rangle = \langle x, \xi \rangle + \langle y, \eta \rangle$$

Note that the bilinear pairing given above is simply the real part of $\langle z, \overline{\zeta} \rangle_c$ where $\overline{\zeta}$ denoes the conjugate of ζ (i.e. if $\zeta = \xi + i\eta$ with $\xi, \eta \in \mathcal{E}$, then $\overline{\zeta} = \xi - i\eta$).

We can now use a construction similar to that in Section 5.1 or use the Minlos theorem (see Theorem 7.1) to get a measure μ_c on $\mathcal{E}'_c$ such that

$$\int_{\mathcal{E}'_c} e^{i\hat{\zeta}(z)}\, d\mu_c(z) = \int_{\mathcal{E}'_c} e^{i\langle z, \zeta \rangle}\, d\mu_c(z) = e^{-|\zeta|_0^2/4} \tag{8.1}$$

for all $\zeta \in \mathcal{E}_c$. Here if $\zeta = \xi + i\eta$, then $\hat{\zeta}$ denotes the real random variable given by

$$\hat{\zeta}(x + iy) = \langle x, \xi \rangle + \langle \eta, y \rangle \qquad \text{for all } x, y \in \mathcal{E}'$$

where $\hat{\xi}$ and $\hat{\eta}$ are defined as in Section 5.1.

8.1.1 Properties of the Gaussian Measure on $\mathcal{E}'_c$

Here we present some standard results about the Gaussian measure μ_c defined on the dual of $\mathcal{E}_c$. In particular we will see that the product measure $\mu_{1/2} \otimes \mu_{1/2}$ on $\mathcal{E}'_c = \mathcal{E}' + i\mathcal{E}'$ is equivalent to the measure μ_c.

Lemma 8.1. *Let $\zeta_1, \zeta_2, \ldots, \zeta_n \in \mathcal{E}_c$ be an orthonormal system for E_c. Then the image of the Gaussian measure μ_c under the map*

$$z \mapsto (\langle z, \zeta_1 \rangle, \cdots, \langle z, \zeta_n \rangle) \in \mathbb{R}^n, \qquad z \in \mathcal{E}'_c$$

is the Gaussian measure on $\mathbb{R}^n$ with mean 0 and variance $\frac{1}{2}$ (i.e. the probability measure with distribution function $\pi^{-n/2} e^{-|t|^2}$).

Proof. Let ν denote the image of μ_c under the above map. So ν is a probability measure on $\mathbb{R}^n$. Computing the characteristic function of ν we see

$$\begin{aligned}
\hat{\nu}(s) = \int_{\mathbb{R}^n} e^{i\langle s, t \rangle} d\nu(t) &= \int_{\mathcal{E}'_c} \exp\Big(i \sum_{k=1}^n s_k \langle z, \zeta_k \rangle\Big) d\mu_c(z) \\
&= \exp\Big(-\tfrac{1}{4}\Big|\sum_{k=1}^n s_k \zeta_k\Big|_0^2\Big) \\
&= \exp\Big(-\tfrac{1}{4} \sum_{i,j=1}^n s_i s_j \langle \zeta_i, \zeta_j \rangle\Big) \\
&= \exp\big(-\tfrac{1}{4}|s|^2\big)
\end{aligned}$$

which is the characteristic function of the Gaussian measure on $\mathbb{R}^n$ with mean 0 and variance $\frac{1}{2}$. $\square$

Lemma 8.2. *Let $\zeta_1, \zeta_2, \dots, \zeta_n \in \mathcal{E}_c$ be an orthonormal system for E_c. For any Gaussian integrable functions $f_1, f_2, \dots, f_n$ on $\mathbb{R}$ we have*

$$\int_{\mathcal{E}_c'} f_1(\langle z, \zeta_1 \rangle) \cdots f_n(\langle z, \zeta_n \rangle) \, d\mu_c(z) = \prod_{k=1}^{n} \int_{\mathcal{E}_c'} f_k(\langle z, \zeta_k \rangle) \, d\mu_c(z)$$

Proof. Apply Lemma 8.1. □

Lemma 8.3. *For any $\zeta \in \mathcal{E}_c$ and $n = 0, 1, 2, \dots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}_c'} |\langle z, \zeta \rangle|^2 \, d\mu_c(z) = |\zeta|_0^2$

(b) $\displaystyle\int_{\mathcal{E}_c'} e^{\langle z, \zeta \rangle} \, d\mu_c(z) = e^{|\zeta|_0^2/4}$

Proof. The identities obviously hold when $\zeta = 0$. So we take $\zeta \in \mathcal{E}_c$ with $\zeta \neq 0$. By Lemma 8.1 we have that

$$\int_{\mathcal{E}_c'} |\langle z, \zeta \rangle|^2 \, d\mu_c(z) = |\zeta|_0^2 \int_{\mathcal{E}_c'} \left| \left\langle z, \frac{\zeta}{|\zeta|_0} \right\rangle \right|^2 d\mu_c(z) = \frac{|\zeta|_0^2}{\sqrt{\pi}} \int_{\mathbb{R}} t^2 e^{-t^2} dt$$

