



HAL
open science

Quelques problèmes en analyse non-commutative

Haonan Zhang

► **To cite this version:**

Haonan Zhang. Quelques problèmes en analyse non-commutative. Functional Analysis [math.FA]. Université Bourgogne Franche-Comté; Polska Akademia Nauk, 2019. English. NNT: 2019UBFCD043 . tel-02549747

HAL Id: tel-02549747

<https://theses.hal.science/tel-02549747>

Submitted on 21 Apr 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



THESE DE DOCTORAT DE L'ETABLISSEMENT UNIVERSITE
BOURGOGNE FRANCHE-COMTE
en co-tutelle avec
l'Institut Mathématique de l'Académie polonaise des sciences

École Doctorale Carnot-Pasteur

spécialité **Mathématiques**

présenté par

Haonan ZHANG

Some problems in noncommutative analysis

Soutenue à Besançon le 4 octobre 2019 devant le jury composé de

Examineur	Prof. Kenny DE COMMER	Vrije Universiteit Brussel
Rapporteur	Prof. Pierre FIMA	Université Paris Diderot
Examineur	Prof. Uwe FRANZ	Université Bourgogne Franche-Comté
Rapporteur	Prof. Bartosz KWAŚNIEWSKI	University of Białystok
Co-directeur	Prof. Adam SKALSKI	Polish Academy of Sciences
Président	Prof. Roland SPEICHER	Universität des Saarlandes
Directeur	Prof. Quanhua XU	Université Bourgogne Franche-Comté

OCTOBER 2019

Laboratoire de Mathématiques de Besançon
16 route de Gray
25030 Besançon, France

École doctorale Carnot-Pasteur

Institute of Mathematics, Polish Academy of Sciences
ul. Śniadeckich 8
00-656 Warszawa, Poland

DECLARATION

I declare that this thesis is the result of my own work.

May 21, 2019
Haonan ZHANG

Haonan ZHANG

We declare that the thesis is ready to be presented to the referees.

May 21, 2019
Quanhua XU

Quanhua XU

May 21, 2019
Adam SKALSKI

Adam Skalski

Acknowledgements

This thesis cannot be finished without the help and support of many people.

First of all, I would like express my deepest gratitude to my supervisor, Professor Quanhua XU, who led me to the area of noncommutative analysis, brought me the opportunity to study in IMPAN, and gave me many helpful guidance regarding my career. He is a great mathematician who has made a lot of significant contributions in many areas, which allows me to ask him any kind of questions. He is also a experienced educator who makes me a better mathematician. I benefit a lot from his wide range of knowledge and I am deeply influenced by his taste of mathematics. I am also very grateful to be invited to have dinner with his family for several times. Many compliments go to the superb cooking of his wife Ms. Haiyan DU.

The same gratitude also goes to my another supervisor, Professor Adam SKALSKI. The first day I met him, I was impressed by his agile thinking, talkative and wide range of knowledge. He is always very patient to me, no matter how stupid questions I ask, how silly mistakes I make, and how slow I react. I benefit from every meeting with him. His passion for mathematics encourages me to dabble in as much areas as I can. Many thanks should go to his families Joanna and Marysia, too. Visiting the Roof Garden of the Warsaw University Library, walking along the Vistula River, and having meals together... I really cherish every second with them in Warsaw. Moreover, thank Adam again for his help with the Polish abstract of this thesis.

It is my honour to have Professor Pierre FIMA and Professor Bartosz KWAŚNIEWSKI to be my referees, and Professor Kenny DE COMMER, Professor Uwe FRANZ and Professor Roland SPEICHER to be jury members. I would like to thank them for their careful reading and many helpful comments.

This thesis was carried out within the Functional Analysis team in LMB as well as the Noncommutative Geometry Laboratory in IMPAN. Firstly, I would like to thank all the members of the two teams. In particular, I express my gratitude to professors (always in alphabetical order) Jean-Christophe BOURIN, Uwe FRANZ, Yulia KUZNETSOVA, Piotr M. HAJAC, Florence LANCIEN, Gilles LANCIEN, Christian LE MERDY, Stefan NEUWIRTH, Alexandre NOU, Tatiana SHULMAN, Adam SKALSKI, Stanisław Lech WORONOWICZ and Quanhua XU for their successful seminars and working groups, from which I benefit a lot. Secondly, special thanks to several professors in University of Warsaw, Professor Piotr NAYAR, Professor Jan OKNIŃSKI, Professor Adam OSEKOWSKI and Professor Piotr M. SOŁTAN, for their excellent lecture courses and using English for the only one among the audiences who does not speak Polish. Lastly, I want to thank Jean-Pierre CHASSARD, Richard FERRERE, Charlène GOURAND, Odile HENRY, Jakub PAULUS, Anna POCZMAŃSKA, Renata PODGÓRSKA-ZAJĄC, Claudia RAKOTSON, Katarzyna SOŁTYK-SOŁTYCKA for their warm and constant help with administrative or technical issues.

Part of this thesis was also finished during several annual summer workshops in Harbin. I would like to thank the organiser Professor Quanhua XU for organizing the workshop and his warm hospitality. I also want to express my gratitude to all the participants for their excellent talks and to the local secretaries Yang ZHOU and Yiqiu ZHU for their kind help.

Many thanks go to several institutes that I have visited and the hosts there. I want to thank Professor Jan MAAS for inviting me to IST Austria, which plays an important role in my application of ISTplus postdoc fellowship. I would like to thank Professor Jan MAAS again for agreeing to be my supervisor and thank Professor László ERDŐS for agreeing to be my co-supervisor in next few years. I also want to thank Professor Hun Hee LEE and Xiao XIONG for the visit to Seoul, Professor Éric RICARD and Professor Roland VERGNIOUX for the visit to Caen, Professor Kenny DE COMMER for the visit to Brussels, Professor Rui LIU for the visit to Tianjin and Professor Shunlong LUO for the visit to Beijing.

Let me take this opportunity to thank Professor Eric CARLEN who helped me a lot during my applications of postdoc positions. The same gratitude also goes to professors Benoît COLLINS, Pierre FIMA, Amury FRESLON, Yasuyuki KAWAHIGASHI, Yoshiko OGATA and Jean ROYDOR for their kind help and suggestions.

Many thanks to several mathematicians, Léonard CADILHAC, Kenny DE COMMER, Uwe FRANZ, Guixiang HONG, Paweł KASPRZAK, Ke LI, Éric RICARD, Piotr M. SOŁTAN, Simeng WANG, Jinsong WU, Zhi YIN and Sang-Gyun YOUN. I gained a lot from discussions with them.

I would like to thank many young colleagues, Alessandro, Benjamin, Bingbing, Clément, Colin, Ignacio, Isabelle, Jacek, Julien, Kai, Kang, Lei, Lucie, Marine, Mateusz, Olga, Paweł, Runlian, Thi Nhu Thao, Xumin, Yixiao, Yongle, Youssef, Zhengxing, and some Chinese students, Chen, Cheng, Hao, Meiling, Mengjia, Pengbai, Tianxiang, Tingting, Wanying, Yinjuan... It is a wonderful experience to spend the last three years with you together. I am grateful to Isabelle for her kind help with language corrections on the French abstract of this thesis.

Special thanks go to my good friends Zehao GUAN, Enhui HUANG, Bingjie LI and Chunyue ZHENG. Thank you for your encouragement and listening along the way. I am very happy to have friends like you in the past years. Wish your theses go well, too.

Last but not least, I indebted a lot to my families. I am very grateful for their unconditional support and encouragement. For my girlfriend Chunzi, words are powerless to express my gratitude. Thank you for everything you have done for me, especially during the hard time.

Merci à tous! Dziękuję bardzo!

Abstract

This PhD thesis is devoted to the study of some problems in noncommutative analysis. It consists of four parts, ranging from quantum groups and noncommutative harmonic analysis to quantum information. Firstly, we decide all the idempotent states on Sekine quantum groups, which is achieved by solving a system of equations using linear algebras and elementary number theory. This answers a question of Franz and Skalski stated in 2009. Secondly, we study the infinitely divisible states on finite quantum groups, i.e., states that admit n -th root for all $n \geq 1$. We show that every infinitely divisible state on a finite quantum group is of Poisson type, that is, it can be represented as an exponential relative to some idempotent state. Thirdly, we give two sufficient conditions for boundedness of L_p -Fourier multipliers on discrete group von Neumann algebras. Very few of such results were known before. Our idea is the observation that in the discrete case it suffices to consider L_p - L_q Fourier multipliers. Finally, in the area of quantum information, we confirm a conjecture of Carlen, Frank and Lieb (and then a weaker conjecture of Audenaert and Datta). As a consequence, we identify all the pairs (α, z) such that the α - z Rényi relative entropy is monotone under completely positive trace preserving maps, or satisfies the Data Processing Inequality. The key part of the proof is a modification of a widely-used variational method. Its power yields simple proofs of many known results.

Keywords

Compact quantum groups, finite quantum groups, idempotent states, infinitely divisible states, Poisson states, noncommutative L_p -spaces, noncommutative Lorentz spaces, group von Neumann algebra, Fourier multipliers, α - z Rényi relative entropy, data processing inequality, joint convexity/concavity.

Résumé

Cette thèse de doctorat est consacrée à l'étude de quelques problèmes d'analyse non commutative. Elle comprend quatre parties, allant des groupes quantiques et de l'analyse harmonique non commutative à l'information quantique. Tout d'abord, nous déterminons tous les états idempotents sur les groupes quantiques de Sekine, ce qui est obtenu en résolvant un système d'équations à l'aide de l'algèbre linéaire et de la théorie des nombres élémentaire. Ceci répond à une question de Franz et Skalski énoncée en 2009. Deuxièmement, nous étudions les états infiniment divisibles sur des groupes quantiques finis, c'est-à-dire les états qui admettent une racine n -ième pour tout $n \geq 1$. Nous montrons que tout état infiniment divisible sur un groupe quantique fini est de type Poisson, c'est-à-dire qu'il peut être représenté sous la forme d'une exponentielle par rapport à un état idempotent. Troisièmement, nous donnons deux conditions suffisantes pour que les multiplicateurs de Fourier de L_p sur les algèbres de von Neumann de groupes discrets soient bornés. Très peu de ces résultats étaient connus auparavant. Notre idée est l'observation que, dans le cas discret, il suffit de considérer les multiplicateurs de Fourier de L_p - L_q . Enfin, dans le domaine de l'information quantique, nous confirmons une conjecture de Carlen, Frank et Lieb (puis une conjecture plus faible d'Audenaert et Datta). En conséquence, nous identifions toutes les paires (α, z) telles que l' α - z entropie relative de Rényi soit monotone sous l'action des applications complètement positives préservant la trace, ou satisfait l'inégalité de traitement des données. La clé de la preuve est une modification d'une méthode variationnelle largement utilisée, qui permet d'obtenir des preuves simples de nombreux résultats connus.

Mots-clefs

Groupes quantiques compacts, groupes quantiques finis, états idempotents, états infiniment divisibles, états de Poisson, espaces L_p non commutatifs, espaces de Lorentz non commutatifs, algèbre de von Neumann de groupe, multiplicateur de Fourier, α - z entropie relative de Rényi, inégalité de traitement des données, convexité/concavité conjointe.

Streszczenie

Niniejsza rozprawa dotyczy pewnych zagadnień nieprzemiennej analizy. Składa się z czterech części, omawiających problemy sięgające od grup kwantowych i nieprzemiennej analizy harmonicznego po teorię kwantowej informacji. W pierwszej części wyznaczamy wszystkie stany idempotentne na grupach kwantowych Sekine, rozwiązując pewien układ równań przy pomocy metod algebry liniowej i elementarnej teorii liczb. Udzielamy tym samym odpowiedzi na pytanie zadane przez Franza i Skalskiego w 2009 roku.

W drugiej części badamy stany nieskończenie podzielne na skończonych grupach kwantowych, czyli stany posiadające n -te pierwiastki dla każdego $n \geq 1$. Pokazujemy, że każdy stan nieskończenie podzielny na skończonej grupie kwantowej jest typu Poissona, czyli posiada przedstawienie jako eksponent względem pewnego stanu idempotentnego.

Trzecia część zawiera pewne dostateczne warunki na L_p -ograniczoność mnożników Fouriera na algebrach von Neumanna grup dyskretnych. Wcześniej znano niewiele wyników tego typu; nowy pomysł w rozprawie polega na tym, że w przypadku dyskretnym wystarczy rozważać mnożniki $L_p - L_q$.

Wreszcie w czwartej części, dotyczącej teorii kwantowej informacji, dowodzimy hipotezy Carlena, Franka i Lieba (implikującej słabszą hipotezę Adenauerta i Datty). Innymi słowy charakteryzujemy wszystkie pary (α, z) dla których α - z entropia Rényi zachowuje się monotonicznie względem działania odwzorowań całkowicie dodatnich zachowujących ślad, a więc spełnia nierówność przetwarzania danych. Kluczowym elementem dowodu jest modyfikacja szeroko stosowanej metody wariacyjnej. Pozwala ona również uzyskać proste dowody wielu znanych wcześniej wyników.

Słowa kluczowe

Zwarte grupy kwantowe, skończone grupy kwantowe, stany idempotentne, stany nieskończenie podzielne, stany Poissona, nieprzemienne przestrzenie L_p , nieprzemienne przestrzenie Lorentza, algebry von Neumanna grup, mnożniki Fouriera, α - z entropia Rényi, nierówność przetwarzania danych, łączna wypukłość/wklęsłość.

Contents

Acknowledgements	5
1 Introduction	15
1.1 From groups to quantum groups	15
1.2 From classical information theory to quantum information theory	18
1.3 Main results	20
2 Idempotent states on Sekine quantum groups	29
2.1 Preliminary: compact quantum groups	29
2.2 Sekine quantum groups	31
2.3 Idempotent states on Sekine quantum groups	33
2.4 The order structure on $\text{Idem}(\mathcal{A}_k)$	43
2.5 Convergence of convolution powers of states on Sekine quantum groups	46
3 Infinitely divisible states on finite quantum groups	49
3.1 Preliminary: Plancherel triple	50
3.2 Plancherel triple induced from an idempotent state	52
3.3 Poisson states on compact quantum groups	57
3.4 Infinitely divisible states on finite quantum groups	59
4 Fourier multipliers on discrete group von Neumann algebras	69
4.1 Preliminary: noncommutative L_p -spaces	69
4.2 Main results	72
4.3 The proofs	74
5 Monotonicity of α-z Rényi relative entropies	77
5.1 Introduction	77
5.2 Background and main results	79
5.3 The proofs	83
Bibliography	89

Chapter 1

Introduction

This PhD thesis is devoted to the study of some problems in noncommutative analysis. These problems originate from classical probability theory on compact groups, classical harmonic analysis and classical information theory. In this thesis we offer new ideas and new tools to overcome various difficulties when dealing with them in the noncommutative setting. More precisely, the thesis studies the following problems.

- (1) *Idempotent states on Sekine quantum groups.* We give concrete formulas for all idempotent states on a family of finite quantum groups: Sekine quantum groups $(\mathcal{A}_k, \Delta_k)$. We also investigate their order structure for k prime. This answers a question of Franz and Skalski [29] stated in 2009. See [76].
- (2) *Infinitely divisible states on finite quantum groups.* Infinite divisible states are states which have n -th root for all $n \geq 1$. We show that any infinitely divisible state on a finite quantum group can be written as the exponential relative to some idempotent state. This generalizes the results of Böge [7] and Parthasarathy [60]. See [77].
- (3) *Fourier multipliers on discrete group von Neumann algebras.* We give two sufficient conditions for boundedness of L_p -Fourier multipliers on discrete group von Neumann algebras. The first one shows that for any discrete group G and any $1 < p < \infty$, any function $\varphi : G \rightarrow \mathbb{C}$ in $\ell_{p^*, \infty}(G)$, where $1/p^* = |1/2 - 1/p|$, yields a L_p -Fourier multiplier on the group von Neumann algebra of G . The second one concerns the radial Fourier multipliers on free group \mathbb{F}_∞ . It shows that if the symbol φ is a radial function on \mathbb{F}_∞ such that $\sup_{n \geq 0} n^{\alpha_p} |\varphi(n)| < \infty$ for some $\alpha_p > \max\{1 - 1/p, 3/2 - 3/p\}$, then the Fourier multiplier is L_p -bounded.
- (4) *Monotonicity of α - z Rényi relative entropies.* The α - z Rényi relative entropies $D_{\alpha, z}$ form a large family of quantum analogues of classical α -Rényi relative entropy. It is a fundamental question in quantum information theory to ask when $D_{\alpha, z}$ is monotone decreasing under completely positive trace preserving maps. We answer this question by considering the joint convexity/concavity of a family of trace functions $\Psi_{p, q, s}$. This confirms a conjecture [10] of Carlen, Frank and Lieb, and a weaker conjecture [2] of Audenaert and Datta. See [75].

1.1 From groups to quantum groups

A topological group is a group G equipped with a topology relative to which the binary operation and the inverse operation are both continuous. It is called *locally compact*

(compact, discrete) if the topology is Hausdorff and locally compact (compact, discrete). A locally compact group G always carries a Radon measure μ , unique up to a positive constant, which is left-invariant: $\mu(K) = \mu(gK)$ for all $g \in G$ and all Borel set $K \subset G$. We call the measure μ the *left Haar measure* on G . Similarly, there exists a Radon measure ν on G (unique up to a positive constant), which is right-invariant. We call the measure ν the *right Haar measure* on G . A locally compact group is called *unimodular* if its left Haar measures and right Haar measures coincide; in this case we call them *Haar measures* for short. A compact group is always unimodular and its Haar measure μ is finite, i.e., $\mu(G) < \infty$. We shall always choose the normalized one, i.e., $\mu(G) = 1$.

For a locally compact abelian group G , a *character* χ on G is a continuous group homomorphism from G to the circle group $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Denote by \widehat{G} the set of all characters on G , then one can also make \widehat{G} into a locally compact abelian group in the following way. Its group operation is given by pointwise multiplication and the unit is the trivial character which takes value one at all elements of G . Its topology is the compact-open topology. We can construct the dual of \widehat{G} , denoted by $\widehat{\widehat{G}}$, in the same way. The *Pontryagin duality theorem* says that G is isomorphic to $\widehat{\widehat{G}}$ canonically. Therefore we may recover a locally compact abelian group by taking its double dual. However, this does not work for nonabelian case. The dual of a locally compact nonabelian group is no longer a group anymore.

The theory of quantum groups was developed for a Pontryagin duality theorem for the nonabelian case. It turns out the dual of a general locally compact group G can be understood as its group von Neumann algebra, still denoted by \widehat{G} . With extra structure on this von Neumann algebra, we may encode the information of this “dual group”, even if it might not exist. This is a naive way to understand the name of “quantum group”. In other words, we shall always investigate the “quantum group” via studying the von Neumann algebra (or C*-algebra) and its extra structure.

What does this extra structure look like? It took a long time in the history to find it and the story is not finished yet. One easily expects the desirable extra structure is economic enough to recover the classical group when the von Neumann algebra is commutative. In particular, the existence of the Haar measure should be possible to be deduced from the structure, like in the classical case. This requirement is so harsh that a widely-accepted theory of *compact quantum groups*, due to Woronowicz [74], emerged only in the end of 1980s. The current widely-used theory of *locally compact quantum groups* was developed by Kustermans and Vaes [48] appeared around 2000. As we mentioned, one of the main difficulties of quantum groups theory is to remove the existence of the Haar measure off the hypotheses of the definition. This was achieved on compact quantum groups in a very nice way by Woronowicz. Such a definition of locally compact quantum groups has not been born yet.

From this one can have a glance that the Haar measure is essential to the theory of locally compact groups. We close this subsection by giving two examples to illustrate the importance of the Haar measure, from algebraic and analytic points of view, respectively.

Firstly, any probability measure μ on a locally compact group G gives a random walk on G . For simplicity, suppose that G is discrete. Then for each step, the probability of moving from $g \in G$ to $h \in G$ is $P(g \rightarrow h) = \mu(g^{-1}h) = \mu(\{g^{-1}h\})$. Under this rule, if we start at the unit $e \in G$ and denote the position of the n -th step by X_n , then we have

$$\begin{aligned} P(X_0 = h) &= \delta_{e,h}, \\ P(X_1 = h) &= P(e \rightarrow h) = \mu(h), \end{aligned}$$

$$\begin{aligned}
P(X_2 = h) &= \sum_{s \in G} P(X_1 = s)P(s \rightarrow h) = \sum_{s \in G} \mu(s)\mu(s^{-1}h) = \mu \star \mu(h), \\
&\dots \\
P(X_n = h) &= \mu^{\star n}(h).
\end{aligned}$$

Here \star denotes the *convolution* product. Generally, any probability measure on a locally compact group gives a random walk. On a locally compact group the *convolution product* of two measures μ_1 and μ_2 is given by

$$\mu_1 \star \mu_2(f) := \int_G \int_G f(xy)\mu_1(x)\mu_2(y), \quad f \in C_0(G),$$

where $C_0(G)$ denotes the set of all continuous functions on G which vanish at infinity. An element μ in $\mathcal{P}rob(G)$ of all probability measures on a locally compact group G is called *idempotent* if $\mu \star \mu = \mu$.

Suppose that G is compact and the convolution powers of the probability measures $\{\mu^{\star n}\}_{n \geq 1}$ converges with respect to the weak* topology, then the limit must be an idempotent probability measure. If one considers the sequence of Cesàro averages $\frac{1}{n} \sum_{k=1}^n \mu^{\star k}$, $n \geq 1$, then it always converges to an idempotent probability measure with respect to the weak* topology. Kawada and Itô [43] showed that idempotent probability measures on G are precisely Haar measures on compact subgroups of G . Then from the limit of the sequence of Cesàro averages relative to some suitable probability measure μ , one may construct the Haar measure on G . This is how Woronowicz constructed the Haar measure (state) on a compact quantum group. See the survey paper [64] for more details.

So the study of idempotent probability measures on compact groups is of great importance and one easily expects similar results in the context of quantum groups. However, the theorem of Kawada and Itô fails even for *finite quantum groups* (compact quantum groups whose underlying C*-algebra is finite-dimensional). Pal [59] gave the first example on an eight-dimensional Kac-Paljutkin quantum group. This implies that, as a quantum analogue of idempotent probability measures on classical groups, idempotent states on the quantum groups do not necessarily correspond to *quantum subgroups* anymore. Then the study of idempotent states usually goes beyond the framework of quantum groups. This brings the difficulty of solving problems involving idempotent states. But on the other hand, it motivates the development of new theories, like *quantum hypergroups* [16, 20, 21, 41].

Secondly, with the left Haar measure μ on a locally compact group G , one can define the L_p -spaces $L_p(G, \mu)$ and the Fourier transform. The latter is the cornerstone of abstract Fourier analysis. If G is abelian, then the Fourier transform of $f \in L_1(G, \mu)$ takes the form:

$$\mathcal{F}(f)(\xi) = \widehat{f}(\xi) = \int_G f(s)\overline{\xi(s)}d\mu(s), \quad \xi \in \widehat{G},$$

where \widehat{G} is the dual of G consisting of all characters on G . By choosing the dual Haar measure $\widehat{\mu}$ on \widehat{G} suitably, the map $L_1(G, \mu) \cap L_2(G, \mu) \ni f \mapsto \widehat{f} \in L_2(\widehat{G}, \widehat{\mu})$ is isometric and can be extended to a unitary between $L_2(G, \mu)$ and $L_2(\widehat{G}, \widehat{\mu})$. This defines the Fourier transform of $f \in L_2(G, \mu)$. The definition of the Fourier transform of $f \in L_p(G, \mu)$, $1 < p < 2$ follows from the famous *Hausdorff-Young inequality*:

$$\|\widehat{f}\|_{L_{p'}(\widehat{G}, \widehat{\mu})} \leq \|f\|_{L_p(G, \mu)}, \quad f \in L_p(G, \mu). \quad (1.1)$$

It is natural to ask what the Fourier transform looks like when G is nonabelian and whether we still have (1.1) or not. For this Kunze [47] made the following observation. Let G be

a locally compact abelian group as above. Let $\lambda(f)$ denote the left regular representation of $f \in L_1(G, \mu)$ on $L_2(G, \mu)$, which is an operator given by

$$(\lambda(f)g)(s) := f \star g(s) = \int_G f(t)g(t^{-1}s)d\mu(t), \quad s \in G, \quad g \in L_2(G, \mu).$$

Denote by L_f the operator on $L_2(G, \mu)$ given by the multiplying by f . Since \mathcal{F} turns convolution into multiplication, we have

$$\mathcal{F}(\lambda(f)g) = \mathcal{F}(f)\mathcal{F}(g) = L_{\mathcal{F}(f)}\mathcal{F}(g), \quad f \in L_1(G, \mu), \quad g \in L_2(G, \mu).$$

Recall that \mathcal{F} is unitary on $L_2(G, \mu)$, so $\lambda(f)$ is unitarily equivalent to the operator $L_{\mathcal{F}(f)}$. This suggests us to use $\lambda(f)$ as a substitute of $\mathcal{F}(f)$. From this Kunze defined the Fourier transform on the locally compact unimodular group (G, μ) and generalized (1.1) to this setting. The dual of G , still denoted by \widehat{G} , is no longer a group, but the von Neumann algebra generated by $\lambda(L_1(G, \mu))$ in $B(L_2(G, \mu))$. It turns out that there is a canonical trace $\widehat{\mu}$ on \widehat{G} , so the noncommutative L_p -space $L_p(\widehat{G}, \widehat{\mu})$ is constructed in the sense of Dixmier [22] and Segal [66]. For the nonunimodular case, the dual \widehat{G} is not necessarily equipped with a trace. Terp solved this problem with the help of the Tomita-Takesaki theory and the noncommutative L_p -spaces associated with a weight. In recent years Cooney [17] and Caspers [13] generalized all these results to locally compact quantum groups.

1.2 From classical information theory to quantum information theory

Classical information theory emerged after the groundbreaking paper [68] of Shannon. *Quantum information theory* intersects the quantum physics and information theory. Roughly speaking, quantum information theory is the study of information theory within the framework of quantum mechanics. It is also known as *quantum Shannon theory* in honour of Shannon.

We fix some notations in this part. We use \mathcal{H} to denote a finite dimensional Hilbert space. We use $\mathcal{P}(\mathcal{H})$ to denote the set of all invertible positive operators over \mathcal{H} , and $\mathcal{D}(\mathcal{H})$ to denote the set of all *quantum states*, or *density operators* over \mathcal{H} , i.e., invertible positive operators over \mathcal{H} with unit trace.

As a measurement of information content of a probability density function p on \mathbb{R} , its *Shannon entropy* is defined as

$$S(p) := - \int_{\mathbb{R}} p(x) \log p(x) dx.$$

Shannon entropy plays an essential role in classical information theory. It admits a natural quantum analogue, referred to as the *von Neumann entropy*:

$$D(\rho) := -\text{Tr} \rho \log \rho, \quad \rho \in \mathcal{D}(\mathcal{H}). \quad (1.2)$$

We remark here that in quantum information theory we usually choose binary logarithm \log_2 . But we will not specify this here, since it will not matter in this thesis.

There are many other entropy quantities which are important in classical information theory, for example, the *Kullback-Leibler divergence*, or the *relative entropy* of p with respect to q :

$$S(p||q) := \int_{\mathbb{R}} p(x) \log \frac{p(x)}{q(x)} dx,$$

where p and q are two density functions on \mathbb{R} . It has an *operational meaning* as follows. Suppose that Alice encodes her message into a sequence of 0 and 1's, and sends them to Bob. Bob will then decode from a sequence of 0 and 1's he received so as to read Alice's message correctly. Unfortunately, because of the noisy channel, what Bob will receive is a sequence of random variables with overlapping distributions. So Bob will encounter a problem of identifying which are 0's and which are 1's. Assume that 0 is sent to a random variable with a density p centered at 0, and 1 is sent to a random variable with a density q centred at 1. Suppose that the n -th signal arriving to Bob is a random variable X_n and all X_n 's are independent. Bob cannot tell that a single signal comes from 0 or 1 if p and q overlap. But the point is, if Alice sends the same message N times, Bob can extract the correct information as when N tends to infinity, and the error decays exponentially to 0. And the order of the exponential decay of the error is given in terms of the relative entropy $S(p||q)$.

