이학 박사 학위논문

Abstract harmonic analysis in quantum information theory

(양자정보이론에서의 추상조화해석학)

2023년 8월

서울대학교 대학원

수리과학부

박상준

Abstract harmonic analysis in quantum information theory

(양자정보이론에서의 추상조화해석학)

지도교수 이훈희

이 논문을 이학 박사 학위논문으로 제출함

2023년 4월

서울대학교 대학원

수리과학부

박상준

박상준의 이학 박사 학위논문을 인준함

2023년 6월

위 원 장 ____________________ (인)

부 위 원 장 ____________________ (인)

위 원 ____________________ (인)

위 원 ____________________ (인)

위 원 ____________________ (인)

Abstract harmonic analysis in quantum information theory

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Sang-Jun Park

Dissertation Director : Professor Hun Hee Lee

Department of Mathematical Sciences
Seoul National University

August 2023

Abstract

Abstract harmonic analysis in quantum information theory

Sang-Jun Park
Department of Mathematical Sciences
The Graduate School
Seoul National University

This Ph.D. thesis delves into the fascinating realm of quantum information theory, employing methods from abstract harmonic analysis. The research is organized into two parts, each focusing on independent topics, based on the research results during the author's doctoral studies [BCL+22, PJPY23, PY23].

In the first part, our primary objective is to present an abstract definition of Gaussian states, inspired by the intriguing mathematical connections between bosonic Gaussian states and stabilizer states. To achieve this, we leverage the phase space formulation, considering a *locally compact abelian group* (LCA) with a proper symplectic structure as the abstract phase space. Within this framework, we naturally define the Weyl unitary operators and characteristic functions. The Gaussian states are then defined through the concept of Gaussian distributions on LCA groups in the sense of Bernstein. Remarkably, this definition establishes a universal framework that unifies many important notions in quantum theory as well as simultaneously explaining bosonic Gaussian states and stabilizer states. Moreover, we justify our definition by showing that pure Gaussian states over a phase space derived from a totally disconnected LCA group can be characterized by the non-negativity of their Wigner quasi-distribution. This result can be interpreted as an analog of Hudson's theorem and a generalization of Gross's result.

In the second part, we develop a theory of quantum entanglement under the symmetry with respect to unitary representations of compact groups. Quantum entanglement plays a vital role as a valuable resource in quantum information processing, and significant efforts have been dedicated to unraveling the mathematical structure of entanglement in recent years. While the general dualities between mapping cones introduced by Størmer can describe various notions related to quantum entanglement, they are not sufficient to effectively deal with entanglement due to the computational hardness of testing entanglement. In this thesis, we show that such duality results carry over into the framework of compact group symmetry. This directly leads to two applications in quantum information theory: (1) the optimization of entanglement witnesses and Schmidt number witnesses, and (2) the equivalence between the problem of PPT=separability and the problem of checking whether every extremal positive map is completely positive or completely copositive under compact group symmetry. The merits of our proposed framework are showcased through detailed analyses of examples, which solve various open problems related to quantum entanglement.

Key words: Abstract harmonic analysis, group representation, Quantum information theory, Gaussian state, Quantum entanglement, Schmidt number
Student Number: 2016-20234

Contents

보존용 학위논문 정오표

페이지	정정 전	정정 後
p. 160 : line 5 p. 160 : line 11	첫 번쨰 ’ Bernstein 방식’ (따옴표 방향 수정)	첫 번째 ‘Bernstein 방식’

Chapter 1

Introduction

This Ph.D. thesis is devoted to the study of problems in Quantum Information Theory (QIT) using methods from abstract harmonic analysis. In particular, we focus on several applications of representations of *locally compact groups* in QIT, based on the three papers as follows.

1. [BCL+22] C. Beny, J. Crann, H. H. Lee, S.-J. Park, and S.-G. Youn. *Gaussian quantum information over general quantum kinematical systems I: Gaussian states.* Preprint, arXiv:2204.08162, 2022

2. [PJPY23] S.-J. Park, Y.-G. Jung, J. Park, and S.-G. Youn. *A universal framework for entanglement detection under group symmetry.* Preprint, arXiv:2301.03849, 2023.

3. [PY23] S.-J. Park and S.-G. Youn. *k-positivity and schmidt number under orthogonal group symmetries.* Preprint, arXiv:2306.00654, 2023.

These papers delve into applications in two indepedent areas of QIT: (1) phase space formulation and Gaussian quantum information [BCL+22], and (2) quantum entanglement theory [PJPY23, PY23]. In this chapter, we provide a brief introduction to these two topics and highlight the aspects where methods from abstract harmonic analysis were effectively applied in our research.

Topic 1: Gaussian property of stabilizer states

(Bosonic) Gaussian states and *stabilizer states* are two fundamental objects in quantum optics and quantum error correction, respectively [WPGP$^+$12, Got97]. Despite their seemingly different definitions and origins, they exhibit several similarities. First of all, they can be understood in term of the phase space formulation developed by H. Weyl [Wey50]. Secondly, when these states are pure, both classes can be characterized via *Hudson's theorem* and its discrete version, i.e., the non-negativity of *Wigner-quasi distribution*, and their underlying wave functions have similar explicit formulas [Hud74, SC83, Gro06]. This supports the notion that stabilizer states can be understood as finite-dimensional analog of Gaussian states.

Motivated by these insights, in Chapter 3, we provide a mathematically complete framework by introducing an abstract definition of Gaussian states. To achieve this, we use Fourier analysis over locally compact abelian (LCA) groups with proper symplectic structures, which serve as abstract phase spaces. We propose a comprehensive definition of Gaussian states, encompassing both Gaussian states and stabilizer states within the most general setting. Specifically, we define Gaussian states using the concept of Gaussian distributions on LCA groups in the sense of Bernstein (Definition 3.3.1). This definition not only unifies Gaussian states and stabilizer states but also offers a universal framework that incorporates various important notions in quantum theory [RSSK$^+$10, Zel20].

Moreover, our formulation of the abstract phase space enables a comprehensive definition of the Wigner quasi-distribution, prompting the exploration of a generalized Hudson's theorem. Notably, we present an affirmative answer to this question when the underlying phase space arises from a *totally disconnected* LCA group (Theorem 3.7.2), thus extending the previous work of Gross [Gro06].

We summarize our results in Table 1.1.

Table 1.1: Summary of the results in Chapter 3 (d: odd, F: 2-regular)

Phase space	Gaussian state	Hudson theorem	Section
$\mathbb{R}^n \times \mathbb{R}^n$	bosonic Gaussian state	True [Hud74, SC83]	
$\mathbb{Z}_d^n \times \mathbb{Z}_d^n$	stabilizer state	True [Gro06]	3.4
$\mathbb{Q}_p^n \times \mathbb{Q}_p^n$	p-adic Gaussian state [Zel20]	True (*New*)	3.4, 3.7
$F \times \widehat{F}$	Fully characterized	Partially true (*New*)	3.4, 3.7
$\mathbb{T}^n \times \mathbb{Z}^n$	standard ONB for $L^2(\mathbb{T})$	True [RSSK+10]	3.5
$\mathbb{Z}_2^n \times \mathbb{Z}_2^n$	None		3.6

Topic 2: Duality and quantum entanglement under group symmetry

Quantum entanglement has been regarded as one of the most fundamental non-classical manifestations in quantum theory [EPR35, Bel64, CHSH69]. Moreover, quantum entanglement serves as a key resource for various quantum information processing tasks, such as cryptography, quantum teleportation, and super-dense coding [HHHH09, GT09]. Several criteria have been developed to detect entanglement, with many of them based on Horodecki's criterion [HHH96]. This criterion establishes that positive maps can be used as entanglement witnesses, leading to the recovery of well-known approaches such as the positive partial-transpose (PPT) criterion [Per96] and reduction criterion [HH99]. In particular, classifying PPT entanglement has been one of the most important issues because of its direct connection with bound entanglement [HHH99]. PPT entangled states are proven to be applicable in performing non-classical tasks [HHH99, VW02, Mas06] and producing secure cryptographic keys [HHHO05, HHHO09, HPHH08]. Unfortunately, determining whether a given bipartite quantum state is entangled is NP-hard in general [Gur03], making it a challenging task to find PPT entangled states despite extensive research.

Another crucial issue in the theory of quantum entanglement is the quantification of entanglement [PV07]. Other than the case of pure states, there are several (non-equivalent) candidates for entanglement measures of mixed states, such as distillable entanglement, entanglement cost, and formation of entanglement. Furthermore, the notion of k-positivity in operator algebra has established a strong connection with the *Schmidt number* [TH00], a natural measure to certify entanglement dimensionality. The Schmidt number has recently gained attention in relation to the *PPT-squared conjecture* and entanglement distillation [HLLMH18, CMHW19, CYT17, CYT19, Car20], and the difficulty arises from the lack of explicit computable examples. Indeed, the problem of determining whether a given linear map is (k-)positive or not is known to be NP-hard, and accurate computations of Schmidt numbers have been possible for very few examples.

On the other hand, both of these concepts can be described in a more general framework, namely the duality between *mapping cones*. The notion of mapping cones was introduced by Størmer [Sr86] to study extension problems of positive linear maps and has been studied in the context of quantum information theory. Mapping cones have two characteristics: (1) they contain sufficiently many classes that are important in quantum information theory, and (2) they can be described via *duality* in many different ways. For example, we have, for a mapping cone $\mathcal{K}$,

- $\Phi \in \mathcal{K} \iff \mathcal{L}^* \circ \mathcal{L}$ is CP for every $\mathcal{L} \in \mathcal{K}^\circ$.
- $X \in C_{\mathcal{K}} := \{C_\Phi : \Phi \in \mathcal{K}\} \iff (\mathrm{id}_A \otimes \mathcal{L}^*)(X) \geq 0 \ \forall \ \mathcal{L} \in \mathcal{K}^\circ$,

where $C_{\mathcal{L}}$ denotes the Choi matrix of $\mathcal{L}$ (refer to (2.2.4)). These equivalences mean that the linear maps in $\mathcal{K}^\circ$ can be considered as *witnesses* for the elements in $\mathcal{K}$ and $C_{\mathcal{K}}$. Indeed, such duality has been applied to characterize many notions in the theory of quantum entanglement, such as separability, entanglement-breaking maps, Schmidt numbers, as well as decomposable maps and k-positive maps [HHH96, TH00, SSrZ09, GKS21]. Nevertheless, the mapping cone $\mathcal{K}^\circ$ is generally too large and complex to efficiently describe the convex structure of $\mathcal{K}$.

In this thesis, we restrict the class $\mathcal{K}$ by considering symmetries with respect to compact groups. Specifically, we mainly consider two types of symmetries: *invariance* of bipartite matrices and *covariance* of linear maps with respect to a unitary representation of a compact group (Section 4.2). Such a restriction is common in quantum information theory, mainly due to the difficulty in analyzing entanglement and in the hope that symmetry allows us to focus on more tractable models.

One of the main results of the thesis shows that the duality between mapping cones fits well with our framework of compact group symmetry, leading to the optimization of witnesses. The statement can be outlined as follows.

Theorem 1.0.1. *Suppose $\mathcal{K}$ is a mapping cone of positive maps on M_{d_A} into M_{d_B}. Then for (π_A, π_B)-covariant map Φ, we have $\Phi \in \mathcal{K}$ if and only if $\mathcal{L} \circ \Phi$ is copmletely positive for every $\mathcal{L} \in \mathrm{Ext}\big((\mathcal{K}^\circ)^* \cap \mathrm{Cov}_1(\pi_B, \pi_A)\big)$, where $\mathrm{Cov}_1(\pi_B, \pi_A)$ is the set of (π_B, π_A)-covariant linear maps whose Choi matrix has unit trace. Furthermore, for $\overline{\pi_A} \otimes \pi_B$-invariant bipartite matrix X, we have $X \in C_{\mathcal{K}}$ if and only if $(\mathrm{id}_A \otimes \mathcal{L})(X) \geq 0$ for every $\mathcal{L} \in \mathrm{Ext}\big((\mathcal{K}^\circ)^* \cap \mathrm{Cov}_1(\pi_B, \pi_A)\big)$.*

This result enables us to flexibly address the problem of PPT entanglement and Schmidt number. Our contributions can be summarized as follows.

Entanglement witness and the problem of PPT = SEP

We optimize the use of *entanglement witnesses* [HHH96] by showing that *only extreme covariant positive maps* are necessary for testing the entanglement of invariant quantum states (Theorem 4.3.1). Additionally, we establish the equivalence between PPT entanglement in invariant states and positive non-decomposable maps in the class of covariant maps (Corollary 4.3.4). This framework enables us to provide solutions to three problems related to "**PPT = SEP**" (Table 1.2), strengthening existing results and resolving many open problems.

Table 1.2: The problem **PPT** = **SEP** under three group symmetries

Group symmetry	PPT=SEP	Strenghthens the results in	Section
Hyperoctaheral group	True	[VW01, KMS20]	5.1
$U \otimes U \otimes U$	False	[EW01]	5.3.1
$U \otimes \overline{U} \otimes U$	True	[COS18]	5.3.2

Schmidt number witness

More generally, it suffices to consider only *(extreme) covariant k-positive maps* to analyze the Schmidt number of invariant quantum states (Theorem 4.3.2). As an application, we completely characterize the Schmidt number of *orthogonally invariant states* (Section 5.2). These states, denoted as $\rho_{a,b}^{(d)} \in M_d \otimes M_d$, are defined as follows:

$$\rho_{a,b}^{(d)} := \frac{1-a-b}{d^2} I_d \otimes I_d + \frac{a}{d} \sum_{i,j=1}^{d} |ii\rangle\langle jj| + \frac{b}{d} \sum_{i,j=1}^{d} |ij\rangle\langle ji|, \qquad (1.0.1)$$

The regions for the Schmidt number of $\rho_{a,b}^{(d)}$ turn out to be highly nontrivial, even in low dimensions, as visualized in Figure 1.1. To the best of our knowledge, our computations provide the first example of the complete characterization of Schmidt numbers in a non-trivial class parameterized by at least two real variables (in arbitrarily high dimensions d).

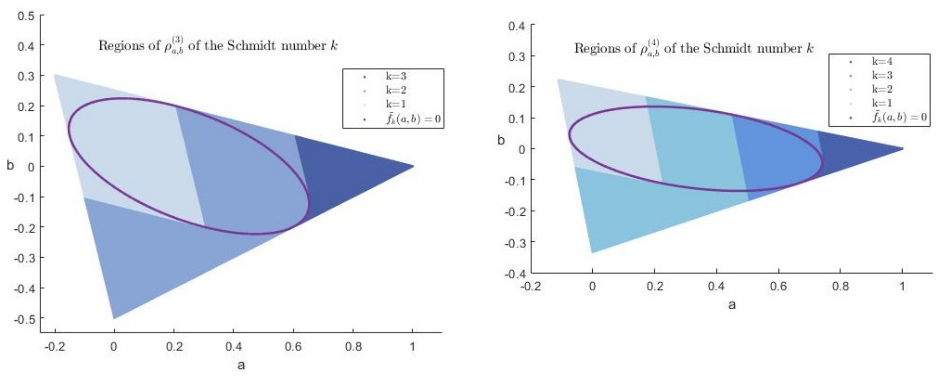

Figure 1.1: Schmidt number of orthogonally invariant states when $d = 3, 4$

Chapter 2

Preliminaries

2.1 Abstract harmonic analysis

In various aspects of abstract harmonic analysis, locally compact groups and their unitary representations play a fundamental role. Let us first introduce some basic definitions related to these concepts. A topological group G is called a *locally compact group* if the underlying topology is locally compact (i.e., every point of G has a precompact neighbornood) and Hausdorff. A *unitary representation* of G is a group homomorphism $\pi : G \to \mathcal{U}(\mathcal{H}_\pi)$ for some underlying Hilbert space $\mathcal{H}_\pi$ which is continuous with respect to the *strong operator topology*, i.e., $x \in G \mapsto \pi(x)\xi \in \mathcal{H}_\pi$ is continuous for every vector $\xi \in \mathcal{H}_\pi$. We further call the representation π *irreducible* if π has no nontrivial invariant subspaces, i.e., the only closed subspaces V of $\mathcal{H}_\pi$ satisfying $\pi(G)V \subset V$ are $\{0\}$ and $\mathcal{H}_\pi$. Note that if π is irreducible, so is the *contragredient representation* $\overline{\pi} : G \to \mathcal{U}(\mathcal{H})$ of π which is defined by $\overline{\pi}(x) = \overline{\pi(x)}$ for all $x \in G$ (for proper choice of orthonormal basis for $\mathcal{H}$). Moreover, two unitary representations $\pi_A : G \to \mathcal{U}(\mathcal{H}_A)$ and $\pi_B : G \to \mathcal{U}(\mathcal{H}_B)$ are called *(unitarily) equivalent* if there exists a unitary operator $U : \mathcal{H}_A \to \mathcal{H}_B$ such that $\pi_B(x) = U\pi_A(x)U^*$, and we denote by $\pi_A \cong \pi_B$ in this case. Let us denote by $\widehat{G}$ the set of equivalence classes of irreducible unitary representations of G.

Irreducible representations form basic building blocks of many functions and operators arising from G. Indeed, the *Gelfand-Raikov Theorem* [Fol16, Theorem 3.34] implies that every locally compact group has sufficiently many (mutually inequivalent) irreducible representations. Every unitary representation of G can be built out of irreducible ones via direct integration [Fol16, Theorem 7.28]. In particular, when G is abelian or compact, the action of irreducible representations play an essential role in the theory of *Fourier transform* on G.

In this section, we gather several preliminary tools from abstract harmonic analysis that will be beneficial for later applications in quantum information theory (QIT). We divide the tools into two parts: the abelian case and the compact case. Each part is for an application to each of two independent theories in QIT. For a more comprehensive understanding of the general theory of abstract harmonic analysis, we refer to [Fol16, HR79, HR70].

2.1.1 Locally compact abelian groups and Fourier analysis

In this subsection we provide preliminaries for Chapter 3 by reviewing the basics of harmonic analysis on locally compact *abelian* (LCA) groups. All LCA groups in this thesis are assumed second countable.

When G is abelian, every irreducible representation is 1-dimensional, i.e., a continuous group homomorphism from G into the *circle group* $\mathbb{T} = \mathcal{U}(1)$ [Fol16, Corollary 3.6]. In this case, $\widehat{G}$ becomes the set of such homomorphisms, and we call $\widehat{G}$ the *dual group* of G and its elements the *characters* on G. Indeed, the set $\widehat{G}$ is an abelian group with respect to pointwise multiplication, and is locally compact (and second countable) when equipped with the topology of compact convergence. The double dual of an LCA group can be canonically identified with the original group, i.e. we have

$$\widehat{(\widehat{G})} \cong G,$$

which is known as *Pontryagin-van Kampen duality*. Under this duality, properties of G manifest in a dual manner in $\widehat{G}$. For instance, an LCA group G is compact if and only if $\widehat{G}$ is discrete ([HR79, 23.17]).

For the most part, we use additive notation for LCA groups, so that the group operation will be denoted by $a + b$ for $a, b \in G$ and the identity of G will be denoted by 0. The inverse of $a \in G$ will be denoted by $-a$. However, we will sometimes use multiplicative notation for dual groups $\widehat{G}$. For example, the identity element for $\widehat{G}$ will be denoted by 1, meaning the constant function with value 1 and the inverse of $\gamma \in \widehat{G}$ will be denoted by γ^{-1} or $\bar{\gamma}$ (meaning complex conjugate). For $a \in G$ and $\gamma \in \widehat{G}$ the duality bracket

$$\langle a, \gamma \rangle := \gamma(a) \in \mathbb{C}$$

will be frequently used. Note that for $\gamma_1, \gamma_2 \in \widehat{G}$ and $a_1, a_2 \in G$ we have

$$\langle a_1 + a_2, \gamma_1 + \gamma_2 \rangle = \langle a_1 + a_2, \gamma_1 \rangle \langle a_1 + a_2, \gamma_2 \rangle = \gamma_1(a_1)\gamma_1(a_2)\gamma_2(a_1)\gamma_2(a_2).$$

Given a closed subgroup H of G (which we write $H \leq G$), the *quotient group* G/H is an LCA group endowed with the quotient topology. Its dual group $\widehat{G/H}$ can be identified with $H^\perp = \{\gamma \in \widehat{G} : \gamma(a) = 1, \ \ a \in H\}$, a closed subgroup of $\widehat{G}$ called the *annihilator* of H. The identification $H^\perp \cong \widehat{G/H}$ ([Fol16, Theorem 4.39]) is given by $\gamma \in H^\perp \mapsto \tilde{\gamma}$, where $\tilde{\gamma}(a + H) := \gamma(a)$, $a \in G$. Here, $a + H$ refers to the *coset* of H with the representative a. The quotient group $\widehat{G}/H^\perp$ can be identified with the dual group $\widehat{H}$ through the map $\gamma + H^\perp \in \widehat{G}/H^\perp \mapsto \gamma|_H \in \widehat{H}$ ([Fol16, Theorem 4.39]). Note that for $H \leq G$, the subgroup H is open if and only if G/H is discrete by definition of the quotient topology.

An LCA group G is equipped with a non-zero, translation-invariant Radon measure $\mu = \mu_G$, called the *Haar measure*, which is unique up to a positive constant. More precisely, for another non-zero, translation-invariant Radon measure on G we can find $c > 0$ such that $\nu = c \cdot \mu$. The choice of Haar measures will be specified later in this thesis. When the underlying group G

is clear from context, we simply write μ. Otherwise, we use the notation μ_G.

For a closed subgroup H of G the Haar measure provides interesting information about H as follows.

$$\textit{We have } 0 < \mu_G(H) < \infty \textit{ if and only if } H \textit{ is open and compact.} \tag{2.1.1}$$

One direction is trivial by local finiteness of μ and [Fol16, Proposition 2.19]. The converse direction follows from the fact that $\mu|_H$ becomes a finite Haar measure of H, so G/H has a G-invariant Radon measure $\overline{\mu}$ satisfying $\overline{\mu}(\{xH\}) = \mu(xH) \in (0, \infty)$, which implies discreteness of G/H by [DE14, Proposition 1.4.4].

The concepts of dual group and Haar measure lead to *Fourier transforms.* For $f \in L^1(G) := L^1(G, \mu)$ and $\gamma \in \widehat{G}$ we define

$$\hat{f}(\gamma) := \int_G f(x)\overline{\gamma(x)}\, d\mu(x),$$

and the *group Fourier transform* $\mathcal{F}_G$ is defined by

$$\mathcal{F}_G : L^1(G) \to C_0(\widehat{G}), \quad f \mapsto \hat{f}, \tag{2.1.2}$$

where $C_0(\widehat{G})$ refers to the space of all continuous functions on $\widehat{G}$ vanishing at infinity. The map $\mathcal{F}_G$ is a norm-decreasing homomorphism with respect to convolution on $L^1(G)$ and pointwise multiplication on $C_0(\widehat{G})$, i.e. we have

$$\mathcal{F}_G(f * g) = \mathcal{F}_G(f) \cdot \mathcal{F}_G(g), \quad f, g \in L^1(G),$$

where $f * g$ is the convolution of f and g given by

$$f * g(x) = \int_G f(y)g(x - y)d\mu(y), \quad x \in G.$$

We will sometimes use the notation $\widehat{f}^G$ instead of $\hat{f}$ when we need to specify which group we are referring to. Let us record the special case when $f = 1_K$

for a compact subgroup K of G:

$$\mathcal{F}_G(1_K) = \mu_G(K)1_{K^\perp}. \tag{2.1.3}$$

Indeed, we have

$$\gamma(y)\int_K \gamma(x)\,d\mu_G(x) = \int_K \gamma(x)\,d\mu_G(x), \forall y \in K$$

so that

$$\int_K \gamma(x)\,d\mu_G(x) = \begin{cases} \mu_G(K), & \gamma \in K^\perp \\ 0, & \text{otherwise} \end{cases}, \tag{2.1.4}$$

and this explains (2.1.3).

The above Fourier transform can be extended to the $L^2(G) = L^2(G,\mu)$-level. More precisely, there is a Haar measure $\mu_{\widehat{G}}$ on $\widehat{G}$ such that $\mathcal{F}_G : L^1(G) \cap L^2(G) \to L^2(\widehat{G})$ is isometric with respect to the corresponding L^2-norms. This map can be extended to a unitary (still denoted)

$$\mathcal{F}_G : L^2(G,\mu_G) \to L^2(\widehat{G},\mu_{\widehat{G}}),$$

by *Plancherel's theorem* [Fol16, Theorem 4.26]. Note that the choice of $\mu_{\widehat{G}}$ depends on μ_G, and we call it the *dual Haar measure* to μ_G. For example, if G is a compact group and if μ is the *normalized* Haar measure, i.e., $\mu(G) = 1$, then the dual Haar measure $\mu_{\widehat{G}}$ becomes the *counting measure* on the discrete group $\widehat{G}$.

The above $\mathcal{F}_G$ allows for an inverse map at the L^2-level, but we have a more direct inversion via the *Fourier inversion theorem* [Fol16, Theorem 4.33]: for $f \in L^1(G)$ such that $\hat{f} \in L^1(\widehat{G})$, we have

$$f(x) = \int_G \hat{f}(\gamma)\gamma(x)\,d\mu_{\widehat{G}}(\gamma), \quad \text{a.e. } x \in G. \tag{2.1.5}$$

If, in addition, f is continuous on G, then the above identity holds for all $x \in G$. When $f \in L^2(G)$ satisfies $\mathcal{F}_G(f) \in L^1(\widehat{G}) \cap L^2(\widehat{G})$, the function f

must be continuous and the above inversion formula also holds by [RS00, Theorem 4.4.13].

The space $L^1(G)$ embeds naturally into the Banach algebra $M(G)$ of all complex Radon measures on G via the map $f \mapsto f\,d\mu$. The Fourier transform extends to a contraction $\mathcal{F}_G : M(G) \to C_b(\widehat{G})$ satisfying

$$\mathcal{F}_G(\nu)(\gamma) = \hat{\nu}(\gamma) := \int_G \overline{\gamma(x)}\,d\mu(x), \quad \nu \in M(G),\ \gamma \in \widehat{G},$$

where $C_b(\widehat{G})$ is the space of bounded continuous functions on $\widehat{G}$. The homomorphism property still holds, i.e. for $\nu_1, \nu_2 \in M(G)$ we have

$$\mathcal{F}_G(\nu_1 * \nu_2) = \mathcal{F}_G(\nu_1) \cdot \mathcal{F}_G(\nu_2),$$

where the convolution $\nu_1 * \nu_2$ is determined by the following relation: for any compactly supported continuous function ϕ on G we have

$$\int_G \phi\, d(\nu_1 * \nu_2) = \int_G \int_G \phi(x)\, d\nu_1(x) d\nu_2(y).$$

We let $M^1(G)$ denote the set of all positive elements in $M(G)$ with total measure 1, namely the *(probability) distributions* on G. A theorem by Bochner [HR70, 33.3] says that the set $\mathcal{F}_G(M^1(G))$ coincides with the set of all continuous *positive definite* functions on $\widehat{G}$ having value 1 at the identity. Recall that a function $f : G \to \mathbb{C}$ is *positive definite* if the matrix $[f(x_i - x_j)]_{i,j=1}^n$ is positive semi-definite for any finite sequence $(x_i)_{i=1}^n \subseteq G$.

The *closed support* of $\nu \in M^1(G)$ (which we write $\overline{\operatorname{supp}}\,\nu$) is defined to be the smallest closed subset $A \subseteq G$ such that $\nu(A) = \nu(G)$. This definition needs to be distinguished with the *(open) support* of a continuous function f on G, which we write $\operatorname{supp} f$, defined by $\operatorname{supp} f = \{x \in G : f(x) \neq 0\}$. We say that $\nu \in M^1(G)$ is *concentrated* on a Borel subset $A \subseteq G$ if $\nu(B) = 0$ for any Borel $B \subseteq G$ such that $A \cap B = \varnothing$.

Proposition 2.1.1. *Let $f : G \to \mathbb{C}$ be a continuous positive definite function on an LCA group G.*

1. *We have* $|f(x)| \le f(0)$ *for any* $x \in G$.

2. *([HR70, Corollary 32.7]) The set* $G_1 := \{x \in G : |f(x)| = f(0)\}$ *is a closed subgroup of* G, $|f|$ *is constant on the cosets of* G_1 *and* $f/f(0)$ *is a character on* G_1.

Let us end this subsection by recalling a fundamental structure theorem of LCA groups due to van Kampen: *An LCA group* G *is isomorphic to* $\mathbb{R}^n \times F$ *(as topological groups) for some LCA group* F *containing a compact open subgroup [HR79, 24.30].*

2.1.2 Compact groups and invariant operators

In this subsection, we review the basics of unitary representations of *compact* (Hausdorff) groups. Moreover, we briefly describe a notion of *invariance* which will be one of the main concept in the method of compact group symmetry in QIT. These provide the preliminaries for Chapters 4 and 5.

Let us suppose that G is a compact group throughout this subsection. For a *unitary representation* $\pi : G \to \mathcal{U}(\mathcal{H})$ of G, a bounded linear operator $X \in B(\mathcal{H})$ is called π*-invariant* if $X\pi(x) = \pi(x)X$ for all $x \in G$ (we remark that this terminology is rather QIT-friendly: in mathematics, we call such X an *intertwining operator* for π). Let us denote by $\mathrm{Inv}(\pi)$ the set of all π-invariant operators. Then $\mathrm{Inv}(\pi) = \{\pi(x) : x \in G\}'$ is a *von Neumann algebra* on $\mathcal{H}$. Moreover, *Schur's theorem* [Fol16, Theorem 3.5] implies that π is irreducible if and only if $\mathrm{Inv}(\pi) = \mathbb{C}\, I_{\mathcal{H}}$.

When G is compact, it is simple to describe the space $\mathrm{Inv}(\pi)$. Indeed, every irreducible representation is finite-dimensional, and every unitary representation can be written as a direct sum of irreducible representations of G [Fol16, Theorem 5.2], that is,

$$\pi \cong \bigoplus_{[\sigma] \in \widehat{G}} \sigma \otimes I_{m_\sigma},$$

where m_σ is the multiplicity (possibly any cardinal) of the irreducible representation σ inside π. Then we can show that

$$\begin{aligned}\mathrm{Inv}(\pi) &\cong \left\{ \bigoplus_{[\sigma]\in\widehat{G}} \sigma(x) \otimes I_{m_\sigma} : x \in G \right\}' \\ &= \bigoplus_{[\sigma]\in\widehat{G}} I_{\mathcal{H}_\sigma} \otimes B(\ell_2(m_\sigma)).\end{aligned}$$

In particular, when π is finite-dimensional, then we can write $\pi \cong \bigoplus_{i=1}^{l} \sigma_i \otimes I_{m_i}$ for some mutually inequivalent irreducible representations $\sigma_1, \ldots, \sigma_l$ of G, $m_i < \infty$, and

$$\mathrm{Inv}(\pi) \cong \bigoplus_{i=1}^{l} I_{n_i} \otimes M_{m_i}, \tag{2.1.6}$$

where $n_i = \dim H_{\sigma_i}$. If $m_i = 1$ for all i, we call π *multiplicity-free.*

2.2 Quantum entanglement

In this section, we provide a concise overview of fundamental definitions related to quantum entanglement, a central concept in quantum information theory (QIT). Our focus is on finite-dimensional complex Hilbert spaces, namely $\mathcal{H} = \mathbb{C}^d$, $\mathcal{H}_A = \mathbb{C}^{d_A}$, $\mathcal{H}_B = \mathbb{C}^{d_B}$, as well as their direct sums and tensor products. The discussion of analogous notions for the infinite-dimensional case will be presented in Chapter 3. We refer to [NC00, Hol19, Wat18] for more details on quantum entanglement and other topics in QIT.

2.2.1 Separability and PPT property

A *quantum state* is a positive matrix $\rho \in B(H)_+$ with $\mathrm{Tr}(\rho) = 1$ and the set of all quantum states in $B(H)$ is denoted by $\mathcal{D}(H)$. A bipartite positive operator $X \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be of *positive partial transpose (PPT)* if

$$(\mathrm{id}_A \otimes \top_B)(X) \geq 0 \tag{2.2.1}$$

where $\top_B$ is the transpose map on $B(\mathcal{H}_B)$, and X is called *separable* if there exist families of positive operators $(X_i^A)_{i=1}^n \subset B(\mathcal{H}_A)_+$ and $(X_i^B)_{i=1}^n \subset B(\mathcal{H}_B)_+$ such that

$$X = \sum_{i=1}^n X_i^A \otimes X_i^B. \tag{2.2.2}$$

In particular, if $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a separable quantum state, then there exists a probability distribution $(p_i)_{i=1}^n$ and a family of product quantum states $(\rho_i^A \otimes \rho_i^B)_{i=1}^n$ such that

$$\rho = \sum_{i=1}^n p_i \rho_i^A \otimes \rho_i^B. \tag{2.2.3}$$

It is clear that separability implies PPT property, but the converse is not true in general. More precisely, all PPT quantum states in $B(\mathcal{H}_A \otimes \mathcal{H}_B)$ are separable if and only if $d_A{\cdot}d_B \leq 6$ [Per96, HHH96, Wor76a, Cho82]. Moreover, it is known that the separability question is NP-hard [Gur03, Gha10].

For $v \in H$, we define linear maps $|v\rangle : \mathbb{C} \to H$ given by $\lambda \mapsto \lambda v$ and $\langle v| : H \to \mathbb{C}$ given by $w \mapsto \langle v|w\rangle$ where $\langle v|w\rangle$ is the inner product of $v, w \in H$ whose first variable is the anti-linear part. In particular, $|\Omega\rangle = \sum_{i=1}^d \frac{1}{\sqrt{d}} |i\rangle \otimes |i\rangle \in H \otimes H$ is called the *maximally entangled Bell state* where $\{|1\rangle, |2\rangle, \cdots, |d\rangle\}$ is the standard orthonormal basis of H. The matrix unit $|i\rangle\langle j|$ and the product vector $|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_k\rangle$ are also denoted by e_{ij} and $|i_1 i_2 \cdots i_k\rangle$ respectively.

The *(normalized) Choi matrix* of a linear map $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is defined by

$$\begin{aligned} C_{\mathcal{L}} &= (\mathrm{id}_A \otimes \mathcal{L})(|\Omega_A\rangle\langle\Omega_A|) = (\mathrm{id}_A \otimes \mathcal{L}) \left(\frac{1}{d_A} \sum_{i,j=1}^{d_A} e_{ij} \otimes e_{ij} \right) \\ &= \frac{1}{d_A} \sum_{i,j=1}^{d_A} e_{ij} \otimes \mathcal{L}(e_{ij}) \in B(\mathcal{H}_A \otimes \mathcal{H}_B). \end{aligned} \tag{2.2.4}$$

Recall that $\mathcal{L}$ is *completely positive* (CP) if and only if the Choi matrix $C_{\mathcal{L}}$

is positive, and $\mathcal{L}$ is *trace-preserving* (TP) if and only if $(\mathrm{id}_A \otimes \mathrm{Tr}_B)(C_{\mathcal{L}}) = \frac{1}{d_A}\mathrm{id}_A$. In particular, if $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is a CPTP linear map, i.e. a *quantum channel* in the Schrödinger's picture, then the Choi matrix C_Φ is a quantum state in $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. We call this *channel-state duality*.

Let $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a linear map. Then $\mathcal{L}$ is called *completely copositive* (CCP) if $\top_B \circ \mathcal{L}$ is completely positive, $\mathcal{L}$ is called *decomposable* if there exist a CP map $\mathcal{L}_1$ and a CCP map $\mathcal{L}_2$ such that $\mathcal{L} = \mathcal{L}_1 + \mathcal{L}_2$, and $\mathcal{L}$ is called PPT if $\mathcal{L}$ is both CP and CCP. Thus, $\mathcal{L}$ is PPT if and only if $C_{\mathcal{L}}$ is PPT.

Another important property of quantum channels is the *entanglement-breaking (EB) property* [HSR03]. A quantum channel $\Phi : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is called EB if the Choi matrix C_Φ is a separable quantum state. Note that any EB quantum channel is PPT, but the converse is not true in general.

2.2.2 Schmidt number and positive maps

Let us now introduce some notions on Schmidt number and (k-)positive maps as dual objects. Every vector $\xi \in \mathcal{H}_A \otimes \mathcal{H}_B$ admits a Schmidt decomposition [NC00] $|\xi\rangle = \sum_{i=1}^k \lambda_i |v_i\rangle \otimes |w_i\rangle$ where $\lambda_1 \geq \cdots \geq \lambda_k > 0$, and $\{v_i\}_{i=1}^k$ and $\{w_i\}_{i=1}^k$ are orthonormal sets in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Here the numbers k and $\{\lambda_i\}_{i=1}^k$ are uniquely determined, and we call k the *Schmidt rank* of ξ and write $\mathrm{SR}(|\xi\rangle) = k$. Now we denote by $\mathbf{P}_{AB}$ the set of positive operators on $\mathcal{H}_A \otimes \mathcal{H}_B$ and consider the following subsets

$$\mathbf{Sch}_{k,AB} := \mathrm{conv}\,\{|\xi\rangle\langle\xi| : \mathrm{SR}(|\xi\rangle) \leq k\}$$

for any natural number k (or simply write $\mathbf{P}$ and $\mathbf{Sch}_k$ when these cause no confusion). Then the *Schmidt number* of a positive bipartite operator $X \in \mathbf{P}_{AB}$ is defined as the smallest natural number k such that $X \in \mathbf{Sch}_k$, and we write $\mathrm{SN}(X) = k$. Note that $\mathrm{SN}(X) \leq \min(d_A, d_B)$ and $\mathbf{Sch}_k = \mathbf{P}_{AB}$ whenever $k \geq \min(d_A, d_B)$. Moreover, $X \in P_{AB}$ is separable if and only if $\mathrm{SN}(X) = 1$.

Let us denote by $B(B(\mathcal{H}_A), B(\mathcal{H}_A))$ the set of all linear maps from $B(\mathcal{H}_A)$ into $B(\mathcal{H}_B)$ and by $B^h(B(\mathcal{H}_A), B(\mathcal{H}_B))$ the set of all *Hermitian preserving maps*, i.e., $\mathcal{L} \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$ with $\mathcal{L}(Z)^* = \mathcal{L}(Z^*)$ for $Z \in B(\mathcal{H}_A)$. We also denote by $\mathcal{POS}_{AB} \subset B^h(B(\mathcal{H}_A), B(\mathcal{H}_B))$ the cone of positive maps from $B(\mathcal{H}_A)$ into $B(\mathcal{H}_B)$. A list of subclasses of positive maps of our interest is the following:

- $\mathcal{POS}_{k,AB}$, the set of *k-positive* maps (note that $\mathcal{POS}_1 = \mathcal{POS}$),
- $\mathcal{CP}_{AB}$, the set of *completely positive (CP)* maps,
- $\mathcal{SP}_{k,AB} := \operatorname{conv}\{\mathrm{Ad}_K : K \in B(\mathcal{H}_B, \mathcal{H}_A), \operatorname{rank}(K) \le k\}$, the set of *k-superpositive* maps [SSrZ09], where $\mathrm{Ad}_K(X) := KXK^*$ is a conjugation map,
- $\mathcal{EB}_{AB} := \mathcal{SP}_1$, the set of *entanglement-breaking* (EB) maps.
- $\mathcal{DEC}_{AB} := \mathcal{CP}_{AB} + (\top_B \circ \mathcal{CP}_{AB})$, the set of *decomposable* maps.
- $\mathcal{PPT}_{AB} := \mathcal{CP}_{AB} \cap (\top_B \circ \mathcal{CP}_{AB})$, the set of *PPT* maps,

Note that we have two nested chains of the subclasses as follows.

$$\mathcal{POS} \supsetneq \mathcal{POS}_2 \supsetneq \cdots \supsetneq \mathcal{POS}_{\min(d_A,d_B)} = \mathcal{CP} = \mathcal{SP}_{\min(d_A,d_B)} \supsetneq \cdots \supsetneq \mathcal{SP}_2 \supsetneq \mathcal{EB}, \quad (2.2.5)$$

$$\mathcal{POS} \supset \mathcal{DEC} \supsetneq \mathcal{CP} \supsetneq \mathcal{PPT} \supset \mathcal{EB}. \quad (2.2.6)$$

Moreover, the two inclusions $\mathcal{POS} \supset \mathcal{DEC}$ and $\mathcal{PPT} \supset \mathcal{EB}$ is in general strict unless $(d_A, d_B) = (2,2), (2,3), (3,2)$ as noted in the previous subsection [Cho75b, Wor76b, HHH96, Hor97]. On the other hand, linear maps acting on quantum systems are often identified with bipartite operators via the so-called *Choi-Jamiołkowski correspondence* [Jk72, Cho75a]. For $\mathcal{L} \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$, the *(normalized) Choi matrix* $C_{\mathcal{L}} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is defined by

$$C_{\mathcal{L}} := (\mathrm{id}_A \otimes \mathcal{L})(|\Omega_A\rangle\langle\Omega_A|) = \frac{1}{d_A} \sum_{i,j=1}^{d_A} |i\rangle\langle j| \otimes \mathcal{L}(|i\rangle\langle j|),$$

where $|\Omega_A\rangle = \frac{1}{\sqrt{d_A}} \sum_{j=1}^{d_A} |jj\rangle \in \mathcal{H}_A \otimes \mathcal{H}_A$ is the maximally entangled vector state on the system A. Then it is known that [Cho75a, Sr82, HSR03, SSrZ09]

- $\mathcal{L}$ is Hermitian preserving if and only if $C_{\mathcal{L}}$ is Hermitian,
- $\mathcal{L}$ is k-positive if and only if $C_{\mathcal{L}} \in \mathbf{BP}_{k,AB}$, the set of *$k$-block positive* operators (that is, it satisfies $\langle \xi | C_\Phi | \xi \rangle \geq 0$ for all $\xi \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that $\mathrm{SR}(|\xi\rangle) \leq k$),
- $\mathcal{L}$ is CP if and only if $C_{\mathcal{L}} \in \mathbf{P}_{AB}$,
- $\mathcal{L}$ is k-superpositive if and only if $C_{\mathcal{L}} \in \mathbf{Sch}_{k,AB}$,
- $\mathcal{L}$ is EB if and only if $C_{\mathcal{L}} \in \mathbf{SEP}_{AB}$,
- $\mathcal{L}$ is decomposable if and only if $C_{\mathcal{L}} \in \mathbf{DEC}_{AB}$, the set of *decomposable* operators (that is, $C_{\mathcal{L}} = X_1 + (\mathrm{id}_A \otimes \top_B)(X_2)$ for some $X_1, X_2 \in \mathbf{P}_{AB}$),
- $\mathcal{L}$ is PPT if and only if $C_{\mathcal{L}} \in \mathbf{PPT}_{AB}$, the set of positive operators on $\mathcal{H}_A \otimes \mathcal{H}_B$ which are of *positive partial transpose (PPT)* (that is, both $C_{\mathcal{L}} \in \mathbf{P}_{AB}$ and $(\mathrm{id}_A \otimes \top_B)(C_{\mathcal{L}}) \in \mathbf{P}_{AB}$ hold).

The adjoint linear map $\mathcal{L}^* \in B(B(\mathcal{H}_B), B(\mathcal{H}_A))$ of $\mathcal{L} \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$ is defined with respect to the Hilbert-Schumidt inner product, i.e.,

$$\mathrm{Tr}(\mathcal{L}(Z)^* W) = \mathrm{Tr}(Z^* \mathcal{L}^*(W)), \quad Z, W \in B(\mathcal{H}_A).$$

Recall that the adjoint operation $\mathcal{L} \mapsto \mathcal{L}^*$ preserves all the properties mentioned above, i.e,. k-positivity, k-superpositivity, PPT, and decomposability.

We conclude this section by presenting two important criteria of entanglement and Schmidt numbers. The following Theorem implies that positive maps and k-positive maps can be regarded as entanglement witnesses and Schmidt number witnesses in QIT.

Theorem 2.2.1 ([HHH96, TH00]). *Let $X \in \mathbf{P}_{AB}$. Then*

1. $X \in \mathbf{SEP}$ *if and only if* $(\mathrm{id}_A \otimes \mathcal{L})(X) \geq 0$ *for all* $\mathcal{L} \in \mathcal{POS}_{AB}$,

2. $X \in \mathbf{Sch}_k$ *if and only if* $(\mathrm{id}_A \otimes \mathcal{L})(X) \geq 0$ *for all* $\mathcal{L} \in \mathcal{POS}_{k,AB}$.

These properties can be formulated in a generalized context using *mapping cones*, as detailed in Chapter 4.

Chapter 3

Gaussian states over general quantum kinematical systems

In the phase space formulation of quantum mechanics [Gro46, Moy49, Wey50, Wig32], states are represented through Wigner/characteristic functions on the underlying kinematical space, and observables are parametrized by the Weyl representation. Primary examples include systems of n-bosonic modes, n-qudit systems, and angle-number systems, with associated phase spaces $\mathbb{R}^{2n}$, $\mathbb{Z}_d^{2n}$ and $\mathbb{T}^n \times \mathbb{Z}^n$, respectively. For these systems, phase space methods underlie important concepts and techniques, such as bosonic Gaussian states and channels [WPGP$^+$12], sharp uncertainty principles [BKW18], finite-dimensional approximations of continuous systems [DVV94, Sch60], the stabilizer formalism of quantum error correction [CRSS98, Got97], and the construction of mutually unbiased bases [DEBZ10, GHW04, Par04]. Applications of phase space techniques continue to emerge in a variety of systems. In particular, the theory of p-adic quantum mechanics [VV89a] has seen a surge of recent activity in connection with the anti de Sitter/conformal field theory (AdS/CFT) correspondence (see e.g., [BHLL18, GKP$^+$17, HMSS18]).

Mathematically, quantum kinematical systems with finitely many degrees of freedom are described by a locally compact abelian (LCA) group G and a cocycle σ. The cocycle induces a symplectic structure on G, which encodes the canonical commutation relations of the associated (σ-projective) Weyl representation. Such abstract quantum kinematical systems have been studied from a variety of perspectives, including finite-dimensional approximations [DHV99], uncertainty relations [Wer16], and generalized metaplectic operators [Wei64]. In this chapter we continue this program by developing a formalism to study Gaussian states (and channels) for general quantum kinematical systems.

Bosonic Gaussian states are defined by the Gaussianity of their associated characteristic functions on the phase space $\mathbb{R}^{2n}$ (see, e.g., [WPGP$^+$12]). Using the natural notion of Gaussian distribution on LCA groups [PRRV63], one arrives at a sensible definition of a Gaussian state. However, in many cases of interest (e.g., G finite or totally disconnected), the corresponding class of states is trivial. To overcome this, we advocate the use of Gaussianity in the sense of Bernstein (or B-Gaussianity for short), which is an LCA generalization of Bernstein's classical result: a real probability distribution μ is Gaussian if and only if the sum and difference of two independent μ-distributed random variables are independent [Ber41]. Our notion of B-Gaussian states, valid for any phase space (G, σ), unifies a variety of examples from the literature, including bosonic Gaussian states, discrete Hudson/stabilizer states [Gro06], vacuum states of p-adic oscillator Hamiltonians [VV89b], (classes of) minimal uncertainty states [OP04], and the (relatively) recently introduced Gaussian states for single mode p-adic systems [Zel14, Zel20].

We completely characterize B-Gaussian states over 2-regular (second countable) LCA groups of the form $G = F \times \widehat{F}$ equipped with the canonical normalized 2-cocycle (see Section 3.1.2 for the cocycle). Here, 2-regularity means that the doubling map $g \mapsto 2g$ is an automorphism of G, and this case includes the systems of n-bosonic modes, n-qudit systems (for odd $d \geq 3$) and p-adic quantum systems. Thanks to van Kampen's structure theorem, the "configuration space" F is of the form $\mathbb{R}^n \times F_c$, where F_c admits a compact open subgroup, and the resulting phase space $G \cong \mathbb{R}^{2n} \times (F_c \times \widehat{F_c})$. Since the Euclidean case is well understood, we begin by focusing on the case where the phase space is $F_c \times \widehat{F_c}$. In this setting, we show that every B-Gaussian state is determined uniquely by a compact open 2-regular isotropic subgroup H of $F_c \times \widehat{F_c}$ and a character on H (Theorem 3.4.1). We also establish a correspondence between pure B-Gaussian states and symmetric bicharacters on compact open 2-regular subgroups K of F_c (Theorem 3.4.19), which complements the covariance matrix parametrization in the bosonic setting. As a consequence of our results when $F = F_c$, we show that, amongst B-Gaussian states over general configuration spaces $F = \mathbb{R}^n \times F_c$, there can be no entanglement across the associated tensor decomposition $L^2(F) = L^2(\mathbb{R}^n) \otimes L^2(F_c)$ of the system Hilbert space (Theorem 3.4.14). This completes the analysis for 2-regular Weyl systems $G = F \times \widehat{F}$.

In the non-2-regular setting, the structure of B-Gaussian states can be dramatically different. We show that B-Gaussian states over angle-number systems with the phase space $\mathbb{T}^n \times \mathbb{Z}^n$ are forced to be pure, and belong to the canonical "Fourier" basis of $L^2(\mathbb{T}^n)$. Over fermionic and hard-core bosonic systems, which have the same phase space $\mathbb{Z}_2^{2n}$ but with different 2-cocycles, we show that there are no B-Gaussian states.