And letting $s = \sqrt{2} t$ we have

$$\frac{|\zeta|_0^2}{\sqrt{\pi}} \int_{\mathbb{R}} t^2 e^{-t^2} \, dt = \frac{|\zeta|_0^2}{2\sqrt{\pi}} \int_{\mathbb{R}} s^2 e^{-s^2/2} \sqrt{2} \, ds = \frac{|\zeta|_0^2}{\sqrt{2\pi}} \int_{\mathbb{R}} s^2 e^{-s^2/2} \, ds = |\zeta|_0^2$$

This gives us the indentity in (a). Using Lemma 8.1 the second identity is obvious. □

As before, we can now define $\langle \cdot, \zeta \rangle$ for any $\zeta \in E_c$ as a μ_c–almost everywhere defined function of $z \in \mathcal{E}_c'$ in $L^2(\mathcal{E}_c', \mu_c)$, the space of all functions $f : \mathcal{E}_c' \to \mathbb{C}$ which are L^2 integrable with respect to μ_c. Take a sequence $\{\zeta_n\}_{n=1}^{\infty}$ in $\mathcal{E}_c$ such that $\lim_{n\to\infty} |\zeta - \zeta_n|_0 = 0$. Using Lemma 8.3 we can see that the functions $\{\langle \cdot, \zeta_n \rangle\}_{n=1}^{\infty}$ form a Cauchy sequence in $L^2(\mathcal{E}_c', \mu_c)$. Thus there exists a $\phi \in L^2(\mathcal{E}_c', \mu_c)$ such that $\lim_{n\to\infty} \langle \cdot, \zeta_n \rangle = \phi$. We denote such a ϕ by $\langle \cdot, \zeta \rangle$.

Proposition 8.4. *For any $\zeta \in E_c$ and $n = 0, 1, 2, \dots$ we have the following:*

(a) $\displaystyle\int_{\mathcal{E}_c'} |\langle z, \zeta \rangle|^2 \, d\mu_c(z) = |\zeta|_0^2$

(b) $\displaystyle\int_{\mathcal{E}_c'} e^{\langle z, \zeta \rangle} \, d\mu_c(z) = e^{|\zeta|_0^2/4}$

Proof. It is easily shown that Lemmas 8.1 and 8.2 are true when $\zeta_1, \zeta_2, \dots, \zeta_n$ are in E_c. Using this, we can mimic the proof of Lemma 8.3 to get the identities. □

Just as we have formed the measure μ on $\mathcal{E}'$, we can use the Minlos theorem (Theorem 7.1) or a construction similar to that found in Section 5.1 to form the Gaussian measure $\mu_{1/2}$ on $\mathcal{E}'$ with mean 0 and variance $\frac{1}{2}$. That is,

$$\int_{\mathcal{E}'} e^{i\langle x,\xi\rangle}\, d\mu_{1/2}(x) = e^{-|\xi|_0^2/4}$$

for all $\xi \in \mathcal{E}$. And by making the identification $\mathcal{E}'_c = \mathcal{E}' \oplus \mathcal{E}'$ we have the product measure $\mu_{1/2} \otimes \mu_{1/2}$ on $\mathcal{E}'_c$. Now observe, letting $\zeta = \xi + i\eta$ with $\xi, \eta \in \mathcal{E}$, we have

$$\int_{\mathcal{E}'_c} e^{i\langle x+iy,\zeta\rangle}\, d\mu_{1/2}(x) \otimes d\mu_{1/2}(y) = \int_{\mathcal{E}'_c} e^{i\langle x+iy,\xi+i\eta\rangle}\, d\mu_{1/2}(x) \otimes d\mu_{1/2}(y)$$

Using the definition of the real inner–product $\langle\cdot,\cdot\rangle$ we get

$$= \int_{\mathcal{E}'_c} e^{i\langle x,\xi\rangle} e^{i\langle y,\eta\rangle}\, d\mu_{1/2}(x) \otimes d\mu_{1/2}(y)$$

Now we apply Fubini's theorem to arrive at

$$\begin{aligned} &= \int_{\mathcal{E}'} e^{i\langle x,\xi\rangle}\, d\mu_{1/2}(x) \int_{\mathcal{E}'} e^{i\langle y,\eta\rangle}\, d\mu_{1/2}(y) \\ &= e^{-|\xi|_0^2/4} e^{-|\eta|_0^2/4} \\ &= e^{-|\zeta|_0^2/4} \end{aligned}$$

Comparing this with equation (8.1), we have that the characteristic functions for $\mu_{1/2} \otimes \mu_{1/2}$ and μ_c are equal. Thus $\mu_{1/2} \otimes \mu_{1/2}$ and μ_c are equivalent as measures on $\mathcal{E}'_c$. Let us mention that because the topology on $\mathcal{E}'$ (and $\mathcal{E}'_c$) has a countable basis, the Borel σ–algebra on $\mathcal{E}' \otimes \mathcal{E}'$ is equal to the product σ–algebra.