In fact, for each $N > 0$, Bob needs to choose $A_N \subset \mathbb{R}^N$ as a measurement, such that if $(X_1, \dots, X_N) \in A_N$, then he accepts p as the governing distribution, and otherwise he accepts q . Fix small $\epsilon > 0$, if $\int_{A_N} p^{\otimes N} > 1 - \epsilon$, then consider

$$\beta_{\epsilon, N}(p, q) := \inf_{A_N \subset \mathbb{R}^N} \left\{ \log \int_{A_N} q^{\otimes N} : \int_{A_N} p^{\otimes N} > 1 - \epsilon \right\}.$$

Then we have [46, 45]

$$\limsup_{N \rightarrow \infty} \frac{1}{N} \beta_{\epsilon, N}(p, q) \leq -S(p||q) \text{ and } \liminf_{N \rightarrow \infty} \frac{1}{N} \beta_{\epsilon, N}(p, q) \geq -\frac{1}{1 - \epsilon} S(p||q). \quad (1.3)$$

A result similar to (1.3) holds in quantum information theory. For this we pause briefly to speculate what the quantum analogue of relative entropy should look like. From (1.2) we know that one should replace the density functions p and q with the density operators ρ and σ , and the integral with the trace. And when ρ and σ commute, we should recover $S(p||q)$, where p, q are constructed from the spectra of ρ and σ , respectively. There are, however, a lot of formulas verifying such conditions, for example,

$$D(\rho||\sigma) := \text{Tr} \rho (\log \rho - \log \sigma), \quad (1.4)$$

and

$$D'(\rho||\sigma) := \text{Tr} \rho \log (\sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}}). \quad (1.5)$$

The formula D defined in (1.4) is known as *Umegaki relative entropy* [71], and it turns out to be the proper formula in the quantum setting with an operational meaning in the sense of (1.3) [35].

Except for the relative entropy S , there is a family of α -versions of relative entropies introduced by Rényi [62], referred to as *α -Rényi relative entropies*:

$$S_\alpha(p||q) := \frac{1}{\alpha - 1} \log \int p^\alpha q^{1-\alpha}, \quad \alpha \in (0, 1) \cup (1, \infty),$$

where p and q are density functions on \mathbb{R} . Many error bounds can be given in terms of S_α [18], so they also admit an operational meaning.

Looking for proper quantum analogues of S_α and studying their properties has become a popular topic in recent years in quantum information theory. Two of the most important quantum versions of S_α are the *quantum α -Rényi relative entropy*:

$$D_\alpha(\rho||\sigma) := \frac{1}{\alpha - 1} \log \text{Tr}(\rho^\alpha \sigma^{1-\alpha}),$$

and the *sandwiched α -Rényi relative entropy* [56, 73]

$$\tilde{D}_\alpha(\rho||\sigma) := \frac{1}{\alpha - 1} \log \operatorname{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha.$$

They both admit operational meanings for certain values of α [54, 55].

It is then a natural question how to put D_α and \tilde{D}_α into one unifying framework. For this Audenaert and Datta [2] introduced the α - z Rényi relative entropy

$$D_{\alpha,z}(\rho||\sigma) := \frac{1}{\alpha - 1} \log \operatorname{Tr}(\sigma^{\frac{1-\alpha}{2z}} \rho^{\frac{\alpha}{z}} \sigma^{\frac{1-\alpha}{2z}})^z, \quad \alpha \in (-\infty, 1) \cup (1, \infty), \quad z > 0,$$

where $\rho, \sigma \in \mathcal{D}(\mathcal{H})$.

For proper quantum analogues of classical entropies, we expect them to verify certain properties in the classical cases. Things become much more difficult in the noncommutative setting. For example, the *Strong Subadditivity* of von Neumann entropy D was conjectured by Lanford and Robinson in 1968 and was proved by Lieb and Ruskai in 1973 using a concavity result of a certain trace function (which is nothing but $\Psi_{p,q,1}$ we are going to discuss later). Here we are interested in the monotonicity of $D_{\alpha,z}$. That is,

$$D_{\alpha,z}(\mathcal{E}(\rho)||\mathcal{E}(\sigma)) \leq D_{\alpha,z}(\rho||\sigma),$$

for all completely positive trace preserving (CPTP) maps \mathcal{E} on $\mathcal{B}(\mathcal{H})$, all $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ and all \mathcal{H} . This inequality is known as the *Data Processing Inequality* (DPI). It is a fundamental inequality in quantum information theory, which indicates that the quantum states ρ and σ become harder to distinguish after the action of CPTP maps. We shall identify all (α, z) such that $D_{\alpha,z}$ verifies DPI, and from the solution the readers will see how the noncommutative techniques are applied to simplify the problem.

1.3 Main results

1.3.1 Idempotent states on Sekine quantum groups

Even if the study of idempotent states is already very thorough [3, 29, 28, 30, 40, 42], few concrete examples on compact quantum groups which are neither commutative nor co-commutative, are known. The first contribution of this thesis is to determine all the idempotent states on a family of finite quantum groups, usually known as *Sekine quantum groups*. This answers a question of Franz and Skalski stated in 2009 [29].

Recall that an idempotent state ϕ on a compact quantum group \mathbb{G} is a state such that $\phi \star \phi = \phi$. When \mathbb{G} is a classical compact group, ϕ is the Haar measure of some compact subgroup of \mathbb{G} [43]. However, it is well-known that this fails for general quantum groups. Even on finite quantum groups, an idempotent state does not necessarily correspond to a quantum subgroup [29, 59]; a quantum hypergroup serves as a substitute here [29]. To this end, we introduce the notion of a *Haar idempotent state*, which is the idempotent state arising as the Haar state on some quantum subgroup of \mathbb{G} . Otherwise it is called a *non-Haar idempotent state*.

Our main result is to determine all the idempotent states on Sekine quantum groups.

Definition 1.1. [29, 67] *Fix $k \geq 2$ an integer. Let η be a primitive k -th root of unity, say, $\eta = e^{\frac{2\pi i}{k}}$, and let $\mathbb{Z}_k := \{0, 1, \dots, k-1\}$ be the cyclic group with order k . Set*

$$\mathcal{A}_k := \bigoplus_{i,j \in \mathbb{Z}_k} \mathbb{C}d_{i,j} \oplus \mathbb{M}_k(\mathbb{C}),$$

where $d_{i,j}$ denotes the corresponding basis of \mathbb{C} . Denote by $\{e_{i,j} : i, j \in \mathbb{Z}_k\}$ the matrix units of the k -by- k full matrix algebra $M_k(\mathbb{C})$. Define

$$\Delta_k(d_{i,j}) := \sum_{m,n \in \mathbb{Z}_k} d_{m,n} \otimes d_{i-m,j-n} + \frac{1}{k} \sum_{m,n \in \mathbb{Z}_k} \eta^{i(m-n)} e_{m,n} \otimes e_{m+j,n+j}, \quad (1.6)$$

$$\Delta_k(e_{i,j}) := \sum_{m,n \in \mathbb{Z}_k} \eta^{m(i-j)} d_{-m,-n} \otimes e_{i-n,j-n} + \sum_{m,n \in \mathbb{Z}_k} \eta^{m(j-i)} e_{i-n,j-n} \otimes d_{m,n}, \quad (1.7)$$

for $i, j \in \mathbb{Z}_k$. Then the pair $(\mathcal{A}_k, \Delta_k)$ forms a finite quantum group, called a Sekine quantum group.

Let $\{\tilde{d}_{i,j}, \tilde{e}_{i,j} : i, j \in \mathbb{Z}_k\}$ be the dual basis of $\{d_{i,j}, e_{i,j} : i, j \in \mathbb{Z}_k\}$. Using this the idempotent states on \mathcal{A}_k are characterized through the following lemma:

Lemma 1.2. *A functional $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s} \in \mathcal{A}'_k$ is an idempotent state if and only if $\alpha_{i,j} \geq 0$ for all $i, j \in \mathbb{Z}_k$, $K := [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k}$ is positive semi-definite, and the following equations hold:*

$$\alpha_{i,j} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r,j-s} \alpha_{r,s} + \frac{1}{k} \sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j,s+j}, \quad i, j \in \mathbb{Z}_k, \quad (1.8)$$

$$\kappa_{r,s} = \sum_{i,j \in \mathbb{Z}_k} \eta^{i(s-r)} \alpha_{i,j} (\kappa_{r+j,s+j} + \kappa_{r-j,s-j}), \quad r, s \in \mathbb{Z}_k, \quad (1.9)$$

$$\mu(1_{\mathcal{A}_k}) = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} + \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 1. \quad (1.10)$$

By solving these equations, we can compute all the idempotent states on \mathcal{A}_k :

Theorem 1.3. [76, Theorem 2.12] *Fix $k \geq 2$ an integer. Then the family of idempotent states on Sekine quantum group \mathcal{A}_k , denoted by $\text{Idem}(\mathcal{A}_k)$, is given through*

$$\text{Idem}(\mathcal{A}_k) = \{h_{\mathcal{A}_k}\} \cup \mathcal{I}_1(\mathcal{A}_k) \cup \mathcal{I}_2(\mathcal{A}_k) \cup \mathcal{I}_3(\mathcal{A}_k),$$

where

(1) $h_{\mathcal{A}_k}$ is the Haar state;

(2) $\mathcal{I}_1(\mathcal{A}_k)$ is the set of idempotent states of the form

$$h_\Gamma := \frac{1}{\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j},$$

with Γ a subgroup of $\mathbb{Z}_k \times \mathbb{Z}_k$.

(3) $\mathcal{I}_2(\mathcal{A}_k)$ is the set of idempotent states of the form

$$h_{\Gamma,l} := \frac{1}{2\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j} + \frac{q}{2k} \sum_{r \equiv l \pmod{q}} \tilde{e}_{r,r},$$

where $\Gamma = \mathbb{Z}_k \times q\mathbb{Z}_k$ with $q|k$, $q > 1$, and $l \in \mathbb{Z}_q$; or

(4) $\mathcal{I}_3(\mathcal{A}_k)$ is the set of idempotent states of the form

$$h_{\Gamma,l,\tau} := \frac{1}{2\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j} + \frac{q}{2k} \sum_{r,s \equiv l \pmod{q}} \tau_{s-r} \tilde{e}_{r,s},$$

where $\Gamma = p\mathbb{Z}_k \times q\mathbb{Z}_k$ with $p > 1$ and $pq = k$, $l \in \mathbb{Z}_q$, and $\tau = (\tau_j)_{j \in q\mathbb{Z}_k} \in \{\pm 1\}^{q\mathbb{Z}_k}$ such that

$$\sum_{j \in q\mathbb{Z}_k} \tau_j \eta^{ij} \geq 0, \quad i \in \mathbb{Z}_k/q. \quad (1.11)$$

Moreover, the family of Haar idempotent states is given by $\{h_{\mathcal{A}_k}\} \cup \mathcal{I}_1(\mathcal{A}_k)$ and the family of non-Haar idempotent states is given by $\mathcal{I}_2(\mathcal{A}_k) \cup \mathcal{I}_3(\mathcal{A}_k)$.

We may define a partial order \prec on $\text{Idem}(\mathcal{A}_k)$ through

$$\phi_1 \prec \phi_2 \quad \text{if} \quad \phi_1 \star \phi_2 = \phi_2.$$

For k prime, $\mathbb{Z}_k \times \mathbb{Z}_k$ has one subgroup of order 1: $\Gamma_0 = \{(0,0)\}$, $k+1$ subgroups of order k :

$$\Gamma_+ = \mathbb{Z}_k \times k\mathbb{Z}_k, \quad \Gamma_- = k\mathbb{Z}_k \times \mathbb{Z}_k, \quad \Gamma_i = \{j(1,i) = (j,ij) : j \in \mathbb{Z}_k\},$$

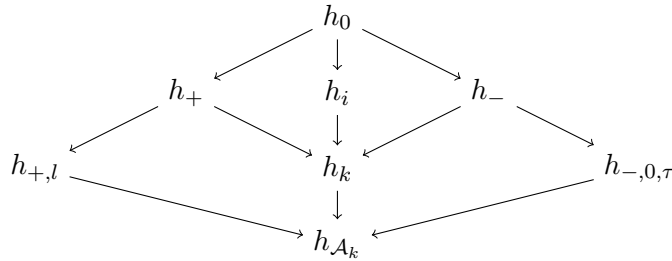
where $i = 1, 2, \dots, k-1$, and one subgroup of order k^2 : $\Gamma_k = \mathbb{Z}_k \times \mathbb{Z}_k$. We remove Γ from the subscripts for convenience, for example $h_+ := h_{\Gamma_+}$, $h_- := h_{\Gamma_-}$, and $h_i := h_{\Gamma_i}$. Then from Theorem 1.3 it follows that:

$$\mathcal{I}_1(\mathcal{A}_k) = \{h_+, h_-, h_i : i = 0, 1, \dots, k\},$$

$$\mathcal{I}_2(\mathcal{A}_k) = \{h_{+,l} : l \in \mathbb{Z}_k\},$$

$$\mathcal{I}_3(\mathcal{A}_k) = \{h_{-,l,\tau} : l \in \mathbb{Z}_k, \tau \text{ verifies (1.11)}\}.$$

Hence we can draw the Hasse diagram of the lattice $(\text{Idem}(\mathcal{A}_k), \prec)$ for prime k as [76, Example 3.3]:



where $i = 1, 2, \dots, k-1$, $l \in \mathbb{Z}_k$, and τ satisfies (1.11). Note that h_0 is the counit on \mathcal{A}_k .

1.3.2 Infinitely divisible states on finite quantum groups

By an *infinitely divisible state* on a compact quantum group \mathbb{G} we mean a state ω on $C(\mathbb{G})$ which admits n -th root ω_n for all $n \geq 1$, that is, ω_n is a state on \mathbb{G} such that $\omega = \omega_n^{\star n}$. Here \star denotes the convolution of bounded linear functionals on $C(\mathbb{G})$: $\phi_1 \star \phi_2 := (\phi_1 \otimes \phi_2)\Delta$, where Δ is the comultiplication. We denote by $\mathcal{I}(\mathbb{G})$ the set of all infinitely divisible states on \mathbb{G} . The second main result of this thesis, is to characterize all the infinitely divisible states on finite quantum groups. This generalizes Böge's result [7] on infinitely divisible

probability measures on finite groups and Parthasarathy's work [60] on infinitely divisible normalized positive definite functions on finite groups.

There is a certain class of infinitely divisible states, states of *Poisson type*, or *Poisson states*. Given an idempotent state ϕ , a bounded linear functional u on $C(\mathbb{G})$ is called ϕ -*bi-invariant* if $u = u \star \phi = \phi \star u$. And if u is ϕ -bi-invariant, we define its exponential with respect to ϕ as:

$$\exp_{\phi}(u) := \phi + \sum_{n \geq 1} \frac{u^{\star n}}{n!}.$$

A state ω on \mathbb{G} is of *Poisson type* if there exists an idempotent state ϕ such that one of the following equivalent conditions holds ([77, Theorem 4.4])

1. $\omega = \omega_1$ with $\{\omega_t\}_{t \geq 0}$ a norm continuous convolution semigroup of states such that $\omega_0 = \phi$;
2. $\omega = \exp_{\phi}(u)$, where u is a ϕ -bi-invariant bounded linear functional on $C(\mathbb{G})$ such that $u(1) = 0$ and $u(x^*x) \geq 0$ for all $x \in C(\mathbb{G})$ with $\phi(x^*x) = 0$;
3. $\omega = \exp_{\phi}(u)$, where $u = r(v - \phi)$, with $r > 0$ and v a ϕ -bi-invariant state on $C(\mathbb{G})$.

Denote by $\mathcal{P}(\mathbb{G})$ the set all states of Poisson type. Clearly, $\mathcal{P}(\mathbb{G}) \subset \mathcal{I}(\mathbb{G})$. Our main result asserts that, the converse inclusion holds for finite quantum groups.

Theorem 1.4. [77, Theorem 4.11] *Let \mathbb{G} be a finite quantum group. Then $\mathcal{I}(\mathbb{G}) = \mathcal{P}(\mathbb{G})$.*

When \mathbb{G} is commutative, it is then a classical finite group G and a state is a probability measure on G . In this case we recover Böge's theorem concerning infinitely divisible probability measures on finite groups:

Theorem 1.5. [7] *Any infinitely divisible probability measure on a finite group is of Poisson type.*

When \mathbb{G} is co-commutative, it is then the dual of finite group Γ and a state is a normalized positive definite function on Γ . In this case we recover Parthasarathy's result on infinitely divisible normalized positive definite functions on finite groups:

Theorem 1.6. [60] *Any infinitely divisible normalized positive definite function on a finite group is of Poisson type.*

1.3.3 Fourier multipliers on discrete group von Neumann algebras

In recent years, the study of L_p -Fourier multipliers on group von Neumann algebras has become one of the most important topics in noncommutative harmonic analysis. Little is known about L_p -Fourier multipliers on group von Neumann algebra \widehat{G} even when the group G is discrete. One example people are particularly interested in is the free group \mathbb{F}_{∞} . It is a challenging problem to generalize classical Hörmander-Mikhlin multiplier theorem to group von Neumann algebras.

Here we offer a new idea regarding L_p -Fourier multipliers, which works for discrete groups. Recall that for any discrete group G , the group von Neumann algebra \widehat{G} is the von Neumann algebra in $B(\ell_2(G))$ generated by all $\lambda(g), g \in G$, where λ is the left regular representation of G . \widehat{G} is equipped with a canonical tracial state τ . A function φ on G is a L_p -Fourier multiplier if $T_{\varphi} : \sum_{\text{finite sum}} a_g \lambda(g) \mapsto \sum_{\text{finite sum}} \varphi(g) a_g \lambda(g)$ extends to a

bounded map on $L_p(\widehat{G}, \tau)$. Here $L_p(\widehat{G}, \tau)$ is defined as the completion of $(\widehat{G}, \|\cdot\|_p)$ with $\|x\|_p := (\tau|x|^p)^{1/p}$. Since τ is finite, the L_p -boundedness of T_φ follows from its L_p - L_q boundedness, whenever $p < q$. This simplifies the problem because one can choose in particular $q = 2$ when $p < 2$ (consider L_2 - L_p if $p > 2$). Our estimate of L_p - L_2 (L_2 - L_p) was inspired by Hörmander's work [36] on L_p - L_q Fourier multipliers and Ricard-Xu's work [63] on hypercontractivity.

The first result concerns all discrete groups. Recall that for any $r > 0$, the space $\ell_{r,\infty}(G)$ consists of all functions $f : G \rightarrow \mathbb{C}$ such that

$$\|f\|_{r,\infty} := \sup_{t>0} t |\{g \in G : |f(g)| \geq t\}|^{\frac{1}{r}} < \infty,$$

where $|S|$ denotes the cardinal of $S \subset G$.

Here and in the following, $A \lesssim_p B$ means $A \leq c_p B$ for some constant $c_p > 0$, and \mathbb{N} denotes the family of natural numbers.

Theorem 1.7. *Let $1 < p < \infty$ and $1/p^* := |1/2 - 1/p|$. Let G be any discrete group. Then for any $\varphi \in \ell_{p^*,\infty}(G)$, we have*

$$\|T_\varphi : L_p(\widehat{G}, \tau) \rightarrow L_p(\widehat{G}, \tau)\| \lesssim_p \|\varphi\|_{p^*,\infty}.$$

Our second result deals with the free group \mathbb{F}_∞ . Thanks to duality, we only consider the case $2 < p < \infty$.

Theorem 1.8. *Let $2 < p < \infty$. Suppose that φ is radial on \mathbb{F}_∞ , i.e., $\varphi(g) = \phi(|g|)$, with $|\cdot|$ the length function on \mathbb{F}_∞ , for some $\phi : \mathbb{N} \rightarrow \mathbb{C}$. Then we have*

$$\|T_\varphi : L_p(\widehat{\mathbb{F}}_\infty) \rightarrow L_p(\widehat{\mathbb{F}}_\infty)\| \leq \left(\sum_{n \geq 0} (1+n)^{\alpha_p} |\phi(n)|^2 \right)^{1/2},$$

where $\alpha_p = \max\{2 - \frac{6}{p}, 1 - \frac{2}{p}\}$.

As a corollary, we obtain the following criterion for radial Fourier multipliers on \mathbb{F}_∞ .

Corollary 1.9. *Suppose that T_φ is a radial multiplier with $\varphi = \phi(|\cdot|)$. Then T_φ is a L_p -Fourier multiplier on $\widehat{\mathbb{F}}_\infty$ if there exists $\epsilon > 0$ such that*

$$\sup_{n \geq 0} n^{1 - \frac{1}{p} + \epsilon} |\phi(n)| < \infty, \quad 2 < p \leq 4,$$

or

$$\sup_{n \geq 0} n^{\frac{3}{2} - \frac{3}{p} + \epsilon} |\phi(n)| < \infty, \quad p \geq 4.$$

From this we obtain radial L_p -Fourier multipliers T_φ with

$$\varphi(g) = \frac{1}{|g|^{1 - \frac{1}{p} + \epsilon}}, \quad 2 < p \leq 4,$$

and

$$\varphi(g) = \frac{1}{|g|^{\frac{3}{2} - \frac{3}{p} + \epsilon}}, \quad p \geq 4,$$

for any $\epsilon > 0$.

1.3.4 Monotonicity of α - z Rényi relative entropies

The intersection of quantum information and noncommutative analysis has appeared in recent years. This gave birth to a series of significant results in both areas and is inaugurating a promising direction of research. The result we are going to talk about is such an example.

Throughout this part \mathcal{H} always denotes a finite dimensional Hilbert space, $\mathcal{B}(\mathcal{H})$ denotes the set of all bounded linear operators over \mathcal{H} , $\mathcal{P}(\mathcal{H})$ denotes the set of all positive linear operators over \mathcal{H} , and $\mathcal{D}(\mathcal{H})$ denotes the subset of $\mathcal{P}(\mathcal{H})$ whose elements have unit trace (density operators). Moreover, we use $\mathcal{B}(\mathcal{H})^\times$ (reps. $\mathcal{P}(\mathcal{H})^\times$ and $\mathcal{D}(\mathcal{H})^\times$) to denote the family of invertible operators in $\mathcal{B}(\mathcal{H})$ (resp. $\mathcal{P}(\mathcal{H})$ and $\mathcal{D}(\mathcal{H})$). We use I to denote the identity operator.

Classical entropy quantities including the Shannon entropy and the α -Rényi relative entropies play a crucial role in classical information theory, or Shannon theory. They admit various quantum analogues, see more details in [2, 10]. It is important, but difficult to decide, among the family of quantum relative entropies, which are right ones in the quantum world. One fundamental property that the right ones must satisfy is the monotonicity under completely positive trace preserving (CPTP) maps, or the *Data Processing Inequality* (DPI). We determine all the (α, z) such that α - z Rényi relative entropy $D_{\alpha,z}$ satisfies DPI by proving a conjecture of Audenaert and Datta [2]. Indeed, we shall establish a stronger conjecture of Carlen, Frank and Lieb [10].

Conjecture 1.10. [10, Conjecture 4] If $1 \leq p \leq 2$, $-1 \leq q < 0$, $(p, q) \neq (1, -1)$ and $s \geq 1/(p+q)$, then for any finite dimensional Hilbert space \mathcal{H} and any $K \in \mathcal{B}(\mathcal{H})^\times$,

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s, \quad A, B \in \mathcal{P}(\mathcal{H})^\times, \quad (1.12)$$

is jointly convex.

On one hand, the study of the joint convexity/concavity of $\Psi_{p,q,s}$ has a long history in mathematical physics. The first important result on joint convexity/concavity $\Psi_{p,q,s}$ is the famous *Lieb's concavity theorem* [49]: $\Psi_{p,q,1}$ is jointly concave for $p, q \geq 0$ such that $p+q \leq 1$. After that many methods have been developed and much progress has been made. More details in the history can be found in the survey paper [10]. The last unsolved case is Conjecture 1.10, for which little has been known.

On the other hand, the joint convexity/concavity of $\Psi_{p,q,s}$ is closely related to the monotonicity of the α - z Rényi relative entropies:

$$D_{\alpha,z}(\rho||\sigma) := \frac{1}{\alpha-1} \log \text{Tr}(\sigma^{\frac{1-\alpha}{2z}} \rho^{\frac{\alpha}{z}} \sigma^{\frac{1-\alpha}{2z}})^z, \quad \alpha \in (-\infty, 1) \cup (1, \infty), \quad z > 0,$$

where $\rho, \sigma \in \mathcal{D}(\mathcal{H})^\times$. The α - z Rényi relative entropies were introduced and studied by Audenaert and Datta [2] and serve as a unifying generalization of the *quantum α -Rényi relative entropies*:

$$D_\alpha(\rho||\sigma) := \frac{1}{\alpha-1} \log \text{Tr}(\rho^\alpha \sigma^{1-\alpha}), \quad \alpha \in (0, 1) \cup (1, \infty),$$

and the *sandwiched α -Rényi entropies* [56, 73]:

$$\tilde{D}_\alpha(\rho||\sigma) := \frac{1}{\alpha-1} \log \text{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha, \quad \alpha \in (0, 1) \cup (1, \infty).$$

Note that $D_{\alpha,1} = D_\alpha$ and $D_{\alpha,\alpha} = \tilde{D}_\alpha$.

Let us come back to the relation between the joint convexity/concavity of $\Psi_{p,q,s}$ and monotonicity of α - z Rényi relative entropy. Recall that $D_{\alpha,z}$ is monotone under CPTP maps if

$$D_{\alpha,z}(\mathcal{E}(\rho)||\mathcal{E}(\sigma)) \leq D_{\alpha,z}(\rho||\sigma), \quad (1.13)$$

for any CPTP map \mathcal{E} on $\mathcal{B}(\mathcal{H})^\times$, for all density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})^\times$ and for any finite dimensional Hilbert space \mathcal{H} . This inequality is known as the *Data Processing Inequality* (DPI). It is known (cf. [10]) that when $K = I$ and $s = 1/(p+q)$, the joint convexity (concavity when $\alpha < 1$) of $\Psi_{p,q,s}$ is essentially equivalent to DPI for $D_{\alpha,z}$, under the following correspondence between the parameters:

$$p = \frac{1-\alpha}{z} \text{ and } q = \frac{\alpha}{z}.$$

We confirmed Conjecture 1.10 using a variational method. The method turns out to be a very powerful tool which yields simpler proofs of many known results. Finally, we obtain the following statement.