The phase space formulation provides another important function on the phase space for a given quantum state, namely the Wigner function. Wigner functions, which are dual to characteristic functions, are always real-valued and integrate to 1 whenever they are integrable, so they are often called "pseudo-probability distributions". The natural question of non-negativity of Wigner functions was answered by Hudson for pure states in single-mode bosonic systems [Hud74], showing that pure states with non-negative Wigner function are precisely the pure Gaussian states. This was later generalized to multi-mode bosonic systems [SC83]. Gross continued this line of research, establishing a discrete Hudson's theorem for n-qudit systems with odd $d \geq 3$ [Gro06]. Our formalism allows one to define Wigner functions in full generality, which, in particular, begs the question of a generalized Hudson's theorem for 2-regular Weyl systems. We partially answer this question by showing that over totally disconnected 2-regular LCA groups of the form $G = F \times \widehat{F}$, a pure state has non-negative continuous Wigner function if and only if it is B-Gaussian.

We refer to Section 2.1.1 for preliminaries on duality and Fourier analysis in the context of locally compact abelian (LCA) groups.

3.1 Preliminaries on general quantum kinematical systems

3.1.1 Phase space structure

Let G be an LCA group equipped with a Borel function $\sigma : G \times G \to \mathbb{T}$ satisfying the conditions

$$\sigma(a,b)\sigma(a+b,c) = \sigma(a,b+c)\sigma(b,c),\ \sigma(a,0) = \sigma(0,b) = 1,\ \text{ a.e. } a,b,c \in G.$$

Note that the above equation holds for almost every $a, b, c \in G$ unless σ is continuous. However, we will often omit the expression "almost every" in the sequel for simplicity. The function σ is called a *2-cocycle* (or a *multiplier*) on G, and determines a *symplectic form* $\Delta : G \times G \to \mathbb{T}$ via

$$\Delta(a,b) := \sigma(a,b)\overline{\sigma(b,a)},\ a,b \in G. \tag{3.1.1}$$

Note that Δ is a *bicharacter*, meaning that Δ is continuous and $\Delta(\cdot, b)$ and $\Delta(a, \cdot)$ are characters on G for all $a, b \in G$ [DV04, p.533]. Note that Borel measurability of σ and Δ being Borel homomorphism in each argument guarantees that Δ is continuous [Mac58, p.281]. We require the map $\Phi_\Delta : G \to \widehat{G}$ given by

$$\Phi_\Delta(a)(b) = \Delta(a,b),\ a,b \in G \tag{3.1.2}$$

to be a topological group isomorphism, in which case we call the associated 2-cocycle σ a *Heisenberg multiplier* (following the terminology of [DV04]). The pair (G, σ) (or rather (G, Δ)) is viewed as the *phase space* underlying a *general quantum kinematical system* (see, e.g., [DV04]).

For example, the standard choice of 2-cocycle on the system of n-bosonic modes with the phase space $G = \mathbb{R}^{2n} \cong \mathbb{R}^n \times \mathbb{R}^n$ is given by

$$\sigma_{\mathrm{boson}}(a, b) = \exp\left(-\frac{i}{2}a^T Jb\right), \quad a, b \in G, \tag{3.1.3}$$

where $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in M_{2n}(\mathbb{R})$ is the matrix of the canonical symplectic form on $\mathbb{R}^{2n}$. Note also that the above map Φ_Δ is different from the usual identification $x \in \mathbb{R}^{2n} \mapsto \gamma_x \in \widehat{\mathbb{R}^{2n}}$ given by $\gamma_x(y) := e^{i\langle x,y\rangle}$, $y \in \mathbb{R}^{2n}$, which we call the *canonical identification*.

From the fact that $\Phi_\Delta(a)(a) = 1$ for any $a \in G$, the isomorphism Φ_Δ is called a *symplectic self-duality* for G [PSV10]. A typical example of an LCA group G with symplectic self-duality is $G = F \times \widehat{F}$ for another LCA group F, and this is exactly the class we will focus on. Note, however, that there exist LCA groups with symplectic self-duality not isomorphic to $F \times \widehat{F}$ for any LCA group F [PSV10, Theorem 11.2].

Since σ is a Heisenberg multiplier, there is a unique (up to unitary equivalence) irreducible unitary projective representation with respect to σ (or σ-representation) $W : G \to \mathcal{U}(\mathcal{H}_W)$ for some Hilbert space $\mathcal{H}_W$ [DV04, Theorem 2]. Being a σ-representation means that the map $a \in G \mapsto W(a)\psi$ is Borel for any $\psi \in \mathcal{H}_W$ and we have

$$W(a)W(b) = \sigma(a, b)W(a + b), \; a, b \in G. \tag{3.1.4}$$

Note that there are important examples of discontinuous 2-cocycles as we can see in Section 3.1.2.

We call W and $W(a)$, $a \in G$, the *Weyl representation* and the *Weyl operators* following the standard terminology. Note that the Weyl operators satisfy the *canonical commutation relations (CCR)*

$$W(a)W(b) = \Delta(a, b)W(b)W(a), \quad a, b \in G. \tag{3.1.5}$$

See [DV04, §3.5] for a concrete model of $\mathcal{H}_W$ and W.

A 2-cocycle σ on an LCA group G is *normalized* if $\sigma(a, -a) = 1$, $a \in G$. This additional requirement on σ is essential to accommodate "Gaussian states" as we can see in Remark 3.3.5(4) below. Fortunately, any 2-cocycle σ allows a *normalization* $\tilde{\sigma}$, which is similar to σ as 2-cocycles in the sense that there exists a Borel function $\xi : G \to \mathbb{T}$ (called a *normalizing factor*) so that

$$\tilde{\sigma}(a, b) = \frac{\xi(a)\xi(b)}{\xi(a+b)}\sigma(a, b), \quad a, b \in G, \tag{3.1.6}$$

defines a normalized 2-cocycle. In this case, the 2-cocycles σ and $\tilde{\sigma}$ determine the same symplectic form $\Delta(a, b) = \sigma(a, b)\overline{\sigma(b, a)} = \tilde{\sigma}(a, b)\overline{\tilde{\sigma}(b, a)}$, and therefore σ is a Heisenberg multiplier if and only if $\tilde{\sigma}$ is. Moreover, if W is an irreducible σ-representation of G acting on $\mathcal{H}_W$, then

$$W_{1/2}(a) := \xi(a)W(a)$$

is an irreducible $\tilde{\sigma}$-representation of G acting on the same Hilbert space $\mathcal{H}_W$. We will take ξ to be a Borel measurable *square root* of the function $a \in G \mapsto \overline{\sigma(a, -a)}$, hence the 1/2 in the notation $W_{1/2}$. Note that a choice of square root is always possible but not unique, in general. Thus, the choice of ξ and $\tilde{\sigma}$ will be specified whenever necessary.

3.1.2 Weyl systems

The main class of quantum kinematical systems we consider have the form $G = F \times \widehat{F}$ for an LCA group F. Such groups admit a *canonical* choice of 2-cocycle, $\sigma_{\text{can}} : G \times G \to \mathbb{T}$ given by

$$\sigma_{\text{can}}((x, \gamma), (x', \gamma')) := \gamma(x'), \; x, x' \in F, \; \gamma, \gamma' \in \widehat{F}. \tag{3.1.7}$$

It is straightforward to see that σ_{can} is a Heisenberg multiplier and we call the pair $(F \times \widehat{F}, \sigma_{\text{can}})$ a *Weyl system*. The group F is called the *configuration space*.

In this case we have a simple description for the unique irreducible σ_{can}-representation $W = W_{\text{can}}$ as follows [Pra11]. We first define the *translation operator* T_x and the *modulation operator* M_γ for $x \in F$ and $\gamma \in \widehat{F}$ acting on $\mathcal{H}_W := L^2(F)$ by

$$T_x f(y) := f(y-x), \;\; M_\gamma f(y) := \gamma(y) f(y), \; f \in L^2(F), \; y \in F.$$

Then, $W : G \to \mathcal{B}(L^2(F))$ is given by

$$W(x,\gamma) := T_x M_\gamma, \; (x,\gamma) \in G.$$

2-Regular groups

The above 2-cocycle σ_{can} is never normalized unless G is trivial. There is a canonical normalization when the group $G = F \times \widehat{F}$ (equivalently, F) is *2-regular*. Here, we say that the abelian group G is 2-regular if the map $a \mapsto 2a$ is an automorphism of G, and we denote its inverse by 2^{-1}. In this case, there is a unique bicharacter ξ such that $\xi(x,\gamma)^2 = \langle x, \gamma \rangle$ [DV04, Lemma 1], namely

$$\xi(x,\gamma) := \langle x,\gamma\rangle^{1/2} := \langle 2^{-1}x, 2^{-1}\gamma\rangle^2 = \langle x, 2^{-1}\gamma\rangle = \langle 2^{-1}x, \gamma\rangle.$$

With this ξ as the normalization factor, we get the *canonical normalization* $\tilde{\sigma}_{\text{can}}$ of σ_{can} given by

$$\tilde{\sigma}_{\text{can}}(a,b) := \Delta(2^{-1}a, 2^{-1}b)^2 = \Delta(a, 2^{-1}b) = \Delta(2^{-1}a, b), \; a,b \in G. \quad (3.1.8)$$

We sometimes write $\tilde{\sigma}_{\text{can}} = \Delta^{1/2}$ for an obvious reason, and we also call the pair $(F \times \widehat{F}, \tilde{\sigma}_{\text{can}})$ a *Weyl system*. Note finally that the corresponding Weyl representation $W_{1/2}$ becomes

$$W_{1/2}(x,\gamma)\psi(y) = \langle x,\gamma\rangle^{1/2} T_x M_\gamma \psi(y) = \langle x,\gamma\rangle^{-1/2}\langle y,\gamma\rangle\psi(y-x), \;\; \psi \in L^2(F).$$

Example 3.1.1. (Bosonic systems) The additive group $\mathbb{R}^n$ is 2-regular, and if we identify $\widehat{\mathbb{R}^n} \cong \mathbb{R}^n$ via $\langle x, \gamma_y \rangle := e^{i\langle x,y\rangle}$, $x, y \in \mathbb{R}^n$, then the formula (3.1.3) is recovered with $\sigma_{\text{boson}} = \tilde{\sigma}_{\text{can}}$. The corresponding symplectic form satisfies

$$\Delta(z, z') = e^{i\langle y,x'\rangle} e^{-i\langle y',x\rangle} = e^{i\langle Jz,z'\rangle}, \quad z = (x, y),\ z' = (x', y') \in \mathbb{R}^{2n},$$

where $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in M_{2n}(\mathbb{R})$ and $\langle \cdot, \cdot \rangle$ refers to the usual inner product on Euclidean spaces. The Weyl representation becomes

$$W_{1/2}(x, y)\psi(t) = e^{-\frac{i}{2}\langle x,y\rangle} e^{i\langle y,t\rangle} \psi(t - x),\ \ \psi \in L^2(\mathbb{R}^n),\ x, y \in \mathbb{R}^n.$$

This is equivalent to the Weyl representation used in [Hol19, §12.2] and [Fol16, §1.3], for example.

Example 3.1.2. (Qudit systems) If $d \geq 3$ is an odd integer then $\mathbb{Z}_d^n$ is a finite 2-regular abelian group. ($2^{-1} = \frac{d+1}{2}$ is the multiplicative inverse of 2 in the ring $\mathbb{Z}_d$.) Similar to above, we have the self-duality $\widehat{\mathbb{Z}_d^n} \cong \mathbb{Z}_d^n$ via

$$\gamma_y(x) = e^{\frac{2\pi i}{d}\langle x,y\rangle}, \quad x, y \in \mathbb{Z}_d^n. \tag{3.1.9}$$

Under the canonical identification

$$\ell^2(\mathbb{Z}_d^n) = \ell^2(\mathbb{Z}_d) \otimes \cdots \otimes \ell^2(\mathbb{Z}_d) \cong \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d,$$

the corresponding multiplication operators $M_y := M_{\gamma_y}$ satisfy

$$M_y = Z^{y_1} \otimes \cdots \otimes Z^{y_n}, \quad y = (y_1, ..., y_n) \in \mathbb{Z}_d^n,$$

where $Z : \mathbb{C}^d \ni |k\rangle \mapsto e^{\frac{2\pi i k}{d}}|k\rangle \in \mathbb{C}^d$ is the qudit generalization of the Pauli Z matrix.

Similarly, the translation operators are given by

$$T_x = X^{x_1} \otimes \cdots \otimes X^{x_n}, \quad x = (x_1, ..., x_n) \in \mathbb{Z}_d^n,$$

where $X : \mathbb{C}^d \ni |k\rangle \mapsto |k+1\rangle \in \mathbb{C}^d$ is the qudit generalization of the Pauli X matrix. The Weyl representation $W : \mathbb{Z}_d^n \times \mathbb{Z}_d^n \to \mathcal{B}((\mathbb{C}^d)^{\otimes n})$ is then simply

$$W(x, y) = e^{\frac{(d+1)\pi i}{d}\langle x,y\rangle} X^{x_1} Z^{y_1} \otimes \cdots \otimes X^{x_n} Z^{y_n}, \quad x, y \in \mathbb{Z}_d^n.$$

In this case the symplectic form satisfies

$$\Delta((x, y), (x', y')) = e^{\frac{2\pi i}{d}(\langle y,x'\rangle - \langle y',x\rangle)}, \quad x, y, x', y' \in \mathbb{Z}_d^n. \tag{3.1.10}$$

Example 3.1.3. (p-adic systems) If p is a prime, the field of p-adic numbers $\mathbf{Q}_p$ is a 2-regular totally disconnected abelian group, along with any finite product $\mathbf{Q}_p^n$. It is well-known that $\widehat{\mathbf{Q}_p} \cong \mathbf{Q}_p$ via the duality

$$\langle x, y\rangle = e^{2\pi i\{xy\}_p}, \quad x, y \in \mathbf{Q}_p,$$

where $\{x\}_p$ is the fractional part of x defined through the (unique) power series representation of x as follows:

$$\{x\}_p = \sum_{n=-k}^{-1} x_n p^n, \quad \text{when} \quad x = \sum_{n=-k}^{\infty} x_n p^n.$$

(see [Fol16, Theorem 4.12], for instance). The symplectic structure on $G = \mathbf{Q}_p^n \times \mathbf{Q}_p^n$ is given similarly as

$$\Delta((x, y), (x', y')) = \prod_{k=1}^{n} e^{2\pi i(\{y_k x'_k\}_p - \{y'_k x_k\}_p)}, \quad x, y, x', y' \in \mathbf{Q}_p^n.$$

Weyl systems over non-2-regular groups I: Angle-number systems

When the LCA group $G = F \times \widehat{F}$ is not 2-regular the canonical normalization (3.1.8) is no longer available. Instead, we will specify a normalization $\tilde{\sigma}_{\text{can}}$ of σ_{can} for each individual case.

We call the quantum system described by $(\mathbb{T}^d \times \mathbb{Z}^d, \tilde{\sigma}_{\text{can}})$ the *angle-number system in d-modes*, which we named after [Wer16, Table I]. Note that there are many physical quantum systems modelled through the angle-number system in 1-mode such as the quantum rotor [RKSE10] and the dynamics of a Josephson junction between two isolated islands [Gir14]. The case $d = 2$ for two rotors can be found in [ACP20, Sec IV. B.].

The canonical 2-cocycle becomes

$$\sigma_{\text{can}}((\theta, n), (\theta', n')) = e^{2\pi i \langle \theta', n \rangle}, \ \ (\theta, n) \in \mathbb{T}^d \times \mathbb{Z}^d.$$

Here, we identify $\mathbb{T} \cong \left[-\frac{1}{2}, \frac{1}{2}\right)$ and for $\theta = (\theta_1, \cdots, \theta_d) \in \mathbb{T}^d \cong \left[-\frac{1}{2}, \frac{1}{2}\right)^d$ and $n = (n_1, \cdots, n_d) \in \mathbb{Z}^d$ we have

$$\langle \theta, n \rangle := n_1\theta_1 + \cdots + n_d\theta_d \in \mathbb{R}. \tag{3.1.11}$$

Our choice of normalizing factor ξ is

$$\xi(\theta, n) = e^{\pi i \langle \theta, n \rangle}, \ (\theta, n) \in \mathbb{T}^d \times \mathbb{Z}^d \cong \left[-\frac{1}{2}, \frac{1}{2}\right)^d \times \mathbb{Z}^d. \tag{3.1.12}$$

Some care needs to be applied here since the identification $\mathbb{T} \cong \left[-\frac{1}{2}, \frac{1}{2}\right)$ does not respect the group structure of $\mathbb{T}$ and ξ is discontinuous at (θ, n) when $\theta_j = -\frac{1}{2}$ for some $1 \le j \le d$, so that the resulting normalization $\tilde{\sigma}_{\text{can}}$ is also discontinuous there.

In this case the associated Weyl representation $W_{1/2}$ becomes

$$W_{1/2}(\theta, n) := e^{\pi i \langle \theta, n \rangle} T_\theta M_n, \ \ (\theta, n) \in \mathbb{T}^d \times \mathbb{Z}^d,$$

which are operators acting on the Hilbert space $\mathcal{H} = L^2(\mathbb{T}^d) \cong \ell^2(\mathbb{Z}^d)$ with the canonical choice of orthonormal basis $\{|e_m\rangle : m \in \mathbb{Z}^d\}$, where $e_m(\theta) = e^{2\pi i \langle \theta, m \rangle}$, $\theta \in \mathbb{T}^d$. We will simply write $|m\rangle$ for $|e_m\rangle$.

3.1.3 Fermions and hardcore bosons

In this section we examine two quantum kinematic systems over the phase space $G = \mathbb{Z}_2^n \times \widehat{\mathbb{Z}_2^n} \cong \mathbb{Z}_2^n \times \mathbb{Z}_2^n = \mathbb{Z}_2^{2n}$.

Fermionic systems

Even though our phase space is of the form $F \times \widehat{F}$, we can endow a 2-cocycle which is not similar to the canonical one (when $n \geq 2$). More precisely, our choice of 2-cocycle is as follows.

$$\sigma_{\text{fer}}(a,b) := (-1)^{a^T A b},\ a,b \in \mathbb{Z}_2^{2n}, \tag{3.1.13}$$

where $A = \begin{bmatrix} 0 & & & & \\ 1 & 0 & & & \\ 1 & 1 & 0 & & \\ \vdots & \vdots & \ddots & \ddots & \\ 1 & 1 & \cdots & 1 & 0 \end{bmatrix}$. Note that the 1-mode case (i.e. $n = 1$) goes back to the canonical 2-cocycle on $\mathbb{Z}_2 \times \mathbb{Z}_2$. We can check that σ_{fer} is a Heisenberg multiplier by observing that $A + A^T$ is invertible. Indeed, we have $A + A^T = \begin{bmatrix} \Omega & E & E & \cdots & E \\ E & \Omega & E & \cdots & E \\ E & E & \Omega & \cdots & E \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ E & E & E & \cdots & \Omega \end{bmatrix}$, where $E = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $\Omega = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then the invertibility of $A + A^T$ is direct from the matrix identity $(I+A)(A+A^T)(I+A^T) = \bigoplus_{j=1}^n \Omega$, where we use the relations $\Omega E = E\Omega = E$ and $E^2 = 2E = 0$.

The quantum kinematical system $(\mathbb{Z}_2^n \times \widehat{\mathbb{Z}_2^n}, \sigma_{\text{fer}})$ describes a *fermionic system in n-modes*. For a detailed explanation, let us recall the *Majorana operators* $c_1, \ldots, c_{2n}$, which are self-adjoint operators acting on $\mathcal{H} = \mathbb{C}^{2^n} = \ell^2(\mathbb{Z}_2^n)$ satisfying the CAR (canonical anti-commutation relations):

$$\{c_j, c_k\} = 2\delta_{jk},\ 1 \leq j,k \leq 2n.$$

Note that c_j's are realized as

$$\begin{aligned} c_{2j-1} &= Y \otimes \cdots \otimes Y \otimes X \otimes I \otimes \cdots \otimes I \\ c_{2j} &= Y \otimes \cdots \otimes Y \otimes Z \otimes I \otimes \cdots \otimes I, \end{aligned}$$

where X and Z appear at the j-th tensor component and X, Y, Z are the 2×2 *Pauli matrices*. The unique irreducible unitary σ_{fer}-representation

$W_{\text{fer}} : \mathbb{Z}_2^{2n} \to \mathcal{U}(2^n)$ is given by

$$W_{\text{fer}}(a) := c_1^{x_1} \cdots c_{2n}^{x_{2n}}, \quad a = (x_1, \cdots, x_{2n}) \in \mathbb{Z}_2^{2n}. \tag{3.1.14}$$

That W_{fer} is a σ_{fer}-representation is straightforward to check. Irreducibility follows from the fact that $\{W_{\text{fer}}(a) : a \in \mathbb{Z}_2^{2n}\}$ forms an orthogonal basis of $M_{2^n}(\mathbb{C})$ with respect to the trace inner product.

We consider a normalization $\tilde{\sigma}_{\text{fer}}$ of σ_{fer} given by

$$\tilde{\sigma}_{\text{fer}}(a,b) := \frac{\xi(a)\xi(b)}{\xi(a+b)}\sigma_{\text{fer}}(a,b), \quad a,b \in \mathbb{Z}_2^{2n}, \tag{3.1.15}$$

where the normalizing factor $\xi : \mathbb{Z}_2^{2d} \to \mathbb{T}$ is chosen to satisfy

$$\xi(a)^2 = \xi(a)\xi(-a) = \tilde{\sigma}_{\text{fer}}(a,-a)\overline{\sigma_{\text{fer}}(a,-a)} = (-1)^{a^T A a}, \quad a \in \mathbb{Z}_2^{2n}.$$

Note that there are many choices for the factor ξ. We will not fix a particular choice of ξ for fermionic systems, but instead consider all possible choices of ξ (see Section 3.6).

Finally, we remark that the unique irreducible $\tilde{\sigma}_{\text{fer}}$-representation is

$$W_{1/2,\text{fer}} := \xi W_{\text{fer}}.$$

Hardcore bosons

Here we consider the canonical 2-cocycle σ_{can} (3.1.7) on $G = \mathbb{Z}_2^n \times \widehat{\mathbb{Z}_2^n} \cong \mathbb{Z}_2^{2n}$. As in the qudit case (Example 3.1.2), the associated Weyl operators have the following form:

$$W_{\text{can}}(x,y) = X^{x_1}Z^{y_1} \otimes \cdots \otimes X^{x_n}Z^{y_n} = h_1^{x_1}h_2^{y_1}h_3^{x_2}h_4^{y_2} \cdots h_{2n-1}^{x_n}h_{2n}^{y_n}, \tag{3.1.16}$$

where X, Z are the standard 2×2 Pauli matrices and the matrices h_j, $1 \leq j \leq 2n$ are given by

$$
\begin{aligned}
h_{2j-1} &= I \otimes \cdots \otimes I \otimes X \otimes I \otimes \cdots \otimes I \\
h_{2j} &= I \otimes \cdots \otimes I \otimes Z \otimes I \otimes \cdots \otimes I,
\end{aligned}
$$

where X and Z appear at the j-th tensor component for $1 \leq j \leq n$. The self-adjoint matrices h_j, $1 \leq j \leq 2n$ are an analogue of Majorana operators and they satisfy

$$h_k h_l = -h_l h_k, \ \ (k,l) = (2j-1, 2j) \text{ or } (2j, 2j-1), \ 1 \leq j \leq n$$

and $h_k h_l = h_l h_k$ for other choices (k,l). In other words, the observables h_j, $1 \leq j \leq 2n$ anti-commute in the same modes and commute for different modes, and the associated quantum system corresponds to *"hardcore bosons"* of n degrees of freedom [CL93, Section II].

To apply our program in this setting, we consider a normalization $\tilde{\sigma}_{\text{can}}$ of σ_{can} given by

$$\tilde{\sigma}_{\text{can}}(a,b) := \frac{\xi(a)\xi(b)}{\xi(a+b)} \sigma_{\text{can}}(a,b), \ \ a, b \in \mathbb{Z}_2^{2n}, \tag{3.1.17}$$

where the normalizing factor $\xi : \mathbb{Z}_2^{2n} \to \mathbb{T}$ is chosen to satisfy

$$\xi(a)^2 = \xi(a)\xi(-a) = \tilde{\sigma}_{\text{can}}(a,-a)\overline{\sigma_{\text{can}}(a,-a)} = (-1)^{a^T L a}, \ \ a \in \mathbb{Z}_2^{2n}, \ \ L := \begin{bmatrix} 0 & 0 \\ I_n & 0 \end{bmatrix}.$$

As in the fermionic system, we will not fix a particular choice for ξ, and the unique irreducible $\tilde{\sigma}_{\text{can}}$-representation is given by $W_{1/2,\text{can}} := \xi W_{\text{can}}$.

3.2 Characteristic and Wigner functions of quantum states

Throughout this and the next section we fix a general quantum kinematical system given by the pair (G, σ) consisting of a second countable LCA group G and a normalized 2-cocycle σ which is a Heisenberg multiplier.

Similar to the bosonic case (e.g. [Hol19, §12]) and certain qudit systems (e.g. [Gro06]), quantum states on $\mathcal{H} := \mathcal{H}_W$ – the irreducible representation space of W – can be recovered through their *characteristic functions* on the phase space G.

Recall that the set of all quantum states on $\mathcal{H}$ (denoted by $\mathcal{D} = \mathcal{D}(\mathcal{H})$) is a subset of $\mathcal{S}^1(\mathcal{H})$, the *trace class* on $\mathcal{H}$ equipped with the trace norm $\|X\|_1 = \mathrm{Tr}(|X|) = \mathrm{Tr}((X^*X)^{\frac{1}{2}})$, $X \in \mathcal{S}^1(\mathcal{H})$. Note that $\mathcal{S}^1(\mathcal{H})$ is a subspace of $\mathcal{S}^2(\mathcal{H})$, the *Hilbert-Schmidt class* on $\mathcal{H}$ equipped with the Hilbert-Schmidt norm $\|X\|_2 = (\mathrm{Tr}(X^*X))^{\frac{1}{2}}$, $X \in \mathcal{S}^2(\mathcal{H})$.

Definition 3.2.1. Let $\rho \in \mathcal{S}^1(\mathcal{H})$. Its *characteristic function* $\chi_\rho \in L^\infty(G)$ is defined by

$$\chi_\rho(a) = \mathrm{Tr}(W_{1/2}(a)^*\rho), \quad a \in G.$$

For a pure state $\rho = |\psi\rangle\langle\psi|$ with $\psi \in \mathcal{H}$, we will simply write χ_ψ instead of $\chi_{|\psi\rangle\langle\psi|}$.

It is straightforward that $\|\chi_\rho\|_\infty \leq \|\rho\|_1$, so χ_ρ is indeed bounded. The terminology "characteristic function" can be justified from the fact that χ_ρ determines the original operator ρ via the *twisted group Fourier transform* on G. See [KL72] and [Mac58] for details of twisted group Fourier transforms on locally compact (not necessarily abelian) groups. In our specific situation, namely that W is the only (up to unitary equivalence) σ-representation, the theory simplifies.

Definition 3.2.2. The *twisted group Fourier transform* $\mathcal{F}_G^\sigma$ on G is given by

$$\mathcal{F}_G^\sigma : L^1(G) \to \mathcal{B}(\mathcal{H}_W), \;\; f \mapsto \hat{f}(W_{1/2}) := \int_G f(a) W_{1/2}(a) d\mu(a) \in B(\mathcal{H}_W), \tag{3.2.1}$$

where the choice of Haar measure μ on G will be specified below in Theorem 3.2.3.

The map $\mathcal{F}_G^\sigma$ is a norm-decreasing $*$-homomorphism with respect to *twisted convolution* and *twisted involution*, defined respectively by

$$(f *_\sigma g)(a) := \int_G f(b) g(a-b) \sigma(b, a-b) d\mu(b), \; a \in G,$$

and

$$f^{\star\sigma}(a) := \overline{\sigma(a,-a) f(-a)}, \; a \in G,$$

for $f, g \in L^1(G)$. More precisely, we have $\mathcal{F}_G^\sigma(f *_\sigma g) = \mathcal{F}_G^\sigma(f) \cdot \mathcal{F}_G^\sigma(g)$ as the product (or composition) of two operators and $\mathcal{F}_G^\sigma(f^{\star\sigma}) = \mathcal{F}_G^\sigma(f)^*$ as the adjoint operator for $f, g \in L^1(G)$. It extends to a unitary operator acting on $L^2(G)$.

Theorem 3.2.3. *(***Twisted Plancherel theorem***, [KL72, Theorem 7.1]) The twisted group Fourier transform $\mathcal{F}_G^\sigma$ extends to a unitary equivalence between $L^2(G)$ and $\mathcal{S}^2(\mathcal{H}_W)$ for a suitable choice of Haar measure μ on G. In particular, we have*

$$\int_G f \bar{g} d\mu = \mathrm{Tr}(\hat{f}(W_{1/2}) \hat{g}(W_{1/2})^*), \;\; f, g \in L^1(G) \cap L^2(G). \tag{3.2.2}$$

Moreover, the extended map $\mathcal{F}_\sigma$ intertwines the left regular σ-representation *$\lambda_\sigma : G \to \mathcal{B}(L^2(G))$ given by*

$$\lambda_\sigma(a) f(b) = \sigma(a, b-a) f(b-a), \; a, b \in G, \; f \in L^2(G),$$

with an amplification of $W_{1/2}$. *More precisely, we have*

$$[\mathcal{F}_G^\sigma \circ \lambda_\sigma(a)](f) = W_{1/2}(a) \cdot [\mathcal{F}_G^\sigma(f)] : L^2(G) \to \mathcal{S}^2(\mathcal{H}_W), \ a \in G, \ f \in L^2(G). \tag{3.2.3}$$

In what follows, we fix the Haar measure μ on G respecting (3.2.2).

The following *twisted Fourier inversion* justifies the "characteristic function" terminology, and will be useful in Section 3.4.

Proposition 3.2.4. *For any* $\rho \in \mathcal{S}^1(\mathcal{H})$ *we have* $\chi_\rho \in L^2(G)$ *and* $\mathcal{F}_G^\sigma(\chi_\rho) = \rho$.

Proof. Since $\mathcal{F}_G^\sigma : L^2(G) \to \mathcal{S}^2(\mathcal{H})$ is unitary, $\mathrm{span}\{\mathcal{F}_G^\sigma(\varphi) : \varphi \in C_c(G)\}$ is dense in $S^2(\mathcal{H})$, where $C_c(G)$ is the space of all continuous functions on G whose closed support is compact. Consequently, $\mathrm{span}\{\mathcal{F}_G^\sigma(\varphi_1)\mathcal{F}_G^\sigma(\varphi_2)^* : \varphi_1, \varphi_2 \in C_c(G)\}$ is dense in $S^1(\mathcal{H})$.

First, for $\rho = \mathcal{F}_G^\sigma(\varphi_1)\mathcal{F}_G^\sigma(\varphi_2)^* = \mathcal{F}_G^\sigma(\varphi_1 *_\sigma \varphi_2^{\star\sigma})$ with $\varphi_1, \varphi_2 \in C_c(G)$, the intertwining relation (3.2.3) with λ_σ entails

$$\varphi_1 *_\sigma \varphi_2^{\star\sigma}(\cdot) = \langle \varphi_1 | \lambda_\sigma(\cdot)\varphi_2 \rangle = \mathrm{Tr}(W_{1/2}(\cdot)^* \mathcal{F}_G^\sigma(\varphi_1)\mathcal{F}_G^\sigma(\varphi_2)^*) = \chi_\rho(\cdot). \tag{3.2.4}$$

For arbitrary $\rho \in \mathcal{S}^1(\mathcal{H})$, there exist a sequence $(\rho_n)_n$ in the space

$$\mathrm{span}\{\mathcal{F}_G^\sigma(\varphi_1)\mathcal{F}_G^\sigma(\varphi_2)^* : \varphi_1, \varphi_2 \in C_c(G)\}$$

such that $\lim_{n\to\infty} \|\rho - \rho_n\|_{S^1(\mathcal{H})} = 0$. Since $\chi_{\rho_n} = (\mathcal{F}_G^\sigma)^{-1}(\rho_n)$ from (3.2.4), we have

$$\begin{aligned}\lim_{n\to\infty} \|(\mathcal{F}_G^\sigma)^{-1}(\rho) - \chi_{\rho_n}\|_{L^2(G)} &= \lim_{n\to\infty} \|(\mathcal{F}_G^\sigma)^{-1}(\rho) - (\mathcal{F}_G^\sigma)^{-1}(\rho_n)\|_{L^2(G)} \\ &\le \lim_{n\to\infty} \|\rho - \rho_n\|_{S^1(\mathcal{H})} = 0.\end{aligned}$$

In particular, the L^2-convergence of $(\chi_{\rho_n})_n$ to $(\mathcal{F}_G^\sigma)^{-1}(\rho)$ implies that a subsequence of $(\chi_{\rho_n})_n$ converges to $(\mathcal{F}_G^\sigma)^{-1}(\rho)$ almost everywhere. On the other hand, the condition $\lim_{n\to\infty} \|\rho - \rho_n\|_{S^1(\mathcal{H})} = 0$ implies $\lim_{n\to\infty} \|\chi_{\rho_n} - \chi_\rho\|_\infty = 0$. Thus, $\chi_\rho = (\mathcal{F}_G^\sigma)^{-1}(\rho) \in L^2(G)$. □

Remark 3.2.5.

1. For $f \in L^2(G)$, the element $\mathcal{F}_G^\sigma(f)$ is originally defined by the $\mathcal{S}^2(\mathcal{H})$-limit of $\mathcal{F}_G^\sigma(f_n) = \hat{f}_n(W_{1/2})$ for some sequence $(f_n) \subseteq L^1(G) \cap L^2(G)$ converging to f in $L^2(G)$. However, we may still express the element $\mathcal{F}_G^\sigma(f)$ via the integral representation $\int_G f(a)W_{1/2}(a)d\mu(a)$ once we understand it as a bounded operator on $\mathcal{H}$ given in the weak sense. Indeed, for any $\xi, \eta \in \mathcal{H}$ we have $\|\chi_{|\xi\rangle\langle\eta|}\|_{L^2(G)} = \||\xi\rangle\langle\eta|\|_{\mathcal{S}^2(\mathcal{H})} = \|\xi\| \cdot \|\eta\|$ by Proposition 3.2.4. Thus,

$$\begin{aligned} |\langle\eta| \int_G f(a)W_{1/2}(a)d\mu(a)|\xi\rangle| &= \left| \int_G f(a)\langle\eta|W_{1/2}(a)|\xi\rangle d\mu(a) \right| \\ &= \left| \int_G f(a)\chi_{|\xi\rangle\langle\eta|}(a)d\mu(a) \right| \\ &\leq \|f\|_{L^2(G)}\|\xi\| \cdot \|\eta\|. \end{aligned}$$

   This explains that the integral $\int_G f(a)W_{1/2}(a)d\mu(a)$ defines a bounded operator on $\mathcal{H}$ in the weak sense. The same computation also tells us that $\mathcal{F}_G^\sigma(f_n)$ converges to $\int_G f(a)W_{1/2}(a)d\mu(a)$ in the weak operator topology of $\mathcal{B}(\mathcal{H})$, which means that

$$\mathcal{F}_G^\sigma(f) = \int_G f(a)W_{1/2}(a)d\mu(a).$$

2. The set $G \times \mathbb{T}$ can be equipped with the "Heisenberg" group law $(x, z) \cdot (y, w) = (x + y, zw\sigma(x, y))$. We denote the resulting locally compact group by $G(\sigma)$, which is a *central extension* of G. The original version of [KL72, Theorem 7.1] (which applies to more general classes of groups) assumes that $G(\sigma)$ has a *type I* regular representation, which is the case for any abstract quantum kinematical system (G, σ). Indeed, the quotient space $G(\sigma)/G$ can easily be identified with the group $\mathbb{T}$, and

the canonical Haar measure on $\mathbb{T}$ is $G(\sigma)$-invariant as well. Thus, we can apply [Kal70, Theorem 1] to conclude that $G(\sigma)$ is type I.

In bosonic systems, one often considers another function on phase space associated to a quantum state ρ. It is called the Wigner function $\mathcal{W} = \mathcal{W}_\rho$, and is defined as the (symplectic) Fourier transform of the characteristic function χ_ρ. This can be done in the full generality. Using the current assumption that G is self-dual via the isomorphism Φ_Δ (3.1.2), we can transfer the group Fourier transform $\mathcal{F}_G$ from (2.1.2) to get the *"symplectic" group Fourier transform* on G

$$\mathcal{F}_G^{\mathrm{sym}} : L^1(G) \to C_0(G)$$

given by

$$\mathcal{F}_G^{\mathrm{sym}}(f)(a) := \int_G f(b)\overline{\Delta(a,b)}d\mu(b),\ a \in G,\ f \in L^1(G).$$

It follows from symplectic self-duality that there is (another) Haar measure μ_G^{sym} on G such that the map $\mathcal{F}_G^{\mathrm{sym}}$ extends to a unitary

$$\mathcal{F}_G^{\mathrm{sym}} : L^2(G,\mu) \to L^2(G,\mu_G^{\mathrm{sym}}). \tag{3.2.5}$$

We may call μ_G^{sym} the symplectic dual Haar measure of μ. We also have the corresponding Fourier inversion theorem as in (2.1.5).

Definition 3.2.6. The *Wigner function* $\mathcal{W}_\rho : G \to \mathbb{C}$ of $\rho \in \mathcal{S}^1(\mathcal{H})$ is defined by the symplectic Fourier transform of its characteristic function $\chi_\rho \in L^2(G)$, i.e. $\mathcal{W}_\rho := \mathcal{F}_G^{\mathrm{sym}}(\chi_\rho)$.

The Wigner function $\mathcal{W}_\rho$ encodes the state ρ in a dual manner to χ_ρ. One such aspect is the following.

Proposition 3.2.7. *For a quantum state $\rho \in \mathcal{D}(\mathcal{H})$ the Wigner function $\mathcal{W}_\rho$*

is always real-valued and if it is integrable, then we have

$$\int_G \mathcal{W}_\rho(a)\, d\mu_G^{\mathrm{sym}}(a) = 1. \tag{3.2.6}$$

Proof. The first conclusion follows from the fact that $W_{1/2}$ is involutive (as it is normalized): $\mathrm{Tr}(\rho W_{1/2}(-a)^*) = \mathrm{Tr}(\rho W_{1/2}(a)) = \overline{\mathrm{Tr}(\rho W_{1/2}(a)^*)}$, $a \in G$. When $\mathcal{W}_\rho \in L^2(G, \mu_G^{\mathrm{sym}})$ is also integrable, then the associated function χ_ρ must be continuous by [RS00, Theorem 4.4.13], so we can safely take evaluation χ_ρ. In particular, we see that $\chi_\rho(0) = 1$, so by Fourier inversion we have $\int_G \mathcal{W}_\rho(a) d\mu_G^{\mathrm{sym}}(a) = 1$. □

The above Proposition (which is well known for bosonic systems) is the reason why Wigner functions are called "pseudo-probability distributions". It is of interest to investigate the class of states whose Wigner functions are actual probability measures, equivalently, non-negative. We will focus on this theme in Section 3.7, but for now we record one useful property of characteristic/Wigner functions which follows directly from the CCR (3.1.5): for $\rho \in \mathcal{D}(\mathcal{H})$ we have

$$\chi_{W_{1/2}(z)^*\rho W_{1/2}(z)}(w) = \overline{\Delta(z,w)}\chi_\rho(w), \quad w, z \in G \tag{3.2.7}$$

$$\mathcal{W}_{W_{1/2}(z)^*\rho W_{1/2}(z)}(w) = \mathcal{W}_\rho(w+z), \quad w, z \in G. \tag{3.2.8}$$

Remark 3.2.8.

1. The above Wigner function exhibits similar properties to bosonic Wigner functions, but we will postpone collecting such properties until the follow-up paper [PJLY23].
2. Our Wigner functions coincide with the ones from [Muk79], [RSSK$^+$10] and [Gro06].

3.3 Gaussian states in general quantum kinematical systems

We first recall some necessary background on Gaussian distributions over second countable LCA groups G, and refer the reader to [Fel08] for details.

Definition 3.3.1. A distribution ν on G is called

- *Gaussian* if its Fourier transform $\hat{\nu}$ on $\widehat{G}$ is of the form

$$\hat{\nu}(\gamma) = \langle \gamma, x \rangle \exp(-\varphi(\gamma)), \quad \gamma \in \widehat{G}, \tag{3.3.1}$$

  for some $x \in G$ and some non-negative continuous $\varphi : \widehat{G} \to \mathbb{R}$ satisfying

$$\varphi(\gamma + \gamma') + \varphi(\gamma - \gamma') = 2(\varphi(\gamma) + \varphi(\gamma')), \quad \gamma, \gamma' \in \widehat{G}. \tag{3.3.2}$$

- *Gaussian in the sense of Bernstein*, or simply *B-Gaussian* if

$$\hat{\nu}(\gamma + \gamma')\hat{\nu}(\gamma - \gamma') = \hat{\nu}(\gamma)^2 |\hat{\nu}(\gamma')|^2, \quad \gamma, \gamma' \in \widehat{G}. \tag{3.3.3}$$

Remark 3.3.2.

1. Gaussian distributions on LCA groups were first studied by Parthasarathy, Rao, and Varadhan [PRRV63] as a generalization of Gaussian distributions on $\mathbb{R}^n$. This concept has been further generalized to B-Gaussian distributions by Rukhin [Ruk69] and by Heyer and Rall [HR72] through analogues of the Kac-Bernstein theorem on LCA groups. Note that if the group G contains a closed subgroup homeomorphic to $\mathbb{T}^2$, then we can always find a B-Gaussian distribution on G which is not Gaussian [Fel08, Lemma 9.6].

2. Any non-negative continuous function $\varphi : \widehat{G} \to \mathbb{R}$ satisfying (3.3.2) is of the form

$$\varphi(\gamma) = \psi(\gamma, \gamma), \ \gamma \in \widehat{G},$$

where $\psi : \widehat{G} \times \widehat{G} \to \mathbb{R}$ is a continuous function satisfying

- $\psi(\gamma_1, \gamma_2) = \psi(\gamma_2, \gamma_1)$,
- $\psi(\gamma_1 + \gamma_2, \gamma_3) = \psi(\gamma_1, \gamma_3) + \psi(\gamma_2, \gamma_3)$,
- $\psi(\gamma_1, \gamma_1) \geq 0$

for any $\gamma_1, \gamma_2, \gamma_3 \in \widehat{G}$. In particular, $\psi \in \mathrm{Hom}(\widehat{G}, \mathrm{Hom}(\widehat{G}, \mathbb{R}))$.

3. From the definition we can easily see that the Fourier transform of a Gaussian distribution ν on G is fully supported, i.e. $\mathrm{supp}\, \nu = \widehat{G}\,\cdot$

We collect some properties of B-Gaussian distributions which will be useful throughout this chapter. An LCA group K is called a *Corwin group* if $2K := \{2k : k \in K\} = K$, i.e., the doubling map is surjective.

Proposition 3.3.3. *Let ν be a B-Gaussian distribution on G and*

$$H = \mathrm{supp}\, \hat{\nu} = \left\{ \gamma \in \widehat{G} : \hat{\nu}(\gamma) \neq 0 \right\}.$$

1. *The set H is an open subgroup of $\widehat{G}$, whose annihilator $H^{\perp}$ is a compact Corwin subgroup of G.*

2. *Suppose that G has no subgroup isomorphic to $\mathbb{T}^2$ and $H = \widehat{G}$. Then ν is a Gaussian distribution on G.*

3. *If G_e, the connected component of the identity of G, contains at most one element of order 2, then $\nu = \nu_0 * (1_K/\mu(K))$ for a compact Corwin subgroup K of G and a Gaussian distribution ν_0 on G. The mentioned hypothesis on G is satisfied when G is discrete or 2-regular.*

Proof. (1) Openess of H is clear, and H being a subgroup is direct from (3.3.3). Moreover, the quotient group $\widehat{G}/H$ is discrete, so that $H^{\perp} \cong \widehat{\widehat{G}/H}$ is compact. For the Corwin property of $H^{\perp}$, it suffices to check that $2\gamma \in H$ implies that $\gamma \in H$ by [Fel08, Lemma 7.2]. But this is also direct from (3.3.3).

(2)&(3) These are [Fel08, Lemma 9.7, Theorem 9.9]. □

We are now ready to define Gaussian states over general kinematic systems.

Definition 3.3.4. A state $\rho \in \mathcal{D}(\mathcal{H})$ is *Gaussian* (resp. *B-Gaussian*) if there is a Gaussian (resp. B-Gaussian) distribution ν on $\widehat{G}$ such that $\chi_\rho = \mathcal{F}_{\widehat{G}}(\nu)$.

Remark 3.3.5.

1. Note that Definition 3.3.4 requires χ_ρ to be the Fourier transform of a (B-)Gaussian distribution on $\widehat{G}$ instead of a (B-)Gaussian distribution on G. This difference does not show up in the bosonic system since the class of Gaussian distributions on $\mathbb{R}^n$ are preserved by Fourier transform.

2. Conjugation with respect to a Weyl operator preserves (B-)gaussian states. More precisely, (3.2.7) tells us that for any $a \in G$ the state $W_{1/2}(a)^* \rho W_{1/2}(a)$ is Gaussian (resp. B-Gaussian) whenever ρ is.

3. Every Gaussian state is clearly a B-Gaussian state. However, the class of all B-Gaussian states is strictly larger than that of all Gaussian states in general. See Example 3.3.6/3.3.7, Theorem 3.4.1, Corollary 3.4.9 and Proposition 3.4.18 below for such cases.

4. In order to secure the existence of B-Gaussian states we need to focus on normalized 2-cocycles. Indeed, suppose $\rho \in \mathcal{D}(\mathcal{H})$ is a B-Gaussian state with respect to the σ-representation W where σ is a general 2-cocycle σ on G. The positivity of ρ says that

$$\chi_\rho(a) = \chi_{\rho^*}(a) = \overline{\sigma(a,-a)}\,\mathrm{Tr}(\rho^* W(-a)) = \overline{\sigma(a,-a)}\;\overline{\chi_\rho(-a)}.$$

Being a Fourier transform of a distribution, we have $\chi_\rho(a) = \overline{\chi_\rho(-a)}, a \in G$. Therefore, we have $\sigma(a,-a) = 1$ whenever $\chi_\rho(a) \neq 0$, i.e. on the support of χ_ρ, which is an open subgroup of G and non trivial in many cases. This is one reason why we require our quantum kinematical system to be equipped with normalized 2-cocycles.

For bosonic systems, Gaussianity and B-Gaussianity coincide with the usual notion of bosonic Gaussian states (see, e.g., [Hol19, §12.3.2]) by the multivariate Kac-Bernstein theorem. See [Fel08] for more details, generalizations, and further references. We now present some examples of B-Gaussian states which were already well-known in the literature under different names. To see this, first recall that for a closed subgroup $H \leq G$, its *symplectic complement* is defined by

$$H^{\Delta} := \{z \in G \mid \Delta(z, h) = 1 \mathcal{F}orall\ h \in H\}.$$

We say that H is *isotropic* (respectively, *maximally isotropic or Lagrangian*) if $H \subseteq H^{\Delta}$ (respectively, $H = H^{\Delta}$).

Example 3.3.6. (Discrete stabilizer states) Let $d \geq 3$ be an odd integer, and consider the Weyl system $(\mathbb{Z}_d^n \times \mathbb{Z}_d^n, \tilde{\sigma}_{\text{can}})$. For a maximally isotropic subgroup H of $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ and $v \in \mathbb{Z}_d^n \times \mathbb{Z}_d^n$ the associated *stabilizer state* (see, e.g., [Gro06, HDDM05]) $|H, v\rangle\langle H, v|$ is the rank-1 projection

$$|H, v\rangle\langle H, v| = \frac{1}{|H|} \sum_{h \in H} \Delta(v, h) W_{1/2}(h) = \frac{1}{d^n} \sum_{h \in H} \Delta(v, h) W_{1/2}(h). \qquad (3.3.4)$$

Indeed, the projection $|H, v\rangle\langle H, v|$ is the unique state stabilized by the abelian group $\left\{\Delta(v, h) W_{1/2}(h) : h \in H\right\}$ [Gro06, Lemma 8], that is,

$$\Delta(v, h) W_{1/2}(h) |H, v\rangle = |H, v\rangle, \quad h \in H.$$

As shown in the proof of [Gro06, Lemma 9], its characteristic function $\chi_{H,v} := \chi_{|H,v\rangle\langle H,v|}$ is of the form

$$\chi_{H,v}(z) = \Delta(v, z) 1_H(z), \ z \in \mathbb{Z}_d^n \times \mathbb{Z}_d^n,$$

where 1_H is the indicator function of H (albeit with a different normalization from [Gro06]). Self-duality of finite abelian groups tells us that there is $v_0 \in \mathbb{Z}_d^n \times \mathbb{Z}_d^n$ such that $\Delta(v, \cdot) = \langle v_0, \cdot \rangle$. Hence, $\chi_{H,v}$ is the Fourier transform of

$\nu = \delta_{v_0} * (\frac{1}{|H^\perp|} 1_{H^\perp})$. Now we check the condition (3.3.3). The character $\Delta(v, \cdot)$ clearly satisfies (3.3.3). Finiteness and 2-regularity of the group $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ imply that H is also 2-regular, and consequently 1_H satisfies (3.3.3). This means that the stabilizer state $|H, z\rangle\langle H, z|$ is a pure B-Gaussian state. Note that H is a non-trivial proper subgroup of $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ since $|H| = d^n$ and the Fourier transform of Gaussian distributions always have full support. Thus, we know that $|H, z\rangle\langle H, z|$ is not a Gaussian state.