Proposition 8.5. *For any $\zeta_1, \zeta_2 \in E_c$ we have that*

$$\int_{\mathcal{E}'_c} e^{\langle z,\zeta_1\rangle_c} \overline{e^{\langle z,\zeta_2\rangle_c}}\, d\mu_c(z) = e^{\langle \zeta_1,\overline{\zeta_2}\rangle_c}$$

Proof. Let $\zeta_1 = \xi_1 + i\eta_1$ and $\zeta_2 = \xi_2 + i\eta_2$ where $\xi_1, \xi_2, \eta_1, \eta_2 \in E$. Then letting $z = x + iy$ we have

$$\begin{aligned} \int_{\mathcal{E}'_c} e^{\langle z,\zeta_1\rangle_c} \overline{e^{\langle z,\zeta_2\rangle_c}}\, d\mu_c(z) &= \int_{\mathcal{E}'_c} e^{\langle x+iy,\xi_1+i\eta_1\rangle_c} \overline{e^{\langle x+iy,\xi_2+i\eta_2\rangle_c}}\, d\mu_{1/2}(x) \otimes d\mu_{1/2}(y) \\ &= \int_{\mathcal{E}'_c} e^{\langle x,\xi_1\rangle - \langle y,\eta_1\rangle + i\langle x,\eta_1\rangle + i\langle y,\xi_1\rangle} \overline{e^{\langle x,\xi_2\rangle - \langle y,\eta_2\rangle + i\langle x,\eta_2\rangle + i\langle y,\xi_2\rangle}}\, d\mu_{1/2}(x) \otimes d\mu_{1/2}(y) \\ &= \int_{\mathcal{E}'} e^{\langle x,\xi_1+\xi_2+i\eta_1-i\eta_2\rangle_c}\, d\mu_{1/2}(x) \int_{\mathcal{E}'} e^{\langle y,-\eta_1-\eta_2+i\xi_1-i\xi_2\rangle_c}\, d\mu_{1/2}(y) \\ &= e^{\frac{1}{4}\langle \xi_1+\xi_2+i\eta_1-i\eta_2,\xi_1+\xi_2+i\eta_1-i\eta_2\rangle_c} e^{\frac{1}{4}\langle -\eta_1-\eta_2+i\xi_1-i\xi_2,-\eta_1-\eta_2+i\xi_1-i\xi_2\rangle_c} \end{aligned}$$

Using the observation that the algebra in the horrid exponent of the last term works just as if $\xi_1, \xi_2, \eta_1, \eta_2$ were real numbers and $\langle \cdot, \cdot \rangle_c$ were multiplication of ordinary complex numbers, after a little work the exponent becomes

$$\langle \xi_1, \xi_2 \rangle + \langle \eta_1, \eta_2 \rangle + i\big(\langle \xi_1, \eta_2 \rangle - \langle \eta_1, \xi_2 \rangle\big)$$

which is equal to $\langle \zeta_1, \overline{\zeta_2} \rangle_c$. Thus

$$\int_{\mathcal{E}'_c} e^{\langle z, \zeta_1 \rangle_c} \overline{e^{\langle z, \zeta_2 \rangle_c}} \, d\mu_c(z) = e^{\langle \zeta_1, \overline{\zeta_2} \rangle_c}$$

□

8.1.2 Relationship with $L^2(\mathcal{E}', \mu)$

Up until now we have developed the space $L^2(\mathcal{E}'_c, \mu_c)$. However we will be primarily concerned with a subspace of $L^2(\mathcal{E}'_c, \mu_c)$. We define this subspace as follows:

$$HL^2(\mu_c) = \text{closed linear span of} \quad \{e^{\langle \cdot, \zeta \rangle_c} \; ; \zeta \in \mathcal{E}_c\} \quad \text{in } L^2(\mathcal{E}'_c, \mu_c)$$

Remark 8.6. The reason for the notation $HL^2(\mu_c)$ is that it can be shown that $HL^2(\mu_c)$ contains all $L^2(\mathcal{E}'_c, \mu_c)$–functions of the form

$$H(\langle \cdot, \zeta_1 \rangle_c, \ldots, \langle \cdot, \zeta_n \rangle_c)$$

where $\zeta_1, \ldots, \zeta_n \in E_c$ and H is a holomorpic function on $\mathbb{C}^n$. (For a proof of this, refer to [1]).

For $\Phi \in (\mathcal{E})'$ we have the S–transform of Φ given by

$$S\Phi(\zeta) = \langle\langle \Phi, :e^{\langle \cdot, \zeta \rangle_c}: \rangle\rangle \qquad \zeta \in \mathcal{E}_c$$

In Section 7.3.1 we saw that for $\phi \in (\mathcal{E})$ the S–transform has an extension $\breve{S}$ where

$$\breve{S}(\phi)(z) = \langle\langle \phi, :e^{\langle \cdot, z \rangle_c}: \rangle\rangle \qquad z \in \mathcal{E}'_c$$

Taking $\phi = :e^{\langle \cdot, \zeta \rangle_c}:$ for some $\zeta \in \mathcal{E}_c$ we see that

$$\breve{S}(:e^{\langle \cdot, \zeta \rangle_c}:)(z) = \langle\langle :e^{\langle \cdot, \zeta \rangle_c}:, :e^{\langle \cdot, z \rangle_c}: \rangle\rangle = e^{\langle z, \zeta \rangle_c} \qquad z \in \mathcal{E}'_c$$