Theorem 1.11. [75, Theorem 1.3] *Suppose that $s > 0$. Then for any $K \in \mathcal{B}(\mathcal{H})^\times$, $\Psi_{p,q,s}$ defined in (1.12) is*

- (1) *jointly concave if $0 \leq p, q \leq 1$ and $0 < s \leq 1/(p+q)$;*
- (2) *jointly convex if $-1 \leq p, q \leq 0$ and $s > 0$;*
- (3) *jointly convex if $-1 \leq \min\{p, q\} \leq 0$, $1 \leq \max\{p, q\} \leq 2$, $(\min\{p, q\}, \max\{p, q\}) \neq (-1, 1)$ and $s \geq 1/(p+q)$.*

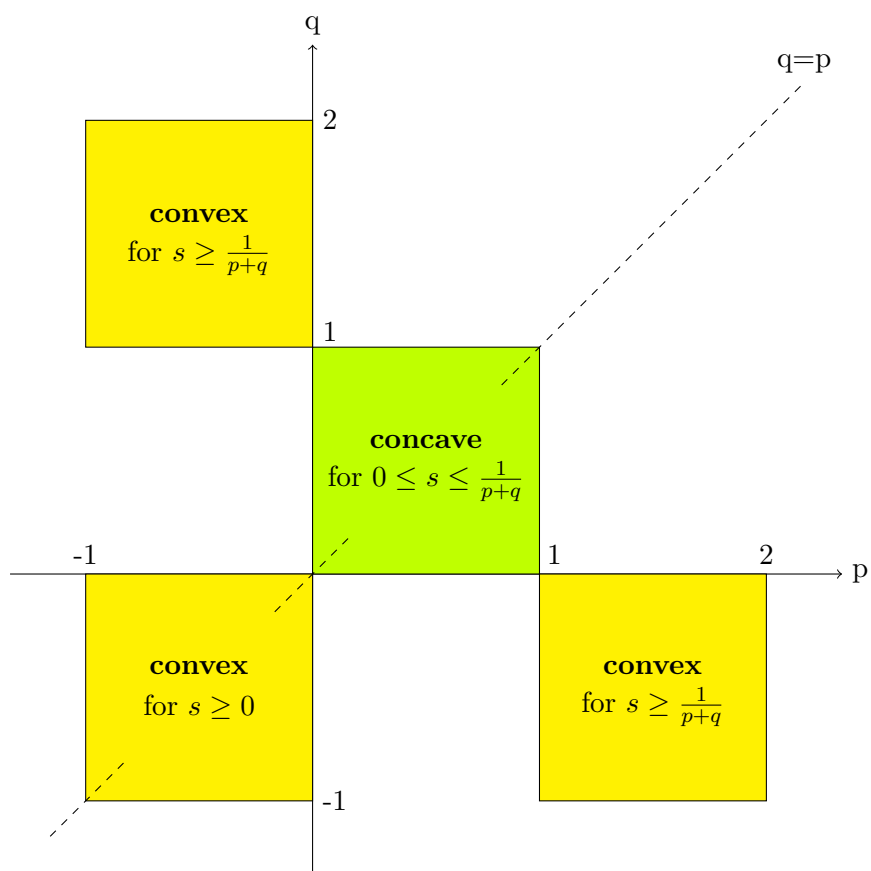
In other cases, there exist \mathcal{H} and $K \in \mathcal{B}(\mathcal{H})^\times$ such that $\Psi_{p,q,s}$ is neither jointly convex nor jointly concave.

The figure 1.1 summarizes the joint convexity/concavity of $\Psi_{p,q,s}$ for all p, q, s . Note that $(1, -1)$ and $(-1, 1)$ do not belong to the area of convexity.

Thus from Theorem 1.11 it follows that

Theorem 1.12. [75, Corollary 1.4] *The α - z relative Rényi entropy $D_{\alpha,z}$ is monotone under all CPTP maps on $\mathcal{B}(\mathcal{H})^\times$ for all \mathcal{H} if and only if one of the following holds*

- (1) $0 < \alpha < 1$ and $z \geq \max\{\alpha, 1-\alpha\}$;
- (2) $1 < \alpha \leq 2$ and $\frac{\alpha}{2} \leq z \leq \alpha$;
- (3) $2 \leq \alpha < \infty$ and $\alpha - 1 \leq z \leq \alpha$.

Figure 1.1: Joint convexity/concavity of $\Psi_{p,q,s}$

Chapter 2

Idempotent states on Sekine quantum groups

The main result of this chapter is the computation of all the idempotent states on Sekine quantum groups, which answers a question of Franz and Skalski stated in 2009 [29]. This is achieved by solving a complicated system of equations using linear algebra and elementary number theory.

We fix some notations for this chapter. For any $k \geq 1$, $\mathbb{M}_k(\mathbb{C})$ will denote the family of all k -by- k complex matrices. We shall use $[\cdot]$ to denote the greatest integer function, i.e., $[x]$ denotes the greatest integer that is smaller than or equal to x . We denote by $\#S$ the cardinal of the set S .

2.1 Preliminary: compact quantum groups

Let us recall the definition and properties of compact quantum groups. We refer to [52, 74] for more details.

Definition 2.1. *Let A be a unital C^* -algebra. If there exists a unital $*$ -homomorphism $\Delta : A \rightarrow A \otimes A$ such that*

1. $(\Delta \otimes \iota)\Delta = (\iota \otimes \Delta)\Delta$;
2. $\{\Delta(a)(1_A \otimes b) : a, b \in A\}$ and $\{\Delta(a)(b \otimes 1_A) : a, b \in A\}$ are linearly dense in $A \otimes A$;

then (A, Δ) is called a compact quantum group and Δ is called the comultiplication on A . Here and in the following, ι always denotes the identity map. We denote $\mathbb{G} = (A, \Delta)$ and $A = C(\mathbb{G})$. For simplicity, we write $\Delta^{(2)} = (\Delta \otimes \iota)\Delta$.

Any compact quantum group $\mathbb{G} = (A, \Delta)$ admits a unique *Haar state*, i.e., a state (positive linear functional) h on A such that

$$(h \otimes \iota)\Delta(a) = h(a)1_A = (\iota \otimes h)\Delta(a), \quad a \in A.$$

Consider an element $u \in A \otimes B(H)$ with $\dim H = n$. By identifying $A \otimes B(H)$ with $\mathbb{M}_n(A)$ we can write $u = [u_{ij}]_{i,j=1}^n$, where $u_{ij} \in A$. The matrix u is called an *n -dimensional representation* of \mathbb{G} if we have

$$\Delta(u_{ij}) = \sum_{k=1}^n u_{ik} \otimes u_{kj}, \quad i, j = 1, \dots, n.$$

A representation u is called *unitary* if u is unitary as an element in $\mathbb{M}_n(A)$, and *irreducible* if the only matrices $T \in \mathbb{M}_n(\mathbb{C})$ such that $uT = Tu$ are multiples of identity matrix. Two representations $u, v \in \mathbb{M}_n(A)$ are said to be *equivalent* if there exists an invertible matrix $T \in \mathbb{M}_n(\mathbb{C})$ such that $Tu = vT$. Denote by $\text{Irr}(\mathbb{G})$ the set of equivalence classes of irreducible unitary representations of \mathbb{G} . For each $\alpha \in \text{Irr}(\mathbb{G})$, denote by $u^\alpha \in A \otimes B(H_\alpha)$ a representative of the class α , where H_α is the finite-dimensional Hilbert space on which u^α acts. In the sequel we write $n_\alpha = \dim H_\alpha$.

Denote $\text{Pol}(\mathbb{G}) = \text{span} \left\{ u_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, \alpha \in \text{Irr}(\mathbb{G}) \right\}$. This is a dense subalgebra of A . On $\text{Pol}(\mathbb{G})$ the Haar state h is faithful. It is well-known that $(\text{Pol}(\mathbb{G}), \Delta)$ is equipped with the Hopf*-algebra structure. That is, there exist a linear antihomomorphism S on $\text{Pol}(\mathbb{G})$, called the *antipode*, and a unital *-homomorphism $\epsilon : \text{Pol}(\mathbb{G}) \rightarrow \mathbb{C}$, called the *counit*, such that

$$(\epsilon \otimes \iota)\Delta(a) = a = (\iota \otimes \epsilon)\Delta(a), \quad a \in \text{Pol}(\mathbb{G}),$$

$$m(S \otimes \iota)\Delta(a) = \epsilon(a)1_A = m(\iota \otimes S)\Delta(a), \quad a \in \text{Pol}(\mathbb{G}).$$

Here m denotes the multiplication map $m : \text{Pol}(\mathbb{G}) \otimes_{\text{alg}} \text{Pol}(\mathbb{G}) \rightarrow \text{Pol}(\mathbb{G})$, $a \otimes b \mapsto ab$. Indeed, the antipode and the counit are uniquely determined by

$$S(u_{ij}^\alpha) = (u_{ji}^\alpha)^*, \quad 1 \leq i, j \leq n_\alpha, \quad \alpha \in \text{Irr}(\mathbb{G}),$$

$$\epsilon(u_{ij}^\alpha) = \delta_{ij}, \quad 1 \leq i, j \leq n_\alpha, \quad \alpha \in \text{Irr}(\mathbb{G}).$$

Remark here that $* \circ S \circ * \circ S = \iota$. Also we have for all $a, b \in \text{Pol}(\mathbb{G})$ that

$$S((\iota \otimes h)(\Delta(b)(1 \otimes a))) = (\iota \otimes h)((1 \otimes b)\Delta(a)), \quad (2.1)$$

$$S((h \otimes \iota)((b \otimes 1)\Delta(a))) = (h \otimes \iota)(\Delta(b)(a \otimes 1)). \quad (2.2)$$

Now we add a remark on the C*-norms on $\text{Pol}(\mathbb{G})$. We are interested in the following two C*-norms on $\text{Pol}(\mathbb{G})$:

(1) the *universal norm*:

$$\|a\|_{\text{u}} := \sup\{\|\pi(a)\| : \pi : \text{Pol}(\mathbb{G}) \rightarrow B(H) \text{ is a unital } *- \text{homomorphism}\};$$

(2) the *reduced norm*:

$$\|a\|_{\text{r}} := \|\pi_h(a)\|,$$

where π_h is the GNS representation associated with the Haar state h .

We shall denote by $C_{\text{u}}(\mathbb{G})$ and $C_{\text{r}}(\mathbb{G})$ the completions of $\text{Pol}(\mathbb{G})$ with respect to $\|\cdot\|_{\text{u}}$ and $\|\cdot\|_{\text{r}}$, respectively. Then the comultiplication Δ and the Haar state h on $\text{Pol}(\mathbb{G})$ admit extensions to $C_{\text{u}}(\mathbb{G})$ (resp. $C_{\text{r}}(\mathbb{G})$), denoted by Δ_{u} and h_{u} (resp. Δ_{r} and h_{r}), respectively. Both $(C_{\text{u}}(\mathbb{G}), \Delta_{\text{u}})$ and $(C_{\text{r}}(\mathbb{G}), \Delta_{\text{r}})$ form compact quantum groups.

Note that the counit ϵ can be always extended to $C_{\text{u}}(\mathbb{G})$, since $\epsilon : \text{Pol}(\mathbb{G}) \rightarrow \mathbb{C}$ is a unital *-homomorphism. This is not always the case for $C_{\text{r}}(\mathbb{G})$. If ϵ can be also extended to $C_{\text{r}}(\mathbb{G})$, then \mathbb{G} is said to be *coamenable*. An equivalent definition is, \mathbb{G} is coamenable iff $\|\cdot\|_{\text{r}} = \|\cdot\|_{\text{u}}$. Note that $\|\cdot\|_{\text{r}} \leq \|\cdot\|_{\text{u}}$ always holds. We refer to [4] for more information. Throughout this thesis, we shall always consider compact quantum group \mathbb{G} on the universal level, so that the counit can always be extended to the $C(\mathbb{G})$.

The Peter-Weyl theory for compact groups can be extended to the quantum case. In particular, it is known that for each $\alpha \in \text{Irr}(\mathbb{G})$ there exists a positive invertible operator

$Q_\alpha \in B(H_\alpha)$ such that $\text{Tr}(Q_\alpha) = \text{Tr}(Q_\alpha^{-1}) := d_\alpha$, which we call the *quantum dimension* of α , and the orthogonality relations hold:

$$h\left(u_{ij}^\alpha (u_{kl}^\beta)^*\right) = \frac{\delta_{\alpha\beta} \delta_{ik} (Q_\alpha)_{lj}}{d_\alpha}, \quad h\left((u_{ij}^\alpha)^* u_{kl}^\beta\right) = \frac{\delta_{\alpha\beta} \delta_{jl} (Q_\alpha^{-1})_{ki}}{d_\alpha},$$

where $\alpha, \beta \in \text{Irr}(\mathbb{G})$, $1 \leq i, j \leq n_\alpha$, $1 \leq k, l \leq n_\beta$.

We call \mathbb{G} a *finite quantum group* if the underlying C^* -algebra $C(\mathbb{G})$ is finite-dimensional. Note that when \mathbb{G} is finite, we have $C(\mathbb{G}) = \text{Pol}(\mathbb{G})$ and then \mathbb{G} is coamenable. In this case each Q_α is the identity and h is a trace, i.e., $h(ab) = h(ba)$ for any $a, b \in C(\mathbb{G})$. Then the orthogonality relation becomes

$$h\left(u_{ij}^\alpha (u_{kl}^\beta)^*\right) = h\left((u_{ij}^\alpha)^* u_{kl}^\beta\right) = \frac{\delta_{\alpha\beta} \delta_{ik} \delta_{jl}}{n_\alpha}, \quad (2.3)$$

where $\alpha, \beta \in \text{Irr}(\mathbb{G})$, $1 \leq i, j \leq n_\alpha$, $1 \leq k, l \leq n_\beta$. Moreover, the antipode S satisfies $S^2 = \iota$. Together with $* \circ S \circ * \circ S = \iota$, one obtains directly that S is $*$ -preserving.

The Pontryagin duality can also be extended to compact quantum groups. We only explain it here for finite quantum groups. If $\mathbb{G} = (A, \Delta)$ is a finite quantum group, then we may construct its dual $\hat{\mathbb{G}} = (\hat{A}, \hat{\Delta})$ as follows. The underlying finite-dimensional C^* -algebra \hat{A} of $\hat{\mathbb{G}}$ is defined as A' , the set of all bounded linear functionals on A . For $\varphi_1, \varphi_2 \in \hat{A}$, their *convolution product* is defined as $\varphi_1 \star \varphi_2 := (\varphi_1 \otimes \varphi_2)\Delta$. We may define the involution on \hat{A} as: $\varphi^* := \overline{\varphi(S(\cdot)^*)}$. Then $(\hat{A}, \star, *)$ becomes a finite-dimensional C^* -algebra. For each $\varphi \in \hat{A}$, set $\hat{\Delta}(\varphi)(a \otimes b) := \varphi(ab)$, $a, b \in A$. Then $\hat{\Delta}(\varphi) \in (A \otimes A)' = A' \otimes A'$ and it is easily seen that $\hat{\Delta}$ defines a comultiplication on \hat{A} . Hence $\hat{\mathbb{G}} = (\hat{A}, \hat{\Delta})$ becomes a finite quantum group. Moreover, it is equipped with a Hopf * -algebra structure with the antipode \hat{S} and the counit $\hat{\epsilon}$ given by $\hat{S}(\varphi) := \varphi S$ and $\hat{\epsilon}(\varphi) := \varphi(1_A)$, respectively. Starting from the finite quantum group $\hat{\mathbb{G}} = (\hat{A}, \hat{\Delta})$, we may also construct its dual. Then in this way we recover the quantum group $\mathbb{G} = (A, \Delta)$.

The *Fourier transform* \mathcal{F} on a finite quantum group $\mathbb{G} = (A, \Delta)$ is a map from A to \hat{A} defined as $\mathcal{F}(a) = h(a \cdot) = h(\cdot a)$, where h is the Haar state on \mathbb{G} . We shall use \hat{a} to denote the its Fourier transform $\mathcal{F}(a)$ for simplicity. Then we have the following *Parseval's identity*:

$$\hat{h}(\hat{a}_1 \hat{a}_2^*) = c h(a_1 a_2^*), \quad a_1, a_2 \in A, \quad (2.4)$$

where \hat{h} is the Haar state on $\hat{\mathbb{G}}$ and $c > 0$ is a constant. If we consider the Fourier transform from \hat{A} to A , then we obtain a similar equation to (2.4).

2.2 Sekine quantum groups

Sekine [67] introduced a family of finite quantum groups, referred to as *Sekine quantum groups*. We follow the notations in [29] here.

Definition 2.2. Fix $k \geq 2$ an integer. Let η be a primitive k -th root of 1, say, $\eta = e^{\frac{2\pi i}{k}}$, and let $\mathbb{Z}_k := \{0, 1, \dots, k-1\}$ be the cyclic group with order k . Set

$$\mathcal{A}_k := \bigoplus_{i,j \in \mathbb{Z}_k} \mathbb{C} d_{i,j} \oplus \mathbb{M}_k(\mathbb{C}),$$

where $d_{i,j}$ is the corresponding unit vector of the copy \mathbb{C} . Denote by $\{e_{i,j} : i, j \in \mathbb{Z}_k\}$ the matrix units of $\mathbb{M}_k(\mathbb{C})$. The comultiplication on \mathcal{A}_k is defined through:

$$\Delta_k(d_{i,j}) := \sum_{m,n \in \mathbb{Z}_k} d_{m,n} \otimes d_{i-m,j-n} + \frac{1}{k} \sum_{m,n \in \mathbb{Z}_k} \eta^{i(m-n)} e_{m,n} \otimes e_{m+j,n+j}, \quad (2.5)$$

$$\Delta_k(e_{i,j}) := \sum_{m,n \in \mathbb{Z}_k} \eta^{m(i-j)} d_{-m,-n} \otimes e_{i-n,j-n} + \sum_{m,n \in \mathbb{Z}_k} \eta^{m(j-i)} e_{i-n,j-n} \otimes d_{m,n}, \quad (2.6)$$

for $i, j \in \mathbb{Z}_k$. Then the pair $(\mathcal{A}_k, \Delta_k)$ forms a finite quantum group, called a Sekine quantum group.

2.2.1 Representations of Sekine quantum groups

We refer to [53] for more discussions on the representation theory of Sekine quantum groups. Let $p, q \in \mathbb{Z}_k$. Then from (2.5) it follows that

$$\begin{aligned} \sum_{i,j \in \mathbb{Z}_k} \eta^{ip+jq} \Delta_k(d_{i,j}) &= \sum_{m,n \in \mathbb{Z}_k} \eta^{mp+nq} d_{m,n} \otimes \sum_{i,j \in \mathbb{Z}_k} \eta^{ip+jq} d_{i,j} \\ &\quad + \sum_{m \in \mathbb{Z}_k} \eta^{-mq} e_{m,m+p} \otimes \sum_{j \in \mathbb{Z}_k} \eta^{jq} e_{j,j+p}, \end{aligned}$$

and from (2.6) it follows that

$$\begin{aligned} \sum_{i \in \mathbb{Z}_k} \eta^{iq} \Delta_k(e_{i,i+p}) &= \sum_{m,n \in \mathbb{Z}_k} \eta^{mp-nq} d_{m,n} \otimes \sum_{i \in \mathbb{Z}_k} \eta^{iq} e_{i,i+p} \\ &\quad + \sum_{i \in \mathbb{Z}_k} \eta^{iq} e_{i,i+p} \otimes \sum_{m,n \in \mathbb{Z}_k} \eta^{mp+nq} d_{m,n}. \end{aligned}$$

Set $\rho_{p,q} := \sum_{m,n \in \mathbb{Z}_k} \eta^{mp+nq} d_{m,n}$ and $\sigma_{p,q} := \sum_{i \in \mathbb{Z}_k} \eta^{iq} e_{i,i+p}$ for all $p, q \in \mathbb{Z}_k$. Then the equations above can be rephrased as

$$\Delta_k(\rho_{p,q}) = \rho_{p,q} \otimes \rho_{p,q} + \sigma_{p,-q} \otimes \sigma_{p,q},$$

$$\Delta_k(\sigma_{p,q}) = \rho_{p,-q} \otimes \sigma_{p,q} + \sigma_{p,-q} \otimes \rho_{p,q},$$

for all $p, q \in \mathbb{Z}_k$. This yields directly that for any $p, q \in \mathbb{Z}_k$,

$$\pi_{p,q} := \begin{pmatrix} \rho_{p,q} & \sigma_{p,-q} \\ \sigma_{p,q} & \rho_{p,-q} \end{pmatrix}$$

is a representation of $(\mathcal{A}_k, \Delta_k)$. Moreover, it is also unitary. To see this, note by definitions of $\rho_{p,q}$ and $\sigma_{r,s}$ that

$$\rho_{p,q}^* = \rho_{-p,-q}, \quad \sigma_{r,s}^* = \eta^{rs} \sigma_{-r,-s},$$

$$\rho_{p,q} \rho_{p',q'} = \rho_{p+p',q+q'}, \quad \rho_{p,q} \sigma_{r,s} = \sigma_{r,s} \rho_{p,q} = 0, \quad \sigma_{r,s} \sigma_{r',s'} = \eta^{rs'} \sigma_{r+r',s+s'},$$

where $p, q, p', q', r, s, r', s' \in \mathbb{Z}_k$. Then

$$\pi_{p,q}^* \pi_{p,q} = \begin{pmatrix} \rho_{-p,-q} & \eta^{pq} \sigma_{-p,-q} \\ \eta^{-pq} \sigma_{-p,q} & \rho_{-p,q} \end{pmatrix} \begin{pmatrix} \rho_{p,q} & \sigma_{p,-q} \\ \sigma_{p,q} & \rho_{p,-q} \end{pmatrix} = \begin{pmatrix} \rho_{0,0} + \sigma_{0,0} & 0 \\ 0 & \rho_{0,0} + \sigma_{0,0} \end{pmatrix},$$

while $\rho_{0,0} + \sigma_{0,0} = \sum_{p,q \in \mathbb{Z}_k} d_{p,q} + \sum_{r \in \mathbb{Z}_k} e_{r,r} = 1_{\mathcal{A}_k}$ is the unit element. So $\pi_{p,q}^* \pi_{p,q} = \text{id}$. Similarly, we have $\pi_{p,q} \pi_{p,q}^* = \text{id}$.

When $q = 0$, $\pi_{p,q}$ is unitarily equivalent to

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \rho_{p,0} & \sigma_{p,0} \\ \sigma_{p,0} & \rho_{p,0} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \rho_{p,0} + \sigma_{p,0} & 0 \\ 0 & \rho_{p,0} - \sigma_{p,0} \end{pmatrix}.$$

For the same reason, if k is even, $\pi_{p,k/2}$ is unitarily equivalent to

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \rho_{p,k/2} & \sigma_{p,k/2} \\ \sigma_{p,k/2} & \rho_{p,k/2} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \rho_{p,k/2} + \sigma_{p,k/2} & 0 \\ 0 & \rho_{p,k/2} - \sigma_{p,k/2} \end{pmatrix}.$$

In such cases $\pi_{p,q}$ can be decomposed into, up to equivalence, two one-dimensional unitary irreducible representations. So we have obtained $2k$ one-dimensional representations when k is odd and $4k$ one-dimensional representations when k is even.

Moreover, $\pi_{p,q}$ is unitarily equivalent to $\pi_{p,-q}$ since

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \rho_{p,q} & \sigma_{p,-q} \\ \sigma_{p,q} & \rho_{p,-q} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \rho_{p,-q} & \sigma_{p,q} \\ \sigma_{p,-q} & \rho_{p,q} \end{pmatrix}.$$

It is known [53] that $\{\pi_{p,q} : 1 \leq q \leq [\frac{k-1}{2}]k\}$ are pairwise inequivalent two-dimensional irreducible representations. Note that although this was pointed out only for k odd in [53], it also holds for k even, following a similar argument.

Hence, up to equivalence, $(\mathcal{A}_k, \Delta_k)$ has $2k$ one-dimensional unitary irreducible representations and $\frac{k(k-1)}{2}$ two-dimensional irreducible representations when k is odd, $4k$ one dimensional unitary irreducible representations and $\frac{k(k-2)}{2}$ two-dimensional irreducible representations when k is even. These are the only irreducible representations. Indeed, one can check this by verifying the dimension.

We end this section by introducing the *Fourier transform* of linear functionals μ on \mathcal{A}_k , denoted by $\hat{\mu}$, at $\pi_{p,q}$:

$$\hat{\mu}(\pi_{p,q}) = \begin{pmatrix} \mu(\rho_{p,q}) & \mu(\sigma_{p,-q}) \\ \mu(\sigma_{p,q}) & \mu(\rho_{p,-q}) \end{pmatrix}, \quad p, q \in \mathbb{Z}_k.$$

It is easy to see that for any functionals μ, ν on \mathcal{A}_k

$$\widehat{\mu \star \nu}(\pi_{p,q}) = \hat{\mu}(\pi_{p,q}) \hat{\nu}(\pi_{p,q}), \quad p, q \in \mathbb{Z}_k, \quad (2.7)$$

where $\mu \star \nu := (\mu \otimes \nu)\Delta$ denotes the convolution of μ and ν .

2.3 Idempotent states on Sekine quantum groups

For a compact quantum group $\mathbb{G} = (A, \Delta)$, denote by A' the set of all bounded linear functionals on A . Then for $\mu, \nu \in A'$ we can define the *convolution* of μ and ν , which we have seen earlier, as a linear functional on A given by the formula

$$\mu \star \nu := (\mu \otimes \nu)\Delta.$$

A state μ on A is called an *idempotent state* if $\mu \star \mu = \mu$. Denote the class of all idempotent states on $\mathbb{G} = (A, \Delta)$ by $\text{Idem}(\mathbb{G})$, or $\text{Idem}(A)$. Idempotent states on compact quantum groups have been characterized in different ways [29, 28].

Example 2.3 (Commutative case). If A is commutative, then \mathbb{G} is isomorphic to $(C(G), \Delta)$, where $C(G)$ denotes the set of continuous functions on a compact group G and Δ is a comultiplication on $C(G)$ given by

$$\Delta(f)(s, t) = f(st), \quad s, t \in G.$$

In this case idempotent state on $C(G)$ arises as idempotent probability measure on G , which, by Kawada and Itô's classical theorem, arises as the Haar measure on a compact subgroup of G .

Let us recall the notion of a quantum subgroup here.

Definition 2.4. If $(A, \Delta_A), (B, \Delta_B)$ are compact quantum groups and $\pi_B : A \rightarrow B$ is a surjective unital $*$ -homomorphism such that $\Delta_B \circ \pi_B = (\pi_B \otimes \pi_B) \circ \Delta_A$, then (B, Δ_B) is called a quantum subgroup of (A, Δ_A) .

Let h_B be the Haar state on B , then $h_B \circ \pi_B$ is an idempotent state on A . If an idempotent state ϕ on A arises in this way, say, $\phi = h_B \circ \pi_B$ for some quantum subgroup (B, Δ_B) with Haar measure h_B of A , then it is called a *Haar idempotent state*. Otherwise, it is called a *non-Haar idempotent state*. So Kawada and Itô's theorem tells us that in the commutative case, all idempotent states are Haar idempotent states.

The existence of non-Haar idempotent state was first proved by Pal [59] on a 8-dimensional Kac-Paljutkin quantum group. Even simpler examples come from co-commutative finite quantum groups [29].

Example 2.5 (Co-commutative case). A finite quantum group $\mathbb{G} = (A, \Delta)$ is said to be *co-commutative* if $\Pi\Delta = \Delta$, where Π denotes the usual tensor flip on $A \otimes A$. Then A is isomorphic to the group algebra $C^*(\Gamma)$ with Γ a finite discrete group. Then there is a one-one correspondence between idempotent states on A and subgroups of Γ . Moreover, there is a one-one correspondence between Haar idempotent states on A and normal subgroups of Γ . So from a non-normal subgroup of Γ one can construct a non-Haar idempotent.

More examples can be found on Sekine quantum groups [29]. Indeed, a small class of non-Haar idempotent states on Sekine quantum groups \mathcal{A}_k was given in [29, Proposition 6.6]. See (2.11) (2.12) below for details.

Now we consider all the idempotent states on \mathcal{A}_k . Fix $k \geq 2$. On \mathcal{A}'_k there is a natural basis:

$$\tilde{d}_{i,j}(d_{m,n}) := \delta_m^i \delta_n^j, \quad \tilde{d}_{i,j}(e_{r,s}) := 0, \quad \tilde{e}_{i,j}(d_{m,n}) := 0, \quad \tilde{e}_{i,j}(e_{r,s}) := \delta_r^i \delta_s^j,$$

where $i, j, m, n, r, s \in \mathbb{Z}_k$. Using this basis, the explicit formula for the convolution of two linear functionals on \mathcal{A}_k is given through the following lemma (see the discussion before [29, Lemma 6.4]).