Later we will show that pure B-Gaussian states in the n-qudit system are precisely the stabilizer states $|H, v\rangle\langle H, v|$ for some $v \in \mathbb{Z}_d^{2n}$ and some maximally isotropic subgroup $H \leq \mathbb{Z}_d^{2n}$, and that there are no Gaussian states (even mixed ones) over the Weyl system $(\mathbb{Z}_d^n \times \mathbb{Z}_d^n, \tilde{\sigma}_{\text{can}})$. (See Theorem 3.4.1, Corollary 3.4.9, Proposition 3.4.18, and Example 3.4.11.) Hence, the Gaussian character of qudit stabilizer states (which belongs to the folklore) is made explicit through the Bernstein identity (4.2) of their characteristic functions.

Example 3.3.7. (Minimum uncertainty states) Consider the Weyl system $(G = F \times \widehat{F}, \tilde{\sigma}_{\text{can}})$ over a 2-regular LCA group G such that F contains a compact open 2-regular subgroup K. Fix $z_0 \in G$. Then

$$\psi = \mu_F(K)^{-1/2} W_{1/2}(z_0) 1_K \in L^2(F)$$

is a minimum uncertainty state in the sense that it saturates the entropic uncertainty relation from [OP04, Theorem 1.5]. The characteristic function $\chi_\psi := \chi_{|\psi\rangle\langle\psi|}$ of $|\psi\rangle\langle\psi|$ then satisfies (by (3.2.7))

$$\chi_\psi(z) = \mu_F^{-1}(K)\Delta(z_0, z)\chi_{|1_K\rangle\langle 1_K|}(z) = \mu_F^{-1}(K)\Delta(z_0, z)\overline{\langle W_{1/2}(z) 1_K, 1_K\rangle}, \quad z \in G.$$

Note that for $y \in K$, $y-x \in K$ if and only if $x \in K$. Hence, for $z = (x, \gamma) \in G$

$$\begin{aligned} \langle W_{1/2}(z)1_K, 1_K \rangle &= \int_G \langle x, \gamma \rangle^{-1/2} \langle y, \gamma \rangle 1_K(y-x) \overline{1_K(y)} d\mu(y) \\ &= 1_K(x) \int_K \langle x, \gamma \rangle^{-1/2} \langle y, \gamma \rangle d\mu(y) \\ &= \mu_F(K) 1_K(x) \langle x, \gamma \rangle^{-1/2} 1_{K^\perp}(\gamma) \end{aligned}$$

By 2-regularity of K, $2^{-1}K = K$. Thus, for $x \in K$ and $\gamma \in K^\perp$

$$\langle x, \gamma \rangle^{-1/2} = \overline{\langle 2^{-1}x, 2^{-1}\gamma \rangle^2} = \overline{\langle 2^{-1}x, \gamma \rangle} = 1,$$

and consequently

$$\chi_\psi(z) = \Delta(z_0, z) 1_{K \times K^\perp}(z),\ z \in G.$$

Similar to the previous example we see that $|\psi\rangle\langle\psi|$ is a pure B-gaussian state. On the other hand, since $K \times K^\perp$ is never equal to the whole phase space $G = F \times \widehat{F}$, $|\psi\rangle\langle\psi|$ is not a Gaussian state as before. The full description of pure B-Gaussian states in this setting will be given in Theorem 3.4.19.

3.4 Weyl systems over 2-regular groups

In this section we focus on the Weyl system $(G = F \times \widehat{F}, \tilde{\sigma}_{\text{can}})$ over a 2-regular LCA group and provide a complete characterization of B-Gaussian states. By the structure theorem of van Kampen, we know that $F \cong \mathbb{R}^n \times F_c$ for some LCA group F_c admitting a compact open subgroup [HR79, 24.30]. So we have $G \cong \mathbb{R}^{2n} \times (F_c \times \widehat{F_c})$. Let us write $G_c = F_c \times \widehat{F_c}$ for later use.

Our strategy is to first characteize B-Gaussian states on the Weyl system $(G_c, \tilde{\sigma}_{\text{can}})$ and then use our result to show that, amongst B-Gaussian states over $G = \mathbb{R}^{2n} \times G_c$, there can be no bipartite entanglement between the subsystems $\mathbb{R}^{2n}$ and G_c. The full characterization then follows naturally.

3.4.1 Systems admitting compact open subgroups

The main goal of this section is to establish the following theorem.

Theorem 3.4.1. *For a state $\rho \in \mathcal{D}(L^2(F_c))$, the following are equivalent:*

1. *ρ is a B-Gaussian state on the Weyl system $(G_c, \tilde{\sigma}_{\text{can}})$;*
2. *there exist a compact open 2-regular isotropic subgroup $H \leq G_c$ and a character $\gamma \in \widehat{H}$ such that*

$$\rho = \rho_{H,\gamma} := \int_H \gamma(z) W_{1/2}(z) d\mu_{G_c}(z). \tag{3.4.1}$$

Moreover, H and γ are uniquely determined.

Let us first focus on the easier direction (2) $\Rightarrow$ (1). The main step in the proof is Proposition 3.4.4, which requires a few preparatory lemmas. For notational simplicity we write $\sigma = \tilde{\sigma}_{\text{can}} = \Delta^{1/2}$ from (3.1.8).

Lemma 3.4.2. *Let H be a compact open 2-regular subgroup of G_c.*

1. *For $z \in G$ we have $z \in H^\Delta$ if and only if $\sigma(z, h) = 1$ for all $h \in H$.*
2. *For $z \in G$, $\displaystyle\int_H \sigma(z, z') d\mu_{G_c}(z') = \begin{cases} \mu(H), & z \in H^\Delta \\ 0, & \text{otherwise} \end{cases}$.*

Proof. (1) If $z \in H^\Delta$, then for all $h \in H$

$$\sigma(z, h) = \Delta^{1/2}(z, h) = \Delta(2^{-1}z, 2^{-1}h)^2 = \Delta(z, 2^{-1}h) = 1$$

as $2^{-1}H \subseteq H$. Conversely, if $\sigma(z, h) = 1$ for all $h \in H$ then again by definition of the normalization

$$\Delta(z, h) = \Delta(2^{-1}z, 2^{-1}(2h))^2 = \sigma(z, 2h) = 1, \quad h \in H.$$

(2) This is from (1) and (2.1.4). ∎

Lemma 3.4.3. *Let H be a compact open subgroup of G_c. Then H^Δ is a compact open subgroup of G_c. Morever, if H is 2-regular then so is H^Δ.*

Proof. Since H is open, the quotient G_c/H is discrete, so that $H^\perp \cong \widehat{G_c/H}$ is compact. Since H is compact, the dual $\widehat{H}$ is discrete, so that $H^\perp$ is open from $\widehat{G_c}/H^\perp \cong \widehat{H}$. Thus, $H^\perp$ is a compact open subgroup of $\widehat{G_c}$. But $H^\perp = \Phi_\Delta(H^\Delta)$ via the isomorphism $\Phi_\Delta : G_c \to \widehat{G_c}$, implying that H^Δ is compact open in G_c.

For the final statement, let $z \in H^\Delta$. Then for all $h \in H$,

$$\Delta(2^{-1}z, h) = \Delta(2^{-1}z, 2^{-1}h)^2 = \sigma(z, h),$$

so the result follows from Lemma 3.4.2 (1). □

Proposition 3.4.4. *The element $\rho_{H,\gamma}$ from* (3.4.1) *is a self-adjoint operator satisfying the relation $\rho_{H,\gamma}^2 = \mu_{G_c}(H)\rho_{H\cap H^\Delta,\gamma}$.*

Proof. Self-adjointness comes from $W_{1/2}(z)^* = W_{1/2}(-z)$, $\overline{\gamma(z)} = \gamma(-z)$. Since the above integral (3.4.1) is WOT-convergent, and multiplication is separately WOT-continuous, we have

$$\begin{aligned}
\rho_{H,\gamma}^2 &= \int_H \int_H \gamma(z)\gamma(z')W_{1/2}(z)W_{1/2}(z')d\mu_{G_c}(z)d\mu_{G_c}(z') \\
&= \int_H \int_H \gamma(z+z')\sigma(z,z')W_{1/2}(z+z')d\mu_{G_c}(z)d\mu_{G_c}(z') \\
&= \int_H \int_H \gamma(z')\sigma(z,z'-z)W_{1/2}(z')d\mu_{G_c}(z)d\mu_{G_c}(z') \\
&= \int_H \int_H \gamma(z')\sigma(z,z')W_{1/2}(z')d\mu_{G_c}(z)d\mu_{G_c}(z') \\
&= \int_H \gamma(z')\Big(\int_H \sigma(z,z')d\mu_{G_c}(z)\Big)W_{1/2}(z')d\mu_{G_c}(z') \\
&= \mu_{G_c}(H)\int_{H\cap H^\Delta} \gamma(z')W_{1/2}(z')d\mu_{G_c}(z') \\
&= \mu_{G_c}(H)\rho_{H\cap H^\Delta,\gamma},
\end{aligned}$$

where the second last equality is Lemma 3.4.2 (2). Note that $H \cap H^\Delta$ is again a compact open 2-regular subgroup by Lemma 3.4.3, so the notation $\rho_{H\cap H^\Delta,\gamma}$ is justified. □

Proof of Theorem 3.4.1. (2) $\Rightarrow$ (1): Since H is isotropic, $H = H \cap H^\Delta$, so Proposition 3.4.4 implies $\rho_{H,\gamma}^2 = \mu_{G_c}(H)\rho_{H,\gamma}$. By the spectral theorem for compact operators, $\rho_{H,\gamma}$ is positive with $\mathrm{spec}(\rho_{H,\gamma}) = \{0, \mu_{G_c}(H)\}$. Moreover, as $\rho_{H,\gamma} = \mathcal{F}^\sigma_{G_c}(\gamma 1_H)$, by Lemma 3.2.4 and injectivity of $\mathcal{F}^\sigma_{G_c}$, we have $\chi_\rho = \gamma 1_H$. In particular, $\mathrm{Tr}(\rho_{H,\gamma}) = \chi_\rho(0) = 1$, so $\rho_{H,\gamma}$ is a state. Its characteristic function satisfies the Bernstein identity (3.3.3):

$$\begin{aligned}\chi_\rho(z+z')\chi_\rho(z-z') &= \gamma(z+z')\gamma(z-z')1_H(z+z')1_H(z-z')\\ &= \gamma(z)^2|\gamma(z')|^2 1_H(z)1_H(z'),\end{aligned}$$

where the last equality uses 2-regularity of H to show $z+z', z-z' \in H$ if and only if $z, z' \in H$. On the other hand, $\chi_\rho = \gamma 1_H$ is continuous and positive definite since $\gamma \in \widehat{H}$ and H is a compact open subgroup [Wei40, Pow40, Rai40]. Consequently, χ_ρ is the Fourier transform of a B-Gaussian distribution, and thus $\rho_{H,\gamma}$ is a B-Gaussian state. □

The other, more involved direction of the proof of Theorem 3.4.1, requires additional preparations. The major step, Proposition 3.4.7, concerns the singularity of Gaussian distributions in our setting, and is based on [Fel08, Proposition 3.14]. We begin with a few general lemmas. Recall that, in this chapter, all LCA groups are assumed to be second countable (hence metrizable).

Lemma 3.4.5. *Let G be an LCA group, and let H be an open subgroup of G. Then $G_e \leq H$, where G_e is the connected component of the identity in G.*

Proof. If $\pi : G \twoheadrightarrow G/H$ denotes the canonical quotient map, then $\pi(G_e)$ is a connected subgroup of the discrete group G/H. Hence, the group $\pi(G_e)$ is trivial, which implies $G_e \leq H$. □

Lemma 3.4.6. *Let G be a 2-regular LCA group admitting a compact open subgroup. Then, any path connected closed subgroup of G must be trivial.*

Proof. Let H be a path connected closed subgroup of G. Together with second countability, we know that $H \cong \mathbb{R}^n \times \mathbb{T}^m$ for some $n \geq 0$ and $m \leq \aleph_0$ [Arm81, 8.27].

First, connectedness of H implies $H \leq G_e$. Since G admits a compact open subgroup, Lemma 3.4.5 implies that G_e compact. Hence, H is compact, which forces $n = 0$.

Second, since G is 2-regular, the doubling map $x \mapsto 2x$ is injective on H. Since this is false for any non-trivial power of $\mathbb{T}$, we must also have $m = 0$. Thus, H is trivial. □

Proposition 3.4.7. *Let G be a non-discrete 2-regular LCA group with a compact open subgroup. Then any Gaussian distribution ν on G is singular with respect to the Haar measure μ on G.*

Proof. We may assume that ν is *symmetric* (meaning $x = 0$ in (3.3.1)) by translation. Then the support C of ν is a connected closed subgroup of G [Fel08, Proposition 3.6]. By Lemma 3.4.6, if C were path connected, it would be trivial, in which case $\nu = \delta_e$ is singular (as G is not discrete).

Suppose C is not path connected. We know by [Fel08, Proposition 3.8, Proposition 3.11] that there is a path connected Polish group L (not necessarily locally compact), a continuous homomorphism $p : L \to C$, and a distribution ν_L on L such that $\nu = p(\nu_L)$ (push-forward measure). Hence, ν is concentrated on the subgroup $p(L)$. We claim that $p(L)$ is Borel with $\mu(p(L)) = 0$, which gives the singularity of ν.

First note that $p(L)$ is the image of the induced map $\tilde{p} : L/\mathrm{Ker}(p) \to C$, which is injective. Since $L/\mathrm{Ker}(p)$ is a Polish group and C is metrizable, it follows that $p(L)$ is Borel by [Tak02, Corollary A.7].

Now suppose, by way of contradiction, that $\mu(p(L)) > 0$. Since G admits a compact open subgroup, G_e is compact by Lemma 3.4.5. Hence, $C \leq G_e$ is compact, forcing $0 < \mu(p(L)) \leq \mu(C) < \infty$, which means that $p(L) = p(L) - p(L)$ contains a neighborhood of the identity of G by [HR79, 20.17]. Thus, $p(L)$ is a subgroup of G with non-empty interior, hence clopen. From the definition of the support we then have $p(L) = C$, which implies that C is path connected; contradiction. $\square$

We are now ready to finish the proof of the main result of this subsection. Recall that $G_c = F_c \times \widehat{F}_c$ where F_c is an LCA group admitting a compact open subgroup.

Proof of Theorem 3.4.1. (1) $\Rightarrow$ (2): Suppose $\rho \in \mathcal{D}(L^2(F_c))$ is a B-Gaussian state. Then χ_ρ is the Fourier transform of a B-Gaussian distribution on $\widehat{G}_c$. Thanks to 2-regularity and Proposition 3.3.3 it is of the form $\chi_\rho = \mathcal{F}_{\widehat{G}_c}(\nu)|_{K^\perp} 1_{K^\perp}$ for a compact Corwin subgroup $K \leq \widehat{G}_c$ and a Gaussian distribution ν on $\widehat{G}_c$. Since $K^\perp$ is open and $\chi_\rho \in L^2(G_c)$ we know that $\mathcal{F}_{\widehat{G}_c}(\nu)|_{K^\perp} \in L^2(K^\perp)$. We claim that

$$(*)\ \ \mathcal{F}_{\widehat{G}_c}(\nu)|_{K^\perp} = \mathcal{F}_{\widehat{G}_c/K}(\nu_K)$$

for some Gaussian distribution ν_K on $\widehat{G}_c/K$. Supposing $(*)$ holds, the measure $\nu_K \in M(\widehat{G}_c/K)$ has square-integrable Fourier transform and so must be absolutely continuous with respect to the Haar measure on $\widehat{G}_c/K$ (with square-integrable Radon-Nikodym derivative, by the Plancherel theorem). This forces K to be open. If not, the group $\widehat{G}_c/K$ is non-discrete, and we can appeal to Proposition 3.4.7 to get the contradiction that ν_K is also singular with respect to the Haar measure on $\widehat{G}_c/K$. Note that $\widehat{G}_c/K$ satisfies the assumption of Proposition 3.4.7: K is a Corwin subgroup of a 2-regular group, so it is automatically 2-regular. Together with 2-regularity of $\widehat{G}_c$, it follows that $\widehat{G}_c/K$ is 2-regular. Also, since $\widehat{G}_c$ contains a compact open subgroup, so too does $\widehat{G}_c/K$ as the canonical quotient map $\pi : \widehat{G}_c \to \widehat{G}_c/K$ is open (see, e.g., [HR79, 5.26]). Thus, K is open, and the Gaussian disctribution ν_K is supported on a connected subset ([Fel08, Proposition 3.6]) of the discrete group $\widehat{G}_c/K$, so that $\nu_K = \delta_{\gamma_0+K}$ for some $\gamma_0 \in \widehat{G}_c$. But then

$$\chi_\rho = \mathcal{F}_{\widehat{G}_c/K}(\nu_K) 1_{K^\perp} = \gamma_0^{-1} 1_{K^\perp},$$

so letting $H = K^{\perp}$, and $\gamma = \gamma_0^{-1}|_H$, we see that H is a compact open 2-regular subgroup of G, $\gamma \in \widehat{H}$, and $\chi_\rho = \gamma 1_H$. Thus, $\rho = \rho_{H,\gamma}$ as in (3.4.1).

Let us go back to the claim (∗). Viewing $C_b(\widehat{G}_c/K) \subseteq C_b(\widehat{G}_c)$ in the canonical fashion (as functions which are constant on the cosets of K), restriction to $C_b(\widehat{G}_c/K)$ induces a probability preserving map from $M(\widehat{G}_c)$ to $M(\widehat{G}_c/K)$. Write ν_K for the image of ν under this map. Then, for all $f \in C_b(\widehat{G}_c/K)$,

$$\langle f, \nu_K \rangle_{(C_b(\widehat{G}_c/K), M(\widehat{G}_c/K))} = \langle f, \nu \rangle_{(C_b(\widehat{G}_c), M(\widehat{G}_c))}.$$

Consequently, ν_K is a Gaussian distribution on $\widehat{G}_c/K$ and for $z \in \widehat{(\widehat{G}_c/K)} \cong K^{\perp} \leq G$,

$$\begin{aligned}
\mathcal{F}_{\widehat{G}_c/K}(\nu_K)(z) &= \int_{\widehat{G}_c/K} \overline{\langle z, \gamma + K \rangle} d\nu_K(\gamma + K) = \langle z^{-1}, \nu_K \rangle_{(C_b(\widehat{G}_c/K), M(\widehat{G}_c/K))} \\
&= \langle z^{-1}, \nu \rangle_{(C_b(\widehat{G}_c), M(\widehat{G}_c))} \\
&= \mathcal{F}_{\widehat{G}_c}(\nu)|_{K^{\perp}}(z).
\end{aligned}$$

It remains to show that H is isotropic. Uniqueness follows from (twisted) Fourier inversion. If we denote $H_0 = H \cap H^{\Delta}$, then $\rho^2 = \mu_{G_c}(H)\rho_{H_0,\gamma}$ by Proposition 3.4.4. Since H_0 is compact, open, isotropic and 2-regular, $\rho_{H_0,\gamma}$ is a B-Gaussian state with $\rho_{H_0,\gamma}^2 = \mu_{G_c}(H_0)\rho_{H_0,\gamma}$. The eigenvalues of $\rho_{H_0,\gamma}$ are therefore 0 and $\mu_{G_c}(H_0)$. Since $\mathrm{Tr}(\rho_{H_0,\gamma}) = 1$, the eigenvalue $\mu_{G_c}(H_0)$ has multiplicity $\mu_{G_c}(H_0)^{-1}$, implying that ρ has the eigenvalue $\mu_{G_c}(H)^{1/2}\mu_{G_c}(H_0)^{1/2}$ with the same multiplicity. From the condition $\mathrm{Tr}\,\rho = 1$ we get

$$\mu_{G_c}(H)^{1/2}\mu_{G_c}(H_0)^{1/2}\mu_{G_c}(H_0)^{-1} = 1,$$

which implies $\mu_{G_c}(H) = \mu_{G_c}(H_0)$. If $z \in H \backslash H_0 = H \cap H_0^c$, then there is an open neighbourhood U of z in $H \backslash H_0$. But then

$$\mu_{G_c}(H) \geq \mu_{G_c}(H_0 \cup U) = \mu_{G_c}(H_0) + \mu_{G_c}(U) > \mu_{G_c}(H_0),$$

contradiction. Thus, $H = H_0$ is isotropic. □

Remark 3.4.8.

1. If G_c admits no compact open *2-regular* subgroup, then Theorem 3.4.1 tells us that there are no B-Gaussian states.

2. There are 2-regular LCA groups with no non-trivial, proper closed 2-regular subgroups. For example, take the 2-adic rationals $\mathbf{Q}_2$. Then $\mathbf{Q}_2$ is 2-regular as it is a field. However, if H is a non-trivial 2-regular closed subgroup of $\mathbf{Q}_2$ then necessarily $2^{-1}H = H$. But then $2^{-n}H = H$ for all $n \in \mathbb{N}$. Pick $x \in H$ with $|x|_2 > 0$. Then $(2^{-n}x)$ is a sequence in H with $|2^{-n}x|_2 = 2^n|x|_2 \to \infty$ as $n \to \infty$. Hence, H is not bounded and therefore not compact. However, every proper closed subgroup of $\mathbf{Q}_2$ is compact (and open) [RS68, Corollary 9], so $H = \mathbf{Q}_2$. A similar argument shows that any closed 2-regular subgroup of $\mathbf{Q}_2^n$ is not compact. In particular, there is no B-Gaussian state over the 2-adic Weyl system $\mathbf{Q}_2^n \times \widehat{\mathbf{Q}_2^n} \cong \mathbf{Q}_2^{2n}$.

The following Corollary is a reason for us to consider B-Gaussian states instead of Gaussian states.

Corollary 3.4.9. *There is no Gaussian state in the Weyl system* $(G_c = F_c \times \widehat{F}_c, \tilde{\sigma}_{\mathrm{can}})$ *unless* F_c *is trivial.*

Proof. If ρ is a Gaussian state, then it is B-Gaussian, so $\rho = \rho_{H,\gamma}$ for H, γ as in Theorem 3.4.1, and $\chi_\rho = \gamma 1_H$. Since every Gaussian state has non-vanishing characteristic function, we have $G_c = H$. However, isotropy of H and non-degeneracy of the symplectic form Δ implies that

$$G_c = H \subset H^\Delta = G_c^\Delta = \{0\}\,.$$

□

Remark 3.4.10. Based on the characterization of B-Gaussian states we can easily determine their von Neumann entropy. Indeed, in the proof of Theorem

3.4.1, we saw that the non-zero spectrum of $\rho_{H,\gamma}$ is $\mu_{G_c}(H)$ with multiplicity $\mu_{G_c}(H)^{-1}$. It follows that

$$S(\rho_{H,\gamma}) = \log(\mu_{G_c}(H)^{-1}). \tag{3.4.2}$$

Example 3.4.11. When F is a 2-regular finite abelian group (here 2-regularity equivalent to F having odd cardinality), our Haar measure on $G = F \times \widehat{F}$ satisfying Theorem 3.2.3 is $\mu(\cdot) = |\cdot|/|F|$, where $|\cdot|$ denotes the cardinality. Therefore, the B-Gaussian state $\rho_{H,\gamma}$ can be written as

$$\rho_{H,\gamma} = \frac{1}{|F|}\sum_{z\in H}\gamma(z)W_{1/2}(z).$$

Moreover, we will see later that $\rho_{H,\gamma}$ is pure if and only if H is maximally isotropic, or equivalently, $|H| = |F|$ (Lemma 3.4.17, Proposition 3.4.18). In particular, if $G = \mathbb{Z}_d^n \times \widehat{\mathbb{Z}_d^n} \cong \mathbb{Z}_d^n \times \mathbb{Z}_d^n$ with d odd, we have $\rho_{H,\gamma} = |H, v\rangle\langle H, v|$ (represented as in (3.3.4)) for some $v \in G$, by symplectic duality. Therefore, *pure B-Gaussian states over* $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ *coincide with stabilizer states of* n*-qudit systems.*

Remark 3.4.12. From the phase space perspective, the starting point of the stabilizer formalism of quantum error correction [CRSS98, Got97] is an isotropic subgroup H of $G = \mathbb{Z}_2^{2n} \cong \mathbb{Z}_2^n \times \widehat{\mathbb{Z}_2^n}$. The same idea works for more general phase groups $G = F_c \times \widehat{F_c}$: for a compact open 2-regular isotropic subgroup $H \leq G$ and a character $\gamma \in \widehat{H}$, one can encode information in the subspace of the system Hilbert space $L^2(F_c)$ which is stabilized/fixed by the action of (the abelian group) $\mathcal{S} = \left\{\gamma(h)W_{1/2}(h) : h \in H\right\}$. The B-Gaussian state $\rho_{H,\gamma}$ is precisely the normalized projection onto the *stabilizer subspace*

$$C(\mathcal{S}) = \left\{\psi \in L^2(F_c) : s|\psi\rangle = |\psi\rangle \text{ for all } s \in \mathcal{S}\right\}.$$

Indeed,

$$P := \mu_G(H)^{-1}\rho_{H,\gamma} = \mu_G(H)^{-1}\int_H \gamma(h')W_{1/2}(h')d\mu_G(h')$$

satisfies $P^2 = P \geq 0$ (Proposition 3.4.4), so P is an orthogonal projection. Moreover, we can show that $\gamma(h)W_{1/2}(h)P = P$ for all $h \in H$ from the definition (since $h \mapsto \gamma(h)W_{1/2}(h)$ is a group homomorphism), so $\mathrm{Ran}(P)$ is contained in $C(\mathcal{S})$. Finally, every vector $|\psi\rangle$ stabilized by $\mathcal{S}$ clearly satisfies $P|\psi\rangle = |\psi\rangle$, which means that $C(\mathcal{S}) \subset \mathrm{Ran}(P)$.

Example 3.4.13. In Zelenov's (relatively recent) papers [Zel14, Zel20], Gaussian states on $L^2(\mathbf{Q}_p)$ were defined by χ_ρ being the indicator function of a *lattice* $L \subseteq \mathbf{Q}_p \times \mathbf{Q}_p$ (multiplied by a suitable character on L). By a lattice, they mean a rank-2 free $\mathbf{Z}_p$-submodule of $\mathbf{Q}_p \times \mathbf{Q}_p$, where $\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}$ is the ring of p-adic integers. Concretely, this means that there exist $\mathbf{Z}_p$-linearly independent $z_1, z_2 \in \mathbf{Q}_p \times \mathbf{Q}_p$ such that $L = \mathbf{Z}_p z_1 \oplus \mathbf{Z}_p z_2$. Their Gaussian terminology was justified through the observation that such indicator functions are eigenfunctions of the symplectic Fourier transform.

Let us check that *Gaussian states in the sense of Zelenov coincide with B-Gaussian states.* To this end, let $G = \mathbf{Q}_p^n \times \mathbf{Q}_p^n$ with p an odd prime (so that G possesses B-Gaussian states, Remark 3.4.8(2)). We equip G with the metric induced by the norm

$$\|z\| = \max_{1 \leq i \leq 2n} |z_i|_p, \quad z = (z_1, ..., z_{2n}) \in G.$$

Note that the closed unit ball of $G = \mathbf{Q}_p^{2n}$ in this norm is $\mathbf{Z}_p^{2n}$.

Let ρ be a B-Gaussian state on $L^2(\mathbf{Q}_p^n)$. Since G is 2-regular and admits a compact open subgroup, by Theorem 3.4.1 there exist a compact open (2-regular) isotropic subgroup H and a character $\gamma \in \widehat{H}$ such that $\rho = \rho_{H,\gamma}$. Note that any closed subgroup of G is automatically 2-regular since it is a $\mathbf{Z}_p$-submodule and $\frac{1}{2} \in \mathbf{Z}_p$ for odd primes p. By compactness there exists $N \in \mathbb{N}$ for which $H \subseteq p^{-N}\mathbf{Z}_p^{2n}$. Hence, $p^N H$ is a $\mathbf{Z}_p$-submodule of the free module $\mathbf{Z}_p^{2n}$. Since $\mathbf{Z}_p$ is a principle ideal domain, $p^N H$ is free of rank at most $2n$. In addition, H, and therefore $p^N H$ is open in $\mathbf{Q}_p^{2n}$, so there is some $k \in \mathbb{N}$ such that $B_{\leq p^{-k}}(0)^{2n} \subseteq p^N H$, where $B_{\leq p^{-k}}(0) = p^k \mathbf{Z}_p$ is the clopen ball of radius p^{-k} in $\mathbf{Q}_p$. It follows that $p^k e_i \in p^N H$, where e_i are the standard basis vectors of $\mathbf{Q}_p^{2n}$, so $p^N H$ contains at least $2n$ independent elements. Therefore, the rank of $p^N H$ is $2n$, implying the existence of $\mathbf{Z}_p$-independent $h_1, ..., h_{2n} \in H$ for which $H = \mathrm{span}_{\mathbf{Z}_p}\{p^{-N}h_1, ..., p^{-N}h_{2n}\}$. Hence, H is a free $\mathbf{Z}_p$-module of rank $2n$ inside $\mathbf{Q}_p^{2n}$, that is, a lattice.

Conversely, let ρ be a Gaussian state on $L^2(\mathbf{Q}_p^n)$ in the sense of Zelenov associated to a lattice L. To prove ρ is B-Gaussian, it suffices to show that L is a 2-regular compact open isotropic subgroup of $\mathbf{Q}_p^n \times \mathbf{Q}_p^n$. Indeed, $L = \bigoplus_{i=1}^{2n} \mathbf{Z}_p z_i$ for some independent $z_1, \ldots, z_{2n} \in \mathbf{Q}_p^{2n}$, and therefore,

$$(p^N\mathbf{Z}_p)^{2n} = \bigoplus_{i=1}^{2n} \mathbf{Z}_p(p^N e_i) \subset L \subset \bigoplus_{i=1}^{2n} \mathbf{Z}_p(p^{-N} e_i) = (p^{-N}\mathbf{Z}_p)^{2n}$$

for sufficiently large N. Since $\bigoplus_{i=1}^{2n} \mathbf{Z}_p z_i$ is clearly closed in $\mathbf{Q}_p^n \times \mathbf{Q}_p^n$, this inclusion explains that L is compact and open. The closedness again implies that L is 2-regular as before. Now we apply the same argument as in the proof of Theorem 3.4.1 for the direction (1) $\Rightarrow$ (2) to show that $\chi_\rho = 1_L$ is a characteristic function of a state only if L is isotropic.

3.4.2 General 2-regular systems

Let us go back to the Weyl system $(F \times \widehat{F}, \tilde{\sigma}_{\mathrm{can}})$ over a general 2-regular LCA group, where $F \cong \mathbb{R}^n \times F_c$ with F_c admitting a compact open subgroup.

Theorem 3.4.14. *Every B-Gaussian state in the Weyl system* $(G = F \times \widehat{F}, \tilde{\sigma}_{\mathrm{can}})$ *is of the form* $\rho_n \otimes \rho_c$*, where* ρ_n *and* ρ_c *are B-Gaussian states in the Weyl system* $(\mathbb{R}^n \times \widehat{\mathbb{R}^n}, \tilde{\sigma}_{\mathrm{can}})$ *and* $(G_c = F_c \times \widehat{F}_c, \tilde{\sigma}_{\mathrm{can}})$*, respectively.*

Proof. Suppose $\rho \in \mathcal{D}(L^2(F))$ is B-Gaussian. Proposition 3.3.3(1) implies that the support of χ_ρ is an open subgroup H of $F \times \widehat{F} \cong \mathbb{R}^{2n} \times (F_c \times \widehat{F}_c)$. Thus, $H \cong \mathbb{R}^{2n} \times K$ for an open subgroup K of $F_c \times \widehat{F}_c$. A straightforward calculation shows that the reduced state $(\mathrm{Tr} \otimes \mathrm{id})\rho \in \mathcal{D}(L^2(F_c))$ satisfies

$$\chi_{(\mathrm{Tr}\otimes\mathrm{id})\rho} = \chi_\rho|_{\{0\}\times G_c},$$

so that $(\mathrm{Tr}\otimes\mathrm{id})\rho$ is a B-Gaussian state over the Weyl system $(G_c, \tilde{\sigma}_{\mathrm{can}})$ with $\chi_{(\mathrm{Tr}\otimes\mathrm{id})\rho}$ supported on K, which must be compact thanks to Theorem 3.4.1.

Now we apply Proposition 3.3.3(3) to get $\chi_\rho = 1_H\gamma\exp(-\varphi)$ for some $\gamma \in \widehat{H}$ and some non-negative continuous $\varphi : H \to \mathbb{R}$ satisfying (3.3.2). Let $\psi : H \times H \to \mathbb{R}$ be the continuous biadditive form associated to φ in Remark 3.3.2(2). We therefore obtain a continuous homomorphism

$$H \ni z \mapsto \psi(z, \cdot) \in \mathrm{Hom}(H, \mathbb{R}),$$

where Hom denotes the set of continuous homomorphisms. Since $H \cong \mathbb{R}^{2n} \times K$, the above homomorphism can be regarded as an element of

$$\mathrm{Hom}(\mathbb{R}^{2n} \times K, \mathrm{Hom}(\mathbb{R}^{2n} \times K, \mathbb{R})),$$

which, by commutativity of $\mathbb{R}$, identifies canonically with the product group

$$\begin{gathered}\mathrm{Hom}(\mathbb{R}^{2n}, \mathrm{Hom}(\mathbb{R}^{2n}, \mathbb{R})) \times \mathrm{Hom}(K, \mathrm{Hom}(\mathbb{R}^{2n}, \mathbb{R})) \\ \times \mathrm{Hom}(\mathbb{R}^{2n}, \mathrm{Hom}(K, \mathbb{R})) \times \mathrm{Hom}(K, \mathrm{Hom}(K, \mathbb{R})).\end{gathered}$$

Under this identification, we may write

$$\psi((x,y),(x',y')) = \left\langle \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} x' \\ y' \end{bmatrix} \right\rangle, \quad x, x' \in \mathbb{R}^{2n},\ y, y' \in K.$$

where $A \in \mathrm{Hom}(\mathbb{R}^{2n}, \mathrm{Hom}(\mathbb{R}^{2n}, \mathbb{R})) \cong M_{2n}(\mathbb{R})$, $B \in \mathrm{Hom}(K, \mathrm{Hom}(\mathbb{R}^{2n}, \mathbb{R})) \cong \mathrm{Hom}(K, \mathbb{R}^{2n})$, $C \in \mathrm{Hom}(\mathbb{R}^{2n}, \mathrm{Hom}(K, \mathbb{R}))$ and $D \in \mathrm{Hom}(K, \mathrm{Hom}(K, \mathbb{R}))$. Since K is compact, $\mathrm{Hom}(K, \mathbb{R}^m) = \{0\}$ for any $m \in \mathbb{N}$. Thus, $B = C = D = 0$, and we have $\psi((x,y),(x',y')) = \langle Ax, x'\rangle$, $x, x' \in \mathbb{R}^{2n}, y, y' \in K$ and consequently

$$\varphi((x,y)) = \psi((x,y),(x,y)) = \langle Ax, x\rangle,\ x \in \mathbb{R}^{2n}, y \in K.$$

Since $\gamma \in \widehat{H} \cong \widehat{\mathbb{R}^{2n} \times K} = \widehat{\mathbb{R}^{2n}} \times \widehat{K}$, we may write $\gamma = \gamma_n \times \gamma_c$ with

$\gamma_n \in \widehat{\mathbb{R}^{2n}}$, $\gamma_c \in \widehat{K}$. Putting things together, we see that

$$\chi_\rho(x,y) = 1_K(y)\gamma_c(y)\gamma_n(x)\exp(-\langle Ax,x\rangle) = \chi_n(x)\chi_c(y), \quad x \in \mathbb{R}^{2n},\ y \in K,$$

where $\chi_n = \chi_\rho|_{\mathbb{R}^{2n}\times\{0\}} = \chi_{(\mathrm{id}\otimes\mathrm{Tr})\rho}$ and $\chi_c = \chi_\rho|_{\{0\}\times K} = \chi_{(\mathrm{Tr}\otimes\mathrm{id})\rho}$ are the characteristic functions of B-Gaussian sates in $\rho_n \in \mathcal{D}(L^2(\mathbb{R}^n))$ and $\rho_c \in \mathcal{D}(L^2(F_c))$, respectively. By uniqueness of characteristic functions, it follows that $\rho = \rho_n \otimes \rho_c$, where $\rho_n = (\mathrm{id}\otimes\mathrm{Tr})\rho$ and $\rho_c = (\mathrm{Tr}\otimes\mathrm{id})\rho$. □

Remark 3.4.15. Theorem 3.4.14 shows that there is a topological obstruction for B-Gaussian states over the Weyl system $(F \times \widehat{F}, \tilde{\sigma}_{\mathrm{can}})$ with $F \cong \mathbb{R}^n \times F_c$ to have bipartite entanglement with respect to the decomposition $L^2(F) \cong L^2(\mathbb{R}^n) \otimes L^2(F_c)$. A similar separability phenomenon is known to hold for minimizers of the entropic uncertainty principle over LCA groups [OP04].

3.4.3 Pure Gaussian states

Based on our characterization (Theorem 3.4.14), every B-Gaussian state in a 2-regular Weyl system $(F \times \widehat{F}, \tilde{\sigma}_{\mathrm{can}})$ is of the form $\rho_n \otimes \rho_c$, where ρ_n and ρ_c are B-Gaussian states in the Weyl systems $(\mathbb{R}^n \times \widehat{\mathbb{R}^n}, \tilde{\sigma}_{\mathrm{can}})$ and $(G_c, \tilde{\sigma}_{\mathrm{can}})$, respectively. Since a product state is pure if and only if each component is pure, and the purity of bosonic Gaussian states has been characterized (see [AGI07, Section 3], for example), the characterization of pure B-Gaussian states reduces to the case of ρ_c. By Theorem 3.4.1, it is of the form $\rho_{H,\gamma}$ for some compact open 2-regular isotropic subgroup $H \leq G_c$ and a character $\gamma \in \widehat{H}$. In Proposition 3.4.18 we will prove that $\rho_{H,\gamma}$ is pure if and only if H is maximally isotropic. Moreover, we show that every pure B-Gaussian state is determined (up to a Weyl translation) by a symmetric bicharacter (Theorem 3.4.19). We begin with some preliminary results.

Lemma 3.4.16. *For any compact open subgroup $H \leq G_c$ we have*

$$\mu(H)\mu(H^\Delta) = 1, \tag{3.4.3}$$

where $\mu = \mu_{G_c}$.

Proof. Let Φ_Δ be the (canonical) symplectic self-duality on G_c. By uniqueness of Haar measures, there exists $c > 0$ for which $\Phi_\Delta(\mu) = c\mu_{\widehat{G}_c}$, where $\Phi_\Delta(\mu)$ is the push-forward measure. Since $H^\perp = \Phi_\Delta(H^\Delta)$, by the Plancherel theorem we have

$$\begin{aligned} 1 &= \left\|\mu(H)^{-1/2}1_H\right\|^2_{L^2(G_c)} = \left\|\mathcal{F}_{G_c}(\mu(H)^{-1/2}1_H)\right\|^2_{L^2(\widehat{G}_c)} \\ &= \left\|\mu(H)^{1/2}1_{H^\perp}\right\|^2_{L^2(\widehat{G}_c)} = \mu(H)\mu_{\widehat{G}_c}(H^\perp) = c^{-1}\mu(H)\mu(H^\Delta). \end{aligned} \tag{3.4.4}$$

It remains to show that $c = 1$. Since G_c admits a compact open 2-regular subgroup, so too does F_c (project onto first coordinate). Let $K \leq F_c$ be such a subgroup. Then as shown in Example 3.3.7, the characteristic function of the state $\psi = \mu_{F_c}(K)^{-1/2}1_K \in L^2(F_c)$ is $\chi_{|\psi\rangle\langle\psi|} = 1_{K\times K^\perp}$. It is easy to see that $K \times K^\perp$ is a compact open Lagrangian subgroup of G_c. Hence, (3.4.4) implies

$$\mu(K \times K^\perp)^2 = \mu(K \times K^\perp)\mu((K \times K^\perp)^\Delta) = c.$$

Theorem 3.2.3 then shows

$$1 = \||\psi\rangle\langle\psi|\|_2^2 = \|1_{K\times K^\perp}\|^2_{L^2(G_c)} = \mu(K \times K^\perp) = \sqrt{c}. \tag{3.4.5}$$

□

Lemma 3.4.17. *Let H be a compact open isotropic subgroup of G_c. Then H is Lagrangian if and only if $\mu_{G_c}(H) = 1$.*

Proof. Let $\mu = \mu_{G_c}$ for simplicity. If $H = H^\Delta$, then $\mu(H) = 1$ is direct from Lemma 3.4.16. Conversely, if $\mu(H) = 1$, then we get $\mu(H) = \mu(H^\Delta) = 1$ from the conditions $\mu(H) \leq \mu(H^\Delta)$ and $\mu(H)\mu(H^\Delta) = 1$. Since $H \subseteq H^\Delta$, this implies that $H = H^\Delta$. Note that H^Δ is compact open by Lemma 3.4.3

□

Combining (3.4.2) and Lemma 3.4.17, together with the fact that a state is pure if and only if its entropy is 0, we get the following conclusion.

Proposition 3.4.18. *A B-Gaussian state $\rho_{H,\gamma}$ is pure if and only if H is Lagrangian.*

We now show that pure B-Gaussian states in $\mathcal{D}(L^2(F_c))$ are determined by a point in the phase space G_c and a symmetric bicharacter, which is the analogue of the first and second moments for pure bosonic Gaussian states. Recall that a bicharacter $\beta : K \times K \to \mathbb{T}$ on an LCA group K is *symmetric* if $\beta(x, y) = \beta(y, x),\ x, y \in K$.

Theorem 3.4.19. *A pure state $\rho = |\psi\rangle\langle\psi| \in \mathcal{D}(L^2(F_c))$ is B-Gaussian if and only if there exists a compact open 2-regular subgroup K of F_c, a symmetric bicharacter $\beta : K \times K \to \mathbb{T}$, $z_0 \in G_c$, and $\alpha \in \mathbb{T}$ such that $\psi = \alpha W(z_0)\psi_0$, where*

$$\psi_0(x) = \mu_{F_c}(K)^{-1/2} 1_K(x)\beta(x, 2^{-1}x), \quad x \in F_c. \tag{3.4.6}$$

Alternatively, for $z_0 = (x_0, \gamma_0)$ we have

$$\psi(x) = \tilde{\alpha}\mu_{F_c}(K)^{-1/2} 1_{K+x_0}(x)\gamma_0(x)\beta(x, 2^{-1}x), \quad x \in F_c,$$

for some $\tilde{\alpha} \in \mathbb{T}$. In this case, $\rho = \rho_{H,\Gamma}$ where $\Gamma = \Delta(z_0, \cdot)$ and

$$H = \{(x, \gamma) \in G_c : x \in K, \gamma|_K = \beta(x, \cdot)\}. \tag{3.4.7}$$

Remark 3.4.20. Note that the above theorem implies that we can choose a continuous wave function for every pure B-Gaussian state. Furthermore, the result includes the characterization of stabilizer states in [Gro06, Lemma 18], which is equivalent to saying that if $d \geq 3$ is an odd integer, every pure B-Gaussian state $\rho = |\psi\rangle\langle\psi| \in \mathcal{D}(\ell^2(\mathbb{Z}_d^n))$ with $\psi(x) \neq 0$ for all $x \in \mathbb{Z}_d^n$ is exactly of the form

$$\psi(x) = d^{-n/2}\omega^{x^T Ax + b^T x + c},$$

where $\omega = \exp(\frac{2\pi i}{d})$, $A \in M_n(\mathbb{Z}_d)$ is a symmetric matrix, $b \in \mathbb{Z}_d^n$, and $c \in \mathbb{R}$.

The proof of Theorem 3.4.19 begins with a connection between compact open 2-regular Lagrangian subgroups and symmetric bicharacters, as follows.

Lemma 3.4.21. *There exists one-to-one correspondence between the family of 2-regular compact open Lagrangian subgroups H of G_c and the family of pairs (K,β) consisting of a compact open 2-regular subgroup K of F_c and a symmetric bicharacter $\beta : K \times K \to \mathbb{T}$, related by equation* (3.4.7)*.*

Proof. For a given pair (K,β), let $H \subset G_c$ be defined by the relation (3.4.7), which can easily be checked to be 2-regular closed subgroup of G_c. The isotropy of H follows from the symmetry of β: for $(x,\gamma),(x',\gamma') \in H$,

$$\Delta((x,\gamma),(x',\gamma')) = \beta(x,x')\overline{\beta(x',x)} = 1.$$

Moreover, for each $x \in K$, the corresponding section

$$H_x := \left\{\gamma \in \widehat{F}_c : (x,\gamma) \in H\right\} = \left\{\gamma \in \widehat{F}_c : \gamma|_K = \beta(x,\cdot)\right\} \tag{3.4.8}$$

is actually a coset of $K^\perp$ in $\widehat{F}_c$. By Fubini's theorem and (3.4.5), we have

$$\mu_{G_c}(H) = \int_K \mu_{\widehat{F}_c}(H_x)\, d\mu_{F_c}(x) = \int_K \mu_{\widehat{F}_c}(K^\perp)\, d\mu_{F_c}(x) = \mu_{F_c}(K)\mu_{\widehat{F}_c}(K^\perp) = 1.$$

This implies that H is open and compact by (2.1.1), and H is Lagrangian by Lemma 3.4.17, which explains one direction of the correspondence.

For the reverse direction, let H be a compact open 2-regular Lagrangian subgroup of G_c. For the natural projection $\pi_{F_c} : (x,\gamma) \in G_c \mapsto x \in F_c$, define $K := \pi_{F_c}(H)$. Then K is a 2-regular compact open subgroup of F_c since π_{F_c} is a continuous homomorphism and an open map. We first claim that for each $x \in K$, we have $H_x = \gamma_x + K^\perp$ for some $\gamma_x \in \widehat{F}_c$, where H_x is from (3.4.8). Indeed, we can pick any $\gamma_x \in \widehat{F}_c$ such that $(x,\gamma_x) \in H$, and then

$$\begin{aligned}\gamma \in H_x &\iff (0,\gamma-\gamma_x) \in H = H^\Delta \\ &\iff \Delta((0,\gamma-\gamma_x),(x',\gamma')) = \gamma(x')\overline{\gamma_x(x')} = 1 \text{ for all } (x',\gamma') \in H \\ &\iff \gamma-\gamma_x \in K^\perp \iff \gamma \in \gamma_x + K^\perp.\end{aligned}$$

Next, we claim that the map $T : K \to \widehat{F}/K^\perp,\ x \mapsto \gamma_x + K^\perp$ is a continuous homomorphism. The additivity is clear from the definition, and the continuity comes from the facts that $\widehat{F}/K^{\perp}$ is discrete and

$$\begin{aligned}\operatorname{Ker} T &= \big\{x \in K : (x,\gamma) \in H \text{ for some } \gamma \in K^{\perp}\big\} \\ &= \bigcup_{\gamma \in K^{\perp}} \{x \in K : 1_H(x,\gamma) \neq 0\}\end{aligned}$$

is open, which in turn comes from the continuity of the function 1_H. Passing through the canonical identification $\widehat{F}/K^{\perp} \cong \widehat{K}$ we obtain a continuous homomorphism $\tilde{T} : K \to \widehat{K}$, and we can readily check that the associated bicharacter $\beta : K \times K \to \mathbb{T}$, $(x, y) \mapsto \gamma_x(y)$ is the one we were looking for. Indeed, β is symmetric since H is isotropic:

$$\beta(x,y)\overline{\beta(y,x)} = \gamma_x(y)\overline{\gamma_y(x)} = \Delta((x,\gamma_x),(y,\gamma_y)) = 1, \quad x, y \in K.$$

The relation (3.4.7) is now straightforward.