Thus $\breve{S}$ maps the linear span of $\{:e^{\langle \cdot, \zeta \rangle_c}: \; ; \zeta \in \mathcal{E}_c\} \subset L^2(\mathcal{E}', \mu)$ into the linear span of $\{e^{\langle \cdot, \zeta \rangle_c} \; ; \zeta \in \mathcal{E}_c\} \subset HL^2(\mu_c)$ by

$$\breve{S}(:e^{\langle \cdot, \zeta \rangle_c}:) = e^{\langle \cdot, \zeta \rangle_c} \qquad \zeta \in \mathcal{E}_c \tag{8.2}$$

It turns out that the S–transform, or more appropriately $\breve{S}$, can be extended to a unitary isomorphism between $L^2(\mathcal{E}', \mu)$ and $HL^2(\mu_c)$, which we denote by U_S.

Theorem 8.7. *There is a unique unitary isomorphism $U_S : L^2(\mathcal{E}', \mu) \to HL^2(\mu_c)$ such that*

$$U_S(:e^{\langle \cdot, \zeta \rangle_c}:) = e^{\langle \cdot, \zeta \rangle_c} \qquad \textit{for all } \zeta \in E_c$$

This is called the Segal-Bargmann transform*.*

Proof. Take $\zeta_1, \zeta_2 \in \mathcal{E}_c$. Then

$$\langle\langle :e^{\langle \cdot, \zeta_1 \rangle_c}:, :e^{\langle \cdot, \zeta_2 \rangle_c}: \rangle\rangle_{L^2(\mathcal{E}', \mu)} = \int_{\mathcal{E}'_c} :e^{\langle x, \zeta_1 \rangle_c}: \overline{:e^{\langle x, \zeta_2 \rangle_c}:}\, d\mu(x)$$

Using Proposition 5.27 we see that $\overline{:e^{\langle x, \zeta_2 \rangle_c}:} =:e^{\langle x, \overline{\zeta_2} \rangle_c}:$. Hence the above becomes

$$\begin{aligned} &= \int_{\mathcal{E}'_c} :e^{\langle x, \zeta_1 \rangle_c}::e^{\langle x, \overline{\zeta_2} \rangle_c}:\ d\mu(x) \\ &= e^{\langle \zeta_1, \overline{\zeta_2} \rangle_c} \qquad \text{by Lemma 5.19} \end{aligned}$$

Thus, by Proposition 8.5 we have

$$\langle\langle :e^{\langle \cdot, \zeta_1 \rangle_c}:, :e^{\langle \cdot, \zeta_2 \rangle_c}: \rangle\rangle_{L^2(\mathcal{E}', \mu)} = \langle\langle e^{\langle \cdot, \zeta_1 \rangle_c}, e^{\langle \cdot, \zeta_2 \rangle_c} \rangle\rangle_{L^2(\mathcal{E}'_c, \mu_c)}$$

for any $\zeta_1, \zeta_2 \in \mathcal{E}_c$. Therefore U_S is a unitary transformation between the linear span of $\{:e^{\langle \cdot, \zeta \rangle_c}: \,;\, \zeta \in \mathcal{E}_c\} \subset L^2(\mathcal{E}', \mu)$ and the linear span of $\{e^{\langle \cdot, \zeta \rangle_c} \,; \zeta \in \mathcal{E}_c\} \subset HL^2(\mu_c)$.

Recall that the set $\{:e^{\langle \cdot, \zeta \rangle_c}: \,;\, \zeta \in \mathcal{E}_c\}$ is dense in $L^2(\mathcal{E}', \mu)$ by Corollary 5.26 and the set $\{e^{\langle \cdot, \zeta \rangle_c} \,; \zeta \in \mathcal{E}_c\}$ is dense in $HL^2(\mu_c)$ by definition. Therefore we have that U_S extends to a unitary isomorphism from $L^2(\mathcal{E}', \mu)$ onto $HL^2(\mu_c)$.

Let $\zeta \in E_c$. Using the conitinuity of U_S we can take a sequence $\{\zeta_n\}_{n=0}^{\infty}$ in $\mathcal{E}_c$ with $\zeta_n \to \zeta$ in E_c to see that:

$$U_S(:e^{\langle \cdot, \zeta \rangle_c}:) = \lim_{n \to \infty} U_S(:e^{\langle \cdot, \zeta_n \rangle_c}:) = \lim_{n \to \infty} e^{\langle \cdot, \zeta_n \rangle_c} = e^{\langle \cdot, \zeta \rangle_c}$$

