A Quantum Stochastic Calculus

William Joseph Spring

A thesis submitted in partial fulfilment of the requirements of the University of Hertfordshire for the degree of

Doctor of Philosophy

The programme of research was carried out in the

School of Computer Science

University of Hertfordshire

May 2012

William Joseph Spring
School of Computer Science,
University of Hertfordshire,
College Lane,
Hatfield. AL10 9AB UK
e-mail: j.spring@herts.ac.uk

Abstract

Martingales are fundamental stochastic process used to model the concept of fair game. They have a multitude of applications in the real world that include, random walks, Brownian motion, gamblers fortunes and survival analysis, Just as commutative integration theory may be realised as a special case of the more general non-commutative theory for integrals, so too, we find classical probability may be realised as a limiting, special case of quantum probability theory.

In this thesis we are concerned with the development of multiparameter quantum stochastic integrals extending non-commutative constructions to the general n parameter case, these being multiparameter quantum stochastic integrals over the positive n - dimensional plane, employing martingales as integrator. The thesis extends previous analogues of type one, and type two stochastic integrals, for both Clifford and quasi free representations. As with one and two dimensional parameter sets, the stochastic integrals constructed form orthogonal, centred L2 - martingales, obeying isometry properties. We further explore analogues for weakly adapted processes, properties relating to the resulting quantum stochastic integrals, develop analogues to Fubini's theorem, and explore applications for quantum stochastic integrals in a security setting.

Acknowledgements

I would like to thank my supervisors Professor Bruce Christianson, and Professor Rod Adams for their continued support throughout this thesis. I could not have wished for two finer supervisors for research at this level. Your support throughout is much appreciated. I would also like to thank J. Vaccaro, A. Chefles and S. Huelga who have also been very encouraging at different stages of the thesis, together with the many people that I have met at conferences and universities.

Finally I would like to thank my wife Jane, my mother Lena and my father William, without whose love, patience and understanding, this would not have been achieved.

Notation

$\mathbb{R}^n_+$ denotes the positive n-dimensional quadrant in $\mathbb{R}^n$, with $n \in \mathbb{N}^+$.

$z = (z_1, z_2, \ldots, z_n)$ represents an element in $\mathbb{R}^n_+$. Each $z_i \in \mathbb{R}_+$.

$z \prec z'$ denotes two elements in $\mathbb{R}^n_+$such that $z_i \leq z'_i$ for $1 \leq i \leq n$.

$z \prec\prec z'$ means that $z_i < z'_i$ for $1 \leq i \leq n$.

$z \vee z'$ denotes the sup of z and z'.

$z \wedge z'$ denotes the inf of z and z'.

$\bigvee_{i=1}^{m} z_i,$ for $z_i \in \mathbb{R}^n_+$ represents the $\sup\{z_1, z_2, \ldots, z_m\}$.

$\bigwedge_{i=1}^{m} z_i,$ for $z_i \in \mathbb{R}^n_+$ represents the $\inf\{z_1, z_2, \ldots, z_m\}$.

Contents

Chapter 1

Introduction

This chapter introduces the problem that this thesis is concerned with, the motivation behind the work, and outlines the contents of each chapter in the thesis.

1.1 The Problem

The motivation for this thesis is driven by various objectives. The first of these is a simplification of the approach taken in developing a theory of quantum stochastic integrals over $\mathbb{R}^n_+$. The complexity involved can, we feel, be unnecessarily daunting and as such we develop, in the spirit of John Walsh [139], a simpler, more intuitive approach here. The second objective is the development of tools required in order to achieve our first objective and our third objective is the identification and exploration of applications to which the non-commutative quantum stochastic integrals developed may be applied. These, in particular, are identified and explored with a view to further development at a later stage. These objectives are, we feel, important promoting accessibility, encouraging future student participation with the material. The development of relatively simple applications, strengthen concepts and further encourage participation.

Quantum based applications developed for qubit based multipartite systems such as the

BB84 [14, 135], E91 [29] and B92 [9] key agreement protocols, the Deutsch-Josza [23, 24] algorithm, the teleportation [13] algorithm, Grovers [40] algorithm and Shor's [100, 101] celebrated algorithms have achieved considerable gain over their classical counterparts.

Quantum based voting protocols have been developed [51, 52, 71] and the application of probability [21] to voting schemes has been developed at the classical level. The third objective in this thesis will lead us to identify quantum based applications of classical concepts relating to voting schemes, and associated tools from cryptology. In this thesis, we will consider cyclic like group structures for application to protocols in quantum cryptology. These, together with the representation theorem contained within, initially led to the development of a Fubini like theorems for multipartite quantum stochastic integrals. This in turn, led to a redevelopment of multipartite stochastic integrals, initiated by the work of Barnett, Streater and Wilde in the quantum setting and Ito, Cairoli and Walsh, Wong and Zakai, and Imkeller in the classical setting. For this presentation we commence with related background material, and then proceed with an exploration of the nature, characteristics and relationships that exist between quantum stochastic integrals as the underlying parameter space $\mathbb{R}_+^n$ varies with n. In the commutative setting the development of the Ito [49], Wong-Zakai [15, 139, 141], and [48] Imkeller integrals together with [58] Stochastic versions of the Fubini Theorem have stimulated research at the quantum level. At the quantum level developments have involved many researchers, including Hudson and Parthasarathy, Streater, Accardi, Lindsay, Sinha and Belavkin. Developments relating to the Ito [46, 80, 86, 87] and the Wong-Zakai integrals [8, 38, 86, 119, 120, 121] have taken place at both the Hilbert space level, and at the operator level with Banach, von Neumann and C^* Algebras. Developments with multidimensional integrals in a non-commutative setting have been achieved [47, 50, 108, 109, 110, 111, 112, 113, 114, 117] together with Fubini related problems [47] and multidimensional integrals on Fock space [50].

We proceed in this work, from the geometric setting first introduced by John Walsh [139] with classical stochastic integrals. These we find have application in the quantum setting, simplifying concepts previously worked with at an operator or vector based level. Our primary motivation, is to simplify the approach taken with general quantum stochastic integrals where the complexity involved can very quickly increase leading to an exploration of the relationships between different types of quantum stochastic integral over $\mathbb{R}_+^m$ and $\mathbb{R}_+^n$. Our second objective involves the development of quantum stochastic Fubini like theorems over multi-dimensional parameter spaces. Finally we develop applications for quantum stochastic integrals based on the Fock space models presented here.

1.2 Structure for the Thesis

We give a brief overview of each of the chapters.

Chapter 2 is a review of those stochastic operator concepts and theorems that relate to the work carried out in subsequent chapters. It draws on both classical and quantum concepts from probability theory, operator theory and non commutative theory.

Chapter 3 describes the standard quantum probability models that we work with in preparation for our work on quantum stochastic integrals. These include the Clifford sheet and quasi-free CAR and CCR sheets for generalised settings over $\mathbb{R}_+^n$ with $n \in \mathbb{N}^+$

Chapter 4 commence with a discussion on irreducible parameter types that form fundamental components in the underlying parameter space $\mathbb{R}_+^n$. These underpin the quantum stochastic integrals developed for the general setting, as analogues of the Itø, Wong-Zakai, and Imkeller integrals found in commutative stochastic theory. Standard results are established including isometry, orthogonality and centred martingale properties. The chapter concludes with a presentation of the general Representation theorem for the Clifford setting and the quasi-free CAR and CCR over $\mathbb{R}_+^3$.

Chapter 5 extends our work on quantum stochastic integral with Fubini interpretations

of the first, second and third kind, these we believe to be a natural development for the quantum setting. Each of the forms are related to each other and using this we describe how they may be applied to the proof for the Representation Theorem over $\mathbb{R}^n_+$, for the Clifford and quasi-free sheets.

Chapter 6 introduces related applications from security to which we apply a selection of quantum stochastic integrals. The discussion commences with related concepts from quantum cryptography, for qubit based multipartite models to the one we have been working with. The discussion returns to the Fock environment where we describe a cyclic like quantum stochastic construction which we explore in applications, as proof of concept, to the Diffie Hellman key agreement protocol and El Gamal algorithm from cryptography. The chapter concludes with a presentation of applications to quantum voting within a quantum probability framework in contrast to the models discussed in [51, 71].

Chapter 7 provides a summary of our contribution to knowledge, and offers suggestions for extending the work presented.

Chapter 2

Stochastic Theory and Related Topics

2.1 Introduction

This chapter is a review of background material used in subsequent chapters. It includes random variables, expectation, stochastic processes, conditional expectation, adapted processes, weakly adapted processes, filtrations, stochastic base; Lesbegue, Baire and Borel space; Hilbert space, von Neumann algebras, and C*-algebras.

In developing a probability theory [137], one is initially motivated by traditional examples; coins, cards, and dice. Sample spaces are established, events (subsets of the sample space) forming a σ-ring (σ-field), associated random variables dependent upon the sample spaces and measures of likelihood, location and dispersion applied to event spaces. Experimental models are abstracted into theoretical models and the discussion embraces uniform, binomial Poisson, exponential and Gaussian distributions. One initially works with Riemann integrals, but requirements that ensue with for example, expectation on random variables such as '$X = 1$ for rationals and 0 otherwise', force one to employ

measure theoretic tools: measurable spaces, measurable functions and measures such as the Lesbegue, Borel and Baire measures [91]. We thus work with probability spaces of the form $(\Omega, \mathcal{F}, P)$, in which Ω denotes a sample space, $\mathcal{F}$ denotes a σ field of measurable events, (subsets) of Ω and P represents a Lesbegue, Borel or Baire probability measure. From here we may derive a link to Segal's (commutative) probability gage space and from there generalise to non-commutative gage spaces employed in a quantum setting, [95]. For further details we defer to [58, 91, 94, 95, 96, 97]

2.2 Probability Spaces, Random Variables and Processes

Definition 1. (Topological Space) [58] Let $(\Omega \neq \emptyset$ be an arbitrary space. A class of sets $\mathcal{F} \subset \Omega$ is called a topology on Ω if $\mathcal{F}$ contains: $\emptyset$ and Ω, the intersection of any two sets belonging to $\mathcal{F}$, and the union of elements from any subset of $\mathcal{F}$.
The pair $(\Omega, \mathcal{F})$ is called a topological space. The sets $A \in \mathcal{F}$ are called open, and the sets $A \in \Omega$ with $A^C \in \mathcal{F}$ are called closed.

Definition 2. (Borel Space, Borel Sets, Borel σ - Algebra) [58, 62] Let $(\Omega, \mathcal{F})$ be a topological space. The σ algebra that is generated by the open sets $(A \in \mathcal{F})$ is called the Borel σ - Algebra on Ω. The elements generated are called Borel sets or Borel measurable sets.

Definition 3. (Random Variable) [62] *A Random Variable is defined to be a measurable function* $X : \Omega \longrightarrow \mathbb{R}$ *such that* $\forall$ *Borel sets* $B \subseteq \mathbb{R}$, $X^{-1}(B) \in \mathcal{F}$.

Here, it is understood that we may work with the equivalence classes from $L^0(\Omega, \mathcal{F}, P)$ in preference to the vector space $\mathcal{L}(\Omega, \mathcal{F}, P)$ of all random variables via the relation $f \sim g \iff f = g$ *a.s.* [62]. The convergence in probability metric $d(f, g) = \int_\Omega min\{1, |f(\omega) - g(\omega)|\} dP(\omega)$ generates the complete metric space (L^0, d), in which $L^0 = L^0(\Omega, \mathcal{F}, P)$ and

Banach spaces $(L^p(\Omega, \mathcal{F}, P)$, $||f||_p = (\int_\Omega |f|^p dP)^{1/p})$, for $1 \leq p < \infty$ and $(L^\infty(\Omega, \mathcal{F}, P)$, $ess\, sup_{\omega\in\Omega}|f(\omega)|)$ otherwise, formed via the given norms.

The definition for a random variable [5], extends to measurable functions with n dimensional codomain, $X : \Omega \longrightarrow \mathbb{R}^n$, $n \in \mathbb{N}^+$, $n \geq 1$.

Definition 4. (Expectation) Let X denote a random variable. The Expectation of X is defined to be the theoretical analogue of the experimental mean average. For X a (continuous) random variable we have $\mathbb{E}(X) = \int_\Omega X dP$. For X a discrete random variable this becomes $\mathbb{E}(X) = \sum\limits_{\omega\in\Omega} X(\omega)P(X = \omega)$

Definition 5. (Stochastic Process) A collection of random variables $\{X_z : z \in I\}$ for some partially ordered index set I, defined on the same Borel space is referred to as a stochastic process. In general, we work with $I \subseteq \mathbb{R}^n_+, n \in \mathbb{N}^+$.

Stochastic processes may be discrete or continuous. A discrete stochastic process X is of the form $(X_i)_{i\in I}$ with $I \subseteq \mathbb{N}^+$, I generally of the form $\{0, 1, 2, 3, \dots\}$ may be finite or countably infinite. A continuous stochastic process is of the form $X = (X_i)_{i\in I}$ with $I \subseteq \mathbb{R}^n_+$. We note that the partially ordered index set I, is often interpreted as time, a subset of $\mathbb{R}_+$, and rather than I one often encounters the use of T for the index set.

Example 1. (Brownian Motion) [62]. A (standard) *Brownian Motion* $(BM_0(\mathbb{R}))$ is a Gaussian family $B = (B_t)_{t\in T}$ of random variables with partially ordered index set T, satisfying:

a) $B_0 = 0$;

b) $\mathbb{E}(B_t) = 0$, $\mathbb{E}(B_sB_t) = min(s, t)$ for $s, t \in T$;

c) $P\{t \mapsto B_t \text{ is continuous on } T\} = 1$

The integral [62] $\int_0^t B_s dB_s$ cannot be realised as a Riemann Stieltjes integral, leading to alternative stochastic integrals being developed, in particular the Itô stochastic integral. Other stochastic integrals include the Stratonovich and Skorokhod stochastic integrals.

Multidimensional stochastic integrals such as the Wong-Zakai, and Imkeller integrals have been developed. We will be particularly interested in multidimensional analogues of the Itô, Wong-Zakai, Imkeller and stochastic integrals defined over larger parameter spaces.

Example 2. (Wiener Process) [58] Let $\mathbf{P}$ denote a probability measure defined on $\Omega = \mathcal{C}([0,\infty))$, (the set of continuous functions on $[0,\infty)$), with respect to which the canonical process X is a Brownian motion. Then $\mathbf{P}$ is called the Wiener measure. The triple $(\Omega, \mathcal{F}, \mathbf{P})$ is the Wiener space, and X is called the canonical Brownian motion or the Wiener process.

Example 3. (Martingales)[1] [89] These may appear in, for example, a medical setting (patient diagnosis), with financial modelling (martingale pricing theory of financial derivatives) and random walks.

Definition 6. (Polish Space) [58] A Polish space is defined to be a separable topological space whose topology is induced by a complete metric. (So all Cauchy sequences are convergent with limits in the space).

Example 4. (Polish Space) [58] $\mathbb{R}^d$, $\mathbb{Z}^d$, $\mathbb{R}^{\mathbb{N}}$, $(C([0,1], \| \ \|_\infty)$ are examples of Polish spaces. Closed subsets of Polish spaces are also Polish spaces. $\mathbb{Q}$, with the Euclidean metric, is not a Polish space.

The following definition and example are given for completeness. They are presented as examples of different processes. The examples and notation are not employed in subsequent discussions.

Definition 7. (Markov Process) [58, 90] Let $I \subset [0,\infty)$ be closed under addition and assume $0 \in I$. A stochastic process $(X_t)_{t\in I}$ is called a time-homogeneous Markov process with distributions $(P_x)_{x\in E}$, E a Polish Space, on the space $(\Omega, \mathcal{F})$ if:

[1] For a definition of martingale see Section 2.6.

a) $\forall x \in E$, X is a stochastic process on the probability space $(\Omega.\mathcal{F}, P_x)$ with $P_x[X = x] = 1$

b) the map $\kappa : E \times \mathcal{B}(E)^{\otimes I} \longrightarrow [0,1], (x, B) \mapsto P_x[X \in B]$ is a stochastic kernel

c) X has the time-homogeneous Markov property (MP):

$\forall A \in \mathcal{B}(E), \forall x \in E$ and $\forall s, t \in I,$, $P_x[X_{t+s} \in A|\mathcal{F}_s] = \kappa_t(X_s, A) \quad P_x\, a.s.$

Here for every $t \in I$, the transition kernel $\kappa : E \times \mathcal{B}(E)^{\otimes I} \longrightarrow [0,1]$ is the stochastic kernel defined for $x \in E$ and $A \in \mathcal{B}(E)$ by

$$\kappa_t(x, A) := \kappa\left(x, \{y \in E^I : y(t) \in A\}\right) = P_x[X_t \in A]$$

The family $(\kappa_t(x, A), t \in I, x \in E, A \in \mathcal{B}(E))$ is also called [58] the family of transition probabilities of X.

Example 5. (Markov Processes) [26, 69, 99] Classically these may be found in, for example, random walk theory, queuing theory where they are used to characterise traffic flow within a network. In a quantum setting they appear in Hidden Variable Theory, in non-commutative probability theory and with random walks.

Definition 8. (Levy Process) [90] Let $X = \{X_t\}_{t \geq 0}$ denote an $\mathbb{R}^d$ valued stochastic process. Then X is said to be a Levy Process (or process with stationary independent increments) if it has the following properties:

a) for almost all ω, $t \to X_t(\omega)$ is right continuous on $[0, \infty)$, with left limits on $(0, \infty)$

b) for $0 \leq t_0 \leq t_1 < \cdots < t_n$, the random variables $Y_j = X_{t_j} - X_{t_{j-1}}$, $(j = 1, 2, \ldots, n)$ are independent

c) the law of $X_{t+h} - X_t$ depends on h, but not on t.

Example 6. (Levy Process) [90] Brownian motion is an example of a Levy process and Levy processes form examples of a Markov processes.

2.3 Filtrations and Adapted Processes

Definition 9. (Filtration) [62] A filtration $(\mathcal{F}_i)_{i\in I}$ is defined to be an increasing family $(\mathcal{F}_i \subseteq \mathcal{F}_j : i \leq j \text{ in } I)$ of sub - σ - fields of $\mathcal{F}$.
So $\mathcal{F}_{i_1} \subseteq \mathcal{F}_{i_2} \subseteq \ldots$ for all $i_1 \leq i_2 \in I$

Definition 10. Stochastic Base [62] For this discussion a stochastic base will denote the 5-tuple $(\Omega, \mathcal{F}, P, (\mathcal{F}_i)_{i\in I}, I)$ with entries as defined above. It is generally understood that for a stochastic base $\mathcal{F}_0$ contains all P null sets and the filtration $(\mathcal{F}_i)_{i\in I}$ is right continuous, by which we mean that $\mathcal{F}_i = \mathcal{F}_{i^+} = \cap_{i<j}\mathcal{F}_j$.

Definition 11. (Adapted Process) [62] A process X is adapted to $(\mathcal{F}_i)_{i\in I}$ if and only if $\forall i \in I$, X_i is $\mathcal{F}_i$ - measurable.

2.4 i-Filtrations and Weakly Adapted Processes

In our discussion on Fubini's Theorem (Chapter 5) we will be interested in i-filtrations and weakly adapted processes. In preparation for this we introduce the concepts for the parameter space $\mathbb{R}^2_+$ of points laying in the positive quadrant of the $\mathbb{R}^2$ plane.

Notation 1. Let z denote points $(z_1, z_2) \in \mathbb{R}^2_+$. The notation describes the more familiar points (x, y) in the Cartesian plane, but have the advantage of being straightforward to extend to the positive n-dimensional plane $\mathbb{R}^n_+$.

Notation 2. [139] Let $z \prec z'$ denote points in $\mathbb{R}^2_+$ such that $z_1 \leq z'_1$ and $z_2 \leq z'_2$ and $z \prec\prec z'$ denote points for which $z_1 < z'_1$ and $z_2 < z'_2$. For $z \prec\prec z'$ the point z' is said to be forward of the point z.

Notation 3. [139] Let $z \vee z'$ denote the supremum of z and z' and $z \wedge z'$ denote the infimum of z and z'. So for $\mathbb{R}^2_+, z \vee z' = (sup\{z_1, z'_1\}, sup\{z_2, z'_2\})$ and $z \wedge z' = (inf\{z_1, z'_1\}, inf\{z_2, z'_2\})$.

Definition 12. (i - Filtration) [139] Let $\mathcal{F}_z^1$ denote the field $\mathcal{F}_{(z_1,\infty)} = \bigvee_{z_2' \leq z_2} \mathcal{F}_{z'}$ with $z' \in I$, and $\mathcal{F}_z^2$ denote the field $\mathcal{F}_{(\infty,z_2)}$. Then an i - filtration $(\mathcal{F}_z^i)_{z\in I}$ is defined to be an increasing family $\{\mathcal{F}_z^i \subseteq \mathcal{F}_{z'}^i : z \prec\prec z' \text{ in } I\}$ of sub - σ - fields of $\mathcal{F}$.

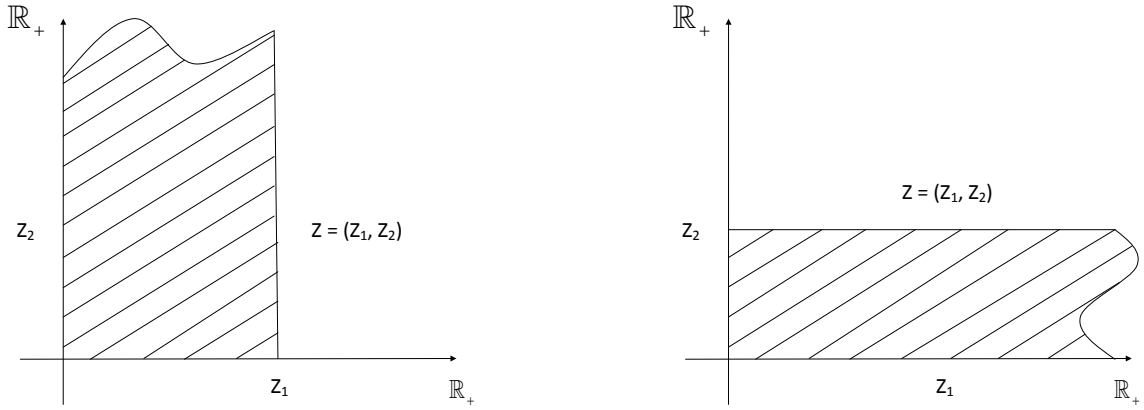

Fig 1. $\mathcal{F}_z^1$ (defined for shaded region in left diagram) and $\mathcal{F}_z^2$ (for right diagram)

We note [15] that $\mathcal{F}_z^1 = \mathcal{F}_{(z_1,z_2)}^1 = \mathcal{F}_{(z_1,z_2')}^1$ and so is independent of the z_2 value. Likewise, $\mathcal{F}_z^2 = \mathcal{F}_{(z_1,z_2)}^2 = \mathcal{F}_{(z_1',z_2)}^2$ is independent of the z_1 value. For the general case over $\mathbb{R}_+^n$ we have $\mathcal{F}_z^i = \mathcal{F}_{(z_1,z_2,...,z_i,...,z_n)}^i = \mathcal{F}_{(z_1',z_2',...,z_i,...,z_n')}^i$ and so is independent of the z_j values, for all $j \neq i$ and define

$$\mathcal{F}_z^i = \mathcal{F}_{(z_1,z_2,...,z_i,...,z_n)}^i = \bigvee_{z_j' \leq z_j} \mathcal{F}_{z'} \text{ with } z' \in I.$$

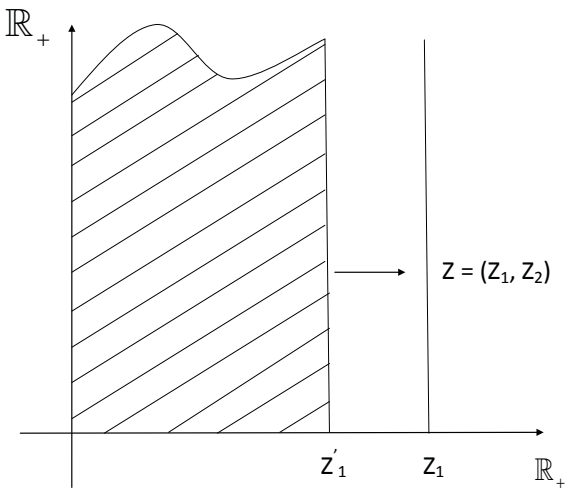

Fig 2. $\mathcal{F}_z^2$ defined for shaded region

Definition 13. (i - Stochastic Base) [62, 139] By an i - stochastic base we mean a 5-tuple $(\Omega, \mathcal{F}, P, (\mathcal{F}_z^i)_{z\in I}, I)$ with entries as defined above. It is understood that for a stochastic base $\mathcal{F}_0$ contains all P null sets and the i - filtration $(\mathcal{F}_z^i)_{z\in I}$ is right continuous, by which we mean that $\mathcal{F}_z^i = \mathcal{F}_{z^+}^i = \bigcap\limits_{z\prec z'} \mathcal{F}_{z'}^i$.

Definition 14. (Weakly Adapted Processes) [139] A process X is said to be weakly adapted if it is adapted to the field $\mathcal{F}_z^1$ or $\mathcal{F}_z^2$. We note that if a process is adapted to both fields $\mathcal{F}_z^1$ and $\mathcal{F}_z^2$ then it is said to be adapted to $\mathcal{F}_z$.

We note [139] that the above σ-fields are often presented as satisfying the following three martingale hypotheses:

(F1) $z \prec\prec z' \Longrightarrow \mathcal{F}_z \subset \mathcal{F}_{z'}$

(F2) $\mathcal{F}_z$ contains all null sets of $\mathcal{F}$

(F3) $\mathcal{F}_z = \underset{z \prec\prec z'}{\cap} \mathcal{F}_{z'}$.

An additional property (fourth hypothesis) may also be presented is referred to as the conditional independence property. Let z, $z' \in I \subseteq \mathbb{R}^n_+$,

(F4) $\mathcal{F}_z$ and $\mathcal{F}_{z'}$ are conditionally independent, given $\mathcal{F}_{z \wedge z'} = \mathcal{F}_z \cap \mathcal{F}_{z'}$.

We define conditional independence following our discussion on conditional expectations.

2.5 Conditional Expectations

For conditional expectations we consider the interpretation of a conditional probability

$$\mathbb{E}(\chi_A|B) = P(A|B) = \frac{P(A \cap B)}{P(B)}$$

as a 'renormalisation' of likelihood given a shift of sample space from Ω to the subspace B. With such a shift follows a corresponding shift in expectation from $\mathbb{E}(X) = \mathbb{E}(X|\Omega)$ to $\mathbb{E}(X|B) = P^{-1}(B)\int_A X dP$, described [62] as 'best estimate' for X given the information contained in B. This interpretation extends to sub σ - fields $\mathcal{F}_z$ of $\mathcal{F}$ in which $\mathbb{E}(X|\mathcal{F}_z)$ denotes a 'best guess' for X given the information in $\mathcal{F}_z$ such that

$$\forall F \in \mathcal{F}_z \int_F X dP = \int_F \mathbb{E}(X|\mathcal{F}_z) dP.$$

Theorem 1. [58] The $\mathbb{E}(X|\mathcal{F}_z)$ exists and is unique (up to equality almost surely).

The Conditional Expectation Operator $\mathbb{E}(X_{z'}|\mathcal{F}_z)$ is a mapping $X_{z'} \mapsto X_z$. Existence follows as a consequence of the Radon Nikodym Theorem.

2.5.1 Conditional Expectations and Projections

The [58, 62] best prediction / estimate is understood to be the

> '$\mathcal{F}$ measurable random variable that minimises the L^2-distance from X'.

One can define conditional expectations in terms of orthogonal projections from $L^2(\mathcal{F})$ onto the subspaces $L^2(\mathcal{F}_z)$ such that

$$\forall F \in \mathcal{F}_z \int_F X dP = \int_F \mathbb{E}(X|\mathcal{F}_z) dP$$

or equivalently

$$\forall f \in L^2(\mathcal{F}_z) \int_\Omega X f dP = \int_\Omega \mathbb{E}(X|\mathcal{F}_z) f dP.$$

This view of the conditional expectation establishes it as the '$\mathcal{F}$ measurable random variable that minimises the L^2-distance from X'.