Finally, one can easily check that the maps $(K, \beta) \mapsto H$ and $H \mapsto (K, \beta)$ are inverses to each other. □

Proof of Theorem 3.4.19. Suppose $\rho = \rho_{H,\Gamma}$ is a pure B-Gaussian state. Then H is a 2-regular Lagrangian compact open subgroup of G_c by Proposition 3.4.18. By considering $\rho_0 := W(z_0)^*\rho W(z_0)$ for $z_0 \in G_c$ such that $\Gamma = \Delta(z_0, \cdot)$, we may assume that $\Gamma \equiv 1$. Moreover, we can choose a pair (K, β) as in Lemma 3.4.21 such that equation (3.4.7) holds. For the conclusion we only need to check that $\chi_\psi = \chi_\rho$ for $\psi(x) = \mu_{F_c}(K)^{-1/2}1_K(x)\beta(x, 2^{-1}x)$, $x \in F_c$. First, we recall that $\chi_\rho(x,\gamma) = 1_H(x,\gamma) = 1_K(x)1_{H_x}(\gamma)$, $(x,\gamma) \in G_c$. Moreover, there is $\gamma_x \in \widehat{F_c}$ such that $H_x = \gamma_x + K^{\perp}$ for each $x \in K$ as in the proof of Lemma 3.4.21. Recall also that $\beta(x, y) = \gamma_x(y)$ with the above choice. Now we observe that

$$\begin{aligned}
\chi_\psi(x,\gamma) &= \int_{F_c} \overline{\gamma(y-2^{-1}x)}\,\overline{\psi(y-x)}\psi(y)d\mu_{F_c}(y) \\
&= \int_K \overline{\gamma(y-2^{-1}x)}\mu_{F_c}(K)^{-1}1_K(y-x)\beta(x,y-2^{-1}x)d\mu_{F_c}(y) \\
&= 1_K(x)\int_K \overline{\gamma(y)}\mu_{F_c}(K)^{-1}\beta(x,y)d\mu_{F_c}(y) \\
&= 1_K(x)\int_K \overline{\gamma(y)}\mu_{F_c}(K)^{-1}\gamma_x(y)d\mu_{F_c}(y) \\
&= 1_K(x)1_{\gamma_x+K^\perp}(\gamma|_K),
\end{aligned}$$

which lead to the desired conclusion.

We also get the converse by following the above calculation process backwards, again combined with Lemma 3.4.21. □

It is well-known that in bosonic systems, every Gaussian state belongs to the norm-closed convex hull of pure Gaussian states ([Ser17, Problem 5.10]). The same phenomenon occurs in our setting.

Lemma 3.4.22. *Let H be a compact open 2-regular isotropic subgroup of G_c. The map $\widehat{G}_c \ni \gamma \mapsto \rho_{H,\gamma} \in \mathcal{S}^1(L^2(F_c))$ is norm continuous.*

Proof. Take a net (γ_i) converging to $\gamma \in \widehat{G}_c$, meaning uniform convergence on compact sets. Since H is a compact open subgroup, it follows that $\gamma_i 1_H \to \gamma 1_H$ in $L^2(G_c)$. Thus, by continuity of the twisted Fourier transform (Theorem 3.2.3)

$$\rho_{H,\gamma_i} = \mathcal{F}_G^\sigma(\gamma_i 1_H) \to \mathcal{F}_G^\sigma(\gamma 1_H) = \rho_{H,\gamma}$$

in $\mathcal{S}^2(L^2(F_c))$. Since $\rho_{H,\gamma_i}^2 = \mu_{G_c}(H)\rho_{H,\gamma_i}$ (Proposition 3.4.4) we have $\sqrt{\rho_{H,\gamma_i}} = \mu_{G_c}(H)^{-1/2}\rho_{H,\gamma_i}$. Similarly, $\sqrt{\rho_{H,\gamma}} = \mu_{G_c}(H)^{-1/2}\rho_{H,\gamma}$. Hence,

$$\left\|\sqrt{\rho_{H,\gamma_i}} - \sqrt{\rho_{H,\gamma}}\right\|_2 = \mu_{G_c}(H)^{-1/2}\left\|\rho_{H,\gamma_i} - \rho_{H,\gamma}\right\|_2 \to 0$$

in $\mathcal{S}^2(L^2(F_c))$. Furthermore, isotropy of H implies $\rho_{H,\gamma_i}\rho_{H,\gamma} = \rho_{H,\gamma}\rho_{H,\gamma_i}$ and

$$\|\rho_{H,\gamma_i} - \rho_{H,\gamma}\|_1 \le \left\|\sqrt{\rho_{H,\gamma_i}} - \sqrt{\rho_{H,\gamma}}\right\|_2 \left\|\sqrt{\rho_{H,\gamma_i}} + \sqrt{\rho_{H,\gamma}}\right\|_2 \to 0.$$

□

Theorem 3.4.23. *Every B-Gaussian state in $\mathcal{S}^1(L^2(F))$ belongs to the norm closed convex hull of pure B-Gaussian states.*

Proof. Thanks to the decomposition $\rho_n \otimes \rho_c$ we can focus on the case of the state $\rho_c = \rho_{H,\gamma}$ for some compact open 2-regular isotropic subgroup H of G_c and a character $\gamma \in \widehat{H}$. Pick a maximal isotropic subgroup K containing H (by Zorn's lemma, if needed). Since $H^\perp$ is a compact open subgroup of $\widehat{G}_c$ and the map $\gamma' \mapsto \rho_{K,\gamma\gamma'}$ is continuous by Lemma 3.4.22, the following state is well defined.

$$\rho = \frac{1}{\mu_{\widehat{G}_c}(H^\perp)} \int_{H^\perp} \rho_{K,\gamma\gamma'} d\mu_{\widehat{G}_c}(\gamma').$$

We only need to check that $\chi_{\rho_{H,\gamma}} = \chi_\rho$ for the desired conclusion by Proposition 3.4.18. Indeed, for $z \in G_c$ we have

$$\begin{aligned}
\chi_\rho(z) &= \operatorname{Tr}\left(W_{1/2}(z)^*\left(\frac{1}{\mu_{\widehat{G}_c}(H^\perp)} \int_{H^\perp} \rho_{K,\gamma\gamma'} d\mu_{\widehat{G}_c}(\gamma')\right)\right) \\
&= \frac{1}{\mu_{\widehat{G}_c}(H^\perp)} \int_{H^\perp} \operatorname{Tr}(W_{1/2}(z)^* \rho_{K,\gamma\gamma'}) d\mu_{\widehat{G}_c}(\gamma') \\
&= \frac{1}{\mu_{\widehat{G}_c}(H^\perp)} \int_{H^\perp} \gamma(z)\gamma'(z) 1_K(z) d\mu_{\widehat{G}_c}(\gamma') \\
&= \frac{\gamma(z)1_K(z)}{\mu_{\widehat{G}_c}(H^\perp)} \int_{H^\perp} \gamma'(z) d\mu_{\widehat{G}_c}(\gamma') \\
&= \gamma(z)1_K(z)1_{H^{\perp\perp}}(z) = \gamma(z)1_{K\cap H}(z) \\
&= \gamma(z)1_H(z) = \chi_{\rho_{H,\gamma}}(z).
\end{aligned}$$

□

3.5 Angle-number systems

In this section we show that B-gaussian states in the angle-number system in d-modes are nothing but the pure states whose wave functions are the elements of the canonical orthonormal basis $\{|m\rangle = |e_m\rangle : m \in \mathbb{Z}^d\} \subseteq \mathcal{H} = L^2(\mathbb{T}^d) \cong \ell^2(\mathbb{Z}^d)$, where $e_m(\theta) = e^{2\pi i\langle \theta, m\rangle}$, $\theta \in \mathbb{T}^d$. Recall that the associated Weyl representation $W_{1/2}$ is

$$W_{1/2}(\theta, n) := e^{\pi i\langle \theta, n\rangle} T_\theta M_n, \quad (\theta, n) \in \mathbb{T}^d \times \mathbb{Z}^d.$$

See Section 3.1.2 for details.

The first step of the proof is to determine the characteristic functions for rank-1 operators acting on $\mathcal{H}$.

Lemma 3.5.1. *For $a, b \in \mathbb{Z}^d$ we have*

$$\chi_{|a\rangle\langle b|}(\theta, n) = \delta_{a-b,n}\, e^{\pi i\langle \theta, a+b\rangle}, \quad (\theta, n) \in \mathbb{T}^d \times \mathbb{Z}^d. \tag{3.5.1}$$

Proof. It is straightforward from the computation

$$\begin{aligned}
\chi_{|a\rangle\langle b|}(\theta, n) &= \langle b|W_{1/2}(-\theta, -n)|a\rangle \\
&= \int_{\mathbb{T}^d} e^{-2\pi i\langle \theta', b\rangle} e^{\pi i\langle \theta, n\rangle} e^{2\pi i\langle (\theta'+\theta), a-n\rangle}\, d\theta' \\
&= e^{\pi i\langle \theta, 2a-n\rangle} \int_{\mathbb{T}^d} e^{2\pi i\langle \theta', a-b-n\rangle}\, d\theta' = \delta_{a-b,n} e^{\pi i\langle \theta, a+b\rangle}.
\end{aligned}$$

□

We again remark that the formula (3.5.1) is only valid for our identification $\theta \in \left[-\frac{1}{2}, \frac{1}{2}\right)^d$ through (3.1.11).

Theorem 3.5.2. *The set of all B-Gaussian states for the angle-number system in d-modes is the set of all pure states of the form $|m\rangle\langle m|$ for some $m \in \mathbb{Z}^d$.*

Proof. Let ρ be a B-Gaussian state with the (open) support H of χ_ρ. Since H is an open subgroup of $G = \mathbb{T}^d \times \mathbb{Z}^d$ we know that $H = \mathbb{T}^d \times K$ for a subgroup

K of $\mathbb{Z}^d$. It is easy to check that the Haar measure μ on G respecting the twisted Plancherel formula (3.2.2) is given by

$$\int_G f\,d\mu = \sum_{n\in\mathbb{Z}^d}\int_{\mathbb{T}^d} f(\theta,n)d\theta,\quad f\in C_c(G).$$

Then, by (3.2.2) and Lemma 3.5.1, we have

$$\begin{aligned}\langle a|\rho|b\rangle = \mathrm{Tr}(\rho(|a\rangle\langle b|)^*) &= \sum_{n\in\mathbb{Z}^d}\int_{\mathbb{T}^d}\chi_\rho(\theta,n)\overline{\chi_{|a\rangle\langle b|}(\theta,n)}\,d\theta\\ &= \sum_{n\in K}\int_{\mathbb{T}^d}\delta_{a-b,n}\chi_\rho(\theta,n)e^{-\pi i\langle\theta,a+b\rangle}\,d\theta\\ &= \int_{\mathbb{T}^d} 1_K(a-b)\chi_\rho(\theta,a-b)e^{-\pi i\langle\theta,a+b\rangle}\,d\theta\end{aligned}$$

for $a,b\in\mathbb{Z}^d$. In particular,

$$\langle a|\rho|a\rangle = \int_{\mathbb{T}^d}\chi_\rho(\theta,0)e^{-2\pi i\langle\theta,a\rangle}\,d\theta = \widehat{\chi_\rho(\cdot,0)}(a),\ a\in\mathbb{Z}^d.$$

On the other hand, the B-Gaussianity of ρ again implies that $g(\cdot) := \chi_\rho(\cdot,0)$ is positive definite and satisfies the B-Gaussian identity (3.3.3) on $\mathbb{T}^d$. Thus, g is the Fourier transform of a B-Gaussian distribution on $\mathbb{Z}^d\cong\widehat{\mathbb{T}^d}$ by Bochner's theorem. Furthermore, we note that $\mathbb{Z}^d$ contains no subgroup homeomorphic to $\mathbb{T}^2$ and g is nowhere vanishing. Then, Proposition 3.3.3(2) tells us that g is the Fourier transform of a Gaussian distribution. If we write $g(\theta) = e^{2\pi i\langle\theta,m\rangle}\exp(-\varphi(\theta))$ for some $m\in\mathbb{Z}^d$ and continuous $\varphi:\mathbb{T}^d\to[0,\infty)$ satisfying (3.3.2), then compactness of $\mathbb{T}^d$ and Remark 3.3.2(2) says that $\varphi\equiv 0$ since $\mathrm{Hom}(\mathbb{T}^d,\mathbb{R}) = \{0\}$. Consequently, we have $\langle a|\rho|a\rangle = \hat{g}(a) = \delta_{m,a}$.

The above computation means that the diagonal part of the operator ρ (as an infinite matrix) is zero except one point. Thus, we can conclude that off-diagonal parts of the positive operator ρ must be zero. This forces $\rho = |m\rangle\langle m|$.

□

Recalling the fact that the Fourier transform of a Gaussian distribution has full support we get the following conclusion.

Corollary 3.5.3. *There is no Gaussian state for the angle-number system in d-modes.*

Remark 3.5.4. The above characterization is consistent with the results about characterizing pure states with non-negative Wigner functions on the angle-number system in 1-mode [RSSK+10].

3.6 Fermions and hard-core bosons

In this section we show that there are no B-Gaussian states in the fermionic and hard-core bosonic systems, introduced in Section 3.1.3. Although stabilizer states exist and are heavily studied in these qubit systems, in comparison with our previous results on finite 2-regular groups, this section shows that qubit stabilizer states do not possess an underlying Gaussian characterization in the sense of Bernstein.

We begin with a simple description of B-Gaussian distributions on $\mathbb{Z}_2^m$.

Proposition 3.6.1. *Every B-Gaussian distribution on $G = \mathbb{Z}_2^m$ is of the form δ_a for some $a \in G$, which is a Gaussian distribution on G.*

Proof. Let μ be a B-Gaussian distribution on $G = \mathbb{Z}_2^m$ and let $H = \operatorname{supp}\hat{\mu}$. Then the annihilator $H^\perp$ is trivial (or equivalently, $H = G$) since it is a compact Corwin subgroup of G in which all elements have order 2. Thus, Proposition 3.3.3 (2) tells us that μ is a Gaussian distribution on G. In particular, $\hat{\mu}$ is a character on $\widehat{G}$ as the associated quadratic function φ must vanish, which means that μ is a point-mass at some point on G. Note finally that it is straightforward to see that every point-mass is a Gaussian distribution.

□

Let us first focus on the hard-core boson setting.

Theorem 3.6.2. *For any choice of normalizing factor* ξ (3.1.17)*, there is no B-Gaussian state on the quantum kinematical system* $(\mathbb{Z}_2^n \times \mathbb{Z}_2^n, \tilde{\sigma}_{\text{can}})$*.*

Proof. Suppose $\rho \in \mathcal{D}((\mathbb{C}^2)^{\otimes n})$ is a B-Gaussian state associated to the (B-)Gaussian distribution δ_a, $a \in \mathbb{Z}_2^{2n}$ (Proposition 3.6.1). By Equation (3.2.7) and the non-degeneracy of Δ, there exists $z_0 \in \mathbb{Z}_2^{2n}$ such that $\rho_0 := W(z_0)^* \rho W(z_0)$ has a characteristic function

$$\chi_{\rho_0}(w) = \overline{\Delta(z_0, w)} \widehat{\delta_a}(w) = (-1)^{z_0^T J w} (-1)^{a^T w} \equiv 1.$$

However, the twisted Fourier inversion (Proposition 3.2.4) gives that

$$\rho_0 = \frac{1}{2^n} \sum_{z \in \mathbb{Z}_2^{2n}} W_{1/2,\text{can}}(z) = \frac{1}{2^n} \sum_{z \in \mathbb{Z}_2^{2n}} \xi(z) W_{\text{can}}(z),$$

and the RHS must define a state. On the other hand, for $z = (x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}_2^{2n}$, observe from (3.1.16) that

$$(\text{id} \otimes \cdots \otimes \text{id} \otimes \text{Tr}) W_{\text{can}}(z) = 2\delta_{0,x_n} \delta_{0,y_n} h_1^{x_1} h_2^{y_1} \cdots h_{2n-3}^{x_{n-1}} h_{2n-2}^{y_{n-1}}.$$

By repeating the procedure, we get

$$(\text{id} \otimes \text{Tr} \otimes \cdots \otimes \text{Tr}) W_{\text{can}}(z) = 2^{n-1} \delta_{0,x_2} \delta_{0,y_2} \cdots \delta_{0,x_n} \delta_{0,y_n} h_1^{x_1} h_2^{y_2}.$$

Therefore,

$$\begin{aligned}(\text{id} \otimes \text{Tr} \otimes \cdots \otimes \text{Tr}) \rho_0 &= \frac{1}{2} \sum_{x_1, y_1 \in \mathbb{Z}_2} \xi(x_1 e_1, y_1 e_1) h_1^{x_1} h_2^{y_1} \\ &= \frac{1}{2}(I \pm X \pm Y \pm Z)\end{aligned}$$

where $e_1 = (1, \ldots, 0) \in \mathbb{Z}_2^n$, from the formulae $\xi(e_1, 0)^2 = \xi(0, e_1)^2 = 1$ and $\xi(e_1, e_1)^2 = -1$. But it is easy to see that, for any choice of signs, the resulting operator is not positive, a contradiction. □

The same method works for fermionic systems.

Theorem 3.6.3. *For any choice of the normalizing factor* ξ (3.1.15), *there is no B-Gaussian state on the quantum kinematical system* $(\mathbb{Z}_2^{2n}, \tilde{\sigma}_{\mathrm{fer}})$.

Proof. As in the hardcore boson case it boils down to check the operator

$$\rho = \frac{1}{2^n} \sum_{a \in \mathbb{Z}_2^{2n}} \xi(a) W_{\mathrm{fer}}(a)$$

is not positive. By the same argument in Theorem 3.6.2, we have

$$(\mathrm{id} \otimes \mathrm{Tr} \otimes \cdots \otimes \mathrm{Tr}) W_{\mathrm{fer}}(a) = 2^{n-1} \delta_{0,x_3} \delta_{0,x_4} \cdots \delta_{0,x_{2n}} c_1^{x_1} c_2^{x_2}$$

for $a = (x_1, \ldots, x_{2n}) \in \mathbb{Z}_2^{2n}$, and therefore,

$$\begin{aligned}(\mathrm{id} \otimes \mathrm{Tr} \otimes \cdots \otimes \mathrm{Tr}) \rho &= \frac{1}{2} \sum_{x_1, x_2 \in \mathbb{Z}_2} \xi(x_1, x_2, 0, \ldots, 0) c_1^{x_1} c_2^{x_2} \\ &= \frac{1}{2}(I \pm X \pm Y \pm Z),\end{aligned}$$

which is a contradiction as before. □

3.7 Hudson's theorem for 2-regular totally disconnected groups

Hudson's theorem [Hud74] and its higher dimensional generalization [SC83] show that pure bosonic Gaussian states can be characterized by non-negativity of their Wigner functions. Gross [Gro06] continued this line of research for the Weyl system with $F = \mathbb{Z}_d^n$, $d(\geq 3)$ odd, characterizing pure states with non-negative Wigner functions as the class of stabilizer states, i.e. pure B-Gaussian states in our terminology. We extend the result of Gross to the case of totally disconnected groups. Recall that a topological space is *totally disconnected* if the only connected sets are singletons. Note that our proof is inspired by the one of Gross [Gro06], but there are fundamentally new aspects to accommodate the infinite group setting.

In this section, F denotes a (second countable) 2-regular totally disconnected LCA group, unless otherwise noted.

Proposition 3.7.1. *(van Dantzig, [VD36], [HR79, Theorem 7.7]) Every open neighborhood of the identity of a totally disconnected locally compact group contains a compact open subgroup.*

Since F contains a compact open subgroup, all the facts from Section 3.4.1 are applicable to the kinematical system $(G = F \times \widehat{F}, \sigma = \tilde{\sigma}_{\text{can}})$ with the corresponding Weyl representation $W = W_{1/2}$ given by

$$W(x,\gamma)\psi(y) = \overline{\langle 2^{-1}x, \gamma\rangle}\langle y,\gamma\rangle\psi(y-x), \quad \psi \in L^2(F),\ x, y \in F, \gamma \in \widehat{F}.$$

Let us express the Wigner function $\mathcal{W}_\psi$ of a vector state $\psi \in L^2(F)$ using *the self-correlation function* as in [Gro06, p.10],

$$\varphi_q(x) := \psi(q + 2^{-1}x)\overline{\psi(q - 2^{-1}x)}, \quad q, x \in F.$$

We first note that

$$\chi_\psi(x,\gamma) = \int \langle 2^{-1}x,\gamma\rangle\overline{\langle y,\gamma\rangle}\,\overline{\psi(y-x)}\psi(y)d\mu_F(y) = \langle 2^{-1}x,\gamma\rangle\widehat{g_x}^F(\gamma)$$

with $g_x(y) = \overline{\psi(y-x)}\psi(y)$, $x, y \in F, \gamma \in \widehat{F}$. On the other hand we have

$$\Delta((q,p),(x,\gamma)) = p(x)\overline{\gamma(q)}, \quad q, x \in F, p, \gamma \in \widehat{F}.$$

Combining the above we get

$$\begin{aligned}\mathcal{W}_\psi(q,p) &= \left[\mathcal{F}^F \otimes (\mathcal{F}^F)^{-1}\right](\chi_\psi)(p,q) = (\mathcal{F}^F g_\cdot(q + 2^{-1}\cdot))(p) \\ &= \widehat{\varphi_q}^F(p), \quad q \in F, p \in \widehat{F}.\end{aligned} \tag{3.7.1}$$

The main theorem of this section is the following.

Theorem 3.7.2 (Hudson's theorem, 2-regular totally disconnected version). *For a pure state $\psi \in L^2(F)$ over the Weyl system $(F \times \widehat{F}, \tilde{\sigma}_{\text{can}})$,* *the following are equivalent:*

1. $\rho = |\psi\rangle\langle\psi|$ *is B-Gaussian,*

2. ψ *is continuous and* $\mathcal{W}_\psi \geq 0$ *a.e.*

The proof for the direction (1) $\Rightarrow$ (2) is a simple combination of Theorem 3.4.1 and Theorem 3.4.19. Indeed, a B-Gaussian pure state $\rho = \rho_{H,\Gamma}$ associated to a Lagrangian subgroup H and a character $\Gamma = \Delta(z_0, \cdot)$ has a characteristic function $\chi_\rho = \Gamma \cdot 1_H$. Therefore we have $\mathcal{W}_\psi(z) = 1_H(z - z_0) \geq 0$. Moreover, (3.4.6) reveals that ψ is continuous.

The reverse direction (2) $\Rightarrow$ (1) is the main difficulty. Let us begin with a lemma which exploits the total disconnectedness of F in a crucial way.

Lemma 3.7.3. *If* $f \in L^1(F)$, $\hat{f} \geq 0$ *a.e., and if* f *is continuous at* 0*, then* $\hat{f} \in L^1$.

Proof. Proposition 3.7.1 and second countability of F give a sequence $\{K_n\}_{n=1}^{\infty}$ of compact open subgroups of F decreasing to the trivial subgroup. Now we claim that $1_{(K_n)^\perp} \to 1$ pointwise on $\widehat{F}$ as $n \to \infty$. Indeed, if $\gamma \in \widehat{F}$ and $\epsilon \in (0, \frac{1}{2})$, then $V = \{x \in F : |\langle x, \gamma\rangle - 1| < \epsilon\}$ is a neighborhood of 0. Choose N such that $K_N \subset V$. Since $K_n \subset V$ for $n \geq N$, we have

$$\begin{aligned}
|1_{(K_n)^\perp}(\gamma) - 1| &= \left|\mu_F(K_n)^{-1}\,\widehat{1_{K_n}}(\gamma) - 1\right| \\
&= \left|\int_V (\overline{\langle x, \gamma\rangle} - 1)\mu_F(K_n)^{-1}\,1_{K_n}(x)\,dx\right| < \epsilon\,(< 1/2).
\end{aligned}$$

Since $|1_{(K_n)^\perp}(\gamma) - 1|$ is either 0 or 1, we have $1_{(K_n)^\perp}(\gamma) = 1$ for all $n \geq N$.

Now we apply the monotone convergence theorem and Fubini's theorem together with the above claim to get

$$\begin{aligned}\int_{\widehat{F}} \hat{f}(\gamma)d\gamma &= \lim_{n\to\infty} \int_{\widehat{F}} \hat{f}(\gamma)1_{(K_n)^\perp}(\gamma)d\gamma \\ &= \lim_{n\to\infty} \int_F \int_{\widehat{F}} f(x)1_{(K_n)^\perp}(\gamma)\overline{\langle x,\gamma\rangle}\, d\gamma\, dx \\ &= \lim_{n\to\infty} \mu_F(K_n)^{-1} \int_F f(x)1_{K_n}(x)dx \\ &= f(0) < \infty.\end{aligned}$$

Note that we used the continuity of f at 0 for the last equality. □

We proceed with an analogue of [Gro06, Lemma 11].

Lemma 3.7.4. *If $\psi \in L^2(F)$ is continuous and $\mathcal{W}_\psi \geq 0$ a.e., then φ_q is a positive definite function on F for each $q \in F$. Moreover, we have*

$$|\psi(q)|^2 \geq |\psi(q+x)|\,|\psi(q-x)|, \tag{3.7.2}$$

$$|\psi(2^{-1}(x+y))|^2 \geq |\psi(x)|\,|\psi(y)|, \tag{3.7.3}$$

and

$$|\varphi_q(2^{-1}(x+y))|^2 \geq |\varphi_q(x)|\,|\varphi_q(y)| \tag{3.7.4}$$

for all $q, x, y \in F$.

Proof. Since ψ is continuous, we know that φ_q is also continuous for all $q \in F$. From our assumption and (3.7.1) we have $\widehat{\varphi_q}^F = \mathcal{W}_\psi(q,\cdot) \geq 0$ a.e.. Moreover, we know $\varphi_q \in L^1(F)$ since $\psi(q \pm 2^{-1}\cdot) \in L^2(F)$, so we can appeal to Lemma 3.7.3 to conclude that $\widehat{\varphi_q}^F$ is integrable. This implies that φ_q is positive definite on F for all $q \in F$ from Fourier inversion.

Now, the positivity of the matrix $\begin{bmatrix} \varphi_q(0) & \varphi_q(2x) \\ \varphi_q(-2x) & \varphi_q(0) \end{bmatrix}$ gives

$$\varphi_q(0)^2 - \varphi_q(2x)\varphi_q(-2x) = |\psi(q)|^4 - |\psi(q+x)|^2|\psi(q-x)|^2 \geq 0,\ x \in F,$$

which is (3.7.2). It is easy to see that (3.7.2) and (3.7.3) are equivalent thanks to 2-regularity and we can apply the latter to get

$$\begin{aligned}|\varphi_q(2^{-1}(x+y))|^2 &= |\psi(q+2^{-2}(x+y))|^2 \times |\psi(q-2^{-2}(x+y))|^2 \\ &\geq |\psi(q+2^{-1}x)||\psi(q+2^{-1}y)| \times |\psi(q-2^{-1}x)||\psi(q-2^{-1}y)| \\ &= |\varphi_q(x)|\,|\varphi_q(y)|, \quad q,x,y \in F.\end{aligned}$$

□

The above lemma has an immediate consequence, which will be crucial for the proof of the main theorem.

Corollary 3.7.5. *Suppose $\psi \in L^2(F)$ is continuous and non-zero with $\mathcal{W}_\psi \geq 0$. The set $\operatorname{supp}\psi$ is balanced (i.e. $x, y \in \operatorname{supp}\psi$ implies $2^{-1}(x+y) \in \operatorname{supp}\psi$) and contains a coset of a compact open subgroup of F. Moreover, $|\psi|$ is constant on any such coset.*

Proof. The set $\operatorname{supp}\psi$ is obviously balanced from the inequality (3.7.3). Since ψ is continuous and not identically zero, $\operatorname{supp}\psi$ is a nonempty open set and the second assertion follows by Proposition 3.7.1. For the last statement we consider a compact open subgroup K of F and $x \in F$ with $x + K \subseteq \operatorname{supp}\psi$. The function $|\psi|$ achieves a minimum $m_x > 0$ on $x + K$, say at x_m, by continuity. However, (3.7.2) implies that

$$m_x^2 = |\psi(x_m)|^2 \geq |\psi(x_m+y)||\psi(x_m-y)| \geq m_x^2, \quad y \in K,$$

which forces $|\psi(x_m+y)| = |\psi(x_m-y)| = m_x$ for all $y \in K$. Since $x_m + K = x + K$, this means that $|\psi| \equiv m_x$ on $x + K$. □

The next is the most important step towards the proof of Theorem 3.7.2. It says that the function $|\psi|$ is constant on its support, which happens to be a coset of a compact open 2-regular subgroup of F.

Lemma 3.7.6. *If $\psi \in L^2(F)$ is a continuous state and $\mathcal{W}_\psi \geq 0$, then there* *exist $x_0 \in F$ and a compact open 2-regular subgroup K of F such that*

$$|\psi| = \mu_F(K)^{-1/2} 1_{x_0+K} \tag{3.7.5}$$

For the proof of Lemma 3.7.6 we consider the following subsets of F:

$$\begin{aligned} K_q &:= \left\{x \in F : |\varphi_q(x)| = \varphi_q(0) = |\psi(q)|^2\right\}, \\ K_q^\epsilon &:= \{x \in F : |\varphi_q(x)| \geq \epsilon\}, \\ L_q &:= \{x \in F : |\varphi_q(x)| > 0\} = \left\{x \in F : q \pm 2^{-1}x \in \operatorname{supp}\psi\right\}, \end{aligned} \tag{3.7.6}$$

for continuous $\psi \in L^2(F)$ with $\mathcal{W}_\psi \geq 0$, $q \in F$ and $\epsilon > 0$. It is obvious that

$$K_q \subset K_q^\epsilon \subset L_q = \bigcup_{\epsilon>0} K_q^\epsilon$$

for $q \in \operatorname{supp}\psi$ and $0 < \epsilon < |\psi(q)|^2$. The following lemma shows that the three sets are actually identical.

Lemma 3.7.7. *If $q \in \operatorname{supp}\psi$ for continuous $\psi \in L^2(F)$ with $\mathcal{W}_\psi \geq 0$, then K_q is a 2-regular compact open subgroup of F, and $K_q = K_q^\epsilon = L_q$ for $0 < \epsilon < |\psi(q)|^2$.*

Proof. We first check that K_q is a compact open subgroup. Proposition 2.1.1 says that K_q is a closed subgroup. Since $\operatorname{supp}\psi$ is an open set containing q there is a compact open subgroup K such that $q+K \subset \operatorname{supp}\psi$ by Proposition 3.7.1. Then $2K \subset K_q$ by the fact that $|\psi| \equiv |\psi(q)|$ on $q+K$ (Corollary 3.7.5) and by the definition of φ_q. Since $2K$ is open (F being 2-regular), K_q has nonempty interior, and is therefore clopen. Moreover, as $\varphi_q \in L^1(F)$, we have

$$\mu_F(K_q)\varphi_q(0) = \int_{K_q} |\varphi_q(x)| dx \leq \|\varphi_q\|_{L^1(F)} < \infty.$$

Consequently, $\mu_F(K_q) < \infty$, which means K_q is compact.

Let us move our attention to K_q^ϵ, $\epsilon \in (0, |\psi(q)|^2)$, a nonempty closed subset of F. By Proposition 2.1.1(2), $|\varphi_q|$ is constant on the cosets of K_q, so that

$$x + K_q \subset K_q^\epsilon \text{ for any } x \in K_q^\epsilon. \tag{3.7.7}$$

Thus, K_q^ϵ is a union of cosets of K_q, and in particular, is open. Moreover, we can observe that K_q^ϵ is actually a finite union of cosets of K_q, i.e.

$$K_q^\epsilon = \bigcup_{i=1}^n (x_i + K_q), \ \ x_i \in K_q^\epsilon, \ 1 \leq i \leq n. \tag{3.7.8}$$

Indeed, we have

$$\mu_F(K_q^\epsilon) \leq \epsilon^{-1} \int_{K_q^\epsilon} |\varphi_q(x)| dx \leq \epsilon^{-1} \|\varphi_q\|_{L^1(F)} < \infty,$$

which gives us the observation since cosets are disjoint with the same (non-zero) Haar measure as K_q.

Now let us show that K_q^ϵ is a subgroup of F. The fact that K_q^ϵ is closed under the inversion $x \mapsto -x$ comes from $|\varphi_q(x)| = |\varphi_q(-x)|$, $x \in F$. In order to show K_q^ϵ is closed under addition, we first observe that K_q^ϵ is closed under the map $x \mapsto 2^{-1}x$ by (3.7.4) with $y = 0$. Thus, it suffices to show that $2K_q^\epsilon \subset K_q^\epsilon$ from the identity $x + y = 2^{-1}(2x + 2y)$. To this end, we only need to check that $2x_k \in K_q^\epsilon$ for $1 \leq k \leq n$. We will focus on the case of x_1 for simplicity. Since K_q^ϵ is closed under the map $x \mapsto 2^{-1}x$ we get a sequence $\{2^{-j}x_1\}_{j=1}^\infty$ in K_q^ϵ. From (3.7.8) we can pick $1 \leq i \leq n$ and $0 \leq j_1 < j_2$ such that $2^{-j_l}x_1 \in x_i + K_q$, $l = 1, 2$. In particular, there exist $y_1, y_2 \in K_q$ such that $2^{-j_l}x_1 = x_i + y_l$, $l = 1, 2$. But then, as $j_2 \geq j_1 + 1$,

$$2^{j_2 - j_1}x_1 = 2^{j_2}x_i + 2^{j_2}y_1 = (x_1 - 2^{j_2}y_2) + 2^{j_2}y_1.$$

Therefore,

$$2x_1 = 2^{-(j_2 - j_1 - 1)}(x_1 - 2^{j_2}(y_2 - y_1)) \in K_q^\epsilon,$$

since $x_1 - 2^{j_2}(y_2 - y_1) \in x_1 + K_q \subset K_q^\epsilon$ and K_q^ϵ is closed under the map $x \mapsto 2^{-1}x$.

So far, we have shown that K_q^ϵ is 2-regular compact open subgroup of F.

Note that we have $q + 2^{-1}K_q^\epsilon = q + K_q^\epsilon \subset \operatorname{supp}\psi$ from the definition of K_q^ϵ and φ_q, which allows us to use Corollary 3.7.5 to get $|\psi| \equiv |\psi(q)|$ on $q + K_q^\epsilon$. Now it follows that $K_q^\epsilon \subset K_q$, and hence $K_q^\epsilon = K_q$.

Finally, $L_q = \bigcup_{\epsilon>0} K_q^\epsilon = K_q$. □

Now we are ready to go back to the proof of Lemma 3.7.6.

Proof of Lemma 3.7.6. We may assume $0 \in \operatorname{supp}\psi$ by considering $\psi_0 = W(x_0, 0)^*\psi = \psi(\cdot + x_0)$ for any chosen $x_0 \in \operatorname{supp}\psi$ if necessary. We claim that $\operatorname{supp}\psi = L_0$, where L_0 is the 2-regular compact open subgroup of F given by (3.7.6) and Lemma 3.7.7. Once the claim is established, we get the desired conclusion directly from Corollary 3.7.5 and the condition $\|\psi\|_{L^2(F)} = 1$.

For the claim we recall the fact

$$(*)\ \ y \in L_q \Leftrightarrow q \pm 2^{-1}y \in \operatorname{supp}\psi.$$

We begin with $x \in L_0$, then we have $2x \in L_0 \Leftrightarrow \pm x \in \operatorname{supp}\psi$ by $(*)$ with $q = 0$. This gives us the inclusion $L_0 \subset \operatorname{supp}\psi$. For the converse we consider $x \in \operatorname{supp}\psi$. Corollary 3.7.5 says that $\operatorname{supp}\psi$ is balanced, then we have $2^{-1}x \in \operatorname{supp}\psi$ from the assumption $0 \in \operatorname{supp}\psi$. Now we apply $(*)$ with $q = 0$ and the fact that L_0 is a group to get $2^{-1}x \pm 2^{-1}x \in \operatorname{supp}\psi$, which is equivalent to $x \in L_{2^{-1}x}$ by $(*)$ with $q = 2^{-1}x$. Since $L_{2^{-1}x}$ is also a group by Lemma 3.7.7, we have $2x \in L_{2^{-1}x}$ and therefore $-2^{-1}x = 2^{-1}x - x \in \operatorname{supp}\psi$ by $(*)$ with $q = 2^{-1}x$, which means that $x \in L_0$ by $(*)$ with $q = 0$. □

We finally complete the proof of Theorem 3.7.2.

Proof of Theorem 3.7.2. (2) $\Rightarrow$ (1): Starting from (3.7.5) of Lemma 3.7.6, we have

$$|\varphi_q(x)| = \mu_F(K)^{-1}1_{x_0+K}(q+2^{-1}x)1_{x_0+K}(q-2^{-1}x) = \mu_F(K)^{-1}1_{x_0+K}(q)1_K(x),$$

where we used the 2-regularity of K in the last equality. Moreover, since φ_q

is continuous and positive definite on K, Proposition 2.1.1(2) implies that

$$\varphi_q(x) = \mu_F(K)^{-1} 1_{x_0+K}(q) 1_K(x) \gamma_q(x) \tag{3.7.9}$$

for some $\gamma_q \in \widehat{K}$. Therefore, we get the Wigner function

$$\mathcal{W}_\psi(q,p) = \widehat{\varphi_q}^F(p) = 1_{x_0+K}(q) 1_{K^\perp}(p - \widetilde{\gamma}_q),$$

where $\tilde{\gamma}_q \in \widehat{F}$ is any extension of γ_q. Here, we use the fact that characters on a closed subgroup can be extended to a character on the whole group [RS00, Theorem 4.2.14]. Now, by considering $\psi_0 := W(x_0, \widetilde{\gamma}_0)^* \psi$ combined with (3.2.8), we may assume that $x_0 = 0$ and $\gamma_0 \equiv 1$.

Going back to (3.7.5) we can write

$$\psi(x) = \mu_F(K)^{-1/2} 1_K(x) \alpha(x)$$

for some continuous function α on K with $|\alpha| \equiv 1$, which gives us

$$\varphi_q(x) = \mu_F(K)^{-1} 1_K(q) 1_K(x) \alpha(q + 2^{-1}x) \overline{\alpha(q - 2^{-1}x)}, \ x \in F. \tag{3.7.10}$$

Comparing (3.7.9) and (3.7.10) (under the condition $x_0 = 0$), we have

$$\alpha(q + 2^{-1}x) \overline{\alpha(q - 2^{-1}x)} = \gamma_q(x), \ \ q, x \in K. \tag{3.7.11}$$

However, the condition $\gamma_0 \equiv 1$ implies that $\alpha(2^{-1}x) = \alpha(-2^{-1}x)$ for all $x \in K$, which means α is symmetric thanks to 2-regularity of K. Therefore,

$$\begin{aligned}
\gamma_q(x) &= \alpha(2^{-1}x + q) \overline{\alpha(2^{-1}x - q)} \\
&= \gamma_{2^{-1}x}(2q) = (\gamma_{2^{-1}x}(q))^2 \\
&= \left(\alpha(2^{-1}(x+q)) \overline{\alpha(2^{-1}(x-q))}\right)^2 \\
&= \left(\alpha(2^{-1}(q+x)) \overline{\alpha(2^{-1}(q-x))}\right)^2 \\
&= \gamma_x(q), \ \ q, x \in K.
\end{aligned}$$

Consequently, we get a symmetric bicharacter $\beta : K \times K \to \mathbb{T}$, $(q, x) \mapsto \gamma_q(x)$ introduced in Section 3.4.3. From the condition (3.7.11) we can easily see that $\alpha(x) = \beta(x, 2^{-1}x)$, $x \in K$, which is the conclusion we wanted as in (3.4.6). $\square$

Question 3.7.8. Can we further generalize the Hudson theorem over 2-regular LCA group with compact open subgroups?

Remark 3.7.9. Note that the original Hudson's theorem [Hud74] and its higher dimensional generalization [SC83] do not assume the continuity of the vector state $\psi \in L^2(\mathbb{R}^n)$. It can be deduced form the single assumption $\mathcal{W}_\psi \geq 0$ a.e..

On the other hand, a corresponding result on the angle-number system in 1-mode has been proved in [RSSK$^+$10]. A careful inspection of the proof reveals that an implicit assumption of the continuity of $\psi \in L^2(F)$ is made in [RSSK$^+$10]. It is not clear whether we could remove the continuity of $\psi \in L^2(F)$ from the assumption in both of the cases at the time of this writing.

Chapter 4

Mapping cone and compact group symmetry

The notion of mapping cones was introduced by Størmer [Sr86] to study extension problems of positive linear maps, and later developed in many directions [SSrZ09, Sko11, Sr12, GKS21, Kye23a]. There are two characteristics of mapping cones: (1) they contain sufficiently many classes important in QIT, (2) they can be described via *duality* in many different ways. In this chapter, we introduce definitions related to this concept, and we develop a theory of operators and linear maps under *compact group symmetry*. In particular, we show that many dualities between mapping cones carry over into the general framework of compact group symmetry. This directly leads to two applications in quantum information theory: (1) the optimization of entanglement witnesses and Schmidt number witnesses, and (2) the equivalence between the problem of *PPT=separability* and the problem of checking whether every extremal positive map is completely positive or completely copositive under compact group symmetry.

We refer to Section 2.1.2 for preliminaries on representation of compact groups and Section 2.2 for basic notions related to quantum entanglement and positive linear maps.

4.1 General theory of mapping cones

Let us briefly recall several notions in convex analysis and the theory of mapping cone. First, $B^h(B(H_A), B(H_B))$ is a real vector space equipped with an inner product

$$\langle \Phi, \Psi \rangle := \mathrm{Tr}(C_\Phi^* C_\Psi) = \mathrm{Tr}(C_\Phi C_\Psi). \tag{4.1.1}$$

For a subset $\mathcal{K} \subset B^h(B(H_A), B(H_B))$, we define the *dual cone* $\mathcal{K}^\circ$ of $\mathcal{K}$ by

$$\mathcal{K}^\circ := \left\{ \Phi \in B^h(B(H_A), B(H_B)) : \langle \Phi, \Psi \rangle \geq 0 \; \forall \, \Psi \in \mathcal{K} \right\}. \tag{4.1.2}$$

It is well-known in convex analysis [Roc70] that $\mathcal{K}^{\circ\circ}$ is the smallest closed convex cone containing $\mathcal{K}$. In particular, $\mathcal{K}$ is a closed convex cone if and only if $\mathcal{K}^{\circ\circ} = \mathcal{K}$. Moreover, for two closed convex cones $\mathcal{K}_1, \mathcal{K}_2 \subset B^h(B(H_A), B(H_B))$, we have

$$(\mathcal{K}_1 \vee \mathcal{K}_2)^\circ = \mathcal{K}_1^\circ \wedge \mathcal{K}_2^\circ \quad \text{and} \quad (\mathcal{K}_1 \wedge \mathcal{K}_2)^\circ = \mathcal{K}_1^\circ \vee \mathcal{K}_2^\circ, \tag{4.1.3}$$

where $\mathcal{K}_1 \vee \mathcal{K}_2 := \mathrm{conv}(\mathcal{K}_1 \cup \mathcal{K}_2)$ and $\mathcal{K}_1 \wedge \mathcal{K}_2 := \mathcal{K}_1 \cap \mathcal{K}_2$.

Following [Sr86, Sko11], a closed convex cone $\mathcal{K} \subset \mathcal{POS}_{AB}$ is called a *mapping cone* if it is invariant under the compositions by CP maps, i.e.,

$$\mathcal{CP}_{BB} \circ \mathcal{K} \circ \mathcal{CP}_{AA} \subset \mathcal{K}, \tag{4.1.4}$$

where $\mathcal{K}_1 \circ \mathcal{K}_2 := \{\Phi \circ \Psi : \Phi \in \mathcal{K}_1, \; \Psi \in \mathcal{K}_2\}$. Since the identity maps $\mathrm{id}_A, \mathrm{id}_B$ are CP maps, (4.1.4) is equivalent to $\mathcal{CP}_{BB} \circ \mathcal{K} \circ \mathcal{CP}_{AA} = \mathcal{K}$.

There are some important aspects on the study of mapping cones. First, if $\mathcal{K}, \mathcal{K}_1, \mathcal{K}_2$ are mapping cones, then so are

$$\mathcal{K}^\circ, \;\; \top_B \circ \mathcal{K}, \;\; \mathcal{K} \circ \top_A, \;\; \mathcal{K}^* := \{\mathcal{L}^* : \mathcal{L} \in \mathcal{K}\}, \;\; \mathcal{K}_1 \vee \mathcal{K}_2, \;\; \mathcal{K}_1 \wedge \mathcal{K}_2.$$

See [Sko11, GKS21] for proofs. Second, all the classes

$$\mathcal{POS}, \mathcal{POS}_k, \mathcal{CP}, \mathcal{SP}_k, \mathcal{EB}, \mathcal{PPT}, \mathcal{DEC} \tag{4.1.5}$$

introduced in Section 2.2.2 are mapping cones, and the associated subset $C_{\mathcal{K}} := \{C_{\mathcal{L}} : \mathcal{L} \in \mathcal{K}\}$ of the Choi matrices and the dual cone $\mathcal{K}^\circ$ are exhibited in Table 4.1 below.

Table 4.1: Mapping cones, Choi correspondences, and dual cones

$\mathcal{K}$	$\mathcal{POS}$	$\mathcal{POS}_k$	$\mathcal{CP}$	$\mathcal{SP}_k$	$\mathcal{EB}$	$\mathcal{PPT}$	$\mathcal{DEC}$
$C_{\mathcal{K}}$	$\mathbf{BP}$	$\mathbf{BP}_k$	$\mathbf{P}$	$\mathbf{Sch}_k$	$\mathbf{SEP}$	$\mathbf{PPT}$	$\mathbf{DEC}$
$\mathcal{K}^\circ$	$\mathcal{EB}$	$\mathcal{SP}_k$	$\mathcal{CP}$	$\mathcal{POS}_k$	$\mathcal{POS}$	$\mathcal{DEC}$	$\mathcal{PPT}$

Let us focus more on direct connections between the Choi correspondences $C_{\mathcal{K}}$ and the dual cones $\mathcal{K}^\circ$. A natural pairing between Hermitian operators $X \in B^h(H_{AB})$ and Hermitian-preserving linear maps $\mathcal{L} \in B^h(B(H_A), B(H_B))$ is given by

$$\langle X, \mathcal{L}\rangle := \mathrm{Tr}(C_{\mathcal{L}} X) = \langle \Omega_A | (\mathrm{id}_A \otimes \mathcal{L}^*)(X) | \Omega_A\rangle. \tag{4.1.6}$$

Then an extended form of the famous *Horodecki criterion* for general mapping cones $\mathcal{K} \subseteq \mathcal{POS}_{A,B}$ is given as follows with respect to the pairing in (4.1.6).

Proposition 4.1.1. *[GKS21, Proposition 4.1] Suppose that a closed convex cone $\mathcal{K} \subset B^h(B(\mathcal{H}_A), B(\mathcal{H}_B))$ satisfies $\mathcal{K} \circ \mathcal{CP}_{AA} \subset \mathcal{K}$. Then the following are equivalent for a linear map $\mathcal{L} \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$:*

1. *$\mathcal{L} \in \mathcal{K}$,*
2. *$(\mathrm{id}_A \otimes \mathcal{L}^*)(X) \in \mathbf{P}_{AA}$ for every $X \in C_{K^\circ}$.*
3. *$\langle X, \mathcal{L}\rangle \geq 0$ for every $X \in C_{\mathcal{K}^\circ}$.*

Moreover, the following are equivalent for an operator $X \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$:

1. $X \in C_{\mathcal{K}}$,
2. $(\mathrm{id}_A \otimes \mathcal{L}^*)(X) \in \mathbf{P}_{AA}$ *for every* $\mathcal{L} \in \mathcal{K}^\circ$,
3. $\langle X, \mathcal{L} \rangle \geq 0$ *for every* $\mathcal{L} \in \mathcal{K}^\circ$.

Note that Proposition 4.1.1 can be applied for arbitrary mapping cone $\mathcal{K}$. For example, the *Horodecki criterion* is for a special case $C_{\mathcal{K}} = \mathbf{SEP}$ and $\mathcal{K}^\circ = \mathcal{POS}$, and it was used to study separability of quantum states [HHH96]. Furthermore, Proposition 4.1.1 has been applied to study quantum states with an upper bound on the Schmidt numbers [TH00], decomposable maps [Sr82], k-positive maps [EK00, TH00], and k-superpositive maps [SSrZ09], etc.

4.2 Group symmetry methods

4.2.1 Compact group symmetry and Twirling operations

In this section, we introduce two important objects to discuss conservation of symmetry, namely *invariant operators* and *covariant linear maps*. Let us suppose that G is a compact group throughout this section. Recall from Section 2.1.2 that for a unitary representation $\pi : G \to \mathcal{U}(\mathcal{H})$ of G, we call $X \in B(\mathcal{H})$ π*-invariant* if

$$\pi(x) X \pi(x)^* = X \tag{4.2.1}$$

for all $x \in G$, and the set of π-invariant operators in $B(\mathcal{H})$ are denoted by $\mathrm{Inv}(\pi)$. While invariance can be regarded as a compact group symmetry for operators, another type of symmetry for linear maps is called covariance. More precisely, for unitary representations $\pi_A : G \to B(\mathcal{H}_A)$ and $\pi_B : G \to B(\mathcal{H}_B)$, a linear map $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is called (π_A, π_B)*-covariant* if

$$\mathcal{L}(\pi_A(x) Y \pi_A(x)^*) = \pi_B(x) \mathcal{L}(Y) \pi_B(x)^* \tag{4.2.2}$$

for all $x \in G$ and $Y \in B(\mathcal{H}_A)$, and let us denote by $\mathrm{Cov}(\pi_A, \pi_B)$ the space of all (π_A, π_B)-covariant linear maps.