Lemma 2.6. For $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s}$, $\nu = \sum_{i,j \in \mathbb{Z}_k} \beta_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \omega_{r,s} \tilde{e}_{r,s} \in \mathcal{A}'_k$, we have

$$\mu \star \nu = \sum_{i,j \in \mathbb{Z}_k} \gamma_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \theta_{r,s} \tilde{e}_{r,s},$$

with

$$\begin{aligned} \gamma_{i,j} &= \sum_{m,n \in \mathbb{Z}_k} \alpha_{m,n} \beta_{i-m, j-n} + \frac{1}{k} \sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \omega_{r+j, s+j}, \quad i, j \in \mathbb{Z}_k, \\ \theta_{r,s} &= \sum_{i,j \in \mathbb{Z}_k} \eta^{i(s-r)} (\alpha_{i,j} \omega_{r+j, s+j} + \beta_{i,j} \kappa_{r-j, s-j}), \quad r, s \in \mathbb{Z}_k. \end{aligned}$$

This gives a characterization of $\text{Idem}(\mathcal{A}_k)$:

Lemma 2.7 ([67, 29]). *A functional $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s} \in \mathcal{A}'_k$ is an idempotent state if and only if $\alpha_{i,j} \geq 0$ for all $i, j \in \mathbb{Z}_k$, $K := [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k}$ is positive semi-definite, and the following equations hold:*

$$\alpha_{i,j} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r,j-s} \alpha_{r,s} + \frac{1}{k} \sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j,s+j}, \quad i, j \in \mathbb{Z}_k, \quad (2.8)$$

$$\kappa_{r,s} = \sum_{i,j \in \mathbb{Z}_k} \eta^{i(s-r)} \alpha_{i,j} (\kappa_{r+j,s+j} + \kappa_{r-j,s-j}), \quad r, s \in \mathbb{Z}_k, \quad (2.9)$$

$$\mu(1_{\mathcal{A}_k}) = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} + \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 1. \quad (2.10)$$

Certainly the Haar state on \mathcal{A}_k

$$h_{\mathcal{A}_k} := \frac{1}{2k^2} \sum_{i,j \in \mathbb{Z}_k} \tilde{d}_{i,j} + \frac{1}{2k} \sum_{r \in \mathbb{Z}_k} \tilde{e}_{r,r},$$

is a Haar idempotent. Franz and Skalski have determined all the Haar idempotents [29, Theorem 6.5] on \mathcal{A}_k . See also Proposition 2.8 below. They have also given some examples of non-Haar idempotents [29, Proposition 6.6]:

$$\phi_l = \frac{1}{2k} \sum_{i \in \mathbb{Z}_k} \tilde{d}_{i,0} + \frac{1}{2} \tilde{e}_{l,l}, \quad l \in \mathbb{Z}_k. \quad (2.11)$$

There are certainly other non-Haar idempotents for special k 's, as pointed out at the end of [29] with the following examples:

$$\frac{1}{4km} \sum_{i \in \mathbb{Z}_k} \sum_{l=0}^{m-1} \tilde{d}_{i,lp} + \frac{1}{2m} \sum_{l=0}^{m-1} \tilde{e}_{lp,lp}, \quad (2.12)$$

whenever $k = pm$ and $p, m \in \mathbb{N}$ such that $p, m \geq 2$.

With the help of some elementary number theoretic considerations, we solve the equations (2.8) (2.9) (2.10) in Lemma 2.7. We will see in the following that the set of idempotent states, other than the Haar state, can be divided into three disjoint classes, denoted by $\mathcal{I}_1(\mathcal{A}_k)$, $\mathcal{I}_2(\mathcal{A}_k)$ and $\mathcal{I}_3(\mathcal{A}_k)$. $\mathcal{I}_1(\mathcal{A}_k)$ consists of all Haar idempotents except the Haar state. $\mathcal{I}_2(\mathcal{A}_k)$ are non-Haar idempotents such that the corresponding matrix $K = [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k}$ is diagonal, which include both (2.11) and (2.12) as subclasses. The third class $\mathcal{I}_3(\mathcal{A}_k)$, which are non-Haar idempotent states with K not diagonal, is an unexpected new discovery.

Note first that if $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s}$ is an idempotent state, then from (2.9) it follows that

$$\sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 2 \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \cdot \sum_{r \in \mathbb{Z}_k} \kappa_{r,r}. \quad (2.13)$$

Together with (2.10), we have either

$$\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = 1, \quad \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 0, \quad (2.14)$$

or

$$\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = \frac{1}{2}. \quad (2.15)$$

The following proposition characterizes all the idempotents verifying (2.14). By [29, Theorem 6.5], such idempotent states, together with the Haar state $h_{\mathcal{A}_k}$, form the family of Haar idempotents.

Proposition 2.8. *Let $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s} \in \mathcal{A}'_k$. Then it is an idempotent state verifying $\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = 1$ and $\sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 0$ if and only if*

$$(1) \quad \kappa_{r,s} = 0 \text{ for all } r, s \in \mathbb{Z}_k;$$

$$(2) \quad \Gamma := \{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \alpha_{i,j} \neq 0\} \text{ is a subgroup of } \mathbb{Z}_k \times \mathbb{Z}_k \text{ and } \alpha_{i,j} = \frac{1}{\#\Gamma}, (i, j) \in \Gamma.$$

Moreover, in this case, such an idempotent state is Haar idempotent. Conversely, any Haar idempotent is either equal to the Haar state $h_{\mathcal{A}_k}$ or of this form:

$$h_\Gamma := \frac{1}{\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j},$$

with Γ a subgroup of $\mathbb{Z}_k \times \mathbb{Z}_k$.

Proof. Since $K = [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k} \geq 0$ and $\text{Tr}(K) = \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 0$, we have $\kappa_{r,s} = 0$ for all $r, s \in \mathbb{Z}_k$. Then (2.9) is trivial and (2.8) becomes

$$\alpha_{i,j} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r, j-s} \alpha_{r,s}, \quad i, j \in \mathbb{Z}_k. \quad (2.16)$$

From $\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = 1$ it follows that $\alpha_{i',j'} \neq 0$ for some $(i', j') \in \mathbb{Z}_k \times \mathbb{Z}_k$. So $\Gamma \neq \emptyset$. From (2.16) and the non-negativity of $\alpha_{i,j}$ we have that $(i_1, j_1) \in \Gamma$ and $(i_2, j_2) \in \Gamma$ imply $(i_1 + i_2, j_1 + j_2) \in \Gamma$. Thus Γ is closed under group operation. Moreover, $(0, 0) = (ki', kj') \in \Gamma$, i.e., Γ contains the unit. Set $M := \max_{i,j \in \mathbb{Z}_k} \alpha_{i,j}$ and suppose that it is attained by α_{i_0, j_0} with $(i_0, j_0) \in \mathbb{Z}_k \times \mathbb{Z}_k$. Clearly $M > 0$. From

$$M = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i_0-r, j_0-s} \alpha_{r,s} \leq M \sum_{r,s \in \mathbb{Z}_k} \alpha_{r,s} = M,$$

it follows that $\alpha_{i_0-r, j_0-s} = M$ as long as $\alpha_{r,s} \neq 0$. So $\#\Gamma \leq \#\{(i, j) : \alpha_{i,j} = M\} \leq \#\Gamma$, that is to say, $\alpha_{i,j} = \frac{1}{\#\Gamma}$ for any $(i, j) \in \Gamma$. Now set (i_0, j_0) equal $(0, 0)$, we have $\alpha_{-r, -s} = M$ as long as $\alpha_{r,s} \neq 0$, i.e., $(-r, -s) \in \Gamma$ if $(r, s) \in \Gamma$. So any $(r, s) \in \Gamma$ has its inverse $(-r, -s)$ in Γ . Hence Γ is a subgroup of $\mathbb{Z}_k \times \mathbb{Z}_k$.

The remaining is a direct consequence of [29, Theorem 6.5]. \square

Remark 2.9. *Let μ be as above. If $\mu = h_\Gamma$, we have*

$$\hat{\mu}(\pi_{i,j}) \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}, \quad i, j \in \mathbb{Z}_k.$$

The following theorem contains the main result of this paper, characterizing the set of idempotent states verifying (2.15), which consists of the Haar state $h_{\mathcal{A}_k}$ and all the non-Haar idempotents.

Before this we need the following well-known *Bézout's identity*:

Lemma 2.10 (Bézout's identity). *For any integers $a, b \geq 1$, there exist integers m, n such that $ma + nb = \text{gcd}(a, b)$, where $\text{gcd}(a, b)$ denotes the greatest common divisor of a and b .*

Note that we can choose $m > 0, n < 0$ or $m < 0, n > 0$ freely. Indeed, we can replace the pair (m, n) with $(m + lb, n - la)$ for any $l \in \mathbb{Z}$.

Theorem 2.11. *Let $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s} \in \mathcal{A}'_k$. Then it is an idempotent state verifying $\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = \frac{1}{2}$ if and only if μ is either:*

(1) the Haar state $h_{\mathcal{A}_k} := \frac{1}{2k^2} \sum_{i,j \in \mathbb{Z}_k} \tilde{d}_{i,j} + \frac{1}{2k} \sum_{r \in \mathbb{Z}_k} \tilde{e}_{r,r}$; or

(2)

$$h_{\Gamma,l} := \frac{1}{2\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j} + \frac{q}{2k} \sum_{r \equiv l \pmod{q}} \tilde{e}_{r,r},$$

where $\Gamma = \mathbb{Z}_k \times q\mathbb{Z}_k$ with $q|k$, $q > 1$, and $l \in \mathbb{Z}_q$; or

(3)

$$h_{\Gamma,l,\tau} := \frac{1}{2\#\Gamma} \sum_{(i,j) \in \Gamma} \tilde{d}_{i,j} + \frac{q}{2k} \sum_{r,s \equiv l \pmod{q}} \tau_{s-r} \tilde{e}_{r,s},$$

where $\Gamma = p\mathbb{Z}_k \times q\mathbb{Z}_k$ with $p > 1$ and $pq = k$, $l \in \mathbb{Z}_q$, and $\tau = (\tau_j)_{j \in q\mathbb{Z}_k} \in \{\pm 1\}^{q\mathbb{Z}_k}$ such that

$$\sum_{j \in q\mathbb{Z}_k} \tau_j \eta^{ij} \geq 0, \quad i \in \mathbb{Z}_{k/q}. \quad (2.17)$$

Remark 2.12. The condition (2.17) is equivalent to positive semi-definiteness of $[\kappa_{r,s}]_{r,s \in \mathbb{Z}_k}$. Such τ always exists as one can choose $\tau_j = 1$ for all j , which is kind of trivial. It is not difficult to construct non-trivial ones. For example, when $k = 2$, there is another τ' with $\tau'_0 = 1$ and $\tau'_1 = -1$ which satisfies (2.17).

Proof of Theorem 2.11. Observe first that for any $j \in \mathbb{Z}_k$, $K = [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k} \geq 0$ implies $[\kappa_{r+j,s+j}]_{r,s \in \mathbb{Z}_k} \geq 0$, thus their Hadamard product $[\kappa_{r,s} \kappa_{r+j,s+j}]_{r,s \in \mathbb{Z}_k} \geq 0$. So we have for any $i, j \in \mathbb{Z}_k$

$$\sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j,s+j} = \sum_{r,s \in \mathbb{Z}_k} \eta^{ir} \overline{\eta^{is}} \kappa_{r,s} \kappa_{r+j,s+j} \geq 0. \quad (2.18)$$

Recall that $\Gamma = \{(i,j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \alpha_{i,j} \neq 0\}$. Since $\sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = \frac{1}{2}$, there exists $(i',j') \in \mathbb{Z}_k \times \mathbb{Z}_k$ such that $\alpha_{i',j'} \neq 0$. This allows us to define

$$p := \min\{i > 0 : (i,j) \in \Gamma \text{ for some } j \in \mathbb{Z}_k\},$$

$$q := \min\{j > 0 : (i,j) \in \Gamma \text{ for some } i \in \mathbb{Z}_k\}.$$

Claim 1: We have $p|k, q|k$, and for any $(i,j) \in \mathbb{Z}_k \times \mathbb{Z}_k$

$$\alpha_{i,j} \neq 0 \Rightarrow p|i \text{ and } q|j. \quad (2.19)$$

To show this, recall that $\alpha_{i,j} \geq 0$, so $\alpha_{i,j} \neq 0$ simply means $\alpha_{i,j} > 0$. From (2.8) and the previous observation (2.18), it follows that

$$(i_1, j_1), (i_2, j_2) \in \Gamma \Rightarrow (m_1 i_1 + m_2 i_2, m_1 j_1 + m_2 j_2) \in \Gamma, \quad m_1, m_2 \in \mathbb{Z}_{\geq 0}, \quad (2.20)$$

and

$$(i_1, j_1) \notin \Gamma, (i_2, j_2) \in \Gamma \Rightarrow (i_1 - m i_2, j_1 - m j_2) \notin \Gamma, \quad m \in \mathbb{Z}_{\geq 1}, \quad (2.21)$$

From Lemma 2.10, there exist integers $m, n > 0$ such that $mp - nk = \gcd(p, k) \leq p$. Suppose that $(p, j_p) \in \Gamma$ for some $j_p > 0$, then (2.20) and Lemma 2.10 yield

$$(mp, m j_p) = (mp - nk, m j_p) = (\gcd(p, k), m j_p) \in \Gamma.$$

From the definition of p we have $\gcd(p, k) = p$, i.e., $p|k$.

For any $\alpha_{i,j} \neq 0$, i.e., $(i,j) \in \Gamma$, there exist, by applying Lemma 2.10 two times, integers $m, n, l > 0$ such that $0 < mp + ni - lk = \gcd(p, i, k) \leq p$. Thus (2.20) and Lemma 2.10 yield

$$(mp + ni, mj_p + nj) = (mp + ni - lk, mj_p + nj) = (\gcd(p, i, k), mj_p + nj) \in \Gamma.$$

So $\gcd(p, i, k) = p$, i.e., $p|i$, which finishes the proof of **Claim 1** for p . The proof for q is similar.

Claim 2: Fix $t \in \mathbb{Z}_k$. Suppose that $|\kappa_{r_0, s_0}| = \max\{|\kappa_{r,s}| : (r,s) \in \mathbb{Z}_k \times \mathbb{Z}_k, r-s = t\}$. Then for any $(i,j) \in \Gamma$, we have

$$\kappa_{r_0, s_0} = \eta^{-it} \kappa_{r_0+j, s_0+j} = \eta^{-it} \kappa_{r_0-j, s_0-j}. \quad (2.22)$$

Moreover, $\eta^{2pt} = 1$.

In fact, from (2.9) it follows that

$$|\kappa_{r_0, s_0}| \leq \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} |\eta^{-it} (\kappa_{r_0+j, s_0+j} + \kappa_{r_0-j, s_0-j})| \leq 2 |\kappa_{r_0, s_0}| \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = |\kappa_{r_0, s_0}|.$$

Thus $\alpha_{i,j} \neq 0$ implies (2.22). Consequently, we have $|\kappa_{r_0+j, s_0+j}| = |\kappa_{r_0-j, s_0-j}| = |\kappa_{r_0, s_0}|$. Repeating this argument for κ_{r_0+j, s_0+j} and κ_{r_0-j, s_0-j} , we have finally

$$|\kappa_{r,s}| = |\kappa_{r_0, s_0}| \text{ for any } r, s \text{ such that } j|r - r_0 = s - s_0, \quad (2.23)$$

whenever $\alpha_{i,j} \neq 0$ for some i . Moreover, (2.22) implies $\kappa_{r_0, s_0} = \eta^{-it} \kappa_{r_0+j, s_0+j} = \eta^{-2it} \kappa_{r_0, s_0}$, so we have $\kappa_{r_0, s_0} \neq 0$ only if $\eta^{2it} = 1$, which, by the definition of p , yields $\eta^{2pt} = 1$. So **Claim 2** is proved.

Recall that $\kappa_{r,r} \geq 0$ for all $r \in \mathbb{Z}_k$, since $K \geq 0$. From $\sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = \frac{1}{2}$, we have $\kappa_{l,l} = \max_{r \in \mathbb{Z}_k} \kappa_{r,r} > 0$ for some l . Suppose $\alpha_{i,q} \neq 0$, then (2.23) implies

$$\kappa_{r,r} = \kappa_{l,l} > 0, \quad r \equiv l \pmod{q}. \quad (2.24)$$

For convenience, let $0 \leq l < q$. From (2.8) and (2.19), we have for any $i \in \mathbb{Z}_k$ and any $q \nmid j$

$$\sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j, s+j} = 0.$$

So for any $q \nmid j$

$$\begin{aligned} 0 &= \sum_{i \in \mathbb{Z}_k} \sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j, s+j} \\ &= \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \kappa_{r+j, s+j} \sum_{i \in \mathbb{Z}_k} \eta^{i(r-s)} \\ &= k \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} \kappa_{r+j, r+j}. \end{aligned}$$

Thus $\kappa_{r,r} \kappa_{r+j, r+j} = 0$ whenever $r \in \mathbb{Z}_k$ and $q \nmid j$. Combining this with (2.24) we obtain

$$\kappa_{r,r} = \begin{cases} \frac{q}{2k} & r \equiv l \pmod{q} \\ 0 & \text{otherwise} \end{cases}. \quad (2.25)$$

From this and the positive semi-definitiveness of K we have

$$\kappa_{r,s} = 0, \text{ if either } q \nmid r - l \text{ or } q \nmid s - l. \quad (2.26)$$

So it remains to compute the submatrix $[\kappa_{r,s}]_{r,s \equiv l \pmod q}$. For this set

$$p' := \min\{i > 0 : (i, 0) \in \Gamma\},$$

$$q' := \min\{j > 0 : (0, j) \in \Gamma\}.$$

These are well-defined, since $(k, 0) = (0, k) = (0, 0) \in \Gamma$. Indeed, suppose $(i', j') \in \Gamma$, then from (2.20) it follows $(0, 0) = (ki', kj') \in \Gamma$.

We have also by (2.20) that

$$p'|i \text{ and } q'|j \Rightarrow (i, j) \in \Gamma. \quad (2.27)$$

So from (2.19) it follows that $p|p'$ and $q|q'$.

Claim 3: $p = p'$ and $q = q'$. As a consequence, we have

$$(i, j) \in \Gamma \text{ if and only if } p|i \text{ and } q|j. \quad (2.28)$$

To prove this, note first that for any $p|i$, there exists $j \in \mathbb{Z}_k$ such that $(i, j) \in \Gamma$. Otherwise, $(i, j) \notin \Gamma$ for all $j \in \mathbb{Z}_k$. Since $(p, j_p) \notin \Gamma$ for some $j_p \in \mathbb{Z}_k$, we have by (2.21) that $(i - p, j) \notin \Gamma$ for all $j \in \mathbb{Z}_k$. This argument gives finally $(0, j) \notin \Gamma$ for all $j \in \mathbb{Z}_k$, which contradicts the fact that $(0, 0) \in \Gamma$. Similarly, for any $q|j$, there exists $i \in \mathbb{Z}_k$ such that $(i, j) \in \Gamma$. This allows us to define for all $p|i$ and $q|j$ that

$$p_j := \min\{i > 0 : (i, j) \in \Gamma\},$$

$$q_i := \min\{j > 0 : (i, j) \in \Gamma\}.$$

Then (2.19) implies $p|p_j$ and $q|q_i$ for all such i, j . Following a similar argument to that showing (2.19), we have by (2.20) and Lemma 2.10 that $p_j|p'$ and $q_i|q'$. Moreover, note that

$$(0, j) \in \Gamma \text{ iff } q'|j, \text{ and } (i, 0) \in \Gamma \text{ iff } p'|i,$$

which is a consequence of definitions of p', q' and (2.20) together with Bézout's identity. Then (2.20) tells us that for any $p|i$

$$(i, q_i + mq') \in \Gamma, \quad m \geq 0; \quad (2.29)$$

and (2.21) tells us that for any $p|i$

$$(i, j - mq_i) = (0 - (-i), j - mq_i) \notin \Gamma, \quad q' \nmid j, m \geq 0. \quad (2.30)$$

So we have for any $p|i$,

$$(i, j) \in \Gamma \text{ iff } j \equiv q_i \pmod{q'}.$$

Now we are ready to prove **Claim 3**. Suppose $q \neq q'$, then for any $p|i$, we have $(i, j(i)) \notin \Gamma$ for some $q|j(i)$ (for example, take $j(i) = q_i + q$). So $\alpha_{i, j(i)} = 0$, and thus from the non-negativity of $\alpha_{m, n}$ and (2.18) we have

$$\sum_{r, s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r, s} \kappa_{r+j(i), s+j(i)} = 0.$$

By (2.26), it becomes

$$\sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j(i),s+j(i)} = \sum_{r,s \equiv l \pmod q} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j(i),s+j(i)} = 0.$$

Fix $p|i$ and the associated $j(i)$, then we have for any $q|t$

$$\kappa_{r,s} \kappa_{r+j(i),s+j(i)} = d_i \kappa_{t+l,l}^2, \text{ for all } r,s \equiv l \pmod q \text{ and } r-s=t, \quad (2.31)$$

where $d_i \in \{\pm 1\}$ is independent of r,s . In fact, this is trivial when $\max_{r,s:r-s=t} |\kappa_{r,s}| = 0$. Set $d_i \equiv 1$ for example. If $\max_{r,s:r-s=t} |\kappa_{r,s}| > 0$, recall that we have for such r,s

$$\kappa_{r,s} = \eta^{p_q(s-r)} \kappa_{r-q,s-q} = \eta^{-p_q t} \kappa_{r-q,s-q} \text{ and } \eta^{2p_q(r-s)} = \eta^{2p_q t} = 1.$$

Clearly, $\eta^{p_q t} = \pm 1$. So (2.31) is also trivial if $\eta^{p_q t} = 1$: we can choose $d_i = 1$. If $\eta^{p_q t} = -1$, then for $r,s \equiv l \pmod q$

$$\kappa_{r,s} \kappa_{r+j(i),s+j(i)} = (-1)^{j(i)/q} \kappa_{r-s+l,l}^2,$$

and we can choose $d_i = (-1)^{j(i)/q}$. Thus (2.31) holds.

Now we have for any $p|i$

$$\begin{aligned} 0 &= \sum_{r,s \equiv l \pmod q} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j(i),s+j(i)} \\ &= \sum_{r,s=tq+l, t \in \mathbb{Z}_{k/q}} \eta^{i(r-s)} d_i \kappa_{r-s+l,l}^2 \\ &= \frac{k}{q} \sum_{t \in \mathbb{Z}_{k/q}} \eta^{itq} d_i \kappa_{tq+l,l}^2. \end{aligned}$$

This clearly holds for any $p \nmid i$ and any d_i because of (2.19) and (2.26). Set $d_i := 1$ for all $p \nmid i$. Thus we have for each $i \in \mathbb{Z}_k$

$$\sum_{t \in \mathbb{Z}_{k/q}} d_i (\eta^q)^{it} \kappa_{tq+l,l}^2 = 0.$$

Then the system of linear equations

$$\sum_{t \in \mathbb{Z}_{k/q}} d_i (\eta^q)^{it} \kappa_{tq+l,l}^2 = 0, \quad i = 0, 1, \dots, \frac{k}{q} - 1.$$

can be represented as

$$DVX = 0, \quad (2.32)$$

where $D = \text{diag}(d_0, d_1, \dots, d_{\frac{k}{q}-1})$ is an invertible $\frac{k}{q} \times \frac{k}{q}$ diagonal matrix, $V = V(1, \eta^q, \dots, \eta^{k-q})$ is an $\frac{k}{q} \times \frac{k}{q}$ Vandermonde matrix, and $X = (\kappa_{l,l}^2, \kappa_{q+l,l}^2, \dots, \kappa_{k-q+l,l}^2)^T$ is a $\frac{k}{q}$ -dimensional vector. Here $V(a_1, a_2, \dots, a_n)$ denotes the $n \times n$ Vandermonde matrix $[a_i^{j-1}]_{i,j=1}^n$. By the definition of η , V is invertible. So we have $X = 0$. But $\kappa_{l,l}^2 = \frac{q^2}{4k^2} \neq 0$, which leads to a contradiction! Hence $q = q'$.

Now $p = p'$ follows directly. Indeed, $q = q'$ implies $q_p = q$, so we have $(p, q) = (p, q_p) \in \Gamma$. Thus $(p, 0) = (p, q) + (0, -q) \in \Gamma$. Hence $p = p'$, which ends the proof of **Claim 3**.

Claim 4: We have either $p = 1$ or $p \geq 2$ and $pq = k$.

We will use a similar argument as above. Before this, let us update several conclusions, following **Claim 3**. Note first that $\kappa_{r,s} = \kappa_{r-s+l,l}$ for all $r, s \equiv l \pmod{q}$, since $(0, q) \in \Gamma$. Moreover, $\kappa_{r,s} \neq 0$ only if $\eta^{p(r-s)} = 1$.

If $p > 1$, we have for any $p \nmid i$:

$$\begin{aligned} 0 &= \sum_{r,s \in \mathbb{Z}_k} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j,s+j} \\ &= \sum_{r,s \equiv l \pmod{q}} \eta^{i(r-s)} \kappa_{r,s} \kappa_{r+j,s+j} \\ &= \sum_{r,s=tq+l, t \in \mathbb{Z}_{k/q}} \eta^{i(r-s)} \kappa_{r-s+l,l}^2 \\ &= \frac{k}{q} \sum_{t \in \mathbb{Z}_{k/q}} \eta^{itq} \kappa_{tq+l,l}^2. \end{aligned}$$

So we have the following system of linear equations:

$$\sum_{t \in \mathbb{Z}_{k/q}} (\eta^q)^{it} \kappa_{tq+l,l}^2 = 0, \quad i \in \{0, 1, 2, \dots, \frac{k}{q} - 1\} \setminus p\mathbb{Z}_k,$$

which can be represented as

$$V'X' = 0,$$

where V' is a $m \times \frac{k}{q}$ submatrix of V , the Vandermonde matrix introduced earlier, with $m = \frac{k}{q} - [\frac{k}{pq}]$ and $X' = X = (\kappa_{l,l}^2, \kappa_{q+l,l}^2, \dots, \kappa_{k-q+l,l}^2)^T$ with n non-zero entries. Since $\kappa_{r-s+l,l}^2 \neq 0$ only if $q|r-s$ and $\frac{k}{p}|r-s$ (because $\eta^{p(r-s)} = 1$), we have $n \leq \frac{k}{\text{lcm}(\frac{k}{p}, q)} = \frac{p}{q} \gcd(\frac{k}{p}, q)$, where $\text{lcm}(a, b)$ denotes the least common multiple of a and b . The fact that $\kappa_{l,l}^2 = \frac{q^2}{4k^2} \neq 0$ requires $m < n$.

If $\gcd(\frac{k}{p}, q) < \frac{k}{p}$, then $\gcd(\frac{k}{p}, q) \leq \frac{k}{2p}$ and for $p \geq 2$,

$$m = \frac{k}{q} - [\frac{k}{pq}] \geq \frac{k}{q} - \frac{k}{pq} \geq \frac{k}{2q} = \frac{p}{q} \cdot \frac{k}{2p} \geq \frac{p}{q} \gcd(\frac{k}{p}, q) \geq n,$$

which leads to a contradiction. So $\gcd(\frac{k}{p}, q) = \frac{k}{p}$, i.e., $k|pq$. Thus $\frac{k}{q} \geq n > m = \frac{k}{q} - [\frac{k}{pq}] \geq \frac{k}{q} - 1$. This happens only if $k = pq$, which ends the proof of the **Claim 4**.

Now we are ready to finish the proof of the theorem.