For z, $z' \in I \subseteq \mathbb{R}^n_+$, we now return to the concept of conditional independence.

2.5.2 Conditional Independence

Definition 15. (Conditional Independence) [139] Let z and $z' \in I$. Let X be bounded and $\mathcal{F}_{z'}$ measurable. Then the σ-fields $\mathcal{F}_z$ and $\mathcal{F}_{z'}$ are said to be conditionally independent if

$$\mathbb{E}(X|\mathcal{F}_z) = \mathbb{E}(X|\mathcal{F}_{z \wedge z'})$$

or equivalently,

$$\mathbb{E}\left(\mathbb{E}(X|\mathcal{F}_z)|\mathcal{F}_{z'}\right) = \mathbb{E}\left(\mathbb{E}(X|\mathcal{F}_{z'})|\mathcal{F}_z\right)$$

An alternative equivalent definition for conditional independence is the following from Cairoli and Walsh.

Definition 16. (Conditional Independence) [15]. Let $(\Omega, \mathcal{F}, P)$ be a probability space. Let $\{\mathcal{F}_z, z \in \mathbb{R}^2_+\}$ be a family of sub-σ-fields of $\mathcal{F}$. Then $\mathcal{F}^1_z$ and $\mathcal{F}^2_z$ are said to be Conditionally Independent if for all bounded random variable X and all $z \in \mathbb{R}^2_+$

$$\mathbb{E}\left(X|\mathcal{F}_z\right) = \mathbb{E}\left(\mathbb{E}\left(X|\mathcal{F}^1_z\right)|\mathcal{F}^2_z\right)$$

For $\mathbb{R}^n_+$ we obtain:

$$\mathbb{E}\left(X|\mathcal{F}_z\right) = \mathbb{E}\left(\mathbb{E}\left(\ldots\mathbb{E}\left(\mathbb{E}\left(X|\mathcal{F}_z^1\right)|\mathcal{F}_z^2\right)|\ldots|\mathcal{F}_z^{n-1}\right)|\mathcal{F}_z^n\right)$$

2.6 Martingales

Various types of martingale are to be found in the literature, some of which we include in the following definition.

Definition 17. *(***Martingales, i-/Weak/Strong Martingales)** [57, 62, 139] Let X denote an L^1 process, with associated filtration $\mathcal{F}$. Then X is said to be a(n):

a) **Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z$ and $\forall z \prec z'$, $\mathbb{E}(X_{z'}|\mathcal{F}_z) = X_z$

b) **sub - Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z$ and $\forall z \prec z'$, $\mathbb{E}(X_{z'}|\mathcal{F}_z) \geq X_z$

c) **super - Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z$ and $\forall z \prec z'$, $\mathbb{E}(X_{z'}|\mathcal{F}_z) \leq X_z$

d) **i - Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z^i$ and $\forall z \prec\prec z'$, $\mathbb{E}(X(z,z']\,|\mathcal{F}_z^i) = 0$

e) **Weak Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z$ and $\forall z \prec\prec z'$, $\mathbb{E}(X(z,z']\,|\mathcal{F}_z) = 0$

f) **Strong Martingale** if $\forall z \in I$, $X_z \in \mathcal{F}_z, X_z$ vanishes on the axes, and

$\forall z \prec\prec z'$, $\mathbb{E}(X(z,z']\,|\bigvee_{1\leq i\leq n}\mathcal{F}_z^i) = 0$

We note [139] that an i martingale is a stochastic process that possesses the martingale property in its i'th component.

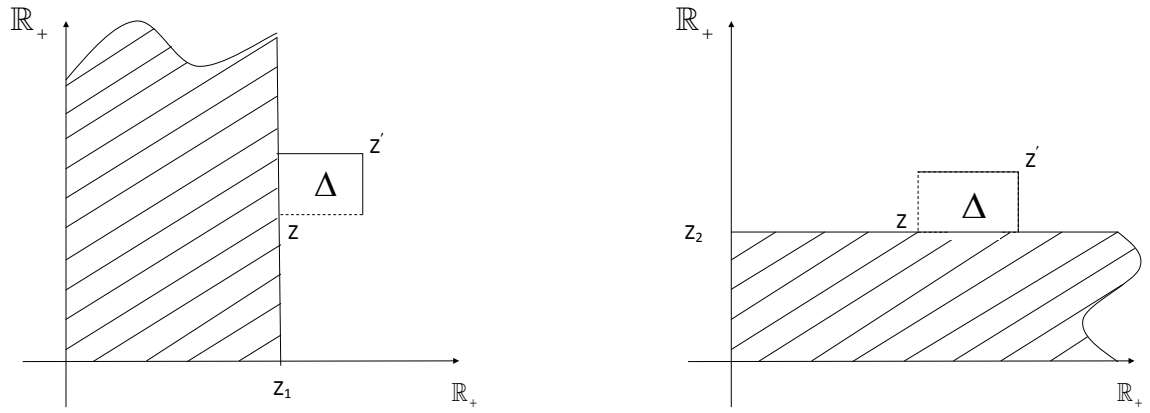

Fig 3. $X(z, z']$ defined over region $\Delta = (z, z']$.
$\mathbb{E}(X(z, z']|\mathcal{F}_z^1) = 0$ (left diagram) and $\mathbb{E}(X(z, z']|\mathcal{F}_z^2) = 0$ (right diagram)

Example 7. [57] Examples of martingales include random walks, modelling a fair game (gambling), filtering problems in engineering, modelling random oscillators, together with applications in finance and in biology.

Theorem 2. *Let $X = (X_n)$ denote a process. Then:*

a) X is a martingale $\iff$ X is both a sub-martingale and a super-martingale

b) X is a martingale over $\mathbb{R}_+^n$ $\iff$ X is an i-martingale $\forall\, i \in \{1, 2, \ldots, n\}$.

Proof. The proof for part a) follows directly from the definitions.

b) X a martingale $\iff$ X is a martingale in each of its coordinates $\iff$ X is an i-martingale for each of it's i-coordinates. To see this we extend the approach given in [15]. Let Δ denote an increment in $\mathbb{R}_+^n$ with

$$\Delta = (z, z'] = ((z_1, z_2, \ldots, z_i, \ldots, z_n), (z_1{}', z_2{}', \ldots, z_i{}', \ldots, z_n{}')] \,.$$

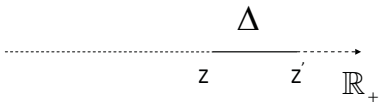

Fig 4. $\Delta = (z, z']$ increment for $\mathbb{R}_+$.

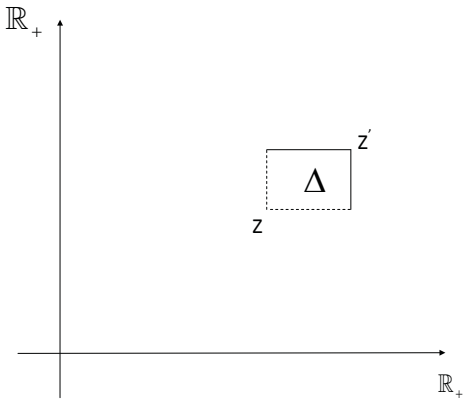

Fig 5. $\Delta = (z, z']$ increments for $\mathbb{R}_+^2$.

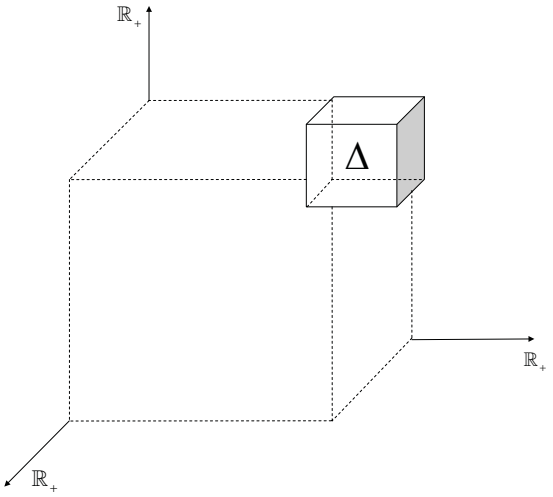

Fig 6. $\Delta = (z, z']$ increments for $\mathbb{R}_+^3$.

$X(\Delta)$ may be represented as a sum of terms of the form $X_{t'} - X_t$ with

$$t' = (t_1, t_2, \ldots, t_{i-1}, z_i', t_{i+1}, \ldots, t_n) \text{ and } t = (t_1, t_2, \ldots, t_{i-1}, z_i, t_{i+1}, \ldots, t_n).$$

Each t_j value is constant for $j \neq i$ and is either z_j' or z_j. For each such difference we have:

$$\mathbb{E}(X_{t'} - X_t|\mathcal{F}_z^i) = \mathbb{E}(X_{t'} - X_t|\mathcal{F}_t^i) = \mathbb{E}(X_{t'} - X_t|\mathcal{F}_z) = 0$$

The result $\mathbb{E}(X(\Delta)|\mathcal{F}_z^i) = 0$, now follows.

For X an i-martingale $\forall\, i \in \{1, 2, \ldots, n\} \Longrightarrow X$ is a martingale over $\mathbb{R}_+^n$ argue as in [15].

□

2.7 Stochastic Integrals

We now consider the classical Itô and Wong-Zakai stochastic integrals [49, 58, 141] with respect to Brownian motion.

2.7.1 The Itô Integral

Let $W = (W_t)_{t\geq 0}$ denote Brownian motion for the space $(\Omega, \mathcal{F}, P)$ with respect to a filtration $\mathbb{F}$. So W is an $\mathbb{F}$ martingale.

let $L^2(P)$ denote the set of measurable functions for $(\Omega, \mathcal{F}, P)$ such that $||f||^2 < \infty$.

Let $\mathcal{E}$ denote the vector space of maps $H : \Omega \times [0, \infty) \longrightarrow \mathbb{R}$ of the form $H_t(\omega) = \sum_{i=1}^{n} h_{t-1}(\omega)\chi_{(t_{i-1},t_i]}$ with $n \in \mathbb{N}$, $0 = t_0 < t_1 < \cdots < t_n$, h_{i-1} bounded and $\mathcal{F}_{i-1}$ measurable. $\mathcal{E}$ is referred to as the vector space of predictable simple processes.

Classically $\mathcal{E}$ is equipped with a (pseudo) norm

$$\| H\|_\epsilon^2 = \sum_{i=1}^{n} \mathbb{E}\left[h_{i-1}^2\right](t_{i-1}, t_i] = \mathbb{E}\left[\int_0^\infty H_s^2 ds\right]$$

Definition 18. (I_t^W **and** I_∞^W) [58] Let $H \in \mathcal{E}$, W denote a Brownian motion process and $t > 0$. We define I_t^W and I_∞^W as

$$I_t^W = \sum_{i=1}^{n} h_{t-1}(W_{t_i \wedge t} - W_{t_{i-1} \wedge t}) \text{ and } I_\infty^W = \sum_{i=1}^{n} h_{t-1}(W_{t_i} - W_{t_{i-1}})$$

Let $\mathcal{E}_0 = \{H : H \text{ is product measurable, adapted and } \| H\|^2 = \mathbb{E}\left[\int_0^\infty H_t^2 dt\right] < \infty\}$. For $\mathcal{E}$ a subspace of $\mathcal{E}_0$, the closure of $\mathcal{E}$ in $\mathcal{E}_0$ will be denoted by $\overline{\mathcal{E}}$.

Definition 19. (The Itô Integral) [58] Let $H \in \mathcal{E}$. The Itô integral is defined to be $\int_0^\infty H_s dW_s := I_\infty^W(H)$, the continuous extension of the map $I_\infty^W : \mathcal{E} \longrightarrow L^2(P)$ to the closure $\overline{\mathcal{E}}$ of $\mathcal{E}$

Theorem 3. (Ito Formula) [58] Let W denote a Brownian motion process. Let t be small, such that W_t is of order $\sqrt{t}$. We formally write $dW_t = \sqrt{t}$ and carry out a Taylor expansion of $F \in \mathcal{C}^2(\mathbb{R})$ with derivative $F^{'}$. Then

$$dF(W_t) = F^{'}(W_t)dW_t + \frac{1}{2}F^{''}(W_t)(dW_t)^2 = F^{'}(W_t)dW_t + \frac{1}{2}F^{''}(W_t)\,dt$$

Which in integral form becomes:

$$F(W_t) - F(W_0) = \int_0^t F^{'}(W_s)dW_s + \int_0^t \frac{1}{2}F^{''}(W_s)ds$$

The following theorem is included as an example of a multidimensional Ito formula, and is given for completeness. The notation is not employed in subsequent discussions and we therefore defer to [58] for further details.

Theorem 4. (Multidimensional Ito Formula) [58] Let Y be a function with continuous square variation. Let $F \in \mathcal{C}^2\left(\mathbb{R}^d\right)$. Then

$$\begin{aligned} F(Y_T) - F(Y_0) &= \int_0^T \nabla F(Y_s) dY_s + \frac{1}{2} \sum_{k,\,l=1}^{d} \int_0^T \delta_k \delta_l F(Y_s) d\langle M^k, M^l \rangle_s \\ &= \sum_{k,\,l=1}^{d} \int_0^t \sigma_s^{k,l} \delta_k F(Y_s) dW_s^l + \sum_{k,\,l=1}^{d} \int_0^t b_s^k \delta_k F(Y_s) ds \\ &\quad + \frac{1}{2} \sum_{k,\,l=1}^{d} \int_0^t a_s^{k,l} \delta_k \delta_l F(Y_s) ds \end{aligned}$$

In particular for Brownian motion, we have:

$$F(W_T) - F(W_0) = \sum_{k=1}^{d} \int_0^t \delta_k F(W_s) dW_s^k + \frac{1}{2} \int_0^t \triangle F(W_s) ds.$$

2.7.2 The Wong-Zakai Integral

Related to the work of Cairoli [16], Cairoli and Walsh [15] and John Walsh [138], Wong and Zakai [141] developed a stochastic calculus for multiparameter processes involving two types of integral, the first an analogue of the Itô integral, related to the integral developed by Cairoli, and the second a new type of stochastic integral, described by John Walsh [139] as being defined over "cockeyed" increments.

Definition 20. (The Wong-Zakai Integral) [141, 142, 143] Let $T = [0,1] \times [0,1]$ and $\{W_z, \mathcal{F}_z, z \in T\}$ be a Wiener process.

$$I_1(\phi) = \int_T \phi(z) dW_z$$

is defined as a generalisation of the Itô integral and referred to as an integral of the first type.

A second stochastic integral

$$I_2(\psi) = \int_T \int_T \psi(z_1, z_2) dW_{z_1}\, dW_{z_2}$$

is defined for so called 'unordered' $z_1 = (x_1, y_1)$ and $z_2 = (x_2, y_2)$ for which $x_1 \leq x_2$, and $y_1 \geq y_2$, points described as "cockeyed" by John Walsh.

The action [141] of I_1 is defined for random functions ϕ satisfying the following conditions:

1. $\phi(\omega, z)$ is a bimeasurable function of (ω, z) with respect to $\mathcal{F} \otimes \mathcal{S}$ with $\mathcal{S}$ the σ algebra of Borel sets in T

2. $\forall\, z \in T$, ϕ_z is $\mathcal{F}_z$ measurable

3. $\int_T E\phi_z^2 < \infty$

For I_2, [141] the action is defined for random functions $\psi(\omega, z, z')$ defined on $\Omega \times T \times T$ satisfying the following conditions:

1. $\psi(\omega, z, z')$ is jointly measurable with respect to $\mathcal{F} \otimes \mathcal{S} \otimes \mathcal{S}$ with $\mathcal{S}$ the σ algebra of Borel sets in T

2. $\forall$ pairs z and $z' \in T \times T$, $\phi(\omega, z, z')$ is $\mathcal{F}_{z \wedge z'}$ measurable

3. $E \int_T \int_T \phi^2(z, z') < \infty$

The above integrals satisfy linearity, inner product and martingale properties and are orthogonal.

2.7.3 The Imkeller Integral

We introduce the Imkeller integral at this point for completeness. Our primary interest here has been the extension of stochastic integrals to $\mathbb{R}^3_+$ and the claim of a new type of integral on page 16 of the paper. We continue our discussion of these increments in Chapter 4, but do not employ the notation used, in our discussion.

Definition 21. (The Imkeller Integral) [48] Let M be a strong martingale with $E(M_1^{4N}) < \infty$.

Let $\mathcal{I} = \{\mathcal{T}\}$

Let $(T, \phi) \in \mathcal{I}$.

The linear mapping $I_0^{(T,\phi)} : \mathcal{E}_{\mathcal{T}} \longrightarrow L^2(\Omega, \mathcal{F}, P)$,

$$\sum_{1 \leq i \leq n} a_i 1_{F_i} \prod_{T \in \mathcal{T}} 1_{A_i^T} \rightarrow \sum_{1 \leq i \leq n} a_i 1_{F_i} \prod_{T \in \mathcal{T}^1} \Delta_{A_i^T} M \prod_{T \in \mathcal{T}^0} [M] (A_i^T)$$

is referred to as an elementary $(T, \phi)-$ integral

We defer to the paper [48] by Peter Imkeller for details regarding the notation.

2.8 Fubini's Theorem

We recall [140] the classical form of Fubini's Theorem for general $L^2(\mathbb{R}^n, d\mu)$

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a point of n - dimensional interval I_1,

$$I_1 = \{\mathbf{x} : a_i \leq x_i \leq b_i,\ i = 1, 2, 3, \ldots, n\}$$

Let $\mathbf{y} = (y_1, y_2, \ldots, y_m)$ be a point of m - dimensional interval I_2,

$$I_2 = \{\mathbf{y} : c_j \leq y_j \leq d_j,\ j = 1, 2, 3, \ldots, m\}$$

The Cartesian product $I = I_1 \times I_2$ denotes the $n + m$ dimensional interval consisting of points $(\mathbf{x}, \mathbf{y}) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$

A function $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ acting on I will be written $f(\mathbf{x}, \mathbf{y})$ and its integral $\int_I f$ will be denoted by $\int\int_I f(x, y) dx dy$

Theorem 5. (Fubini's Theorem) [140]. Let $f(x,y) \in L(I), I = I_1 \times I_2$. Then
a) for almost every $x \in I_1, f(x,y)$ is measurable and integrable on I_2 for y;
b) as a function of x, $\int_{I_2} f(x,y)dy$ is measurable and integrable on I_1 and

$$\int\int_I f(x,y)dx\,dy = \int_{I_1}[\int_{I_2} f(x,y)dy]dx$$

Fubini's theorem also extends to Itô integrals taking the following form.

Theorem 6. [58] Let $X \in \mathcal{C}_{qv}$. Let $g : [0,\infty) \longrightarrow \mathbb{R}$ be continuous and (in the interior) twice continuously differentiable in the second coordinate with derivative $\delta_2 g$. Then

$$\int_0^s \left(\int_0^t g(u,v)du\right) dX_v = \int_0^t \left(\int_0^s g(u,v)dX_v\right) du$$

and

$$\int_0^s \left(\int_0^v g(u,v)du\right) dX_v = \int_0^s \left(\int_u^s g(u,v)dX_v\right) du$$

2.9 Algebras

Definition 22. (Field) We define a field to be an abelian group with respect to both addition and multiplication that also satisfies the distributive law and the no-divisors of zero law.

Definition 23. (Vector (Linear) Space) A vector (linear) space (V,F) over a field F, is defined to be a set of elements V, such that $(V,+)$ forms an abelian group and $\forall\,\alpha,\beta \in F, v, v_1, v_2 \in V$:

a) $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$

b) $(\alpha + \beta)v = \alpha v + \beta v$

c) $\alpha(\beta v) = (\alpha\beta)v$

d) $1.v = v,$ with $1 \in F$ (the multiplicative identity from F)

Definition 24. (Inner Product Space) An Inner Product Space is a vector space V with an inner product defined for all elements $v_1, v_2 \in V$. For this discussion inner products will be linear in their first argument and conjugate linear in their second argument.

Definition 25. (Hilbert Space) A Hilbert space $\mathcal{H}$ is a complete inner product space.

Inner products may also be viewed as norms via the relation $\| x \| = \sqrt{(x,x)}$. For $x_i \perp x_j$, for all $i \neq j$, $1 \leq i, j \leq n$ we note that $\| \sum_{i=1}^{n} x_i \|^2 = \sum_{i=1}^{n} \| x_i \|^2$. For real valued inner products we have the relation, $(x,y) = \frac{1}{4}\left[\| x+y \|^2 - \| x-y \|^2 \right]$ whilst for complex inner product spaces we have the relation $(x,y) = \frac{1}{4}\left[\| x+y \|^2 - \| x-y \|^2 \right] + i\left[\| x+iy \|^2 - \| x-iy \|^2 \right]$. It follows that an inner product space may also be viewed as a normed space, by which we mean a vector space with a norm defined upon it.

Definition 26. (Banach Space) A Banach Space is defined to be a normed space that is complete with respect to its norm.

Definition 27. Algebra [63] An Algebra $\mathcal{A}$ over a field F is a vector space $\mathcal{A}$ over F such that for each ordered pair of elements $x, y \in \mathcal{A}$ a unique product $xy \in \mathcal{A}$ is defined such that $\forall x, y, z \in \mathcal{A}$ and scalars $\alpha \in F$:

$$(xy)z = x(yz)$$

$$x(y+z) = xy + xz$$

$$(x+y)z = xz + yz$$

$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

A normed space that is also an algebra satisfying Holders inequality for each of its elements is described as a normed algebra. So $\forall x, y$ in the algebra $\mathcal{A}$,

$$||xy|| \leq ||x||||y||.$$

If the normed algebra also has an identity then the norm of the identity is 1. A complete, normed algebra is is said to be a Banach Algebra. If additionally $\forall x \in \mathcal{A}, ||x|| = ||x^*||$ then $\mathcal{A}$ is said to be a C^*-Algebra.

Definition 28. (GNS) [10, 127] Given a C^* - Algebra $\mathcal{A}$ with identity, and a state ω, there is a Hlbert space $\mathcal{H}_\omega$ and a representation $\pi_\omega : \mathcal{A} \longrightarrow \mathcal{B}(\mathcal{H}_\omega)$ s.t.

a) $\mathcal{H}_\omega$ contains a cyclic vector ψ_{π_ω}

b) $\omega(A) = (\psi_{\pi_\omega}, \pi_\omega(\mathcal{A})\psi_{\pi_\omega})$,

c) every other representation π in a Hilbert Space $\mathcal{H}_\pi$ with a cyclic vector ψ such that $\omega(A) = (\psi, \pi(A)\psi)$, is unitarily equivalent to π_ω

Definition 29. (Tensor product) [10, 55, 80, 88]. Let $\mathcal{E}$ denote the set of conjugate bilinear forms $\{\phi_1 \otimes \phi_2\}$ acting on $\mathcal{H}_1 \times \mathcal{H}_2$ by the rule $(\phi_1 \otimes \phi_2)[h_1, h_2] = (h_1, \phi_1)(h_2, \phi_2)$. We may define an inner product on $\mathcal{E}$ by $(\phi \otimes \chi, \mu \otimes \nu) = (\phi, \mu)(\chi, \nu)$, extend by linearity and hence define the Tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ of two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ as the completion of the set of finite linear combinations of elements in $\mathcal{E}$. We note that in agreement with the finite dimensional tensor product structures found in, for example, quantum information theory [78]:

a) $\forall \alpha \in \mathbb{C} \quad \alpha(|v\rangle \otimes |w\rangle) = (\alpha|v\rangle \otimes |w\rangle) = (|v\rangle \otimes \alpha|w\rangle)$

b) $(\sum_{i=1}^{m} |v_i\rangle \otimes |w\rangle) = \sum_{i=1}^{m} (|v_i\rangle \otimes |w\rangle)$

c) $|v\rangle \otimes (\sum_{j=1}^{n} |w_j\rangle) = \sum_{j=1}^{n} (|v\rangle \otimes |w_j\rangle)$

d) $\{|i\rangle\}_{i=1}^{m}$ a basis for $\mathcal{H}_1$ and $\{|j\rangle\}_{j=1}^{m}$ a basis for $\mathcal{H}_2 \Longrightarrow \{|i\rangle \otimes |j\rangle\}$ a basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ with dimension mn.

Theorem 7. [78, 88]. Let $\{\phi_k\}$ and $\{\psi_l\}$ denote orthonormal bases for Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. Then $\{\phi_k \otimes \psi_l\}$ is an orthonormal basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Theorem 8. [88]. Let (M_1, μ_1) and (M_2, μ_2) be measurable spaces so that $L^2(M_1, d\mu_1)$ and $L^2(M_2, d\mu_2)$ are separable. Then

a) There is a unique isomorphism from the tensor product $L^2(M_1, d\mu_1) \otimes L^2(M_2, d\mu_2)$ to $L^2(M_1 \times M_2, d\mu_1 \otimes d\mu_2)$ so that $f \otimes g \mapsto fg$.

b) If $\mathcal{H}'$ is a separable Hilbert space , then there is a unique isomorphism from $L^2(M_1, d\mu_1) \otimes \mathcal{H}')$ to $L^2(M_1, d\mu_1; \mathcal{H}'))$ so that $f(x) \otimes \phi \mapsto f(x)\phi$

c) There is a unique isomorphism from $L^2(M_1 \times M_2, d\mu_1 \otimes d\mu_2)$ to $L^2(M_1, d\mu_1; L^2(M_2, d\mu_2))$ such that $f(x, y)$ is taken into the function $x \mapsto f(x, \circ)$.

2.10 Non Commutative Probability

In the quantum setting we will work with a stochastic base of the form $(\mathcal{H}, \mathcal{A}, (\mathcal{A}_z), m, I)$ in which $\mathcal{H}$ denotes a Hilbert space structure, (for example Fermi-Fock space), $\mathcal{A}$ may denote either a von Neumann Algebra, a $C*$-Algebra, or a Hilbert Space, $(\mathcal{A}_z)$ will denote an associated filtration of $\mathcal{A}$, m will represent a gage or state, (a linear functional acting on $\mathcal{A}$) and I will denote a subset of the parameter set, $\mathbb{R}^n_+$, with $z \in I \subseteq \mathbb{R}^n_+$.

Definition 30. Topologies on $\mathcal{B}(\mathcal{H})$ [82, 88] Various topologies exist for $\mathcal{B}(\mathcal{H})$, the set of bounded operators acting on a Hilbert Space. We define four such topologies:

a) The Uniform topology (also known as the Norm topology) on $\mathcal{B}(\mathcal{H})$ is the topology induced by the norm $\| A \| = \underset{x \neq 0}{sup} \frac{\|Ax\|}{x}$ with $A \in \mathcal{B}(\mathcal{H})$ and $x \neq 0 \in \mathcal{H}$

b) The Strong topology on $\mathcal{B}(\mathcal{H})$ is the locally convex vector space topology associated with the family of semi-norms of the form $x \mapsto \| Ax \|$ with $A \in \mathcal{B}(\mathcal{H})$ and $x \in \mathcal{H}$

c) The Weak topology on $\mathcal{B}(\mathcal{H})$ is the locally convex vector space topology associated with the family of semi-norms of the form $x \mapsto |(Ax|y)|$ with $A \in \mathcal{B}(\mathcal{H})$ and x, $y \in \mathcal{H}$

d) The σ-weak topology on $\mathcal{B}(\mathcal{H})$ (also known as the ultraweak topology) is the locally convex vector space topology associated with the family of semi-norms of the form $A \mapsto |\,Tr(Ax)|$ with $A \in \mathcal{B}(\mathcal{H})$ and $x \in T(\mathcal{H})$.

From an operator perspective we have the following:

Definition 31. Operator Convergence [63] Let X and Y be normed spaces. A sequence (A_n) of operators $A_n \in \mathcal{B}(X,Y)$ is said to be:
1) Uniformly Convergent if (A_n) converges in the norm on $\mathcal{B}(X,Y)$. So $\exists A \in \mathcal{B}(X,Y)$ such that $\| A_n - A \| \longrightarrow 0$;
2) Strongly Convergent if (A_n) converges strongly in Y. So $\exists A \in \mathcal{B}(X,Y)$ such that $\forall\, x \in X$, $\| A_n x - Ax \| \longrightarrow 0$;
3) Weakly Convergent if $(A_n x)$ converges weakly in Y for every $x \in X$. So $\exists A \in \mathcal{B}(X,Y)$ such that $\forall\, x \in X$, $\forall\, f \in Y'$, $|f(A_n x) - f(Ax)| \longrightarrow 0$;

Definition 32. (Filtration) [62] Let $\mathcal{A}$ denote a von Neumann algebra, a filtration (or nest of algebras) $(\mathcal{A}_z)$ of $\mathcal{A}$ consists of von Neumann subalgebras of $\mathcal{A}$ in which $\cup_z(\mathcal{A}_z)$ are ultraweakly dense in $\mathcal{A}$, $\cup_{z<z'}(\mathcal{A}_z)$ is ultraweakly dense in $\mathcal{A}_{z'}$ and $\cap_{z>z'}\mathcal{A}_z = \mathcal{A}'_z$.