An averaging technique called the *twirling operation* is a standard method to analyze invariant operators and covariant linear maps. First of all, we can choose the Haar measure μ_G of G by the probability measure, i.e., $\mu_G(G) = 1$, and μ_G is always *unimodular* (i.e., left- and right-invariant). Let us simply write $d\mu_G(x) = dx$. Then the π-*twirling map* $\mathcal{T}_\pi : B(\mathcal{H}) \to \mathrm{Inv}(\pi)$ is defined by

$$\mathcal{T}_\pi(X) = \int_G \pi(x) X \pi(x)^* dx \tag{4.2.3}$$

for all $X \in B(\mathcal{H})$. Note that the integration is well-defined in terms of Bochner integral since $\|\pi(x)X\pi(x)^*\| = \|X\|$ for all x, and the translation-invariance property of the Haar measure guarantees that $\mathcal{T}_\pi(X) \in \mathrm{Inv}(\pi)$ for all $X \in B(\mathcal{H})$. Moreover, $\mathcal{T}_\pi : B(H) \to \mathrm{Inv}(\pi)$ is unital, $\|\mathcal{T}_\pi(X)\| \leq \|X\|$ for all $X \in B(\mathcal{H})$, and $X \in \mathrm{Inv}(\pi)$ if and only if $\mathcal{T}_\pi(X) = X$ (necessity is clear, and for sufficiency we again use the translation-invariance of the Haar measure to show that $\mathcal{T}_\pi \circ \mathcal{T}_\pi = \mathcal{T}_\pi$). Therefore, $\mathcal{T}_\pi$ is a projection (more precisely, a *conditional expectation* [Tak02, Definition 3.3]) onto the von Neumann subalgebra $\mathrm{Inv}(\pi)$ of $B(\mathcal{H})$.

For unitary representations $\pi_A : G \to \mathcal{U}(\mathcal{H}_A)$ and $\pi_B : G \to \mathcal{U}(\mathcal{H}_B)$, the twirling $\mathcal{T}_{\pi_A,\pi_B}\mathcal{L}$ of $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is defined by

$$(\mathcal{T}_{\pi_A,\pi_B}\mathcal{L})(X) = \int_G \pi_B(x)^* \mathcal{L}(\pi_A(x) X \pi_A(x)^*) \pi_B(x)\, dx \tag{4.2.4}$$

for all $X \in B(\mathcal{H}_A)$. Then similarly, the twirling operation $\mathcal{T}_{\pi_A,\pi_B}$ is a well-defined projection from $B(B(\mathcal{H}_A), B(\mathcal{H}_B))$ onto $\mathrm{Cov}(\pi_A, \pi_B)$.

Let us collect some useful properties of the twirling operations.

Proposition 4.2.1. *For any unitary representations π_A and π_B of G, the twirling map $\mathcal{T}_{\pi_A \otimes \pi_B}$ preserves separability and PPT property of bipartite operators. Furthermore, the twirling operation $\mathcal{T}_{\pi_A,\pi_B}$ preserves positivity, CP, TP, CCP, PPT, decomposability, and EB property of linear maps.*

Proof. It is straightforward from the definitions and closedness of the spaces associated with each of the properties mentioned above. For example, the set of all decomposable linear maps $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ is closed in $B(B(\mathcal{H}_A), B(\mathcal{H}_B))$ with respect to the natural (Euclidean) topology. □

For a linear map $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$, the *adjoint map* $\mathcal{L}^* : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ of $\mathcal{L}$ is a linear map satisfying

$$\mathrm{Tr}(\mathcal{L}(X)\, Y) = \mathrm{Tr}(X\, \mathcal{L}^*(Y)) \tag{4.2.5}$$

for all $X \in B(\mathcal{H}_A)$ and $Y \in B(\mathcal{H}_B)$. Recall that the adjoint operation $\mathcal{L} \mapsto \mathcal{L}^*$ preserves positivity, CP, CCP, PPT, and decomposability.

Proposition 4.2.2. *Let $\pi : G \to \mathcal{U}(H)$, $\pi_A : G \to \mathcal{U}(\mathcal{H}_A)$ and $\pi_B : G \to \mathcal{U}(\mathcal{H}_B)$ be unitary representations of G. Then we have the following.*

1. *$Tr((\mathcal{T}_\pi X)\, Y) = Tr(X(\mathcal{T}_\pi Y))$ for any $X, Y \in B(H)$.*
2. *$\mathcal{T}_{\pi_A \otimes \pi_B} \circ (\top_A \otimes \mathrm{id}_B) = (\top_A \otimes \mathrm{id}_B) \circ \mathcal{T}_{\overline{\pi_A} \otimes \pi_B}$ where $\top_A$ is the transpose on $B(\mathcal{H}_A)$.*
3. *$(\mathcal{T}_{\pi_A, \pi_B} \mathcal{L})^* = \mathcal{T}_{\pi_B, \pi_A}(\mathcal{L}^*)$ for any linear map $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$.*
4. *The Choi matrix of $\mathcal{T}_{\pi_A, \pi_B} \mathcal{L}$ is given by $\mathcal{T}_{\overline{\pi_A} \otimes \pi_B}(C_{\mathcal{L}})$ for any linear map $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$.*

Proof. (1) Since the Haar measure on the compact group G is invariant under the inverse $x \mapsto x^{-1}$, we have

$$\mathrm{Tr}((\mathcal{T}_\pi X)\, Y) = \int_G \mathrm{Tr}(\pi(x) X \pi(x^{-1}) Y) dx \tag{4.2.6}$$

$$= \mathrm{Tr}\left(X \int_G \pi(x^{-1}) Y \pi(x) dx \right) \tag{4.2.7}$$

$$= \mathrm{Tr}\left(X \int_G \pi(x) Y \pi(x^{-1}) dx \right) = \mathrm{Tr}(X(\mathcal{T}_\pi Y)) \tag{4.2.8}$$

for any $X, Y \in B(H)$.

(2) It suffices to show the equality for product operators $X = P \otimes Q$, and the conclusion follows immediately from the observation

$$\pi_A(x)P^T\pi_A(x)^* = \left(\overline{\pi_A(x)}P\pi_A(x)^T\right)^T. \tag{4.2.9}$$

(3) For any $X \in B(\mathcal{H}_A)$ and $Y \in B(\mathcal{H}_B)$, we have

$$\begin{aligned}
&\mathrm{Tr}(X\,(\mathcal{T}_{\pi_B,\pi_A}\mathcal{L}^*)\,(Y)) && (4.2.10)\\
&= \int_G \mathrm{Tr}(X\pi_A(x)^*\mathcal{L}^*(\pi_B(x)Y\pi_B(x)^*)\pi_A(x))dx && (4.2.11)\\
&= \int_G \mathrm{Tr}(\pi_B(x)^*\mathcal{L}(\pi_A(x)X\pi_A(x)^*)\pi_B(x)\,Y)dx && (4.2.12)\\
&= \mathrm{Tr}((\mathcal{T}_{\pi_A,\pi_B}\mathcal{L})\,(X)\,Y), && (4.2.13)
\end{aligned}$$

which gives us the desired conclusion.

(4) First of all, note that

$$\begin{aligned}
&\sum_{i,j=1}^{d_A}(\overline{\pi_A(x)}e_{ij}\pi_A(x)^T)\otimes(\pi_B(x)\mathcal{L}(e_{ij})\pi_B(x)^*) && (4.2.14)\\
&= \sum_{i,j=1}^{d_A} e_{ij}\otimes(\pi_B(x)\mathcal{L}(\pi_A(x)^*e_{ij}\pi_A(x))\pi_B(x)^*). && (4.2.15)
\end{aligned}$$

for each $x \in G$. Indeed, the LHS (4.2.14) can be understood as

$$d_A(\mathrm{id}_A \otimes (\mathrm{Ad}_{\pi_B(x)} \circ \mathcal{L}))\left((\overline{\pi_A(x)} \otimes \mathrm{id}_A)|\Omega_A\rangle\langle\Omega_A|(\pi_A(x)^T \otimes \mathrm{id}_A)\right), \tag{4.2.16}$$

and the RHS (4.2.15) can be understood as

$$d_A(\mathrm{id}_A \otimes (\mathrm{Ad}_{\pi_B(x)} \circ \mathcal{L}))\left((\mathrm{id}_A \otimes \pi_A(x)^*)|\Omega_A\rangle\langle\Omega_A|(\mathrm{id}_A \otimes \pi_A(x))\right) \tag{4.2.17}$$

where $\mathrm{Ad}_V(Y) = VYV^*$. Moreover, the so-called *ricochet property*

$$(X \otimes \mathrm{id}_A)|\Omega_A\rangle = (\mathrm{id}_A \otimes X^T)|\Omega_A\rangle, \quad X \in B(\mathcal{H}_A), \tag{4.2.18}$$

implies (4.2.16) = (4.2.17). Finally, taking the Haar integral on both sides completes the proof. □

Combining Proposition 4.2.2 (2), (3), and (4) with the fact that both $\mathrm{Inv}(\pi_A \otimes \pi_B)$ and $\mathrm{Cov}(\pi_A, \pi_B)$ are the images of the twirling projections, we obtain the following useful properties.

Corollary 4.2.3. *Let $X \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a bipartite operator and $\mathcal{L} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ be a linear map. Then*

1. *$X \in \mathrm{Inv}(\pi_A \otimes \pi_B)$ if and only if $(\top_A \otimes id)(X) \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)$.*
2. *$\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$ if and only if $\mathcal{L}^* \in \mathrm{Cov}(\pi_B, \pi_A)$.*
3. *$\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$ if and only if $C_{\mathcal{L}} \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)$.*

Remark 4.2.4. The results in Corollary 4.2.3 have been noted in various contexts, [EW01, Lemma 6], [GBW21, Lemma 11], and [LY22, Proposition 5.1, Theorem 3.5] for examples. Moreover, extendibility to more general contexts of compact quantum group symmetry was proved in [LY22].

We can even write an explicit formula of $\mathcal{T}_\pi$ when $\pi \cong \bigoplus_{i=1}^{l} \sigma_i \otimes I_{m_i}$ is a finite-dimensional unitary representation as before, so that the relation (2.1.6) holds. Indeed, we can further show that $\mathcal{T}_\pi$ is trace-preserving (TP). Note that for any finite-dimensional von Neumann subalgebra $\mathcal{M}$ of M_d, there is a unique TP conditional expectation of M_d onto $\mathcal{M}$ [BO08, Lemma 1.5.11]. For example, the map $X \in M_n \otimes M_m \mapsto \frac{1}{n}(I_n \otimes \mathrm{Tr}_n)(X)$ is the unique TP conditional expectation onto $\mathcal{M} = I_n \otimes M_m$. This observation allows us to get the following explicit formula of the twirling map $\mathcal{T}_\pi$ for the case $\mathcal{M} = \mathrm{Inv}(\pi)$.

Proposition 4.2.5. *In (2.1.6), let Π_i be the orthogonal projection from H onto $H_i \cong \mathbb{C}^{n_i} \otimes \mathbb{C}^{m_i}$. Then the twirling $\mathcal{T}_\pi(X)$ of $X \in B(H)$ is given by*

$$\mathcal{T}_\pi(X) = \bigoplus_{i=1}^{l} \frac{1}{n_i} I_{n_i} \otimes \mathrm{Tr}_{n_i}(\Pi_i X \Pi_i). \tag{4.2.19}$$

In particular, if the irreducible decomposition of π is multiplicity-free, i.e., if $m_i \equiv 1$ for all $i = 1, 2, \cdots, l$, then

$$\mathcal{T}_\pi(X) = \sum_{i=1}^{l} \frac{\mathrm{Tr}(\Pi_i X)}{n_i} \Pi_i. \tag{4.2.20}$$

4.2.2 Duality between mapping cones under compact group symmetry

From now on, we describe how the duality results between mapping cones can be naturally carried over into our framework of compact group symmetry.

Lemma 4.2.6. *Let π_A, π_B be two unitary representations of G. For two linear maps $\Phi, \Psi \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$, we have*

$$\langle \mathcal{T}_{\pi_A,\pi_B}\Phi, \Psi\rangle = \langle \Phi, \mathcal{T}_{\pi_A,\pi_B}\Psi\rangle. \tag{4.2.21}$$

Moreover, for an operator $X \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ and a linear map $\mathcal{L} \in B(B(\mathcal{H}_A), B(\mathcal{H}_B))$, we have

$$\langle \mathcal{T}_{\overline{\pi_A}\otimes\pi_B} X, \mathcal{L}\rangle = \langle X, \mathcal{T}_{\pi_A,\pi_B}\mathcal{L}\rangle. \tag{4.2.22}$$

Proof. Both two assertions follow from Proposition 4.2.2. More precisely, we have

$$\begin{aligned}\langle \mathcal{T}_{\pi_A,\pi_B}\Phi, \Psi\rangle &= \mathrm{Tr}((C_{(\mathcal{T}_{\pi_A,\pi_B}\Phi)})^* C_\Psi) = \mathrm{Tr}((\mathcal{T}_{\overline{\pi_A}\otimes\pi_B} C_\Phi)^* C_\Psi) \\ &= \mathrm{Tr}(C_\Phi^* \mathcal{T}_{\overline{\pi_A}\otimes\pi_B} C_\Psi) = \mathrm{Tr}(C_\Phi^* C_{(\mathcal{T}_{\pi_A,\pi_B}\Psi)}) = \langle \Phi, \mathcal{T}_{\pi_A,\pi_B}\Psi\rangle\end{aligned}$$

which yields (4.2.21). The proof of (4.2.22) is similar. □

Let us use the following notations

$$\begin{aligned}\mathrm{Inv}(\pi)^{\mathbf{S}} &:= \mathrm{Inv}(\pi) \cap \mathbf{S}, \\ \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}} &:= \mathrm{Cov}(\pi_A, \pi_B) \cap \mathcal{K}.\end{aligned}$$

for any subsets $\mathbf{S} \subset B(H)$ and $\mathcal{K} \subset B(B(\mathcal{H}_A), B(\mathcal{H}_B))$. For example, the subset $\mathrm{Inv}(\pi)^{\mathcal{D}} = \mathrm{Inv}(\pi) \cap \mathcal{D}(H)$ is the set of π-invariant quantum states. Recall that positivity, complete positivity, and EB property are preserved under twirling operation $\mathcal{L} \mapsto \mathcal{T}_{\pi_A,\pi_B}\mathcal{L}$ [PJPY23, Proposition 2.1]. This leads us to the question of which class $\mathcal{K}$ of linear maps is invariant under the twirling operation, i.e., $\mathcal{T}_{\pi_A,\pi_B}\mathcal{K} \subset \mathcal{K}$. The following Proposition 4.2.7 implies that this property holds whenever $\mathcal{K}$ is a mapping cone.

Proposition 4.2.7. *For a closed convex cone $\mathcal{K} \in B^h(B(\mathcal{H}_A), B(\mathcal{H}_B))$, the following are equivalent:*

1. $\mathcal{T}_{\pi_A,\pi_B}\mathcal{K} \subset \mathcal{K}$,
2. $\mathcal{T}_{\pi_A,\pi_B}(\mathcal{K}^\circ) \subset \mathcal{K}^\circ$,
3. $\mathcal{T}_{\pi_B,\pi_A}(\mathcal{K}^*) \subset \mathcal{K}^*$,
4. $\mathcal{T}_{\overline{\pi_A}\otimes\pi_B} C_{\mathcal{K}} \subset C_{\mathcal{K}}$.

In this case, we have $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}}} = \mathcal{T}_{\overline{\pi_A}\otimes\pi_B} C_{\mathcal{K}}$ *and* $\mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}} = \mathcal{T}_{\pi_A,\pi_B}\mathcal{K}$. *Moreover, the above conditions hold if $\mathcal{CP}_{BB} \circ \mathcal{K} \circ \mathcal{CP}_{AA} \subset \mathcal{K}$.*

Proof. The equivalence (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) is a direct result of Proposition 4.2.2. For (1) $\Rightarrow$ (2), observe that for $\Phi \in \mathcal{K}^\circ$ and $\Psi \in \mathcal{K}$,

$$\langle \mathcal{T}_{\pi_A,\pi_B}\Phi, \Psi\rangle = \langle \Phi, \mathcal{T}_{\pi_A,\pi_B}\Psi\rangle \geq 0$$

under the assumption $\mathcal{T}_{\pi_A,\pi_B}\mathcal{K} \subset \mathcal{K}$. The other direction (2) $\Rightarrow$ (1) follows from (1) $\Rightarrow$ (2) since $\mathcal{K}^{\circ\circ} = \mathcal{K}$.

The second statement is also clear from the properties $\mathcal{T}_{\overline{\pi_A}\otimes\pi_B} \circ \mathcal{T}_{\overline{\pi_A}\otimes\pi_B} = \mathcal{T}_{\overline{\pi_A}\otimes\pi_B}$ and $\mathcal{T}_{\pi_A,\pi_B} \circ \mathcal{T}_{\pi_A,\pi_B} = \mathcal{T}_{\pi_A,\pi_B}$. For the last assertion, it is enough to note that the twirling operations preserve positivity of linear maps, and that $\mathcal{T}_{\pi_A,\pi_B}\Phi$ is approximated by the convex combination of $\mathrm{Ad}_{\pi_B(x)^*} \circ \Phi \circ \mathrm{Ad}_{\pi_A(x)} \in \mathcal{K}$ for $x \in G$. $\square$

Recall that $\mathcal{K}$ and $C_{\mathcal{K}^\circ}$ determines each other via the generalized Horodecki criterion (Proposition 4.1.1). One of our main results in this section is to establish an analogous result for $\mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}}$ and $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}^\circ}}$ as follows.

Theorem 4.2.8. *Suppose that a closed convex cone $\mathcal{K} \subset B^h(B(\mathcal{H}_A), B(\mathcal{H}_B))$ satisfies $\mathcal{CP}_{BB} \circ \mathcal{K} \circ \mathcal{CP}_{AA} \subset \mathcal{K}$. Then the following are equivalent for a (π_A, π_B)-covariant linear map $\mathcal{L}$:*

1. $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}}$,
2. $(\mathrm{id}_A \otimes \mathcal{L}^*)(X) \in \mathbf{P}_{AA}$ *for every* $X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}^\circ}}$,
3. $\langle X, \mathcal{L} \rangle \geq 0$ *for every* $X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}^\circ}}$.

Moreover, the following are equivalent for a $\overline{\pi_A} \otimes \pi_B$-invariant bipartite operator X:

1. $X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}}}$,
2. $(\mathrm{id}_A \otimes \mathcal{L}^*)(X) \in \mathbf{P}_{AA}$ *for every* $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}^\circ}$,
3. $\langle X, \mathcal{L} \rangle \geq 0$ *for every* $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}^\circ}$.

Proof. Let us prove only the first assertion. Then the other one is analogous. Note that (1) $\Rightarrow$ (2) follows from Proposition 4.1.1 and (2) $\Rightarrow$ (3) is clear from the relation (4.1.6), so it suffices to prove the direction (3) $\Rightarrow$ (1). Since $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$, we have

$$\langle X, \mathcal{L} \rangle = \langle X, \mathcal{T}_{\pi_A, \pi_B} \mathcal{L} \rangle = \langle \mathcal{T}_{\overline{\pi_A} \otimes \pi_B} X, \mathcal{L} \rangle$$

for all $X \in C_{\mathcal{K}^\circ}$ by Lemma 4.2.6. Now $\mathcal{T}_{\overline{\pi_A} \otimes \pi_B} X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}^\circ}}$ by Proposition 4.2.7, so the assumption (3) implies that $\langle X, \mathcal{L} \rangle \geq 0$ for all $X \in C_{\mathcal{K}^\circ}$. Therefore, Proposition 4.1.1 again implies that $\mathcal{L} \in \mathcal{K}$.

□

Note that $\mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}}$ plays as detectors for $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_{\mathcal{K}^\circ}}$ via the pairing, and we can prove that much fewer detectors from $\mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}}$ are enough for the test if $\mathcal{K}$ is a nonzero *mapping cone*, i.e., $\mathcal{K} \subset \mathcal{POS}_{AB}$. Let us start with a compact convex subset

$$\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{K}} := \left\{\Phi \in \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{K}} : \mathrm{Tr}\, C_\Phi = 1\right\}.$$

Now Theorem 4.2.8 implies that the only extreme points of $\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{K}^\circ}$ are enough as detectors for $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_\mathcal{K}}$ since every compact convex set in a finite-dimensional space can be written as a convex hull of its extreme points.

Corollary 4.2.9. *If $\mathcal{K} \subset \mathcal{POS}_{AB}$ is a nonzero mapping cone, then the following are equivalent for $X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)$:*

1. $X \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{C_\mathcal{K}}$,
2. $(\mathrm{id}_A \otimes \mathcal{L}^*)(X) \in \mathbf{P}_{AA}$ *for every* $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{K}^\circ})$,
3. $\langle X, \mathcal{L}\rangle \geq 0$ *for every* $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{K}^\circ})$.

We conclude this section by further examining the structure of the set $\mathrm{Cov}_1(\pi_A, \pi_B)$. The following lemma asserts that under certain mild conditions on π_A and π_B, we can further reduce $\mathrm{Cov}_1(\pi_A, \pi_B)$.

Lemma 4.2.10. 1. *If π_B is irreducible and $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$, then $\mathcal{L}(I_A) = c\, I_B$ for some constant c. In particular,*

$$\mathrm{Cov}_1(\pi_A, \pi_B) = \{\Phi \in \mathrm{Cov}(\pi_A, \pi_B) : \Phi(I_A/d_A) = I_B/d_B\}$$

2. *If π_A is irreducible and $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$, then there is a constant c such that $\mathrm{Tr}(\mathcal{L}(X)) = c\ \mathrm{Tr}(X)$ for every $X \in B(H_A)$. In particular,*

$$\mathrm{Cov}_1(\pi_A, \pi_B) = \{\Phi \in \mathrm{Cov}(\pi_A, \pi_B) : \Phi \textit{ is TP}\}$$

Proof. 1. From the irreducibility of π_B and the identity

$$\pi_B(x)\mathcal{L}(\mathrm{id}_A)\pi_B(x)^* = \mathcal{L}(\pi_A(x)\pi_A(x)^*) = \mathcal{L}(\mathrm{id}_A), \tag{4.2.23}$$

we have $\mathcal{L}(\mathrm{id}_A) \in \mathrm{Inv}(\pi_B) = \mathbb{C} \cdot \mathrm{id}_B$.

2. The adjoint map $\mathcal{L}^*$ is (π_B, π_A)-covariant by Corollary 4.2.3 (2), so $\mathcal{L}^*(\mathrm{Id}_B) = c\,\mathrm{Id}_A$ for some c by (1). In this case, we have

$$\mathrm{Tr}(\mathcal{L}(X)) = \mathrm{Tr}(\mathcal{L}(X)\,\mathrm{Id}_B) = \mathrm{Tr}(X\,\mathcal{L}^*(\mathrm{Id}_B)) = c\,\mathrm{Tr}(X) \tag{4.2.24}$$

for any $X \in B(\mathcal{H}_A)$.

□

For the moment, let us remark that the above lemma allows us to resolve one technical issue on *channel-state duality*: the set of quantum channels from $B(H_A)$ into $B(H_B)$ is not in general identified with the set $\mathcal{D}(H_A \otimes H_B)$ of bipartite quantum states via Choi-Jamiołkowski correspondence. However, when π_A is irreducible, then the Choi correspondence gives one-to-one correspondence between the set $\mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{CPTP}} = \mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{CP}}$ of (π_A, π_B)-covariant quantum channels and the set $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$ of $\overline{\pi_A} \otimes \pi_B$-invariant quantum states (as already noted in [GBW21, Lemma 15]). This leads us to question whether the (reduced) channel-state duality

$$\widetilde{C} : \mathrm{Cov}(\pi_A, \pi_B)^{\mathcal{CPTP}} \to \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}} \tag{4.2.25}$$

is bijective under conditions weaker than the irreducibility of π_A. However, Proposition 4.2.11 shows that this is not possible.

Proposition 4.2.11. *Let $\pi_A : G \to \mathcal{U}(\mathcal{H}_A)$ and $\pi_B : G \to \mathcal{U}(\mathcal{H}_B)$ be unitary representations of G. Then the channel-state duality $\widetilde{C}$ in (4.2.25) is bijective if and only if π_A is irreducible.*

Proof. Let us prove the if part first. For any $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$ there exists completely positive $\mathcal{L} \in \mathrm{Cov}(\pi_A, \pi_B)$ such that $C_{\mathcal{L}} = \rho$ by Corollary 4.2.3 (3). Moreover, $\mathcal{L}$ should be trace-preserving. Indeed, irreducibility of π_A implies that there exists a constant c such that $\mathrm{Tr}(\mathcal{L}(X)) = c\mathrm{Tr}(X)$ for all $X \in$

$B(\mathcal{H}_A)$ by Lemma 4.2.10 (2), and we have

$$c = \frac{c}{d_A}\sum_{i=1}^{d_A}\mathrm{Tr}(e_{ii}) = \frac{1}{d_A}\sum_{i=1}^{d_A}\mathrm{Tr}(e_{ii}\otimes\mathcal{L}(e_{ii})) = \mathrm{Tr}(C_{\mathcal{L}}) = 1. \tag{4.2.26}$$

Conversely, if we assume that $\pi_A = \pi_A^{(1)}\oplus\pi_A^{(2)}$ with $\mathcal{H}_A = \mathcal{H}_A^{(1)}\oplus\mathcal{H}_A^{(2)}$ and if Π_1 is the orthogonal projection from $\mathcal{H}_A$ onto $\mathcal{H}_A^{(1)}$, then we can take a CP non-TP map $\mathcal{L}: B(\mathcal{H}_A)\to B(\mathcal{H}_B)$ given by

$$\mathcal{L}(X) = \frac{d_A}{d_B\cdot\dim\mathcal{H}_A^{(1)}}\mathrm{Tr}(\Pi_1 X)\,\mathrm{id}_B \tag{4.2.27}$$

whose Choi matrix is

$$C_{\mathcal{L}} = \left(\frac{1}{\dim\mathcal{H}_A^{(1)}}\Pi_1\right)\otimes\left(\frac{1}{d_B}\mathrm{id}_B\right)\in\mathrm{Inv}(\overline{\pi_A}\otimes\pi_B)^{\mathcal{D}}. \tag{4.2.28}$$

□

4.3 A framework to characterize entanglement under group symmetry

In this section, we utilize Theorem 4.2.8 and Corollary 4.2.9 to derive novel results in the field of quantum entanglement. The first one is the case $\mathcal{K} = \mathcal{EB}_{AB}$, $\mathcal{K}^\circ = \mathcal{POS}_{AB}$, and $C_{\mathcal{K}} = \mathbf{SEP}_{AB}$. Then these results allow us to optimize entanglement witnesses *covariant* positive linear maps are enough to characterize separability of bipartite *invariant* quantum states. We note that similar findings have been reported in the literature, albeit with specific symmetries considered [Kay11, GÏ1, SN21].

Theorem 4.3.1. *For two finite-dimensional representations $\pi_A: G\to B(\mathcal{H}_A)$ and $\pi_B: G\to B(\mathcal{H}_B)$, let $\rho\in\mathrm{Inv}(\overline{\pi_A}\otimes\pi_B)^{\mathcal{D}}$ and accordingly take $\Phi\in\mathrm{Cov}_1(\pi_A,\pi_B)^{\mathcal{CP}}$ such that $C_\Phi=\rho$ (Note that Φ becomes a quantum channel when π_A is irreducible, by Lemma 4.2.10). The following are equivalent.*

1. $\rho \in \mathbf{SEP}_{AB}$,
2. $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \in \mathbf{P}_{AA}$ *for any* $\mathcal{L} \in \mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$,
3. $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \in \mathbf{P}_{AA}$ *for any* $\mathcal{L} \in \mathrm{Ext}\left(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}\right)$,
4. $\Phi \in \mathcal{EB}_{AB}$,
5. $\mathcal{L} \circ \Phi \in \mathcal{CP}_{AA}$ *for any* $\mathcal{L} \in \mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$,
6. $\mathcal{L} \circ \Phi \in \mathcal{CP}_{AA}$ *for any* $\mathcal{L} \in \mathrm{Ext}\left(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}\right)$.

Next, the case $(\mathcal{K}, \mathcal{K}^\circ, C_{\mathcal{K}}) = (\mathcal{SP}_k, \mathcal{POS}_k, \mathbf{Sch}_k)$ provides a new systematic way to compute the Schmidt numbers of $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$ using $\mathrm{Ext}(\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{POS}_k})$ as a complete family of Schmidt number witnesses.

Theorem 4.3.2. *For a* $\overline{\pi_A} \otimes \pi_B$*-invariant bipartite quantum state* ρ*, the following are equivalent:*

1. $\mathrm{SN}(\rho) \leq k$,
2. $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \in \mathbf{P}_{AA}$ *for every* $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}_k})$,
3. $\langle \Omega_A | (\mathrm{id}_A \otimes \mathcal{L})(\rho) | \Omega_A \rangle \geq 0$ *for every* $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}_k})$.

The above Theorem 4.3.2 will be applied for concrete applications in Section 5.2.

From now on, let us focus on the question of whether PPT property coincides with separability, i.e. problem $\mathbf{PPT} = \mathbf{SEP}$ for invariant quantum states.

Proposition 4.3.3. *Let* $\mathcal{L} : B(\mathcal{H}_B) \to B(\mathcal{H}_A)$ *be* (π_B, π_A)*-covariant. Then*

1. $\mathcal{L} \in \mathcal{POS}_{BA}$ *if and only if* $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \in \mathbf{P}_{AA}$ *for any separable* $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$.
2. $\mathcal{L}$ *is decomposable if and only if* $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \geq 0$ *for any PPT* $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$.

Proof. Clear from Theorem 4.2.8 with the cases $\mathcal{K} = \mathcal{EB}$ and $\mathcal{K} = \mathcal{PPT}$. □

Corollary 4.3.4. *Let $\pi_A : G \to \mathcal{U}(\mathcal{H}_A)$ and $\pi_B : G \to \mathcal{U}(\mathcal{H}_B)$ be unitary representations of G. Then the following are equivalent.*

1. $\mathbf{PPT} = \mathbf{SEP}$ *in* $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$.
2. $\mathcal{PPT} = \mathcal{EB}$ *in* $\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{CP}}$.
3. $\mathcal{POS} = \mathcal{DEC}$ *in* $\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$.

Proof. ((1) $\implies$ (3)) If $\mathcal{L} \in \mathrm{Cov}(\pi_B, \pi_A)^{\mathcal{POS}}$, then $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \geq 0$ for every separable (hence every PPT) state $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$. Thus, $\mathcal{L}$ is decomposable by Proposition 4.3.3.

((3) $\implies$ (1)) If $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$ is a PPT state, then $(\mathrm{id}_A \otimes \mathcal{L})(\rho) \geq 0$ for every decomposable (hence every positive) linear map $\mathcal{L} \in \mathrm{Cov}(\pi_B, \pi_A)$. Thus, ρ is separable by Theorem 4.2.9.

((1) $\iff$ (2)) is clear by the Choi-Jamiołkowski correspondence. □

Finally, we claim that the decomposability of the extremal elements in $\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$ is much easier to check thanks to the following theorem.

Theorem 4.3.5. *Let $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}})$. Then $\mathcal{L}$ is decomposable if and only if $\mathcal{L}$ is CP or CCP.*

Proof. Let us focus only on the case where π_A is irreducible since the other case is analogous. If $\mathcal{L}$ is decomposable, then there exist a CP map $\mathcal{L}_1$ and a CCP map $\mathcal{L}_2$ such that $\mathcal{L} = \mathcal{L}_1 + \mathcal{L}_2$. By taking the twirling operation $\mathcal{T}_{\pi_B, \pi_A}$, we have $\mathcal{L} = \mathcal{L}_1' + \mathcal{L}_2'$ where $\mathcal{L}_i' = \mathcal{T}_{\pi_B, \pi_A}(\mathcal{L}_i) \in \mathrm{Cov}(\pi_B, \pi_A)$. Note that $\mathcal{L}_1'$ is CP and $\mathcal{L}_2'$ is CCP, and we can further write $\mathcal{L}_i' = \lambda_i \mathcal{L}_i''$ for some $\lambda_i \geq 0$, $\lambda_1 + \lambda_2 = 1$, and $\mathcal{L}_i'' \in \mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$ by Lemma 4.2.10 (1). Then extremality of $\mathcal{L}$ allows us to conclude that $\mathcal{L} = \mathcal{L}_1''$ or $\mathcal{L} = \mathcal{L}_2''$, which proves the assertion. The other direction is immediate. □

To summarize, our strategy to study the problems $\mathbf{PPT} = \mathbf{SEP}$ and $\mathcal{PPT} = \mathcal{EB}$ consists of the following three independent steps.

[**Step 1**] The first step is to characterize all elements in $\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$ for given specific unitary representations π_A and π_B. If we take the adjoint operation, this step is equivalent to characterize all elements in $\mathrm{CovPosTP}(\pi_A, \pi_B)$.

[**Step 2**] The next step is to solve the problem $\mathcal{POS} = \mathcal{DEC}$ in $\mathrm{Cov}_1(\pi_B, \pi_A)$. In particular, for a given extremal element $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}})$, $\mathcal{L}$ is decomposable if and only if $\mathcal{L}$ is CP or CCP. If $\mathcal{POS} = \mathcal{DEC}$ holds, then both the problems $\mathbf{PPT} = \mathbf{SEP}$ in $\mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathcal{D}}$ and $\mathcal{PPT} = \mathcal{EB}$ in $\mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{CP}}$ have the affirmative answer.

[**Step 3**] If there exists a non-decomposable element $\mathcal{L}$ in $\mathrm{Cov}_1(\pi_B, \pi_A)^{\mathcal{POS}}$, then the last step is to realize $\mathcal{L}$ as a detector for following PPT entangled objects:

- $\Phi \in \mathrm{Cov}_1(\pi_A, \pi_B)^{\mathcal{PPT}}$ for which $\mathcal{L} \circ \Phi \notin \mathcal{CP}$,
- $\rho \in \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)^{\mathbf{PPT}}$ for which $(\mathrm{id} \otimes \mathcal{L})(\rho) \notin \mathbf{P}$.

Chapter 5

Applications to quantum entanglement

5.1 Hyperoctaheral group symmetry and entanglement detection

One of the main applications of the results in Section 4.3 is a complete characterization of EB property for quantum channels $\Phi : M_d \to M_d$ of the form

$$\Phi(X) = a\frac{\mathrm{Tr}(X)}{d}I_d + bX + cX^T + (1-a-b-c)\,\mathrm{diag}(X). \tag{5.1.1}$$

The main result of this section is as follows.

Theorem 5.1.1. *Let Φ be a quantum channel of the form* (5.1.1)*. Then Φ is entanglement-breaking if and only if Φ is PPT.*

Remark 5.1.2. Note that the quantum channels of the form (5.1.1) under the condition $a+b+c=1$ are called the *generalized Werner-Holevo channels*, and their Choi matrices are given by

$$C_\Phi = \frac{1-b-c}{d^2}I_d \otimes I_d + b|\Omega_d\rangle\langle\Omega_d| + \frac{c}{d}F_d, \tag{5.1.2}$$

where $F_d = \sum_{i,j=1}^{d} e_{ij} \otimes e_{ji}$ is the flip matrix. The subclasses corresponding to the cases $b = 0$ or $c = 0$ are called *the Werner states* and the isotropic states respectively, and their separability was studied in [Wer89, HH99, Wat18, SN21]. Furthermore, it was proved in [VW01] that **PPT** = **SEP** holds for all quantum states of the form (5.1.2).

A starting point for a proof of Theorem 5.1.1 is to observe that any quantum channel of the form (5.1.1) is covariant with respect to the *hyperoctahedral group* or *signed symmetric group* $\mathcal{H}(d)$. One of the equivalent ways to realize the hyperoctahedral group is to define $\mathcal{H}(d)$ as a subgroup of the orthogonal group $\mathcal{O}(d)$ generated by permutation matrices and diagonal orthogonal matrices. In other words, every element in $\mathcal{H}(d)$ is written as an orthogonal matrix $\sum_{i=1}^{d} s_i |\sigma(i)\rangle\langle i|$ for $s_1, s_2, \ldots, s_n \in \{\pm 1\}$ and $\sigma \in \mathcal{S}_d$. We define $\mathrm{Inv}(H \otimes H)$ and $\mathrm{Cov}(H, H)$ with respect to the fundamental representation $H \in \mathcal{H}(d) \mapsto H \in \mathcal{O}(d)$, which is irreducible as proved below.

Lemma 5.1.3. *The fundamental representation $H \in \mathcal{H}(d) \mapsto H \in \mathcal{O}(d)$ is irreducible.*

Proof. The identity

$$HXH^T = \sum_{i,j=1}^{d} s_i s_j X_{ij} |\sigma(i)\rangle\langle\sigma(j)| = \sum_{i,j=1}^{d} s_{\sigma^{-1}(i)} s_{\sigma^{-1}(j)} X_{\sigma^{-1}(i)\sigma^{-1}(j)} |i\rangle\langle j| \tag{5.1.3}$$

and the invariance property $HXH^T = X$ for all $H \in \mathcal{H}(d)$ tell us that

$$s_{\sigma(i)} s_{\sigma(j)} X_{\sigma(i)\sigma(j)} = X_{ij} \tag{5.1.4}$$

for all $s_1, \ldots, s_d \in \{\pm 1\}$ and $\sigma \in \mathcal{S}_d$. This implies that $X_{ii} \equiv X_{11}$ for all $1 \le i \le d$ and $X_{ij} = 0$ for all $i \ne j$, i.e., $X = X_{11}\, I_d \in \mathbb{C} \cdot I_d$. □

Let us denote by $\mathcal{W}$ the space of linear maps spanned by the following four unital TP maps $\psi_0, \psi_1, \psi_2, \psi_3 : M_d \to M_d$, where

$$\begin{cases} \psi_0(X) = \frac{\mathrm{Tr}(X)}{d} I_d, \\ \psi_1(X) = X, \\ \psi_2(X) = X^T, \\ \psi_3(X) = \mathrm{diag}(X) = \sum_{i=1}^d X_{ii} |i\rangle\langle i|. \end{cases} \tag{5.1.5}$$

It is straightforward to check $\psi_i \in \mathrm{Cov}(H, H)$ for $i = 0, \dots, 3$, so we have $\mathcal{W} \subseteq \mathrm{Cov}(H, H)$. To prove $\mathrm{Cov}(H, H) = \mathcal{W}$, let us note the fact that any $\mathcal{L} \in \mathrm{Cov}(H, H)$ satisfies the so-called *diagonal orthogonal covariance (DOC)* property, i.e.

$$\mathcal{L}(ZXZ^T) = Z\mathcal{L}(X)Z^T \tag{5.1.6}$$

for all $X \in M_d$ and diagonal orthogonal matrices Z. This class of channels has been analyzed recently in [SN21, SN22, SDN22]. In particular, it is shown that any DOC map $\mathcal{L}$ can be parameterized by a triple $(A, B, C) \in M_d^3$ satisfying $\mathrm{diag}(A) = \mathrm{diag}(B) = \mathrm{diag}(C)$ such that

$$\mathcal{L}(X) = \mathrm{diag}(A|\mathrm{diag}\, X\rangle) + \widetilde{B} \odot X + \widetilde{C} \odot X^T, \tag{5.1.7}$$

where $|\mathrm{diag}\, Y\rangle = \sum_{i=1}^d Y_{ii}|i\rangle$, $\widetilde{Y} = Y - \mathrm{diag}(Y)$, and $\odot$ denotes the Schur product (or Hadamard product) between matrices. In this case, let us denote by $\mathcal{L} = \mathcal{L}_{A,B,C}$.

Proposition 5.1.4. *The space* $\mathrm{Cov}(H, H)$ *is spanned by the four unital TP positive maps* $\psi_0, \psi_1, \psi_2,$ *and* ψ_3 *from* (5.1.5).

Proof. We already know $\mathcal{W} \subseteq \mathrm{Cov}(H, H)$. To show the reverse inclusion, let us pick an arbitrary $\mathcal{L} \in \mathrm{Cov}(H, H)$. Since $\mathcal{L}$ is DOC, there exists $(A, B, C) \in M_d^3$ such that $\mathcal{L} = \mathcal{L}_{A,B,C}$ of the form (5.1.7). Note that $\mathcal{L}$ further satisfies

$$\mathcal{L}(P_\sigma X P_\sigma^T) = P_\sigma \mathcal{L}(X) P_\sigma^T \tag{5.1.8}$$

for all $X \in M_d$ and $\sigma \in \mathcal{S}_d$. Here, $P_\sigma = \sum_{i=1}^d |\sigma(i)\rangle\langle i|$ is the permutation matrix associated with σ.

Let us take $X = e_{ij}$. If $i = j$, then (5.1.8) implies

$$\sum_{k=1}^{d} A_{k\sigma(i)}|k\rangle\langle k| = \sum_{k=1}^{d} A_{ki}|\sigma(k)\rangle\langle\sigma(k)|, \tag{5.1.9}$$

which means that $A_{ik} = A_{\sigma(i)\sigma(k)}$ for all $1 \le i, k \le d$ and $\sigma \in \mathcal{S}_d$. Therefore, $A_{ii} \equiv A_{11}$ for all i and $A_{ik} \equiv A_{12}$ for all $i \neq k$. On the other hand, if $i \neq j$, then (5.1.8) becomes

$$B_{\sigma(i)\sigma(j)}|\sigma(i)\rangle\langle\sigma(j)| + C_{\sigma(j)\sigma(i)}|\sigma(j)\rangle\langle\sigma(i)| \tag{5.1.10}$$

$$= B_{ij}|\sigma(i)\rangle\langle\sigma(j)| + C_{ji}|\sigma(j)\rangle\langle\sigma(i)|, \tag{5.1.11}$$

which gives $B_{ij} \equiv B_{12}$ and $C_{ij} \equiv C_{12}$ for all $i \neq j$. Consequently, the formula (5.1.7) now gives

$$\mathcal{L} = dA_{12}\psi_0 + B_{12}\psi_1 + C_{12}\psi_2 + (A_{11} - A_{12} - B_{12} - C_{12})\psi_3 \in \mathcal{W}, \tag{5.1.12}$$

which in turn shows $\mathrm{Cov}(H, H) \subseteq \mathcal{W}$. □

From now, let us denote (H, H)-covariant unital (and TP) maps by

$$\psi_{a,b,c} = a\psi_0 + b\psi_1 + c\psi_2 + (1 - a - b - c)\psi_3 \tag{5.1.13}$$

for simplicity, where $\psi_0, \dots, \psi_3$ are from (5.1.5). By recalling that $\psi_{a,b,c}$ can be understood as a DOC map $\mathcal{L}_{A,B,C}$ and that complete positivity of DOC maps is fully characterized in [SN21, Section 6], we can show that $\psi_{a,b,c}$ is CPTP if and only if

$$\begin{cases} 0 \le a \le \frac{d}{d-1}, \\ \frac{a}{d} - \frac{1}{d-1} \le b \le 1 - \frac{d-1}{d}a, \\ -\frac{a}{d} \le c \le \frac{a}{d}. \end{cases} \tag{5.1.14}$$

Note that the set of $(a, b, c) \in \mathbb{R}^3$ satisfying (5.1.14) is a tetrahedron depicted in Figure 5.1.

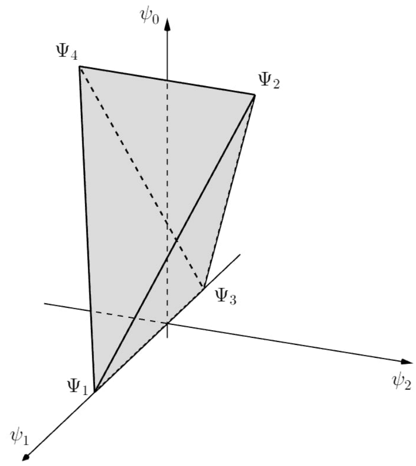

Figure 5.1: The region of $\mathrm{Cov}(H,H)^{\mathcal{CPTP}}$

In particular, there are exactly four extremal (H,H)-covariant quantum channels corresponding to the four vertices given by

$$\begin{cases} \Psi_1 = \psi_1, \\ \Psi_2 = \frac{d}{d-1}\psi_0 + \frac{1}{d-1}\psi_2 - \frac{2}{d-1}\psi_3, \\ \Psi_3 = -\frac{1}{d-1}\psi_1 + \frac{d}{d-1}\psi_3, \\ \Psi_4 = \frac{d}{d-1}\psi_0 - \frac{1}{d-1}\psi_1, \end{cases} \tag{5.1.15}$$

whose Choi matrices are (up to normalization) four mutually orthogonal projections. On the other hand, it is easy to see that

$$T_d \circ \psi_{a,b,c} = \psi_{a,b,c} \circ T_d = \psi_{a,c,b}, \quad a,b,c \in \mathbb{C}. \tag{5.1.16}$$

Therefore, the set of all PPT quantum channels $\psi_{a,b,c}$ is given by

$$\begin{aligned} \mathrm{Cov}_1(H,H)^{\mathcal{PPT}} &= \mathrm{Cov}(H,H)^{\mathcal{CPTP}} \cap T_d\left(\mathrm{Cov}(H,H)^{\mathcal{CPTP}}\right) \\ &= \left\{ \psi_{a,b,c} : \begin{array}{c} 0 \le a \le \frac{d}{d-1}, \\ \max(\frac{a}{d} - \frac{1}{d-1}, -\frac{a}{d}) \le b, c \le \min(1 - \frac{d-1}{d}a, \frac{a}{d}) \end{array} \right\}. \end{aligned} \tag{5.1.17}$$

The convex set $\mathrm{Cov}_1(H,H)^{\mathcal{PPT}}$ can be geometrically understood as the intersection of two tetrahedrons describing the region of CP and CCP (H, H)-covariant TP maps (depicted by blue- and red-dotted lines, respectively, in Figure 2). Moreover, if $d \geq 3$, this set has exactly eight vertices (denoted by $v_0, \dots v_7$).

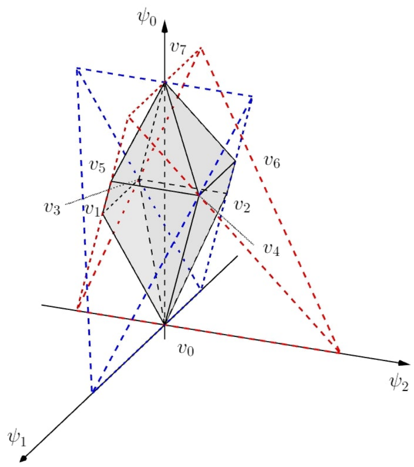

Figure 5.2: The region of $\mathrm{Cov}_1(H, H)^{\mathcal{PPT}}$

We will now explain why the above polytope is precisely identical to the set of all entanglement-breaking (H, H)-covariant channels to prove Theorem 5.1.1.

[**Step 1+Step 2**] We first characterize the set $\mathrm{Cov}_1(H, H)^{\mathcal{POS}}$ in terms of the parameters a, b, and c. Our strategy is to start with the convex hull $\mathcal{V}_d$ of $\mathrm{Cov}(H, H)^{\mathcal{CPTP}} \cup T_d \left(\mathrm{Cov}(H, H)^{\mathcal{CPTP}}\right)$, which is an octahedron with eight vertices as exhibited in Figure 5.3. Then $\mathcal{V}_d \subseteq \mathrm{Cov}_1(H, H)^{\mathcal{POS}}$ is immediate since any element of $\mathcal{V}_d$ is decomposable. The following Theorem 5.1.5 states that these two convex sets coincide, i.e., $\mathcal{V}_d = \mathrm{Cov}_1(H, H)^{\mathcal{POS}}$.

Theorem 5.1.5. *Let $d \geq 3$. Then the convex set $\mathrm{Cov}_1(H, H)^{\mathcal{POS}}$ has exactly 8 extreme points*

$$\Psi_1,\ \Psi_2,\ \Psi_3,\ \Psi_4,\quad \Psi_1 \circ T_d,\ \Psi_2 \circ T_d,\ \Psi_3 \circ T_d,\ \Psi_4 \circ T_d, \tag{5.1.18}$$

where $\Psi_1, \dots, \Psi_4$ are given by (5.1.15)*. In particular, all positive (H, H)-*

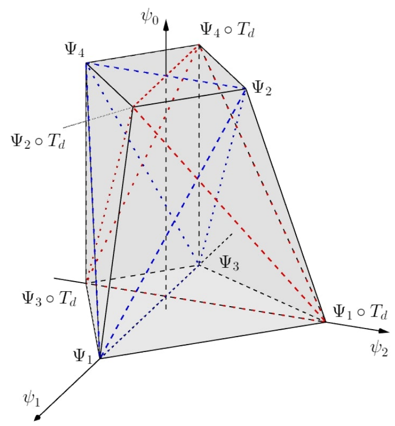

Figure 5.3: The region of $\mathrm{Cov}_1(H,H)^{\mathcal{POS}}$

covariant maps are decomposable.