(i) Suppose $p = 1$. In this case $\Gamma = \{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : q|j\}$, and

$$\kappa_{r,s} = \begin{cases} \frac{1}{2p} & r = s \equiv l \pmod{q} \\ 0 & \text{otherwise.} \end{cases}$$

Hence (2.8) becomes

$$\alpha_{i,j} = \sum_{(r,s) \in \Gamma} \alpha_{i-r,j-s} \alpha_{r,s} + \frac{q}{4k^2}, \quad q|j.$$

Let $M := \max\{\alpha_{i,j} : (i, j) \in \Gamma\}$ and suppose that $\alpha_{i_0, j_0} = M$. Then

$$M = \alpha_{i_0, j_0} = \sum_{(r,s) \in \Gamma} \alpha_{i_0-r, j_0-s} \alpha_{r,s} + \frac{q}{4k^2} \leq M \sum_{(r,s) \in \Gamma} \alpha_{r,s} + \frac{q}{4k^2} = \frac{M}{2} + \frac{q}{4k^2},$$

which implies $M \leq \frac{q}{2k^2}$. Moreover, $M \geq \frac{1}{2q\Gamma} = \frac{q}{2k^2}$. So $M = \frac{q}{2k^2}$, and thus

$$\alpha_{i,j} = \frac{q}{2k^2}, \quad (i,j) \in \Gamma.$$

If $q = 1$, we have $\mu = h_{\mathcal{A}_k}$, which is nothing but (1). Otherwise, we obtain (2).

(ii) Suppose $p > 1$ and $k = pq$. In this case $n = \frac{k}{q} = p, m = \frac{k}{q} - [\frac{k}{pq}] = p - 1$. Since $\kappa_{l,l}^2 = \frac{1}{4p^2}$, the equation $V'X' = 0$ possesses exactly one solution: $X' = (\frac{1}{4p^2}, \dots, \frac{1}{4p^2})^T$. That is to say,

$$\kappa_{r,s} = \begin{cases} \kappa_{0,0} = \frac{1}{2p} & r = s, r, s \equiv l \pmod{q} \\ \kappa_{0,s-r} = \pm \frac{1}{2p} & r \neq s, r, s \equiv l \pmod{q} \\ 0 & \text{otherwise.} \end{cases}$$

So the fact that $K \geq 0$ is equivalent to the positive semi-definiteness of the circulant matrix $[\kappa_{r,s}]_{r,s \equiv l \pmod{q}}$. Since the set of all the eigenvalues of $[\kappa_{r,s}]_{r,s \equiv l \pmod{q}}$ is

$$\left\{ \sum_{j \in q\mathbb{Z}_k} \kappa_{0,j} \eta^{ij}, i \in \mathbb{Z}_{k/q} \right\},$$

we have $K \geq 0$ if and only if

$$\sum_{j \in q\mathbb{Z}_k} \tau_j \eta^{ij} \geq 0, \quad i \in \mathbb{Z}_{k/q},$$

where $\tau_j := \kappa_{0,j} \in \{\pm 1\}, j \in q\mathbb{Z}_k$.

Now (2.8) is equivalent to

$$\alpha_{i,j} = \sum_{(m,n) \in \Gamma} \alpha_{i-m,j-n} \alpha_{m,n} + \frac{1}{4k}, \quad (i,j) \in \Gamma.$$

Following a similar argument as above, we have

$$\alpha_{i,j} = \frac{1}{2k}, \quad (i,j) \in \Gamma.$$

This gives (3), and the proof of the theorem is complete. \square

Remark 2.13. Let μ be as above. Then

1. $\mu = h_{\Gamma,l}$ if and only if

$$\mu(\rho_{i,j}) = \begin{cases} \frac{1}{2} & i = 0, \frac{k}{q} | j \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \mu(\sigma_{i,j}) = \begin{cases} \frac{1}{2} \eta^{jl} & i = 0, \frac{k}{q} | j \\ 0 & \text{otherwise} \end{cases},$$

if and only if

$$\hat{\mu}(\pi_{i,j}) = \begin{cases} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \eta^{-jl} \\ \frac{1}{2} \eta^{jl} & \frac{1}{2} \end{pmatrix} & i = 0, \frac{k}{q} | j \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{otherwise} \end{cases}$$

2. $\mu = h_{\Gamma, l, \tau}$ if and only if

$$\mu(\rho_{i,j}) = \begin{cases} \frac{1}{2} & q|i, p|j \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \mu(\sigma_{i,j}) = \begin{cases} \frac{1}{2}\tau_j\eta^{jl} & q|i, p|j \\ 0 & \text{otherwise} \end{cases},$$

if and only if

$$\hat{\mu}(\pi_{i,j}) = \begin{cases} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_{-j}\eta^{-jl} \\ \frac{1}{2}\tau_j\eta^{jl} & \frac{1}{2} \end{pmatrix} & q|i, p|j \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{otherwise} \end{cases}$$

Denote by $\mathcal{I}_1(\mathcal{A}_k)$, $\mathcal{I}_2(\mathcal{A}_k)$ and $\mathcal{I}_3(\mathcal{A}_k)$ the family of idempotent states of the forms h_Γ , $h_{\Gamma, l}$ and $h_{\Gamma, l, \tau}$ respectively. Then the discussions above can be rephrased as

Theorem 2.14. *Fix $k \geq 2$ an integer. Then the family of idempotent states $\text{Idem}(\mathcal{A}_k)$ on Sekine quantum group \mathcal{A}_k is given through*

$$\text{Idem}(\mathcal{A}_k) = \{h_{\mathcal{A}_k}\} \cup \mathcal{I}_1(\mathcal{A}_k) \cup \mathcal{I}_2(\mathcal{A}_k) \cup \mathcal{I}_3(\mathcal{A}_k).$$

2.4 The order structure on $\text{Idem}(\mathcal{A}_k)$

Franz and Skalski introduced in [29] the order relation on the set of idempotent states of a finite quantum group. We recall this definition for Sekine quantum groups here.

Definition 2.15. *Let $\phi_1, \phi_2 \in \text{Idem}(\mathcal{A}_k)$. Denote by \prec the partial order on $\text{Idem}(\mathcal{A}_k)$ given through*

$$\phi_1 \prec \phi_2 \quad \text{if} \quad \phi_1 \star \phi_2 = \phi_2.$$

In this order the Haar state $h_{\mathcal{A}_k}$ and the counit ϵ are, respectively, the biggest and smallest idempotent state in $\text{Idem}(\mathcal{A}_k)$. Let $\mu, \nu \in \text{Idem}(\mathcal{A}_k)$. We use superscripts to label all the symbols which appeared before. For example,

$$\mu := \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}^{(\mu)} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s}^{(\mu)} \tilde{e}_{r,s}, \quad \nu := \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}^{(\nu)} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s}^{(\nu)} \tilde{e}_{r,s}.$$

We introduce the partial order \prec in the family of 2 by 2 idempotent matrices $\mathcal{J} := \{A \in \mathbb{M}_2(\mathbb{C}) : A^2 = A\}$:

$$A \prec B \text{ if } AB = B, \quad A, B \in \mathcal{J},$$

and the partial order \prec in the family of subgroups of $\mathbb{Z}_k \times \mathbb{Z}_k$:

$$\Gamma \prec \Lambda \text{ if } \Gamma \subset \Lambda, \quad \Lambda, \Gamma \leq \mathbb{Z}_k \times \mathbb{Z}_k.$$

Then from (2.7), $\mu \prec \nu$ if and only if

$$\hat{\mu}(\pi_{i,j}) \prec \hat{\nu}(\pi_{i,j}), \quad i, j \in \mathbb{Z}_k, \tag{2.33}$$

Our main result in this section is the following theorem, characterizing the order structure in the lattice $(\text{Idem}(\mathcal{A}_k), \prec)$.

Theorem 2.16. *Let μ, ν be idempotent states, other than the Haar state, on \mathcal{A}_k as above. Then $\mu \prec \nu$ if and only if one of the following holds:*

$$(1) \quad \mu = h_{\Gamma^{(\mu)}}, \nu = h_{\Gamma^{(\nu)}} \in \mathcal{I}_1(\mathcal{A}_k) \text{ and } \Gamma^{(\mu)} \prec \Gamma^{(\nu)};$$

(2) $\mu = h_{\Gamma(\mu)} \in \mathcal{I}_1(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$ and $\Gamma(\mu) \prec \Gamma(\nu)$;

(3) $\mu = h_{\Gamma(\mu)} \in \mathcal{I}_1(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu), \tau(\nu)} \in \mathcal{I}_3(\mathcal{A}_k)$ and $\Gamma(\mu) \prec \Gamma(\nu)$;

(4) $\mu = h_{\Gamma(\mu), l(\mu)}, \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$, $\Gamma(\mu) \prec \Gamma(\nu)$ and $l(\mu) \equiv l(\nu) \pmod{q^{(\nu)}}$;

(5) $\mu = h_{\Gamma(\mu), l(\mu), \tau(\mu)} \in \mathcal{I}_3(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$, $\Gamma(\mu) \prec \Gamma(\nu)$ and

$$\tau_j^{(\nu)} = \eta^{j(l(\nu)-l(\mu))} \text{ for } j \text{ such that } \frac{k}{q^{(\nu)}} = p^{(\nu)}|j;$$

(6) $\mu = h_{\Gamma(\mu), l(\mu), \tau(\mu)}, \nu = h_{\Gamma(\nu), l(\nu), \tau(\nu)} \in \mathcal{I}_3(\mathcal{A}_k)$, $\Gamma(\mu) = \Gamma(\nu)$ and

$$\tau_j^{(\nu)} = \tau_j^{(\mu)} \eta^{j(l(\nu)-l(\mu))} \text{ for } j \text{ such that } p^{(\mu)} = p^{(\nu)}|j.$$

Proof. By (2.33), if $\hat{\mu}(\pi_{i,j}) \prec \hat{\nu}(\pi_{i,j})$, then $\hat{\mu}(\pi_{i,j}) = 0$ implies $\hat{\nu}(\pi_{i,j}) = 0$, and $\hat{\nu}(\pi_{i,j}) = I$ implies $\hat{\mu}(\pi_{i,j}) = I$. That is to say,

$$\{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \hat{\mu}(\pi_{i,j}) = 0\} \subset \{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \hat{\nu}(\pi_{i,j}) = 0\}, \quad (2.34)$$

and

$$\{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \hat{\nu}(\pi_{i,j}) = I\} \subset \{(i, j) \in \mathbb{Z}_k \times \mathbb{Z}_k : \hat{\mu}(\pi_{i,j}) = I\}. \quad (2.35)$$

So from Remark 2.9 and Remark 2.13 it follows that

1. if $\mu \in \mathcal{I}_3(\mathcal{A}_k)$, then $\nu \notin \mathcal{I}_2(\mathcal{A}_k)$;
2. if $\nu \in \mathcal{I}_1(\mathcal{A}_k)$, then $\mu \in \mathcal{I}_1(\mathcal{A}_k)$.

Hence we have only the following six cases:

(1) $\mu = h_{\Gamma(\mu)}, \nu = h_{\Gamma(\nu)} \in \mathcal{I}_1(\mathcal{A}_k)$. Then $\mu \prec \nu$ if and only if

$$\alpha_{i,j}^{(\nu)} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r, j-s}^{(\mu)} \alpha_{r,s}^{(\nu)}, \quad i, j \in \mathbb{Z}_k.$$

For $(i, j) \notin \Gamma(\nu)$, we have $\alpha_{i-r, j-s}^{(\mu)} \alpha_{r,s}^{(\nu)} = 0, \forall r, s \in \mathbb{Z}_k$. Choosing $(r, s) = (0, 0)$, we have $\alpha_{i,j}^{(\mu)} = 0$, i.e., $(i, j) \notin \Gamma(\mu)$. So $\Gamma(\mu) \prec \Gamma(\nu)$.

(2) $\mu = h_{\Gamma(\mu)} \in \mathcal{I}_1(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$. Then $\mu \prec \nu$ if and only if

$$\alpha_{i,j}^{(\nu)} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r, j-s}^{(\mu)} \alpha_{r,s}^{(\nu)}, \quad i, j \in \mathbb{Z}_k, \quad (2.36)$$

and

$$\kappa_{r,r}^{(\nu)} = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}^{(\mu)} \kappa_{r+j, r+j}^{(\nu)}, \quad r, s \in \mathbb{Z}_k. \quad (2.37)$$

From a similar argument as in (1), we have that (2.36) implies $\Gamma(\mu) \prec \Gamma(\nu)$. So $\Gamma(\mu) = \mathbb{Z}_k \times q^{(\mu)}\mathbb{Z}_k$ with $q^{(\nu)}|q^{(\mu)}$. In this case (2.37) always holds.

(3) $\mu = h_{\Gamma(\mu)} \in \mathcal{I}_1(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu), \tau(\nu)}$. Then $\mu \prec \nu$ if and only if

$$\alpha_{i,j}^{(\nu)} = \sum_{r,s \in \mathbb{Z}_k} \alpha_{i-r, j-s}^{(\mu)} \alpha_{r,s}^{(\nu)}, \quad i, j \in \mathbb{Z}_k, \quad (2.38)$$

and

$$\kappa_{r,s}^{(\nu)} = \sum_{i,j \in \mathbb{Z}_k} \eta^{i(s-r)} \alpha_{i,j}^{(\mu)} \kappa_{r+j, s+j}^{(\nu)}, \quad r, s \in \mathbb{Z}_k. \quad (2.39)$$

From a similar argument as in (2), we have $\Gamma(\mu) = p^{(\mu)}\mathbb{Z}_k \times q^{(\mu)}\mathbb{Z}_k \prec \Gamma(\nu) = p^{(\nu)}\mathbb{Z}_k \times q^{(\nu)}\mathbb{Z}_k$. Or equivalently, $p^{(\nu)}|p^{(\mu)}$ and $q^{(\nu)}|q^{(\mu)}$. In this case (2.39) always holds.

(4) $\mu = h_{\Gamma(\mu), l(\mu)}, \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$. From Remark 2.13 and (2.34) it follows that $q^{(\nu)}|q^{(\mu)}$. So $\Gamma(\mu) \prec \Gamma(\nu)$. Moreover, $\hat{\mu}(\pi_{i,j}) \prec \hat{\nu}(\pi_{i,j})$ requires that for all $\frac{k}{q^{(\nu)}}|j$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\eta^{-jl(\nu)} \\ \frac{1}{2}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\eta^{-jl(\mu)} \\ \frac{1}{2}\eta^{jl(\mu)} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\eta^{-jl(\nu)} \\ \frac{1}{2}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix},$$

which is equivalent to

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\eta^{-jl(\nu)} \\ \frac{1}{2}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4} + \frac{1}{4}\eta^{j(l(\nu)-l(\mu))} & \frac{1}{4}\eta^{-jl(\nu)}(1 + \eta^{j(l(\nu)-l(\mu))}) \\ \frac{1}{4}\eta^{jl(\nu)}(1 + \eta^{j(l(\mu)-l(\nu))}) & \frac{1}{4} + \frac{1}{4}\eta^{j(l(\mu)-l(\nu))} \end{pmatrix}.$$

That is to say,

$$\eta^{j(l(\nu)-l(\mu))} = 1 \text{ for all } \frac{k}{q^{(\nu)}}|j.$$

So $l(\mu) \equiv l(\nu) \pmod{q^{(\nu)}}$.

(5) $\mu = h_{\Gamma(\mu), l(\mu), \tau(\mu)} \in \mathcal{I}_3(\mathcal{A}_k), \nu = h_{\Gamma(\nu), l(\nu)} \in \mathcal{I}_2(\mathcal{A}_k)$. Following a similar argument as above, it follows that $\mu \prec \nu$ if and only if $q^{(\nu)}|q^{(\mu)}$ and

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_j^{(\nu)}\eta^{-jl(\nu)} \\ \frac{1}{2}\tau_j^{(\nu)}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\eta^{-jl(\mu)} \\ \frac{1}{2}\eta^{jl(\mu)} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_j^{(\nu)}\eta^{-jl(\nu)} \\ \frac{1}{2}\tau_j^{(\nu)}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix},$$

if and only if $\Gamma(\mu) \prec \Gamma(\nu)$ and

$$\tau_j^{(\nu)} = \eta^{j(l(\nu)-l(\mu))} \text{ for } j \text{ such that } \frac{k}{q^{(\nu)}} = p^{(\nu)}|j.$$

(6) $\mu = h_{\Gamma(\mu), l(\mu), \tau(\mu)}, \nu = h_{\Gamma(\nu), l(\nu), \tau(\nu)} \in \mathcal{I}_3(\mathcal{A}_k)$. From Remark 2.13 and (2.34) it follows that $p^{(\nu)}|p^{(\mu)}$ and $q^{(\nu)}|q^{(\mu)}$. Since $p^{(\mu)}q^{(\mu)} = p^{(\nu)}q^{(\nu)} = k$, we have $p^{(\mu)} = p^{(\nu)}, q^{(\mu)} = q^{(\nu)}$. Thus $\Gamma(\mu) = \Gamma(\nu)$. Moreover,

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_j^{(\nu)}\eta^{-jl(\nu)} \\ \frac{1}{2}\tau_j^{(\nu)}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_j^{(\mu)}\eta^{-jl(\mu)} \\ \frac{1}{2}\tau_j^{(\mu)}\eta^{jl(\mu)} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\tau_j^{(\nu)}\eta^{-jl(\nu)} \\ \frac{1}{2}\tau_j^{(\nu)}\eta^{jl(\nu)} & \frac{1}{2} \end{pmatrix},$$

which is equivalent to

$$\tau_j^{(\nu)} = \tau_j^{(\mu)}\eta^{j(l(\nu)-l(\mu))} \text{ for } j \text{ such that } p^{(\mu)} = p^{(\nu)}|j.$$

□

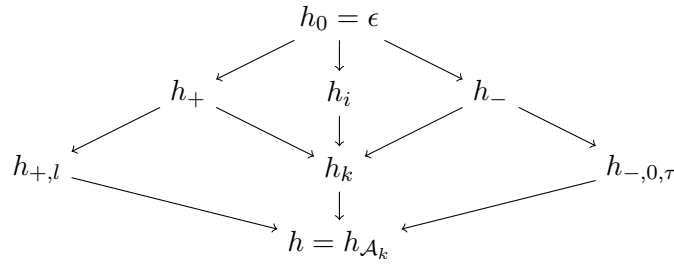
We present here the order structure on $\text{Idem}(\mathcal{A}_k)$ for k prime.

Example 2.17. When k is a prime number, $\mathbb{Z}_k \times \mathbb{Z}_k$ has one subgroup of order 1: $\Gamma_0 = \{(0, 0)\}$, $k + 1$ subgroups of order k :

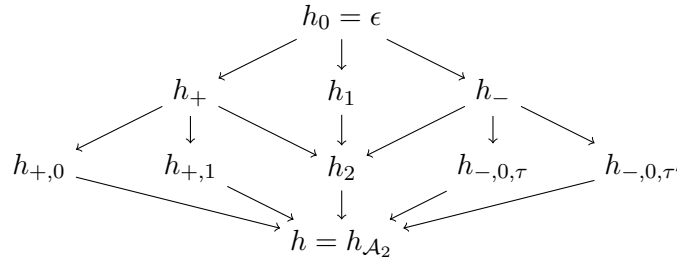
$$\Gamma_+ = \mathbb{Z}_k \times k\mathbb{Z}_k, \quad \Gamma_- = k\mathbb{Z}_k \times \mathbb{Z}_k, \quad \Gamma_i = \{j(1, i) = (j, ij) : j \in \mathbb{Z}_k\},$$

where $i = 1, 2, \dots, k - 1$, and one subgroup of order k^2 : $\Gamma_k = \mathbb{Z}_k \times \mathbb{Z}_k$.

Then Proposition 2.8 gives $k + 3$ idempotent states: $h_+ := h_{\Gamma_+}$, $h_- := h_{\Gamma_-}$, and $h_i := h_{\Gamma_i}$, $i = 0, 1, \dots, k$, in which $h_0 = \epsilon$ is the counit. The idempotent state in Theorem 2.11 (1) is the Haar state $h = h_{\mathcal{A}_k}$. By Theorem 2.11 (2), the Haar idempotent states of the form $h_{\Gamma, l}$ are $h_{+, l} := h_{\Gamma_+, l}$ with $l \in \mathbb{Z}_k$. And the Theorem 2.11 (3) tells us that $h_{-, 0, \tau} := h_{\Gamma_-, 0, \tau}$ are the only elements in $\mathcal{I}_3(\mathcal{A}_k)$, where τ verifies (2.17). From Theorem 2.16 we can draw the Hasse diagram of the lattice $(\text{Idem}(\mathcal{A}_k), \prec)$ as:



where $i = 1, 2, \dots, k - 1$, $l \in \mathbb{Z}_k$, and τ represents a family of parameters which satisfy (2.17). When $k = 2$, the Hasse diagram reads precisely as:



Here τ is the trivial one that satisfies (2.17), i.e., $\tau_0 = \tau_1 = 1$; and τ' is given through $\tau'_0 = 1$ and $\tau'_1 = -1$, as we have mentioned in Remark 2.12. One should compare this diagram with the one in [27] of eight-dimension Kac-Paljutkin quantum group.

Note that the Hasse diagram for $k = 2$ coincides with that of the lattice of subgroups of the dihedral group D_4 (with the partial order reversed). Indeed, from discussions in Section 1, \mathcal{A}_2 has 8 one-dimensional representations and no 2-dimensional ones. Hence it is co-commutative, and therefore equal to $C^*(\Gamma)$ for some classical group Γ . This group is nothing but D_4 . To see this, take $x = \rho_{11} + \sigma_{11}$ and $y = \rho_{10} + \sigma_{10}$. It is not difficult to verify that $y^2 = x^4 = 1$ and $xyx = x^{-1}$. Moreover, x and y do not admit any other independent relations. So \mathcal{A}_2 is the group algebra of D_4 , and thus the lattice of idempotent states on \mathcal{A}_2 is nothing but the lattice of subgroups of D_4 .

2.5 Convergence of convolution powers of states on Sekine quantum groups

We end this chapter by saying a few words on the convergence of convolution powers of states on Sekine quantum groups. This is related to random walks on quantum groups [27, 53].

Fix a state $\mu = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \tilde{d}_{i,j} + \sum_{r,s \in \mathbb{Z}_k} \kappa_{r,s} \tilde{e}_{r,s}$ on \mathcal{A}_k . Then clearly $\{\mu^{*n}\}_{n \geq 1}$ converges if and only if $\{\hat{\mu}(\pi_{p,q})^n\}_{n \geq 1}$ converges for all $p, q \in \mathbb{Z}_k$. The following proposition gives a sufficient condition that guarantees the convergence.

Proposition 2.18. *Let μ be as above. Then $\{\mu^{*n}\}_{n \geq 1}$ converges if $\alpha_{0,0} > 0$.*

Proof. Fix $p, q \in \mathbb{Z}_k$. Denote by λ_1, λ_2 the eigenvalues of $\hat{\mu}(\pi_{p,q})$. Let $\lambda \in \{\lambda_1, \lambda_2\}$, then we have

$$(\lambda - \mu(\rho_{p,q}))(\lambda - \mu(\rho_{p,-q})) = \mu(\sigma_{p,q})\mu(\sigma_{p,-q}).$$

Since $\pi_{p,q}$ is unitary, $\|\hat{\mu}(\pi_{p,q})\| = \|(\text{id}_{\mathbb{M}_2(\mathbb{C})} \otimes \mu)(\pi_{p,q})\| \leq 1$. Thus $|\lambda| \leq 1$. Note that

$$|\mu(\rho_{p,q})| = \left| \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \eta^{ip+jq} \right| \leq \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}, \quad (2.40)$$

and from $K = [\kappa_{r,s}]_{r,s \in \mathbb{Z}_k} \geq 0$ it follows that

$$|\mu(\sigma_{p,q})| = \left| \sum_{l \in \mathbb{Z}_k} \kappa_{l,l+p} \eta^{ql} \right| \leq \sum_{l \in \mathbb{Z}_k} |\kappa_{l,l+p}| \leq \frac{1}{2} \sum_{l \in \mathbb{Z}_k} (\kappa_{l,l} + \kappa_{l+p,l+p}) = \sum_{r \in \mathbb{Z}_k} \kappa_{r,r}.$$

If $|\lambda| = 1$, then the equations above yield

$$\begin{aligned} (1 - \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j})^2 &\leq (|\lambda| - |\mu(\rho_{p,q})|)(|\lambda| - |\mu(\rho_{p,-q})|) \\ &\leq |(\lambda - \mu(\rho_{p,q}))(\lambda - \mu(\rho_{p,-q}))| \\ &= |\mu(\sigma_{p,q})\mu(\sigma_{p,-q})| \\ &\leq (1 - \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j})^2. \end{aligned}$$

Hence

$$(1 - \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j})^2 = (1 - |\mu(\rho_{p,q})|)(1 - |\mu(\rho_{p,-q})|),$$

which gives $|\mu(\rho_{p,q})| = |\mu(\rho_{p,-q})| = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}$. Since $\alpha_{0,0} > 0$, we have $\mu(\rho_{p,q}) = \mu(\rho_{p,-q}) = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} > 0$. So λ can be nothing but 1. That is to say, $\lambda \in \{z \in \mathbb{Z} : |z| < 1\} \cup \{1\}$. Hence $\{\hat{\mu}(\pi_{p,q})^n\}_{n \geq 1}$ converges if $\hat{\mu}(\pi_{p,q})$ is not similar to the Jordan normal form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

If $\lambda_1 = \lambda_2 = 1$, then from

$$2 = \lambda_1 + \lambda_2 = \mu(\rho_{p,q}) + \mu(\rho_{p,-q}) \leq 2 \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} \leq 2$$

it follows that $\mu(\rho_{p,q}) = \mu(\rho_{p,-q}) = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j} = 1$. Thus $\mu(\sigma_{p,q}) = \mu(\sigma_{p,-q}) = \sum_{r \in \mathbb{Z}_k} \kappa_{r,r} = 0$. That is to say, $\hat{\mu}(\pi_{p,q})$ equals identity, not similar to the Jordan normal form as above, which finishes the proof. \square

Remark 2.19. *In the proof we only used $\alpha_{0,0} > 0$ to deduce $\mu(\rho_{p,q}) = \mu(\rho_{p,-q}) = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}$ from $|\mu(\rho_{p,q})| = |\mu(\rho_{p,-q})| = \sum_{i,j \in \mathbb{Z}_k} \alpha_{i,j}$. Recalling (2.40), to make sure that $\{\mu^{*n}\}_{n \geq 1}$ converges when $\alpha_{0,0} = 0$, it suffices to assume $\#\{\eta^{ip+jq} : \alpha_{i,j} \neq 0\} \geq 2$ for all $p, q \in \mathbb{Z}_k$.*

Chapter 3

Infinitely divisible states on finite quantum groups

In this chapter we study the states of Poisson type and infinitely divisible states on compact quantum groups. Each state of Poisson type is infinitely divisible, i.e., it admits n -th root for all $n \geq 1$. The main result is that on finite quantum groups infinitely divisible states must be of Poisson type. This generalizes Böge's theorem concerning infinitely divisible measures (commutative case) and Parthasarathy's result on infinitely divisible positive definite functions (co-commutative case).

1. The space of bounded measures on a compact (semi)group is equipped with a natural convolution operation. The convolution of two probability measures is still a probability measure. *Infinitely divisible probability measures* are probability measures that admit n -th root for all $n \geq 1$, where the root is also a probability measure. On finite groups such probability measures have been shown to be of Poisson type, see [7] and [65].
2. A *positive definite function* on a compact group G is a continuous function $\phi : G \rightarrow \mathbb{C}$ such that $[\phi(g_i^{-1}g_j)]_{i,j=1}^n$ is a positive semi-definite matrix for all $g_1, \dots, g_n \in G$ and for all $n \geq 1$. It is *normalized* if $\phi(e) = 1$, where e is the unit of G . The pointwise product of two normalized positive definite functions on G is again a normalized positive definite function. From this we can define infinitely divisible normalized positive definite functions on a compact group in a natural way. This is thoroughly studied by Parthasarathy [60]. As a special case, he proved that every infinitely divisible normalized positive definite function on a finite group is of Poisson type, although the notion "Poisson type" was not explicitly defined in his paper.