Definition 33. (W^*-Algebra) [92, 93, 128]. A C^*-Algebra, $\mathcal{U}$ is said to be a W^*-Algebra if it is a dual space as a Banach space.

W^*-Algebras have been shown [92] to be a von Neumann algebras by Shôichirô Sakai.

Definition 34. (Gage) [98]. A gage on a W^*-algebra $\mathcal{A}$ is a completely additive non-negative function m on the projections in $\mathcal{A}$ which is unitarily invariant: $m(U^*PU) = m(P)$ if P is any projection and U is any unitary in $\mathcal{A}$; and has the (non-triviality) feature that any nonzero projection in $\mathcal{A}$ bounds a projection in $\mathcal{A}$ on which m is finite and positive.

We will work with a faithful, central, normal gage.

Example 8. Define m on $\mathcal{A}$ by $m(.) = (\Omega, .\Omega)$; where Ω denotes $1 \in \mathbb{C} = \mathcal{H}_0 \subset \mathcal{F}(\mathcal{H})$ (the Fermi-Fock space). m is said to be:

a) faithful if $A \in \mathcal{A}, A \geq 0, m(A) = 0 \Longrightarrow A = 0$,

b) central if $\forall A, B \in \mathcal{A},\ m(AB) = m(BA)$

c) normal if given a family $\{P_\alpha\}$ of mutually orthogonal projections in $\mathcal{A}$,
$m(\sum_\alpha P_\alpha) = \sum_\alpha m(P_\alpha)$

We note that the gage m is tracial on the Clifford algebra generated by $\Psi(f) = a^*(f) + a(f)$. We also note that for $\mathcal{H}_1$, $\mathcal{H}_2$ orthogonal real subspaces of $\mathcal{H}$ the von Neumann algebras $\mathcal{A}_1$, $\mathcal{A}_2$ generated by the $\psi(u)$, as u varies in $\mathcal{H}_1$, $\mathcal{H}_2$ resp. are independent: $m(AB) = m(A)m(B)$, for $A \in \mathcal{A}_1, B \in \mathcal{A}_2$ [39, 96].

Definition 35. (State) [10] A state ω is a positive linear functional (ω is an element in the dual of $\mathcal{U}$ s.t. $\omega(A^*A) \geq 0$) over the *-algebra $\mathcal{U}$ with $\| \omega \| = 1$

2.11 Noncommutative L^p Spaces

Noncommutative analogues [95, 130] of classical L^p spaces may be formed for $1 \leq p < \infty$, in which $L^p(\mathcal{A})$ is taken to be the completion of $\mathcal{A}$ with respect to the norm $\| a\|_p = m(|a|^p)^{1/p} = (\Omega, (a^*a)^{p/2}\Omega)^{1/p}$. These may be extended to include $L^\infty(\mathcal{A})$ as $\mathcal{A}$ with the operator norm $\| a\|_\infty = \| a\|$.

Definition 36. (Conditional Expectation) [125, 126, 131, 132, 133, 134] Let $\mathcal{A}$ be a von Neumann Algebra and $\mathcal{B}$ be a von Neumann subalgebra of $\mathcal{A}$. Let $E : \mathcal{A} \longrightarrow \mathcal{B}$ be a linear mapping s.t.

a) E is a σ-weakly continuous faithful projection of norm 1

b) $\forall x \in \mathcal{A},\ E(x^*x) \geq 0$

c) $\forall x, z \in \mathcal{B}, \forall y \in \mathcal{A},\ E(xyz) = xE(y)z$

d) $\forall x \in \mathcal{A},\ E(x^*)E(x) \leq E(x^*x)$

Then E is said to be a Conditional Expectation.

Noncommutative Conditional Expectations [39, 86] may be established for $L^p(\mathcal{A})$ spaces as can filtrations, adapted processes martingales and stochastic integrals. We consider such constructions in the next chapter, defined over the general parameter space $\mathbb{R}^n_+$ with $n \in \mathbb{N}^+$.

2.12 Summary

In this chapter we have presented background material from various sources as a reference point for material in the chapters that follow. In the next chapter we present standard models relating to quantum stochastic integrals.

Chapter 3

Standard Models

3.1 Fock Space and Second Quantisation

Each of the models discussed in this chapter involves a stochastic base of the form $(\mathcal{H}, \mathcal{A}, g, (\mathcal{A}_z), \mathbb{R}^n_+)$, in which $\mathcal{H}$ denotes different Fock space constructions. Fock spaces were introduced by V. Fock [35] in 1932. Examples [7, 66] of Fock space are to be found in, quantum probability, quantum field theory, quantum theory of light, and more recently quantum information processing. They have been used in the representation of multipartite states and to describe their subsequent development within *Fermi-Dirac* and *Bose-Einstein* systems. In 1953, J. Cook published *The Mathematics of Second Quantisation* [20] in response to inconsistencies emerging from the *first quantisation*.

3.1.1 Fock Space

Definition 37. (Fock Space) [11, 20, 35] Let $\mathcal{H}$ denote a Hilbert space and $\mathcal{H}^r$ the r-fold tensor product of $\mathcal{H}$ with itself. We define the free (or full) Fock space generated by $\mathcal{H}$ as

$$\mathcal{F}(\mathcal{H}) = \bigoplus_{r\geq 0}^{\infty} \mathcal{H}^r = \mathbb{C} \oplus \mathcal{H} \oplus \mathcal{H}^2 \oplus \mathcal{H}^3 \oplus \ldots\ldots\ldots$$

with $\mathcal{H}^0 = \mathbb{C}$. $\mathcal{F}(\mathcal{H})$ consists of sequences of vectors $(\psi^r)_{n\geq 0}$, in which each $\psi^r \in \mathcal{H}^r$ and at most, only a finite number of non-zero terms are to be found. The tensor space $\mathcal{H}^r$ may be identified with sequences of the form $(0, \dots, 0, \psi^r, 0, \dots) \in \mathcal{F}(\mathcal{H})$ in which terms not in the rth position are defined to be zero.

Proposition 1. [88] Let $\mathcal{H}$ be a separable Hilbert space. Then the inner product closure of $\mathcal{H}^r$ and $\mathcal{F}(\mathcal{H})$ form Hilbert spaces.

Proof. For $\mathcal{H}^r$ and $\mathcal{F}(\mathcal{H})$, closure, addition and scalar multiplication laws follow by construction, establishing $\mathcal{H}^r$ as a linear space. For the inner product rules on $\mathcal{H}^r$ with respect to the conjugate bilinear form $(\ ,\ )_{\mathcal{H}^r} = \prod_{i=1}^{r} (\ ,\ )_{\mathcal{H}}$ we proceed as follows. Let $\psi^r \in \mathcal{H}^r = \overset{r}{\underset{i=1}{\otimes}} \mathcal{H}^i = \mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, the completion of $\mathcal{E}^1$ with respect to the inner product $(\ ,\ )_{\mathcal{H}^r}$. $\mathcal{H}$ has an orthonormal basis $\{e_i\}$ from which it follows that $\{\overset{r}{\underset{j=1}{\otimes}} e_{i_j}\}$ is an orthonormal basis for $\mathcal{H}^r$. $\psi^r \in \mathcal{H}^r$ may be written in the form $\psi_1 \otimes \cdots \otimes \overset{i}{\psi}_r$ with $\psi_i \in \mathcal{H} \Longrightarrow (\psi_1 \otimes \cdots \otimes \psi_r, \psi_1 \otimes \cdots \otimes \psi_r)_{\mathcal{H}^r} = \prod_{i=1}^{r} (\psi_i, \psi_i)_{\mathcal{H}} \geq 0$. For $(\psi_1 \otimes \cdots \otimes \psi_r, \psi_1 \otimes \cdots \otimes \psi_r)_{\mathcal{H}^r} = 0$ there exits j with $1 \leq j \leq r$ such that $\psi_j = 0$ from which it follows that $\psi_1 \otimes \cdots \otimes \psi_r = 0$. Linearity in the first argument of $(\ ,\ )_{\mathcal{H}^r}$ follows by construction. Lastly, with respect to the inner product rules we note that $(\psi_1 \otimes \cdots \otimes \psi_r, \phi_1 \otimes \cdots \otimes \phi_r)_{\mathcal{H}^r} = \prod_{i=1}^{r} (\psi_i, \phi_i)_{\mathcal{H}} = \overline{\prod_{i=1}^{r} (\phi_i, \psi_i)}_{\mathcal{H}} = \overline{(\phi_1 \otimes \cdots \otimes \phi_r, \psi_1 \otimes \cdots \otimes \psi_r)_{\mathcal{H}^r}}$. Completeness for the Hilbert space property follows by construction. For $\mathcal{F}(\mathcal{H})$ we use the sum of the inner products defined on each $\mathcal{H}^r$, in agreement [11] with the norm $\| \psi\|^2 = |\psi^0|^2 + \sum_{i\geq 1} (\psi^i, \psi^i)$, noting that for $\bigoplus_{r\geq 0}^{\infty} \mathcal{H}^r$ only a finite number of the ψ^i are non - zero. For $\mathcal{F}(\mathcal{H})$ a Hilbert space we require the sum of inner products to be finite, and take the completion $\overline{\bigoplus_{r\geq 0}^{\infty} \mathcal{H}^r}$ of the algebraic direct sum $\mathcal{F}(\mathcal{H})$ with respect to the sum of the inner products $|\psi^0|^2 + \sum_{i\geq 1} (\psi^i, \psi^i)$. □

[1] See Definition 29 (Tensor Products) on page 25

3.1.2 Operators

Movement [11] between each of the tensor spaces $\mathcal{H}^r$ may be achieved through the action of creation and annihilation operators $a^*(f)$ and $a(f)$ with $f \in \mathcal{H}$, on the $\mathcal{H}^r$, in which

$$a^*(f)(\overset{r}{\underset{i=1}{\otimes}} f_i) = \sqrt{r+1} \overset{r+1}{\underset{i=1}{\otimes}} f_i \text{ with } f_1 = f$$

and

$$a(f)(\overset{r}{\underset{i=1}{\otimes}} f_i) = \sqrt{r}(f, f_1) \overset{r}{\underset{i=2}{\otimes}} f_i$$

For $\mathcal{H} = L^2(\mathbb{R}^n_+)$ and $\mathfrak{h} = L^2(\mathbb{R}_+)$ it may be shown [88] that
$\mathcal{H} = L^2(\mathbb{R}^n_+) \cong L^2(\mathbb{R}_+)^n = \mathfrak{h}^n$. It follows that we may identify the $\mathcal{F}(\mathcal{H})$ as subsets of $\mathcal{F}(\mathfrak{h})$ for each value of n and extend the association between $\mathcal{F}(\mathfrak{h})$ and its creation and annihilation operator a^* and a, to a family $(\mathcal{F}(\mathfrak{h}), \mathcal{F}(\mathfrak{h}^r), \{a^\#_r\}_{n\geq 1})$ of Fock spaces and associated operators in which $a^\#_r$ denotes a^*_r and a_r the creation and annihilation operators for $\mathcal{F}(\mathfrak{h}^r) = \mathcal{F}(L^2(\mathbb{R}^r_+))$ as opposed to $\mathcal{F}(\mathfrak{h})$. Summarising, we have the following.

Lemma 1. Let $\mathcal{H} = L^2(\mathbb{R}^n_+)$ and $\mathfrak{h} = L^2(\mathbb{R}_+)$. Then for $n \in \mathbb{N}^+$ $\mathcal{F}(\mathcal{H})$ may be identified as a sub-Fock Space of $\mathcal{F}(\mathfrak{h})$

Two subspaces of $\mathcal{F}(\mathcal{H})$ of particular interest are the *Boson-Fock* and *Fermi-Fock* spaces $\mathcal{F}_\pm(\mathcal{H})$ in which $\mathcal{F}_+(\mathcal{H})$ consists of symmetric sequences $(\psi^r)_{r\geq 0}$ and $\mathcal{F}_-(\mathcal{H})$ anti-symmetric sequences, reflecting the property that bosons may interchange position without detection

$$\psi^r = \psi(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_r) = \psi(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_r)$$

whilst a change in position between any two fermions results in a change in sign

$$\forall i \neq j,\ \psi^r = \psi(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_r) = -\psi(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_r)$$

The Boson-Fock subspace $\mathcal{F}_+(\mathcal{H})$ of $\mathcal{F}$ may be obtained by employing the symmetric operator S to $\mathcal{F}(\mathcal{H})$ as

$$\mathcal{F}_+(\mathcal{H}) = S\mathcal{F}(\mathcal{H}) \text{ by } \overset{r}{\underset{i=1}{\otimes}} f_i \overset{S}{\longmapsto} \underset{\pi}{\Sigma} \overset{r}{\underset{i=1}{\otimes}} f_{\pi(i)} \text{ for each } \mathcal{H}^r \text{ in } \mathcal{F}$$

with $\pi \in S_r$ the set of permutations for $1, 2, \ldots, r$. Similarly, we apply the anti-symmetric operator A to $\mathcal{F}(\mathcal{H})$ to obtain the Fermi-Fock subspace

$$\mathcal{F}_-(\mathcal{H}) = A\mathcal{F}(\mathcal{H}) \text{ by } \overset{r}{\underset{i=1}{\otimes}} f_i \overset{A}{\longmapsto} \underset{\pi}{\Sigma}(-1)^{\text{order of } \pi} \overset{r}{\underset{i=1}{\otimes}} f_{\pi(i)}$$

for each $\mathcal{H}^r$ in $\mathcal{F}(\mathcal{H})$. The Bose-Fock and Fermi-Fock spaces each form Hilbert spaces.

3.1.3 CAR and CCR Relations

The creation and annihilation operators satisfy the following relations.

Definition 38. *[11, 78]* The Canonical Anticommutation Relations for the creation and annihilation operators are defined as

$$\{a^*(f), a^*(g)\} = a^*(f)a^*(g) + a^*(g)a^*(f) = 0$$
$$\{a(f), a(g)\} = a(f)a(g) + a(g)a(f) = 0$$
$$\text{and } \{a(f), a^*(g)\} = a(f)a^*(g) + a^*(g)a(f) = (f, g)\mathbb{I}$$

The Canonical Commutation Relations for the creation and annihilation operators are

defined as

$$[a^*(f), a^*(g)] = a^*(f)a^*(g) - a^*(g)a^*(f) = 0$$
$$[a(f), a(g)] = a(f)a(g) - a(g)a(f) = 0$$
$$\text{and } [a(f), a^*(g)] = a(f)a^*(g) - a^*(g)a(f) = (f, g)\mathbb{I}$$

3.2 Clifford Model

We begin this section with the construction of non-commutative analogues of the classical probability space $(X, \mathcal{F}, \mu)$. These are realised in the form of a probability gage space $(\mathfrak{F}(\mathcal{H}), \mathcal{A}, g)$ [95, 94] which in turn form part of the quantum stochastic base $(\mathcal{F}(\mathcal{H}), \mathcal{A}, g, (\mathcal{A}_z), \mathbb{R}^n_+)$.

3.2.1 The Probability Gage Space

For the Clifford quantum stochastic base $\mathcal{H}$ denotes $L^2\left(\mathbb{R}^n_+\right)$, described as a fermion one particle space for $\mathfrak{F}(\mathcal{H})$ the associated antisymmetric fermi - Fock space defined over $\mathcal{H}$ [11, 20, 35, 54, 72, 108, 119].

The $\mathcal{A}$ in our stochastic base is used to denote the von Neumann Algebra of operators obtained in the weak closure of the set of polynomials formed by elements of the form $\psi(f) = a(f)^* + a(f)$, with $f \in L^2_{loc}(\mathbb{R}^n_+)$. We note that $\forall f \in L^2_{loc}(\mathbb{R}^n_+)$ the $\psi(f)$ are self adjoint since the operators $a^*(f)$ and $a(f)$ are each bounded.

Lemma 2. Let f and g denote real valued functions in $L^2\left(\mathbb{R}^n_+\right)$. Then the Fermi field operators $\psi(f) : \mathfrak{F}(\mathcal{H}) \longrightarrow \mathfrak{F}(\mathcal{H})$ defined by $h \mapsto \psi(f)h = (a^*(f) + a(f))h$ satisfy a form of Canonical Anticommutation Relation in which $\{\psi(f), \psi(g)\} = 2(f, g)$.

Proof.

$$\begin{aligned}
\{\psi(f),\psi(g)\} &= \psi(f)\psi(g)+\psi(g)\psi(f)\\
&= (a^*(f)+a(f))(a^*(g)+a(g))+(a^*(g)+a(g))(a^*(f)+a(f))\\
&= a^*(f)a^*(g)+a^*(f)a(g)+a(f)a^*(g)+a(f)a(g)+a^*(g)a^*(f)\\
&\qquad +a^*(g)a(f)+a(g)a^*(f)+a(g)a(f)\\
&= \{a^*(f),a^*(g)\}+\{a^*(f),a(g)\}+\{a^*(g),a(f)\}+\{a(f),a(g)\}\\
&= \{a^*(f),a(g)\}+\{a^*(g),a(f)\} \quad \text{by CAR's}\\
&= 2Re(f,g)\mathbb{I} \quad \text{by CAR's}\\
&= 2(f,g)\mathbb{I} \quad \text{since } f,g \text{ real valued}
\end{aligned}$$

□

For our gage g we define a mapping from $L^\infty(A)=\mathcal{A}\longrightarrow\mathbb{C}$ by $a\mapsto g(a)=(\Omega,a\Omega)$, which may be used to generate associated L^p spaces with norm

$$\parallel a \parallel_p = g(|a|^p)^{1/p} = (\Omega,(a^*a)^{p/2}\Omega)^{1/p}$$

3.2.2 The Clifford Stochastic Base

To complete our stochastic base we extend the probability gage space to include an index set $I\subseteq\mathbb{R}^n_+$ and a filtration of subsets of $\mathcal{A}$ defined on posets from $\mathbb{R}^n_+$. The filtrations $(\mathcal{A}_z)_{z\in\mathbb{R}^n_+}$ are generated by conditional expectations (projections), of the form $g(\circ|\mathcal{B})$ with $\mathcal{B}\subseteq\mathcal{A}$. Closely related to the stochastic base and subsequent development of stochastic integrals are stochastic processes of the form (ψ_z) generated by the Fermi field operators ψ via the mapping $\psi(f)\mapsto\psi_z=\psi(\chi_{[0,z]}f)$ in which $[0,z]$ denotes the n-dimensional cuboid with infimum zero and supremum z an element in the partially ordered index set. The resulting stochastic process is a centred martingale. The

conditional expectation exists since the state is tracial on the algebra generted by the $\psi(f)$'s and may be extended [86] to a contraction $L^p(\mathcal{A}) \longrightarrow L^p(\mathcal{B})$ with $1 \leq p \leq \infty$.

3.3 The Quasi-Free CAR Model

3.3.1 The Stochastic Base

The QF CAR stochastic base takes the form $(\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H}), \mathcal{A}, \omega, (\mathcal{A}_z), \mathbb{R}^n_+)$. The Hilbert space $\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H})$ is a tensor product of anti - symmetric fermi-Fock spaces $\mathcal{F}(\mathcal{H})$ in which $\mathcal{H}$ is $L^2(R)$, and $R \subseteq \mathbb{R}^n_+$ is a closed n - dimensional cuboid with $inf\, R$ based at the origin.

The von Neumann algebra $\mathcal{A}$ is generated by the fermion creation and annihilation operators acting on $\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H})$ as f varies in $L^2(R)$. The algebra generated is a C^*-algebra $\mathcal{C}$. For $\mathcal{A}$ we take the double commutant $\mathcal{C}^{''}$ of $\mathcal{C}$. The fermion creation and annihilation operators over $\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H})$ operators are defined [33] to be:

$$b^*(f) = b_0^*((1-\rho)^{1/2} f) \otimes \mathbb{I} + \Gamma(-1) \otimes b_0(\rho^{1/2} \overline{f})$$

and

$$b(f) = b_0((1-\rho)^{1/2} f) \otimes \mathbb{I} + \Gamma(-1) \otimes b_0^*(\rho^{1/2} \overline{f})$$

Here b_0^* and b_0 denote the creation and annihilation operators over $\mathcal{F}(\mathcal{H})$, ρ denotes a measurable function on R with $0 < \rho < 1$, and the action of $\Gamma(-1)$ on $\mathcal{F}(\mathcal{H})$ is defined as $\Gamma(-1)\Omega_0 = \Omega_0$ on $\mathcal{H}_0 = \mathbb{C}$, and $\otimes^n(-1)$ on $\mathcal{H}^r = \otimes^r \mathcal{H}$.

For our gage we work with [11, 33, 85] the state $\omega : \mathcal{C} \longrightarrow \mathbb{C}$ defined by $\omega(u) = (u\Omega, \Omega)$ with $\Omega = \Omega_0 \otimes \Omega_0$, defining a gauge-invariant quasi-free state on the $C^* -$ algebra $\mathcal{C}$ in which $\omega(b^*(f)) = \omega(b(g)) = 0$ and $\omega(b^*(f)b(g)) = (\rho f, g)_{L^2(R)}$.

The filtration that we use is $(\mathcal{H}_z)$ for $z \in R$ together with projections on $\mathcal{H}$. We could use C^* filtrations or von Neumann filtrations with ω-invariant conditional expectations on $\mathcal{C}$ or $\mathcal{A}$ respectively.

As in the Clifford case the creation and annihilation operators generate centred martingales, this time in the form of $(\{b^{\#}(\chi_{R_z}u) : z \in R\})$, $b^{\#}$ denoting b^* or b.

3.4 The Quasi-Free CCR Model

3.4.1 The Stochastic Base

The Quasi-Free CCR stochastic base [11, 87, 110, 120] is defined to be $\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H})$ in which $\mathcal{F}(\mathcal{H})$ denotes the symmetric Boson-Fock space over the Hilbert space $\mathcal{H} = L^2(R)$. For the algebra $\mathcal{A}$, we employ the unital polynomial * - algebra generated by the boson creation and annihilation operators, c^* and c acting on $\mathcal{F}(\mathcal{H}) \otimes \mathcal{F}(\mathcal{H})$. These satisfy the CCR properties and are defined as:

$$c^*(f) = c_0^*((1+\tau)^{1/2}f) \otimes \mathbb{I} + \mathbb{I} \otimes c_0(\tau^{1/2}\overline{f})$$

and

$$c(f) = c_0((1+\tau)^{1/2}f) \otimes \mathbb{I} + \mathbb{I} \otimes c_0^*(\tau^{1/2}\overline{f})$$

with c_0^* and c_0 the creation and annihilation operators acting on the Boson - Fock space $\mathcal{F}(\mathcal{H})$, τ a measurable function on $\mathbb{R}_+^n$ such that $\tau \in L^\infty_{loc}(\mathbb{R}_+^n)$ and $\tau(z) > 0$

The gauge invariant quasi-free state ω takes on the role of 'gage'for the CCR stochastic base. It is defined similarly to the CAR case, with $\Omega = \Omega_0 \otimes \Omega_0$ denoting the tensor product of the boson-Fock (rather than fermi-Fock) no-particle vector. f and g are elements in $\mathcal{D}(\tau^{1/2}) = \{f : \tau^{1/2}f \in L^2(\mathbb{R}_+^n)\}$.

The filtration $(\mathcal{A}_z)$ will now denote the filtration $(\mathcal{F}(\mathcal{H})_z)$, the closure of the unital polynomial *-algebra generated the boson creation and annihilation operators $a^*(f)$ and $a(f)$ on $\mathcal{F}(\mathcal{H})$ as f varies in $L^2(\mathbb{R}^n_+)$ with support in R_z.
Once again the families $\{a^\#(\chi_{R_z}u)\Omega : z \in R\}$ form centred martingales, with $a^\#$ denoting a^* or a.

3.5 The Stochastic Base and Underlying Parameter Space

In this thesis, we work in the positive region $\mathbb{R}^n_+$ of $\mathbb{R}^n$ employing points in $\mathbb{R}^n_+$ as analogues of the indexing parameter 'time' for each of the stochastic processes defined. Parameter spaces for the case $n = 2$ and $n = 3$ have been explored in [15, 139] and [48] respectively. We explore these and more general parameter spaces further identifying 'reducible' and 'irreducible' sets in $\mathbb{R}^3_+, \mathbb{R}^4_+$ and the general parameter space $\mathbb{R}^n_+$, with a view to establishing links between these and multiparameter quantum stochastic integrals. Partially ordered sets (POSETS) in $\mathbb{R}^n_+$ lead to the development of filtrations, conditional expectations, projections and martingales employed in the construction of quantum stochastic integrals as analogues of those found in the classical theory for stochastic integration.

3.5.1 POSETS in $\mathbb{R}^n_+$

For the case $n = 1$ POSETS are defined in terms of forward increments [86], when working with Ito constructions. In this case the increment $\Delta \subset \mathbb{R}_+$ is forward of some point of interest $t \in \mathbb{R}_+$. We note that there exists just one *type* of increment for the Ito construction which we refer to as a *type 1 increment*, (see Fig. 7). For the case $n = 2$ [15, 119, 141], *type 1* increments are defined in an analogous way to the $n = 1$ case, with all points in $\Delta \subset \mathbb{R}^2_+$ are forward of some point of interest $z \in \mathbb{R}^2_+$, (see Fig. 8).

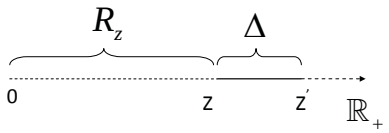

Fig 7. Type 1 increment Δ for $\mathbb{R}_+$, forward of z and R_z.

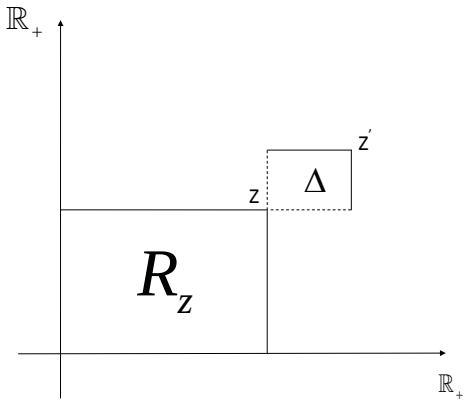

Fig 8. Type 1 increment Δ for $\mathbb{R}_+^2$, forward of z and R_z.

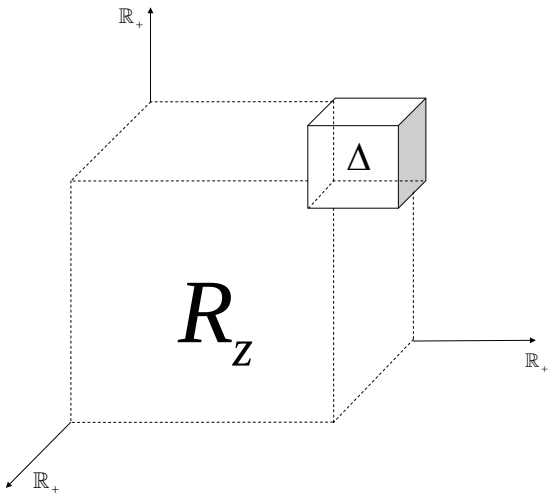

Fig 9. Type 1 increment Δ for $\mathbb{R}_+^3$, forward of z and R_z.

Following the work of Wong and Zakai, a new type of increment was established referred to as a *type 2 increment* and described by John Walsh [139] as 'cockeyed' increments. Here two increments are established forward of the region R_z, one in the 'z_1'direction, the other in an orthogonal 'z_2'direction. This corresponded to the development of a new Wong - Zakai stochastic integral.