Proof. Since $\Psi_1,\dots,\Psi_4$ are CP and $\Psi_1\circ T_d,\dots,\Psi_4\circ T_d$ are CCP, the convex hull $\mathcal{V}_d$ of these 8 maps is obviously contained in $\mathrm{Cov}_1(H,H)^{\mathcal{POS}}$. To show the reverse inclusion $\mathrm{Cov}_1(H,H)^{\mathcal{POS}} \subseteq \mathcal{V}_d$, we observe that the set

$$V_d := \left\{(a,b,c)\in\mathbb{R}^3 \,:\, \psi_{a,b,c}\in\mathcal{V}_d\right\} \subset \mathbb{R}^3 \tag{5.1.19}$$

is the convex hull of 8 points

$$\begin{cases} (0,1,0)\,,\left(\frac{d}{d-1},0,\frac{1}{d-1}\right),\left(0,-\frac{1}{d-1},0\right),\left(\frac{d}{d-1},0,-\frac{1}{d-1}\right), \\ (0,0,1)\,,\left(\frac{d}{d-1},\frac{1}{d-1},0\right),\left(0,0,-\frac{1}{d-1}\right),\left(\frac{d}{d-1},-\frac{1}{d-1},0\right), \end{cases} \tag{5.1.20}$$

which are got from (5.1.15) and (5.1.16). Therefore, V_d can be understood as the region of $(a,b,c)\in\mathbb{R}^3$ satisfying the following inequalities:

$$\begin{cases} (1) & 0\le a\le \frac{d}{d-1}, \\ (2) & \frac{d-2}{d}a+b+c\le 1, \\ (3) & \frac{d-2}{d}a+|b-c|\le 1, \\ (4) & b+c\ge -\frac{1}{d-1}, \\ (5) & b-(d-1)\,c\le 1, \\ (6) & c-(d-1)\,b\le 1. \end{cases} \tag{5.1.21}$$

Now if $\psi_{a,b,c} \notin \mathcal{V}_d$ (which is equivalent to $(a,b,c) \notin V_d$, and hence violates at least one of the inequalities (1) - (6) in (5.1.21)), we can choose a unit vector $\xi \in \mathbb{C}^d$ such that $\psi_{a,b,c}(|\xi\rangle\langle\xi|)$ is not positive semidefinite as in Table 5.1. This shows $\mathrm{Cov}_1(H,H)^{\mathcal{POS}} \subseteq \mathcal{V}_d$.

Table 5.1: Non-positivity outside V_d

(a,b,c) violates (1)	$\lvert\xi\rangle = \lvert 1\rangle \implies \psi_{a,b,c}(\lvert\xi\rangle\langle\xi\rvert) \ngeq 0$
(a,b,c) violates (2)	$\lvert\xi\rangle = \frac{1}{\sqrt{2}}(\lvert 1\rangle + \lvert 2\rangle) \implies \psi_{a,b,c}(\lvert\xi\rangle\langle\xi\rvert) \ngeq 0$
(a,b,c) violates (3)	$\lvert\xi\rangle = \frac{1}{\sqrt{2}}(\lvert 1\rangle + i\lvert 2\rangle) \implies \psi_{a,b,c}(\lvert\xi\rangle\langle\xi\rvert) \ngeq 0$
(a,b,c) violates (4)	$\lvert\xi\rangle = \frac{1}{\sqrt{d}}\sum_{k=1}^{d}\lvert k\rangle \implies \psi_{a,b,c}(\lvert\xi\rangle\langle\xi\rvert) \ngeq 0$
(a,b,c) violates (5) or (6)	$\lvert\xi\rangle = \frac{1}{\sqrt{d}}\sum_{k=1}^{d} e^{\frac{2\pi i k}{d}}\lvert k\rangle \implies \psi_{a,b,c}(\lvert\xi\rangle\langle\xi\rvert) \ngeq 0$

□

Proof of Theorem 5.1.1. The conclusion is straightforward from Proposition 5.1.4, Theorem 5.1.5, and Corollary 4.3.4. □

Remark 5.1.6. 1. Note that Theorem 5.1.5 gives a complete characterization of all positive linear maps ψ spanned by $\psi_0, \psi_1, \psi_2, \psi_3$. This strengthens the results in Section 5 of [KMS20] focusing on positive linear maps spanned only by ψ_0, ψ_1, ψ_3 without ψ_2.

2. Theorem 5.1.5 tells us not only $\mathcal{POS} = \mathcal{DEC}$, but also explicit decompositions of our positive covariant maps into sums of CP and CCP maps. Note that this was one of the open questions raised in Section 6.c of [KMS20]. We refer to Appendix 5.1.1 for more details.

5.1.1 Covariant positive maps with respect to monomial unitary groups

In Section 5 and Section 6 of [KMS20], the authors analyzed the general structure of irreducibly covariant linear maps under some natural symmetries of the symmetric group $\mathcal{S}_4$ and the monomial unitary group $\mathcal{MU}(d,n)$, and presented new examples of positive irreducibly covariant maps. In this section, we elaborate on how our Theorem 5.1.5 strengthens their results and resolves several open questions raised in [KMS20].

On one side, they considered irreducibly (τ_3,τ_3)-covariant maps, where $\tau_3 : \mathcal{S}_4 \to \mathcal{U}(3)$ is a 3-dimensional irreducible component of the canonical representation $\sigma \in \mathcal{S}_4 \mapsto \sum_{k=1}^4 |\sigma(k)\rangle\langle k| \in \mathcal{U}(4)$. More precisely, this canonical representation is not irreducible; it allows an invariant 1-dimensional subspace $\mathbb{C}\cdot|v\rangle$ with $|v\rangle = \sum_{k=1}^d |k\rangle$ and the other 3-dimensional invariant subspace $V = (\mathbb{C}\cdot|v\rangle)^\perp$. Then the fundamental representation $\tau_3 : \mathcal{S}_4 \to \mathcal{U}(3)$ is defined by $\tau_3(\sigma) = \Pi_V \sigma\big|_V \in \mathcal{U}(3)$ for all $x \in \mathcal{S}_4$, where Π_V is the orthogonal projection from $\mathbb{C}^4$ onto V.

The authors characterized all (τ_3,τ_3)-covariant maps and suggested a sufficient condition for positivity using the the so-called *inverse reduction map criterion* [MRS15]. On the other hand, it was shown in [LY22, Section 6.1.1] that, up to a change of basis, the (τ_3,τ_3)-covariant maps are precisely the linear combinations of $\Psi_1, \Psi_2, \Psi_3, \Psi_4 : M_3(\mathbb{C}) \to M_3(\mathbb{C})$ from (5.1.15) with $d = 3$. In other words, we have $\mathrm{Cov}(\tau_3,\tau_3) = \mathrm{Cov}(H,H)$ up to a unitary equivalence. Thus, Theorem 5.1.5 gives the complete solution to the open question of the characterization of all positive (τ_3,τ_3)-covariant maps raised in [KMS20].

On the other side, recall that the *monomial unitary group* $\mathcal{MU}(d)$ is a subgroup of $\mathcal{U}(d)$ generated by all permutation matrices and all diagonal unitary matrices. Moreover, the subgroup $\mathcal{MU}(d,n)$ of $\mathcal{MU}(d)$ is generated by all permutation matrices and all diagonal matrices of the form $\sum_{i=1}^d \omega_i |i\rangle\langle i|$ where $\omega_i \in \{1, e^{2\pi i/n}, \dots, e^{2(n-1)\pi i/n}\}$, In particular, we have $\mathcal{MU}(d,2) = \mathcal{H}(d)$.

For a closed subgroup G of $\mathcal{U}(d)$, we denote by $\pi_G : x \in G \mapsto x \in \mathcal{U}(d)$ the fundamental representation of G, temporarily in this section. It was shown in [KMS20] that, if $n \geq 3$, then

$$\mathrm{Cov}(\pi_{\mathcal{MU}(d,n)}, \pi_{\mathcal{MU}(d,n)}) = \mathrm{span}\,\{\psi_0, \psi_1, \psi_3\} \tag{5.1.22}$$

where ψ_0, ψ_1, ψ_3 are from (5.1.5). Moreover, the authors characterized all positive maps in this class and proved that all $(\pi_{\mathcal{MU}(d,n)}, \pi_{\mathcal{MU}(d,n)})$-covariant positive maps are decomposable for $n \geq 3$. However, explicit decompositions were left as an open question, and the authors conjectured that a non-decomposable positive map may arise under $(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)})$-covariance.

Our results in this thesis resolve their open questions in the sense that $(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)})$-covariance does not make a difference, but a weaker condition $(\pi_{\mathcal{MU}(d,2)}, \pi_{\mathcal{MU}(d,2)})$-covariance does. Furthermore, their $\mathcal{POS} = \mathcal{DEC}$ result in $\mathrm{Cov}(\pi_{\mathcal{MU}(d,n)}, \pi_{\mathcal{MU}(d,n)})$ with $n \geq 3$ (Section 6.c of [KMS20]) extends to a more general result $\mathcal{POS} = \mathcal{DEC}$ in $\mathrm{Cov}(\pi_{\mathcal{MU}(d,2)}, \pi_{\mathcal{MU}(d,2)})$ with explicit decompositions into the sum of CP and CCP maps.

1. More precisely, it is clear that

$$\mathrm{Cov}(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)}) \subseteq \mathrm{Cov}(\pi_{\mathcal{MU}(d,n)}, \pi_{\mathcal{MU}(d,n)}) = \mathrm{span}\,\{\psi_0, \psi_1, \psi_3\}\,, \tag{5.1.23}$$

   and all the three maps ψ_0, ψ_1, and ψ_3 are covariant with respect to general diagonal unitary matrices. Therefore, for $n \geq 3$ we have

$$\mathrm{Cov}(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)}) = \mathrm{Cov}(\pi_{\mathcal{MU}(d,n)}, \pi_{\mathcal{MU}(d,n)}) = \mathrm{span}\,\{\psi_0, \psi_1, \psi_3\}\,. \tag{5.1.24}$$

   Therefore, there is no positive non-decomposable element inside $\mathrm{Cov}(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)})$.

2. On the other hand, since $\mathcal{MU}(d,2) = \mathcal{H}(d)$, we have

$$\mathrm{Cov}(\pi_{\mathcal{MU}(d,2)}, \pi_{\mathcal{MU}(d,2)}) = \mathrm{Cov}(H, H) = \mathrm{span}\,\{\psi_0, \psi_1, \psi_2, \psi_3\}\,, \tag{5.1.25}$$

   by Proposition 5.1.4. Moreover, $\mathcal{POS} = \mathcal{DEC}$ in $\mathrm{Cov}(\pi_{\mathcal{MU}(d)}, \pi_{\mathcal{MU}(d)})$

from Section 6.c of [KMS20] is strengthened to $\mathcal{POS} = \mathcal{DEC}$ in the larger space $\mathrm{Cov}(\pi_{\mathcal{MU}(d,2)}, \pi_{\mathcal{MU}(d,2)})$ with explicit decompositions by Theorem 5.1.5.

5.2 k-positivity and Schmidt number under Orthogonal group symmetry

There are very few examples whose k-positivity or Schmidt numbers have been fully characterized. Even in the following cases

$$\mathcal{L}^{(d)}_{a,b}(Z) := (1-a-b)\frac{\mathrm{Tr}(Z)}{d} I_d + aZ + bZ^\top, \tag{5.2.1}$$

$$\rho^{(d)}_{a,b} := \frac{1-a-b}{d^2} I_d \otimes I_d + a|\Omega_d\rangle\langle\Omega_d| + \frac{b}{d}F_d, \tag{5.2.2}$$

their k-positivity and Schmidt numbers have not been fully characterized. Here, $|\Omega_d\rangle := \frac{1}{\sqrt{d}}\sum_{j=1}^d |jj\rangle$ is the maximally entangled state and $F_d := \sum_{i,j=1}^d |ij\rangle\langle ji|$ is the flip matrix. Let us write $\mathcal{L}_{a,b} := \mathcal{L}^{(d)}_{a,b}$ and $\rho_{a,b} := \rho^{(d)}_{a,b}$ for simplicity. On the problem of k-positivity, the answers for some special cases $\mathcal{L}_{a,0}$, $\mathcal{L}_{0,b}$, and $\mathcal{L}_{a,1-a}$, were obtained from [Tom85], and some other cases were considered in [TT83]. On the other hand, Schmidt numbers of the *isotropic states* $\rho_{a,0}$ [HH99] were computed in [TH00], and Schmidt numbers of the *Werner states* $\rho_{0,b}$ [Wer89] were also known (see [Kye23b, Theorem 1.7.4] for example). Despite the partial answers to the cases of single parameters, the problems of the general cases $\mathcal{L}_{a,b}$ and $\rho_{a,b}$ remain open. To our best knowledge, our result is the first example of computations of the Schmidt numbers for non-trivial two-dimensional families of quantum states in arbitrarily high dimensional settings.

A crucial observation is that the above quantum objects $\mathcal{L}_{a,b}$ and $\rho_{a,b}$ are linked via the standard orthogonal group symmetries. Let G be the orthogonal group $\mathcal{O}(d)$, and let $\pi_A(O) = \pi_B(O) = O$ be the standard representation of $\mathcal{O}(d)$. In this case, we denote by $\mathrm{Cov}(O,O) = \mathrm{Cov}(\pi_A, \pi_B)$ and

$\mathrm{Inv}(O \otimes O) = \mathrm{Inv}(\overline{\pi_A} \otimes \pi_B)$ for simplicity. Then we have $\rho_{a,b} = C_{\mathcal{L}_{a,b}}$ and $\mathrm{Cov}_1(O, O) = \{\mathcal{L}_{a,b} : a, b \in \mathbb{C}\}$, as noted in [VW01, Has18]. Moreover, $\mathcal{L}_{a,b}$ is Hermitian-preserving if and only if $a, b \in \mathbb{R}$.

In this section, we aim to establish a complete characterization of k-positivity of $\mathcal{L}_{a,b}$ and Schmidt number of $\rho_{a,b}$ in terms of the parameters a and b. Then k-block positivity of $\rho_{a,b}$ and k-superpositivity of $\mathcal{L}_{a,b}$ are immediate through the Choi-Jamiołkowski map.

Our strategy consists of two steps. The first step is to employ some methodologies from [Tom85] to study k-positivity of $\mathcal{L}_{a,b} \in \mathrm{Cov}_1(O, O)$ in a direct way (Theorem 5.2.1), and the second step is to apply Theorem 4.3.2 to compute the Schmidt numbers of all $\rho_{a,b} \in \mathrm{Inv}(O \otimes O)^{\mathcal{D}}$ accurately (Theorem 5.2.4).

5.2.1 k-positivity of orthogonally covariant maps

Note that positivity and complete positivity of $\mathcal{L}_{p,q}$ were completely characterized recently in a more general setting, namely the *hyperoctahedrally covariant maps* (Section 5.1). This section is devoted to characterizing k-positivity of all $\mathcal{L}_{p,q} \in \mathrm{Cov}_1(O, O)$, which generalizes the results from [Tom85]. Indeed, for the following convex subsets

$$P_k := \left\{(p, q) \in \mathbb{R}^2 : \mathcal{L}_{p,q} \in \mathcal{POS}_k\right\},\ 1 \leq k \leq d, \tag{5.2.3}$$

we prove $P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_d$ with explicit geometric and algebraic descriptions. First of all, the geometric structures of the convex subsets P_k can be categorized into four distinct cases.

1. The region P_1 is *trapezoid-shaped* with vertices $(1, 0)$, $(0, -\frac{1}{d-1})$, $(-\frac{1}{d-1}, 0)$, and $(0, 1)$.

2. If $1 < k \leq \frac{d}{2}$, the region P_k is *quadrilateral-shaped* with vertices $(1, 0)$, $(0, -\frac{1}{d-1})$, $(-\frac{1}{kd-1}, 0)$, and $(-\frac{1}{kd+k-1}, \frac{k}{kd+k-1})$.

3. If $\frac{d}{2} < k < d$, the region P_k is bounded by a piecewise-linear curve joining $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2}), (1,0), (0,-\frac{1}{d-1})$, and $(-\frac{1}{kd-1}, 0)$ in that order, and by a conic (i.e. a quadratic curve) passing through $(-\frac{1}{kd-1}, 0)$ and $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$.

4. Lastly, the region P_d is a *triangle* with vertices $(1,0), (0,-\frac{1}{d-1})$, and $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$.

A visualization of the above characterizations for special cases $d = 3$ and $d = 4$ are given in the following Figure 5.4.

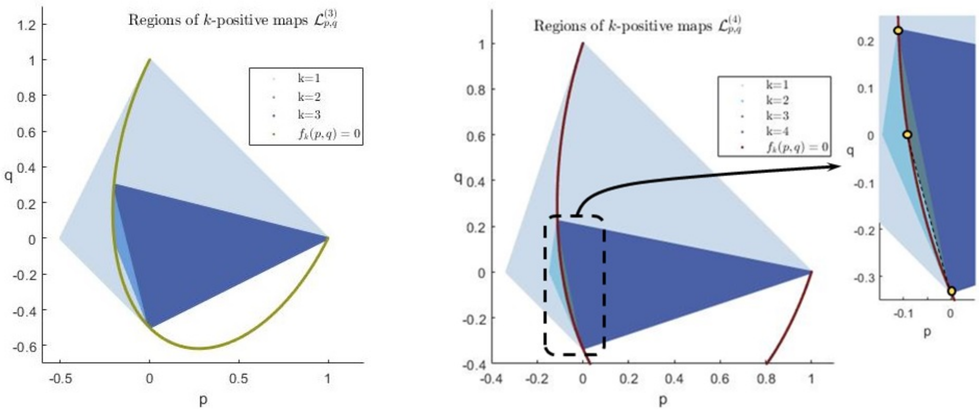

Figure 5.4: The regions of k-positive maps $\mathcal{L}^{(d)}_{p,q}$ for $d = 3, 4$

We now present explicit algebraic descriptions of the regions P_k (equivalently, $\mathcal{POS}_k$) in the following theorem.

Theorem 5.2.1. *Let $\mathcal{L}_{p,q}$ be a linear map of the form* (5.2.1)*. Then*

1. $\mathcal{L}_{p,q} \in \mathcal{POS}$ if and only if $\begin{cases} p-(d-1)q \le 1, \\ q-(d-1)q \le 1, \\ -\frac{1}{d-1} \le p+q \le 1. \end{cases}$

2. $\mathcal{L}_{p,q} \in \mathcal{POS}_k$ $(1 < k \leq \frac{d}{2})$ *if and only if* $\begin{cases} p-(d-1)q \leq 1, \\ p+(d+1)q \leq 1, \\ (kd-1)p+(d-1)q \geq -1, \\ q-(kd-1)p \leq 1. \end{cases}$

3. $\mathcal{L}_{p,q} \in \mathcal{POS}_k$ $(\frac{d}{2} < k < d)$ *if and only if* $\begin{cases} p-(d-1)q \leq 1, \\ p+(d+1)q \leq 1, \\ (kd-1)p+(d-1)q \geq -1, \\ f_k(x,y) \leq 0, \end{cases}$

where $f_k(x,y)$ *is a quadratic polynomial explicitly given by*

$$\begin{aligned} f_k(x,y) =&(kd-1)x^2-(d^3-kd^2-kd-d+2)xy+(d-1)y^2 \\ &-(kd-2)x-(d-2)y-1. \end{aligned} \tag{5.2.4}$$

4. $\mathcal{L}_{p,q} \in \mathcal{CP}$ *if and only if* $\begin{cases} p-(d-1)q \leq 1, \\ p+(d+1)q \leq 1, \\ (d+1)p+q \geq -\frac{1}{d-1}. \end{cases}$

Note that (1) and (4) of Theorem 5.2.1, i.e. positivity and complete positivity of $\mathcal{L}_{p,q}$, are straightforward from (5.1.21) and (5.1.14). Thus, our main focus is to prove (2) and (3) of Theorem 5.2.1. Let us recall a criterion of k-positivity proposed in [Tom85, Lemma 1].

Proposition 5.2.2. *Let* $1 \leq k \leq d$. *Then a linear map* $\mathcal{L} : M_d \to M_d$ *is* k*-positive if and only if the bipartite matrix*

$$C_k^v(\mathcal{L}) := \sum_{i,j=1}^{k} |i\rangle\langle j| \otimes \mathcal{L}(|v_i\rangle\langle v_j|) \in M_k \otimes M_d \tag{5.2.5}$$

is positive semidefinite for any choice of an orthonormal subset $\{v_1, \ldots, v_k\}$ *of* $\mathbb{C}^d$.

The following lemma plays a crucial role in applying the above Proposition 5.2.2 to prove (2) and (3) of Theorem 5.2.1.

Lemma 5.2.3. *For $1 \le k \le d$, we have*

$$\min \sum_{j,j'=1}^{k} |\langle v_j | \overline{v_{j'}} \rangle|^2 = \max(2k-d, 0), \tag{5.2.6}$$

where $\overline{w}$ is the complex conjugation of $w \in \mathbb{C}^d$ and the minimum is taken over all orthonormal subsets $\{v_1, \dots, v_k\} \subset \mathbb{C}^d$.

Proof. If $2k \le d$, then we can take $|v_j\rangle = \frac{1}{\sqrt{2}}(|2j-1\rangle + i|2j\rangle)$ $(j = 1, \dots, k)$ and check $\langle v_j | \overline{v_{j'}} \rangle = 0$ for every j, j', so the equality (5.2.6) holds. From now, let us focus on the case $2k > d$. First, we consider an arbitrary orthonormal subset $\{v_1, \dots, v_k\} \subset \mathbb{C}^d$ and orthogonal projections $\Pi_v = \sum_{j=1}^k |v_j\rangle\langle v_j|$ and $\Pi_{\overline{v}} = \sum_{j=1}^k |\overline{v_j}\rangle\langle\overline{v_j}|$. Then we can observe that

$$\sum_{j,j'} |\langle v_j | \overline{v_{j'}} \rangle|^2 = \mathrm{Tr}(\Pi_v \Pi_{\overline{v}}) \ge \dim(\mathrm{Ran}(\Pi_v) \cap \mathrm{Ran}(\Pi_{\overline{v}}))$$

and the right hand side is equal to

$$\dim(\mathrm{Ran}(\Pi_v)) + \dim(\mathrm{Ran}(\Pi_{\overline{v}})) - \dim(\mathrm{Ran}(\Pi_v) + \mathrm{Ran}(\Pi_{\overline{v}})).$$

Thus we have $\sum_{j,j'} |\langle v_j | \overline{v_{j'}} \rangle|^2 \ge 2k - d$. On the other hand, let us take a specific orthonormal subset $\{v_1, v_2, \cdots, v_k\} \subseteq \mathbb{C}^d$ where $|v_j\rangle = \frac{1}{\sqrt{d}} \sum_{l=1}^d \omega^{l(j-1)} |l\rangle$ $(j = 1, \dots, k)$ and $\omega = \exp(\frac{2\pi i}{d})$. Then we can check that the desired equality $\sum_{j,j'} |\langle v_j | \overline{v_{j'}} \rangle|^2 = 2k - d$ holds from the relation

$$\langle v_j | \overline{v_{j'}} \rangle = \frac{1}{d} \sum_{l=1}^{d} \omega^{-l(j+j'-2)} = \begin{cases} 1 & \text{if } j + j' - 2 \equiv 0 \bmod d, \\ 0 & \text{otherwise.} \end{cases}$$

□

Proof of Theorem 5.2.1 (2) and (3). For an orthonormal subset $\{v_1, \dots, v_k\}$

in $\mathbb{C}^d$, the associated bipartite matrix in (5.2.5) is given by

$$C_k^v(\mathcal{L}_{p,q}) = \frac{1-p-q}{d} I_k \otimes I_d + pk|\Omega_k^v\rangle\langle\Omega_k^v| + qF_k^v,$$

where $\begin{cases} |\Omega_k^v\rangle = \frac{1}{\sqrt{k}} \sum_{j=1}^k |j\rangle \otimes |v_j\rangle \in \mathbb{C}^k \otimes \mathbb{C}^d, \\ F_k^v = \sum_{i,j=1}^k |i\rangle\langle j| \otimes |\overline{v_j}\rangle\langle\overline{v_i}| \in \mathcal{M}k \otimes \mathcal{M}d. \end{cases}$ Moreover, we can write $F_k^v = \Pi_{\mathcal{S}}^v - \Pi_{\mathcal{A}}^v$, where $\Pi_{\mathcal{S}}^v$ is the projection onto the (symmetric) space span$\left\{\frac{|i\rangle|\overline{v_j}\rangle + |j\rangle|\overline{v_i}\rangle}{\sqrt{2}} : 1 \le i \le j \le k\right\}$ and $\Pi_{\mathcal{A}}^v$ is the projection onto the (anti-symmetric) space span$\left\{\frac{|i\rangle|\overline{v_j}\rangle - |j\rangle|\overline{v_i}\rangle}{\sqrt{2}} : 1 \le i < j \le k\right\}$. Note that $\mathrm{Ran}(\Pi_{\mathcal{S}}^v) \perp \mathrm{Ran}(\Pi_{\mathcal{A}}^v)$, and $|\Omega_k^v\rangle \perp \mathrm{Ran}(\Pi_{\mathcal{A}}^v)$ since

$$\left\langle \Omega_k^v \middle| \frac{e_i \otimes \overline{v_j} - e_j \otimes \overline{v_i}}{\sqrt{2}} \right\rangle = \frac{1}{\sqrt{2k}} (\langle v_i|\overline{v_j}\rangle - \langle v_j|\overline{v_i}\rangle) = 0,$$

for all $1 \le i < j \le k$. Therefore, after rewriting

$$C_k^v(\mathcal{L}_{p,q}) = (A(I_{kd} - \Pi_{\mathcal{A}}^v) + pk|\Omega_k^v\rangle\langle\Omega_k^v| + q\Pi_{\mathcal{S}}^v) \oplus (A-q)\,\Pi_{\mathcal{A}}^v$$

with $A := \frac{1-p-q}{d}$ for an orthogonal decomposition, the desired condition $C_k^v(\mathcal{L}_{p,q}) \in \mathbf{P}_{kd}$ is equivalent to $A - q \ge 0$ and

$$A(I_{kd} - \Pi_{\mathcal{A}}^v) + pk|\Omega_k^v\rangle\langle\Omega_k^v| + q\Pi_{\mathcal{S}}^v \in \mathbf{P} \tag{5.2.7}$$

(the condition $k \ge 2$ ensures that $\Pi_{\mathcal{A}}^v$ is nonzero).

A technical difficulty on (5.2.7) is that $|\Omega_k^v\rangle\langle\Omega_k^v|$ and $\Pi_{\mathcal{S}}^v$ are not simultaneously diagonalizable since

$$|\Omega_k^v\rangle\langle\Omega_k^v| \cdot \Pi_{\mathcal{S}}^v \neq \Pi_{\mathcal{S}}^v \cdot |\Omega_k^v\rangle\langle\Omega_k^v|$$

in general unless $\{v_i\}_{i=1}^k \subset \mathbb{R}^d$. To overcome this, let us take $|\xi_1\rangle = \Pi_{\mathcal{S}}^v|\Omega_k^v\rangle \in \mathrm{Ran}(\Pi_{\mathcal{S}}^v)$ and consider $|\Omega_k^v\rangle = |\xi_1\rangle + |\xi_2\rangle$. Then

$$\xi_2 \perp (\mathrm{Ran}(\Pi_{\mathcal{S}}^v) \cup \mathrm{Ran}(\Pi_{\mathcal{A}}^v)).$$

Moreover, we have the following block matrix decomposition

$$
\begin{aligned}
&A(I_{kd} - \Pi_{\mathcal{A}}^v) + pk|\Omega_k^v\rangle\langle\Omega_k^v| + q\Pi_{\mathcal{S}}^v \\
&\cong \begin{pmatrix} (A+q)\Pi_{\mathcal{S}}^v + pk|\xi_1\rangle\langle\xi_1| & pk|\xi_1\rangle\langle\xi_2| \\ pk|\xi_2\rangle\langle\xi_1| & A(I - \Pi_{\mathcal{S}}^v - \Pi_{\mathcal{A}}^v) + pk|\xi_2\rangle\langle\xi_2| \end{pmatrix}.
\end{aligned} \tag{5.2.8}
$$

An important fact to note on (5.2.8) is that $\mathrm{rank}(\Pi_{\mathcal{S}}^v) = \frac{k(k+1)}{2} \geq 2$ and $\mathrm{rank}(I - \Pi_{\mathcal{S}}^v - \Pi_{\mathcal{A}}^v) = d^2 - k^2 \geq 2$ since $1 < k < d$. Therefore, the block matrix in (5.2.8) is positive semidefinite if and only if

$$
\begin{cases}
(a) \quad A + q \geq 0, \\
(b) \quad A \geq 0, \\
(c) \quad A + q + pk\|\xi_1\|^2 \geq 0, \\
(d) \quad A + pk\|\xi_2\|^2 \geq 0, \\
(e) \quad (A + q + pk\|\xi_1\|^2)\,(A + pk\|\xi_2\|^2) \geq (pk)^2\|\xi_1\|^2\|\xi_2\|^2.
\end{cases} \tag{5.2.9}
$$

Since $\|\xi_1\|^2 + \|\xi_2\|^2 = \|\Omega_k^v\|^2 = 1$, the conditions (d) and (e) can be understood as

$$
\begin{cases}
(d') \quad A + pk - pk\|\xi_1\|^2 \geq 0, \\
(e') \quad (A+q)(A+pk) - pkq\|\xi_1\|^2 \geq 0.
\end{cases} \tag{5.2.10}
$$

Note that the first two conditions (a) and (b) are independent of the choices of an orthonormal subset $\{v_i\}_{i=1}^k \subset \mathbb{C}^d$, and that the other inequalities in (c), (d') and (e') are linear in $\|\xi_1\|^2$. Since the inequalities in (c), (d') and (e') should hold for all possible choices of $\{v_i\}_{i=1}^k \subseteq \mathbb{C}^d$, it suffices to calculate the maximum and minimum values of $\|\xi_1\|^2$.

Recall that $|\Omega_k^v\rangle = |\xi_1\rangle \in \mathrm{Ran}(\Pi_{\mathcal{S}}^v)$ whenever $\{v_i\}_{i=1}^k \subset \mathbb{R}^d$ (choose $|v_i\rangle = |i\rangle$ for example), so the maximum of $\|\xi_1\|^2$ is 1. For the minimum of $\|\xi_1\|^2$, the following expression of $\|\xi_1\|^2$ in terms of $v_1, v_2, \cdots, v_k$

$$\begin{aligned}\|\xi_1\|^2 &= \langle \Omega_k^v | \Pi_{\mathcal{S}}^v | \Omega_k^v \rangle \\ &= \langle \Omega_k^v | F_k^v | \Omega_k^v \rangle \quad (\because |\Omega_k^v\rangle \perp \mathrm{Ran}(\Pi_{\mathcal{A}}^v)) \\ &= \frac{1}{k}\sum_{j,j'} \langle v_j | \overline{v_{j'}} \rangle \cdot \langle \overline{v_{j'}} | v_j \rangle = \frac{1}{k}\sum_{j,j'} |\langle v_j | \overline{v_{j'}} \rangle|^2.\end{aligned}$$

allows us to apply Lemma 5.2.3 to conclude that $\min \|\xi_1\|^2 = \frac{\max(2k-d,0)}{k}$.

To summarize, $\mathcal{L}_{p,q} \in \mathcal{POS}_k$ if and only if the six inequalities (a), (b), (c), (d'), (e'), and $A - q \geq 0$ hold for $\|\xi_1\|^2 \in \left\{1, m := \frac{\max(2k-d,0)}{k}\right\}$ and $A = \frac{1-p-q}{d}$. For the cases $1 < k \leq d/2$, we have $m = 0$ and obtain the inequalities in (2). Also, for the cases $d/2 < k < d$, we have $m = \frac{2k-d}{k}$ and obtain the inequalities in (3). In particular, the inequality $f_k(x,y) \leq 0$ is coming from (e') with $\|\xi_1\|^2 = \frac{2k-d}{k}$. □

5.2.2 Schmidt numbers of orthogonally invariant quantum states

Now we are almost ready to compute the Schmidt numbers of all quantum states of the form

$$\rho_{a,b} := \frac{1-a-b}{d^2} I_d \otimes I_d + a|\Omega_d\rangle\langle\Omega_d| + \frac{b}{d} F_d \tag{5.2.11}$$

Let us denote by $S_k := \{(a,b) \in \mathbb{R}^2 : \rho_{a,b} \in \mathbf{Sch}_k\}$. The main aim of this Section is to prove $S_1 \subsetneq S_2 \subsetneq \cdots \subsetneq S_d$ with both geometric and algebraic descriptions. Our strategy is to combine Theorem 4.3.2 and the explicit descriptions of $P_k = \{(p,q) \in \mathbb{R}^2 : \mathcal{L}_{p,q} \in \mathcal{POS}_k\}$ (Theorem 5.2.1).

First of all, Theorem 4.3.2 implies that we have

$$\begin{aligned} &\mathrm{SN}(\rho_{a,b}) \le k \\ \iff& \langle \Omega_d | (\mathrm{id}_d \otimes \mathcal{L}_{p,q})(\rho_{a,b}) | \Omega_d \rangle \ge 0 \text{ for all } (p,q) \in \mathrm{Ext}(P_k) \\ \iff& \begin{pmatrix} p & q \end{pmatrix} \begin{pmatrix} d+1 & 1 \\ 1 & d+1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \ge -\frac{1}{d-1} \text{ for all } (p,q) \in \mathrm{Ext}(P_k). \end{aligned} \tag{5.2.12}$$

Let us denote by

$$H_{p,q} = \left\{ (x,y) \in \mathbb{R}^2 : px + qy \le 1 \right\} \tag{5.2.13}$$

for all $(p,q) \in \mathbb{R}^2 \setminus \{(0,0)\}$, and by $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ a linear isomorphism given by

$$\alpha : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto -(d-1) \begin{pmatrix} d+1 & 1 \\ 1 & d+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{5.2.14}$$

Then we have the following identity:

$$S_k = \bigcap_{(p,q)\in \mathrm{Ext}(P_k)} H_{\alpha(p,q)}. \tag{5.2.15}$$

This is where a detailed geometric analysis of P_k (Theorem 5.2.1) manifests its efficacy. Indeed, Theorem 5.2.1 states that the geometric structures of P_k are categorized into four distinct cases $\begin{cases} (1) & k=1 \\ (2) & 1<k\le \frac{d}{2} \\ (3) & \frac{d}{2}<k<d \\ (4) & k=d \end{cases}$. Furthermore, for the three cases (1), (2), (4), the associated regions P_k are compact convex sets with at most four extreme points. Thus, it is enough to use at most four Schmidt number witnesses $\mathcal{L}_{p,q}$ to determine S_k by Theorem 4.3.2 and (5.2.15), and the consequence is that S_k is an intersection of at most four closed half-planes for the three cases (1), (2), (4). All our discussions above are summarized into the following theorem.

Theorem 5.2.4. *Let $\rho_{a,b}$ be a bipartite matrix of the form* (5.2.2) *and* $1 \leq k \leq d$. *Then we have*

$$S_k = \bigcap_{(p,q) \in \mathrm{Ext}(P_k)} H_{\alpha(p,q)}$$

where α and $H_{p,q}$ are from (5.2.13) *and* (5.2.14). *Moreover, we have the following algebraic descriptions for the three cases* $\begin{cases} (1) & k=1, \\ (2) & 1<k\leq \frac{d}{2}, \\ (4) & k=d. \end{cases}$

1. $\rho_{a,b} \in \mathbf{SEP}$ *if and only if* $\begin{cases} -\frac{1}{d-1} \leq (d+1)a+b \leq 1, \\ -\frac{1}{d-1} \leq a+(d+1)b \leq 1. \end{cases}$

2. $\rho_{a,b} \in \mathbf{Sch}_k$ $(1<k\leq \frac{d}{2})$ *if and only if* $\begin{cases} -\frac{1}{d-1} \leq (d+1)a+b \leq \frac{kd-1}{d-1}, \\ a+(d+1)b \leq 1, \\ -\frac{d-k+1}{kd+k-1}a + b \geq -\frac{1}{d-1}. \end{cases}$

4. $\rho_{a,b} \in \mathbf{Sch}_d = \mathbf{P}$ *if and only if* $\begin{cases} a-(d-1)b \leq 1, \\ a+(d+1)b \leq 1, \\ (d+1)a+b \geq -\frac{1}{d-1}. \end{cases}$

We should remark that the remaining case (3) is quite different from the other cases since there are infinitely many extreme points in P_k. In this case, we will utilize some elementary geometric tools from projective geometry to overcome the technical issue. Indeed, we need a quadratic curve to describe S_k for the cases $\frac{d}{2} < k < d$. This excluded case (3) will be discussed with details independently in Subsection 5.2.2.

Although we postpone the proof of the remaining case $\frac{d}{2} < k < d$ to Subsection 5.2.2, let us exhibit a visualized geometric structures of S_1, S_2, $\cdots$, S_d in the following Figure 5.5, particularly for the cases $d=3$ and $d=4$.

As in the case of k-positivity of $\mathcal{L}_{p,q}$, the geometric structures of the convex subsets S_k can be categorized into the following four distinct cases.

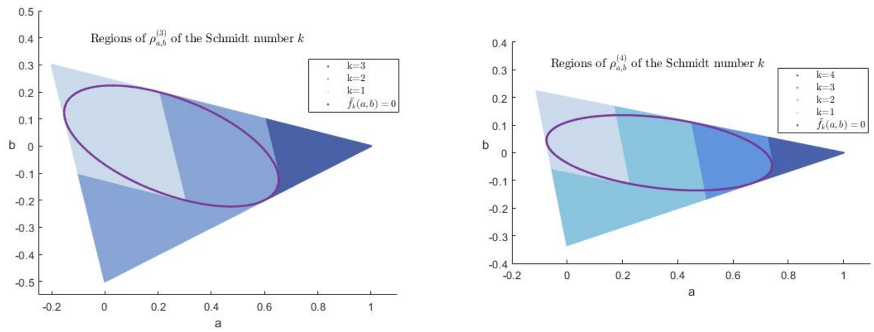

Figure 5.5: Regions of $\rho^{(d)}_{a,b}$ of the Schmidt number k for $d = 3, 4$

1. The region S_1 is *rhombus-shaped* with vertices $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$, $(\frac{1}{d+2}, \frac{1}{d+2})$, $(\frac{d}{d^2+d-2}, -\frac{2}{d^2+d-2})$, and $(-\frac{1}{d^2+d-2}, -\frac{1}{d^2+d-2})$.

2. If $1 < k \leq \frac{d}{2}$, then the region S_k is *trapezoid-shaped* with vertices $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$, $(\frac{kd+k-2}{d^2+d-2}, \frac{d-k}{d^2+d-2})$, $(\frac{kd+k-1}{d^2+d-2}, -\frac{k+1}{d^2+d-2})$, and $(0, -\frac{1}{d-1})$.

3. If $\frac{d}{2} < k < d$, then the region S_k is bounded by a piecewise-linear curve joinig $(\frac{d}{3d-2k}, -\frac{2d-2k}{(d-1)(3d-2k)})$, $(0, -\frac{1}{d-1})$, $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$, $(\frac{kd+k-2}{d^2+d-2}, \frac{d-k}{d^2+d-2})$ and $(\frac{k^2d+k^2+d-3k}{k(d^2+d-2)}, -\frac{(d-k+1)(d-k)}{k(d^2+d-2)})$ in that order, and then joined smoothly by an ellipse from $(\frac{k^2d+k^2+d-3k}{k(d^2+d-2)}, -\frac{(d-k+1)(d-k)}{k(d^2+d-2)})$ to $(\frac{d}{3d-2k}, -\frac{2d-2k}{(d-1)(3d-2k)})$.

4. The region S_d is the same with $P_d = \{(a, b) : \mathcal{L}_{a,b} \in \mathcal{CP}\}$, i.e. S_d is a *triangle* with vertices $(1, 0)$, $(0, -\frac{1}{d-1})$, and $(-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$.

Algebraic descriptions of S_k for the cases $\frac{d}{2} < k < d$

Let us focus on explicit algebraic descriptions of

$$S_k = \bigcap_{(p,q)\in \mathrm{Ext}(P_k)} H_{\alpha(p,q)} = \alpha^{-1}\left(\bigcap_{(p,q)\in \mathrm{Ext}(P_k)} H_{p,q} \right) \tag{5.2.16}$$

for the cases $\frac{d}{2} < k < d$. In this case, we have

$$\mathrm{Ext}(P_k) = \left\{ \left(\frac{-2}{d^2+d-2}, \frac{d}{d^2+d-2} \right), (1, 0), \left(0, \frac{-1}{d-1} \right), \left(\frac{-1}{kd-1}, 0 \right) \right\} \cup C_k$$

by Theorem 5.2.1 (3). Here, C_k is a conic arc in the second quadrant and is parametrized by a smooth, regular, and strictly convex curve

$$\gamma : [0,1] \to C_k \tag{5.2.17}$$

satisfying $f_k(\gamma(t)) \equiv 0$, $\gamma(0) = (-\frac{1}{kd-1}, 0)$ and $\gamma(1) = (-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2})$. Then (5.2.16) implies that $\tilde{S}_k := \alpha(S_k)$ is given by

$$H_{-\frac{2}{d^2+d-2}, \frac{d}{d^2+d-2}} \cap H_{1,0} \cap H_{0,-\frac{1}{d-1}} \cap H_{-\frac{1}{kd-1},0} \cap \bigcap_{t\in[0,1]} H_{\gamma(t)}, \tag{5.2.18}$$

and the most technical problem is to demonstrate that $\bigcap\limits_{t\in[0,1]} H_{\gamma(t)}$ is a convex set bounded by two lines and one conic arc as in the following Figure 5.6.

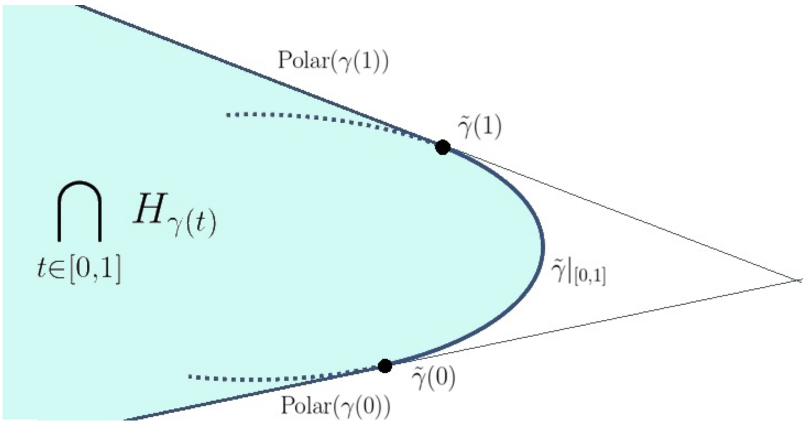

Figure 5.6: Geometric description of the intersection $\bigcap\limits_{t\in[0,1]} H_{\gamma(t)}$

Here, we need to explain the *dual curve* and the *pole-polar duality* from projective geometry [BK86, Cox03]. Firstly, we have an explicit formula for the dual curve $\tilde{\gamma}$ of a strictly convex smooth curve γ. Recall that a plane curve $\gamma : I \to \mathbb{R}^2$ defined on an open interval I is called *strictly convex* if the number of intersection points between γ and an arbitrary line is at most 2. If γ is smooth, then the strict convexity of γ is equivalent to that for every $t \in I$, the image of γ is contained in the same half-plane whose boundary is the tangent line l_t at $\gamma(t)$, and $\gamma(t)$ is the unique intersection point of l_t and γ. For a strictly convex smooth curve $\gamma = (p(t), q(t))$ (with additional conditions in Lemma 5.2.5), we define its dual curve $\tilde{\gamma}$ by

$$\tilde{\gamma}(t) := \left(\frac{q'(t)}{p(t)q'(t) - q(t)p'(t)}, \frac{-p'(t)}{p(t)q'(t) - q(t)p'(t)} \right). \qquad (5.2.19)$$

Secondly, the pole-polar duality is a bijective correspondence between $\mathbb{R}^2 \setminus \{(0,0)\}$ and the set of all lines that are not passing through the origin $(0,0)$ in $\mathbb{R}^2$. Associated to $(p,q) \in \mathbb{R}^2 \setminus \{(0,0)\}$ is a line

$$l = \left\{ (x,y) \in \mathbb{R}^2 : px + qy = 1 \right\}.$$

In this case, we call l the *polar* of P and P the *pole* of l (with respect to the unit circle $C : x^2 + y^2 = 1$), and denote by $l =: \mathrm{Polar}(P)$ and $P =: \mathrm{Pole}(l)$ respectively. Note that we have

$$\tilde{\gamma}(t) = \mathrm{Pole}(l_t)$$

for all $t \in I$, where l_t denotes the line tangent to γ at $\gamma(t)$.

The following Lemma 5.2.5 establishes the connection between the dual curve $\tilde{\gamma}$ and the intersection $\bigcap_{(p,q)\in C_k} H_{p,q}$. This seems a well-known fact, but we provide a proof for readers' convenience.

Lemma 5.2.5. *Let I be an open interval and $\gamma : I \to \mathbb{R}^2 \setminus \{(0,0)\}$ be a smooth, regular, and strictly convex curve. Suppose that for every $t \in I$, the tangent lines l_t at $\gamma(t)$ do not pass through the origin $(0,0)$, and the origin is in the same (closed) half-plane with γ with respect to l_t. Then the dual curve $\tilde{\gamma} : I \to \mathbb{R}^2 \setminus \{(0,0)\}$ from (5.2.19) satisfies the following properties.*

1. $\mathrm{Polar}(\gamma(t))$ *is tangent to $\tilde{\gamma}$ at $\tilde{\gamma}(t)$ for each $t \in I$.*

2. *$\tilde{\gamma}$ is smooth and strictly convex, and the origin is in the same half-plane with $\tilde{\gamma}$ with respect to* $\mathrm{Polar}(\gamma(t))$.

3. *For any closed interval* $[t_0, t_1] \subset I$*, the intersection*

$$\bigcap_{t\in[t_0,t_1]} H_{\gamma(t)}$$

is the largest convex region containing $(0,0)$*, which is bounded by two lines* $\mathrm{Polar}(\gamma(t_0))$ *and* $\mathrm{Polar}(\gamma(t_1))$ *as well as the dual curve* $\tilde{\gamma}|_{[t_0,t_1]}$ *(as in Figure 5.6).*

4. *If* γ *represents a connected part of a conic, then so is* $\tilde{\gamma}$*.*

Proof. Set $\gamma(t) = (p(t), q(t))$. Then the equation of l_t is given by

$$q'(t)(x - p(t)) - p'(t)(y - q(t)) = 0. \qquad (5.2.20)$$

Note that the given assumptions imply that $p(t)q'(t) - q(t)p'(t) \neq 0$ for all $t \in I$, so by continuity, we may assume $p(t)q'(t) - q(t)p'(t) > 0$ for all $t \in I$ without loss of generality. In particular, the dual curve $\widetilde{\gamma}$ from (5.2.19) is a well-defined smooth curve, and (5.2.20) implies that $\tilde{\gamma}(t) = \mathrm{Pole}(l_t)$ for all $t \in I$. Let us write $\tilde{\gamma}(t) = (\tilde{x}(t), \tilde{y}(t))$ for simplicity and explain why the four conclusions (1)-(4) hold.

(1) It is enough to check that

$$\begin{aligned} p(t)\tilde{x}(t) + q(t)\tilde{y}(t) &= 1, \\ p(t)\tilde{x}'(t) + q(t)\tilde{y}'(t) &= 0. \end{aligned}$$

Indeed, the first equation comes from the fact that $\tilde{\gamma}(t) = \mathrm{Pole}(l_t)$, and the second equation is obtained by differentiating the first equation and the identity $p'(t)\tilde{x}(t) + q'(t)\tilde{y}(t) \equiv 0$ from (5.2.19).

(2) Note that the strict convexity of γ implies that

$$q'(t)(p(s) - p(t)) - p'(t)(q(s) - q(t)) < 0, \quad t \neq s \in I, \qquad (5.2.21)$$

which is equivalent to

$$p(s)\tilde{x}(t) + q(s)\tilde{y}(t) < 1, \quad t \neq s \in I. \tag{5.2.22}$$

Thus, both the origin and $\tilde{\gamma}$ are in the same half-plane with respect to $\mathrm{Polar}(\gamma(s))$. Moreover, (5.2.22) implies that $\tilde{\gamma}$ is strictly convex, and smoothness is immediate from the explicit description (5.2.19) of $\tilde{\gamma}$.

(3) Let T be the largest convex region containing $(0,0)$ bounded by two lines $\mathrm{Polar}(\gamma(t_0))$, $\mathrm{Polar}(\gamma(t_1))$, and the dual curve $\tilde{\gamma}|_{[t_0,t_1]}$. First, it is immediate to see that $T \subseteq \bigcap_{t\in[t_0,t_1]} H_{\gamma(t)}$. Indeed, T should be contained in the same plane with $(0,0)$ with respect to each tangent line $l_t = \mathrm{Pole}(\gamma(t))$ for all $t \in I$, and this implies $T \subseteq H_{\gamma(t)}$ for all $t \in [t_0, t_1]$. On the other side, let us pick an element $(u,v) \notin T$ and let l be the straight line passing through the origin and (u,v). Then l intersects with one of $\mathrm{Polar}(\gamma(t_0))$, $\mathrm{Polar}(\gamma(t_1))$, and $\tilde{\gamma}|_{[t_0,t_1]}$. For the first two cases, (u,v) and $(0,0)$ are not on the same half-plane with respect to either $\mathrm{Polar}(\gamma(t_0))$ or $\mathrm{Polar}(\gamma(t_1))$, so $(u,v) \notin \bigcap_{t\in[t_0,t_1]} H_{\gamma(t)}$. For the remaining case, if we suppose that l contains certain $\tilde{\gamma}(t)$, then $(0,0)$ and (u,v) are not on the same plane with respect to $H_{\gamma(t)}$. Hence, we can conclude that $T^c \subseteq \left(\bigcap_{t\in[t_0,t_1]} H_{\gamma(t)}\right)^c$, i.e. $\bigcap_{t\in[t_0,t_1]} H_{\gamma(t)} \subseteq T$.