We shall give two proofs of our main results. Let us explain the difficulty of this problem in the quantum group setting. Consider the infinitely divisible states on the dual of a finite group G , that is, we shall study positive definite functions $\omega : G \rightarrow \mathbb{C}$ with $\omega(e) = 1$, such that for all $n \geq 1$, there exists positive definite function ω_n on G satisfying $\omega_n(e) = 1$ and $\omega = \omega_n^n$. Recall that a function $f : G \rightarrow \mathbb{C}$ is positive definite if $[f(st^{-1})]_{s,t \in S}$ is positive semi-definite for any finite subset $S \subset G$. We shall prove that such ω can be written as an exponential. A key observation of the proof is that, the support of ω (which is the same as that of ω_n for each n) forms a subgroup of G . In fact, there exists a subsequence of $\{\omega_n\}_{n \geq 1}$ which converges to an idempotent normalized positive definite function ϕ and one can easily show that the support of ϕ is necessarily a

subgroup of G . So we may transfer the problem to the subgroup and always assume that ω (and all ω_n) is non-zero everywhere. However, on the one hand, it is difficult to capture the idempotent state (the substitute of idempotent normalized positive definite function in quantum setting) for which it has the same “support” as ω . On the other hand, in the quantum group case we can not always transfer the problem to a quantum subgroup, as the idempotent state might be non-Haar. For this we introduce the *Plancherel triple* and the first section gathers some properties of the Plancherel triple coming from an idempotent state on a finite quantum group.

Let us fix some notations for this chapter. For any C^* -algebra A , we use A' to denote the set of bounded linear functionals on A . We use $\mathbb{M}_n(\mathbb{C})$ to denote the n -by- n full complex matrix algebra. We will follow the notations of compact quantum groups in the last chapter, but we will not recall them here in detail.

3.1 Preliminary: Plancherel triple

In this section we introduce the notion of *Plancherel triple*, which is slightly different from the same notion in [24]. Moreover, one can compare it with the so-called *D-pairs* discussed in [44]. Let A, B be two finite-dimensional C^* -algebras. Suppose that

$$\langle \cdot, \cdot \rangle : A \times B \rightarrow \mathbb{C},$$

is a non-degenerate bilinear form. Then through $\langle \cdot, \cdot \rangle$, B can be identified with A' . Indeed, the map $B \rightarrow A', b \mapsto \langle \cdot, b \rangle$ is injective, since $\langle \cdot, \cdot \rangle$ is non-degenerate. So B can be viewed as a subspace of A' and then $\dim B \leq \dim A' = \dim A$. Similarly, A can be viewed as a subspace of B' and $\dim A \leq \dim B' = \dim B$. Hence $\dim A = \dim B$ and $B = A'$ (also $A = B'$).

Definition 3.1. *Let the triple $(A, B, \langle \cdot, \cdot \rangle)$ be as above. Then it is called a Plancherel triple if*

- (1) *the comultiplications $\Delta_A : A \rightarrow A \otimes A$ and $\Delta_B : B \rightarrow B \otimes B$ are positive, where Δ_A is the adjoint of the map given by $B \otimes B \rightarrow B, b_1 \otimes b_2 \mapsto b_1 b_2$ and Δ_B is the adjoint of the map defined through $A \otimes A \rightarrow A, a_1 \otimes a_2 \mapsto a_1 a_2$;*
- (2) *the counits $\epsilon_A := \langle \cdot, 1_B \rangle : A \rightarrow \mathbb{C}$ and $\epsilon_B := \langle 1_A, \cdot \rangle : B \rightarrow \mathbb{C}$ are $*$ -homomorphisms;*
- (3) *the Haar functionals $h_A := \langle \cdot, p_B \rangle$ and $h_B := \langle p_A, \cdot \rangle$ are faithful, positive and tracial, where $p_A \in A$ and $p_B \in B$ are support projections of ϵ_A and ϵ_B , respectively, i.e.,*

$$p_A = p_A^* = p_A^2, \quad a p_A = p_A a = \epsilon_A(a) p_A, \quad a \in A,$$

$$p_B = p_B^* = p_B^2, \quad b p_B = p_B b = \epsilon_B(b) p_B, \quad b \in B;$$

- (4) *the Fourier transforms $\mathcal{F}_A : A \rightarrow B, a \mapsto \hat{a}$ and $\mathcal{F}_B : B \rightarrow A, b \mapsto \check{b}$ satisfy:*

$$h_B(\hat{a}_1 \hat{a}_2^*) = c h_A(a_1 a_2^*), \quad (3.1)$$

$$h_A(\check{b}_1 \check{b}_2^*) = c' h_B(b_1 b_2^*), \quad (3.2)$$

for all $a_1, a_2 \in A, b_1, b_2 \in B$ and some $c, c' > 0$, where \hat{a} and \check{b} are defined through:

$$\langle x, \hat{a} \rangle := h_A(xa), \quad \langle \check{b}, y \rangle := h_B(by), \quad x \in A, y \in B.$$

Note that the above definition is self-dual, that is, (B, A, \langle, \rangle) forms a Plancherel triple if (A, B, \langle, \rangle) is a Plancherel triple, where $(b, a) := \langle a, b \rangle, a \in A, b \in B$. We have the following properties of a Plancherel triple.

Proposition 3.2. *Let (A, B, \langle, \rangle) be a Plancherel triple. Suppose that $A = \bigoplus_{\alpha=1}^m \mathbb{M}_{n_\alpha}(\mathbb{C})$ with the matrix units $\{e_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$. Let $\{\widetilde{e}_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$ be the dual basis of $\{e_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$.*

- (1) *We have $\mathcal{F}_A(e_{ij}^\alpha) = c_\alpha \widetilde{e}_{ji}^\alpha$ for some positive number c_α .*
- (2) *Suppose that $e^{\alpha_0} = p_A$. Then $\widetilde{e}^{\alpha_0} = \epsilon_A = 1_B$. Consequently, $h_B(1_B) = 1$ and then h_B is a state.*
- (3) *We have the orthogonality relation:*

$$h_B \left(\widetilde{e}_{ij}^\alpha (e_{kl}^\beta)^* \right) = \frac{\delta_{\alpha\beta} \delta_{ik} \delta_{jl}}{cc_\alpha},$$

for all $\alpha, \beta, i, j, k, l$, where c is the constant appearing in (3.1).

- (4) *We have*

$$h_B \left(\widetilde{e}_{ij}^\alpha \right) = \delta_{\alpha_0\alpha}, \quad (3.3)$$

and

$$\epsilon_B \left(\widetilde{e}_{ij}^\alpha \right) = \delta_{ij}, \quad (3.4)$$

for all α, i, j .

Proof. (1) For any $a = \sum_{\alpha=1}^m \sum_{i,j=1}^{n_\alpha} a_{ij}^\alpha e_{ij}^\alpha \in A$, we have by definition

$$\langle a, \mathcal{F}_A(e_{ij}^\alpha) \rangle = h_A(ae_{ij}^\alpha) = a_{ji}^\alpha h_A(e_{jj}^\alpha) = h_A(e_{jj}^\alpha) \widetilde{e}_{ji}^\alpha(a).$$

Since h_A is tracial, $h_A(e_{jj}^\alpha)$ is independent of j . So

$$\langle a, \mathcal{F}_A(e_{ij}^\alpha) \rangle = c_\alpha \widetilde{e}_{ji}^\alpha(a), \quad a \in A,$$

with $c_\alpha = h_A(e_{jj}^\alpha) > 0$. Thus $\mathcal{F}_A(e_{ij}^\alpha) = c_\alpha \widetilde{e}_{ji}^\alpha$, since \langle, \rangle is non-degenerate.

- (2) For any $a = \sum_{\alpha=1}^m \sum_{i,j=1}^{n_\alpha} a_{ij}^\alpha e_{ij}^\alpha \in A$, we have by definition

$$a^{\alpha_0} e^{\alpha_0} = ap_A = \epsilon_A(a)p_A = \langle a, 1_B \rangle e^{\alpha_0}.$$

Then

$$\widetilde{e}^{\alpha_0}(a) = a^{\alpha_0} = \langle a, 1_B \rangle, \quad a \in A.$$

Hence $\widetilde{e}^{\alpha_0} = \epsilon_A = 1_B$.

- (3) This is a direct consequence of (3.1) and (1).

- (4) By (2) and (3) we have

$$h_B \left(\widetilde{e}_{ij}^\alpha \right) = h_B \left(\widetilde{e}_{ij}^\alpha (\widetilde{e}^{\alpha_0})^* \right) = \frac{\delta_{\alpha_0\alpha}}{cc_{\alpha_0}}.$$

In particular, we have

$$1 = h_B(1_B) = h_B \left(\widetilde{e}^{\alpha_0} (\widetilde{e}^{\alpha_0})^* \right) = \frac{1}{cc_{\alpha_0}}.$$

This proves (3.3). To show (3.4), recall that by definition,

$$\epsilon_B \left(\widetilde{e_{ij}^\alpha} \right) = \langle 1_A, \widetilde{e_{ij}^\alpha} \rangle = \widetilde{e_{ij}^\alpha}(1_A) = \delta_{ij}.$$

□

Example 3.3. Let (A, Δ) be a finite quantum group with dual $(\hat{A}, \hat{\Delta})$. Then $(A, \hat{A}, \langle, \rangle)$ forms a Plancherel triple. Here the bilinear form \langle, \rangle is given by $\langle a, \varphi \rangle := \varphi(a)$. The comultiplications, counits, Haar states, and Fourier transforms are the usual comultiplications, counits, Haar states, and Fourier transforms on A and \hat{A} , respectively.

3.2 Plancherel triple induced from an idempotent state

In this section we will construct a Plancherel triple from an *idempotent state* on a finite quantum group $\mathbb{G} = (A, \Delta)$. Recall that an idempotent state on \mathbb{G} is a state ϕ such that $\phi \star \phi = \phi$. It is well-known that (see for example [29]) when considered as an element in \hat{A} , $p = \phi$ is a *group-like projection* in \hat{A} . By a group-like projection of the finite quantum group $\hat{\mathbb{G}} = (\hat{A}, \hat{\Delta})$ we mean a non-zero element $p \in \hat{A}$ such that $p = p^* = p^2$ and

$$\hat{\Delta}(p)(1 \otimes p) = p \otimes p = \hat{\Delta}(p)(p \otimes 1), \quad \hat{S}(p) = p. \quad (3.5)$$

Our aim in this section is to show that $(A_\phi, \hat{A}_p, \langle, \rangle)$ forms a Plancherel triple, where $A_\phi = (\phi \otimes \iota \otimes \phi)\Delta^{(2)}(A)$ is a C*-subalgebra of A , $\hat{A}_p := p\hat{A}p$ is a C*-subalgebra of \hat{A} and the bilinear form is inherited from the one on the pair (A, \hat{A}) . In the following we shall explain the constructions of A_ϕ and \hat{A}_p in detail.

Before this we remark here that these constructions have already been studied by many people [20, 29, 16, 28]. Many results are well-known and their proofs are omitted here.

3.2.1 C*-subalgebra A_ϕ

In this subsection we construct and study the C*-subalgebra A_ϕ . Denote by $\text{Idem}(\mathbb{G})$ the set of all idempotent states on a compact quantum group \mathbb{G} . Recall that if $\phi \in \text{Idem}(\mathbb{G})$, we have $\phi = \phi S$ on $\text{Pol}(\mathbb{G})$, where S is the antipode on $\text{Pol}(\mathbb{G})$ [29].

The first lemma is a special case of [29, Lemma 3.1], and also a variation of [52, Lemma 4.3].

Lemma 3.4. *Let ϕ be an idempotent state on a compact quantum group \mathbb{G} . For $b \in A$ define $\phi_b(a) := \phi(ab)$ for all $a \in A$. Then we have*

$$\phi \star \phi_b = \phi(b)\phi.$$

For $\phi \in \text{Idem}(\mathbb{G})$ set $\mathbb{E}_\phi^\ell := (\phi \otimes \iota)\Delta$ and $\mathbb{E}_\phi^r := (\iota \otimes \phi)\Delta$. The next lemma lists some useful properties of \mathbb{E}_ϕ^ℓ and \mathbb{E}_ϕ^r .

Lemma 3.5. *Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group.*

- (1) $\mathbb{E}_\phi^\ell(a^*) = \mathbb{E}_\phi^\ell(a)^*$, $\mathbb{E}_\phi^r(a^*) = \mathbb{E}_\phi^r(a)^*$, $a \in A$.
- (2) $\Delta\mathbb{E}_\phi^\ell = (\mathbb{E}_\phi^\ell \otimes \iota)\Delta$, $\Delta\mathbb{E}_\phi^r = (\iota \otimes \mathbb{E}_\phi^r)\Delta$.
- (3) $(\iota \otimes \mathbb{E}_\phi^\ell)\Delta = (\mathbb{E}_\phi^r \otimes \iota)\Delta$.
- (4) $\mathbb{E}_\phi^\ell\mathbb{E}_\phi^r = \mathbb{E}_\phi^r\mathbb{E}_\phi^\ell$.

(5) For any $a, b \in A$,

$$\mathbb{E}_\phi^\ell(a)\mathbb{E}_\phi^\ell(b) = \mathbb{E}_\phi^\ell(a\mathbb{E}_\phi^\ell(b)) = \mathbb{E}_\phi^\ell(\mathbb{E}_\phi^\ell(a)b), \quad (3.6)$$

$$\mathbb{E}_\phi^r(a)\mathbb{E}_\phi^r(b) = \mathbb{E}_\phi^r(a\mathbb{E}_\phi^r(b)) = \mathbb{E}_\phi^r(\mathbb{E}_\phi^r(a)b). \quad (3.7)$$

Consequently, we have $\mathbb{E}_\phi^\ell\mathbb{E}_\phi^\ell = \mathbb{E}_\phi^\ell$ and $\mathbb{E}_\phi^r\mathbb{E}_\phi^r = \mathbb{E}_\phi^r$.

Proof. (1)-(4) are just straightforward computations. For (5) we prove (3.6) first. For this note that it suffices to show the first equation for any a, b the coefficients of unitary representation of \mathbb{G} . The case for general a, b follows from the linearity and density. Let $\{u_{ij}^\alpha, 1 \leq i, j \leq n_\alpha\}$ be the coefficients of the irreducible unitary representations $u^\alpha, \alpha \in \text{Irr}(\mathbb{G})$. On the one hand, for any u_{ij}^α and u_{kl}^β we have

$$\mathbb{E}_\phi^\ell(u_{ij}^\alpha)\mathbb{E}_\phi^\ell(u_{kl}^\beta) = \sum_{s=1}^{n_\alpha} \sum_{t=1}^{n_\beta} \phi(u_{is}^\alpha)\phi(u_{kt}^\beta)u_{sj}^\alpha u_{tl}^\beta.$$

On the other hand,

$$\mathbb{E}_\phi^\ell(\mathbb{E}_\phi^\ell(u_{ij}^\alpha)u_{kl}^\beta) = \sum_{r=1}^{n_\alpha} \sum_{t=1}^{n_\beta} \phi(u_{ir}^\alpha)\phi(u_{rs}^\alpha u_{kt}^\beta)u_{sj}^\alpha u_{tl}^\beta.$$

Now by using Lemma 3.4 we have for any $b \in A$

$$\phi(b)\phi(u_{is}^\alpha) = \sum_{r=1}^{n_\alpha} \phi(u_{ir}^\alpha)\phi(u_{rs}^\alpha b), \quad 1 \leq i, s \leq n_\alpha, \alpha \in \text{Irr}(\mathbb{G}).$$

Choosing b as u_{kt}^β , we have

$$\begin{aligned} \mathbb{E}_\phi^\ell(\mathbb{E}_\phi^\ell(u_{ij}^\alpha)u_{kl}^\beta) &= \sum_{r=1}^{n_\alpha} \sum_{t=1}^{n_\beta} \left(\sum_{s=1}^{n_\alpha} \phi(u_{ir}^\alpha)\phi(u_{rs}^\alpha u_{kt}^\beta) \right) u_{sj}^\alpha u_{tl}^\beta \\ &= \sum_{s=1}^{n_\alpha} \sum_{t=1}^{n_\beta} \phi(u_{is}^\alpha)\phi(u_{kt}^\beta)u_{sj}^\alpha u_{tl}^\beta = \mathbb{E}_\phi^\ell(u_{ij}^\alpha)\mathbb{E}_\phi^\ell(u_{kl}^\beta). \end{aligned}$$

So $\mathbb{E}_\phi^\ell(a)\mathbb{E}_\phi^\ell(b) = \mathbb{E}_\phi^\ell(\mathbb{E}_\phi^\ell(a)b)$. In the same way one can show that $\mathbb{E}_\phi^r(a)\mathbb{E}_\phi^r(b) = \mathbb{E}_\phi^r(a\mathbb{E}_\phi^r(b))$, then (3.6) is proved. Note that by choosing $b = 1_A$ in (3.6), we obtain $\mathbb{E}_\phi^\ell\mathbb{E}_\phi^\ell = \mathbb{E}_\phi^\ell$. The proof of (3.7) and $\mathbb{E}_\phi^r\mathbb{E}_\phi^r = \mathbb{E}_\phi^r$ is similar. \square

Now we define $\mathbb{E}_\phi := \mathbb{E}_\phi^\ell\mathbb{E}_\phi^r = \mathbb{E}_\phi^r\mathbb{E}_\phi^\ell$. The map \mathbb{E}_ϕ shares the similar properties of \mathbb{E}_ϕ^ℓ and \mathbb{E}_ϕ^r , see the following lemma (1)-(4). Moreover, \mathbb{E}_ϕ commutes with the antipode S , as the following lemma (5) shows. This enables the algebra $\mathbb{E}_\phi(A)$ to possess nicer properties than $\mathbb{E}_\phi^\ell(A)$ and $\mathbb{E}_\phi^r(A)$. We shall choose $\mathbb{E}_\phi(A)$ to be our A_ϕ .

Lemma 3.6. *Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group. Then*

$$(1) \mathbb{E}_\phi(a^*) = \mathbb{E}_\phi(a)^*, a \in A.$$

$$(2) \Delta\mathbb{E}_\phi = (\mathbb{E}_\phi^\ell \otimes \mathbb{E}_\phi^r)\Delta.$$

$$(3) (\mathbb{E}_\phi \otimes \mathbb{E}_\phi)\Delta = (\iota \otimes \mathbb{E}_\phi^\ell)\Delta\mathbb{E}_\phi = (\mathbb{E}_\phi^r \otimes \iota)\Delta\mathbb{E}_\phi.$$

$$(4) \mathbb{E}_\phi(a)\mathbb{E}_\phi(b) = \mathbb{E}_\phi(a\mathbb{E}_\phi(b)) = \mathbb{E}_\phi(\mathbb{E}_\phi(a)b), a, b \in A. \text{ Consequently, } \mathbb{E}_\phi\mathbb{E}_\phi = \mathbb{E}_\phi.$$

Hence $A_\phi := \mathbb{E}_\phi(A)$ is a unital C^* -subalgebra of A . Moreover,

(5) $S\mathbb{E}_\phi = \mathbb{E}_\phi S$ on $\text{Pol}(\mathbb{G})$.

Proof. Again we omit the proof of (1)-(4) here. The fact that A_ϕ is a unital C^* -subalgebra follows directly from these properties. To prove (5), it suffices to check the equality for $u_{ij}^\alpha, 1 \leq i, j \leq n_\alpha, \alpha \in \text{Irr}(\mathbb{G})$, the coefficients of unitary representation of \mathbb{G} . And that is a consequence of

$$\begin{aligned} S\mathbb{E}_\phi(u_{ij}^\alpha) &= S(\phi \otimes \iota \otimes \phi)\Delta^{(2)}(u_{ij}^\alpha) \\ &= \sum_{k,l=1}^{n_\alpha} \phi(u_{ik}^\alpha)\phi(u_{lj}^\alpha)S(u_{kl}^\alpha) \\ &= \sum_{k,l=1}^{n_\alpha} \phi(u_{ik}^\alpha)\phi(u_{lj}^\alpha)(u_{lk}^\alpha)^*, \end{aligned}$$

and

$$\begin{aligned} \mathbb{E}_\phi S(u_{ij}^\alpha) &= (\phi \otimes \iota \otimes \phi)\Delta^{(2)}((u_{ji}^\alpha)^*) \\ &= \sum_{k,l=1}^{n_\alpha} \phi((u_{ki}^\alpha)^*)\phi((u_{jl}^\alpha)^*)(u_{lk}^\alpha)^* \\ &= \sum_{k,l=1}^{n_\alpha} \phi(u_{ik}^\alpha)\phi(u_{lj}^\alpha)(u_{lk}^\alpha)^*, \end{aligned}$$

where the last equality follows from the facts that $\phi = \phi S$ on $\text{Pol}(\mathbb{G})$ and $S(u_{ij}^\alpha) = (u_{ji}^\alpha)^*$. \square

3.2.2 ϕ -bi-invariant functionals

Let ϕ be an idempotent state on a compact quantum group $\mathbb{G} = (A, \Delta)$. A functional $u \in A'$ is called ϕ -bi-invariant if $u\phi = \phi u = u$. In this subsection we characterize the ϕ -bi-invariant functionals. It turns out that one can transfer each ϕ -bi-invariant functional on A to its restriction to A_ϕ , preserving the norm and the $*$ -algebra structure. See [19] for related work.

For linear functionals φ_1, φ_2 on A_ϕ , one can also define their convolution product within $(A_\phi)'$: $\varphi_1 \star \varphi_2$ is defined as $(\varphi_1 \otimes \varphi_2)\Delta_\phi$. And for any linear functional φ on $\mathbb{E}_\phi(\text{Pol}(\mathbb{G}))$ one can also define its involution within $(A_\phi)'$: $\varphi^* := \varphi(S(\cdot)^*)$. Still, we write $\varphi_1 \varphi_2$ for short to denote $\varphi_1 \star \varphi_2$. Note here that φ^* is well-defined because $S\mathbb{E}_\phi = \mathbb{E}_\phi S$.

We formulate the results of ϕ -bi-invariant functionals here without the proof. Note that in the sequel we shall use $\|u\|$ to denote the norm of $u \in A'$ as a functional on A . Moreover, we suppose that $A = C_u(\mathbb{G})$.

Lemma 3.7. *Let $\phi \in \text{Idem}(\mathbb{G})$ and $u \in A'$. Then u is ϕ -bi-invariant if and only if $u = u|_{A_\phi}\mathbb{E}_\phi$. In this case, the following hold:*

- (1) $\|u\| = \|u|_{A_\phi}\|$;
- (2) u is a positive linear functional (resp. a state) on A if and only if $u|_{A_\phi}$ is a positive linear functional (resp. a state) on A_ϕ ;
- (3) $u^*|_{A_\phi} = (u|_{A_\phi})^*$ on $\mathbb{E}_\phi(\text{Pol}(\mathbb{G}))$;
- (4) if u and v in A' are both ϕ -bi-invariant, then $(uv)|_{A_\phi} = u|_{A_\phi}v|_{A_\phi}$;
- (5) $\phi = \epsilon\mathbb{E}_\phi = \epsilon|_{A_\phi}\mathbb{E}_\phi$.

3.2.3 The Plancherel triple $(A_\phi, \hat{A}_p, \langle, \rangle)$

Let $\mathbb{G} = (A, \Delta)$ be a finite quantum group. Let ϕ be an idempotent state on \mathbb{G} , then $p = \phi$ is a group-like projection in \hat{A} . By Lemma 3.6, $A_\phi = \mathbb{E}_\phi(A)$ is a finite dimensional C*-algebra. Clearly $\hat{A}_p = p\hat{A}p$ is also a finite dimensional C*-algebra. Moreover, we have $(A_\phi)' = \hat{A}_p$. In fact, the bilinear form on $A_\phi \times \hat{A}_p$ is non-degenerate. On the one hand, if $x \in A_\phi$ such that $u(x) = 0$ for all $u \in \hat{A}_p$, then $x = 0$. To see this, for any $u \in \hat{A}$, since $x = \mathbb{E}_\phi(x)$ and $u\mathbb{E}_\phi \in \hat{A}_p$, we have

$$u(x) = u(\mathbb{E}_\phi(x)) = (u\mathbb{E}_\phi)(x) = 0.$$

This gives $x = 0$. On the other hand, if $u \in \hat{A}_p$ such that $u(x) = 0$ for all $x \in A_\phi$, then $u = 0$. For this, take any $x \in A$. Recall that $\mathbb{E}_\phi(x) \in A_\phi$ and $u = u|_{A_\phi}\mathbb{E}_\phi$ by Lemma 3.6, then

$$u(x) = u|_{A_\phi}\mathbb{E}_\phi(x) = u(\mathbb{E}_\phi(x)) = 0,$$

which yields $u = 0$. The main result of this subsection is the following proposition.

Proposition 3.8. *Let A_ϕ and \hat{A}_p be as above. Then $(A_\phi, \hat{A}_p, \langle, \rangle)$ forms a Plancherel triple, where the bilinear form is inherited from the one on the pair (A, \hat{A}) .*

Proof. Since $(A_\phi)' = \hat{A}_p$, the bilinear form \langle, \rangle on the pair (A_ϕ, \hat{A}_p) is non-degenerate. Now we check that the triple $(A_\phi, \hat{A}_p, \langle, \rangle)$ verifies the conditions (1)-(4) of Definition 3.1. For simplicity, in the sequel we shall use \langle, \rangle to denote the bilinear forms on the different pairs (A, \hat{A}) , (A_ϕ, \hat{A}_p) and their corresponding tensor products $(A \otimes A, \hat{A} \otimes \hat{A})$ and $(A_\phi \otimes A_\phi, \hat{A}_p \otimes \hat{A}_p)$. The readers can distinguish them easily. We shall use $h := h_A$ and $\hat{h} := h_B$ to denote the Haar states on \mathbb{G} and $\hat{\mathbb{G}}$, respectively.

- (1) In this case, we claim that the comultiplications on A_ϕ and \hat{A}_p are respectively $\Delta_\phi := (\mathbb{E}_\phi \otimes \mathbb{E}_\phi)\Delta|_{A_\phi}$ and $\hat{\Delta}_p := (p \otimes p)\hat{\Delta}|_{\hat{A}_p}(\cdot)(p \otimes p)$. Then automatically they are positive. Indeed, by definition,

$$\langle \Delta_{A_\phi}(a), x \otimes y \rangle = \langle a, xy \rangle = (x \otimes y)\Delta(a), \quad a \in A_\phi, x, y \in \hat{A}_p.$$

By Lemma 3.7, we have $x = x\mathbb{E}_\phi$ and $y = y\mathbb{E}_\phi$. Thus $(x \otimes y)\Delta(a) = (x \otimes y)\Delta_\phi(a)$ and

$$\langle \Delta_{A_\phi}(a), x \otimes y \rangle = \langle \Delta_\phi(a), x \otimes y \rangle, \quad a \in A_\phi, x, y \in \hat{A}_p.$$

Since \langle, \rangle is non-degenerate, we have $\Delta_{A_\phi} = \Delta_\phi$. This proves the claim. Similarly, one can show $\Delta_{\hat{A}_p} = \hat{\Delta}_p$.