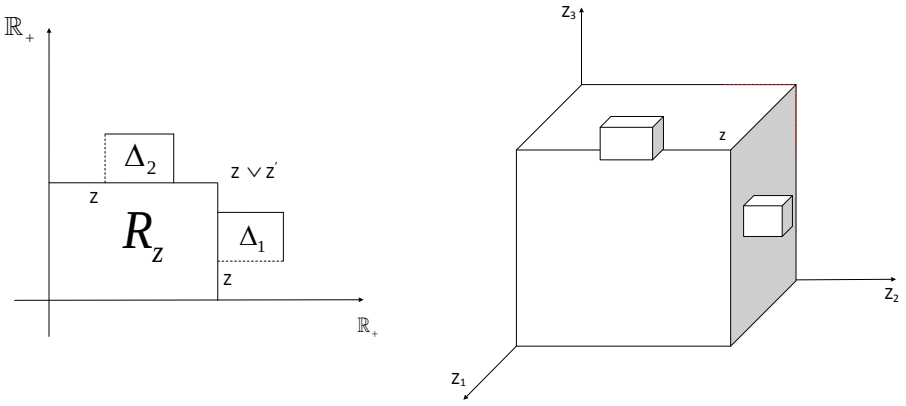

Fig 10. Type 2 Increments for $\mathbb{R}^2_+$ and $\mathbb{R}^3_+$ respectively, forward of z and R_z.

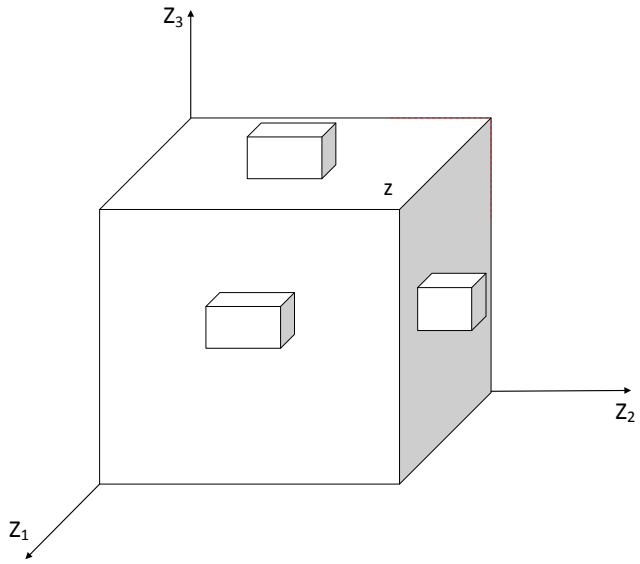

Fig 11. Type 3 increment for $\mathbb{R}^3_+$ forward of z and R_z.

For the case $n = 3$ analogues of the type 1 increment follow and a type 3 increment involving three Δ_i each forward of the 'cuboid' R_z in just one parameter.
In the case of a type 2 increment we meet more than one possibility [48]. Type 2 increments comprise of two Δ_i with Δ_1 and Δ_2 "cockeyed" again with respect to R_z in the sense suggested by John Walsh. Two possible cases for type 2 increments emerge for the case $n = 3$. Case 1 has Δ_1 forward of R_z in two directions (say x_1 and x_2 with $x_1 \perp x_2$) and Δ_2 forward of the region R_z in just one, the remaining direction (x_3 perpendicular to both x_1 and x_2). The infimum of Δ_1 wrt x_1 and x_2 lies along an edge of R_z, whilst Δ_2 is based on a face of R_z. Case 2 has Δ_1 forward of R_z in two variables (say x_1 and x_2) and Δ_2 also forward of R_z in two variables (say x_1 and x_3). It was considered that case 2 could lead to a new type of 'mixed' stochastic integral in [48]. We explore this in the next chapter.

3.6 Summary

In this chapter we have presented standard models that we will use in the development of quantum stochastic integrals over $\mathbb{R}^n_+$. The parameter space over which our stochastic processes are defined has also been introduced and examples of the different types of increment that exist for $n = 1,\ 2,\ \text{and}\ 3$. In the next chapter we continue the discussion on parameter spaces, as new material, exploring different types of increment for $n \geq 4$. The increments are categorised as irreducible or composite (reducible) and used in the development of different types of quantum stochastic integral.

Chapter 4

Stochastic Integrals

4.1 Introduction

In this chapter we extend the work carried out on quantum stochastic integrals over $\mathbb{R}_+$ and $\mathbb{R}_+^2$ to a more general setting for quantum stochastic integrals defined over $\mathbb{R}_+^n$ for $n \in \mathbb{N}^+$. We note that the possibility for different *type r increments* poses the threat of greater complexity emerging in our discussions, in contrast to our goal of simplifying the complexity involved, via the underlying parameter space.

Our findings [112, 118] at the three dimensional level lead to further exploration with a four dimensional positive parameter base and from there, to general n-dimensional parameter bases. We begin organising sets in $\mathbb{R}_+^n$ by identifying those sets (later thought of as increments) forward of an n-dimensional cuboid R_z that may be categorised as irreducible, as opposed to composite [106, 107, 116] in form. Here we are concerned with irreducibility of form with respect to n-dimensional cuboids R_z.[1]
We conjecture the following result established later as our discussion develops:

Conjecture 1. *All increments in $\mathbb{R}_+^n$ may be expressed in terms of type r increments (defined below) and hence all quantum stochastic integrals (QSI's) may be expressed in*

[1] See Fig's. 7, 8 and 9 on page 40 for R_z.

terms of Type r QSI's. Further the representation is unique up to equivalence (commutativity).

Increments throughout our discussion will therefore increase in complexity subject only to the number of available orthogonal directions parallel to the underlying 'axes'.

4.2 Type r Increments

As stated in Chapter 1, our primary motivation in this work is to simplify the approach taken with general quantum stochastic integrals where the complexity involved can quickly become daunting. The geometric approach employed leads us to different types of increment lying in $\mathbb{R}^n_+$ particularly for the case $n \geq 3$. A particular fundamental increment that we work with, is referred to as a *type r increment*.

Definition 39. (Type r Increments) Let R denote a closed cuboid in which $inf R = (0, 0, \ldots, 0)$. Let $z = (z_1, z_2, \ldots, z_n) = sup\, R$. Let $1 \leq r \leq n$. We define the characteristic function for a type r increment to be of the form $\chi_{\Delta_1} \ldots \chi_{\Delta_r}$. Each of the Δ_i denote increments forward of R (and hence the point z), in one or more of the n parameters parallel to the orthogonal axes. Each parameter is to be forward of R (and hence z), in one and only one of the r increments Δ_i. A Type r increments will be denoted by the notation $\Delta_1 \overset{\wedge}{\wedge} \ldots \overset{\wedge}{\wedge} \Delta_r$ in which the r increments Δ_i will be mutually disjoint to each other as subsets of $\mathbb{R}^n_+$.

Example 9. *See Fig 7, 8, 9, 10 and 11 on pages 40 and 41.*

Definition 40. (Type r Points) A type r point is defined to be a point of the form $(z_1, z_2, \ldots, z_r) \in \mathbb{R}^n_+ \times \ldots \mathbb{R}^n_+$ the r-fold product of $\mathbb{R}^n_+$ with itself, such that each $z_i \in \Delta_i \subseteq \mathbb{R}^n_+$ and each Δ_i a component in a type r increment $\Delta_1 \overset{\wedge}{\wedge} \ldots \overset{\wedge}{\wedge} \Delta_r$.

Example 10. A type 1 point would be a single point lying in a type 1 increment forward of R_z, whilst a type 2 point is of the form (z_1, z_2) with $z_1 \in \Delta_1$ and $z_2 \in \Delta_2$ such that $\Delta_1 \overset{\wedge}{\wedge} \Delta_2$.

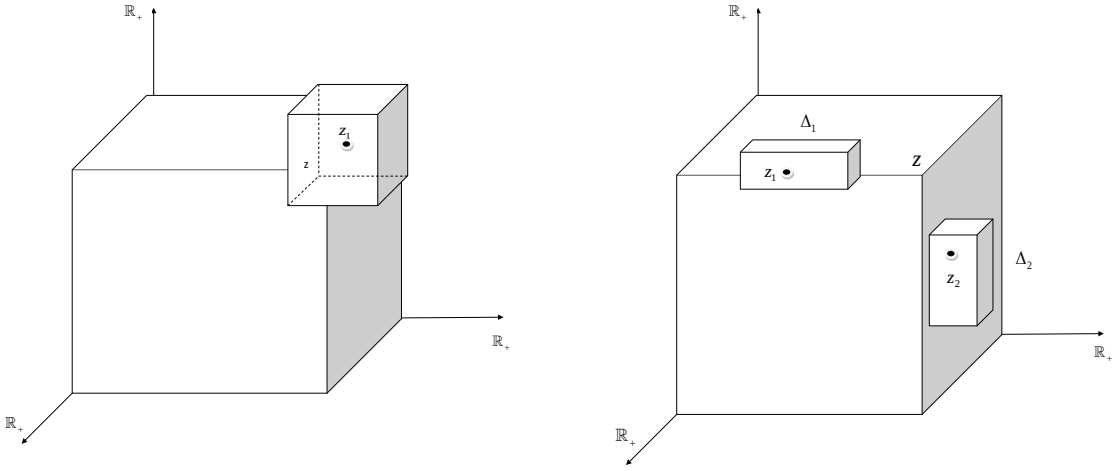

Fig 12. Type 1 and type 2 points in $\mathbb{R}^3_+$, forward of R_z.

4.2.1 Type r Partial Ordering in $\mathbb{R}^{nr}_+$

Having defined the type of increments that we will work with we verify that for any point $z'' \in \mathbb{R}^{nr}_+$ there exist directed sets of type r points in $\mathbb{R}^n_+$, relative to z'' that we can work with. We describe a partial order that can be employed to form type r increments.

Definition 41. (Partial Order) [6] Let X denote a set and let the relation $\sim$ be defined between some elements of the set. X is said to be *partially ordered under* $\sim$ if the following conditions are satisfied among the elements of X that are "comparable" with respect to $\sim$.

1) Let $a \in X$. Then $a \sim a$. (reflexive);

2) For a, $b \in X$, if $a \sim b$ and $b \sim a$ then $a = b$. (antisymmetric);

3) Let a, b, $c \in X$. Then $a \sim b$ and $b \sim c \Longrightarrow a \sim c$ (transitive).

We note that various forms of poset exist. One such example is an irreflexive ($(a \nsim a.)$, asymmetric (if $a \sim b$ then $b \nsim a$) partial order, also described as a strict partial order.

Example 11. In [64] Leslie Lamport develops a model to describe the ordering of events occurring in a distributed system. In the model constructed, Lamport introduces the *happened before relation*, a strict partial order. For the *happened before relation* it is assumed that an event a cannot happen before it happens, for example, in sending or receiving a message, (irreflexive condition). It is also assumed that if an event a happens before an event b (as for example with the transmission and receipt of a message) then event b does not happen before event a, (a message is not received before it is transmitted), (asymmetric condition). The transitive condition is shown to hold.

Lemma 3. Type r points in the r-fold product $\left(\mathbb{R}_+^n\right)^r = \mathbb{R}_+^n \times \ldots \mathbb{R}_+^n$ may be used to form a partial-ordering for $\mathbb{R}_+^n \times \ldots \mathbb{R}_+^n$.

Proof. Let $z = (z_1, \ldots, z_r)$ denote a type r point in $\mathbb{R}_+^n \times \ldots \mathbb{R}_+^n$ relative to a point $z^{''} \in \mathbb{R}_+^n$. Each component z_i of z is a point in $\mathbb{R}_+^n$. We consider the components $z_{ik} \in \mathbb{R}$ of each $z_i \in \mathbb{R}^n$ relative to the components $z_k^{''}$ of $z^{''}$ and define a 'new'point $z^{'} \in \mathbb{R}^n$ as follows: for $z_{ik} < z_k^{''}$ let $z_{ik}^{'}$ denote any point in $\mathbb{R}$ such that $z_{ik} \leq z_{ik}^{'} \leq z_k^{''}$, otherwise let $z_{ik}^{'}$ denote any point in $\mathbb{R}$ such that $z_{ik}^{'} \geq z_k^{''}$.

Define $z^{'} = \left(z_1^{'}, z_2^{'}, \ldots, z_i^{'}, \ldots z_r^{'}\right)$. Then $z^{'}$ is a type r point in $\mathbb{R}_+^n \times \ldots \mathbb{R}_+^n$ relative to the point $z^{''} \in \mathbb{R}_+^n$, and in particular $z^{'}$ is a type r point in $\mathbb{R}_+^n \times \ldots \mathbb{R}_+^n$ relative to the point $z^{''} = \bigvee_{i=1}^{r} \{z_1, \ldots, z_i, \ldots, z_r\}$.

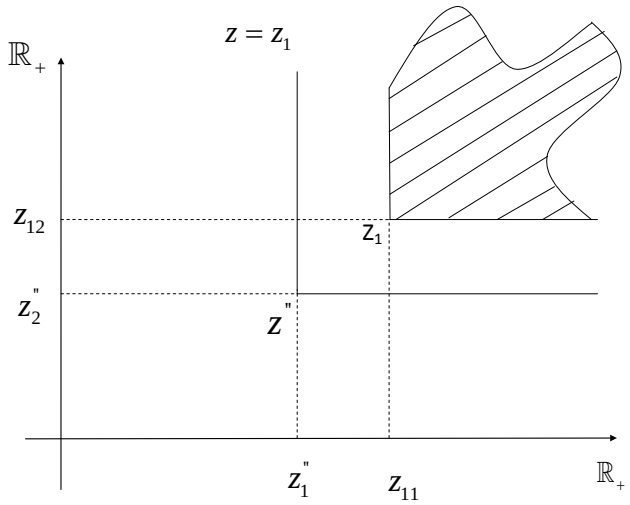

Fig 13. For n = 2: Type 1 point $z' = z_1'$ selected from shaded region.

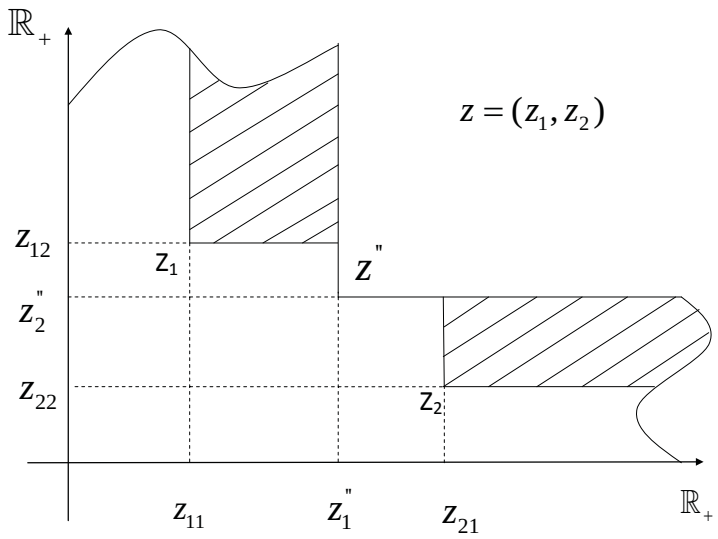

Fig 14. For n = 2: Type 2 point $z' = (z_1', z_2')$ selected from shaded regions.

Since $z^{'}$ denotes any point satisfying the above it follows that all points in a rectangle Δ with $inf\,\Delta = z^{''}$ and $sup\,\Delta = z^{'}$ are type r points.

Using the above algorithm we define a relation $\sim$, for z and $z^{'}$ in $\mathbb{R}^n_+ \times \ldots \mathbb{R}^n_+$ relative to a given point $z^{''} \in \mathbb{R}^n_+$, such that $z \sim z^{'}$. The $\sim$ relation is reflexive, antisymmetric and transitive.

□

Following the above discussion we note that not only is $z^{'}$ a type r point in $\mathbb{R}^n_+ \times \ldots \mathbb{R}^n_+$ relative to the point $z^{''} \in \mathbb{R}^n_+$, but in particular that $z^{'}$ is also a type r point in $\mathbb{R}^n_+ \times \ldots \mathbb{R}^n_+$ relative to the point $z^{''} = \overset{r}{\underset{i=1}{\vee}}\{z_1, \ldots, z_i, \ldots, z_r\}$. Since $z^{'}$ denotes any point satisfying the algorithm given in the above proof it follows that all points in a rectangle Δ with $inf\,\Delta = z^{''}$ and $sup\,\Delta = z^{'}$ are type r points.

Type r increments will be shown to be irreducible forms of increment that may be used to describe, and hence generate other forms of increment that may occur in $\mathbb{R}^n_+$.

4.3 Examples

In this section we are particularly interested in exploring *type 2 increments* found in $\mathbb{R}^3_+$ the 3 dimensional positive parameter base for stochastic integrals motivated initially by Peter Imkeller's work [48] on a stochastic calculus for strong martingales.

4.3.1 The 3-Dimensional Parameter Space

For $\mathbb{R}^3_+$, a type 1 increment is of the form Δ with each point $z' = (z'_1, z'_2, z'_3) \in \Delta$ forward of, or equal to $z = (z_1, z_2, z_3) = inf\,\Delta = sup\,R$. I refer to this as a (3) increment since each of the three variables $z_i{'}$ of z' satisfies the inequality $z_i{'} \geq z_i$. A type 2 increment will involve a pair of Δ's, Δ_1 and Δ_2 with one increment forward of $inf\Delta_1 \vee inf\Delta_2$ in two variables whilst the other increment is forward of $inf\Delta_1 \vee inf\Delta_2$ in the remaining

unused, third variable. So, for example, $z'_1 \geq z_1$, $z'_2 \geq z_2$ and $z'_3 < z_3$ for $z' \in \Delta_1$ and $z'_1 < z$, $z'_2 < z_2$ and $z'_3 \geq z_3$ for $z' \in \Delta_2$. I refer to this as a (2,1) increment. In contrast, a (1,2) increment involves Δ_1 with one variable forward of $inf\Delta_1 \vee inf\Delta_2$ and Δ_2 with the remaining two unused variables forward of $inf\Delta_1 \vee inf\Delta_2$. A type 3 increment involves three such Δ's, each forward of the point $inf\Delta_1 \vee inf\Delta_2 \vee inf\Delta_3$ in one and only one variable at a time. This is also referred to as a (1,1,1) increment in which each variable is forward of $inf\Delta_1 \vee inf\Delta_2 \vee inf\Delta_3$ in one and only one of the Δ_i's.
One may consider here, as in [48], the possibility for a new type of increment, Δ of

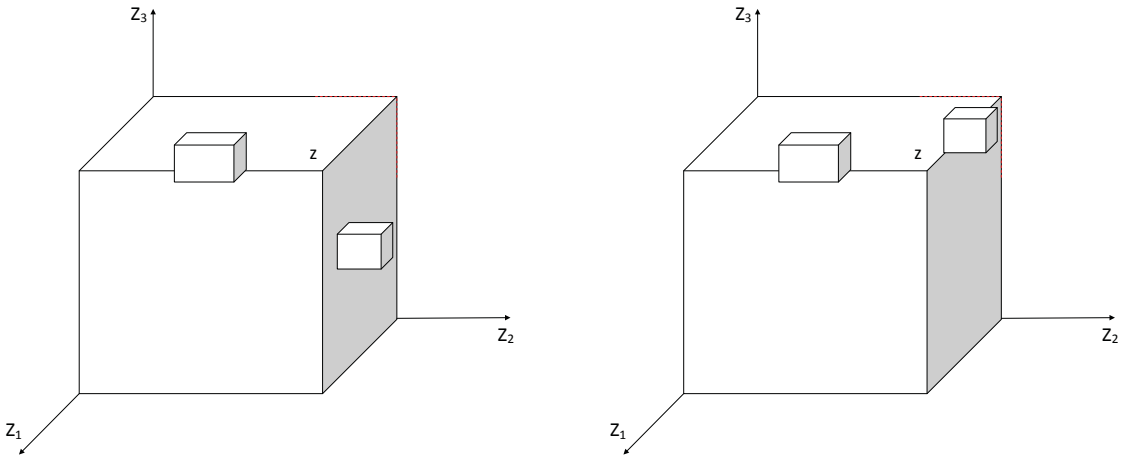

Fig 15. Type 2 Increments and $\mathbb{R}^3_+$, forward of R_z.

the form $\Delta_1\Delta_2$ in which say Δ_1 is forward of $inf\Delta_1 \vee inf\Delta_2$ in the traditional x and y directions whilst Δ_2 is forward of $inf\Delta_1 \vee inf\Delta_2$ in the y and z directions, a (2,2) type of arrangement. Such an increment however, is seen to be a composite form which may be expresed as a limiting case of the type 2 increments introduced above.

Lemma 4. *A (2,2) increment in $\mathbb{R}^3_+$ is a limit of type 2 increments.*

Proof. Let R_z denote the cuboid such that $infR_z = (0, 0, 0)$ and
$z = (z_1, z_2, z_3) = inf\Delta_1 \vee inf\Delta_2$. Without loss of generality we may let the common variable for Δ_1 and Δ_2 be in the third z_3 component, and the 'height' for each Δ_i

(perpendicular to the face of R_z associated with each Δ_i) be the same, say h. This is acceptable since the operators (that we subsequently consider[2] acting on the parameter space will be linear with respect to the Δ_i. We proceed by cutting the two increments in half using a cut parallel to the $z_1 - z_2$ plane, through the z_3 component at $z_3' = z_3 + h/2$. This produces a $(1,2)$ increment, and a $(2,1)$ increment with respect to the cuboid $R_{z'}$ and two $(2,2)$ increments, one with respect to R_z, the other with respect to $R_{z'}$. The volume of each 'new' increment is reduced by one half the volume of the Δ_i that it is a subset of.

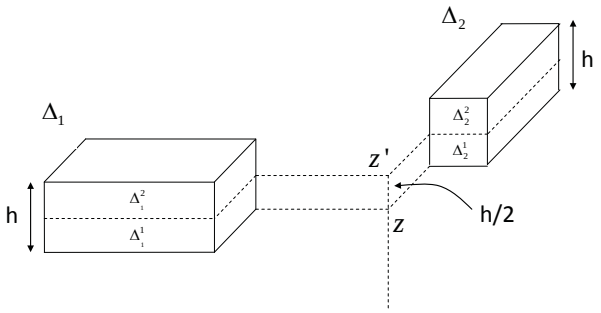

Fig 16. A Limit of Type 2 increments in $\mathbb{R}^3_+$ forward of R_z.

Retaining the $(1,2)$ and $(2,1)$ increments and repeating the process, recursively, with the smaller $(2,2)$ increments, we obtain a sum of type 2 increments whose limit corresponds to the original volume V (the sum produce a GP with first value $V/2$ and common ratio $1/2$). It follows that we may express any linear operator acting on a $(2,2)$ increment as the limit of the sum of the same operator acting on type 2 ($(2,1)$ and $(1,2)$) increments.

□

We shall see in subsequent chapters, that the significance of different irreducible types of increment is that they lead to different types of quantum stochastic integral. We now consider the four dimensional parameter space, since it is here that we do meet a new type of increment.

[2]See for example the type r quantum stochastic integrals

4.3.2 The 4-Dimensional Parameter Space

In $\mathbb{R}^4_+$ we work with type 1, 2, 3 and 4 increments based on the 'four dimensional cuboid' R_z with $z = sup\, R$. For a type 1 increment, (also referred to as a (4) increment, since for points in Δ_1, all four variables are forward of those in R_z), each of the points in Δ_1 is forward of or equal to the point $z = inf\, \Delta_1 = sup\, R_z$. Type 2 increments take the form of a (1,3) increment or a (2,2) increment. A (1,3) increment involves two sets Δ_1 and Δ_2 in which one set, say Δ_1 increases in one component, whilst the other set Δ_2 increases in the remaining three components. It is here, for the first time, that a new type of increment appears, which we refer to as a (2,2) increment. Types (1,3) and (3,1) are by symmetry the same type of increment. A type (2,2) increment however, is new. Types (1,3) and (2,2) are irreducible forms to each other and thus will lead to orthogonal type 2 integrals over the $\mathbb{R}^4_+$ parameter space.

Lemma 5. In $\mathbb{R}^4_+$ type (1,3) and type (2,2) increments are irreducible and hence disjoint in form with respect to R_z.

Proof. Any cuts parallel to the axes for a type (1,3) or (2,2) result in the same type of increments, since they satisfy the same criteria for their type. A (1,3) increment Δ_1 and Δ_2 for $z \in \Delta_1$ has three of its four components within the $R_{z''}$ cuboid whilst $z' \in \Delta_2$ has just one component within $R_{z''}$. For the (2,2) increment two components of $z \in \Delta_1$ are within $R_{z''}$ whilst the 'other ' two components of $z' \in \Delta_2$ are to be found within $R_{z''}$. This condition is unaltered with any cuts parallel to the axes, hence no increments occur that we can use to construct a different type of increment. □

Type 3 increments involve three sets Δ_1, Δ_2, and Δ_3 in which two of the sets have 1 dimensional increments in different directions whilst the remaining set has a 2 dimensional increment. I refer to these as (1,1,2) increments noting its equivalence, by symmetry, in form to the types (1,2,1) and (2,1,1). Finally a type 4 increment consists

of 4 sets Δ_1, Δ_2, Δ_3 and Δ_4, each of which involves an increment in just one dimension (parallel to the axes), type(1,1,1,1), and each increment occurs in just one of the four $\Delta_i's$.

Lemma 6. Each of the increments Type 1, Type 2, Type 3 and Type 4 are irreducible in form and disjoint for increments of the same size.

Proof. Cutting each of the types, parallel to the 'planes 'leads to increments of the same form so from the perspective of form, leads to irreducible forms, unlike, for example, the (2,2) increment in $\mathbb{R}^3_+$.

□

Essentially then, we have five different types of increment occuring in $\mathbb{R}^4_+$, type (4), type (1,3), type (2,2), type (1,1,2) and type (1,1,1,1). One could continue this discussion in $\mathbb{R}^5_+, \mathbb{R}^6_+, \mathbb{R}^7_+, \ldots$ with greater combinations of increment being generated, but at this stage we have covered enough different types of increment to constructively commence a discussion on general increments and from there stochastic integrals, projections and martingales relating to general parameter spaces.

4.3.3 The General Parameter Space

For the general case we work over $\mathbb{R}^n_+$ with type r increments. Clearly there will be one type 1 increment with all components forward of R_z for some $z \in \mathbb{R}^n_+$, a type (n) increment and one type n increment of the form $(1, 1, 1, \ldots, 1, 1, 1)$. Various types of increment may occur in $\mathbb{R}^n_+$ and so we wish to show that these may be expressed in terms of irreducible increments.

Proposition 2. Let $\Delta_i^{'}$ denote an increment in $\mathbb{R}^n_+$. Let $\prod_{i=1}^{r} \Delta_i^{'}$ denote a product of characteristic functions $\chi_{\Delta_i'}$ acting on the $\Delta_i^{'}$ such that each of the n orthogonal

variables in $\mathbb{R}^n_+$ occur in at least one of the $\Delta_i^{'}$. Then $\prod_{i=1}^{r}\Delta_i^{'}$ may be expressed to within ϵ in terms of a sum of type r irreducible increments $\prod_{i=1}^{r}\Delta_i$.

Proof. Each increment may start with the same n dimensional volume by construction. Let X denote a type r characteristic function with increments $\prod_{i=1}^{r}\chi_{\Delta_i^{'}}$ such that just two of the increments, $\Delta_1^{'}$ and $\Delta_2^{'}$ share a common axis. (For example, for $n=3$ and $r=2$ above, the shared axis was z_3). Cut each of the the $\Delta_i^{'}$ in half relative to the common axis, so if the common axis is z_i then $\Delta_i^{'}$ is cut into an 'upper'half $z \in \Delta_i^{'\,\text{upper}} \Longrightarrow \forall j \neq i,\ z_j = z_j^{'}$ and $z_i > z_i^{'}$ and a lower half $\Delta_i^{'\,\text{lower}}$

$$\begin{aligned}
X &= \chi_{\Delta_1^{'}}\chi_{\Delta_2^{'}}\prod_{i=3}^{r}\Delta_i^{'} \\
&= (\chi_{\Delta_1^{'}\,\text{upper}} + \chi_{\Delta_1^{'}\,\text{lower}})(\chi_{\Delta_2^{'}\,\text{upper}} + \chi_{\Delta_2^{'}\,\text{lower}})\prod_{i=3}^{r}\Delta_i^{'} \\
&= \chi_{\Delta_1^{'}\,\text{upper}}\chi_{\Delta_2^{'}\,\text{upper}}\prod_{i=3}^{r}\Delta_i^{'} + \chi_{\Delta_1^{'}\,\text{lower}}\chi_{\Delta_2^{'}\,\text{lower}}\prod_{i=3}^{r}\Delta_i^{'} \\
&\quad + \chi_{\Delta_1^{'}\,\text{upper}}\chi_{\Delta_2^{'}\,\text{lower}}\prod_{i=3}^{r}\Delta_i^{'} + \chi_{\Delta_1^{'}\,\text{lower}}\chi_{\Delta_2^{'}\,\text{upper}}\prod_{i=3}^{r}\Delta_i^{'}
\end{aligned}$$

The first two terms in the last line are the same type of increment as X but with $\frac{1}{4}$ the original n dimensional volume. The last two terms are now irreducible since the inf Δ_i, z_i value for an upper increment is greater than the inf Δ_i, z_i value for a lower increment.