(4) This is a direct consequence from Plücker's formula [BK86, Section 9.1], which states that the degree of the dual curve $\tilde{\gamma}$ is $n(n-1)$ for any non-singular plane algebraic curve γ of degree n (in our case, $n = 2$). Alternatively, more elementary arguments can be found in [CG96, AZ07]. $\square$

From now on, let us focus more on the special case $\gamma : [0,1] \to C_k$ from (5.2.17). We may assume that γ is extended to the smooth, regular, and strictly convex curve (still denoted by γ) on an open interval $I \supset [0,1]$ such that $f_k \circ \gamma \equiv 0$. Then Lemma 5.2.5 (4) implies that there exists a quadratic polynomial $\tilde{f}_k(x,y)$ such that

$$\tilde{f}_k\left((\alpha^{-1} \circ \tilde{\gamma})(t)\right) \equiv 0.$$

Here, $\tilde{\gamma}$ is the dual curve of γ, and α is the linear isomorphism from (5.2.14). A notable fact is that $\alpha^{-1} \circ \tilde{\gamma}$ always represents an ellipse. For this conclusion, the following lemma provides more concrete information on the quadratic polynomial $\tilde{f}_k(x, y)$.

Lemma 5.2.6. *The quadratic equation $\tilde{f}_k(x, y) = 0$ holds for the following five points (a_i, b_i) $(1 \le i \le 5)$*

$$\left(-\tfrac{d}{k(d^2+d-2)}, \tfrac{d^2-kd+d-2k}{k(d^2+d-2)}\right), \left(\tfrac{d^2-kd+d-k-1}{d^2+d-2}, -\tfrac{d-k+1}{d^2+d-2}\right), \left(\tfrac{2kd-d^2+2k-d-2}{d^2+d-2}, \tfrac{2d-2k}{d^2+d-2}\right),$$
$$\left(\tfrac{k^2d+k^2+d-3k}{k(d^2+d-2)}, -\tfrac{(d-k+1)(d-k)}{k(d^2+d-2)}\right), \left(\tfrac{d}{3d-2k}, -\tfrac{2d-2k}{(d-1)(3d-2k)}\right),$$

with the associated tangent lines l_i $(1 \le i \le 5)$

$$(d+1)x + y = -\tfrac{1}{d-1}, \quad x + (d+1)y = -\tfrac{1}{d-1}, \quad x + (d+1)y = 1,$$
$$(d+1)x + y = \tfrac{kd-1}{d-1}, \quad x - (d-1)y = 1,$$

respectively. Furthermore, if $\frac{d}{2} < k < d$, the conic determined by the equation $\tilde{f}_k(x, y) = 0$ is inscribed in the convex pentagon bounded by the above five tangent lines. In particular, the equation $\tilde{f}_k(x, y) = 0$ should represent an ellipse.

Proof. Let us begin with the following expression

$$f_k(x, y) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F \tag{5.2.23}$$

with the coefficients

$$\begin{cases} A = kd - 1, \quad B = -(d^3 - kd^2 - kd - d + 2), \quad C = d - 1, \\ D = -kd + 2, \quad E = -d + 2, \quad F = -1, \end{cases}$$

from (5.2.4). If we write $\gamma(t) = (p(t), q(t))$, then we have

$$\tilde{\gamma}(t) = -\left(\frac{2Ap(t) + Bq(t) + D}{Dp(t) + Eq(t) + 2F}, \frac{2Cq(t) + Bp(t) + E}{Dp(t) + Eq(t) + 2F}\right) \tag{5.2.24}$$

thanks to (5.2.23) and (5.2.14).

Recall that $\alpha^{-1}(\tilde{\gamma}(t))$ are solutions of the equation $\tilde{f}_k(x,y) = 0$ for all $t \in I$. Thus, in order to single out five points (a_i, b_i) satisfying $\tilde{f}_k(a_i, b_i) = 0$, it is enough to note that the following five points $(p(t_i), q(t_i))$ $(1 \le i \le 5)$

$$(1,0), (0,1), \left(0, \frac{-1}{d-1}\right), \left(\frac{-1}{kd-1}, 0\right), \left(\frac{-2}{d^2+d-2}, \frac{d}{d^2+d-2}\right)$$

are solutions to the equation $f_k(x,y) = 0$. Then (5.2.24) provides us with the associated five points $(a_i, b_i) = \alpha^{-1}(\tilde{\gamma}(t_i))$ listed in the statement. Furthermore, the tangent lines l_i at (a_i, b_i) satisfying $\tilde{f}_k(a_i, b_i) = 0$ are given by $\mathrm{Polar}(\alpha(p(t_i), q(t_i)))$, by Lemma 5.2.5 (1). Thus, we can write down what the tangent lines are explicitly, as in the statement. Lastly, it is immediate to check that when $\frac{d}{2} < k < d$, those five tangent lines consist of a convex pentagon, and the corresponding points (a_i, b_i) of tangency are on each of the pentagon's sides. This observation forces the quadratic equation $\tilde{f}_k(x,y) = 0$ to represent an ellipse inscribed in this pentagon. □

Remark 5.2.7. While the dual quadratic equation $\tilde{f}_k(x,y) = 0$ in our consideration always represents an ellipse thanks to Lemma 5.2.6, the quadratic equation $f_k(x,y) = 0$ can represent both an ellipse and a hyperbola. For example, the quadratic equation $f_k(x,y) = 0$ for $d = 5$ is given by

$$(5k-1)p^2 - (122-30k)pq + 4q^2 - (5k-2)p - 3q - 1 = 0,$$

and this represents a hyperbola if $k = 3$ and an ellipse if $k = 4$.

Finally, we are ready to describe the intersection

$$\bigcap_{(p,q)\in C_k} H_{\alpha(p,q)} = \alpha^{-1}\left(\bigcap_{(p,q)\in C_k} H_{p,q}\right)$$

from (5.2.18). Recall that $\left(\frac{-1}{kd-1}, 0\right)$ and $\left(\frac{-2}{d^2+d-2}, \frac{d}{d^2+d-2}\right)$ are the two endpoints (p,q) of the connected conic arc C_k, and their associated points (a,b) satisfying $\tilde{f}_k(a,b) = 0$ are given by $\left(\frac{k^2d+k^2+d-3k}{k(d^2+d-2)}, -\frac{(d-k+1)(d-k)}{k(d^2+d-2)}\right)$ and $\left(\frac{d}{3d-2k}, -\frac{2d-2k}{(d-1)(3d-2k)}\right)$. Let us denote by L the line segment between these two points, and let us assume (by changing the sign if necessary) that the inequality $\tilde{f}_k(x, y) \leq 0$ represents a filled ellipse.

Corollary 5.2.8. *Let $(a, b) \in \mathbb{R}^2$. Then $(a, b) \in \bigcap_{(p,q)\in C_k} H_{\alpha(p,q)}$ if and only if (a, b) satisfies $\tilde{f}_k(a, b) \leq 0$ or satisfies the following three conditions:*

1. $(d+1)a + b \leq \frac{kd-1}{d-1}$,
2. $a - (d-1)b \leq 1$,
3. $(3d - k + 3)a - (kd + k - 3)b - \frac{d^2+kd-k-3}{d-1} \leq 0$.

Proof. By Lemma 5.2.5 (3) and Lemma 5.2.6, the intersection $\bigcap_{(p,q)\in C_k} H_{\alpha(p,q)}$ is the largest convex region containing $(0, 0)$ bounded by the two tangent lines $(d+1)x + y = \frac{kd-1}{d-1}$, $x - (d-1)y = 1$ and the dual curve $\tilde{\gamma}|_{[0,1]}$. We refer the readers to Figure 5.6 for a visualized understanding. Note that $\tilde{f}_k(x, y) \leq 0$ represents a filled ellipse which we denote by E, and E is a subset of the intersection $\bigcap_{(p,q)\in C_k} H_{\alpha(p,q)}$ by Lemma 5.2.6. Furthermore, $\bigcap_{(p,q)\in C_k} H_{\alpha(p,q)} \setminus E$ is a subset of the largest convex region bounded by the two tangent lines $(d+1)x + y = \frac{kd-1}{d-1}$, $x - (d-1)y = 1$ and the line segment L between $\left(\frac{k^2d+k^2+d-3k}{k(d^2+d-2)}, -\frac{(d-k+1)(d-k)}{k(d^2+d-2)}\right)$ and $\left(\frac{d}{3d-2k}, -\frac{2d-2k}{(d-1)(3d-2k)}\right)$. Hence, the conclusion follows immediately. ☐

Now we are ready to complete the proof for the cases $\frac{d}{2} < k < d$.

Theorem 5.2.9. *Let $\rho_{a,b}$ be a bipartite matrix of the form (5.2.2) and $\frac{d}{2} < k < d$. Then $\rho_{a,b} \in \mathbf{Sch}_k$ if and only if $\tilde{f}_k(a, b) \leq 0$ or (a, b) satisfies the following inequalities:*

$$\begin{cases} -\frac{1}{d-1} \leq (d+1)a + b \leq \frac{kd-1}{d-1}, \\ a + (d+1)b \leq 1, \\ a - (d-1)b \leq 1, \\ (3d - k + 3)a - (kd + k - 3)b - \frac{d^2+kd-k-3}{d-1} \leq 0. \end{cases}$$

Here, $\tilde{f}_k$ is the quadratic polynomial from Lemma 5.2.6 such that the inequality $\tilde{f}_k(x,y) \leq 0$ represents a filled ellipse.

Proof. Since $\bigcap_{(p,q)\in C_k} H_{p,q} \subseteq H_{-\frac{2}{d^2+d-2},\frac{d}{d^2+d-2}} \cap H_{-\frac{1}{kd-1},0}$, we have

$$\tilde{S}_k := \alpha(S_k) = H_{1,0} \cap H_{0,-\frac{1}{d-1}} \cap \bigcap_{(p,q)\in C_k} H_{p,q} \tag{5.2.25}$$

from (5.2.18). Thus, we have

$$\begin{aligned} S_k = \alpha^{-1}(\tilde{S}_k) &= \alpha^{-1}\left(H_{1,0}\right) \cap \alpha^{-1}\left(H_{0,-\frac{1}{d-1}}\right) \cap \alpha^{-1}\left(\bigcap_{(p,q)\in C_k} H_{p,q}\right) \\ &= H_{-(d^2-1),-(d-1)} \cap H_{1,d+1} \cap \bigcap_{(p,q)\in C_k} H_{\alpha(p,q)}. \end{aligned}$$

and the conclusion follows immediately from Lemma 5.2.6 and Corollary 5.2.8.

□

Remark 5.2.10. It is worth remarking that a small perturbation can produce a drastic increment of the Schmidt number. Recall that S_d is a triangle, and let us parameterize the southern-eastern edge of S_d by $\eta : [0,1] \to S_d$ such that $\eta(0) = (0, -\frac{1}{d-1})$ and $\eta(1) = (1,0)$. Then $\rho_{\eta(t)}$ is always entangled, and the Schmidt numbers $\mathrm{SN}(\rho_{\eta(t)})$ exhibit a monotonically increasing pattern of

$$2, \lceil \tfrac{d}{2} \rceil, \lceil \tfrac{d}{2} \rceil + 1, \lceil \tfrac{d}{2} \rceil + 2, \cdots, d,$$

as t increases from 0 to 1. Note that there is a huge gap between 2 and $\lceil \frac{d}{2} \rceil$, which seems entirely new and highly non-trivial. This phenomenon does not appear on the other line segments in the boundary of S_d, and some other known cases such as $\rho_{a,0}$ and $\rho_{0,b}$. The only known patterns were $1, 2, 3, \cdots, d$ (isotropic states) or $1, 2$ (Werner states) to our best knowledge.

5.3 Tripartite systems with unitary group symmetries

Recall that a tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes H_C)$ is called *A-BC separable* (resp. *A-BC PPT*) if ρ is separable (resp. PPT) in the situation where $B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes H_C)$ is understood as the bipartite system $B(\mathcal{H}_A) \otimes B(\mathcal{H}_B \otimes H_C)$. Furthermore, C-AB or B-AC separability (resp. PPT) is defined similarly. We will focus on the situation where $\mathcal{H}_A = \mathcal{H}_B = H_C = \mathbb{C}^d$, and let us denote by

$$\begin{cases} X^{\top_A} = (T_d \otimes \mathrm{id}_{d^2})(X), \\ X^{\top_B} = (I_d \otimes T_d \otimes I_d)(X), \\ X^{\top_C} = (\mathrm{id}_{d^2} \otimes T_d)(X), \end{cases} \tag{5.3.1}$$

the three partial transposes of $X \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes H_C) = M_{d^3}(\mathbb{C})$.

The main purpose of this section is to apply our results in Section 4.3 as new sources to study the problems **PPT** = **SEP**, equivalently the problems $\mathcal{POS} = \mathcal{DEC}$ for some tripartite invariant quantum states. In Section 5.3.1, we exhibit positive non-decomposable covariant maps $\mathcal{L} : M_d \to M_{d^2}$ satisfying

$$\mathcal{L}(\overline{U} X U^T) = (U \otimes U)\mathcal{L}(X)(U \otimes U)^* \tag{5.3.2}$$

for all unitary matrices $U \in \mathcal{U}(d)$ and $X \in M_d$. This result is parallel to the fact **PPT** $\neq$ **SEP** for *tripartite Werner states* [EW01], i.e. tripartite quantum states $\rho \in M_{d^3}(\mathbb{C})$ satisfying

$$(U \otimes U \otimes U)\rho = \rho(U \otimes U \otimes U) \tag{5.3.3}$$

for all unitary matrices $U \in \mathcal{U}(d)$.

On the other hand, in Section 5.3.2, we show that a strong contrast **PPT** = **SEP** holds for *quantum orthogonally invariant* quantum states. More generally, we prove that **PPT** = **SEP** holds for any tripartite quantum states $\rho \in M_{d^3}(\mathbb{C})$ satisfying

$$(U \otimes \overline{U} \otimes U)\rho = \rho(U \otimes \overline{U} \otimes U) \tag{5.3.4}$$

for all unitary matrices $U \in \mathcal{U}(d)$.

5.3.1 Tripartite Werner states

Let π_A, π_{BC} be unitary representations of the unitary group $\mathcal{U}(d)$ given by $\pi_A(U) = \overline{U}$ and $\pi_{BC}(U) = U \otimes U$. Then the elements in InvQS($\overline{\pi_A} \otimes \pi_{BC}$) are called *tripartite Werner states*. Let us write $\mathrm{Inv}(U^{\otimes 3}) = \mathrm{Inv}(\overline{\pi_A} \otimes \pi_{BC})$ and $\mathrm{Cov}(\overline{U}, UU) = \mathrm{Cov}(\pi_A, \pi_{BC})$ for simplicity. The application of Schur-Weyl duality [EW01] or von Neumann's bicommutant theorem [Wat18, Theorem 7.15] implies that the space $\mathrm{Inv}(U^{\otimes 3})$ is spanned by six unitary operators $\{V_\sigma : \sigma \in \mathcal{S}_3\}$. Here, $V_\sigma : (\mathbb{C}^d)^{\otimes 3} \to (\mathbb{C}^d)^{\otimes 3}$ is determined by $V_\sigma(\xi_1 \otimes \xi_2 \otimes \xi_3) = \xi_{\sigma^{-1}(1)} \otimes \xi_{\sigma^{-1}(2)} \otimes \xi_{\sigma^{-1}(3)}$ for any $\xi_1, \xi_2, \xi_3 \in \mathbb{C}^d$ and $\sigma \in \mathcal{S}_3$, or equivalently,

$$V_\sigma = \sum_{j_1, j_2, j_3 = 1}^{d} |j_1 j_2 j_3\rangle\langle j_{\sigma(1)} j_{\sigma(2)} j_{\sigma(3)}|. \tag{5.3.5}$$

Recall that A-BC PPT property and separability of $\rho \in \mathrm{Inv}(U^{\otimes 3})^{\mathcal{D}}$ were already characterized in [EW01], and it was shown that **PPT** = **SEP** if and only if $d = 2$. Therefore, a direct application of Corollary 4.3.4 gives us the following result.

Theorem 5.3.1. *All positive $(UU, \overline{U})$-covariant maps are decomposable if and only if $d = 2$. By taking the adjoint operation $\mathcal{L} \mapsto \mathcal{L}^*$, the same conclusion holds for positive $(\overline{U}, UU)$-covariant maps.*

In the remaining of this section, we will assume $d \geq 3$ and exhibit positive non-decomposable $(\overline{U}, UU)$-covariant maps.

[**Step 1**] First of all, let us characterize all elements in $\mathrm{Cov}(\overline{U}, UU)^{\mathcal{POS}}$. Note that Corollary 4.2.3 (3) implies that the space $\mathrm{Cov}(\overline{U}, UU)$ is spanned by the following six linear maps $\mathcal{L}_\sigma$ whose *unnormalized* Choi matrices are the operators $V_\sigma \in \mathrm{Inv}(U^{\otimes 3})$ in (5.3.5):

$$\begin{cases} \mathcal{L}_e(X) = (\mathrm{Tr}\, X) \cdot I_d \otimes I_d, \\ \mathcal{L}_{(12)}(X) = X^T \otimes I_d, \\ \mathcal{L}_{(13)}(X) = I_d \otimes X^T, \\ \mathcal{L}_{(23)}(X) = (\mathrm{Tr}\, X) \cdot \sum_{j_2,j_3=1}^d |j_3 j_2\rangle\langle j_2 j_3|, \\ \mathcal{L}_{(123)}(X) = \sum_{j_1,j_2,j_3=1}^d X_{j_1 j_2} |j_2 j_3\rangle\langle j_3 j_1|, \\ \mathcal{L}_{(132)}(X) = \sum_{j_1,j_2,j_3=1}^d X_{j_1 j_3} |j_2 j_3\rangle\langle j_1 j_2|. \end{cases} \tag{5.3.6}$$

Lemma 5.3.2. *Let $\mathcal{L} = \sum_{\sigma \in \mathcal{S}_3} a_\sigma \mathcal{L}_\sigma \in \mathrm{Cov}(\overline{U}, UU)$. Then $\mathcal{L} \in \mathcal{POS}_{A,BC}$ if and only if*

$$\begin{cases} (1) \quad a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R} \quad \text{and} \quad a_{(132)} = \overline{a_{(123)}}, \\ (2) \quad a_e \geq \max\left\{-a_{(12)}, -a_{(13)}, |a_{(23)}|\right\}, \\ (3) \quad a_e + a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)} \geq 0, \\ (4) \quad \left(a_e + a_{(12)}\right)\left(a_e + a_{(13)}\right) \geq \left|a_{(23)} + a_{(123)}\right|^2. \end{cases} \tag{5.3.7}$$

Proof. Since every unit vector $\xi \in \mathbb{C}^d$ can be written as $|\xi\rangle = \overline{U}|1\rangle$ for some $U \in \mathcal{U}(d)$, the $(\overline{U}, UU)$-covariance property implies that $\mathcal{L}$ is positive if and only if $\mathcal{L}(e_{11}) \geq 0$. Moreover, $\mathcal{L}(e_{11})$ has a matrix decomposition

$$\begin{aligned} \mathcal{L}(e_{11}) \cong\; & (a_e + a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)}) 1 \oplus (a_e + a_{(23)})\, \mathrm{id}_{d-1} \\ & \oplus \left(\bigoplus_{j=2}^d \begin{bmatrix} a_e + a_{(12)} & a_{(23)} + a_{(123)} \\ a_{(23)} + a_{(132)} & a_e + a_{(13)} \end{bmatrix} \right) \oplus \left(\bigoplus_{2 \leq i < j \leq d} \begin{bmatrix} a_e & a_{(23)} \\ a_{(23)} & a_e \end{bmatrix} \right) \end{aligned} \tag{5.3.8}$$

with respect to the bases $\{|11\rangle\}$, $\{|22\rangle, |33\rangle, \ldots, |dd\rangle\}$, $\{|1j\rangle, |j1\rangle\}$ for $j = 2, \ldots, d$, and $\{|ij\rangle, |ji\rangle\}$ for $2 \leq i < j \leq d$, respectively. Therefore, $\mathcal{L}(e_{11}) \geq 0$ if only if (5.3.7) holds. □

The next step is to classify CP and CCP conditions in $\mathrm{Cov}(\overline{U}, UU)$ to find all PPT elements in $\mathrm{Inv}(U^{\otimes 3})^{\mathcal{D}}$.

Lemma 5.3.3. *Let $\mathcal{L} = \sum_\sigma a_\sigma \mathcal{L}_\sigma$ and let $X = \sum_\sigma a_\sigma V_\sigma$. Then*

1. *$\mathcal{L}$ is CP if and only if $X \geq 0$ if and only if*

$$\begin{cases} a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R} \text{ and } a_{(123)} = \overline{a_{(132)}}, \\ a_e + a_{(123)} + a_{(132)} \geq |a_{(12)} + a_{(13)} + a_{(23)}|, \\ 2a_e - a_{(123)} - a_{(132)} \geq 0, \\ (a_e + \omega a_{(123)} + \overline{\omega} a_{(132)})(a_e + \overline{\omega} a_{(123)} + \omega a_{(132)}) \\ \qquad \geq \left|\omega a_{(12)} + \overline{\omega} a_{(13)} + a_{(23)}\right|^2. \end{cases} \tag{5.3.9}$$

2. *$\mathcal{L}$ is CCP if and only if $X^{\top_A} \geq 0$ if and only if*

$$\begin{cases} a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R} \text{ and } a_{(123)} = \overline{a_{(132)}}, \\ a_e \geq |a_{(23)}|, \\ 2a_e + a_{(123)} + a_{(132)} + d(a_{(12)} + a_{(13)}) \geq 0, \\ \left(a_e + a_{(23)} + \frac{d+1}{2}(a_{(12)} + a_{(13)} + a_{(123)} + a_{(132)})\right) \\ \qquad \times \left(a_e - a_{(23)} + \frac{d-1}{2}(a_{(12)} + a_{(13)} - a_{(123)} - a_{(132)})\right) \\ \qquad \geq \frac{d^2-1}{4}(|a_{(12)} - a_{(13)}|^2 + |a_{(123)} - a_{(132)}|^2). \end{cases} \tag{5.3.10}$$

These characterizations were already known from [EW01, Lemma 2 and Lemma 8], but with a different parametrization. An elaboration on Lemma 5.3.3 is attached in Appendix C using the following identifications

$$\operatorname{span}\{V_\sigma : \sigma \in \mathcal{S}_3\} \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}), \tag{5.3.11}$$

$$\operatorname{span}\left\{V_\sigma^{\top_A} : \sigma \in \mathcal{S}_3\right\} \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}) \tag{5.3.12}$$

as $*$-algebras.

[**Step 2**] All extremal elements in $\mathrm{Cov}_1(\overline{U}, UU)^{\mathcal{POS}}$ are completely characterized in the following lemma. Our proof is straightforward but rather cumbersome, so we attach the proof in Appendix 5.4.2.

Lemma 5.3.4. *Let $\mathcal{L} = \sum_\sigma a_\sigma \mathcal{L}_\sigma \in \mathrm{Cov}(\overline{U}, UU)$. Then the following are equivalent.*

1. $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\overline{U}, UU)^{\mathcal{POS}})$

2. $a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R}$, $a_{(123)} = \overline{a_{(132)}}$, *and the associated 6-tuple*

$$(a_e, a_{(12)}, a_{(13)}, a_{(23)}, Re(a_{(123)}), Im(a_{(123)})) \in \mathbb{R}^6 \tag{5.3.13}$$

is one of the following three types:

Type I	$c_1(1, -1, -1, -1, 1, 0)$
Type II	$c_2(0, A, B, 0, C, \pm\sqrt{AB - C^2})$
Type III	$c_3(\frac{A+B+2C}{2}, \frac{A-B-2C}{2}, \frac{-A+B-2C}{2}, \frac{A+B+2C}{2}, -\frac{A+B}{2}, \pm\sqrt{AB - C^2})$

where $A, B \geq 0$, $C \in \mathbb{R}$, $AB \geq C^2$, *and the normalizing constants* c_1, c_2, *and* c_3 *are chosen to satisfy the TP condition*

$$d^2 a_e + d(a_{(12)} + a_{(13)} + a_{(23)}) + (a_{(123)} + a_{(132)}) = 1. \tag{5.3.14}$$

Then, combining Lemma 5.3.3 and Lemma 5.3.4, we can check that

- Every $\mathcal{L} \in \text{Ext}(\text{Cov}_1(\overline{U}, UU)^{\mathcal{POS}})$ of Type I is CP,
- Every $\mathcal{L} \in \text{Ext}(\text{Cov}_1(\overline{U}, UU)^{\mathcal{POS}})$ of Type II is CCP,
- Let $\mathcal{L} \in \text{Ext}(\text{Cov}_1(\overline{U}, UU)^{\mathcal{POS}})$ of Type III. Then
  - $\mathcal{L}$ is CP if and only if $A = B = C$,
  - $\mathcal{L}$ is CCP if and only if $A = B = -C$.

Thus, Type III (with neither $A = B = C$ nor $A = B = -C$) provides explicit positive non-decomposable maps in $\text{Cov}(\overline{U}, UU)^{\mathcal{POS}}$ by Theorem 4.3.5. For example, we can choose $A = 1, B = 0$, and $C = 0$ to obtain a specific extremal element

$$\mathcal{L}_0 = \mathcal{L}_e + \mathcal{L}_{(12)} - \mathcal{L}_{(13)} + \mathcal{L}_{(23)} - \mathcal{L}_{(123)} - \mathcal{L}_{(132)} \in \text{Ext}(\text{Cov}_1(\overline{U}, UU)^{\mathcal{POS}}) \tag{5.3.15}$$

up to a normalizing constant.

[**Step 3**] On the dual side, the chosen positive non-decomposable map $\mathcal{L}_0^* \in \mathrm{CovPos}(UU, \overline{U})$ should play a role as a PPT entanglement detector. Indeed, if we take

$$\rho_t = \frac{1}{d^3 + (t+1)d^2 + 2t} \left(\frac{d+t}{d} V_e + V_{(13)} + \frac{t}{d} V_{(123)} + \frac{t}{d} V_{(132)} \right) \tag{5.3.16}$$

with $0 < t \leq 3.89$ and $d \geq 3$, then $\rho_t \in \mathrm{Inv}(U^{\otimes 3})^{\mathcal{D}}$ is A-BC PPT by Lemma 5.3.3. Moreover, it is straightforward to see that

$$\begin{aligned} &(d^3 + (t+1)d^2 + 2t) \cdot (\mathrm{id} \otimes \mathcal{L}_0^*)(\rho_t) \\ &= \left(d^2 + (t+2)d + 3t - \frac{2t}{d} \right) \mathrm{id}_d \otimes \mathrm{id}_d - \left(d^2 + (2t+2)d \right) |\Omega_d\rangle\langle\Omega_d| \end{aligned} \tag{5.3.17}$$

has a negative eigenvalue $-t\left(d + \frac{2}{d} - 3\right) < 0$. Consequently, the quantum state ρ_t is A-BC PPT entangled by Theorem 4.3.1 or by Horodecki's criterion.

Remark 5.3.5. Note that ρ_t is also C-AB PPT entangled since $V_{(13)}\rho_t V_{(13)} = \rho_t$. On the other hand, ρ_t is not B-AC PPT (and hence entangled). Indeed, we can observe that

$$\rho_t^{\top_B} = V_{(12)} (V_{(12)} \rho_t V_{(12)})^{\top_A} V_{(12)}, \tag{5.3.18}$$

but $V_{(12)}\rho_t V_{(12)}$ is not A-BC PPT since

$$V_{(12)}\rho_t V_{(12)} = \frac{1}{d^3 + (t+1)d^2 + 2t} \left(\frac{d+t}{d} V_e + V_{(23)} + \frac{t}{d} V_{(123)} + \frac{t}{d} V_{(132)} \right) \tag{5.3.19}$$

does not satisfy the CCP condition (5.3.10).

It might be interesting if we can find a tripartite PPT-entangled Werner state with respect to all the three partitions A-BC, B-AC, and C-AB. However, Lemma 7 of [EW01] implies that there is no such an example $\rho = \sum_\sigma a_\sigma V_\sigma$ if one of the following conditions is satisfied:

- $a_{(12)} = a_{(13)}$ and $a_{(123)} = a_{(132)}$,
- $a_{(13)} = a_{(23)}$ and $a_{(123)} = a_{(132)}$,

- $a_{(23)} = a_{(12)}$ and $a_{(123)} = a_{(132)}$,

We leave the general situation as an open question.

5.3.2 Tripartite quantum orthogonally invariant quantum states

Within the framework of compact quantum groups, it is well-known that the orthogonal group $\mathcal{O}(d)$ allows a universal object, namely the *free orthogonal quantum group* $\mathcal{O}_d^+$ [Wan95, Tim08]. In other words, the invariance property with respect to $\mathcal{O}_d^+$ is a stronger notion than the (classical) orthogonal group invariance. See [LY22] for a general discussion on invariant quantum states and covariant quantum channels with quantum group symmetries.

In this section, we focus on the space $\mathrm{Inv}(O_+^{\otimes 3})$ of the tripartite *quantum orthogonally invariant operators* spanned by five tripartite operators

$$T_\sigma = V_\sigma^{\top_B} = \sum_{j_1,j_2,j_3=1}^{d} |j_1 j_{\sigma(2)} j_3\rangle\langle j_{\sigma(1)} j_2 j_{\sigma(3)}| \tag{5.3.20}$$

for $\sigma \in \mathcal{S}_3 \setminus \{(13)\} = \{e, (12), (23), (123), (132)\}$. See Appendix 5.4.4 for more discussions on (5.3.20) and $\mathcal{O}_d^+$. Although Theorem 4.3.1 does not cover quantum group symmetries, any $X \in \mathrm{Inv}(O_+^{\otimes 3})$ satisfies the following group invariance property

$$(U \otimes \overline{U} \otimes U)X(U \otimes \overline{U} \otimes U)^* = X \tag{5.3.21}$$

for all $U \in \mathcal{U}(d)$ thanks to Corollary 4.2.3 (1). This transfers our problem to the realm of classical group symmetries. More precisely, we have

$$\mathrm{Inv}(O_+^{\otimes 3}) \subseteq \mathrm{Inv}(U \otimes \overline{U} \otimes U) = \mathrm{Inv}(\overline{\pi_A} \otimes \pi_{BC}) \tag{5.3.22}$$

where $\pi_A(U) = \overline{U}$ and $\pi_{BC}(U) = \overline{U} \otimes U$. The main theorem of this section is the following.

Theorem 5.3.6. *Let $\rho \in \mathrm{Inv}(U \otimes \overline{U} \otimes U)^{\mathcal{D}}$. Then ρ is A-BC separable if and only if ρ is A-BC PPT. In particular, A-BC PPT= A-BC SEP holds in* $\mathrm{Inv}(O_+^{\otimes 3})^{\mathcal{D}}$.

Remark 5.3.7. Theorem 5.3.6 implies $\mathcal{POS} = \mathcal{DEC}$ in $\mathrm{Cov}(U, U\overline{U})$ by Corollary 4.3.4, and equivalently, $\mathcal{POS} = \mathcal{DEC}$ in $\mathrm{Cov}(U, \overline{U}U)$. We remark that the latter class was analyzed recently in [COS18, BCS20]. In particular, k-positivity and decomposability were discussed for a special subclass of $\mathrm{Cov}(U, \overline{U}U)$ for $d = 3$ in [COS18], and it was questioned whether certain 2-positive non-decomposable map exists in $\mathrm{Cov}(U, \overline{U}U)$. However, our Theorem 5.3.6 gives the complete answer $\mathcal{POS} = \mathcal{DEC}$ in the whole class $\mathrm{Cov}(U, \overline{U}U)$ regardless of the dimension d, and this means that (k-)positive non-decomposable maps cannot exist in $\mathrm{Cov}(U, \overline{U}U)$.

Remark 5.3.8. Note that, for any unitary representation π of a compact group, the following three problems

- $\mathbf{PPT}_{A,BC} = \mathbf{SEP}_{A,BC}$ in $\mathrm{Inv}(\pi \otimes \pi \otimes \pi)$
- $\mathbf{PPT}_{B,AC} = \mathbf{SEP}_{B,AC}$ in $\mathrm{Inv}(\pi \otimes \pi \otimes \pi)$
- $\mathbf{PPT}_{C,AB} = \mathbf{SEP}_{C,AB}$ in $\mathrm{Inv}(\pi \otimes \pi \otimes \pi)$

are equivalent. However, Theorem 5.3.6 implies that this equivalence is no longer true when π is replaced by a unitary representation of a compact quantum group. Indeed, a B-AC PPT entangled state $V_{(12)}\rho_t V_{(12)} \in \mathrm{Inv}(U^{\otimes 3})$ from (5.3.19) is transferred to the following B-AC PPT entangled state in $\mathrm{Inv}(O_+^{\otimes 3})$:

$$\begin{aligned}
&(V_{(12)}\rho_t V_{(12)})^{\top_B} \\
&= \frac{1}{d^3 + (t+1)d^2 + 2t}\left(\frac{d+t}{d}T_e + T_{(23)} + \frac{t}{d}T_{(123)} + \frac{t}{d}T_{(132)}\right). \qquad (5.3.23)
\end{aligned}$$

In other words, the problem of $\mathbf{PPT}_{A,BC} = \mathbf{SEP}_{A,BC}$ is not equivalent to the problem of$\mathbf{PPT}_{B,AC} = \mathbf{SEP}_{B,AC}$ in $\mathrm{Inv}(O_+^{\otimes 3})^{\mathcal{D}}$. A reason for this genuine quantum phenomenon is that the associated C^*-algebra of $\mathcal{O}_d^+$ is non-commutative.

[**Step 1**] Let us apply Corollary 4.3.4 to prove that $\mathcal{POS} = \mathcal{DEC}$ holds in $\mathrm{Cov}_1(\overline{U}U, \overline{U})^{\mathcal{POS}} = \mathrm{Cov}_1(\pi_{BC}, \pi_A)^{\mathcal{POS}}$, or equivalently, $\mathcal{POS} = \mathcal{DEC}$ holds in $\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}}$. Recall that the space $\mathrm{Cov}(\overline{U}, \overline{U}U)$ is spanned by six linear maps

$$\mathcal{M}_\sigma = (T_d \otimes I_d) \circ \mathcal{L}_\sigma \tag{5.3.24}$$

for $\sigma \in \mathcal{S}_3$, where $\mathcal{L}_\sigma$ is given by (5.3.6). Then the unnormalized Choi matrix of $\mathcal{M}_\sigma$ is given by T_σ.

Lemma 5.3.9. *Let $d \geq 3$ and $\mathcal{M} = \sum_\sigma a_\sigma \mathcal{M}_\sigma \in \mathrm{Cov}(\overline{U}, \overline{U}U)$. Then $\mathcal{M}$ is positive if and only if*

$$\begin{cases} (1) \quad a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R} \ \ \textit{and} \ \ a_{(132)} = \overline{a_{(123)}}, \\ (2) \quad a_e \geq \max\left\{0, -a_{(12)}, -a_{(13)}\right\}, \\ (3) \quad a_e + a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)} \geq 0, \\ (4) \quad a_e + (d-1)a_{(23)} \geq 0, \\ (5) \quad (a_e + a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)})(a_e + (d-1)a_{(23)}) \\ \qquad\qquad \geq (d-1)|a_{(23)} + a_{(123)}|^2. \end{cases} \tag{5.3.25}$$

Proof. As in the proof of Lemma 5.3.2, the positivity of $\mathcal{M}$ is equivalent to $\mathcal{M}(e_{11}) \geq 0$. Moreover, $\mathcal{M}(e_{11}) \in M_d \otimes M_d$ has a matrix decomposition

$$M \oplus (a_e + a_{(12)})\ \mathrm{id}_{d-1} \oplus (a_e + a_{(13)})\ \mathrm{id}_{d-1} \oplus a_e\ \mathrm{id}_{(d-1)(d-2)}, \tag{5.3.26}$$

where

$$M = \begin{bmatrix} c & (a_{(23)} + a_{(132)})\langle v| \\ (a_{(23)} + a_{(123)})|v\rangle & a_{(23)}|v\rangle\langle v| \end{bmatrix} + a_e\, I_d \tag{5.3.27}$$

with $c = a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)}$ and $v = (1, 1, \ldots, 1)^T \in \mathbb{C}^{d-1}$. The four matrices in the matrix decomposition (5.3.26) are with respect to the bases $\{|11\rangle, |22\rangle, \ldots, |dd\rangle\}$, $\{|12\rangle, |13\rangle, \ldots, |1d\rangle\}$, $\{|21\rangle, |31\rangle, \ldots, |d1\rangle\}$, and $\{|ij\rangle : i, j \neq 1 \text{ and } i \neq j\}$, respectively. Thus, $\mathcal{M}(e_{11}) \geq 0$ if and only if the conditions (1) and (2) in (5.3.25) hold and $M \geq 0$. Moreover, we can rewrite (5.3.27) as

$$M - a_e I_d = V \begin{bmatrix} c & \sqrt{d-1}\overline{\alpha} \\ \sqrt{d-1}\alpha & (d-1)a_{(23)} \end{bmatrix} V^*, \tag{5.3.28}$$

where $\alpha = a_{(23)} + a_{(123)}$ and $V = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{d-1}}|v\rangle \end{bmatrix} \in M_{d,2}(\mathbb{C})$ is an isometry. Thus, the nonzero eigenvalues of $M - a_e I_d$ are the same with those of $\begin{bmatrix} c & \sqrt{d-1}\overline{\alpha} \\ \sqrt{d-1}\alpha & (d-1)a_{(23)} \end{bmatrix}$. Consequently, the condition $M \geq 0$ is equivalent to the conditions (3), (4), and (5) of (5.3.25). $\square$

Thanks to Lemma 5.3.3, it is easy to derive CP and CCP conditions in $\mathrm{Cov}(\overline{U}, \overline{U}U)$ or A-BC PPT condition in $\mathrm{Inv}(U \otimes \overline{U} \otimes U)^{\mathcal{D}}$.

Lemma 5.3.10. *Let $d \geq 3$ and $\mathcal{M} = \sum_{\sigma \in \mathcal{S}_3} a_\sigma \mathcal{M}_\sigma \in \mathrm{Cov}(\overline{U}, \overline{U}U)^{\mathcal{POS}}$. Then*

1. *$\mathcal{M}$ is CP if and only if the operator*

$$V_{(12)} \left(\sum_{\sigma \in \mathcal{S}_3} a_\sigma V_\sigma \right) V_{(12)} = \sum_{\sigma \in \mathcal{S}_3} a_{(12)\sigma(12)} V_\sigma \tag{5.3.29}$$

satisfies the condition (5.3.10).

2. *$\mathcal{M}$ is CCP if and only if the operator*

$$V_{(13)} \left(\sum_{\sigma \in \mathcal{S}_3} a_\sigma V_\sigma \right) V_{(13)} = \sum_{\sigma \in \mathcal{S}_3} a_{(13)\sigma(13)} V_\sigma \tag{5.3.30}$$

satisfies the condition (5.3.10).

Proof. Let $X = \sum_{\sigma \in \mathcal{S}_3} a_\sigma V_\sigma \in \mathrm{Inv}(U^{\otimes 3})$ and $X' = V_{(12)} X V_{(12)}$. Then $\mathcal{M}$ is

CP if and only if

$$\sum_{\sigma\in\mathcal{S}_3} a_\sigma T_\sigma = X^{\top_B} = V_{(12)}(X')^{\top_A}V_{(12)} \geq 0, \tag{5.3.31}$$

which is equivalent to $(X')^{\top_A} \geq 0$. On the other hand, let $X'' = V_{(13)}XV_{(13)}$. Then $\mathcal{M}$ is CCP if and only if

$$\left(\sum_{\sigma\in\mathcal{S}_3} a_\sigma T_\sigma\right)^{\top_A} = \left(X^{\top_C}\right)^T = \left(V_{(13)}(X'')^{\top_A}V_{(13)}\right)^T \geq 0, \tag{5.3.32}$$

and this is equivalent to $(X'')^{\top_A} \geq 0$. □

[**Step 2**] We refer the reader to Appendix 5.4.2 for a proof of the following Lemma 5.3.11 classifying all extremal elements in $\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}}$.

Lemma 5.3.11. *Let $d \geq 3$ and $\mathcal{M} = \sum_{\sigma\in\mathcal{S}_3} a_\sigma \mathcal{M}_\sigma \in \mathrm{Cov}(\overline{U}, \overline{U}U)^{\mathcal{POS}}$. Then the following are equivalent.*

1. $\mathcal{M} \in \mathrm{Ext}(\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}})$,

2. $a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R}$, $a_{(123)} = \overline{a_{(132)}}$, *and the associated 6-tuple*

$$(a_e, a_{(12)}, a_{(13)}, a_{(23)}, Re(a_{(123)}), Im(a_{(123)})) \in \mathbb{R}^6 \tag{5.3.33}$$

is one of the following four types:

$$\begin{array}{ll} \textit{Type I} & c_1(d-1, -1, 1-d, -1, 1, 0), \\ \textit{Type II} & c_2(d-1, 1-d, -1, -1, 1, 0), \\ \textit{Type III} & c_3(0, A+B-2C, 0, B, C-B, \pm\sqrt{AB-C^2}), \\ \textit{Type IV} & c_4(0, 0, A+B-2C, B, C-B, \pm\sqrt{AB-C^2}), \end{array}$$

where $A, B \geq 0$, $C \in \mathbb{R}$, $AB \geq C^2$, and c_i $(i = 1, 2, 3, 4)$ are normalizing constants chosen to satisfy the TP condition

$$d^2 a_e + d(a_{(12)} + a_{(13)} + a_{(23)}) + (a_{(123)} + a_{(132)}) = 1. \tag{5.3.34}$$

Proof of Theorem 5.3.6. Let us assume $d \geq 3$. According to Theorem 4.3.5 and Lemma 5.3.11, it suffices to show that $\mathcal{M} = \sum_{\sigma\in\mathcal{S}_3} a_\sigma \mathcal{M}_\sigma$ is CP or CCP whenever $(a_\sigma)_{\sigma\in\mathcal{S}_3}$ is one of the four Types I - IV. Now, by applying Lemma 5.3.10, we can check that

- Every $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}})$ of Type I or Type III is CP,
- Every $\mathcal{L} \in \mathrm{Ext}(\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}})$ of Type II or Type IV CCP,

thanks to the conditions $A, B \geq 0$ and $AB \geq C^2$. When $d = 2$, we refer to Appendix 5.4.3 for the complete proof. □

5.4 Appendix for Section 5.3

5.4.1 Characterization of $\mathrm{Inv}(U^{\otimes 3})^{\mathbf{PPT}}$

Recall that if $d \geq 3$, there exist $*$-algebra isomorphisms

$$F : \mathrm{Inv}(U \otimes U \otimes U) \to \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}), \tag{5.4.1}$$

$$G : \mathrm{Inv}(\overline{U} \otimes U \otimes U) \to \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}) \tag{5.4.2}$$

by the representation theory of the unitary group $\mathcal{U}(d)$. Moreover, the authors in [EW01] proposed specific choice of $*$-isomorphisms F and G that can be used to characterize the PPT condition of $X = \sum_{\sigma\in\mathcal{S}_3} a_\sigma V_\sigma \in \mathrm{Inv}(U^{\otimes 3})$. For the convenience of the reader, we again present explicit maps F and G in terms of the bases $\{V_\sigma : \sigma \in \mathcal{S}_3\}$ and $\left\{V_\sigma^{\top_A} : \sigma \in \mathcal{S}_3\right\}$ of $\mathrm{Inv}(U^{\otimes 3})$ and $\mathrm{Inv}(\overline{U} \otimes U \otimes U)$, respectively, in Table 2.

Proof of Lemma 5.3.3. Let $X = \sum_{\sigma\in\mathcal{S}_3} a_\sigma V_\sigma$. Then $X^* = X$ is equivalent to $a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R}$ and $a_{(123)} = \overline{a_{(132)}}$ since $\{V_\sigma\}_{\sigma\in\mathcal{S}_3}$ is linearly

Table 5.2: The isomorphisms F and G $(\omega = e^{2\pi i/3})$

X	$F(X)$	$X^{\top_A}$	$G(X^{\top_A})$
V_e	$(1, 1, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix})$	$V_e^{\top_A}$	$(1, 1, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix})$
$V_{(12)}$	$(1, -1, \begin{bmatrix} 0 & \overline{\omega} \\ \omega & 0 \end{bmatrix})$	$V_{(12)}^{\top_A}$	$(0, 0, \begin{bmatrix} \frac{d+1}{2} & \frac{\sqrt{d^2-1}}{2} \\ \frac{\sqrt{d^2-1}}{2} & \frac{d-1}{2} \end{bmatrix})$
$V_{(13)}$	$(1, -1, \begin{bmatrix} 0 & \omega \\ \overline{\omega} & 0 \end{bmatrix})$	$V_{(13)}^{\top_A}$	$(0, 0, \begin{bmatrix} \frac{d+1}{2} & -\frac{\sqrt{d^2-1}}{2} \\ -\frac{\sqrt{d^2-1}}{2} & \frac{d-1}{2} \end{bmatrix})$
$V_{(23)}$	$(1, -1, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix})$	$V_{(23)}^{\top_A}$	$(1, -1, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix})$
$V_{(123)}$	$(1, 1, \begin{bmatrix} \overline{\omega} & 0 \\ 0 & \omega \end{bmatrix})$	$V_{(123)}^{\top_A}$	$(0, 0, \begin{bmatrix} \frac{d+1}{2} & -\frac{\sqrt{d^2-1}}{2} \\ \frac{\sqrt{d^2-1}}{2} & -\frac{d-1}{2} \end{bmatrix})$
$V_{(132)}$	$(1, 1, \begin{bmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{bmatrix})$	$V_{(132)}^{\top_A}$	$(0, 0, \begin{bmatrix} \frac{d+1}{2} & \frac{\sqrt{d^2-1}}{2} \\ -\frac{\sqrt{d^2-1}}{2} & -\frac{d-1}{2} \end{bmatrix})$

independent. Now $X \geq 0$, or equivalently, $F(X) \geq 0$ holds if and only if

$$(a_e + a_{(123)} + a_{(132)}) \pm (a_{(12)} + a_{(13)} + a_{(23)}) \geq 0 \quad \text{and} \tag{5.4.3}$$

$$\begin{bmatrix} a_e + \overline{\omega} a_{(123)} + a_{(123)}\omega & \overline{\omega} a_{(12)} + \omega a_{(13)} + a_{(23)} \\ \omega a_{(12)} + \overline{\omega} a_{(13)} + a_{(23)} & a_e + \omega a_{(123)} + \overline{\omega} a_{(132)} \end{bmatrix} \geq 0, \tag{5.4.4}$$

which is equivalent to the condition (5.3.9). Similarly, we get the equivalence between the condition $X^{\top_A} \geq 0$ and (5.3.10). □

5.4.2 Extremal positive maps in $\mathrm{Cov}_1(\overline{U}, UU)^{\mathcal{POS}}$ and $\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}}$

This section is to give detailed proofs of Lemma 5.3.4 and Lemma 5.3.11. For convenience, we assume $a_e, a_{(12)}, a_{(13)}, a_{(23)} \in \mathbb{R}$, $a_{(123)} = \overline{a_{(132)}}$, and write $r = \mathrm{Re}(a_{(123)})$ and $s = \mathrm{Im}(a_{(123)})$ throughout this section.

Let $\mathcal{P}_0$ be the set of all tuples $(a_e, a_{(12)}, a_{(13)}, a_{(23)}, r, s)$ satisfying (5.3.7) and the TP condition

$$d^2 a_e + d(a_{(12)} + a_{(13)} + a_{(23)}) + (a_{(123)} + a_{(132)}) = 1. \tag{5.4.5}$$

Then $\mathcal{P}_0$ describes the condition $\sum_\sigma a_\sigma \mathcal{L}_\sigma \in \mathrm{Cov}_1(\overline{U}, UU)^{\mathcal{POS}}$ exactly, so $\mathcal{P}_0$ must be a convex and compact subset of $\mathbb{R}^6$. For simplification of the condition (5.3.7), let us consider a linear isomorphism

$$\alpha : (a_e, a_{(12)}, a_{(13)}, a_{(23)}, r, s) \mapsto (a_e, A, B, C, r, s) \tag{5.4.6}$$

of $\mathbb{R}^6$, where $A = a_e + a_{(12)}$, $B = a_e + a_{(13)}$, and $C = a_{(23)} + r$. Then $\mathcal{P} = \alpha(\mathcal{P}_0)$ is the set of all tuples $(a_e, A, B, C, r, s) \in \mathbb{R}^6$ satisfying

$$\begin{cases} (1) & A, B \geq 0, \\ (2) & AB \geq C^2 + s^2, \\ (3) & A + B + C + r \geq a_e \geq |C - r|, \\ (4) & d(d-2)a_e + d(A + B + C) - (d-2)r = 1. \end{cases} \tag{5.4.7}$$

Note that we have $\mathrm{Ext}(\mathcal{P}_0) = \alpha^{-1}(\mathrm{Ext}(\mathcal{P}))$. That is, it suffices to find the extreme points of $\mathcal{P}$ and restore the coefficients $(a_\sigma)_{\sigma \in \mathcal{S}_3}$ to get the corresponding extremal positive $(\overline{U}, UU)$-covariant maps.