□

8.2 Independence and Products for U_S

Recall that for each $\xi \in E$ we have the μ–almost everywhere defined random variable

$$\hat{\xi} = \langle \cdot, \xi \rangle$$

with mean and variance given by

$$\int_{\mathcal{E}'} \langle x, \xi \rangle\, d\mu(x) = 0 \qquad \text{and} \qquad \int_{\mathcal{E}'} |\langle x, \xi \rangle|^2\, d\mu(x) = |\xi|_0^2$$

respectively (see Proposition 5.6). Now let V be a closed subspace of E and let σ_V be the completed σ–algebra generated by the random variables $\langle \cdot, v\rangle$ with $v \in V$. Let V and W be orthogonal subspaces of E. For $v \in V$ and $w \in W$, the random variables $\langle \cdot, v\rangle$ and $\langle \cdot, w\rangle$ are independent by Lemma 5.3. Therefore the σ–algebras generated by σ_V and σ_W are independent relative to μ. It follows that the map

$$j_{VW} : L^2(\mathcal{E}', \mu|\sigma_V) \otimes L^2(\mathcal{E}', \mu|\sigma_W) \to L^2(\mathcal{E}', \mu) : f \otimes g \mapsto fg \tag{8.3}$$

is a unitary ismorphism onto $L^2(\mathcal{E}', \mu|\sigma_{V+W})$.

Lemma 8.8. *The linear span of* $\{:e^{\langle \cdot, v\rangle}:;\ v \in V\}$ *is dense in* $L^2(\mathcal{E}', \mu|\sigma_V)$.

Proof. Take an arbitrary $\phi \in L^2(\mathcal{E}', \mu|\sigma_V)$. It is sufficient to show that $\langle\langle \phi, :e^{\langle \cdot, v\rangle}:\rangle\rangle =$ 0 for all $v \in V$ implies $\phi = 0$. Suppose ϕ has Wiener–Itô expansion given by

$$\Phi = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, F_n\rangle_c$$

. Then by Theorem 5.17 $\langle\langle \phi, :e^{\langle \cdot, v\rangle}:\rangle\rangle$ is given by

$$\langle\langle \phi, :e^{\langle \cdot, v\rangle}:\rangle\rangle = \sum_{n=0}^{\infty} \langle F_n, v^{\otimes n}\rangle_c, \qquad v \in V$$

Since $\langle\langle \phi, :e^{\langle \cdot, tv\rangle}:\rangle\rangle = 0$, we have for any real t

$$\langle\langle \phi, :e^{\langle \cdot, tv\rangle}:\rangle\rangle = \sum_{n=0}^{\infty} t^n \langle F_n, v^{\otimes n}\rangle_c = 0$$

Therefore $F_0 = 0$ and inductively, $\langle F_n, v^{\otimes n}\rangle_c = 0$ for all $v \in V$. Since F_n is a symmetric n–linear map we can apply the polarization identity to see that

$$\langle F, v_1 \widehat{\otimes} \cdots \widehat{\otimes} v_n\rangle_c = \frac{1}{n!} \sum_{k=1}^{n} (-1)^{n-k} \sum_{j_1 < \cdots < j_k} \langle F_n, (v_{j_1} + \cdots v_{j_k})^{\otimes n}\rangle_c = 0$$

So $F_n = 0$ for all $n \geq 0$. Hence $\phi = 0$. □

Theorem 8.9. *If V and W are closed orthogonal subspaces of E, then for any $\phi_V \in L^2(\mathcal{E}', \mu|\sigma_V)$ and $\phi_W \in L^2(\mathcal{E}', \mu|\sigma_W)$,*

$$U_S(\phi_V \phi_W) = U_S(\phi_V) U_S(\phi_W)$$

Proof. By Lemma 8.8 $\{: e^{\langle \cdot, v\rangle}:;\ v \in V\}$ spans a dense subspace of $L^2(\mathcal{E}', \mu|\sigma_V)$ and $\{:e^{\langle \cdot, w\rangle}:;\ w \in W\}$ spans a dense subspace of $L^2(\mathcal{E}', \mu|\sigma_W)$. Since U_S is continuous we may assume $\phi_V = :e^{\langle \cdot, v\rangle}:$ and $\phi_W = :e^{\langle \cdot, w\rangle}:$ for some $v \in V$ and some $w \in W$. Now

$$\begin{aligned} U_S(\phi_V \phi_W) &= U_S(:e^{\langle \cdot, v+w\rangle}:) && \text{since } v \text{ and } w \text{ are orthogonal} \\ &= e^{\langle \cdot, v+w\rangle_c} && \text{by Theorem 8.7} \\ &= e^{\langle \cdot, v\rangle_c} e^{\langle \cdot, w\rangle_c} \\ &= U_S(:e^{\langle \cdot, v\rangle}:) U_S(:e^{\langle \cdot, w\rangle}:) && \text{again by Theorem 8.7} \end{aligned}$$

□

8.3 Hidden Subspace Algorithm

Here we use the concepts developed throughout this chapter to present a mathematically rigorous formulation of the hidden subspace algorithm.