For a type r increment sharing one axis between m of the r increments, $0 < m < r$, apply a proof by induction cutting as indicated in the example above. Repeated applications of the process lead to a sum of irreducible type r increments together with a sum of the same type but of decreasing volume, each cut reducing the overall volume for the same type of increments as X by a factor of one half.

For increments sharing more than one common axis apply the cutting process to those axes and proceed as above.

□

Following the discussion on type r increments above we now construct stochastic integrals over general parameter spaces for the Clifford and Quasi-Free settings.

4.4 The Clifford Representation

We return now to the Clifford Model, first introduced in Section 3.2 in which each of the elements in the quantum stochastic base $(\mathcal{F}(\mathcal{H}), \mathcal{A}, g, (\mathcal{A}_z), \mathbb{R}^n_+)$ were defined.

4.4.1 Simple Adapted Processes

Definition 42. (Elementary Adapted Processes) A map
$h : \mathbb{R}^n_+ \times \cdots \times \mathbb{R}^n_+ \longrightarrow L^2(\mathcal{A})$ is said to be a $\mathcal{A}$ valued elementary r adapted process if there exist $\Delta_1, \ldots \Delta_r$ with $\Delta_1 \overset{\wedge}{\wedge} \ldots \overset{\wedge}{\wedge} \Delta_r$, and h is of the form $h(z_1, \ldots, z_r) = a \overset{r}{\underset{i=1}{\pi}} \chi_{\Delta_i}(z_i)$, with $a \in \mathcal{A}_{inf\Delta_1 \vee \cdots \vee inf\Delta_r}$

Definition 43. (Type r Quantum Stochastic Clifford Integrals)
Let $h(z_1, \ldots, z_r) = a \overset{r}{\underset{i=1}{\pi}} \chi_{\Delta_i}(z_i)$, denote elementary r adapted processes with $a \in \mathcal{A}_{inf\Delta_1 \vee \cdots \vee inf\Delta_r}$ and each $z_i \in \mathbb{R}^n_+$. We define the type r Clifford integral $\mathcal{S}_r$ of h, with respect to Ψ, over R_z to be

$$\begin{aligned} \mathcal{S}_r(h, z, f_1, \ldots, f_r) &= \int_{R_z} \ldots \int_{R_z} h(z_1, \ldots, z_r) d\Psi_{z_1}(f_1) \ldots d\Psi_{z_r}(f_r) \\ &= a \overset{r}{\underset{i=1}{\pi}} \Psi(\chi_{\Delta_i \cap R_z} f_i) \end{aligned}$$

We extend to simple adapted processes on $\mathbb{R}^n_+ \times \cdots \times \mathbb{R}^n_+$ and their respective integrals via linearity.

Example 12. For the case of $\mathbb{R}_+$ the increment Δ_z, forward of $z \in \mathbb{R}_+$ is an interval of the form $[z, z')$ and leads to the Ito - Clifford integral as discussed in [86].

Example 13. For $\mathbb{R}^2_+$ the increment Δ_z takes the form of a square in which all points are forward (in both parameters) of the point $z \in \mathbb{R}^2_+$ and led to the 2- parameter version of the Ito-Cifford integral. In addition to the square forward of z in 2 parameters it is also possible to form a Wong-Zakai Clifford integral, as quantum analogue of the classical Wong-Zakai integral involving two increments in the parameter space each of which contain points that are forward of $sup\, R = z \in \mathbb{R}^2_+$ in just one component, [120, 121].

Example 14. The case of $\mathbb{R}^3_+$ leads one to consider increments forward of a point $z \in \mathbb{R}^3_+$ in three, two and one parameters, leading to further new integrals [48].

Example 15. For the general case of the parameter space $\mathbb{R}^n_+$ we work with increments Δ^r_z, with $1 \leq r \leq n$ containing points forward of $z = sup\, R$ one of each of the available n parameters, occurring in the available Δ_i. For $r = n$ we obtain a quantum analogue of the Ito integral, for $r = n - 1$ we obtain n quantum analogues of the Wong-Zakai integral and for the general case we obtain ${}^nC_r$ quantum integrals involving r increments with points forward of z in p_1 parameters for Δ_1, p_2 parameters for $\Delta_2, \ldots, p_r$ parameters for Δ_r, with $\sum_{i=1}^{r} p_i = n$.

Theorem 9. (Isometry) Each of the integrals given above satisfy isometry properties.

Proof. Let the integral be a type r $1 \leq r \leq n$. The other cases are similar. We extend the approach taken with type I and type II integrals [119] over $L^2(\mathbb{R}^2_+)$ to more general quantum stochastic integrals for the case of $L^2(\mathbb{R}^n_+)$.
Let h denote a simple process with disjoint Δ_{ij}. Then:

$$\| \mathcal{S}_r(h, z, f_1, \ldots, f_r)\|_2^2 = \sum_{i=1}^{m} (\Omega, a_i^* a_i \Omega) \prod_{j=1}^{r} (f_j, f_j)$$

since the off-diagonal elements each cancel out due the gage being both cyclic and independent

$$= \int_{R_z} \dots \int_{R_z} \| h\|_2^2 \prod_{j=1}^{r} |f_j|^2 dz_1 dz_2 \dots dz_r$$

See [111] for further details. □

Theorem 10. (Orthogonality) Let $r_1 \neq r_2 \in \mathbb{N}^+$ with $1 \leq r_1, r_2 \leq n$. Then type r_1 and type r_2 quantum stochastic integrals are orthogonal.

Proof. The integrals generate products of the form $\prod_{i=1}^{r_1} \psi(\chi_{\Delta_i})$ and $\prod_{j=1}^{r_2} \psi(\chi_{\Delta_j})$. Since $r_1 \neq r_2$, $\exists \Delta_i$, and Δ_j that cannot be matched / paired off, or (at worst), $\exists$ at least one Δ_i that is disjoint with all of the other Δ_j's. By independence of the gage, the gage of any such product is zero [39]. For a single ψ the gage is zero, since the (ψ) form centred martingales.

□

The centred martingale property established in [119] for the two parameter case extends to the r-parameter case again by independence of the gage m. As a result general r-parameter quantum stochastic integrals for simple adapted processes each satisfy isometry and orthogonality properties as centred martingales.

Theorem 11. (Martingale) Each of the above integrals form centred martingales

Proof. This again follows by independence of the gage. For further details see [113]. □

4.5 Completion

The integrals described above extend via the representation theorem (discussed in Sections 4.7 and 5.5) which establishes closure, (or alternatively, via the isometry

property, to an appropriate completion of the simple adapted processes) in $L^2(\mathcal{A})$. Such integrals continue to satisfy the isometry and martingale properties. Processes belonging to the respective completions of type r simple processes are themselves found to be orthogonal, isometric centred martingales.

4.5.1 Two Dimensional Parameter Set

An alternative approach to working with the completion of the simple adapted processes is to show that the space is weakly closed. In this subsection we illustrate the case for $\mathbb{R}^2_+$. These are early workings of this material employing approaches taken in [39, 86, 88]. The approach extends naturally to processs over the parameter space $\mathbb{R}^n_+$. We note that the results also follow from the representation theorem discussed at the end of this chapter.

Let T_1 be a compact set in $\mathbb{R}^2_+$ and $T_2 = A \times B$ a compact subset of $\mathbb{R}^2_+ \times \mathbb{R}^2_+$ with $A \wedge\!\!\wedge B$. Let $L^2_\Psi(T_1)$ denote the set of processes in $L^2(T_1, d\mu; L^2(\mathcal{A}))$ and likewise $L^2_{\Psi\Psi}(T_2)$ denote the set of processes in $L^2(T_2, d\mu; L^2(\mathcal{A}))$ where $L^2(T_i, d\mu; L^2(\mathcal{A}))$ denotes complex Hilbert spaces of $L^2(\mathcal{A})$ valued measurable maps on T_i.

Lemma 7. The continuous Type I (resp Type II) L^2 processes may be approximated arbitrarily closely by simple Type I (resp Type II) L^2 processes.

Proof. Let $g \in L^2_{\Psi\Psi}(T_2)$ denote a continuous L^2 processes on T_2. Since $g : T_2 \to L^2(\mathcal{A})$ is continuous and T_2 is compact, it follows that g is uniformly continuous on T_2. Any open cover for T_2 has a finite subcover hence we may generate a subcover for T_2 of discs radius δ. Taking projections of these onto the axes we may form a δ net of squares parallel to the axes. Taking the projection of the midpoints z of each δ square onto the axes we can generate a $\frac{\delta}{2}$ net for T_2. Any points within a $\frac{\delta}{2}$ square will be at most $\frac{\sqrt{2}}{2}\delta$ apart. Let Δ_{z_i} denote the $\frac{\delta}{2}$ square with lower left coordinate $z_i \in A$ likewise $\Delta_{z'_i}$ denote the $\frac{\delta}{2}$ square with lower left coordinate $z'_i \in B$. Given $(z, z') \in T_2 = A \times B$ it follows

$\exists\, \Delta_{z_i}$ and $\Delta_{z'_j}$ s.t. $z \in \Delta_{z_i}, z' \in \Delta_{z'_j}$. Since $A \hat{\wedge} B$ it follows that $\forall\, i, j\ \ \Delta_{z_i} \hat{\wedge} \Delta_{z'_j}$. We take $g(z_i, z'_j)$ as our approximation to $g(z, z')$. By uniform continuity
$\|(z, z') - (z_i, z'_j)\|_2 < \frac{\delta}{2} < \delta \Longrightarrow \|g(z, z') - g(z_i, z'_j)\|_2 < \epsilon$, the δ being dependent upon the choice of ϵ. For our simple processes we take $h = \sum_{i=1}^{m} \sum_{j=1}^{n} g(z_i, z'_j) \chi_{\Delta_{z_i}} \chi_{\Delta_{z_j}}$ for which we note $\|g(z, z') - h(z, z')\|_2 < \epsilon$ with $h \in L^2_{\Psi\Psi}(T_2)$. The same argument with minor modifications (for T_1 instead of T_2) establishes the lemma.

□

Lemma 8. *[39, 86]* Let $X \in L^2(\mathcal{A})$. Then $\mathbb{E}(X|\mathcal{A}_\bullet) : \mathbb{R}^2_+ \to L^2(\mathcal{A})$ by $z \mapsto \mathbb{E}(X|\mathcal{A}_z)$ is continuous.

Proof. $z \mapsto \chi_z$ is strongly continuous on $\mathcal{H} = L^2(\mathbb{R}^2_+, d\mu)$
$\Longrightarrow z \mapsto \Gamma(\chi_z)$ is strongly continuous on $\Lambda(\mathcal{H})$
$\Longrightarrow z \mapsto \mathbb{E}(X|\mathcal{A}_z)$ is strongly continuous on $L^2(\mathcal{A})$
Here $\mathbb{E}(X|\mathcal{A}_z) = D^{-1}\Gamma(\chi_z)DX$, $L^2(\mathcal{A}) = D^{-1}\Lambda(\mathcal{H})$ and D is the duality transform as defined in [96, 97].

□

Lemma 9. The set of processes L^2_Ψ and $L^2_{\Psi\Psi}$ are complex Hilbert Spaces.

Proof. We show that $L^2_\Psi(T_1)$ is a closed subspace of $L^2(T_1, d\mu; L^2(\mathcal{A}))$ and that $L^2_{\Psi\Psi}(T_2)$ is a closed subspace of $L^2(T_2, d\mu; L^2(\mathcal{A}))$.
Let $f_n \longrightarrow f$ in $L^2(T_i, d\mu; L^2(\mathcal{A})), i = 1, 2$; be s.t. (f_n) is a sequence in $L^2_\Psi(T_1)$ (or $L^2_{\Psi\Psi}(T_2)$). Since $f_n \longrightarrow f$ in measure, it follows that $\forall\, \epsilon > 0$, with $\epsilon = 2^{-r}, \exists\, n_r$ s.t.
$\forall\, n \geq n_r \ \ \mu(\{z : \|f_{n_r}(z) - f(z)\|_2 \geq \epsilon = 2^{-r}\}) < \epsilon = 2^{-r}$.
Let $A_r = \{z : \|f_{n_r}(z) - f(z)\|_2 \geq \epsilon = 2^{-r}\}$ and $B_i = \cup_{r=i}^{\infty} A_r$.
Then $\forall r \geq i, \|f_{n_r}(z) - f(z)\|_2 \leq 2^{-r} \Longrightarrow f_{n_r}(z) \to f(z)$
$\Longrightarrow \forall z \notin \cap_{i=1}^{\infty} B_i, f_{n_r}(z) \to f(z)$.

For $z \in \cap_{i=1}^{\infty} B_i$ we have $\mu(\cap_{i=1}^{\infty} B_i) \leq \mu(\cup_{r=i}^{\infty} A_r) \leq \sum_{r=i}^{\infty} \mu A_r \leq \sum_{r=i}^{\infty} 2^{-r} = 2^{1-i}$

Hence $\mu(\cap_{i=1}^{\infty} \cup_{r=i}^{\infty} A_r) = 0 \Longrightarrow f_{n_r}(z) \to f(z)\mu$ a.e. in $L^2(\mathcal{A}) \Longrightarrow \exists$ subsequence (f_{n_r}) s.t. $f_{n_r}(z) \to f(z)$ μ a.e. in $L^2(\mathcal{A})$.

Now $f_{n_r}(z) \in L^2(\mathcal{A}_z)\mu$ a.e. $\Longrightarrow f(z) \in L^2(\mathcal{A}_z)\mu$ a.e. since: (for $i = 1$)) $L^2(\mathcal{A}_z)$ is a closed subspace of $L^2(\mathcal{A})$ and (for $i = 2$)) $z = (z_1, z_2), z_1 \in M_1, z_2 \in M_2, M_1$ and $M_2 \subseteq \mathbb{R}^2_+, z_i$ "cockeyed" $\Longrightarrow f_{n_r}(z) = f_{n_r}(z_1, z_2) \in L^2(\mathcal{A}_{z_1 \wedge z_2}) \Longrightarrow f(z) \in L^2(\mathcal{A}_{z_1 \wedge z_2})$ since $L^2(\mathcal{A}_{z_1 \wedge z_2})$ closed.

□

Theorem 12. *The simple processes are dense in L^2_Ψ and $L^2_{\Psi\Psi}$*

Proof. We show that the simple processes in $L^2_{\Psi\Psi}$ are dense in $L^2_{\Psi\Psi}$. The same argument with appropriate modifications establishes the case for L^2_Ψ.

Let $M_i = [z_i, z_i']$ for $i \in \{1, 2\}$ and $f \in L^2_{\Psi\Psi}(M_1 \times M_2) \subseteq L^2_{\Psi\Psi}(M_1 \times M_2, d\mu, L^2(\mathcal{A})$. Then $\forall \epsilon > 0, \exists\, n \in \mathbb{N}$, $\theta_j \in C(M_1 \times M_2)$ and $X_j \in L^2(\mathcal{A})$ with $1 \leq j \leq n$ s.t.
$\int_{M_1 \times M_2} \|f(z, z') - \sum_{j=1}^n \theta_j(z, z') X_j\|_2^2 d\mu < \epsilon$, since
$L^2(M_1 \times M_2, d\mu, L^2(\mathcal{A})) \simeq L^2(M_1 \times M_2) \otimes L^2(\mathcal{A}) \simeq \overline{C(M_1 \times M_2)}^{\|\cdot\|_2} \otimes L^2(\mathcal{A})$, (see [88] for example). $f \in L^2_{\Psi\Psi}(M_1 \times M_2) \Longrightarrow f(z, z') \in L^2(\mathcal{A}_{z \wedge z'}), \theta_j \in \mathbb{R}$ or $\mathbb{A}$ and since $\mathbb{E}(.|\mathcal{A}_{z \wedge z'}) : L^2(\mathcal{A}_{z \wedge z'}) \to L^2(\mathcal{A}_{z \wedge z'})$ is a contraction,
$\int_{M_1 \times M_2} \|f(z, z') - \sum_{j=1}^n \theta_j(z, z') \mathbb{E}(X_j|\mathcal{A}_{z \wedge z'})\|_2^2 d\mu$
$= \int_{M_1 \times M_2} \|\mathbb{E}(f(z, z') - \sum_{j=1}^n \theta_j(z, z') X_j|\mathcal{A}_{z \wedge z'})\|_2^2 d\mu < \epsilon$.

Now $\theta_j(\cdot, \cdot)\mathbb{E}(X_j|\mathcal{A}_{\cdot \wedge \cdot})$ is by Lemma 8 a continuous L^2 process and hence is in $L^2_{\Psi\Psi}(M_1 \times M_2)$. It follows by Lemma 7 that there exists a simple process in $L^2_{\Psi\Psi}$ s.t. we can approximate $\theta_j(\cdot, \cdot)\mathbb{E}(X_j|\mathcal{A}_{\cdot \wedge \cdot})$ in $L^2_{\Psi\Psi}$. It follows that $f(\cdot, \cdot)$ can also be approximated by simple processes in $L^2_{\Psi\Psi}(M_1 \times M_2)$. □

4.6 Quasi-Free Quantum Stochastic Integrals

In this section we describe Quasi-free stochastic integrals for $\mathcal{H}$. Such integrals may also be realised for C^* algebras, $\mathcal{U}$ and von Neumann Algebras, $\mathcal{A}$. We first define the integral for elementary adapted processes and then extend by linearity to simple adapted processes.

Definition 44. Let $h(z_1, \ldots, z_r) = a \overset{r}{\underset{i=1}{\pi}} \chi_{\Delta_i}(z_i)$, denote elementary r adapted processes with $a \in \mathcal{H}_{inf\Delta_1 \wedge \cdots \wedge inf\Delta_r}$ and each $z_i \in \mathbb{R}^n_+$. We define the type r quasi-free integral $\mathcal{S}_r$ of h over R_z to be

$$\begin{aligned}\mathcal{S}_r(h, z, f_1, \ldots, f_r) &= \int_{R_z} \ldots \int_{R_z} h(z_1, \ldots, z_r) db^{\#}_{z_1}(f_1) \ldots db^{\#}_{z_r}(f_r) \\ &= a \overset{r}{\underset{i=1}{\pi}} b^{\#}(\chi_{\Delta_i \cap R_z} f_i)\end{aligned}$$

where $b^{\#}$ may denote either b or b^*. We extend by linearity to $\mathcal{H}$-valued simple adapted processes.

The quasi-free CCR stochastic integrals are similarly defined in terms of $c^{\#}$.

Type r integrals for both the CAR and CCR cases each result in 2^r different possible stochastic integrals, two type I and four type two integrals, and so forth. Each of the integrals satisfies isometry conditions and extends via isometry to a completion of the $\mathcal{H}$-valued simple adapted processes. As with Clifford Stochastic integrals, it may be shown that theses integrals are orthogonal to each other, orthogonal to Ω and generate families of martingales.

Theorem 13. The type r quasi-free CAR quantum stochastic integral satisfies the isometry property.

Proof. We consider the isometry condition for the Quasi free CAR case. Let h denote a

simple r - adapted process over $\mathbb{R}^n_+$. Then

$$\begin{aligned}
\| \mathcal{S}_r(h,z,f_1,\ldots,f_r)\|_2^2 =& \| \int_{R_z}\ldots\int_{R_z} h(z_1,\ldots,z_r)db^{\#}_{z_1}(f_1)\ldots db^{\#}_{z_r}(f_r)\|_2^2 \\
&= \|\sum_i a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\|_2^2 \\
&= (\sum_i a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\Omega, \sum_k a_k \overset{r}{\underset{l=1}{\pi}} b^{\#}(\chi_{\Delta_l\cap R_z}f_l)\Omega) \\
&= \sum_{i,k}(a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\Omega,\ a_k \overset{r}{\underset{l=1}{\pi}} b^{\#}(\chi_{\Delta_l\cap R_z}f_l)\Omega) \\
&= \sum_i \|(a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\|_2^2
\end{aligned}$$

The off-diagonal elements all disappear to give the last line. This follows by noting that a_i, a_k and $\overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j) \in \overset{r}{\underset{\substack{p=1\\p\neq q}}{\vee}} \mathcal{U}^p_{z_k}$, a_i, a_k and $\overset{r}{\underset{l=1}{\pi}} b^{\#}(\chi_{\Delta_l\cap R_z}f_l) \in \overset{r}{\underset{\substack{q=1\\q\neq p}}{\vee}} \mathcal{U}^q_{z_l}$ and $b^{\#}$ is both a $\overset{r}{\underset{\substack{p=1\\p\neq q}}{\vee}} \mathcal{U}^p_{z_k}$ and a $\overset{r}{\underset{\substack{q=1\\q\neq p}}{\vee}} \mathcal{U}^q_{z_l}$ martingale.

The point here is that if the off diagonals are different then there is always one increment in $\mathbb{R}^n_+$ that can be isolated from the others. Taking conditional expectations with respect to the filtrations provides the result. Alternatively [85], we can use the property that $\omega(\overset{r}{\underset{i=1}{\Pi}} b^*(f_i)\overset{r}{\underset{j=1}{\Pi}} b(g_{r-j})$ may be expressed in terms of the $\omega(b^*(f_i)b(g_{r-i}))$ which for disjoint sets is zero. To continue with the diagonal elements, we obtain the following:

$$\begin{aligned}
\sum_i \|(a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\|_2^2 &= \sum_i(\overset{r}{\underset{j=1}{\pi}}\Omega,\ b^{\#^*}(\chi_{\Delta_j\cap R_z}f_j)a_i^*a_i \overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\Omega) \\
&= \sum_i(\Omega,\ a_i^*a_i \overset{r}{\underset{j=1}{\pi}} b^{\#^*}(\chi_{\Delta_j\cap R_z}f_j)\overset{r}{\underset{j=1}{\pi}} b^{\#}(\chi_{\Delta_j\cap R_z}f_j)\Omega)
\end{aligned}$$

using the ω product [33] we obtain

$$= \begin{cases} \sum\limits_i \prod\limits_{j=1}^{r} \omega(b^*(\chi_{\Delta_j \cap R_z} f_j) b(\chi_{\Delta_j \cap R_z} f_j))(\Omega,\, a_i^* a_i \Omega) & \text{for } b^{\#} = b \\ \sum\limits_i \prod\limits_{j=1}^{r} (\Delta_j \cap R_z f_j,\, \Delta_j \cap R_z f_j) - \omega(b^*(\chi_{\Delta_j \cap R_z} f_j) b(\chi_{\Delta_j \cap R_z} f_j)(\Omega,\, a_i^* a_i \Omega) & \text{for } b^{\#} = b^* \end{cases}$$

with appropriate modifications for a mixture of integrators b^* and b

$$= \begin{cases} \sum\limits_i \int_{\Delta_1} \dots \int_{\Delta_r} \rho^r(z) |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz & \text{for } b^{\#} = b \\ \sum\limits_i \int_{\Delta_1} \dots \int_{\Delta_r} (1 - \rho(z))^r |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz & \text{for } b^{\#} = b^* \end{cases}$$

with appropriate modifications for a mixture of integrators b^* and b

$$= \begin{cases} \int_{R_z} \dots \int_{R_z} \sum\limits_i \prod\limits_{j=1}^{r} \chi_{\Delta_i j} \rho^r(z) |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz & \text{for } b^{\#} = b \\ \int_{R_z} \dots \int_{R_z} \sum\limits_i \prod\limits_{j=1}^{r} \chi_{\Delta_i j} (1 - \rho(z))^r |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz & \text{for } b^{\#} = b^* \end{cases}$$

$$= \int_{R_z} \dots \int_{R_z} (\sum_i a_i \prod_{j=1}^{r} \chi_{\Delta_i j} \Omega,\, \sum_j a_k \prod_{k=1}^{r} \chi_{\Delta_k l} \Omega)\, d\mu(z)$$

$$= \int_{R_z} \dots \int_{R_z} \parallel h(z) \Omega \parallel_2^2 d\mu(z)$$

where $d\mu(z) = \rho^r(z) |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz$ for $b^{\#} = b$
and $(1 - \rho(z))^r |f_1(z)|^2 \dots |f_r(z)|^2 \parallel a_i \Omega \parallel_2^2 dz \dots dz$ for $b^{\#} = b^*$.

□

The orthogonality and centred martingale properties follow similarly for the general quasi-free CAR case with similar developments for the quasi-free CCR model generating the following results.

Theorem 14. A given instance of a type r quasi-free (QF) CAR QSI is orthogonal to different instances of type r QF CAR QSI's and type s QF CAR QSI's.

Theorem 15. Type r QF CAR QSI's form centred martingales.

For the quasi-free CCR quantum stochastic integrals we do not have the Pauli Principle, hence the creation and annihilation operators form unbounded operators [11]. We work in this case with the $*$ - algebra of operators formed from sums and products of $c^{\#}$ operators and obtain the following result.

Theorem 16. Type r QF CCR QSI's form orthogonal, isometric, centred martingales.

4.7 Representation Theorems

The general Representation Theorem for the Clifford case over the parameter space $\mathbb{R}^n_+$ has been published in [110]. The quasi-free CAR and CCR case for $n = 3$ has also been published in [115]. These two refereed papers are included in the appendices. The general theorem for the Clifford model is:

Theorem 17. (The Clifford Representation Theorem) Let $(X_z)_{z\in\mathbb{R}^n_+}$ denote an $L^2(\mathcal{A})$ valued martingale adapted to the family $(\mathcal{A}_z)_{z\in\mathbb{R}^n_+}$ of von Neumann subalgebras of $\mathcal{A}$. Then $\exists$ unique $f_i \in L^2_{\psi^n}$ s.t.

$$X_z = X_0 + \sum_{i=1}^{n} \mathcal{S}_i(f_i, z)$$

The uniqueness of f, g, and h for the case $n = 3$ and the f_i in the general case follows by application of the conditional expectation operator and isometry.[119]

Proof. See [110] (Appendix C), for details. □

For the quasi-free CAR and CCR case over $\mathbb{R}^3_+$, the theorem takes the following form.

Theorem 18. (Quasi-Free CAR and CCR Representations) Let $\{X_z|z \in R\}$ denote a $\mathcal{H}$-valued martingale. Then there exist unique α, $f_1, \ldots f_6$ such that

$$X = \alpha\Omega + \sum_{i=1}^{2} \iint_{R_z} db^{\#}_{z'} f_i(z') + \sum_{j=3}^{6} \iint_{R_z} \iint_{R_z} db^{\#}_{z'} db^{\#}_{z''} f_j(z', z'')$$

Proof. See [115] (Appendix C), for details.

□

Over $\mathbb{R}^n_+$ each type r integral may generate 2^r different quantum stochastic integrals. These are determined by the r martingale integrators $b^{\#}$ according to whether it represents b or b^*. The theorems take the following form:

Theorem 19. (The General Quasi-Free CAR and CCR Representations) Let $\{X_z|z \in R\}$ denote a $\mathcal{H}$-valued martingale. Then there exist unique α, and f_i such that

$$X = \alpha\Omega + \sum_{r=1}^{n} \sum_{i=1}^{2^r} \iint_{R_z} \prod_{j=1}^{r} db^{\#}_{j_{z'}} f_i(z'_1, \ldots z'_j)$$

Proof. Having established that we may represent any increment in $\mathbb{R}^n_+$ to within ϵ of a sum of type r increments, a combination of the approaches taken with the above papers yields the result.