Lemma 5.4.1. *Let $\mathcal{S}$ be the set of tuples (A, B, C, s) satisfying (1) and (2) of (5.4.7). Then $\mathcal{S}$ is a convex cone in $\mathbb{R}^4$. Moreover, if $x_0 = x_1 + x_2$ in $\mathcal{S}$ with $x_i = (A_i, B_i, C_i, s_i)$ and if $A_0 B_0 = C_0^2 + s_0^2$, then $x_1 = \lambda_1 x_0, x_2 = \lambda_2 x_0$ for some $\lambda_1, \lambda_2 \geq 0$. In other words, the half-line $\mathbb{R}_+ x_0$ is an extremal ray of $\mathcal{S}$.*

Proof. It is straightforward that $x \in \mathcal{S}$ implies $\lambda x \in \mathcal{S}$ for all $\lambda \geq 0$. Let us write $x_i = (A_i, B_i, C_i, s_i) \in \mathcal{S}$ for $i = 1, 2$. Then $A_1 + A_2 \geq 0$ and $B_1 + B_2 \geq 0$, so the last thing to check is

$$(A_1 + A_2) \cdot (B_1 + B_2) \geq (C_1 + C_2)^2 + (s_1 + s_2)^2. \tag{5.4.8}$$

Let us choose $C_i' \geq |C_i|$, $s_i' \geq |s_i|$ such that $A_iB_i = (C_i')^2 + (s_i')^2$. Then, indeed, we have

$$(A_1 + A_2)(B_1 + B_2) \geq A_1B_1 + 2\sqrt{A_1B_1A_2B_2} + A_2B_2 \tag{5.4.9}$$
$$= (C_1')^2 + (s_1')^2 + 2\sqrt{((C_1')^2 + (s_1')^2)((C_2')^2 + (s_2')^2)} + (C_2')^2 + (s_2')^2 \tag{5.4.10}$$
$$\geq (C_1')^2 + (s_1')^2 + 2(C_1'C_2' + s_1's_2') + (C_2')^2 + (s_2')^2 \tag{5.4.11}$$
$$= (C_1' + C_2')^2 + (s_1' + s_2')^2 \geq (C_1 + C_2)^2 + (s_1 + s_2)^2. \tag{5.4.12}$$

by applying the AM-GM inequality and the Cauchy-Schwarz inequality. Therefore, $x_1 + x_2 \in \mathcal{S}$, which proves that $\mathcal{S}$ is a convex cone. The latter statement follows by investigating the equality condition carefully in the above inequality, which is left to the reader. □

Proof of Lemma 5.3.4. It is sufficient to show that all the extreme points $\mathbf{x} = (a_e, A, B, C, r, s)$ of $\mathcal{P}$ are classified into the following three types up to normalizing constants: for $A, B \geq 0$ and $AB \geq C^2$,

Type I′	$(1, 0, 0, 0, 1, 0)$,
Type II′	$(0, A, B, C, C, \pm\sqrt{AB - C^2})$,
Type III′	$(\frac{A+B+2C}{2}, A, B, C, -\frac{A+B}{2}, \pm\sqrt{AB - C^2})$.

If $AB > C^2 + s^2$, then we can choose $s' > |s|$ such that $AB = C^2 + (s')^2$. In this case, $\mathbf{x}_\pm^{(0)} = (a_e, A, B, C, r, \pm s') \in \mathcal{P}$, and $\mathbf{x}$ is a (nontrivial) convex combination of $\mathbf{x}_+^{(0)}$ and $\mathbf{x}_-^{(0)}$. Thus, $\mathbf{x}$ is not extremal in $\mathcal{P}$.

From now on, we assume $AB = C^2 + s^2$ (i.e., $s = \pm\sqrt{AB - C^2}$) and divide the condition (3) of (5.4.7) into the following cases.

[Case 1] $A + B + C + r \geq a_e > |C - r|$. Then for sufficiently small $\delta > 0$,

$$\mathbf{x}_\pm^{(1)} = \left(a_e \mp \frac{2(A+B+C)}{d-2}\delta, A \pm A\delta, B \pm B\delta, C \pm C\delta, r \mp \frac{d(A+B+C)}{d-2}\delta, s \pm s\delta\right) \tag{5.4.13}$$

are elements of $\mathcal{P}$, and $\mathbf{x} = (\mathbf{x}_+^{(1)} + \mathbf{x}_-^{(1)})/2$. Therefore, $\mathbf{x} \notin \mathrm{Ext}(\mathcal{P})$.

[Case 2] $A + B + C + r > a_e = |C - r| > 0$. Here we consider only the case $C > r$ since the other case $C < r$ can be argued similarly. Then for sufficiently small $\delta > 0$,

$$\mathbf{x}_{\pm}^{(2)} = (a_e \pm (C-k)\delta, A \pm A\delta, B \pm B\delta, C \pm C\delta, r \pm k\delta, s \pm s\delta) \qquad (5.4.14)$$

are elements of $\mathcal{P}$, where $k \in \mathbb{R}$ satisfies

$$d(d-2)(C-k) + d(A+B+C) - (d-2)k = 0 \qquad (5.4.15)$$

so that the condition (4) of (5.4.7) holds for $\mathbf{x}_{\pm}^{(2)}$. Since $\mathbf{x} = (\mathbf{x}_{+}^{(2)} + \mathbf{x}_{-}^{(2)})/2$, it is not extremal.

[Case 3] $A+B+C+r \geq a_e = |C-r| = 0$, so $C = r$. We claim that $\mathbf{x} = (0, A, B, C, C, s) \in \mathrm{Ext}(\mathcal{P})$ corresponding to Type II$'$. Suppose that $\mathbf{x}$ is a convex combination of $\mathbf{x}_{\pm}^{(3)} = (a_{\pm}, A_{\pm}, B_{\pm}, C_{\pm}, r_{\pm}, s_{\pm}) \in \mathcal{P}$. Then the condition $a_e = 0$ and $a_{\pm} \geq 0$ imply $a_{\pm} = 0$, which again forces $|C_{\pm} - r_{\pm}| = 0$. Therefore, Lemma 5.4.1 implies that $\mathbf{x}_{\pm}^{(3)} = (0, A_{\pm}, B_{\pm}, C_{\pm}, C_{\pm}, s_{\pm}) = \lambda_{\pm}\mathbf{x}$ for some $\lambda_{\pm} \geq 0$. Now the TP condition (5.4.7) (4) implies $\lambda_{\pm} = 1$, so $\mathbf{x} = \mathbf{x}_{\pm}^{(3)}$.

[Case 4] $A+B+C+r = a_e = C-r \geq 0$. Then $r = -\frac{A+B}{2}$ and $\mathbf{x} = (\frac{A+B+2C}{2}, A, B, C, -\frac{A+B}{2}, s)$. Here we claim that $\mathbf{x} \in \mathrm{Ext}(\mathcal{P})$ which corresponds to Type III$'$ (note that $A+B \geq 2\sqrt{AB} = 2\sqrt{C^2+s^2} \geq 2|C|$, so $r = -\frac{A+B}{2}$ conversely implies $C \geq r$). If $\mathbf{x}$ is a convex combination of $\mathbf{x}_{\pm}^{(4)} = (a_{\pm}, A_{\pm}, B_{\pm}, C_{\pm}, r_{\pm}, s_{\pm}) \in \mathcal{P}$, then the condition (5.4.7) (3) for $\mathbf{x}_{\pm}^{(4)}$ implies $A_{\pm}+B_{\pm}+C_{\pm}+r_{\pm} = a_{\pm} = |C_{\pm}-r_{\pm}|$. We may assume $A_+ \geq A \geq A_-$ without loss of generality, so Lemma 5.4.1 implies

$$\mathbf{x}_{+}^{(4)} = \left(\frac{A+B+2C}{2} + \delta', A + A\delta, B + B\delta, C + C\delta, -\frac{A+B}{2} + \delta'', s + s\delta\right) \qquad (5.4.16)$$

for some $\delta \geq 0$, $\delta', \delta'' \in \mathbb{R}$, and $\delta' = (A+B+C)\delta + \delta''$ from $A_+ + B_+ + C_+ + r_+ = a_+$. Now for the case $a_+ = r_+ - C_+ \geq 0$, we have

$$0 \leq A+B+2C = -(A+B+2C)\delta \leq 0. \qquad (5.4.17)$$

However, this says $A+B = -2C$ and $\mathbf{x} = (0, A, B, C, C, s)$, which can be absorbed into *Case 3*. For the case $a_+ = C_+ - r_+$, we have $\delta'' = -\frac{A+B}{2}\delta$ and $\delta' = \frac{A+B+2C}{2}\delta$. However, then the TP condition (5.4.7) (4) implies

$$\left(d(d-2)\frac{A+B+2C}{2} + d(A+B+C) + (d-2)\frac{A+B}{2}\right)\delta = 0, \quad (5.4.18)$$

which is possible only if $\delta = 0$. Therefore, $\mathbf{x} = \mathbf{x}_+^{(4)} = \mathbf{x}_-^{(4)}$.

[Case 5] $A+B+C+r = a_e = r - C \geq 0$. Then $A+B = -2C$, and the previous inequality $A+B \geq 2\sqrt{AB} \geq 2|C|$ implies $A = B = -C \geq 0$ and $s = 0$. Thus, $\mathbf{x} = (r-C, -C, -C, C, r, 0)$ with $C \leq 0$ and $r \geq C$. Then our problem is divided into the following three subcases.

- If $C < 0$ and $r > C$, then $\mathbf{x} \notin \mathrm{Ext}(\mathcal{P})$ since $\mathbf{x} = (\mathbf{x}_+^{(5)} + \mathbf{x}_-^{(5)})/2$, where

$$\mathbf{x}_\pm^{(5)} = \left(r - C \mp \frac{2}{d-2}\delta, -C \pm \delta, -C \pm \delta, C \mp \delta, r \mp \frac{d}{d-2}\delta, 0\right) \in \mathcal{P} \quad (5.4.19)$$

  for sufficiently small $\delta > 0$.

- If $r = C$, then $\mathbf{x} = (0, -C, -C, C, C, 0)$ is extremal since it can be absorbed into *Case 3*.

- If $C = 0$, then $\mathbf{x} = r(1,0,0,0,1,0)$ is indeed extremal (corresponding to Type I′) since the point $(A,B,C,s) = (0,0,0,0)$ is an extreme point of $\mathcal{S}$ in Lemma 5.4.1 and since r is uniquely determined by the TP condition (5.4.7) (4).

□

Now we shall prove Lemma 5.3.11 using similar arguments. Let $\mathcal{Q}_0$ be the set of all tuples $(a_e, a_{(12)}, a_{(13)}, a_{(23)}, r, s)$ satisfying (5.3.25) and (5.4.5), and then consider a linear isomorphism

$$\beta : (a_e, a_{(12)}, a_{(13)}, a_{(23)}, r, s) \mapsto (A, B, C, p, q, s) \quad (5.4.20)$$

of $\mathbb{R}^6$, where $\begin{cases} A = \sum_{\sigma \in \mathcal{S}_3} a_\sigma, \ B = \frac{a_e}{d-1} + a_{(23)}, \ C = a_{(23)} + r, \\ p = a_e + a_{(12)}, \ q = a_e + a_{(13)}. \end{cases}$ Then $\mathcal{Q} =$

$\beta(\mathcal{Q}_0)$ becomes the set of all tuples $(A, B, C, p, q, s) \in \mathbb{R}^6$ satisfying

$$\begin{cases} (1) \quad A, B, p, q \geq 0, \\ (2) \quad AB \geq C^2 + s^2, \\ (3) \quad A + B - 2C \leq p + q, \\ (4) \quad (-d^2 + d + 1)A - (d-1)^2 B + 2d(d-1)C + (d^2-1)(p+q) = 1. \end{cases} \tag{5.4.21}$$

Proof of Lemma 5.3.11. It is sufficient to show that the extreme points $\mathbf{y} = (A, B, C, p, q, s)$ of $\mathcal{Q}$ are classified into the following four types up to normalizing constants: for $A, B \geq 0$ and $AB \geq C^2$,

$$\begin{array}{ll} \text{Type I}' & (0,0,0,1,0,0), \\ \text{Type II}' & (0,0,0,0,1,0), \\ \text{Type III}' & (A, B, C, A+B-2C, 0, \pm\sqrt{AB - C^2}), \\ \text{Type IV}' & (A, B, C, 0, A+B-2C, \pm\sqrt{AB - C^2}). \end{array}$$

As in the proof of Lemma 5.3.4, we may assume $AB = C^2 + s^2$. Furthermore, we may assume $p = 0$ or $q = 0$ since $\mathbf{y}$ is a convex combination of $\mathbf{y}_\pm^{(0)} \in \mathcal{Q}$, where $\mathbf{y}_+^{(0)} = (A, B, C, p+q, 0, s)$ and $\mathbf{y}_-^{(0)} = (A, B, C, 0, p+q, s)$. Let us first assume $q = 0$ and divide the condition (3) of (5.4.21) into the following three cases.

[Case 1] $(A, B) \neq (0,0)$ and $A + B - 2C < p$. Then for sufficiently small $\delta > 0$,

$$\mathbf{y}_\pm^{(1)} = (A \pm A\delta, B \pm B\delta, C \pm C\delta, p \pm \delta', 0, s \pm s\delta) \in \mathcal{Q} \tag{5.4.22}$$

where $\delta' \in \mathbb{R}$ satisfies

$$\big((-d^2 + d + 1)A - (d-1)^2 B + 2d(d-1)C\big)\,\delta + (d^2-1)\delta' = 0, \tag{5.4.23}$$

so that the condition (4) of (5.4.21) holds for $\mathbf{y}_\pm^{(1)}$. Since $\mathbf{y} = (\mathbf{y}_+^{(1)} + \mathbf{y}_-^{(1)})/2$ and $\mathbf{y}_+^{(1)} \neq \mathbf{y}_-^{(1)}$, we have $\mathbf{y} \notin \mathrm{Ext}(\mathcal{Q})$.

[Case 2] $A = B = 0$ (hence $C = s = 0$). Then $\mathbf{y} = p(0,0,0,1,0,0)$ is extremal in $\mathcal{Q}$ (corresponding to Type I$'$) since $(A, B, C, s) = (0, 0, 0, 0)$ is an extreme point of $\mathcal{S}$ in Lemma 5.4.1 and since p is uniquely determined by (5.4.21) (4).

[Case 3] $A+B-2C = p$. In this case, we claim that $\mathbf{y} = (A, B, C, A+B-2C, 0, s) \in \text{Ext}(\mathcal{Q})$, which corresponds to Type III$'$. Indeed, if $\mathbf{y}$ is a convex combination of $\mathbf{y}^{(2)}_{\pm} = (A_\pm, B_\pm, C_\pm, p_\pm, q_\pm, s_\pm) \in \mathcal{Q}$, then the conditions $q = 0$ and $q_\pm \geq 0$ imply $q_\pm = 0$. Moreover, the conditions $A + B - 2C = p$ and $A_\pm + B_\pm - 2C_\pm \leq p_\pm$ imply $A_\pm + B_\pm - 2C_\pm = p_\pm$. Now applying Lemma 5.4.1, we can write

$$\mathbf{y}^{(2)}_{+} = (A(1+\delta), B(1+\delta), C(1+\delta), (A+B-2C)(1+\delta), 0, s(1+\delta)) \quad (5.4.24)$$

for some $\delta \in \mathbb{R}$. On the other hand, the TP condition (5.4.21) (4) for $\mathbf{y}^{(2)}_{+}$ gives

$$(dA + 2(d-1)B - 2(d-1)C)\,\delta = 0. \quad (5.4.25)$$

However,

$$dA + 2(d-1)B = A + (d-1)B + (d-1)(A+B) \geq 2(d-1)C \quad (5.4.26)$$

since $A + B \geq 2C$, and the equality above holds only if $A = B = C = p = s = 0$ which is impossible. Therefore, (5.4.25) holds only if $\delta = 0$, and hence we have $\mathbf{y} = \mathbf{y}^{(2)}_{+} = \mathbf{y}^{(2)}_{-}$.

Finally, we can proceed analogously when $p = 0$ and get the tuples of Type II$'$ and Type IV$'$ as extreme points of $\mathcal{Q}$. □

5.4.3 Proof of Theorem 5.3.6 when $d = 2$

When $d = 2$, we have an additional relation

$$V_e - V_{(12)} - V_{(13)} - V_{(23)} + V_{(123)} + V_{(132)} = 0. \quad (5.4.27)$$

Therefore, $\{V_\sigma\}_{\sigma\in\mathcal{S}_3}$ is no longer linearly independent, and both the spaces $\mathrm{Inv}(U^{\otimes 3}) = \mathrm{span}\,\{V_\sigma : \sigma \in \mathcal{S}_3\}$ and $\mathrm{Inv}(U\otimes\overline{U}\otimes U) = \mathrm{span}\,\{T_\sigma : \sigma\in\mathcal{S}_3\}$ are 5-dimensional. In particular, we have $\mathrm{Inv}(O_+^{\otimes 3}) = \mathrm{Inv}(U\otimes\overline{U}\otimes U)$ in this case.

We can write a general element in $\mathrm{Cov}(\overline{U},\overline{U}U)$ as $\mathcal{M} = \sum_{\sigma\in\mathcal{S}_3\setminus\{e\}} a_\sigma \mathcal{M}_\sigma$. Then $\mathcal{M}$ is positive if and only if

$$\begin{cases} a_{(12)}, a_{(13)}, a_{(23)} \geq 0 \ \text{ and } \ a_{(132)} = \overline{a_{(123)}}, \\ a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)} \geq 0, \\ (a_{(12)} + a_{(13)} + a_{(23)} + a_{(123)} + a_{(132)})a_{(23)} \geq |a_{(23)} + a_{(123)}|^2, \end{cases} \tag{5.4.28}$$

by following the same proof in Lemma 5.3.9. Now let us write $(r,s) = (\mathrm{Re}(a_{(123)}), \mathrm{Im}(a_{(123)}))$ for convenience and consider a linear isomorphism

$$\tilde{\beta} : (a_{(12)}, a_{(13)}, a_{(23)}, r, s) \mapsto (a_{(12)}, A, B, C, s), \tag{5.4.29}$$

of $\mathbb{R}^5$, where $A = a_{(12)} + a_{(13)} + a_{(23)} + 2r$, $B = a_{(23)}$, and $C = a_{(23)} + r$. Then the set $\widetilde{\mathcal{Q}} = \left\{\tilde{\beta}(a_{(12)}, a_{(13)}, a_{(23)}, r, s) : \mathcal{M} \in \mathrm{Cov}_1(\overline{U},\overline{U}U)^{\mathcal{POS}}\right\}$ is equal to the set of tuples $(a_{(12)}, A, B, C, s) \in \mathbb{R}^5$ satisfying

$$\begin{cases} (1) \quad A, B \geq 0, \\ (2) \quad AB \geq C^2 + s^2, \\ (3) \quad 0 \leq a_{(12)} \leq A + B - 2C, \\ (4) \quad A + B - C = \frac{1}{2}. \end{cases} \tag{5.4.30}$$

In order to find the extreme points $\mathbf{y} = (a_{(12)}, A, B, C, s)$ of $\widetilde{\mathcal{Q}}$, note that we still have $AB = C^2 + s^2$ as in the proof of Lemma 5.3.11. Moreover, we have $a_{(12)} = 0$ or $A + B - 2C$ since $\mathbf{y}$ is a convex combination of $\mathbf{y}_+ = (A + B - 2C, A, B, C, s)$ and $\mathbf{y}_- = (0, A, B, C, s)$. Therefore, we can list all possible extreme points of $\widetilde{\mathcal{Q}}$ in the following two types:

$$\begin{array}{ll} \text{Type I}' & (A + B - 2C, A, B, C, \pm\sqrt{AB - C^2}), \\ \text{Type II}' & (0, A, B, C, \pm\sqrt{AB - C^2}), \end{array}$$

for $A, B \geq 0$, $AB \geq C^2$, and $A + B - C = \frac{1}{2}$. Moreover, any extreme point of Type I$'$ corresponds to a tuple

$$(a_{(12)}, a_{(13)}, a_{(23)}, r, s) = (A + B - 2C, 0, B, C - B, \pm\sqrt{AB - C^2}), \quad (5.4.31)$$

so the associated linear map $\mathcal{M} = \sum_{\sigma \in \mathcal{S}_3 \setminus \{e\}} a_\sigma \mathcal{M}_\sigma$ is CP by Lemma 5.3.10 (note that Lemma 5.3.10 (1) still gives a sufficient condition for $\mathcal{M}$ to be CP when $d = 2$). Similarly, any extreme point of Type II$'$ corresponds a CCP map. In other words, every element in $\mathrm{Ext}(\mathrm{Cov}_1(\overline{U}, \overline{U}U)^{\mathcal{POS}})$ is CP or CCP, thus $\mathcal{POS} = \mathcal{DEC}$ holds in $\mathrm{Cov}_1(\overline{U}U, \overline{U})^{\mathcal{POS}}$. This completes the proof of Theorem 5.3.6 by Corollary 4.3.4.

5.4.4 Quantum orthogonal symmetry

Within the framework of *compact quantum groups*, the orthogonal group $\mathcal{O}(d)$ is understood as the space $C(\mathcal{O}(d))$ of continuous functions on $\mathcal{O}(d)$ endowed with the co-multiplication $\Delta : C(\mathcal{O}(d)) \to C(\mathcal{O}(d) \times \mathcal{O}(d))$ given by

$$(\Delta f)(x, y) = f(xy) \quad (5.4.32)$$

for all $x, y \in \mathcal{O}(d)$ and $f \in C(\mathcal{O}(d))$. Moreover, there exists a family of continuous functions $(\pi_{ij})_{1 \leq i,j \leq d}$ generating $C(\mathcal{O}(d))$ and

$$\Delta(\pi_{ij}) = \sum_{k=1}^{d} \pi_{ik} \otimes \pi_{kj} \in C(\mathcal{O}(d)) \otimes_{min} C(\mathcal{O}(d)) \cong C(\mathcal{O}(d) \times \mathcal{O}(d)) \quad (5.4.33)$$

for all $1 \leq i, j \leq d$, where $\otimes_{min}$ means the minimal tensor product between C^*-algebras.

The *free orthogonal quantum group* $\mathcal{O}_d^+$ is a liberation of $\mathcal{O}(d)$ in the sense that the space $C(\mathcal{O}_d^+)$ of 'non-commutative' continuous functions on $\mathcal{O}_d^+$ is the universal unital C^*-algebra generated by d^2 self-adjoint operators u_{ij} satisfying that $u = \sum_{i,j=1}^{d} e_{ij} \otimes u_{ij}$ is a unitary, i.e. $u^*u = uu^* = I_d \otimes 1$

in $M_d \otimes C(\mathcal{O}_d^+)$. The quantum group structure is encoded in the unital $*$-homomorphism $\Delta : C(\mathcal{O}_d^+) \to C(\mathcal{O}_d^+) \otimes_{min} C(\mathcal{O}_d^+)$ determined by

$$\Delta(u_{ij}) = \sum_{k=1}^{d} u_{ik} \otimes u_{kj}.$$

Then $u = \sum_{i,j=1}^{d} e_{ij} \otimes u_{ij}$ is the standard unitary representation of $\mathcal{O}_d^+$ satisfying $u^c = \sum_{i,j=1}^{d} e_{ij} \otimes u_{ij}^* = u$ in the sense of [Wor87, Ban96]. The 3-fold tensor representation $u \boxtimes u \boxtimes u \in M_d^{\otimes 3} \otimes C(\mathcal{O}_d^+)$ of u is defined by

$$u \boxtimes u \boxtimes u = \sum_{i_1,j_1,i_2,j_2,i_3,j_3=1}^{d} e_{i_1j_1} \otimes e_{i_2j_2} \otimes e_{i_3j_3} \otimes u_{i_1j_1} u_{i_2j_2} u_{i_3j_3}. \tag{5.4.34}$$

Then the space $\mathrm{Inv}(O_+^{\otimes 3})$ in Section 5.3.2 is understood as the space $\mathrm{Inv}(u \boxtimes u \boxtimes u)$ of operators $X \in M_d^{\otimes 3}$ satisfying

$$(u \boxtimes u \boxtimes u) \cdot (X \otimes 1) = (X \otimes 1) \cdot (u \boxtimes u \boxtimes u) \tag{5.4.35}$$

in view of [LY22]. To sketch a proof of this fact, we can observe that the 5 operators T_σ ($\sigma \in \mathcal{S}_3 \setminus \{(13)\}$) in (5.3.20) are linearly independent, and the operators T_σ satisfy (5.4.35) using the identity

$$(u \boxtimes u)(|\Omega_d\rangle \otimes 1) = |\Omega_d\rangle \otimes 1. \tag{5.4.36}$$

Thus, $\mathrm{Inv}(O_+^{\otimes 3}) \subseteq \mathrm{Inv}(u \boxtimes u \boxtimes u)$. Moreover, the space $\mathrm{Inv}(u \boxtimes u \boxtimes u)$ should be of dimension five thanks to the representation theory of $\mathcal{O}_d^+$ (see Corollary 6.4.12 and Corollary 5.3.5 of [Tim08]). Hence, we have $\mathrm{Inv}(O_+^{\otimes 3}) = \mathrm{Inv}(u \boxtimes u \boxtimes u)$.

Bibliography

[ACP20] Victor V. Albert, Jacob P. Covey, and John Preskill. Robust encoding of a qubit in a molecule. *Phys. Rev. X*, 10:031050, Sep 2020.

[AGI07] Gerardo Adesso, Salvatore M. Giampaolo, and Fabrizio Illuminati. Geometric characterization of separability and entanglement in pure gaussian states by single-mode unitary operations. *Phys. Rev. A*, 76:042334, Oct 2007.

[Arm81] David L. Armacost. *The structure of locally compact abelian groups*, volume 68 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1981.

[AZ07] A. V. Akopyan and A. A. Zaslavsky. *Geometry of Conics (Mathematical World)*. American Mathematical Society, 12 2007.

[Ban96] Teodor Banica. Théorie des représentations du groupe quantique compact libre O(n). *C. R. Acad. Sci. Paris Sér. I Math.*, 322(3):241–244, 1996.

[BCL+22] Cedric Beny, Jason Crann, Hun Hee Lee, Sang-Jun Park, and Sang-Gyun Youn. Gaussian quantum information over general quantum kinematical systems i: Gaussian states. Preprint, arXiv:2204.08162, 2022.

[BCS20] Ivan Bardet, Benoît Collins, and Gunjan Sapra. Characterization of equivariant maps and application to entanglement detection. *Ann. Henri Poincaré*, 21(10):3385–3406, 2020.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.*, 1(3):195–200, 1964.

[Ber41] S. N. Bernstein. On a property which characterizes a gaussian distribution. *Proceedings of the Leningrad Polytechnic Institute.*, 217(03):21—22, 1941.

[BHLL18] Arpan Bhattacharyya, Ling-Yan Hung, Yang Lei, and Wei Li. Tensor network and (p-adic) AdS/CFT. *J. High Energy Phys.*, (1):139, front matter + 53, 2018.

[BK86] BRIESKORN and KNÖRRER. *Plane Algebraic Curves.* Birkhäuser, 1986.

[BKW18] Paul Busch, Jukka Kiukas, and R. F. Werner. Sharp uncertainty relations for number and angle. *J. Math. Phys.*, 59(4):042102, 16, 2018.

[BO08] Nathanial P. Brown and Narutaka Ozawa. *C^*-algebras and finite-dimensional approximations*, volume 88 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2008.

[Car20] Daniel Cariello. Inequalities for the Schmidt number of bipartite states. *Lett. Math. Phys.*, 110(4):827–833, 2020.

[CG96] H. S. M. Coxeter and Samuel L. Greitzer. *Geometry Revisited (New Mathematical Library).* American Mathematical Society, 9 1996.

[Cho75a] Man Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10:285–290, 1975.

[Cho75b] Man Duen Choi. Positive semidefinite biquadratic forms. *Linear Algebra Appl.*, 12(2):95–100, 1975.

[Cho82] M.D. Choi. Positive linear-maps. In *in Operator Algebras and Applications (Kingston, 1980), Proc.Sympos.Pure.Math.*, volume 38, pages 583–590. Amer.Math.Soc., 1982.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[CL93] Eric A. Carlen and Elliott H. Lieb. Optimal hypercontractivity for Fermi fields and related noncommutative integration inequalities. *Comm. Math. Phys.*, 155(1):27–46, 1993.

[CMHW19] Matthias Christandl, Alexander Müller-Hermes, and Michael M. Wolf. When do composed maps become entanglement breaking? *Ann. Henri Poincaré*, 20(7):2295–2322, 2019.

[COS18] Benoît Collins, Hiroyuki Osaka, and Gunjan Sapra. On a family of linear maps from $M_n(\mathbb{C})$ to $M_{n^2}(\mathbb{C})$. *Linear Algebra Appl.*, 555:398–411, 2018.

[Cox03] H.S.M. Coxeter. *Projective Geometry*. Springer, 10 2003.

[CRSS98] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[CYT17] Lin Chen, Yu Yang, and Wai-Shing Tang. Schmidt number of bipartite and multipartite states under local projections. *Quantum Inf. Process.*, 16(3):Paper No. 75, 27, 2017.

[CYT19] Lin Chen, Yu Yang, and Wai-Shing Tang. Positive-partial-transpose square conjecture for $n = 3$. *Phys. Rev. A*, 99:012337, Jan 2019.

[DE14] Anton Deitmar and Siegfried Echterhoff. *Principles of harmonic analysis*. Universitext. Springer, Cham, second edition, 2014.

[DEBZ10] THOMAS DURT, BERTHOLD-GEORG ENGLERT, INGEMAR BENGTSSON, and KAROL ŻYCZKOWSKI. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[DHV99] T. Digernes, E. Husstad, and V. S. Varadarajan. Finite approximation of Weyl systems. *Math. Scand.*, 84(2):261–283, 1999.

[DV04] Trond Digernes and V. S. Varadarajan. Models for the irreducible representation of a Heisenberg group. *Infin. Dimens. Anal. Quantum Probab. Relat. Top.*, 7(4):527–546, 2004.

[DVV94] Trond Digernes, V. S. Varadarajan, and S. R. S. Varadhan. Finite approximations to quantum systems. *Rev. Math. Phys.*, 6(4):621–648, 1994.

[EK00] Myoung-Hoe Eom and Seung-Hyeok Kye. Duality for positive linear maps in matrix algebras. *Math. Scand.*, 86(1):130–142, 2000.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[EW01] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $U \bigotimes U \bigotimes U$ symmetry. *Phys. Rev. A*, 63:042111, Mar 2001.

[Fel08] Gennadiy Feldman. *Functional equations and characterization problems on locally compact abelian groups*, volume 5 of *EMS Tracts in Mathematics*. European Mathematical Society (EMS), Zürich, 2008.

[Fol16] Gerald B. Folland. *A course in abstract harmonic analysis*. Textbooks in Mathematics. CRC Press, Boca Raton, FL, second edition, 2016.

[GÏ1] Otfried Gühne. Entanglement criteria and full separability of multi-qubit quantum states. *Phys. Lett. A*, 375(3):406–410, 2011.

[GBW21] Martina Gschwendtner, Andreas Bluhm, and Andreas Winter. Programmability of covariant quantum channels. *Quant.*, 5(6):488, 2021.

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Inf. Comput.*, 10(3-4):343–360, 2010.

[GHW04] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A (3)*, 70(6, part B):062101, 23, 2004.

[Gir14] S. M. Girvin. *Quantum Machines: Measurement and Control of Engineered Quantum Systems: Lecture Notes of the Les Houches Summer School: Volume 96, July 2011*. Oxford University Press, 06 2014. Chap. 3.

[GKP+17] Steven S. Gubser, Johannes Knaute, Sarthak Parikh, Andreas Samberg, and Przemek Witaszczyk. p-adic AdS/CFT. *Comm. Math. Phys.*, 352(3):1019–1059, 2017.

[GKS21] Mark Girard, Seung-Hyeok Kye, and Erling Størmer. Convex cones in mapping spaces between matrix algebras. *Linear Algebra and its Applications*, 608:248–269, 2021.

[Got97] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, 1997. Ph. D. Thesis, e-print quant-ph/9705052.

[Gro46] H. J. Groenewold. On the principles of elementary quantum mechanics. *Physica*, 12:405–460, 1946.

[Gro06] D. Gross. Hudson's theorem for finite-dimensional quantum systems. *J. Math. Phys.*, 47(12):122107, 25, 2006.

[GT09] Otfried Gühne and Géza Tóth. Entanglement detection. *Physics Reports*, 474(1):1–75, 2009.

[Gur03] Leonid Gurvits. Classical deterministic complexity of Edmond's problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 10–19. ACM, New York, 2003.

[Has18] Anna-Lena K. Hashagen. *Symmetry Methods in Quantum Information Theory*. PhD thesis, Technische Universität München Lehrstuhl für mathematische Physik, 2018. Thesis (Ph.D.).

[HDDM05] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. *Phys. Rev. A (3)*, 71(4):042315, 9, 2005.

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206–4216, Jun 1999.

[HHH96] MichałHorodecki, PawełHorodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1-2):1–8, 1996.

[HHH99] Paweł Horodecki, Michał Horodecki, and Ryszard Horodecki. Bound entanglement can be activated. *Phys. Rev. Lett.*, 82:1056–1059, Feb 1999.

[HHHH09] Ryszard Horodecki, PawełHorodecki, MichałHorodecki, and Karol Horodecki. Quantum entanglement. *Rev. Modern Phys.*, 81(2):865–942, 2009.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, Apr 2005.

[HHHO09] Karol Horodecki, MichałHorodecki, PawełHorodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inform. Theory*, 55(4):1898–1929, 2009.

[HLLMH18] Marcus Huber, Ludovico Lami, Cécilia Lancien, and Alexander Müller-Hermes. High-dimensional entanglement in states with positive partial transposition. *Phys. Rev. Lett.*, 121:200503, Nov 2018.

[HMSS18] Matthew Heydeman, Matilde Marcolli, Ingmar A. Saberi, and Bogdan Stoica. Tensor networks, p-adic fields, and algebraic curves: arithmetic and the $\mathrm{AdS}_3/\mathrm{CFT}_2$ correspondence. *Adv. Theor. Math. Phys.*, 22(1):93–176, 2018.

[Hol19] Alexander S. Holevo. *Quantum systems, channels, information—a mathematical introduction.* Texts and Monographs in Theoretical Physics. De Gruyter, Berlin, [2019] ©2019. Second edition [of 2986302].

[Hor97] PawełHorodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232(5):333–339, 1997.

[HPHH08] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki. Low-dimensional bound entanglement with one-way distillable cryptographic key. *IEEE Trans. Inform. Theory*, 54(6):2621–2625, 2008.

[HR70] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis. Vol. II: Structure and analysis for compact groups. Analysis on locally compact Abelian groups.* Die Grundlehren der mathematischen Wissenschaften, Band 152. Springer-Verlag, New York-Berlin, 1970.

[HR72] Herbert Heyer and Christian Rall. Gausssche Wahrscheinlichkeitsmasse auf Corwinschen Gruppen. *Math. Z.*, 128:343–361, 1972.

[HR79] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis. Vol. I*, volume 115 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, second edition, 1979. Structure of topological groups, integration theory, group representations.

[HSR03] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Rev. Math. Phys.*, 15(6):629–641, 2003.

[Hud74] R. L. Hudson. When is the Wigner quasi-probability density non-negative? *Rep. Mathematical Phys.*, 6(2):249–252, 1974.

[Jk72] A. Jamioł kowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Mathematical Phys.*, 3(4):275–278, 1972.

[Kal70] Robert R. Kallman. Certain topological groups are type I. *Bull. Amer. Math. Soc.*, 76:404–406, 1970.

[Kay11] Alastair Kay. Optimal detection of entanglement in greenberger-horne-zeilinger states. *Phys. Rev. A*, 83:020303, Feb 2011.

[KL72] Adam Kleppner and Ronald L. Lipsman. The Plancherel formula for group extensions. I, II. *Ann. Sci. École Norm. Sup. (4)*, 5:459–516; ibid. (4) 6 (1973), 103–132, 1972.

[KMS20] Piotr Kopszak, Marek Mozrzymas, and MichałStudziński. Positive maps from irreducibly covariant operators. *J. Phys. A*, 53(39):395306, 33, 2020.

[Kye23a] Seung-Hyeok Kye. Compositions and tensor products of linear maps between matrix algebras. *Linear Algebra Appl.*, 658:283–309, 2023.

[Kye23b] Seung-Hyuk Kye. Positive maps in quantum information theory. Lecture note (ver. 2023 March) available at `http://www.math.snu.ac.kr/~kye/lecture/22_2_topic/QIT_230309.pdf`, 2023.

[LY22] Hun Hee Lee and Sang-Gyun Youn. Quantum channels with quantum group symmetry. *Comm. Math. Phys.*, 389(3):1303–1329, 2022.

[Mac58] George W. Mackey. Unitary representations of group extensions. I. *Acta Math.*, 99:265–311, 1958.

[Mas06] Lluís Masanes. All bipartite entangled states are useful for information processing. *Phys. Rev. Lett.*, 96:150501, Apr 2006.

[Moy49] J. E. Moyal. Quantum mechanics as a statistical theory. *Proc. Cambridge Philos. Soc.*, 45:99–124, 1949.

[MRS15] Marek Mozrzymas, Adam Rutkowski, and MichałStudziński. Using non-positive maps to characterize entanglement witnesses. *J. Phys. A*, 48(39):395302, 11, 2015.

[Muk79] N. Mukunda. Wigner distribution for angle coordinates in quantum mechanics. *American Journal of Physics*, 47(2):182–187, 02 1979.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[OP04] Murad Özaydin and Tomasz Przebinda. An entropy-based uncertainty principle for a locally compact abelian group. *J. Funct. Anal.*, 215(1):241–252, 2004.

[Par04] K. R. Parthasarathy. On estimating the state of a finite level quantum system. *Infin. Dimens. Anal. Quantum Probab. Relat. Top.*, 7(4):607–617, 2004.

[Per96] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, 1996.

[PJLY23] Sang-Jun Park, Crann Jason, Hun Hee Lee, and Sang-Gyun Youn. Gaussian quantum information over general quantum kinematical systems ii: Gaussian channels. in preparation, 2023.

[PJPY23] Sang-Jun Park, Yeong-Gwang Jung, Jeongeun Park, and Sang-Gyun Youn. A universal framework for entanglement detection under group symmetry. Preprint, arXiv:2301.03849, 2023.

[Pow40] A. Powzner. Über positive Funktionen auf einer Abelschen Gruppe. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 28:294–295, 1940.

[Pra11] Amritanshu Prasad. An easy proof of the Stone-von Neumann-Mackey theorem. *Expo. Math.*, 29(1):110–118, 2011.

[PRRV63] K. R. Parthasarathy, R. Ranga Rao, and S. R. S. Varadhan. Probability distributions on locally compact abelian groups. *Illinois J. Math.*, 7:337–369, 1963.

[PSV10] Amritanshu Prasad, Ilya Shapiro, and M. K. Vemuri. Locally compact abelian groups with symplectic self-duality. *Adv. Math.*, 225(5):2429–2454, 2010.

[PV07] M. Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Information and Computation*, 7, 04 2007.

[PY23] Sang-Jun Park and Sang-Gyun Youn. k-positivity and schmidt number under orthogonal group symmetries. Preprint, arXiv:2306.00654, 2023.

[Rai40] D. Raikov. Positive definite functions on commutative groups with an invariant measure. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 28:296–300, 1940.

[RKSE10] Philippe Raynal, Amir Kalev, Jun Suzuki, and Berthold-Georg Englert. Encoding many qubits in a rotor. *Phys. Rev. A*, 81:052327, May 2010.

[Roc70] R. Tyrrell Rockafellar. *Convex analysis*. Princeton Mathematical Series, No. 28. Princeton University Press, Princeton, N.J., 1970.

[RS68] Lewis Robertson and Bert M. Schreiber. The additive structure of integer groups and p-adic number fields. *Proc. Amer. Math. Soc.*, 19:1453–1456, 1968.

[RS00] Hans Reiter and Jan D. Stegeman. *Classical harmonic analysis and locally compact groups*, volume 22 of *London Mathematical Society Monographs. New Series.* The Clarendon Press, Oxford University Press, New York, second edition, 2000.

[RSSK+10] I. Rigas, L. L. Sánchez-Soto, A. B. Klimov, J. Řeháček, and Z. Hradil. Non-negative Wigner functions for orbital angular momentum states. *Phys. Rev. A (3)*, 81(1):012101, 4, 2010.

[Ruk69] A. L. Rukhin. On a theorem of s. n. bernshtein. *Mathematical notes of the Academy of Sciences of the USSR*, 6(3):638–641, Sep 1969.

[SC83] Francisco Soto and Pierre Claverie. When is the Wigner function of multidimensional systems nonnegative? *J. Math. Phys.*, 24(1):97–100, 1983.

[Sch60] Julian Schwinger. Unitary operator bases. *Proceedings of the National Academy of Sciences of the United States of America*, 46(4):570–579, 1960.

[SDN22] Satvik Singh, Nilanjana Datta, and Ion Nechita. Ergodic theory of diagonal orthogonal covariant quantum channels, 2022.

[Ser17] Alessio Serafini. *Quantum continuous variables.* CRC Press, Boca Raton, FL, 2017. A primer of theoretical methods.

[Sko11] Ł ukasz Skowronek. Cones with a mapping cone symmetry in the finite-dimensional case. *Linear Algebra Appl.*, 435(2):361–370, 2011.

[SN21] Satvik Singh and Ion Nechita. Diagonal unitary and orthogonal symmetries in quantum theory. *Quantum*, 5:519, August 2021.

[SN22] Satvik Singh and Ion Nechita. The PPT^2 Conjecture Holds for All Choi-Type Maps. *Annales Henri Poincare*, 23(9):3311–3329, 2022.

[Sr82] Erling Stø rmer. Decomposable positive maps on C^*-algebras. *Proc. Amer. Math. Soc.*, 86(3):402–404, 1982.

[Sr86] Erling Stø rmer. Extension of positive maps into $B(\mathcal{H})$. *J. Funct. Anal.*, 66(2):235–254, 1986.

[Sr12] Erling Stø rmer. Tensor products of positive maps of matrix algebras. *Math. Scand.*, 111(1):5–11, 2012.

[SSrZ09] Ł ukasz Skowronek, Erling Stø rmer, and Karol Życzkowski. Cones of positive maps and their duality relations. *J. Math. Phys.*, 50(6):062106, 18, 2009.

[Tak02] M. Takesaki. *Theory of operator algebras. I*, volume 124 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2002. Reprint of the first (1979) edition, Operator Algebras and Non-commutative Geometry, 5.

[TH00] Barbara M. Terhal and Paweł Horodecki. Schmidt number for density matrices. *Phys. Rev. A (3)*, 61(4):040301, 4, 2000.

[Tim08] Thomas Timmermann. *An Invitation to Quantum Groups and Duality*. European Mathematical Society, 2008.

[Tom85] Jun Tomiyama. On the geometry of positive maps in matrix algebras. II. *Linear Algebra Appl.*, 69:169–177, 1985.

[TT83] Toshiyuki Takasaki and Jun Tomiyama. On the geometry of positive maps in matrix algebras. *Math. Z.*, 184(1):101–108, 1983.

[VD36] D. Van Dantzig. Zur topologischen Algebra. III. Brouwersche und Cantorsche Gruppen. *Compositio Math.*, 3:408–426, 1936.

[VV89a] V. S. Vladimirov and I. V. Volovich. p-adic quantum mechanics. *Comm. Math. Phys.*, 123(4):659–676, 1989.

[VV89b] V. S. Vladimirov and I. V. Volovich. A vacuum state in p-adic quantum mechanics. *Phys. Lett. B*, 217(4):411–415, 1989.

[VW01] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, Nov 2001.

[VW02] Karl Gerd H. Vollbrecht and Michael M. Wolf. Activating distillation with an infinitesimal amount of bound entanglement. *Phys. Rev. Lett.*, 88:247901, May 2002.

[Wan95] Shuzhou Wang. Free products of compact quantum groups. *Comm. Math. Phys.*, 167(3):671–692, 1995.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[Wei40] André Weil. *L'intégration dans les groupes topologiques et ses applications*. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 869. Hermann & Cie, Paris, 1940. [This book has been republished by the author at Princeton, N. J., 1941.].

[Wei64] André Weil. Sur certains groupes d'opérateurs unitaires. *Acta Math.*, 111:143–211, 1964.

[Wer89] Reinhard F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989.

[Wer16] Reinhard F. Werner. Uncertainty relations for general phase spaces. *Frontiers of Physics*, 11(3):110305, Apr 2016.

[Wey50] Hermann Weyl. *The theory of groups and quantum mechanics.* Dover Publications, Inc., New York, 1950. Translated from the second (revised) German edition by H. P. Robertson, Reprint of the 1931 English translation.

[Wig32] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, Jun 1932.

[Wor76a] S. L. Woronowicz. Nonextendible positive maps. *Comm. Math. Phys.*, 51(3):243–282, 1976.

[Wor76b] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, 10(2):165–183, 1976.

[Wor87] S. L. Woronowicz. Compact matrix pseudogroups. *Comm. Math. Phys.*, 111(4):613–665, 1987.

[WPGP$^+$12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[Zel14] E. I. Zelenov. p-adic model of quantum mechanics and quantum channels. *Proc. Steklov Inst. Math.*, 285(1):132–144, 2014. Translation of Tr. Mat. Inst. Steklova **2**85 (2014), 140–153.

[Zel20] E. I. Zelenov. Entropy gain in p-adic quantum channels. *Physics of Particles and Nuclei*, 51(4):485–488, Jul 2020.

국문초록

본 학위논문에서는 추상조화해석학에서의 방법론을 적용하여 양자정보이론의 흥미로운 영역들을 들여다 보고자 한다. 본 논문의 구성은 저자의 학위과정 중 연구결과 [BCL+22, PJPY23, PY23]에 기반하여, 독립적인 주제를 담고 있는 두 개의 파트로 나누어 볼 수 있다.

첫 번째 파트에서는 가우시안상태와 안정자상태 (stabilizer state)가 흥미로운 수학적 유사성을 가짐에 착안하여, 일반화 된 가우시안상태의 정의를 제안하는것이 주된 목표이다. 이를 위해, 적당한 사교구조를 가진 국소컴팩트가환군 (LCA (locally compact abelian) 군)을 물리적 위상공간 (phase space)으로 사용하는 추상위상공간을 생각한다. 이러한 프레임워크 내에서 우리는 일반화 된 Weyl 유니터리 작용소 및 양자특성함수를 자연스럽게 정의할 수 있다. 그러고나면 LCA 군 위에서 정의된 여러가지 가우시안 분포의 모델 중 'Bernstein 방식'을 적용하여 추상적인 가우시안상태를 정의해 볼 수 있다. 놀랍게도 이러한 추상적 가우시안상태는 보존가우시안상태 및 안정자상태 뿐 아니라 양자이론에 등장하는 여러가지 중요한 개념들을 어우르는 보편적인 방식을 제공해 준다. 그 뿐 아니라, 위상공간이 완전분리 (totally disconnected) LCA 군으로부터 비롯된 경우, 순수가우시안상태는 각각의 Wigner 준확률분포 (quasi-distribution)가 확률분포를 이룬다는 성질로부터 완전히 특정지을 수 있게 된다. 이는 보존시스템에서의 Hudson 정리를 다른 종류의 위상공간에서 얻은 것으로 볼수 있어 '가우시안상태'라는 명칭에 또 하나의 정당성을 부여해 준다. 또한 위 결과는 Gross의 결과를 일반화 한 것이기도 하다.

두 번째 파트에서는 컴팩트군 표현에 대한 대칭성 하에서의 양자얽힘이론을 다룬다. 양자얽힘은 양자정보프로세에서의 핵심적인 자원 역할을 하고, 최근 몇 년간 양자얽힘의 수학적 구조를 파악하기 위해 수많은 노력이 이루어져 왔다. 일반적으로 Størmer가 도입한 사상콘 (mapping cone) 사이의 쌍대성으로부터 양자얽힘과 관련된 많은 개념들을 설명할수 있음에도, 양자얽힘 자체에 대한 계산복잡도적인 어려움으로 인해 이를 효과적으로 다루는 것은 쌍대성만으로는 충분하지 않다. 본 학위논문에서는 이러한 쌍대성이 일반적인 상황 뿐 아니라 컴팩트군 대칭성을 부여하였을때에도 잘 적용된다는 사실을 살펴본다. 이 관찰로부터 다음의 두 가지 중요한 결과를 얻을 수

있다: 컴팩트군 대칭 하에서의 (1) 얽힘 관측기 (entanglement witness) 및 슈미트수 관측기 (Schmidt number witness) 사용의 최적화, (2) 'PPT=얽힘' 문제와 '양사상=분해가능사상' 문제의 동치성. 위 결과를 적용하여 양자얽힘과 관련된 여러가지 구체적인 사례분석과 더불어 다양한 난제를 해결해 줄 수 있었는데, 이러한 점에서 우리의 결과가 단순 이론에 그치지 않고 강력한 응용가치가 있음을 알아보도록 한다.

주요어휘: 추상조화해석학, 군 표현, 양자정보이론, 가우시안상태, 양자얽힘, 슈미트수
학번: 2016-20234

감사의 글