Suppose we have a functional $\phi : E \to \mathbb{R}^n$ with a hidden closed subspace $V \subset E$ such that

$$\phi(\xi + v) = \phi(\xi) \qquad \text{for all } v \in V$$

We would like to determine V to some extent. First we can extend ϕ to the domain E_c, as follows: For $\zeta = \xi + i\eta$ with $\xi, \eta \in E$, we define

$$\phi(\zeta) = \phi(\xi) + \phi(\eta)$$

And of course we have

$$\phi(\zeta + v) = \phi(\zeta) \qquad \text{for all } v \in V_c$$

In the original algorithm we used two rigged Hilbert spaces. The first we denoted by H_E. In our version the space H_E becomes the Hilbert space $L^2(\mathcal{E}', \mu)$ (or one of the unitarily isomorphic spaces $HL^2(\mu_c)$ or $\Gamma(E)$). The original algorithm also made use of the rigged Hilbert space $H_{\mathbb{R}^n}$. We now define $H_{\mathbb{R}^n}$ to be the space of all complex functions f on $\mathbb{R}^n$ such that $f \neq 0$ at only a countable number of points and $\sum_{x\in\mathbb{R}^n} |f(x)|^2 < \infty$. Equip $H_{\mathbb{R}^n}$ with the inner–product

$$(f, g) = \sum_{x\in\mathbb{R}^n} f(x)\overline{g(x)}$$

This makes $H_{\mathbb{R}^n}$ a non–separable Hilbert space. For $H_{\mathbb{R}^n}$ we have orthonormal basis given by

$$|x\rangle = 1_{\{x\}} \qquad \text{with} \qquad \langle x|y\rangle = \delta_{xy}$$

We will again make use of a black box

$$U_\phi : L^2(\mathcal{E}', \mu) \otimes H_{\mathbb{R}^n} \to L^2(\mathcal{E}', \mu) \otimes H_{\mathbb{R}^n}$$

which performs the operation

$$U_\phi \Phi \otimes |z\rangle = \Phi \otimes |z + \phi(f_1)\rangle$$

where we use the unique decomposition $\Phi(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, f_n\rangle_c$ with $f_n \in E_c^{\widehat{\otimes} n}$.

We now outline each step of the algorithm in detail:

8.3.1 Step 0

In the original version we begin in the state $|0\rangle|0\rangle \in H_E \otimes H_{\mathbb{R}^n}$. Here we take a unit vector Φ in $L^2(\mathcal{E}', \mu)$ and begin in the state

$$|\psi_0\rangle = \Phi\,|0\rangle$$

of $L^2(\mathcal{E}', \mu) \otimes H_E$. The only restriction we place on Φ is that for any subspace W of E we can decompose Φ into $\Phi = \Phi_W \Phi_{W^\perp}$ where $\Phi_W \in L^2(\mathcal{E}', \mu|\sigma_W)$ and $\Phi_{W^\perp} \in L^2(\mathcal{E}', \mu|\sigma_{W^\perp})$ (as in Theorem 8.9). Then, in particular, Φ can be decomposed into $\Phi = \Phi_V \Phi_{V^\perp}$, where V is the hidden subspace of the functional ϕ.

8.3.2 Step 1

This step is the one that is altered the least from the original algorithm. Here we apply the black box U_ϕ to $|\psi_0\rangle$ in order to arrive at

$$|\psi_1\rangle = U_\phi|\psi_0\rangle = \Phi\,|\phi(f_1)\rangle$$

where $f_1 \in E_c$ is the element obtained through the Wiener–Itô decomposition $\Phi(x) = \sum_{n=0}^{\infty} \langle :x^{\otimes n}:, f_n \rangle_c$ as described above.

8.3.3 Step 2

In place of the Fourier transform in the original algorithm we use U_S (actually $U_S \otimes I$) to get

$$|\psi_2\rangle = (U_S \otimes I)|\psi_1\rangle = U_S(\Phi)|\phi(f_1)\rangle.$$

Now we use that

$$U_S\Phi = U_S(\Phi_V \Phi_{V^\perp}) = U_S(\Phi_V)U_S(\Phi_{V^\perp})$$

(from Theorem 8.9) to arrive at

$$|\psi_2\rangle = U_S(\Phi_V)U_S(\Phi_{V^\perp})|\phi(f_1)\rangle$$

Since $\phi(\xi) = \phi(\xi_{V^\perp})$ for all $\xi \in E_c$ we have

$$|\psi_2\rangle = U_S(\Phi_V)U_S(\Phi_{V^\perp})|\phi(P_{V^\perp} f_1)\rangle$$

where $P_{V^\perp}$ is the orthogonal projection onto $V^\perp$.

We can then write $|\psi_2\rangle$ as

$$|\psi_2\rangle = U_S(\Phi_V)|\Omega(P_{V^\perp} f_1)\rangle$$

where $|\Omega(P_{V^\perp} f_1)\rangle = U_S(\Phi_{V^\perp})|\phi(P_{V^\perp} f_1)\rangle$.