□

4.8 Summary

In this chapter we have discussed type r increments, general parameter spaces, developed new type r quantum stochastic integrals and established that isometry, orthogonality and martingale properties extend to these new integrals. We have developed Representation theorems and have found that the growing complexity involved in using

the geometric approach so far employed is no longer, the simpler intuitive approach that was first conjectured with integrals over general parameter spaces. With this in mind we look to develop an alternative approach in order to maintain the simpler intuitive approach to this work. This is our focus for the next chapter.

Chapter 5

Fubini's Theorem

5.1 Introduction

In this chapter we explore the possibility for extending Fubini's theorem from the classical to the quantum setting for operators adapted to the filtration $(\mathcal{A}_z)^i_{z\in\mathbb{R}^n_+}$. Our initial motivation for the development of this material is to simplify the proof for the multiparameter quantum stochastic representation theorem, and is, we believe, a new quantum development of the theorem.

5.2 i - Processes

Following the discussion given in chapter two on classical i-martingales we now develop quantum i-filtrations, conditional expectations and martingales for stochastic processes over $\mathbb{R}^n_+$. The stochastic base that we will work with is the 6-tuple

$$(\mathcal{F}(\mathcal{H}),\, \mathcal{A},\, (\mathcal{A}_z)_{z\in\mathbb{R}^n_+},\, (\mathcal{A}^i_z)_{\substack{z\in\mathbb{R}^n_+\\ 1\le i\le n}},\, g,\, \mathbb{R}^n_+)$$

with $\mathcal{F}(\mathcal{H})$, $\mathcal{A}$, $(\mathcal{A}_z)_{z\in\mathbb{R}^n_+}$, g, $\mathbb{R}^n_+$ defined earlier.

Definition 45. We define

$$\mathcal{A}^i_z = \mathcal{A}^i_{(z_1, z_2, ..., z_n)} = \mathcal{A}_{(\infty, \infty, ..., \infty, z_i, \infty, ..., \infty)} = \bigvee_{\substack{z_j \\ j \neq i}} \mathcal{A}_{(z_1, z_2, ..., z_{j-1}, z_j, z_{j+1}, ... z_n)}$$

to be the von Neumann algebra generated by polynomials in $\psi(z)$ such that the i-th component of $z \in \mathbb{R}^n_+$ is a fixed constant.

For this discussion we include the axes in our description $\mathbb{R}^n_+$ and observe that $\mathcal{A}_z = \bigcap_i \mathcal{A}^i_z = \bigcup_{z' \prec z} \mathcal{A}_{z'} = \bigcap_{z \prec z''} \mathcal{A}_{z'}$ (ultraweak closure), $\mathcal{A} = \bigcup_z \mathcal{A}_z$ (ultraweak closure), and $\mathcal{A}_z \cap \mathcal{A}_{z'} = \mathcal{A}_{z \wedge z'}$ (ultraweak closure). We say that $(\mathcal{A}^i_z)$ is an i-filtration if $\forall z_1 \prec z_2,\ \mathcal{A}^i_{z_1} \subseteq \mathcal{A}^i_{z_2}$ is an increasing family of sub von Neumann algebras of $\mathcal{A}$.

Definition 46. A process X is said to be an i-adapted (weakly adapted) process if

$$\forall\, z \in \mathbb{R}^n_+ \quad X_z \in \mathcal{A}^i_z$$

and an i-martingale if

$$m(X_{z'} \,|\, \mathcal{A}^i_z) = X_{(z'_1, z'_2, ..., z_{i-1}, z_i, z_{i+1}, ..., z'_n)}.$$

So an i-martingale is a martingale with respect to its ith coordinate. If X is weakly adapted for all $1 \leq i \leq n$ then X is said to be an adapted process.

It follows that $m(X_{z'} \,|\, \mathcal{A}_z) = m\left(m\left(\ldots\, m\left(m\left(X_{z'} | \mathcal{A}^1_z\right) | \mathcal{A}^2_z\right) \ldots | \mathcal{A}^{n-1}_z\right) | \mathcal{A}^n_z\right)$ and that the [15, 139] conditional commutativity (conditional independence) property (F4),

$$m\left(m\left(X_{z'} | \mathcal{A}^i_z\right) | \mathcal{A}^j_z\right) = m\left(m\left(X_{z'} | \mathcal{A}^j_z\right) | \mathcal{A}^i_z\right)$$

holds for $1 \leq i,\, j \leq n$. The following result therefore holds.

Theorem 20. Let $X = (X_n)$ denote a quantum stochastic process over $\mathbb{R}^n_+$. Then X is a martingale $\iff$ X is an i-martingale $\forall\, i \in \{1, 2, \ldots, n\}$.

Example 16. For the case $n = 2$ with $z = (z_1, z_2) \in \mathbb{R}^2_+$ the 1-filtration $\mathcal{A}^1_z$ denotes the von Neumann algebra generated by operators defined over the parameter space $[0, z_1) \times [0, \infty)$ whilst the 2-filtration $\mathcal{A}^2_z$ denotes the von Neumann algebra generated by operators defined over the parameter space $[0, \infty) \times [0, z_2)$.

i-filtrations are analogues of classical i-filtrations described in [139] by John Walsh when considering the possibility for 2-parameter stochastic processes being realised classically as martingales with respect to one (or more) of the available parameters.

5.3 Fubini

The classical Fubini theorem for integrals may take the following form:

Theorem 21. *[140] Let $x \in I_1 \subset \mathbb{R}^m$, and $y \in I_2 \subset \mathbb{R}^n$ with I_1, I_2 compact closed intervals. Let $f(x, y) \in L(I), I = I_1 \times I_2$. Then*
i) for almost every $x \in I_1, f(x, y)$ is measurable and integrable on I_2 as a function of y;
ii) as a function of x, $\int_{I_2} f(x, y)dy$ is measurable and integrable on I_1 and
iii) $\int\int_I f(x, y)dx\, dy = \int_{I_1}[\int_{I_2} f(x, y)dy]dx$

For $I \subset \mathbb{R}^2_+$, $m = n = 1$ with both I_1 and I_2 compact closed intervals in $\mathbb{R}$, with

$$\int\int_I f(x, y)dx\, dy = \int_{I_1}[\int_{I_2} f(x, y)dy]dx = \int_{I_2}[\int_{I_1} f(x, y)dx]dy$$

For the quantum setting we consider three forms that can be interpreted as quantum analogues of Fubini's theorem.

5.4 First Form

Let $h(z_1, z_2) = a\chi_{\Delta_1}\chi_{\Delta_2}$ with $\Delta_1 \overset{\wedge}{\wedge} \Delta_2$ and $a \in \mathcal{A}_{inf\Delta_1 \vee inf\Delta_2}$ denote a type 2 elementary adapted process with $\Delta_i \subset \mathbb{R}^2_+$. The type 2 quantum stochastic integral for h with respect to Ψ is of the form

$$\mathcal{S}_r(h, z, f_1, f_2) = \int_{R_z}\int_{R_z} h(z_1, z_2) d\psi_{z_1}(f_1) d\psi_{z_2}(f_2) = a \overset{2}{\underset{i=1}{\pi}} \psi(\chi_{\Delta_i \cap R_z} f_i)$$

in which R_z denotes the region of integration in $\mathbb{R}^2_+$, R_z a closed rectangle with $inf\, R_z = (0, 0)$, the origin.

We note that if $a \in \mathcal{A}_{inf\Delta_1 \vee inf\Delta_2}$ then $a \in \mathcal{A}^1_{inf\Delta_1 \vee inf\Delta_2}$ and $a \in \mathcal{A}^2_{inf\Delta_1 \vee inf\Delta_2}$. Following the presentation given by John Walsh [139], for the classical setting we develop analogues of type i-stochastic integrals for the quantum setting.

Definition 47 (Type i-Quantum Stochastic Integrals)**.** Let h_i denote an elementary i-adapted process over $\mathbb{R}^2_+$ of the form $h_i(z) = a\chi_\Delta(z)$ with $a \in \mathcal{A}^i_{inf\,\Delta}$, $i \in \{1, 2\}$.
A type i - quantum stochastic integral for an elementary i - adapted process h with respect to Ψ is of the form

$$\mathcal{S}(h, z, f) = \int_{R_z} h_i(z') d\Psi(f) = \int_{R_z} a\chi_\Delta(z') d\Psi(f) = a\Psi(\chi_{\Delta \cap R_z}(z') f)$$

As with previous definitions for quantum stochastic integrals, the above integrals extend by linearity to simple processes.

Over $\mathbb{R}^2_+$, a type 2 integral $\mathcal{S}_2$ with $\Delta_1 \overset{\wedge}{\wedge} \Delta_2$ we note that $a \in \mathcal{A}^1_{inf\,\Delta_2}, a \in \mathcal{A}^2_{inf\,\Delta_1}$,

$a\Psi(\chi_{\Delta_1\cap R_z}f_1)\in\mathcal{A}^1_{inf\,\Delta_2}$, and $a\Psi(\chi_{\Delta_2\cap R_z}f_1)\in\mathcal{A}^2_{inf\,\Delta_1}$ from which it follows that

$$\begin{aligned}\mathcal{S}(h,z,f_1,f_2)&=\int_{R_z}\int_{R_z}h(z_1,z_2)d\Psi(f_1)d\Psi(f_2)=\int_{R_z}(\int_{R_z}a\chi_{\Delta_1}d\Psi(f_1))\chi_{\Delta_2}d\Psi(f_2)\\&=\int_{R_z}a\Psi(\chi_{\Delta_1\cap R_z}f_1)\chi_{\Delta_2}d\Psi(f_2)\\&=a\Psi(\chi_{\Delta_1\cap R_z}f_1)\Psi(\chi_{\Delta_2\cap R_z}f_2)\\&=a\prod_{i=1}^{2}\Psi(\chi_{\Delta_i\cap R_z}f_i)\end{aligned}$$

If we denote the integral $\int_{R_z}\int_{R_z}h(z_1,z_2)d\Psi(f_1)d\Psi(f_2)$ by $\mathcal{S}_{\Delta_1\Delta_2}$ then it follows from the CAR's that $\mathcal{S}_{\Delta_1\Delta_2}=-\mathcal{S}_{\Delta_2\Delta_1}$. So a change in the order of integration changes the sign of the integral. For a general type r integral on an elementary adapted process we obtain, as an application of the CAR relationship, the following proposition.

Proposition 3. Let $\prod_{i=1}^{r}\Delta_i=\Delta_1\Delta_2\ldots\Delta_r$ denote $\chi_{\Delta_1}\chi_{\Delta_2}\ldots\chi_{\Delta_r}$ with $\Delta_i\overset{\wedge}{\wedge}\Delta_j\quad\forall i.\,j\in\{1,2,\ldots,r\}$. Let P denote a permutation of the integers $1,2,\ldots,r$, and

$$\epsilon(P)=\begin{cases}1 & \text{if } P \text{ is an even permutation,}\\ -1 & \text{if } P \text{ is an odd permutation.}\end{cases}.$$

Let a be a product of Ψ's with $\Psi\in\mathcal{A}_z$ with $z=sup\bigvee_{i=1}^{r}\{inf\,\Delta_1,\ldots inf\,\Delta_i,\ldots inf\,\Delta_r\}$.

Then $\mathcal{S}_{\prod_{i=1}^{r}\Delta_i}=(-1)^t\epsilon(P)\,\mathcal{S}_{\prod_{i=1}^{m}\Delta_{P(i)}\prod_{j=m+1}^{r}\Delta_{P(j)}}$ with $t=\begin{cases}0 & \text{for } a \text{ even,}\\ m & \text{for } a \text{ odd.}\end{cases}$.

Here $m\in\mathbb{N}^+$, $1\le m\le r$ and $a\in\mathcal{A}_z$ is generated by products of the Ψ's. In general $a\in\mathcal{A}_z$ is the limit of sums and products of the Ψ's. The above result extends by linearity to simple sums and products. For the general case $a\in\mathcal{A}_z$, a is either even, or odd or a sum of even and odd $a_i\in\mathcal{A}_z$. It follows that the next theorem holds.

Theorem 22. Let $h \in L^2(\mathcal{A})$. $t = \begin{cases} 0 & \text{for } h \text{ even,} \\ m & \text{for } h \text{ odd} \end{cases}$.

Then $\mathcal{S}(h)_{\prod_{i=1}^{r}\Delta_i} = (-1)^t\epsilon(P)_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}$

Proof. Let $h_j \in L^\infty(\mathcal{A}) \xrightarrow{L^2} h \in L^2(\mathcal{A})$. Then $\forall j$, h_j is a sum of even and odd products. Let h_j^+ denote the sum of even products and h_j^- denote the sum of odd products. Let $h^+ = L^2 - \lim_{j\to\infty} h_j^+$, $h^- = L^2 - \lim_{j\to\infty} h_j^-$ and $h = h^+ + h^-$ in $L^2(\mathcal{A})$. So for each j we group the sum of even and odd parts with L^2 limits h^+ and h^- respectively, with $h = h^+ + h^-$. We note that

$$\begin{aligned}
\mathcal{S}(h_j)_{\prod_{i=1}^{r}\Delta_i} &= \mathcal{S}(h_j^+)_{\prod_{i=1}^{r}\Delta_i} + \mathcal{S}(h_j^-)_{\prod_{i=1}^{r}\Delta_i} \\
&= \epsilon(P)\{{}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j^+)_{\prod_{j=m+1}^{r}\Delta_{P(j)}} + (-1)^m \quad {}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j^-)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}\} \\
&= (-1)^t\epsilon(P)\{{}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j^+)_{\prod_{j=m+1}^{r}\Delta_{P(j)}} + \quad {}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j^-)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}\} \\
&= (-1)^t\epsilon(P)_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j^+ + h_j^-)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}
\end{aligned}$$

Hence for $h \in L^2(\mathcal{A})$,

$$\begin{aligned}
&\|\mathcal{S}(h)_{\prod_{i=1}^{r}\Delta_i} - \quad (-1)^t\epsilon(P)_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}\|_2^2 \\
= \;& \|\mathcal{S}(h)_{\prod_{i=1}^{r}\Delta_i} - \mathcal{S}(h_j)_{\prod_{i=1}^{r}\Delta_i} + (-1)^t\epsilon(P)\{{}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j)_{\prod_{j=m+1}^{r}\Delta_{P(j)}} - {}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}\}\|_2^2 \\
\leq \;& \|\mathcal{S}(h-h_j)_{\prod_{i=1}^{r}\Delta_i}\|_2^2 + \|{}_{\prod_{i=1}^{m}\Delta_{P(i)}}\mathcal{S}(h_j-h)_{\prod_{j=m+1}^{r}\Delta_{P(j)}}\|_2^2 \longrightarrow 0 \text{ as } j\to\infty \text{ by isometry}
\end{aligned}$$

□

The first form demonstrates that a type r quantum stochastic integral can be viewed as a multiple integral in which the order of integration is (up to sign difference),

commutative. Comparing the first form for $r = 2$ (for example), with the 'classical' Fubini, we note that first form multiple integration is still performed over '$\mathbb{R}^2_+$' rather than '$\mathbb{R}_+$' (or '$\mathbb{R}$') and that this extends to the general case.

We now therefore seek an alternative form of Fubini Theorem such that each of the integrators in our multiple integral, live in dimensions lower than those initially given, consistent with the classical case, whereby a type r integral may be seen as a combination of type m and type n integrals with $m + n = r$. We will fix $a \in \mathcal{A}_z$ for the following discussion, focusing primarily upon the parameter space $\mathbb{R}^n_+$.

5.5 Second Form

In this section we propose an alternative form of Fubini theorem for type r quantum stochastic integrals over $\mathbb{R}^n_+$, that focuses on varying underlying parameter spaces $\mathbb{R}^m_+$ and $\mathbb{R}^{m'}_+$ (with $m + m' = n$), upon which the martingale integrators (Ψ_z) depend rather than the integrators themselves. This involves a change of focus and interpretation from the first form of Fubini theorem.

For elementary adapted processes over the parameter space $\mathbb{R}^2_+$, integrals over R_z generate operators that are a combination of type 1 and type 2 operators $a\Psi(\chi_{\Delta\cap R_z} f)$, and $a\Psi(\chi_{\Delta_1\cap R_z} f_1)\Psi(\chi_{\Delta_2\cap R_z} f_2)$. For the general parameter space $\mathbb{R}^n_+$ we obtain Integrals (operators) that are a combination of products of the form $a\prod_{i=1}^{r}\Psi(\chi_{\Delta_i\cap R_z} f_i)$ with $1 \leq r \leq n$.

Let $n = 2$. For type 1 and 2 QSI's (quantum stochastic integrals) Δ is a rectangle in $\mathbb{R}^2_+$ which may be partitioned in various ways. Let Δ be partitioned along the 'horizontal'axis generating p regions Δ_i of equal area. It follows that a type 1 QSI may

be expressed in terms of vertical and horizontal 'increments.'

$$\begin{aligned}\int_{R_z} a\chi_\Delta d\Psi(f) &= a\Psi(\chi_{\Delta\cap R_z} f) = \sum_{i=1}^{p} a\Psi(\chi_{\Delta_i\cap R_z} f) = \sum_{i=1}^{p}\int_{R_z} a\chi_{\Delta_i} d\Psi(f) \\ &= \lim_{p\longrightarrow\infty}\sum_{i=1}^{p} a\Psi(\chi_{\Delta\cap L_i\cap R_z} f) \text{ as the rectangles } \Delta_i \rightarrow \text{ vertical lines } L_i \text{ in } \Delta \\ &= \int_{R_z\cap\Delta}\int_{R_z\cap L_i} a\chi_\Delta d\Psi(f) dz_1 \quad \text{where } z_1 \text{ denotes the horizontal variable.}\end{aligned}$$

The first part of the stochastic integral is similar to classical line integrals over $\mathbb{R}^2_+$ [138] whilst the double integral is similar to a stochastic Fubini integral [58], (see also chapter 2) a combination of Lesbegue and stochastic integrals.

For the type 2 QSI we consider Ψ as an $\mathcal{A}^1_z$ martingale process (which we will denote by Ψ^1) for Δ_1, and as an $\mathcal{A}^2_z$ martingale process Ψ^2 for Δ_2. A type 2 QSI may be expressed as

$$\begin{aligned}&\int_{R_z}\int_{R_z} a\chi_{\Delta_1\cap R_z} d\Psi(f_1)\chi_{\Delta_2\cap R_z} d\Psi(f_2) \\ &\qquad = a\Psi(\chi_{\Delta_1\cap R_z} f_1)\Psi(\chi_{\Delta_2\cap R_z} f_2) \\ &\qquad = a\Psi^1(\chi_{\Delta_1\cap R_z} f_1)\Psi^2(\chi_{\Delta_2\cap R_z} f_2) \\ &\qquad = \int_{R_z\cap\Delta_2}\int_{R_z\cap L_j}\left(\int_{R_z\cap\Delta_1}\int_{R_z\cap L_i} a\chi_{\Delta_1} d\Psi^1(f_1)dz_1\right)\chi_{\Delta_2} d\Psi^2(f_2)dz_2 \\ &\qquad = \int_{R_z\cap\Delta_2}\int_{R_z\cap\Delta_1}\left(\int_{R_z\cap L_j}\int_{R_z\cap L_i} a\chi_{\Delta_1} d\Psi^1(f_1)\chi_{\Delta_2} d\Psi^2(f_2)\right)dz_1dz_2 \\ &\qquad = \int_{R_z\cap\Delta_1}\int_{R_z\cap\Delta_2}\left(\int_{R_z\cap L_j}\int_{R_z\cap L_i} a\chi_{\Delta_1} d\Psi^1(f_1)\chi_{\Delta_2} d\Psi^2(f_2)\right)dz_2dz_1\end{aligned}$$

The last line follows since the sums for the approximations relating to the outer

integrals can be summed in any order.

We therefore have a relationship between the first and second form of Fubini Theorem for the case $n = 2$. What then of the general case?

For the general parameter space $\mathbb{R}^n_+$, type r QSI's involve working with integrators Ψ that are martingales with respect to filtrations of the form $\underset{i}{\vee}\mathcal{A}^i$ and may be expressed in the form

$$\begin{aligned} a\prod_{i=1}^{r}\Psi(\chi_i f_i) &= \int\limits_{R_z\cap\Delta_1}\cdots\int\limits_{R_z\cap\Delta_r}\left(\int\limits_{R_z\cap L_{i_r}}\cdots\int\limits_{R_z\cap L_{i_1}} a\chi_{\Delta_1}d\Psi^1(f_1)\ldots\chi_{\Delta_r}d\Psi^r(f_r)\right)dz_r\ldots dz_1 \\ &= \int\limits_{R_z\cap\left(\bigcup\limits_{i=1}^{r}\Delta_i\right)}\left(\int\limits_{R_z\cap L_{i_r}}\cdots\int\limits_{R_z\cap L_{i_1}} a\chi_{\Delta_1}d\Psi^1(f_1)\ldots\chi_{\Delta_r}d\Psi^r(f_r)\right)dz_1 \end{aligned}$$

Proposition 4. *Let $\{\Psi\}$ denote a stochastic process defined over $\mathbb{R}^n_+$.*

Then:

$$\begin{aligned} \{\Psi\} \text{ is a martingale over } \mathbb{R}^n_+ &\iff \{\Psi\} \text{ is an } i- \text{ martingale for } 1\le i\le n \\ &\iff \{\Psi\} \text{ is a martingale over } \mathbb{R}^{n-1}_+ \text{ for } 1\le i\le n. \end{aligned}$$

Proof. ($\Longrightarrow$) This follows from the definition of martingale applied to $(\Psi(\chi_\Delta))$, a linear stochastic process with $\Delta\subseteq\mathbb{R}^n_+$ expressed in terms of the regions R_z.

($\Longleftarrow$) $\mathcal{A}_z = \underset{i=1}{\overset{r}{\wedge}}\mathcal{A}^i_z \subset \mathcal{A}^i_z$ for $1\le i\le r$. Repeated application of the conditional expectation with respect to $\mathcal{A}^i_z$ establishes the martingale property, both for $\mathbb{R}^n_+$ and $\mathbb{R}^{n-1}_+$

□

Remark 1. Given a stochastic process $\{X_z\}_{z\in I}$ with $\Delta_i\subseteq\mathbb{R}^n_+$ and $X_z\in\mathcal{A}=L^\infty(\mathcal{A})\subseteq L^2(\mathcal{A})$ we note that $\mathcal{A}$ is generated by sums and products of the form $\sum\limits_{j=1}^{m}\prod\limits_{i=1}^{r}\psi_{ij}$ with $\psi_{ij}=\psi_j(\chi_{\Delta_i}f_i)$. We would like to consider X_z in terms of a slightly

different form $\prod_{i=1}^{r} \psi_i$, an extended, more general stochastic processes, still related to X_z via linearity and isometry, as required. The QSLI's developed in the second form, have given us a significant move in this direction. If the f_i can be associated with projections over $\mathbb{R}_+^{n-1}$ then X_z will have 'images' over $\mathbb{R}_+^{n-1}$ of the form $X_z' = \prod_{i=1}^{r} \psi_i'$ with $\psi_i' = \psi'(\chi_{\Delta_i} f_i)$ and $f_i \in L^\infty(\mathbb{R}_+^{n-1})$. These will be QSI's over $\mathbb{R}_+^{n-1}$ with martingale integrators associated with those used over $\mathbb{R}_+^n$.

5.6 Third Form

We now consider $\mathcal{A}_z$, with a view to expressing these in terms of QSLI's. Each $a \in \mathcal{A}_z$ is, by construction, formed from sums and products of the $\psi(\Delta_i)s$ with $\Delta_i \subseteq \mathbb{R}_+^n$ or, the weak / strong limit of such sums and products. Each of the $\psi(\Delta_i)$ is a QSI's, (or a limit of such sums) and hence may be expressed in terms of QSLI's. The integrals may be a variety of integral types, from type r integrals to type i integrals, each may be interpreted as a QSLI and any product $\prod_{i=1}^{p} \psi(\Delta_i)$ may be viewed as nested QSLI's. Extending the approach taken in the second form to include operators in $\mathcal{A}_z$ as nested QSLI's allows us to view our type r QSI's as a sum of slices from corresponding algebras defined over $\mathbb{R}_+^{n-1}$. Although the f_i issue is still not resolved, we have moved far enough to achieve one of our goals which is to simplify the proof for the Representation theorem further, since convergence obtained for type r QSI over $\mathbb{R}_+^n$ to products of the Ψ's via the cutting process can now be applied at much lower dimensions and followed by inductive arguments for products over $\mathbb{R}_+^n$.

5.7 Representation Theorem

Following our discussion at the end of the last chapter and the discussion here on QSLI's we note that QSLI's may be employed in the proof to the representation theorem. For

(ψ) a $\mathbb{R}_+^n$ martingale it follows that (ψ) is an $\mathbb{R}_+^{n-1}$ martingale. Proceeding as in previous examples with the cutting process [110] we may show that for $n = 2$ sums and products of ψ's in $L^2(\mathcal{A})$ may be expressed as a sum of type r QSI's or at worst the limit of a sum of type r QSI's. Assuming that the result holds for products of ψ's over $\mathbb{R}_+^{n-1}$ we can use an induction argument via the QSLI 'sheets'which may be viewed as martingale processes over $\mathbb{R}_+^{n-1}$. Applying the cutting process to increments in $\mathbb{R}_+^n$ cuts increments associated with the QSLI 'sheets'over $\mathbb{R}_+^{n-1}$. Since this holds for each of the n $\mathbb{R}_+^{n-1}$ 'planes' the result follows over $\mathbb{R}_+^n$. The same argument holds for the quasi-free cases over $\mathbb{R}_+^n$.

In particular, we note:

1) for any product X, in the Clifford or quasi-free models we may apply the quantum stochastic Fubini Theorem and focus on the 'slices'through the difference between X and the type r approximations to X;

2) for $f_i \in L^2(\mathbb{R}_+^n)$ we note that f_i is a an equivalence class, which we may represent as $[f_i]$ and from which we may choose any representative f_i. Each f_i can be sliced parallel to the plane $\mathbb{R}_+^m$ with $1 \leq m \leq n$ and for each slice we may associate the $f_i \in L^2(\mathbb{R}_+^n)$ with the family of slices parallel to the plane $\mathbb{R}_+^m$.

3) for each slice $\tilde{f}_i$, the difference truly lies in the algebra generated by the elements $\psi(\Delta_i \tilde{f}_i)$ with $\Delta_i \subseteq \mathbb{R}_+^m$ and $\tilde{f}_i \in L^2\mathbb{R}_+^m)$.

4) with each slice defined over $\mathbb{R}_+^m$ we may employ an inductive argument, commencing with $n = 2$, where such slices, each tend to zero as the number of cuts tends to infinity and hence that the original difference over $\mathbb{R}_+^n$ also tends to zero.

Remark 2. The slicing approach discussed above creates a link between martingales over $\mathbb{R}_+^m$ and i-martingales over $\mathbb{R}_+^n$ which can be employed also, for example, in the proof that quantum stochastic integrals are martingales.

5.8 Summary

In this chapter we have worked with i-processes, to develop different forms of Fubini theorem which we have applied to the Representation theorem in order to simplify the proof given. In the next chapter we begin the development of two new applications of quantum stochastic integrals to tools employed in cryptographic and voting protocols.

Chapter 6

Applications

6.1 Introduction

In this chapter we look at some applications to which we may apply our quantum stochastic integrals. The applications considered relate to some of the tools employed in a security setting, where we find a range of algorithms and protocols relating to authentication, anonymity, confidentiality, integrity, and non-repudiation. Many of these tools rely on finite field theory and in particular properties of cyclic groups, to achieve their aims. With the appearance of Shor's algorithm [100, 101], concerns regarding many of these algorithms emerged, particularly for government and commercial ventures, in which the perception held was that they would affect the long term viability of such classically based schemes. The quantum setting, however may offer possibilities for the future, and investment in quantum research relating to computing, communication and security has been forthcoming. In the next two sections, we meet background material set in qubit based multipartite systems. The purpose of this is to set in context the influences and motivation for the remaining sections in which cyclic groups are constructed using quantum stochastic integrals and quantum implementations are described, with a view to future development.

6.2 Quantum Cryptography

Classical cryptography protocols based on cyclic groups are generally based upon the perceived difficulty in solving either the Integer Factorisation Problem (IFP), or the Discrete Logarithm Problem (DLP). Both of these problems are believed to belong to the NP complexity space, however no known proof to support this belief exists.