- (2) The counits on A_ϕ and \hat{A}_p are respectively $\epsilon_\phi := \epsilon|_{A_\phi}$ and $\hat{\epsilon}_p := \hat{\epsilon}|_{\hat{A}_p}$. Here ϵ and $\hat{\epsilon}$ are respectively the counits on A and \hat{A} . In fact, by definition,

$$\epsilon_{A_\phi} = \langle \cdot, 1_{\hat{A}_p} \rangle = \langle \cdot, 1_{\hat{A}} \rangle|_{A_\phi} = \epsilon_\phi, \quad \epsilon_{\hat{A}_p} = \langle 1_{A_\phi}, \cdot \rangle = \langle 1_A, \cdot \rangle|_{\hat{A}_p} = \hat{\epsilon}_p.$$

Then it is easy to check that $\epsilon_\phi : A_\phi \rightarrow \mathbb{C}$ and $\hat{\epsilon}_p : \hat{A}_p \rightarrow \mathbb{C}$ are both *-homomorphisms.

- (3) On the one hand, the support projection $p_{\hat{A}}$ of $\hat{\epsilon} = \epsilon_{\hat{A}}$ verifies

$$p_{\hat{A}}p = pp_{\hat{A}} = \hat{\epsilon}(p)p_{\hat{A}} = \phi(1_A)p_{\hat{A}} = p_{\hat{A}}.$$

So $p_{\hat{A}} \in \hat{A}_p$. Moreover,

$$bp_{\hat{A}} = p_{\hat{A}}b = \hat{\epsilon}(b)p_{\hat{A}} = \hat{\epsilon}_p(b)p_{\hat{A}}, \quad b \in \hat{A}_p.$$

Therefore the support projection of $\hat{\epsilon}_p$ is $p_{\hat{A}_p} = p_{\hat{A}}$. Thus the Haar functional on A_ϕ is

$$h_\phi := h_{A_\phi} = \langle \cdot, p_{\hat{A}_p} \rangle = \langle \cdot, p_{\hat{A}} \rangle|_{A_\phi} = h|_{A_\phi}.$$

On the other hand, by Lemma 3.6,

$$\mathbb{E}_\phi(p_A)\mathbb{E}_\phi(a) = \mathbb{E}_\phi(p_A\mathbb{E}_\phi(a)) = \epsilon(\mathbb{E}_\phi(a))\mathbb{E}_\phi(p_A) = \epsilon_\phi(\mathbb{E}_\phi(a))\mathbb{E}_\phi(p_A), \quad a \in A.$$

Similarly, $\mathbb{E}_\phi(p_A)\mathbb{E}_\phi(a) = \epsilon_\phi(\mathbb{E}_\phi(a))\mathbb{E}_\phi(p_A)$, $a \in A$. By choosing $a = p_A$, we obtain that $\mathbb{E}_\phi(p_A)^2 = \phi(p_A)\mathbb{E}_\phi(p_A)$. So $q := \frac{1}{\phi(p_A)}\mathbb{E}_\phi(p_A)$ is a self-adjoint projection in A_ϕ such that

$$qa = aq = \epsilon_\phi(a)q, \quad a \in A_\phi.$$

That is, $p_{A_\phi} = q$ is the support projection of ϵ_ϕ . So the Haar functional on \hat{A}_p is

$$\hat{h}_p := h_{\hat{A}_p} = \langle p_{A_\phi}, \cdot \rangle = \frac{1}{\phi(p_A)} \langle \mathbb{E}_\phi(p_A), \cdot \rangle = \frac{1}{\phi(p_A)} \langle p_A, \cdot \rangle|_{\hat{A}_p} = \frac{1}{\phi(p_A)} \hat{h}|_{\hat{A}_p}.$$

Hence the Haar functionals h_ϕ and \hat{h}_p are faithful, positive and tracial.

- (4) For any $a \in A_\phi$, we claim that $\mathcal{F}_A(a) = h(\cdot a) \in \hat{A}_p$, i.e., $\mathcal{F}_A(a)$ is ϕ -bi-invariant. Indeed, by (2.1),

$$(\phi \otimes h(\cdot a))\Delta(x) = (\phi \otimes h)(\Delta(x)(1 \otimes a)) = (\phi \circ S \otimes h)((1 \otimes x)\Delta(a)), \quad a \in A_\phi, x \in A.$$

Since $\phi = \phi S$ and $\mathbb{E}_\phi(a) = a$, we have

$$(\phi \otimes h(\cdot a))\Delta(x) = (\phi \otimes h)((1 \otimes x)\Delta(a)) = h(x\mathbb{E}_\phi^\ell(a)) = h(xa), \quad a \in A_\phi, x \in A.$$

Hence $\phi \star h(\cdot a) = h(\cdot a)$, for all $a \in A_\phi$. From (2.2) and $\mathbb{E}_\phi^r(a) = a$ one can deduce in a similar way that $h(\cdot a) \star \phi = h(\cdot a)$. Thus $\mathcal{F}_A(a) = h(\cdot a)$ is ϕ -bi-invariant for all $a \in A_\phi$. This proves our claim. Now for any $a \in A_\phi$ we have

$$\langle x, \mathcal{F}_{A_\phi}(a) \rangle = h_\phi(xa) = h(xa) = \langle x, \mathcal{F}_A(a) \rangle, \quad x \in A_\phi.$$

Since $\mathcal{F}_A(a) \in \hat{A}_p$, $\mathcal{F}_{A_\phi}(a)$ is the image of $\mathcal{F}_A(a)$ under the natural inclusion $\hat{A}_p \rightarrow \hat{A}$. Hence the Parseval's identity (2.4) on the pair (A, \hat{A}) yields

$$\hat{h}_p(\mathcal{F}_{A_\phi}(a_1)\mathcal{F}_{A_\phi}(a_2)^*) = \hat{h}(\mathcal{F}_A(a_1)\mathcal{F}_A(a_2)^*) = ch(a_1a_2^*) = ch_\phi(a_1a_2^*), \quad a_1, a_2 \in A_\phi.$$

Similarly, one can show that

$$h_\phi(\mathcal{F}_{\hat{A}_p}(b_1)\mathcal{F}_{\hat{A}_p}(b_2)^*) = c'\hat{h}_p(b_1b_2^*), \quad b_1, b_2 \in \hat{A}_p,$$

for some constant $c' > 0$. □

3.3 Poisson states on compact quantum groups

Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group. Recall that A is always viewed as $C^u(\mathbb{G})$. Denote by $\mathcal{S}(A)$ the set of all states on A . For each $\phi \in \text{Idem}(\mathbb{G})$, we say that $\{\omega_t\}_{t \geq 0}$ is a *convolution semigroup of functionals* on A starting from ϕ if

- (1) $\omega_t \in A'$ for each $t \geq 0$.
- (2) $\omega_{s+t} = \omega_s \omega_t$ for all $s, t \geq 0$.
- (3) $\omega_0 = \phi$.

If moreover, each $\omega_t \in \mathcal{S}(A)$, we call $\{\omega_t\}_{t \geq 0}$ a *convolution semigroup of states* starting from ϕ . We say that the convolution semigroup of states $\{\omega_t\}_{t \geq 0}$ is *norm continuous* if

$$\lim_{t \rightarrow 0^+} \|\omega_t - \phi\| = 0.$$

Recall here that $\|u\|$ denotes the norm of $u \in A'$ as a functional on A . Moreover, it is a Banach norm, since

$$\|uv\| = \|(u \otimes v)\Delta\| \leq \|u\|\|v\|, \quad u, v \in A'.$$

For a ϕ -bi-invariant functional $u \in A'$ define

$$\exp_\phi(u) := \phi + \sum_{n \geq 1} \frac{u^n}{n!}.$$

Then it is easy to check that $\{\exp_\phi(tu)\}_{t \geq 0}$ form a norm continuous convolution semigroup of functionals. We aim to find sufficient and necessary conditions on u such that $\{\exp_\phi(tu)\}_{t \geq 0}$ is a convolution semigroup of states. For this we make some notations. A functional $u \in A'$ is called *Hermitian* if $u(x^*) = \overline{u(x)}$ for all x ; it is further called *conditionally positive definite with respect to ϕ* if $u(x^*x) \geq 0$ for all x such that $\phi(x^*x) = 0$. The main theorem in this section is as follows.

Theorem 3.9. *Suppose that $\mathbb{G} = (A, \Delta)$ is a compact quantum group. Let $\phi \in \text{Idem}(\mathbb{G})$. Then for $u \in A'$, the following statements are equivalent.*

- (1) $u(1_A) = 0$, u is ϕ -bi-invariant and conditionally positive definite w.r.t. ϕ .
- (2) $u = r(v - \phi)$, where $r \geq 0$ and v is a ϕ -bi-invariant state.

The following proposition proves Theorem 3.9 on the level of unital C^* -algebras. It can be considered as a special case of Theorem 3.9 when $\phi = \epsilon$ is the counit. In this case each $u \in A'$ is ϵ -bi-invariant and $\phi = \epsilon$ is a character.

Proposition 3.10. *Let A be a unital C^* -algebra with ϵ a character. Then for any non-zero bounded linear functional u on A such that $u(1_A) = 0$ and $u(x^*x) \geq 0$ for all $x \in A$ such that $\epsilon(x^*x) = 0$, we have $u = r(v - \epsilon)$, where $r > 0$ and v is a state.*

Proof. Note first that $\epsilon(x^*x) = |\epsilon(x)|^2$. So $\epsilon(x^*x) = 0$ if and only if $x \in \ker \epsilon = \{x : \epsilon(x) = 0\}$. Let $u_0 := u|_{\ker \epsilon}$ be the restriction of u to $\ker \epsilon$. By assumption, u_0 is a bounded linear positive functional on the ideal $\ker \epsilon$. So it admits a unique positive linear extension \widetilde{u}_0 to A such that $\widetilde{u}_0|_{\ker \epsilon} = u_0$ and $\|\widetilde{u}_0\| = \|u_0\|$. Hence for any $x \in A$, we have $x - \epsilon(x)1_A \in \ker \epsilon$ and thus

$$u(x) = u(x - \epsilon(x)1_A) = u_0(x - \epsilon(x)1_A) = \widetilde{u}_0(x - \epsilon(x)1_A) = r(v - \epsilon)(x),$$

where $r := \|\widetilde{u}_0\| = \|u_0\| > 0$ and $v := \frac{1}{r}\widetilde{u}_0$ is a state. □

Now we are ready to prove Theorem 3.9. The idea is to restrict the problem to A_ϕ , and then transfer the decomposition from A_ϕ to A .

Proof of Theorem 3.9. The direction (2) \Rightarrow (1) is clear. To prove (1) \Rightarrow (2), suppose $u \neq 0$ and write $u = u|_{A_\phi} \mathbb{E}_\phi$ by Lemma 3.7. Note that $\epsilon|_{A_\phi}$ is a character on the unital C^* -algebra A_ϕ . From the definition of u , we have $u|_{A_\phi}(1_{A_\phi}) = 0$. Moreover, for any $x \in A$ such that $\epsilon|_{A_\phi}(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) = 0$, we have by Lemma 3.5 and Lemma 3.7 that

$$0 = \epsilon|_{A_\phi}(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) = \epsilon|_{A_\phi} \mathbb{E}_\phi(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) = \phi(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)).$$

Again, by Lemma 3.5 and Lemma 3.7, the conditionally positive definiteness of u with respect to ϕ implies

$$u|_{A_\phi}(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) = u|_{A_\phi} \mathbb{E}_\phi(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) = u(\mathbb{E}_\phi(x)^* \mathbb{E}_\phi(x)) \geq 0.$$

So we have by Proposition 3.10 that $u|_{A_\phi} = r(w - \epsilon|_{A_\phi})$ with $r > 0$ and w a state on A_ϕ . Set $v := w\mathbb{E}_\phi$, then v is, by Lemma 3.7, a ϕ -bi-invariant state on A such that

$$u = u|_{A_\phi} \mathbb{E}_\phi = r(w\mathbb{E}_\phi - \epsilon|_{A_\phi} \mathbb{E}_\phi) = r(v - \phi),$$

as desired. \square

Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group. Let $\phi \in \text{Idem}(\mathbb{G})$. We denote by $\mathcal{N}_\phi(\mathbb{G})$ the class of functionals $u \in A'$ that satisfy the conditions (2) in Theorem 3.9. Then for each $u \in \mathcal{N}_\phi(\mathbb{G})$, $\omega := \exp_\phi(u)$ is a state. In fact, since $u = r(v - \phi)$ for some $r > 0$ and ϕ -bi-invariant state v , we have by Lemma 3.18 that

$$\exp_\phi(u) = \exp_\phi(r(v - \phi)) = \exp_\phi(rv) \exp_\phi(-r\phi) = e^{-r} \exp_\phi(rv).$$

The fact that it is a positive functional follows from the definition of \exp_ϕ and the fact that rv is a positive functional. Moreover, since $u(1_A) = 0$, we get

$$\exp_\phi(u)(1_A) = \phi(1_A) = 1.$$

Definition 3.11. Let \mathbb{G} be a compact quantum group. Let $\phi \in \text{Idem}(\mathbb{G})$. Set

$$\mathcal{P}_\phi(\mathbb{G}) := \{\exp(u) : u \in \mathcal{N}_\phi(\mathbb{G})\},$$

and denote $\mathcal{P}(\mathbb{G}) := \bigcup_{\phi \in \text{Idem}(\mathbb{G})} \mathcal{P}_\phi(\mathbb{G})$. Then any $\omega \in \mathcal{P}(\mathbb{G})$ is said to be of Poisson type, or a Poisson state on \mathbb{G} .

Recall that any norm continuous convolution semigroup of states $\{\omega_t\}_{t \geq 0}$ on a compact quantum group $\mathbb{G} = (A, \Delta)$ can be recovered by exponentiation with a bounded generator $u := \lim_{t \rightarrow 0^+} \frac{1}{t}(\omega_t - \omega_0)$. It is not difficult to see that $u(1_A) = 0$ and u is conditionally positive definite with respect to ω_0 , since these hold for each $\frac{1}{t}(\omega_t - \omega_0)$, $t > 0$. Then together with Theorem 3.9 we have the following result.

Theorem 3.12. Let ϕ be an idempotent state on a compact quantum group $\mathbb{G} = (A, \Delta)$. For any non-zero bounded linear functional ω on A such that $\omega\phi = \phi\omega = \omega$, the following are equivalent

- (1) $\omega = \omega_1$ with $\{\omega_t\}_{t \geq 0}$ a norm continuous convolution semigroup of states such that $\omega_0 = \phi$;

(2) $\omega = \exp_\phi(u)$, where $u \in A'$ is ϕ -bi-invariant, $u(1_A) = 0$, and $u(x^*x) \geq 0$ for all $x \in A$ such that $\phi(x^*x) = 0$;

(3) $\omega = \exp_\phi(u)$, where $u = r(v - \phi)$, with $r > 0$ and v a ϕ -bi-invariant state on A .

Remark 3.13. The convolution semigroup of states $\{\omega_t\}_{t \geq 0}$ on a compact quantum group \mathbb{G} is said to be weakly continuous if $\omega_t(a) \rightarrow \omega_0(a)$, $t \rightarrow 0^+$ for any $a \in C(\mathbb{G})$. Clearly norm continuous convolution semigroup of states is weakly continuous. When \mathbb{G} is a finite quantum group, the converse also holds. But for general compact quantum group \mathbb{G} , there exists weakly continuous convolution semigroup of states which is not norm continuous. In this case, the generator is unbounded.

3.4 Infinitely divisible states on finite quantum groups

In this section we prove the main result.

Definition 3.14. Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group. A state $\omega \in \mathcal{S}(A)$ is said to be infinitely divisible if $\omega = \omega_n^n$ for some $\omega_n \in \mathcal{S}(A)$ and for all $n \geq 1$. We use $\mathcal{I}(\mathbb{G})$ to denote the set of all infinitely divisible states on \mathbb{G} .

Clearly Poisson states are infinitely divisible. In fact, for any $\omega \in \mathcal{P}(\mathbb{G})$, we have $\omega \in \mathcal{P}_\phi(\mathbb{G})$ for some $\phi \in \text{Idem}(\mathbb{G})$. Then we may write ω as $\omega = \exp_\phi(u)$ with $u \in \mathcal{N}_\phi(\mathbb{G})$. Note that for any $n \geq 1$, $\frac{u}{n} \in \mathcal{N}_\phi(\mathbb{G})$, so $\omega_n := \exp_\phi(\frac{u}{n})$ is also a state. Moreover, by Lemma 3.18, we have $\omega = \omega_n^n$. So ω is infinitely divisible.

Our main result in this section is that any infinitely divisible state on a finite quantum group is a Poisson state. From now on, unless stated otherwise, $\mathbb{G} = (A, \Delta)$ always denotes a finite quantum group.

The following lemma is well-known, and the proof follows from standard arguments.

Lemma 3.15. Let $A = \bigoplus_{k=1}^m \mathbb{M}_{n_k}(\mathbb{C})$ with matrix units $\{e_{ij}^k : 1 \leq i, j \leq n_k, 1 \leq k \leq m\}$. Denote the dual basis by $\{\omega_{ij}^k\}$. Then for any $\omega = \sum_{k=1}^m \sum_{i,j=1}^{n_k} a_{ij}^{(k)} \omega_{ij}^k$, ω is a positive linear functional if and only if $[a_{ij}^{(k)}]_{i,j=1}^{n_k}$ is positive semi-definite for each k . In this case, $\|\omega\| = \sum_{k=1}^m \sum_{i=1}^{n_k} a_{ii}^{(k)}$.

As a direct consequence, we have the following decomposition, which is quite easy but very helpful.

Corollary 3.16. Let $A = \bigoplus_{k=1}^m \mathbb{M}_{n_k}(\mathbb{C})$ with matrix units $\{e_{ij}^k : 1 \leq i, j \leq n_k, 1 \leq k \leq m\}$. Denote the dual basis by $\{\omega_{ij}^k\}$. Let $\omega = \sum_{k=1}^m \sum_{i,j=1}^{n_k} a_{ij}^{(k)} \omega_{ij}^k$ such that for each k either $[a_{ij}^{(k)}]_{i,j=1}^{n_k} \geq 0$ or $[a_{ij}^{(k)}]_{i,j=1}^{n_k} \leq 0$. Then $\omega_+ := \sum_{k \in \Lambda} \sum_{i,j=1}^{n_k} a_{ij}^{(k)} \omega_{ij}^k$ and $\omega_- := \sum_{k \notin \Lambda} \sum_{i,j=1}^{n_k} a_{ij}^{(k)} \omega_{ij}^k$ are positive functionals on A such that

$$\omega = \omega_+ - \omega_- \text{ and } \|\omega\| = \|\omega_+\| + \|\omega_-\|,$$

where Λ is the set of all the k 's such that $[a_{ij}^{(k)}]_{i,j=1}^{n_k} \geq 0$.

Another important corollary is as follows.

Corollary 3.17. Let (A, B, \langle, \rangle) be a Plancherel triple. Then for any positive linear functional $u \in A'$, we have

$$h_B(u) \leq \epsilon_B(u).$$

Proof. Suppose that $A = \bigoplus_{\alpha=1}^m \mathbb{M}_{n_\alpha}(\mathbb{C})$ with the matrix units $\{e_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$. By Lemma 3.15 we may write u as $u = \sum_{\alpha=1}^m \sum_{i,j=1}^{n_\alpha} a_{ij}^\alpha \widetilde{e_{ij}^\alpha}$, where each $[a_{ij}^\alpha]_{i,j=1}^{n_\alpha}$ is positive semi-definite and $\{\widetilde{e_{ij}^\alpha}\}$ is the dual basis of $\{e_{ij}^\alpha\}$. Suppose that $\widetilde{e^{\alpha_0}} = 1_B$. Then by (3.3) and (3.4), we have

$$h_B(u) = a^{\alpha_0} \leq \sum_{\alpha=1}^m \sum_{i=1}^{n_\alpha} a_{ii}^\alpha = \epsilon_B(u). \quad \square$$

Let $\mathbb{G} = (A, \Delta)$ be a finite quantum group. Then for any $u \in A' = \hat{A}$ we denote by $\|u\|_{\hat{A}}$ the C^* -norm of u as an element in C^* -algebra \hat{A} . Recall that $\|u\|$ is the norm of u as a functional. Moreover, we have $\|u\|_{\hat{A}} \leq \|u\|$.

Let ϕ be an idempotent state on finite quantum group $\mathbb{G} = (A, \Delta)$. For any $u \in A'$ such that $u = u\phi = \phi u$ and $\|u - \phi\| < 1$, define the *logarithm of u with respect to ϕ* as

$$\log_\phi(u) := - \sum_{k \geq 1} \frac{(\phi - u)^k}{k}.$$

Then we have the following properties of logarithm and exponential.

Lemma 3.18. *Suppose that $\mathbb{G} = (A, \Delta)$ is a finite quantum group. Let ϕ be an idempotent state on A , then for any bounded linear functionals u, v on A such that $u = u\phi = \phi u$ and $v = v\phi = \phi v$, we have*

- (1) $\exp_\phi(\log_\phi(u)) = u$, if $\|u - \phi\| < 1$.
- (2) $\log_\phi(\exp_\phi(u)) = u$, if $\|u\| < \log 2$.
- (3) $\exp_\phi(u + v) = \exp_\phi(u) \exp_\phi(v)$ if $uv = vu$.
- (4) $\log_\phi(uv) = \log_\phi(u) + \log_\phi(v)$, if $uv = vu$ and the following holds:

$$\|u - \phi\| < 1, \quad \|v - \phi\| < 1, \quad \text{and} \quad \|uv - \phi\| < 1.$$

- (5) If moreover, u is a state such that

$$\|u - \phi\| < \frac{1}{2} \quad \text{and} \quad \|u^n - \phi\| < \frac{1}{2}$$

for some $n \geq 1$, then

$$\|u^k - \phi\| < \frac{1}{2} \quad \text{for all } 1 \leq k \leq n.$$

Consequently, in such a case we have

$$\log_\phi(u^k) = k \log_\phi(u) \quad \text{for all } 1 \leq k \leq n.$$

Proof. (1)-(4) are direct and hold for all Banach algebras. To show (5), let u_ϕ be the restriction of u to A_ϕ . Then by Lemma 3.7, u_ϕ is a state on a finite-dimensional C^* -algebra A_ϕ . Moreover,

$$\|u - \phi\| = \|(u_\phi - \epsilon_\phi)\mathbb{E}_\phi\| = \|u_\phi - \epsilon_\phi\|,$$

where ϵ_ϕ denotes the restriction of counit ϵ of A to A_ϕ . Write $A_\phi = \bigoplus_{k=1}^m \mathbb{M}_{n_k}(\mathbb{C})$ with matrix units $\{e_{ij}^k : 1 \leq i, j \leq n_k, 1 \leq k \leq m\}$. Let $\{\omega_{ij}^k\}$ be the dual basis. By Lemma

3.15, $u_\phi = \sum_{k=1}^m \sum_{i,j=1}^{n_k} b_{ij}^{(k)} \omega_{ij}^k$ with $[b_{ij}^{(k)}]_{i,j=1}^{n_k} \geq 0$ and $\|u_\phi\| = \sum_{k=1}^m \sum_{i=1}^{n_k} b_{ii}^{(k)} = 1$. Since ϵ_ϕ is a character on A_ϕ , there exists k_0 such that $n_{k_0} = 1$ and $\omega^{k_0} = \epsilon_\phi$. Thus $u_\phi - \epsilon_\phi = (b^{(k_0)} - 1)\epsilon_\phi + \sum_{k \neq k_0} \sum_{i,j=1}^{n_k} b_{ij}^{(k)} \omega_{ij}^k$ verifies the condition of Corollary 3.16 and it follows that

$$\|u_\phi - \epsilon_\phi\| = 1 - b^{(k_0)} + \sum_{k \neq k_0} \sum_{i=1}^{n_k} b_{ii}^{(k)} = 2 - 2b^{(k_0)} = -2(u_\phi - \epsilon_\phi)(e^{k_0}).$$

So for $v_1 := u - \phi$ we have $\|v_1\| = \|w_1\| = -2w_1(e^{k_0})$, where $w_1 = v_1|_{A_\phi}$. Similarly for $v_j := u^j - \phi$ and $w_j := v_j|_{A_\phi}$ we have

$$\|v_j\| = \|w_j\| = -2w_j(e^{k_0}), \quad j \geq 1. \quad (3.8)$$

Now we show (5) by the induction argument. Clearly it holds for $n = 1$. Suppose for now that it holds for n . Set $r := \|v_1\|$, $s := \|v_n\|$ and $t := \|v_{n+1}\|$. From $(v_1 + \phi)(v_n + \phi) = v_{n+1} + \phi$ it follows that $v_{n+1} = v_1 + v_n + v_1 v_n$ and thus by Lemma 3.7 (4) that $w_{n+1} = w_1 + w_n + w_1 w_n$. This, together with (3.8) and Lemma 3.7 (1), yields that

$$t = r + s - 2(w_1 w_n)(e^{k_0}) \geq r + s - 2\|w_1 w_n\| = r + s - 2\|v_1 v_n\| \geq r + s - 2rs.$$

Then

$$(1 - 2r)(1 - 2s) = 4rs - 2r - 2s + 1 \geq 1 - 2t.$$

By assumption, $1 - 2r, 1 - 2t > 0$, so $1 - 2s > 0$. Hence u and u^n verify the conditions in (4), and we obtain

$$\log_\phi(u^{n+1}) = \log_\phi(u) + \log_\phi(u^n) = \log_\phi(u) + n \log_\phi(u) = (n+1) \log_\phi(u),$$

where in the second equality we have used the induction for n . This finishes the proof for $n+1$ and then shows (5). \square

Remark 3.19. In fact, to prove (5) we have used the fact that $\|u + v\| = \|u\| + \|v\|$ for all $u, v \in \mathcal{N}_\phi(\mathbb{G})$.

Proposition 3.20. Let ω be an infinitely divisible state on a finite quantum group $\mathbb{G} = (A, \Delta)$. Let ϕ be an idempotent state on A . Assume that there exists a sequence $\{\omega_{m_j}\}_{j \geq 0}$ of roots of states of ω , with $\omega = \omega_{m_j}^{m_j}$, for all j , such that

- (1) $\{m_j\}_{j \geq 0}$ is strictly increasing;
- (2) $\omega_{m_j} = \omega_{m_j} \phi = \phi \omega_{m_j}$ for all j ;
- (3) $\omega_{m_j} = \omega_{m_{j+1}}^{n_j}$ for some positive integer $n_j, j \geq 0$;
- (4) $\omega_{m_j} \rightarrow \phi$, as $j \rightarrow \infty$.

Then $\omega \in \mathcal{P}_\phi(\mathbb{G})$.

Proof. Assume that $\{\omega_{m_j}\}$ contains infinitely many different elements, otherwise $\omega = \phi \in \mathcal{P}_\phi(\mathbb{G})$. By (4), we can choose $j_0 > 0$ such that $\|\omega_{m_j} - \phi\| < 1/2$ for all $j \geq j_0$. This inequality, together with (2), allows us to define

$$v_0 := \log_\phi(\omega_{m_{j_0}}), \quad \text{and } v := m_{j_0} v_0.$$

Then by the definition of $\omega_{m_{j_0}}$ and Lemma 3.18 (1)(2),

$$\omega = \omega_{m_{j_0}}^{m_{j_0}} = \left(\exp_\phi(\log_\phi(\omega_{m_{j_0}})) \right)^{m_{j_0}} = \exp_\phi(m_{j_0} v_0) = \exp_\phi(v).$$

To prove $\omega \in \mathcal{P}_\phi(\mathbb{G})$, it suffices to show that $v \in \mathcal{N}_\phi(\mathbb{G})$. For this we check that v verifies Theorem 3.9 (1). Clearly, $v(1_A) = 0$, since ω_{j_0} is a state. By the definition of logarithm, $v = v\phi = \phi v$. It remains to show that for any $x \in A$ such that $\phi(x^*x) = 0$, we have $v_0(x^*x) \geq 0$. By (3) we have

$$\omega_{m_{j_0}} = \omega_{m_j}^{N_j}, \quad j \geq j_0,$$

where $N_j := n_{j_0} \cdots n_{j-1}$. Recall that for all $j \geq j_0$, $\|\omega_{m_j} - \phi\| < 1/2$. Thus by Lemma 3.18 (5) we have

$$\log_\phi(\omega_{m_j}) = \frac{1}{N_j} \log_\phi(\omega_{m_{j_0}}) = \frac{v_0}{N_j},$$

and by Lemma 3.18 (1)

$$\omega_{m_j} = \exp_\phi \left(\frac{v_0}{N_j} \right), \quad j \geq j_0.$$

The condition (1) implies that $N_j \rightarrow \infty$ as $j \rightarrow \infty$. Now for any $x \in A$ such that $\phi(x^*x) = 0$, we have

$$0 \leq \omega_{m_j}(x^*x) = \phi(x^*x) + \frac{v_0(x^*x)}{N_j} + \sum_{m \geq 2} \frac{v_0^m(x^*x)}{N_j^m \cdot m!} = \frac{v_0(x^*x)}{N_j} + O\left(\frac{1}{N_j^2}\right),$$

for all $j \geq j_0$. Hence

$$v_0(x^*x) + O\left(\frac{1}{N_j}\right) \geq 0, \quad j \geq j_0.$$

Letting $j \rightarrow \infty$, we have $v_0(x^*x) \geq 0$, which ends the proof. \square

As this proposition suggests, to show that an infinitely divisible state is of Poisson type, it is important to capture the idempotent state which the infinitely divisible state is “supported on”. For this we need two lemmas. The first one is an easy fact in matrix theory.