8.3.4 Step 3

Apply $U_S^{-1} \otimes I$ to get

$$|\psi_3\rangle = (U_S^{-1} \otimes I)|\psi_2\rangle = U_S^{-1} U_S(\Phi_V)|\Omega(P_{V^\perp} f_1)\rangle = \Phi_V \, |\Omega(P_{V^\perp} f_1)\rangle$$

8.3.5 Step 4: Measurement

We now need to measure Φ_V in some way to obtain information about the subspace V. Up until this point we let Φ be an arbitrary unit vector in $L^2(\mathcal{E}', \mu)$. However, in order to complete the algorithm, we need to be a bit more specific about our choice of initial state. We now take a random non-zero vector $\xi \in E$ and let Φ be given by

$$\Phi = :e^{\langle \cdot, \xi \rangle}:$$

Remark 8.10. Technically, by the postulates of quantum mechanics our state should always be a unit vector in our state space $L^2(\mathcal{E}', \mu) \otimes H_{\mathbb{R}^n}$. Of course, we could accomplish this easily by dividing by the norm of $:e^{\langle \cdot, \xi \rangle}:$. However, this only confuses things, and we will leave it off.

With this choice of Φ it is easy to see that Φ_V and $\Phi_{V^\perp}$ work out to be

$$\Phi_V =:e^{\langle \cdot, \xi_V \rangle}: \qquad \text{and} \qquad \Phi_{V^\perp} =:e^{\langle \cdot, \xi_{V^\perp} \rangle}:$$

For $n = 0, 1, 2, \ldots$, let P_n be the orthogonal projection onto the closed linear span of

$$\{\langle :\cdot^{\otimes n}:, f_n \rangle_c \, ; \, f_n \in E_c^{\widehat{\otimes} n}\}$$

Obviously $P_n P_m = \delta_{nm} P_n$. Recalling that

$$:e^{\langle \cdot, \xi_V \rangle}: = \sum_{n=0}^{\infty} \frac{1}{n!} \langle :\cdot^{\otimes n}:, \xi_V^{\otimes n} \rangle$$

we see that $P_n(:e^{\langle \cdot, \xi_V \rangle}:) = \frac{1}{n!} \langle :\cdot^{\otimes n}:, \xi_V^{\otimes n} \rangle$.

Therefore measuring with respect to $\{P_n\}_{n=0}^{\infty}$ produces $\frac{1}{n!} \langle :\cdot^{\otimes n}:, \xi_V^{\otimes n} \rangle$ for some n. From this we can extract $\xi_V \in V$. Thus we have a hidden subspace for ϕ, namely $\{\mathbb{R}\xi_V\}$, which runs through the hidden subspace V. And, of course, running the procedure k times will produce a k–dimensional hidden subspace (provided the dimension of the hidden subspace is less than equal to k).

Chapter 9

Concluding Remarks

As we have seen the subject of White Noise Analysis is well suited for making notions of quantum computation credible when functions over infinite dimensional Hilbert spaces are involved. Moreover, it also serves as a great means for bringing common finite dimensional identities and theories over to the infinite dimensional setting.

Although, we have primarily concerned ourselves with the Hidden Subspace Algorithm, which is an adaptation of the Shor period finding algorithm, there are a few other algorithms which have been constructed for continuous variables. In [26], Pati and Braunstein develop a Deutsch–Jozsa algorithm for continuous variables. This algorithm takes a function $f : \mathbb{R} \to \{0, 1\}$ which is known to be constant or balanced and determines which is the case (i.e. if f is constant or balanced). By balanced we mean that $\lambda(\{x \in \mathbb{R} \mid f(x) = 0\}) = \lambda(\{x \in \mathbb{R} \mid f(x) = 1\})$, where λ is the Lebesgue measure. Using the techniques presented here it may be possible to develop such an algorithm for a suitable function $\Phi : \mathcal{E}' \to \{0, 1\}$ using the Gaussian measure on $\mathcal{E}'$, for a suitable function space $\mathcal{E}$.

In [27], Braunstein, Lloyd, and Pati extended Grover's search algorithm to the continuous variable setting. Although, perhaps more difficult, this algorithm may have an extendsion to Hilbert spaces of infinite dimension.

As mentioned by Lomonaco and Kauffman in [21], it may be possible to modify the Hidden Subspace Algorithm in order to develop a quantum algorithm which computes the Jones polynomial or other knot invariants. For such an algorithm the theory of White Noise Analysis is not enough. Non–communtative infinite dimensional distribution theory is needed for this undertaking. In such an algorithm the Hilbert space E may possibly be replaced by the space $\mathcal{A}$ of gauge connections and a modification of the functional integral

$$\widehat{\psi}(K) = \int_{\mathcal{A}} DA\, \psi(A)\, \mathcal{W}_K(A)$$

where $\mathcal{W}_K(A)$ is the Wilson loop

$$\mathcal{W}_K(A) = \mathrm{tr}\Big[P \exp\Big(\oint_K A\Big)\Big]$$

may be necessary. If $\psi(A)$ is chosen correctly, the functional integral $\widehat{\psi}(A)$ is a knot or link invariant. For an appropriate choice of gauge group, this invariant can reproduce the original Jones polynomial or other invariants [12].

Bibliography

[1] S. Albeverio, B. C. Hall, and A. N. Sengupta, *The Segal–Bargmann transform for two dimensional quantum Yang–Mills*, Infinite Dimensional Analysis, Quantum Probability and Related Topics, 2 (1999), pp. 27 – 49.