Central to many of the constructions employed in the classical setting and also found in the quantum setting is the concept of generator, or primitive, an element that can be used to generate a cyclic group under the repeated application of a binary operation such as addition or multiplication relative to an irreducible divisor. Examples from classical cryptography [122, 124], include both symmetric and asymmetric key systems. A symmetric key system involves the use of one key, shared between a sender and receiver to encrypt and decrypt data in a communication. The Advanced Encryption Standard [22], and the Data Encryption Standard are two such examples. For asymmetric key systems [25] we meet algorithms based on the [1], integer factorisation problem (IFP), such as RSA, the Rivest, Shamir, Adleman algorithm, the discrete logarithm problem (DLP) with the El Gamal algorithm [37], the elliptic curve discrete logarithm problem (ECDLP) with again the El Gamal algorithm, Menezes, Vanstone, Okamoto algorithm, the hyperelliptic curve discrete logarithm problem (HCDLP) [19], and pairing based schemes, with the Tate Pairing and Weyl Pairing. In contrast to algorithms used for confidentiality purposes, finite fields may also be employed to help maintain integrity and develop authentication tools. Examples of these are to be found in, for example, network analysis, [83]. for the successful delivery of network traffic. Various anonymity protocols make use of finite field theory, [17] with applications based on the application of generated fields from algebraic number theory and algebraic geometry. These lead to the employment of finite fields, [59, 74] elliptic curves, [60] hyperelliptic curves and pairings, for the development of secure algorithms. Secure that

is, unless Shor's algorithm [100, 101], can be efficiently implemented in a quantum computer. If or when this happens, asymmetric key schemes based on either the IFP, DLP, ECDLP, or HCDLP will, be rendered obsolete.

In the quantum setting finite fields have appeared concerning the complexity of performing Galois field arithmetic [123], in Shor's algorithm for the IFP and DLP, with phase space [56] defined over finite fields and with maximally unbiased bases [42, 73, 84, 43] together with Galois rings and operators [106, 107].

6.3 Observations on Irreducibility, Operators and Algebras

In this section concepts of entanglement, irreducibility and prime are introduced with the discussion centering on similarities and differences that exist between constructions involving entanglement and their classical counterparts as found in, for example, algebraic number theory. We observe throughout this discussion that being prime, irreducible or entangled is not, in general, a permanent state, but one very much dependent upon the set in which the object resides. The definition for a prime may be presented in various ways[1], for example in terms of D an integral domain, or in terms of algebraic numbers.

Definition 48. (Prime) Let $p \in D$ with D an integral domain, s.t. $p \neq 0, 1$. Then p is said to be prime if $p = ab$ with $a, b \in D \Longrightarrow p|a$ or $p|b$ but not both.

Definition 49. (Algebraic Integers) [76] Let $\alpha \in \mathbb{C}$ be a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree d, with d the minimum degree such that α is a root of such polynomial. Then α is said to be an *algebraic integer* of degree d.

In terms of algebraic numbers $p \in R$ (a commutative ring with identity) is said to be prime if it is not a unit and $p|mn \Longrightarrow p|m$ or $p|n$

[1] A number divisible by itself and 1 only, but not 1.

Definition 50. (Irreducible) An object a in a ring R with identity 1_R is said to be irreducible if $a = bc \neq 0$, with $b, c \in R \Longrightarrow b$ or c is a unit. A unit in a commutative ring R is an element $\alpha \in R$ s.t. $\exists \beta \in R$ with $\alpha\beta = 1_R$.

It is well known that in a unique factorisation domain [UFD] an irreducible is prime but that otherwise irreducibles are not always prime. In general we have $\{primes\} \subseteq \{irreducibles\}$ with equality guaranteed only within a UFD.

Theorem 23. (The failure of Unique Factorisation is the failure of Irreducibles to be Prime) [76]. Let F be a number field and α an element in the ring $\mathcal{O}_F$ of algebraic integers lying in F. Then α can be factored into a product of irreducible elements. Moreover, every non-zero $\alpha \in \mathcal{O}_F$ has such a unique factorisation into a product of irreducibles, up to order and associates if and only if every irreducible element of $\mathcal{O}_F$ is prime.

Example 17. *In* $\mathbb{Z}(\sqrt{2}, \sqrt{5})$ $3 = 1 \times 3 = (\sqrt{5} - \sqrt{2})(\sqrt{5} + \sqrt{2})$. It follows that 3 is not prime in $\mathbb{Z}(\sqrt{2}, \sqrt{5})$.

In the case of mixed states the situation is not quite so straightforward. A separable mixed state may be expressed as a linear combinations of tensor products in which the components of each tensor product contains a linear factor, a superposition of fundamental qubit states. Otherwise it is an entangled state. Recognising that a mixed state is separable [30] is not always straightforward.

6.3.1 Entanglement - spatial separation with local unitaries

For the case of $\mathcal{H}^n$, $n \in \mathbb{R}$ it is well known [32, 79] that local unitary operations preserve entanglement. Of particular interest to the discussion in hand is the following definition regarding equivalent states.

Definition 51. *Equivalent States under LOCC* [77, 75, 136] Two states $|\psi\rangle$ and $|\phi\rangle$ are said to be equivalent under LOCC (Local Operations with Classical Communication) if $\exists$ local unitaries $M_1, \dots M_n \, s.t. |\psi\rangle = M_1 \otimes \cdots \otimes M_n |\phi\rangle$.

In 1742 Goldbach conjectured that $\forall n \in \mathbb{N}$, n even, could be expressed as a sum of two primes or ones. It followed, given the truth of the conjecture that $\forall m = 2n + 1$, with $m \geq 7$, m could be expressed as the sum of three odd prime numbers. Euler responded with the conjecture that $\forall m = 4n + 2$, $m \geq 6$, m could be expressed as the sum of two primes, each of the form $4n + 1$ or one. In considering a corresponding case for entangled states it is clear that all states may be expressed in terms of entangled states since, for example the Bell states form a basis for any Hilbert space $\mathcal{H}$ under consideration.

Theorem 24. Let the volume of a separable state be bounded. Then every separable state may be expressed as sum of two entangled states

Proof. Given a separable state $|\psi\rangle$ $\exists$ (since the state is bounded [53] say by ϵ) an entangled state outside of the epsilon ball. Let $|\phi\rangle$ denote the entangled state found and $|\xi\rangle$ the difference between them. Then $|\psi\rangle = \frac{1}{2}((|\psi\rangle + |\xi\rangle) + (|\psi\rangle - |\xi\rangle))$ with $(|\psi\rangle \pm |\xi\rangle)$ both entangled.

□

The fundamental theorem of arithmetic states that any integer may be uniquely expressed (up to order of factors) as a product of primes. This begs the question as to whether such a result exists for the states of an arbitrary Hilbert Space.

Theorem 25. Every pure state may be uniquely expressed as a product of separable and/or entangled states.

Proof. A state $|\psi\rangle \in \mathcal{H}^n$ is either entangled or decomposable [44]. If it is entangled then we are done. If it is decomposable then $|\psi\rangle = |\phi\rangle_r \otimes |\xi\rangle_s \in \mathcal{H}^r \otimes \mathcal{H}^s = \mathcal{H}^n$ with $0 < r, \, s < n$.

Consider $|\phi\rangle_r \in \mathcal{H}^r$ (the same argument will hold for $|\xi\rangle_s \in \mathcal{H}^s$). If $|\phi\rangle_r$ is entangled then $|\psi\rangle$ is a product of an entangled state and $|\xi\rangle_s$. If $|\phi\rangle_r$ is decomposable then we may express $|\phi\rangle_r$ as a product of states each belonging to Hilbert spaces with smaller dimension than $\mathcal{H}^r$. Continuing with this process we obtain products involving either entangled states or states in $\mathcal{H}$ - a superposition of say $|0\rangle$ and $|1\rangle$. $|\phi\rangle_r$ is therefore a product of entangled and/or 'separable' sub states formed from $\mathcal{H}$. Applying the same argument to $|\xi\rangle_s$ gives the result. For uniqueness consider the inner product applied to two possibly different representations of $|\psi\rangle$.

□

Entanglement, irreducibility and being prime are each dependent upon the space against which they are referenced, so it is natural to seek a condition that is not dependent upon the space under discussion. One such condition is the greatest common divisor and we use this to motivate the following definition.

Definition 52. Let $\{|\phi_i\rangle\}_{i=1}^n$ denote elements in a Hilbert space $\mathcal{H}$. Then the elements $\{|\phi_i\rangle\}_{i=1}^n$ are said to be relatively entangled if there are no common factors throughout.

One can think of relative entanglement as the analogue of coprime for irreducible or prime numbers and one could equally well refer to relative entanglement as coentanglement.

Theorem 26. The relatively entangled pure states are invariant under a change of ambient space as are relatively entangled classes

Proof. In losing entanglement via global unitaries being realised as local ones, and unitary equivalence being achieved between the once entangled state and separable states, the once entangled representation still retains its non factorisable property. Thus relative entanglement is maintained.

□

This section opens up discussion on the comparison between entanglement, irreducibility and primes leading to the possibility for further research in a number of related directions. In particular, the density of entangled states (and separable states) in a fixed n-dimensional Hilbert space, congruency, analogues for finite fields and applications. On the one hand it is a cautionary note, being irreducible is a relative statement that can quickly change. It is also a motivating note as we explore an alternative approach to realising cyclic groups via quantum stochastic integrals.

6.4 Generators in a von Neumann Algebra - Fubini

Each stage of integration with a Fubini quantum integral generates an operator $\psi(\chi_{\Delta_i}) \in \mathcal{A}$ leading to a sequence $(\psi(\chi_{\Delta_i}))_i$ with $1 \leq i \leq r$. Each of the $\psi(\chi_{\Delta_i})$ satisfy the CAR properties and hence are of period 2 satisfying $\psi(\chi_{\Delta_i})\psi(\chi_{\Delta_i}) = \mathbb{I}$ for $|\Delta_i|^2 = \frac{1}{2}$.

The order in which we apply the Fubini sub-integrals leads, up to sign difference, to the same result. However the application of each sub-integral generates ${}^rC_s = \frac{r!}{s!(r-s)!}$ possible ways of realising a product of s $\psi(\chi_{\Delta_i})'s$ from the r available. So it is possible to generate a final stochastic integral in a variety of different ways. It follows that we may associate a variety of different sequences with any given quantum stochastic Fubini integral. Not only can we generate a particular sequence, but for applications of the sub-integrals beyond r we can generate alternative sequences back to a constant multiple of the identity operator in $\mathcal{A}$. So, i- filtrations may be employed to generate any product (and hence sequence) of $\psi(\chi_{\Delta_i})'s$. For notational simplicity we will refer to each $\psi(\chi_{\Delta_i})$ as ψ_i.

Example 18. (Sequence) Let $1 \leq n, i \leq 3$. For any of the $\Delta_i \subseteq \mathbb{R}^3_+$ we can generate each of the ψ_i in any order, (and separately). So we can generate a sequence of elements

as shown below. Note, we ignore sign differences as at ψ_3:

$$\mathbb{I} \xrightarrow{\psi_1} \psi_1 \xrightarrow{\psi_2} \psi_1\psi_2 \xrightarrow{\psi_3} \psi_1\psi_2\psi_3 \xrightarrow{\psi_1} \psi_2\psi_3 \xrightarrow{\psi_2} \psi_3 \xrightarrow{\psi_3} \mathbb{I}$$

Here we apply the QSI process to the sequence $\chi_{\Delta_1}\chi_{\Delta_2}\chi_{\Delta_3}\chi_{\Delta_1}\chi_{\Delta_2}\chi_{\Delta_3}$ in turn. The QSI process applied to χ_{Δ_i} with respect to i filtrations we identify as a cyclic process with outcome determined by the original sequence $\chi_{\Delta_1}\chi_{\Delta_2}\chi_{\Delta_3}\chi_{\Delta_1}\chi_{\Delta_2}\chi_{\Delta_3}$.

We therefore have a method for generating a collection of elements which are cyclic in nature via the QSI acting as primitive. The outcome is not dependent upon the binary operation, irreducibility and starting element but on n, r, the increments Δ_i, and the order in which the i-integrals are applied.

Example 19. Group Properties Closure, associativity, identity, and inverse properties follow from the algebraic properties of the von Neumann algebra $\mathcal{A}$. Commutativity is anticommutative for CAR algebras and commutative for CCR algebras. For ψ_i we have anticommutativity. To obtain commutativity we either need to ignore signs (CAR Fermion case) or use CCR Boson algebra.

Standard classical examples for cyclic groups include $\mathbb{Z}_p$, $\mathbb{Z}[x]/f(x)$ in which $f(x)$ denotes an irreducible function and $E_p(a, b)$ elliptic curves defined over finite fields. Such groups have been used with success in error detection [65, 83], correction [65, 68, 2] and cryptology [19, 22, 25, 28, 37, 31, 36, 59, 60, 61, 74, 3, 102, 105]. For the quantum setting we consider the following examples.

Example 20. Discrete Logarithm Problem Given a cyclic group as described above with orbit 2r the Diffie Hellman Problem is to establish the value x such that the xth application of the quantum stochastic i integral process generates the given product $\prod_{i=1}^{s} \psi_i$ The hidden element here is the order of integration.

Example 21. Diffie-Hellman Key Agreement Protocol We use an example to illustrate the protocol.

Let Alice and Bob agree a type 2 (2,1) product of $\psi\chi_\Delta$'s over $\mathbb{R}^2_+$. For our example let Alice use a pair of Δ's, Δ_1 and Δ_2 such that the z_2 coordinates for inf Δ_1 and inf Δ_2 are the same. Let Bob use one Δ_3 cockeyed to the pair of Δ_i chosen by Alice. So for $i \in \{1,2\}$, $\Delta_i \wedge \Delta_3$.

Alice sends to Bob $\psi(\chi_{\Delta_1})\psi(\chi_{\Delta_2})$ to which Bob applies $\psi(\chi_{\Delta_3})$ and Bob reciprocates sending $\psi(\chi_{\Delta_3})$ to Alice who applies $\psi(\chi_{\Delta_1})\psi(\chi_{\Delta_2})$. Both Alice and Bob have now agreed the same quantum 'key'.

This is susceptible to a 'man in the middle attack' as is the classical Diffie Hellman key agreement protocol, but the example illustrates as proof of concept.

The Diffie Hellman protocol can be used with $n \in \mathbb{N}^+$ and for r participants a type r quantum stochastic i-integral can be employed.

Example 22. (El-Gamal)

We work with a particular value of n, throughout, for the parameter space.

Bob publishes his public key which involves a primitive $\alpha = \Psi(\Delta_i)$, a starting operator for the sequence, its i - integral $\beta = \prod_{j=1}^{s} \Psi(\Delta_j)$, n the dimension for the parameter space and r the type of integrals being used. Bob's private key will consist of two elements, s and the type r sequence of length $2r$, in particular, the Δ's used to generate the i-integrals sent.

Alice selects, a type r sequence K of Δ's

$$\left(\chi_{\Delta_{\pi(1)}}, \chi_{\Delta_{\pi(2)}}, \ldots, \chi_{\Delta_{\pi(r)}}, \chi_{\Delta_{\pi'(1)}}, \ldots, \chi_{\Delta_{\pi'(r)}}\right)$$

in which π and π' are two randomly selected permutations of $k \in \mathbb{Z}^*_{r+1}$.

Let m denote the operator to be encrypted. Define encryption $e(m,K) = \left(\alpha^k, m\beta^k\right)$

where k denotes the point to which integration takes place with respect to each of the domains in Alice's sequence - from position 1 to position k in Alice's sequence. For decryption we have $d(e(m,K)) = m\beta^k\alpha^{kr} = m\alpha^{rk}\alpha^{kr} = \pm m$ subject to parity, by which we mean the number of commutes required in order to obtain each of the ψ's adjacent to the same operator, thus generating m times a product of $\mathbb{I}$'s. (As before we select the Δ's so that $|\Delta|^2 = \frac{1}{2}$.

A major problem for security protocols built on the Integer Factorisation Problem or the Discrete Logarithm Problem is that they can be broken through repeated application of Shor's algorithm. The algorithm takes an element from the cyclic group and derives the order of the element which is then used to break the original security protocol. Here we have more information required to establish the cyclic group. In particular we need to know the order for the application of the i-integrals and possibly information regarding the starting $\psi(\Delta_i)$.

Conjecture 2. *The above cyclic group is not susceptible to an attack using Shor's algorithm.*

6.5 Quantum Voting

The first paper to be published on quantum voting was by Vaccaro, Spring and Chefles [51] in 2005 closely followed by Buzek, Bielikova, Hillery, and Ziman [71] just two weeks later. Both of these were preceded by a paper by Christandl and Wehner [18] on quantum anonymity during 2004. There are various types of voting protocol available to users [103] and for an introduction to the area we defer to [4, 12, 21, 34, 52, 81].

6.5.1 The Ballot

We employ the use of a finite Fock space $\mathcal{F}_{2n}(\mathcal{H}) = \overset{2n}{\underset{i=0}{\oplus}}\mathcal{H}^i$ in which n denotes the maximum number of voters in the ballot. The system (Fock space) is initialised with a starting vector in $\mathcal{H}^n$. The ballot will be in response to a question or statement requiring a yes or no response. A yes / no response will reflect agreement / disagreement with the question or statement posed. For a yes vote the creation operator will be applied whilst for a no vote the annihilation operator will be applied. To obtain a result we will apply the number operator, aa^* to the result.

6.5.2 Voting Scheme for s candidates

One such voting scenario involves n voters casting votes, at a local tally centre where authentication and anonymity protocols are employed. Once collected these are then collected and securely sent to a central (global) tally centre for processing. We consider one approach to recording each vote cast via creation operators on finite dimensional Fock space.

We assume that once a vote is cast it will not be changed. This isn't essential, but simplifies the model. We use the creation operator $a^*(f_i)$ on a 'finite' Fock space

$$\mathcal{F}_j(\mathcal{H}) = \bigoplus_{i=1}^{n}\mathcal{H}_i = \mathbb{C} \oplus \mathcal{H} \cdots \oplus \mathcal{H}_n \qquad 1 \leq j \leq n$$

to record a vote for each candidate. For $f_i \in L^2(\mathbb{R}^n_+)$, we use a different $f_1, f_2, \ldots, f_s$ to represent each of the s candidates that a voter may access in the quantum voting scheme under discussion. The Pauli exclusion principle for fermions states that no two fermions can exist in the same state. Hence Fermi Fock space is inappropriate for this model and we work with the Bose-Fock space $\mathcal{F}_+(\mathcal{H})$, with $\mathcal{H} = L^2(\mathbb{R}^n_+)$. Given the existence of s registered candidates for our voting scheme we take the s-tuple $(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_i, \ldots, \mathcal{F}_s)$

with each $\mathcal{F}_i \subseteq \mathcal{F}_+(\mathcal{H})$, to represent the occupancy space for candidate i.
Hence we have s possible finite dimensional Fock spaces that we use to record the voting tally for each of the candidates. Each subspace of the sequence represents a tally space for candidate i, recording the number of votes cast for the candidate through repeated applications of the creation operator to the space $\mathcal{F}_i$. The action of the creation operator $a(f_i)$ on $\mathcal{F}_i$ to denote the casting of a vote for candidate i. So the idea here is to use different Fock Spaces to represent each candidate. The application of a creation operator each time a vote is made moves a state from $\mathcal{H}_r \mapsto \mathcal{H}_{r+1}$. Note that we could add a further space upon which each vote is recorded to give a total tally for the votes cast. The precise operator used to record a vote for candidate i being
$\mathbb{I} \oplus \mathbb{I} \oplus \cdots \oplus a^*(f_i) \oplus \cdots \oplus \mathbb{I}$.
An algorithm such as El Gamal could be employed to obscure the number of votes cast for each candidate as the votes would be moved to different occupancy spaces until decrypted at the central tally centre. Measurement, once again could be achieved via the number operator.
To accommodate a change in vote one could employ the annihilation operator to move the total number of votes cast for a candidate from one space to a lower occupancy space.

6.6 Summary

In this chapter we have looked at a selection of concepts and influences found in the qubit based multipartite setting related to cryptography and voting protocols. We have described applications of quantum stochastic integrals to the development of quantum based cryptography in terms of cyclic groups generated by quantum stochastic integrals, Diffie - Hellman and El-Gamal algorithms and have further described applications to quantum voting.

Chapter 7

Contributions to Knowledge and Conclusions

7.1 Introduction

This chapter reviews the contribution to knowledge that this thesis makes and outlines a range of research areas that could be developed as a result of this work.

7.2 Contribution to Knowledge

The original goals for this thesis were to develop general quantum stochastic integrals focusing on the underlying parameter space as a means of simplifying concepts previously worked with at an operator or vector based level but over $\mathbb{R}_+^n$ rather than $\mathbb{R}$ or $\mathbb{R}_+^2$. To explore relationships between stochastic integrals over $\mathbb{R}_+^m$ and $\mathbb{R}_+^n$ and to develop applications for quantum stochastic integrals based on the Fock space models presented here.

Our primary motivation, has been achieved.

• We have derived isometry, centred martingale and orthogonality properties for the

general case with the Clifford and quasi-free setting. The Clifford results have been presented at the Fifth International Conference on Applied Mathematics and Computing. The paper was refereed and published in the International Journal of Pure and Applied Mathematics.

• Representation Theorems have been developed over $\mathbb{R}_+^n$ for the Clifford and quasi-free CAR and CCR setting. The Clifford results have been presented at the 23rd Quantum and White Noise Conference held at CIMAT, Guanajuato, Mexico and published as a refereed paper[1].

• The Quasi-free CAR and CCR Representation Theorems over $\mathbb{R}_+^2$ were presented at the 28th Quantum and White Noise Conference held at Santiago, Chile. This research was also refereed and published. The general case over $\mathbb{R}_+^n$ is contained here.

• We have also identified irreducible parameter types for the general parameter spaces $\mathbb{R}_+^n$, established equivalence between different parameter types and used these to generate simple proofs for, for example the Representation Theorems.

Relationships between different quantum stochastic integrals have been achieved.

• To this end we have developed Fubini like quantum stochastic forms. The first of these involved general type r quantum stochastic integrals and relational properties were explored.

• The first form was extended to a second quantum stochastic form involving quantum stochastic line integrals. These were related to the commutative stochastic Fubini Theorem and a relationship between the first and second form established.

• The second form has been extended to a third form. These have been applied to the proof of the Representation Theorem, simplifying the proof over $\mathbb{R}_+^n$.

Applications have been explored within a quantum cryptography setting. These we see as work in progress providing proof of concept status. They constitute areas of interest

[1]This was significant for me in that not only did I have the opportunity to present my work to major researchers in this area, and meet researchers whose work I had read but I also got to present at the same venue that John Walsh had presented at some years earlier.

for future research in an applied setting.

• As part of a team of three we have published the first research paper on quantum voting and surveying. This paper was initially posted on xxx.lanl.gov and subsequently published as a refereed paper in the Journal Physical Review A.

• We have identified a 'cyclic'group structure generated by quantum stochastic integrals with creation operators as integrator.

• We have used these to construct Diffie Hellman quantum key agreement protocols and El Gamal encryption/decryption protocols. We have also applied the quantum stochastic structure to develop a quantum voting model.

7.3 Future Research

Future work resulting from this thesis will include:

• Further research at the quantum stochastic level with Fubini like QSI's, and path integrals, viewed from a parameter base level,

• Development at the (stochastic) differential equation level following on from the Representation Theorem,

• Applications. The security applications with Fock space are new areas of research and as such can be developed with Quantum Probability models or qubit, qutrit models. Quantum voting is a young area of research with many different forms of voting scheme at the classical level.

7.4 Conclusions

We have reviewed the work achieved in this thesis and outlined areas for further research. The applications achieve proof of concept and further research is underway.

Bibliography

[1] R. L. Rivest A. Shamir and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[2] A. H. Shen A. Yu Kitaev and M. N. Vyalyi. *Classical and Quantum Computation.* Graduate Studies in Mathematics.

[3] Tatsuaki Okamoto Alfred J. Menezes and Scott A. Vanstone. *Handbook of Applied Cryptography.* Discrete Mathematics and its Applications. CRC, 1997.

[4] Todd R. Andel and Alec Yasinsac. Secure internet voting protocol for overseas military voters. *Pre-Proceedings: Bringing Protocols to Life, 20th International Workshop on Security Protocols, Cambridge*, 2012.

[5] David Applebaum. *Levy Processes and Stochastic Calculus.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 2009.

[6] Ceorge Bachman and Lawrence Narici. *Functional Analysis.* Academic Press, 1966.

[7] P. Durganandini Behzad Lari and Pramod S. Joag. Multipartite entanglement in fermionic systems via a geometric measure. *quant-ph/10072908 v3*, pages 1– 25, 2010.

[8] V. P. Belavkin. A banach algebra approach to noncommutative integration. In *31st Quantum Probability and Related Topics*, JNCASR, Jakkur, Bangalore, India, 14th - 17th August, 2010.

[9] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Lett*, 68, 1992.

[10] Ola Bratteli and Derek W. Robinson. *Operator Algebras and Quantum Statistical Mechanics 1.* Texts and Monographs in Physics. Springer-Verlag, 2010.

[11] Ola Bratteli and Derek W. Robinson. *Operator Algebras and Quantum Statistical Mechanics II.* Texts and Monographs in Physics. Springer-Verlag, 2012.

[12] Feng Hao Brian Randell and Dylan Clarke. Self enforcing electronic voting. *Pre-Proceedings: Bringing Protocols to Life, 20th International Workshop on Security Protocols, Cambridge*, 2012.

[13] C. Crepeau R. Josza A. Peres C. H. Bennett, G. Brassard and W. K. Wootters. Teleporting an unknown quantum state via dual classical and epr channels. *Phys. Rev. Lett.*, pages 1895–1899, 1993.

[14] G. Brassard C. H. Bennett. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, page 175, 1984.

[15] Cairoli and J. Walsh. Stochastic integrals in the plane. *Acta Math*, pages 111 – 183, 1975.

[16] R. Cairoli. On a stochastic differential equation. *Compte Rendus Acad. Sc. Paris*, pages 1739 – 1742, 1972.

[17] David Chaum. The dining cryptographers problem: Unconditional sender and receiver untraceability. *Journal of Cryptology*, 1: p65–75, 1988.

[18] Matthias Christandl and Stephanie Wehner. Quantum anonymous transmissions. *quant-ph/0409201*, 2004.

[19] Henri Cohen and Gerhard Frey (et. al.). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, volume Discrete Mathematics and its Application. Chapman & Hall/CRC, 2006.

[20] J. M. Cook. The mathematics of second quantisation. *Trans. Amer. Math. Soc.*, 74:222–245, 1953.

[21] Peter J. Coughlin. *Probabilistic Voting Theory*. Cambridge University Press, 2008.

[22] Joan Daemen and Vincent Rijmen. *The Design of Rijndael, AES - The Advanced Encryption Algorithm*. Springer - Verlag, Berlin Heidelberg, 2002.

[23] D. Deutsch. Quantum theory, the church turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97, 1985.

[24] D. Deutsch and R. Josza. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439:553, 1992.

[25] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions in Information Theory*, IT-22, 6:644–654, 1976.

[26] Robert Gallager Dimitri Bertsekas. *Data Networks*. Prentice Hall, 2nd edition, 1992.

[27] Shahar Dolev and Itamar Pitowsky. A quantum secret ballot. *quant-ph/0602087v2*, 2006.

[28] Harold M. Edwards. *Divisor Theory*. Birkhauser, 1990.

[29] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[30] Dan Kenigsberg Eli Biham, Gilles Brassard and Tal Mor. Quantum computing without entanglement. *quant/ph 0306182*, pages 1 – 18, 2003.

[31] Andreas Enge. Computing discrete logarithms in high genus hyperelliptic jacobeans in provably subexponential time. *Mathematics of Computation*, 71:729–742, 2001.

[32] F. Hulpke *et al*. Unitarity as preservation of entropy and entanglement in quantum systems. *quant-ph/0407118 v3*, pages 1–10, 2005.

[33] D. E. Evans. Completely positive quasi-free maps on the car algebra. *Commun. Math. Phys.*, **70**:53, 1979.

[34] Dylan Clarke Feng Hao and Brian Randell. Analysis of issues and challenges of e-voting in the uk. *Pre-Proceedings: Bringing Protocols to Life, 20th International Workshop on Security Protocols, Cambridge*, 2012.

[35] V. Fock. Konfigurationsraum und zweite quantelung. *Zeitschrift fur Physik*, 75:622–647, 1932.

[36] Gerhard Frey and H. G. Ruck. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Mathematics of Computation*, 62, 206:865–874, 1976.

[37] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Advances in cryptology: Proceedings of CRYPTO 84. Lecture Notes in Computer Science. 196.*, 196:10–18, 1984.

[38] John Gough. Quantum stratonovich calculus and the quantum wong-zakai theorem. *math-ph/0511046v2*, pages 1–24, 2006.

[39] L. Gross. Existance and uniqueness of physical ground states. *J. Funct. Analysis*, 10:52–109, 1972.

[40] L. Grover. A fast quantum mechanical algorithm for database search. *STOC'28*, pages 212–219, 1996.

[41] Josef Gruska. *Quantum Computing*. McGraw Hill, 1999.

[42] Michael Planat Haret Rosu and Metod Saniga. From finite projective geometry to quantum phase enciphering. In *The 7th International Conference on Quantum Communication, Measurement and Computing*, University of Strathclyde, Glasgow, 2004.

[43] H. Heydari. *J. Phys A: Math. Gen*, 39:9839–9844, 2006.

[44] Mika Hirvensalo. *Quantum Computing*. Natural Computing. Springer - Verlag, New York, 2001.

[45] Dmitri Horoshko? and Sergei Kilin. Quantum anonymous voting with anonymity check. *quant-ph/09115065*, 2009.

[46] R. L. Hudson and K. R. Parthasarathy. Unification of fermion and boson stochastic calculus. *Communications in Mathematical Physics*, pages 457–470, 1986.

[47] Robin Hudson and Paul Jones. Unitary double product integrals as bogolubov implementors (the pseudo-rotation case). In *31st Quantum Probability and Related Topics*, JNCASR, Jakkur, Bangalore, India, 14th - 17th August, 2010.

[48] P. Imkeller. A stochastic calculus for continuous n-parameter strong martingales. *Stochastic Processes and their Applications*, 20:1–40, 1985.

[49] Kiyosi. Itô. On stochastic differential equations. *Memoirs of the American Mathematical Society*, 4:1–51, 1951.

[50] Un Cig Ji. Stochastic integral representations of quantum martingales on multiple fock space. *Math.PR/0707.2144 v1*, pages 489–505, 2007.

[51] John A. Vaccaro Joseph Spring and Anthony Chefles. Quantum protocols for anonymous voting and surveying. *quant/ph 0504161*, pages 1 – 8, 2005.

[52] John A. Vaccaro Joseph Spring and Anthony Chefles. Quantum protocols for anonymous voting and surveying. *Physical Review A, 012333*, 75, 2007.

[53] A. Sempera K. Zyczkowski, P. Horodecki and M. Lewenstein. On the volume of the set of mixed entangled states. *quant/ph 9804024*, pages 1 – 14, 1998.

[54] Richard V. Kadison and John R. Ringrose. *Fundamentals of the Theory of Operator Algebras*. vol. I. Academic Press, 1983.

[55] Richard V. Kadison and John R. Ringrose. *Fundamentals of the Theory of Operator Algebras*. vol. I - III. Academic Press, 1991.

[56] Mahew J. Hoffman Kathleen S. Gibbons and William K. Wooters. Discrete phase space based on finite fields. *quant-ph/0401155*, 2004.

[57] Fima C. Klebaner. *Introduction to Stochastic Calculus with Applications*. Imperial College Press, 3rd edition, 2012.

[58] Achim Klenke. *Probability Theory: A Comprehensive Course*. Universitext. Springer, 2008.

[59] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[60] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[61] Neal Koblitz. *A Course in Number Theory and Cryptography*. GTM 114. Springer - Verlag, New York, 2nd edition, 1994.

[62] P. E. Kopp. *Martingales and Stochastic Integrals*. Cambridge University Press, 1984.

[63] Erwin Kreyszig. *Advanced Engineering mathematics*. Wiley, 1979.

[64] L. Lamport. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21, No. 7:558–565, 1978.

[65] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications*. CUP, Cambridge, 1994.

[66] Rodney Loudon. *The quantum Theory of Light*. OUP, Oxford, 2000.

[67] Jan C. A. Van Der Lubbe. *Basic Methods of Cryptography*. CUP, Cambridge, 1998.

[68] F. J. MacWilliams and N. J. Sloane. *The Theory of Error Correcting Codes*. North Holland, New York, 1981.

[69] G. Mapp. Exploring markov models for gate limited service and their application to network - based services. In *(MON9), Mathematics of Networks*, Cambridge, UK, 18th September, 1999.

[70] Mark Hillery Marianna Bonanome, Vladimir Buzek and Mario Ziman. Towards protocols for quantum-ensured privacy and secure voting. *quant-ph/11085090*, 2011.

[71] Vladimir Buzek Mark Hillery, Mario Ziman and Martina Bielikova. Towards quantum-based privacy and voting. *quant-ph/0505041*, 2005.

[72] Paul-Andre Meyer. *Quantum Probability for Probabilists*, volume 1538 of *LNM*. Springer-Verlag, 1995.

[73] Serge Perrine Michael Planat, Haret Rosu and Metod Saniga. Finite algebraic geometric structures underlying mutually unbiased quantum measurements. *R. Buchanan et al. (es.); Time, Quantum and the Subjective;quant-ph/0503159*, pages 409–426, 2004.

[74] V. Miller. Use of elliptic curves in cryptography. *Advances in Cryptology*, Crypto 85:417–426, 1985.

[75] Akimasa Miyake and Frank Verstraete. Multipartite entanglement in 2 x 2 x n quantum systems. *quant-ph/0307067*, pages 1– 9, 2004.

[76] Richard A. Mollin. *Algebraic Number Theory*. Chapman & Hall/CRC, 1999.

[77] F. Verstraete J. Dehaene B.De Moor and H. Verschelde. Four qubits can be entangled in nine different ways. *Physical Review A*, 65:1 – 5, 2002.

[78] Michael A. Nielsen and Isaac J. Chuang. *Quantum Computation and Quantum Information*. CUP, Cambridge, UK, 10th anniversary edition, 2010.

[79] E. Karpov P. Navez and N. J. Cerf. Cloning quantum entanglement in arbitrary dimensions. *quant-ph/0503148*, pages 1–6, 2005.

[80] K. R. Parthasarathy. *An Introduction to Quantum Stochastic Calculus*. Monographs in Mathematics. Birkhauser, 1992.

[81] Nathanael Paul and Andrew S. Tanenbaum. The design of a trustworthy voting system. In *ACSAC 2009: The Annual Computer Security Applications Conference*, Sheraton Waikiki Hotel, Honolulu, Hawaii, 2009.

[82] Gert K. Pederson. *C*-Algebras and their Automorphism Groups*, volume L.M.S. Monographs. Academic Press, London, New York, San Francisco, 1979.

[83] Larry L. Peterson and Bruce S. Davie. *Computer Networks*. Morgan Kaufmann, 5th edition, 2011.

[84] Michael Planat. Huyghens, bohr, riemann and galois phase locking. *International Journal of Modern Physics B;quant-ph/0510044*, pages 1–18, 2005.

[85] R. Powers and E. Størmer. Free states of the canonical anticommutation relations. *Commun. Math. Phys.*, pages 1–33, 1970.

[86] C. Barnett R. F. Streater and I. F. Wilde. The ito-clifford integral. *J. Funct. Analysis* , 48 (2):172–212, 1982.

[87] C. Barnett R. F. Streater and I. F. Wilde. Quasi-free quantum stochastic integrals for the car and ccr. *J. Funct. Analysis* , 52 (1):19–47, 1983.

[88] Michael Reed and Barry Simon. *Functional Analysis*. Academic Press, 1980.

[89] Richard D. Richmond Robert L. Hagerman. Random walks, martingales and the otc. *Journal of Finance*, 28(4):897–909, 1973.

[90] L. C. G. Rogers and D. Williams. *Diffusions, Markov Processes and Martingales I & II*. Cambridge Mathematical Library. Cambridge University Press, 2010.

[91] Jeffrey S. Rosenthal. *A First Look at Rigorous Probability Theory*. Oxford Science Publications. OUP, 2000.

[92] Shôichirô Sakai. *Operator Algebras in Dynamical Systems*, volume 41 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1991.

[93] Shôichirô Sakai. *C*- and W*- Algebras*. Springer-Verlag, 1996.

[94] Irving Segal. Correction to the paper 'a non-commutative extension of abstract integration'. *Ann of Math*, 58:595–596, 1953.

[95] Irving Segal. A non-commutative extension of abstract integration. *Ann of Math*, 57: pp 401–457, 1953.

[96] Irving E. Segal. Tensor algebras over hilbert spaces i. *Trans. Amer. Math. Soc.*, 81:106–134, 1956.

[97] Irving E. Segal. Tensor algebras over hilbert spaces ii. *Ann. of Math.*, 63:160–175, 1956.

[98] Irving E. Segal and Ray A. Kunze. *Integrals and Operators*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1978.

[99] Ahmed D. Shaikh. Significance of joint density plots in markov internet traffic modelling. In *(MON9), Mathematics of Networks*, Cambridge, UK, 18th September, 1999.

[100] Peter W. Shor. Algorithms for quantum computation: Discrete log and factoring. *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science - FOCS*, pages 20–22, 1994.

[101] Peter W. Shor. Polynomial time algorithms for prime factorisation and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[102] Joseph H. Silverman and Joe Suzuki. Elliptic curve discrete logarithms and the index calculus. *Advances in Cryptology*, Asiacrypt 98:110–125, 1998.

[103] Electoral Reform Society. Voting systems. *http//www.electoral-reform.org.uk/index.htm*, 2006.

[104] Fei Gao Song Lin, Qiao-Yan Wen and Fu-Chen Zhu. Improving the security of multiparty quantum secret sharing based on the improved bostrmfelbinger protocol. *Optics Communication*, 281(17):45534554, 2008.

[105] Joseph Spring. A case of standard attacks against the dlp and ecdlp. Technical Report 391, University of Hertfordshire, Quantum Information Group, School of Computer Science, FEIS, Hatfield, UK, 2003.

[106] Joseph Spring. Entanglement and irreducibilty. *Quantum Communication, Measurement and Computing 8*, AIP, 2007.

[107] Joseph Spring. Quantum primitives. *Quantum Communication, Measurement and Computing 9*, AIP, 2009.

[108] William J. Spring. The ito-clifford wong-zakai integrals and martingale representation. *Foundations of Probability and Physics - 4*, AIP, 2007.

[109] William J. Spring. Martingale representation in the clifford and quasi-free sheet. *Quantum Communication, Measurement and Computing 8*, AIP, 2007.

[110] William J. Spring. Quasi-free stochastic integrals and martingale representation. *Quantum Probability and White Noise Analysis*, 23:236–241, 2007.

[111] William J. Spring. Multiparameter processes over the clifford sheet. *International Journal of Pure and Applied Mathematics*, 49(3), 2008.

[112] William J. Spring. Multiparameter quantum stochastic processes. In *30th Quantum Probability and Related Topics*, Pontificia Universidad Catolica, de Chile, Santiago, Chile, 23rd - 28th September, 2009.

[113] William J. Spring. Quantum stochastic processes. *Quantum Communication, Measurement and Computing 9*, AIP, 2009.

[114] William J. Spring. A discussion on multiparameter processes. In *31st Quantum Probability and Related Topics*, JNCASR, Jakkur, Bangalore, India, 14th - 17th August, 2010.

[115] William J. Spring. Multiparameter quantum stochastic processes. *Quantum Probability and White Noise Analysis*, 28:323–329, 2010.

[116] William J. Spring. Quantum generators. In *Quantum Communication, Measurement and Computing 10*, University of Queensland, Brisbane, Australia, 19th - 23rd July, 2010.

[117] William J. Spring. Type r quantum stochastic integrals. In *Quantum Communication, Measurement and Computing 10*, University of Queensland, Brisbane, Australia, 19th - 23rd July, 2010.

[118] William J. Spring. Multidimensional quantum stochastic integrals. *Quantum Communication, Measurement and Computing 10*, AIP, 2011.

[119] William J. Spring and Ivan F. Wilde. The wong-zakai-clifford quantum stochastic integral. *Reports on Mathematical Physics*, 42:389–399, 1998.

[120] William J. Spring and Ivan F. Wilde. Quasi-free quantum stochastic integrals in the plane. *Reports on Mathematical Physics*, 49:63–76, 2002.

[121] William J. Spring and Ivan F. Wilde. Quasi-free fermion planar quantum stochastic integrals. *Quantum Probability and White Noise Analysis*, 15:243–253, 2003.

[122] William Stallings. *Cryptography and Network Security - Principles and Practices*. Prentice Hall, international, 5th edition, 2010.

[123] Gilles Brassard Stephane Beauregard and Jose Manuel Fernandez. Quantum arithmetic on galois fields. *quant/ph 0301163*, pages 1 – 29, 2003.

[124] Douglas R. Stinson. *Cryptography: Theory and Practice*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, New York, 3rd edition, 2005.

[125] Serban Stratila. *Modular Theory in Operator Algebras*. Abacus Press, Tunbridge Wells, Kent, England, 1981.

[126] Serban Stratila and Laszlo Zsido. *Lectures on Von Neumann Algebras*. Abacus Press, Tunbridge Wells, Kent, England, 1979.

[127] F. Strocchi. *Mathematical Structure of Quantum Mechanics*. Advanced Series in Mathematical Physics - Vol.27. World Scientific, 2005.

[128] Masamichi Takesaki. *Theory of Operator Algebras I, II, III*, volume 124,125,127 of *Encyclopaedia of Mathematical Sciences: Operator Algebras and Non-Commutative Geometry V, VI, VIII*. Springer-Verlag, 2003.

[129] Koutarou Suzuki Tatsuaki Okamoto and Yuuki Tokunaga. Quantum voting scheme based on conjugate coding. *NTT Technical Review*, 6(1):1 – 8, 2008.

[130] Marianne Terp. *L^p Spaces Associated with Von Neumann Algebras*. Lic. Scient Thesis. University of Odense, 1981.

[131] Hisaharu Umegaki. Conditional expectation in an operator algebra. *Tohoku Math. J. (2)* , 6 No. 2-3:177–181, 1954.

[132] Hisaharu Umegaki. Conditional expectation in an operator algebra ii. *Tohoku Math. J. (2)* , 8 No. 1:86–100, 1956.

[133] Hisaharu Umegaki. Conditional expectation in an operator algebra iii. *Kodai Math. Sem. Rep.*, 11 No. 2:51–64, 1959.

[134] Hisaharu Umegaki. Conditional expectation in an operator algebra iv. *Kodai Math. Sem. Rep.*, 14 No. 2:59–86, 1962.

[135] Grgoire Ribordy Valerio Scarani, Antonio Acn and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92(057901), 2004.

[136] W. Dur G. Vidal and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62, 062314:1–12, 2000.

[137] Jan von Plato. *Creating Modern Probability*. Cambridge Studies in Probability, Induction and Decision Theory. Cambridge University Press, 1994.

[138] John Walsh. Stochastic integrals in the plane. *Proceedings of the International Congress of Mathematicians*, pages 189 – 194, 1974.

[139] John Walsh. *Martingales With A Multidimensional Parameter and Stochastic Integrals in the Plane*, volume 1215 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[140] Richard L. Wheeden and Antoni Zygmund. *Measure and Integral*, volume 43 of *Pure and Applied Mathematics*. Marcel Dekker Inc., 1977.

[141] E. Wong and M. Zakai. Martingales and stochastic integrals for processes with a multidimensional parameter. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 29:109–122, 1974.

[142] E. Wong and M. Zakai. Weak martingales and stochastic integrals in the plane. *The Annals of Probability*, 4(4):570–586, 1976.

[143] E. Wong and M. Zakai. An extension of stochastic integrals in the plane. *The Annals of Probability*, 5(5):770–778, 1977.

Index

Appendices

Appendix A

Cryptographic Algorithms

A.1 The Diffie Hellman Key Agreement Protocol

This is a classical key agreement protocol, in contrast to a key exchange protocol, since neither sender nor receiver know the key until the end of the protocol. The protocol is based upon the discrete logarithm problem and hence is based upon a finite multiplicative cyclic group, generated by a primitive element α. The primitive α generates the integers $1, 2, 3, \ldots, p-1$, where p is an agreed prime number. α is often referred to as a primitive root of p, by which we mean that α generates each of the integers from 1 up to $p-1$.

Definition 53. Given a finite cyclic group $(G, \circ)$ with n elements we define a primitive for the group to be any element α that generates the entire group under the binary operation $\circ$. The finite cyclic group may be denoted by the symbol $\langle\alpha\rangle$.

We recall the discrete logarithm problem:

Definition 54. Given a prime number p, primitive α, and $\beta \in \langle\alpha\rangle = 1, 2, 3, \ldots, p-1$, (the cyclic group generated by α), the discrete logarithm problem is to find a value r such that $\beta = \alpha^r \, mod \, p$.

The protocol runs as follows:

Let Alice and Bob denote the senders and receivers.

1. Bob and Alice agree the primitive before starting the protocol.
2. Alice and Bob select secret random numbers a, and b respectively.
3. Alice sends α^a to Bob whilst Bob sends α^b to Alice.
4. Alice and Bob now possess the same key $k = \alpha^a b$.

Alice and Bob can now use the same key in a symmetric key cryptography scheme [122] such as DES (the Data Encryption Scheme) or AES (the Advanced Encryption Scheme) to exchange data.

A.2 The Classical El-Gamal Encryption Scheme

Let Alice and Bob denote sender and receiver respectively. We therefore consider the case in which Alice wishes to send ciphertext to Bob. Since this is a public key cryptosystem Alice will use Bobs public key to encrypt the plaintext message and Bob will decrypt using his private key.

The plaintext messages are broken into blocks of size less than p, p being a suitable prime number, selected so that the DLP is unlikely to be broken during the time period that security is sought. Different characters used in Alice's plaintext messages are associated with one and only one value in $\mathbb{Z}_p^*$. For a trivial example, take
$A = 1$, $B = 2$, $C = 3, \ldots$

A.2.1 The Classical El-Gamal Encryption and Decryption Algorithm

Bob's public key is the triple (p, α, β), in which α is a primitive for $\mathbb{Z}_p^*$.

Bob's private key is $r = log_\alpha(\beta)$.

In addition to using Bob's public key for encryption, Alice also selects a random number $k \in \mathbb{Z}_{p-1}$ and uses this in the encryption process.

Given $m \in \mathbb{Z}_p^*$, a plaintext value, encryption is defined to be

$$e(m,k) = (\alpha^k mod p, m\beta^k mod p)$$

producing a ciphertext value in $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$. This is sent to Bob who decrypts the ciphertext pair using

$$d(\alpha^k mod p, m\beta^k mod p) = [m\beta^k mod p((\alpha^k mod p)^r)^{-1}] mod p$$

Appendix B

Voting Protocols

B.1 Goals, Protocols and Algorithms

In any secure communication between two or more parties one is interested in achieving a range of goals. Amongst these is authentication, confidentiality, integrity, non-repudiation and, particularly in the case of voting, anonymity.

B.1.1 Authentication

Authentication involves convincing the parties that you wish to communicate with, that you are entitled to communicate with them. In the case of your computer this involves the provision of a username and password. For an election, a poll card, name and address.

B.1.2 Confidentiality

Confidentiality involves keeping data confidential to oneself and those parties that are intended should have access to the data. Confidentiality is often achieved through a combination of symmetric and/or asymmetric cryptographic algorithms. Examples of symmetric algorithms could include AES [22] (the Advanced Encryption Scheme) and

DES [67] (the Data Encryption Standard). Examples of asymmetric algorithms could include RSA [1] (the Rivest, Shamir, Adleman algorithm whose security relies upon on the perceived difficulty in solving the Integer factorisation Problem for suitably selected values) and El-Gamal [3, 19, 37, 59, 74] (reliant upon the perceived difficulty in solving the Discrete Logarithm Problem / Elliptic Curve Discrete Logarithm Problem for suitably chosen values and/or curves).

B.1.3 Integrity

Integrity involves measuring change to data between sender and receiver. The intention is that data sent, by the sender Alice should be the same as the data received by the receiver, Bob. With classical distributed systems this involves the use of hash functions [3, 83] such as the SHA and MDn series of algorithms, Cyclic Redundancy Checks, parity checks and checksums. With quantum algorithms, [9, 14, 41, 78] such as BB84 and B92 it involves the use of no-cloning, measurement by an eavesdropper leading to disturbance and check bits between Alice and Bob.

B.1.4 Non-Repudiation

Non-repudiation involves ensuring that actions that a party have made cannot be denied. For example if I have cast a vote, in a voting scheme then the protocol ensures that denial will not be entertained. The use of digital signatures is one mechanism for achieving this.

B.1.5 Anonymity

With a voting scheme, anonymity is often desirable, and involves breaking any links that exist between a cast vote and the voter. The following section discusses this in more detail.

B.2 Classical Voting Schemes

[This section is taken from [51] and presented here for completeness. For references see the paper which may be accessed from the following section].

Various properties have emerged from the literature as being desirable attributes of classical secret ballot voting schemes. Amongst these is the concept of resilience which involves the properties of universal verifiability, privacy, and robustness. A universally verifiable election scheme is a scheme deemed open to scrutiny by all interested parties. Compliance with this property ensures that ballots are carried out correctly and that subsequent tallies are fairly assessed. For a scheme satisfying the privacy property an honest participant is assured that their vote remains confidential, provided that the number of attackers does not grow too large. With the property of robustness, an election scheme has the capacity to recover from faults again, provided that the number of parties involved does not grow too large. Schemes satisfying these three properties are said to be resilient. Another desirable property of an election scheme, particularly as a counter to the risk of vote buying or coercion, is that it is receipt-free. Receipt-free election schemes ensure that voters cannot prove, to other parties, the particular vote cast within the scheme. Further desirable properties are to be found in the literature, for example. Voting protocols performed within a classical setting are in general grouped according to their use of homomorphisms, MIX nets, and blind signatures.

B.2.1 Homomorphic Election Schemes

These involve the use of a homomorphic, probabilistic encryption scheme consisting of a plaintext space V, a ciphertext space C each of which form group structures under appropriate binary operations and together with a family of homomorphic encryption schemes such that by . Homorphic election Schemes are important since they allow one

to derive tallies without the need to decrypt individual votes. Such schemes lead to resilient election schemes.

B.2.2 MIX net schemes

MIX nets were first introduced by Chaum, and have found applications in scenarios involving anonymity, elections and payments. A MIX net election scheme involves the use of shuffle machine agents referred to as MIX servers, which take as input a ciphertext vector these could be, for example, encrypted votes submitted by, for example, voters and produces as output a permuted vector which the components are shuffled of corresponding output for example, decrypted votes such that the link between the source for each ciphertext encrypted vote and its resulting plaintext vote remains hidden. The resilience properties of privacy, verifiability and robustness may be presented in terms of t-privacy, t-verifiability, and t-robustness, where it is understood that t refers to the number of malicious MIX servers that the scheme can withstand given at most n?2 malicious sources. A scheme satisfying the above three t-properties is said to be t resilient. The development of classical MIX net schemes to achieve, in particular, privacy initially led to ciphertext whose size was proportional to the number of MIX servers involved in the scheme. This problem was resolved by Park, Itoh, and Kurosawa, resulting in ciphertext whose length was independent of the number of MIX servers. Sako and Kilian, produced a general MIX net scheme satisfying verifiability but failing with regard to robustness. The first resilient MIX net scheme was produced by Ogata, Kurosawa, Sako, and Takatani.

B.2.3 Blind signature schemes

These were also introduced by Chaum and have been developed with applications in anonymity, election, and payment schemes. The basic concept involves obtaining a

signature to authenticate a message, for example, an encrypted vote, without the signer being able to observe the message vote itself or its signature. Verification regarding the signature is however supported by such schemes whilst maintaining privacy regarding the actual plaintext. A signer is thus denied the ability to link a particular plaintext with its corresponding blind signature. Variations upon such schemes are to be found with, for example, fair blind signatures in which the possibility of, for example, blackmail is discussed.

B.2.4 Sender untraceability schemes

These schemes allow information to be sent anonymously. For example, in Chaums Dining Cryptographers Problem a group of diners wish to determine if either an external agency or one of the group is paying anonymously for the meal. The solution requires 1 bit of information to be broadcast anonymously using a communication channel available to all diners. The simplest situation occurs for three diners with only two possible scenarios: one diner is to pay the bill or no diners pay the bill. The diner who pays broadcasts the message 1 in the following way. Each diner shares a single binary-digit one-time pad with the other two. The broadcast is executed by each diner adding the two numbers on the one time pads he or she holds. If one of the diners is paying he or she adds 1 to the value of the sum. The results modulo 2 are announced publicly to all diners. The sum of the 3 broadcast messages modulo 2 is 1 only if the message 1 is sent by a paying diner otherwise it is 0. Thus a message is broadcast but the identity of a paying diner is untraceable. The security of a classical scheme is deemed to be one of two varieties: computational or unconditional also known as information-theoretic security. A scheme which can be broken in principle but requires more computing power than a realistic adversary can access in a given critical time is deemed computationally secure. Examples are schemes based on the integer

factorization problem and the discrete logarithm problem. Such computationally secure schemes are under threat from quantum computing. On the other hand, a scheme which is secure even if an adversary has unlimited computing resources is said to be unconditionally secure. A one time pad encryption scheme is unconditionally secure. Homomorphic maps and mixed nets not based on the one time pad are computationally secure. Blind signatures can be applied in an unconditionally secure manner to authenticate a vote and sender untraceability provides anonymity with unconditional security. Chaums secret ballot protocol, which uses blind signature and sender untraceability schemes, allows unconditionally secret voting. The sender untraceability component of the protocol requires one-time pads between all pairs of voters, that is N(N-1)/2 one time pads are required for a ballot with N voters.

B.3 Quantum Voting Schemes

Quantum voting protocols first appeared [51, 71] in April and May 2005 and has developed at a steady rate with papers [27, 45, 70, 104, 129] describing schemes based on entanglement (comparative ballot, anonymous survey, travelling ballot, distributed ballot), on conjugate coding; schemes with voter identity and multiparty secret sharing. Each scheme developed, has been based on multipartite qubit systems. We seek to explore the development of quantum based voting schemes employing tools developed in quantum probability. Our motivation for this being what appear to be, natural tools for the collection of votes cast.

Appendix C

Publications

There are 5 refereed papers relating to the work presented in this thesis. The first was taken as the starting point for this work which is interested in quantum stochastic integrals defined over a general parameter space.
In order the papers are:

W. J. SPRING, Multiparameter Quantum Stochastic Processes, QPRT 30, Quantum Probability and White Noise Analysis, 28, (2010), [115]
$< http://www.worldscientific.com/doi/pdf/10.1142/9789814338745_0019 >$

W. J. SPRING, Multiparameter Quantum Processes over the Clifford Sheet, International Journal of Pure and Applied Mathematics, (Invited), 49, (No. 3), (2008), 451-457 [111] $< http://www.ijpam.eu/contents/2008-49-3/19/19.pdf >$

W. J. SPRING, Quasi-Free Stochastic Integrals and Martingale Representation, Quantum Probability and White Noise Analysis, 23, (2007), [110]
$< http://www.worldscientific.com/doi/pdf/10.1142/9789812835277_0019 >$

J. A.VACCARO, J. SPRING AND A. CHEFLES, Quantum Protocols for Anonymous Voting and Surveying $< http://link.aps.org/abstract/PRA/v75/e012333 >$, Physical Review A $< http://pra.aps.org/ >$, 75, 012333 (2007) [52]

W. J. SPRING, The Ito-Clifford Wong-Zakai Integrals and Martingale Representation, Foundations of Probability and Physics 4, AIP, (2007) (Developed from earlier work), [108]

$< http://www.springer.com/physics/quantum+physics/book/978-0-7354-0391-8?otherVersion=978-0-7354-0391-8 >$

Other papers accepted to conferences (not presented here) include:

W. J. SPRING, Multidimensional Quantum Stochastic Integrals, Quantum Communication, Measurement and Computing 10, AIP, (2011), [118]

W. J. SPRING, Quantum Stochastic Processes, Quantum Communication, Measurement and Computing 9, AIP, (2009), [113]

W. J. SPRING, Martingale Representation in the Clifford and Quasi-Free Sheet, (CAR), Quantum Communication, Measurement and Computing 8, AIP, (2007), [109]