[2] J. J. Becnel, *Delta function for an affine subspace.* submitted for publication, March 2006.

[3] J. J. Becnel, *Equivalence of topologies and Borel fields for countably–Hilbert spaces*, Proceeding of the AMS, 134 (2006), pp. 581–590.

[4] J. J. Becnel and A. N. Sengupta, *The Schwartz space: Tools for white noise analysis.* submitted for publication, December 2004.

[5] J. J. Becnel and A. N. Sengupta, *An infinite dimensional integral identity for the Segal–Bargmann transform.* submitted for publication, March 2006.

[6] J. B. Conway, *Functions of One Complex Variable*, vol. 1, Springer-Verlag, New York, New York, second ed., 1978.

[7] K. Devlin, *The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles of Our Time*, Basic Books, New York, New York, 2002.

[8] I. Gel'fand and G. Shilov, *Spaces of Fundamental and Generalized Functions*, vol. 2 of Generalized Functions, Academic Press, New York, New York, 1968.

[9] I. Gel'fand and N. Y. Vilenkin, *Application of Harmonic Analysis*, vol. 4 of Generalized Functions, Academic Press, New York, New York, 1964.

[10] E. Gerjuoy, *Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers.* http://xxx.lanl.gov/abs/quant-ph/0411184, 29 pages, May 2004.

[11] L. K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Physical Review Letters, 79 (1997), pp. 325 – 328.

[12] A. Hahn, *The Wilson loop observables of Chern-Simons theory on R^3 in axial gauge*, Commun. Math. Phys., 3 (2004), pp. 467 – 499.

[13] L. Hörmander, *The Analysis of Linear Partial Differential Operators*, vol. 1, Springer-Verlag, New York, New York, 1983.

[14] K. Itô, *Introduction to Probability Theory*, Cambridge University Press, New York, New York, 1984.

[15] G. Köthe, *Topological Vector Spaces I*, vol. 1, Springer-Verlag, Berlin, Germany, 1969.

[16] I. Kubo, *Itô formula for generalized Brownian functionals*, vol. 49 of Lecture Notes in Control and Information Scis, Springer–Verlag, New York, New York, 1983.

[17] H.-H. Kuo, *White Noise Distribution Theory*, Probability and Stochastic Series, CRC Press, Inc., New York, New York, 1996.

[18] S. J. Lomonaco, ed., *Proceedings of Symposia in Applied Mathematics*, vol. 58, Providence, RI, 2002, American Mathematical Society.

[19] S. J. Lomonaco, *Shor's quantum factoring algorithm*, in Lomonaco [18], pp. 161–179.

[20] S. J. Lomonaco and L. H. Kauffman, *A continuous variable shor algorithm.* http://xxx.lanl.gov/abs/quant-ph/0210141, 12 pages, October 2002.

[21] S. J. Lomonaco and L. H. Kauffman, *Continuous quantum hidden subgroup algorithms*, in Proceedings of SPIE, vol. 5105, 2003, pp. 80 – 88.

[22] V. Mihai and A. N. Sengupta, *The Radon-Gauss Transform.* in prepartion, 2005.

[23] J. R. Munkres, *Topology*, Prentice Hall, Inc., Upper Saddle River, New Jersey, second ed., 2000.

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, United Kingdom, 2000.

[25] N. Obata, *White Noise Calculus and Fock Space*, Lecture Notes in Mathematics, Springer–Verlag, New York, New York, 1994.

[26] A. K. Pati and S. L. Braunstein, *Deutsch-jozsa algorithm for continuous variables.* http://xxx.lanl.gov/abs/quant-ph/0207108, 3 pages, July 2002.

[27] A. K. Pati, S. L. Braunstein, and S. Lloyd, *Quantum searching with continuous variables.* http://xxx.lanl.gov/abs/quant-ph/0002082, 4 pages, June 2000.

[28] M. Reed and B. Simon, *Fourier Analysis, Self-Adjointness*, vol. 2 of Methods of Modern Mathematical Physics, Academic Press, San Diego, California, 1975.

[29] A. Robertson and W. Robertson, *Topological Vector Spaces*, Cambridge University Press, London, 1964.

[30] W. Rudin, *Real and Complex Analysis*, WCB/McGraw-Hill, Boston, Massachusetts, third ed., 1987.

[31] W. Rudin, *Functional Analysis*, McGraw-Hill, New York, second ed., 1991.

[32] H. H. Schaefer, *Topological Vector Spaces*, The Macmillan Company, New York, New York, 1966.

[33] P. Shor, *Polynomial–time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. on Computing, 26 (1995), pp. 1484 – 1509.

[34] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, New Jersey, 1955.

[35] Y.-C. Wong, *Introductory Theory of Topological Vector Spaces*, Marcel Dekker, Inc., New York, New York, 1992.

Vita

Jeremy J. Becnel was born in the small community of Kraemer, Louisiana, on August 11, 1979. He finished his undergraduate studies in mathematics and computer science at Nicholls State University in May 2001. In August 2001 he came to Louisiana State University to pursue graduate studies in mathematics. He earned a master of science degree in mathematics from Louisiana State University in December 2002. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2006.