Lemma 3.21. *Let $P \in \mathbb{M}_n(\mathbb{C})$ be a self-adjoint projection. Let $A, B \in \mathbb{M}_n(\mathbb{C})$ be such that $A = AP = PA$, $AB = P$ and $\|A\| \leq 1$, $\|B\| \leq 1$. Here $\|\cdot\|$ denote the C^* -norm in matrix algebra. Then $A^*A = AA^* = P$. Consequently, if u and v are states on a finite quantum group $\mathbb{G} = (A, \Delta)$ such that $u = u\phi = \phi u$ and $uv = \phi$, where ϕ is an idempotent state on \mathbb{G} , then $u^*u = uu^* = \phi$.*

Proof. Since P is a self-adjoint projection, we may assume without loss of generality that

$$P = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$

where I_r is the identity in $\mathbb{M}_r(\mathbb{C})$ with $r = \text{rank}(P)$. From $A = AP = PA$ and $AB = P$ it follows

$$A = \begin{pmatrix} A_r & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} B_r & * \\ * & * \end{pmatrix},$$

with $A_r B_r = I_r$. Note that

$$1 = \|I_r\| = \|A_r B_r\| \leq \|A_r\| \|B_r\| \leq \|A\| \|B\| \leq 1.$$

So $\|A_r\| = \|B_r\| = 1$. This is to say,

$$\|A_r^* A_r\| = 1 = \|B_r B_r^*\| = \|(A_r^* A_r)^{-1}\|.$$

Then all the eigenvalues of $A_r^*A_r$ must be 1 and thus $A_r^*A_r = I_r$. Hence $B_r = A_r^*$ and thus $A^*A = AA^* = P$.

The remaining part follows from the facts that $p = \phi$ is a self-adjoint projection in \hat{A} and

$$\|u\|_{\hat{A}} \leq \|u\| = 1, \quad \|v\|_{\hat{A}} \leq \|v\| = 1.$$

□

Lemma 3.22. *Let (A, B, \langle, \rangle) be a Plancherel triple. Suppose that $u \in B$ is a state on A such that $uu^* = u^*u = \epsilon_A$, where ϵ_A is the counit of A . Then u is an n -th root of ϵ_A for some $n \leq \dim B$.*

Proof. Suppose that $A = \bigoplus_{\alpha=1}^m \mathbb{M}_{n_\alpha}(\mathbb{C})$ with the matrix units $\{e_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$. Let $\{\widetilde{e}_{ij}^\alpha\}$ be the dual basis. Then by Lemma 3.15 we can write u as

$$u = \sum_{\alpha=1}^m p_\alpha \sum_{i,j=1}^{n_\alpha} a_{ij}^\alpha \widetilde{e}_{ij}^\alpha,$$

where $p_\alpha \geq 0$, $\sum_{\alpha=1}^m p_\alpha = 1$ and $[a_{ij}^\alpha]_{i,j=1}^{n_\alpha}$ positive semi-definite with trace one. Let α_0 be such that $\widetilde{e}^{\alpha_0} = 1_B$. Then we can write $u = p_{\alpha_0} \widetilde{e}^{\alpha_0} + v$ with $v = \sum_{\alpha \neq \alpha_0} p_\alpha \sum_{i,j=1}^{n_\alpha} a_{ij}^\alpha \widetilde{e}_{ij}^\alpha$ such that $\|v\| = \sum_{\alpha \neq \alpha_0} p_\alpha = 1 - p_{\alpha_0}$. Note that $uu^* = p_{\alpha_0}^2 \widetilde{e}^{\alpha_0} + p_{\alpha_0}(v + v^*) + vv^*$. Then by (3.3), $h_B(v) = h_B(v^*) = 0$. Since v and v^* are both positive functionals, $vv^*(\cdot) = \langle \Delta_A(\cdot), v \otimes v^* \rangle$ is also a positive functional on A . Hence we have by Corollary 3.17 that

$$h_B(vv^*) \leq \epsilon_B(vv^*) = |\epsilon_B(v)|^2 = (1 - p_{\alpha_0})^2.$$

So we have

$$1 = h_B(1_B) = h_B(uu^*) = p_{\alpha_0}^2 + h_B(vv^*) \leq p_{\alpha_0}^2 + (1 - p_{\alpha_0})^2 = 1 - 2p_{\alpha_0} + 2p_{\alpha_0}^2,$$

which yields $p_{\alpha_0}(p_{\alpha_0} - 1) \geq 0$. Recall that $0 \leq p_{\alpha_0} \leq 1$, hence either $p_{\alpha_0} = 0$ or $p_{\alpha_0} = 1$. That is to say, either $h_B(u) = 0$ or $u = \epsilon_A$. Since for any $n \geq 1$, u^n is again a state such that $u^n u^{*n} = \epsilon_A$, we obtain, by a similar argument, that either $h_B(u^n) = 0$ or $u^n = \epsilon_A$.

If u is not an n -th root of ϵ_A for all $1 \leq n \leq \dim B$, then we have

$$h_B(u^n) = 0, \quad n = 1, 2, \dots, \dim B. \quad (3.9)$$

Note that we may choose $m \leq \dim B$ such that u is unitary in $\mathbb{M}_m(\mathbb{C})$. Set $P(\lambda) := \det(\lambda I_m - u) = \sum_{i=0}^m a_i \lambda^i$, then Cayley-Hamilton Theorem implies that $P(u) = 0$, where I_m denotes the identity matrix in $\mathbb{M}_m(\mathbb{C})$. Since u is unitary in $\mathbb{M}_m(\mathbb{C})$, we have $a_0 = (-1)^m \det(u) \neq 0$. But by (3.9)

$$a_0 h_B(I_m) = a_0 h_B(I_m) + \sum_{i=1}^m a_i h_B(u^i) = h_B(P(u)) = 0.$$

Thus $a_0 = 0$, which leads to a contradiction. So we must have $u^m = \epsilon_A$ for some $1 \leq m \leq \dim B$. □

The following proposition, gathering the main ingredients of preceding lemmas, will be used to prove Theorem 3.24.

Proposition 3.23. *Let $\mathbb{G} = (A, \Delta)$ be a finite quantum group with dual $\hat{\mathbb{G}} = (\hat{A}, \hat{\Delta})$. Suppose that $u, v \in \mathcal{S}(A)$ and $\phi \in \text{Idem}(\mathbb{G})$ are such that $u = u\phi = \phi u$ and $uv = \phi$. Then there exists a positive integer $m \leq \dim \hat{A}$ such that $u^m = \phi$.*

Proof. From Lemma 3.21 it follows $u^*u = uu^* = \phi$. Let u_ϕ and ϵ_ϕ be the restrictions of u and the counit ϵ of A to A_ϕ , respectively. From Proposition 3.8 $(A_\phi, \hat{A}_\phi, \langle, \rangle)$ forms a Plancherel triple. By Lemma 3.7, u_ϕ is a state on A_ϕ such that $u_\phi u_\phi^* = \epsilon_\phi$. So Lemma 3.22 implies $u_\phi^m = \epsilon_\phi$ for some $m \leq \dim \hat{A}_\phi \leq \dim \hat{A}$. Hence Lemma 3.7 gives $u^m = u_\phi^m \mathbb{E}_\phi = \epsilon_\phi \mathbb{E}_\phi = \phi$. \square

Now we are ready to prove the main result.

Theorem 3.24. *Let $\mathbb{G} = (A, \Delta)$ be a finite quantum group. Then $\mathcal{P}(\mathbb{G}) = \mathcal{I}(\mathbb{G})$.*

The first proof. $\mathcal{P}(\mathbb{G}) \subset \mathcal{I}(\mathbb{G})$ is clear. Let $\omega \in \mathcal{I}(\mathbb{G})$. We claim that for any positive integer $N \geq 2$, there exists a sequence $\{b_n\}_{n \geq 0}$ of roots of ω such that $b_0 = \omega, b_{n-1} = b_n^N, n \geq 1$. Indeed, since A is finite dimensional, the set of states $Z = \mathcal{S}(A)$ is compact with respect to the norm topology. Thus $\prod_{j \geq 0} Z_j$, where $Z_j = Z$ for all j , is compact with respect to the product topology. Let $a_n \in Z$ be any n -th root of ω for all $n \geq 0$. Then the sequence of non-empty closed sets

$$W_k := \bigcup_{j \geq k} \{a_{N^j}\} \times \{a_{N^{j-1}}\} \times \cdots \times \{a_{N^1}\} \times \prod_{i \geq j} Z_i, \quad k \geq 1,$$

is decreasing: $W_1 \supset W_2 \supset \cdots$, and thus any finite intersection of $\{W_k\}_{k \geq 1}$ is non-empty. By compactness of $\prod_{j \geq 0} Z_j$, $\bigcap_{k \geq 1} W_k \neq \emptyset$. Hence one can choose $(b_0, b_1, \dots) \in \bigcap_{k \geq 1} W_k$ such that

$$b_0 = \omega, \quad b_{n-1} = b_n^N, \quad n \geq 1.$$

This proves the claim.

Choose $N = (\dim \hat{A})! \geq 2$ and let $\{b_n\}_{n \geq 0}$ be as above. Since Z is compact, there exists a subsequence $\{c_j\}_{j \geq 0}$ of $\{b_i\}_{i \geq 0}$ such that c_j converges to some $c \in Z$. If we fix a non-negative integer i , we have $b_i = c_j^{r_j}$ for sufficient large j and some integer $r_j \geq N \geq 2$. That is,

$$b_i = c_j c_j^{r_j-1} = c_j^{r_j-1} c_j. \quad (3.10)$$

We can assume that $c_j^{r_j-1}$ converges to some $d_i \in Z$, otherwise consider some subsequence, since $\{c_j^{r_j-1}\}_{j \geq 0} \subset Z$. Thus letting $j \rightarrow \infty$ in (3.10), we have

$$b_i = c d_i = d_i c, \quad i \geq 0. \quad (3.11)$$

This implies $b_i \in cZ \cap Zc$ for all $i \geq 0$. From the choice of c_j we have $c_j \in cZ \cap Zc$ for all $j \geq 0$. Then for any i the corresponding $c_j^{r_j-1} \in cZ \cap Zc$ for all j , which implies that $d_i \in cZ \cap Zc$ by the compactness of $cZ \cap Zc$. Now consider (3.10) for $\{c_j\}_{j \geq 0}$, instead of $\{b_i\}_{i \geq 0}$, we obtain an updated version of (3.11):

$$c_j = c d'_j = d'_j c, \quad j \geq 0, \quad (3.12)$$

where $d'_j \in cZ \cap Zc$. Letting $j \rightarrow \infty$, consider the subsequence of $\{d'_j\}_{j \geq 0}$ if necessary, one obtains

$$c = c d = d c, \quad (3.13)$$

where $d \in cZ \cap Zc$ by the compactness of $cZ \cap Zc$. Suppose $d = c e$ for some $e \in Z$, then $d^2 = d c e = c e = d$, i.e., d is an idempotent state. By Proposition 3.23, we obtain $c^m = d$ for some $m \leq \dim \hat{A}$. Since our choice of N satisfies $m|N$, we have

$$c_j^N \rightarrow c^N = (c^m)^{\frac{N}{m}} = d, \quad \text{as } j \rightarrow \infty.$$

Denote by ϕ the idempotent state d . Set $\omega_0 := \omega$ and $\omega_n := c_n^N$ for all $n \geq 1$. Then $\omega_n \rightarrow \phi$ as n tends to ∞ . By definition, $\{\omega_n\}_{n \geq 0}$ is a subsequence of $\{b_j\}_{j \geq 0}$, thus $\omega_{n-1} = \omega_n^{s_n}$ with $N|s_n$ for all $n \geq 1$. Moreover, from (3.12) we have

$$\omega_n = c_n^N = (cd'_n)^N = c^N d_n'^N = \phi d_n'^N = \phi(\phi d_n'^N) = \phi \omega_n, \quad n \geq 0.$$

Similarly, $\omega_n = \omega_n \phi, n \geq 0$. Hence $\{\omega_n\}_{n \geq 0}$ verifies the conditions of Proposition 3.20, and consequently $\omega \in \mathcal{P}_\phi(\mathbb{G})$. \square

Before giving the second proof, we introduce the following proposition, which could be formulated and proved for a general Banach algebra.

Proposition 3.25. *Let $\mathbb{G} = (A, \Delta)$ be a compact quantum group, with A separable. Let ω be an infinitely divisible state on \mathbb{G} . Suppose that there exist an idempotent state ϕ and a sequence of ϕ -bi-invariant roots $\{\omega_{n_k}\}_{k \geq 1}$ of ω , where $\{n_k\}_{k \geq 1}$ is an increasing sequence of positive integers, such that $\omega_{n_k}^{n_k} = \omega$ for all $k \geq 1$, and*

$$\sup_{k \geq 1} n_k \|\omega_{n_k} - \phi\| = M < \infty, \quad (3.14)$$

then $\omega \in \mathcal{P}_\phi(\mathbb{G})$.

Proof. Recall that $\{\varphi \in A' : \|\varphi\| \leq M\}$ is compact with respect to weak* topology for each $M > 0$. Then from (3.14) we have for some subsequence of $\{n_k\}_{k \geq 1}$, still denoted by $\{n_k\}_{k \geq 1}$, that $n_k(\omega_{n_k} - \phi)$ converges to an element $u \in A'$ with respect to the weak* topology. Then $u = \lim_{k \rightarrow \infty} n_k(\omega_{n_k} - \phi) \in \mathcal{N}_\phi(\mathbb{G})$ and $\exp_\phi(u)$ is a Poisson state. It suffices to show that $\omega = \exp_\phi(u)$. Set

$$u_{n_k} := \sum_{m \geq 2} \frac{(\omega_{n_k} - \phi)^m}{m!}, \quad k \geq 1.$$

It is well-defined, since $\sup_{k \geq 1} \|\omega_{n_k} - \phi\| < \infty$. Moreover, from (3.14) it follows that

$$\|u_{n_k}\| \leq \sum_{m \geq 2} \frac{1}{m!} \left(\frac{M}{n_k}\right)^m \leq \frac{1}{n_k^2} \sum_{m \geq 2} \frac{M^m}{m!},$$

whence

$$\lim_{k \rightarrow \infty} n_k \|u_{n_k}\| = 0,$$

and

$$\lim_{k \rightarrow \infty} (1 + \|u_{n_k}\|)^{n_k} = \lim_{k \rightarrow \infty} (1 + \|u_{n_k}\|)^{\frac{1}{\|u_{n_k}\|} \cdot n_k \|u_{n_k}\|} = 1.$$

Hence

$$\begin{aligned} \|\omega - \exp_\phi(n_k(\omega_{n_k} - \phi))\| &= \|\omega_{n_k}^{n_k} - (\omega_{n_k} + u_{n_k})^{n_k}\| \\ &\leq \sum_{m=1}^{n_k} \binom{n_k}{m} \|\omega_{n_k}^{n_k-m} u_{n_k}^m\| \\ &\leq \sum_{m=1}^{n_k} \binom{n_k}{m} \|u_{n_k}\|^m = (1 + \|u_{n_k}\|)^{n_k} - 1, \end{aligned}$$

which tends to 0 as $k \rightarrow \infty$. This shows $\omega = \exp_\phi(u)$ and finishes the proof. \square

The second proof of Theorem 3.24. Again, $\mathcal{P}(\mathbb{G}) \subset \mathcal{I}(\mathbb{G})$ is clear. Let $\omega \in \mathcal{I}(\mathbb{G})$. From the first proof we know that there exist an idempotent state $\phi \in \text{Idem}(\mathbb{G})$ and a sequence of roots $\{\omega_{n_k}\}_{k \geq 0} \subset \mathcal{S}(A)$ with $\{n_k\}_{k \geq 0}$ an increasing sequence of positive integers such that

$$\omega_{n_k}^{n_k} = \omega, \quad \omega_{n_k} = \omega_{n_k} \phi = \phi \omega_{n_k}, \quad k \geq 0,$$

and $\omega_{n_k} \rightarrow \phi$ as $k \rightarrow \infty$. Let u and u_{n_k} be the restrictions of ω and ω_{n_k} to A_ϕ for all $k \geq 0$, respectively. Then from Lemma 3.7 u is a state on A_ϕ such that $\{u_{n_k}\}_{k \geq 0}$ is a sequence of roots of u in $\mathcal{S}(A_\phi)$ verifying

$$u_{n_k}^{n_k} = u \text{ and } u_{n_k} \rightarrow \epsilon_\phi, \quad k \rightarrow \infty,$$

where ϵ_ϕ is the counit of A_ϕ . Now we repeat a calculation in Lemma 3.22. Suppose that $A = \bigoplus_{\alpha=1}^m \mathbb{M}_{n_\alpha}(\mathbb{C})$ with the matrix units $\{e_{ij}^\alpha : 1 \leq i, j \leq n_\alpha, 1 \leq \alpha \leq m\}$. Let $\{\widetilde{e}_{ij}^\alpha\}$ be the dual basis. Then by Lemma 3.15 we can write u as

$$u_{n_k} = \sum_{\alpha=1}^m p_{\alpha,k} \sum_{i,j=1}^{n_\alpha} a_{ij}^{\alpha,k} \widetilde{e}_{ij}^\alpha$$

with $p_{\alpha,k} \geq 0$, $\sum_{\alpha=1}^m p_{\alpha,k} = 1$ and $[a_{ij}^{\alpha,k}]_{i,j=1}^{n_\alpha}$ is positive semi-definite with trace one for each k . Let α_0 be such that $\widetilde{e}^{\alpha_0} = \epsilon_\phi = 1_{\hat{A}_p}$. By Corollary 3.16 and the assumption,

$$\|u_{n_k} - \epsilon_\phi\| = 2(1 - p_{\alpha_0,k}) \rightarrow 0, \quad k \rightarrow \infty. \quad (3.15)$$

So $p_{\alpha_0,k} \rightarrow 1$ as $k \rightarrow \infty$.

Now for each $q > 0$ we introduce the L_q -norm (quasi-norm when $q < 1$) induced by \hat{h}_p . Recall that $\hat{h}_p = \frac{1}{\phi(p_A)} \hat{h}|_{\hat{A}_p}$ is a tracial state on \hat{A}_p . Namely, we define

$$\|x\|_q := [\hat{h}_p(|x|^q)]^{\frac{1}{q}}, \quad x \in \hat{A}_p,$$

where $|x| = (x^*x)^{\frac{1}{2}}$. Then Hölder's inequality still holds and we have

$$\|u\|_{\frac{2}{n_k}} = \|u_{n_k}^{n_k}\|_{\frac{2}{n_k}} \leq \|u_{n_k}\|_2^{n_k}, \quad k \geq 0. \quad (3.16)$$

Note that u is invertible in \hat{A}_p . Indeed, for large k there holds

$$\|u_{n_k} - \epsilon_\phi\|_{\hat{A}_p} \leq \|u_{n_k} - \epsilon_\phi\| < 1,$$

then we have that u_{n_k} is invertible for large k . So $u = u_{n_k}^{n_k}$ is also invertible in \hat{A}_p .

Following a similar calculation to that in Lemma 3.22, we obtain

$$\hat{h}_p(u_{n_k} u_{n_k}^*) \leq p_{\alpha_0,k}^2 + (1 - p_{\alpha_0,k})^2.$$

This, together with (3.16), yields

$$\hat{h}_p(|u|^{\frac{1}{n_k}}) = \|u\|_{\frac{2}{n_k}}^{\frac{2}{n_k}} \leq \|u_{n_k}\|_2^2 = \hat{h}_p(u_{n_k} u_{n_k}^*) \leq p_{\alpha_0,k}^2 + (1 - p_{\alpha_0,k})^2,$$

for all k . Since $p_{\alpha_0,k} \rightarrow 1$ as $k \rightarrow \infty$, there exists $K > 0$ such that for all $k \geq K$, $\frac{1}{2} \leq p_{\alpha_0,k} \leq 1$. Thus for all $k \geq K$, $1 - p_{\alpha_0,k} \leq p_{\alpha_0,k}$ and then

$$\hat{h}_p(|u|^{\frac{1}{n_k}}) \leq p_{\alpha_0,k}^2 + (1 - p_{\alpha_0,k})^2 \leq p_{\alpha_0,k}^2 + p_{\alpha_0,k}(1 - p_{\alpha_0,k}) = p_{\alpha_0,k}. \quad (3.17)$$

Combining this with (3.15), we have

$$n_k \|u_{n_k} - \epsilon_\phi\| = 2n_k(1 - p_{\alpha_0, k}) \leq 2n_k(1 - \hat{h}_p(|u|^{\frac{1}{n_k}})) = 2n_k \hat{h}_p(1_{\hat{A}_p} - |u|^{\frac{1}{n_k}})$$

for all $k \geq K$. Since u is invertible in \hat{A}_p , $n(1_{\hat{A}_p} - |u|^{\frac{1}{n}})$ converges to $-\log |u|$ in norm as $n \rightarrow \infty$. Then there exists a constant $M < \infty$ such that

$$\sup_{n \geq 1} n \hat{h}_p(1_{\hat{A}_p} - |u|^{\frac{1}{n}}) \leq M.$$

Thus from Lemma 3.7 it follows that

$$\sup_{k \geq 0} n_k \|\omega_{n_k} - \phi\| = \sup_{k \geq 0} n_k \|u_{n_k} - \epsilon_\phi\| \leq \sup_{k \geq 0} 2n_k \hat{h}_p(1_{\hat{A}_p} - |u|^{\frac{1}{n_k}}) < \infty.$$

Hence $\omega \in \mathcal{P}_\phi(\mathbb{G})$ by Proposition 3.25. □

Remark 3.26. *Both proofs rely on the capture of idempotent state which the infinitely divisible state is “supported on” and the sequence of roots converging to this idempotent state. After this the first proof aims to show that this sequence of roots can be chosen to form a submonogeneous convolution semigroup (Proposition 3.20 (3)), while the idea of the second proof is derived from a general result, Proposition 3.25, concerning the decay property (3.14) of this sequence of roots. The inequality (3.17) also allows us to simplify the proof of the main theorem in [60] for the finite group case.*

Chapter 4

Fourier multipliers on discrete group von Neumann algebras

The study of the L_p -boundedness of Fourier multipliers on locally compact groups has become one of the most important subjects in noncommutative analysis in recent years [14, 15, 31, 38, 39, 57]. However, few examples of L_p -Fourier multipliers are known for $1 < p \neq 2 < \infty$ even in the discrete group case. In particular, the radial Fourier multipliers on free groups are of interest, but lack concrete examples. In this chapter, for general p , we give one sufficient condition on the L_p -boundedness of Fourier multipliers on general discrete groups, and one sufficient condition on the L_p -boundedness of radial Fourier multipliers on free groups. This provides us with some concrete examples of L_p -Fourier multipliers. In particular, our results will put forward the recent attempts to generalize Hörmander-Mikhlin type multiplier theorem on the free group von Neumann algebras.

We shall use a basic fact that $L_p(\widehat{G}) \subset L_q(\widehat{G})$ whenever $q \leq p$ for any discrete group G , since the canonical trace τ on \widehat{G} is a state. Based on this fact the problem of L_p -boundedness of Fourier multiplier can be turned into the study of L_p - L_2 (L_2 - L_p if $p > 2$) boundedness of Fourier multiplier. Our main ideas then come from the study of L_p - L_q Fourier multipliers originally from Hörmander [36] and results on hypercontractivity of Ricard and Xu [63]. This conversion simplifies the problem in the discrete case.

We fix some notations for this chapter. Here and in the following, $A \lesssim_p B$ means $A \leq c_p B$ for some constant $c_p > 0$. The notations $\lesssim_{p,q}$ and $\lesssim_{p,q,r}$ should be understood in a similar way. We use $\#S$ to denote the cardinal of a set S .

4.1 Preliminary: noncommutative L_p -spaces

In this section we collect some necessary preliminaries on noncommutative L_p -spaces and noncommutative Lorentz spaces.

4.1.1 Noncommutative L_p -spaces and Lorentz spaces associated with a semifinite von Neumann algebra

We concentrate ourselves on noncommutative L_p -spaces associated with semifinite von Neumann algebras, which were first laid out in the early 1950s by Segal [66] and Dixmier [22]. The noncommutative Lorentz spaces will be treated at the same time. We refer to [61] for more discussions.

Let \mathcal{M} be a semifinite von Neumann algebra equipped with a normal semifinite faithful (*n.s.f.*) trace τ . Denote by \mathcal{M}^+ the positive cone of \mathcal{M} . Let $\mathcal{S}^+ = \mathcal{S}^+(\mathcal{M})$ denote the set of all $x \in \mathcal{M}^+$ such that $\tau(\text{supp}(x)) < \infty$, where $\text{supp}(x)$ denotes the support projection of x . Let $\mathcal{S} = \mathcal{S}(\mathcal{M})$ be the linear span of \mathcal{S}^+ . Then \mathcal{S} is a weak*-dense *-subalgebra of \mathcal{M} . Given $0 < p < \infty$, we define

$$\|x\|_p := [\tau(|x|^p)]^{\frac{1}{p}}, \quad x \in \mathcal{S},$$

where $|x| = (x^*x)^{\frac{1}{2}}$ is the modulus of x . Then $(\mathcal{S}, \|\cdot\|_p)$ is a normed (or quasi-normed for $p < 1$) space. Its completion is called *noncommutative L_p -space associated with (\mathcal{M}, τ)* , denoted by $L_p(\mathcal{M}, \tau)$, or simply by $L_p(\mathcal{M})$. As usual, we set $L_\infty(\mathcal{M}, \tau) = \mathcal{M}$ equipped with the operator norm.

For $1 \leq p < \infty$, the dual space of $L_p(\mathcal{M})$ is $L_{p'}(\mathcal{M})$ ($1/p + 1/p' = 1$) with respect to the duality

$$\langle x, y \rangle := \tau(xy), \quad x \in L_p(\mathcal{M}), y \in L_{p'}(\mathcal{M}).$$

In particular, $L_1(\mathcal{M})$ is identified with \mathcal{M}_* , the predual of \mathcal{M} , via the map $j(x) := \tau(x \cdot), x \in L_1(\mathcal{M})$.

The elements in $L_p(\mathcal{M})$ can be viewed as closed densely defined operators on \mathcal{H} (\mathcal{H} being the Hilbert space on which \mathcal{M} acts). A linear closed operator x is said to be *affiliated with \mathcal{M}* if it commutes with all unitary elements in \mathcal{M}' , the commutant of \mathcal{M} , i.e., $xu = ux$ for any unitary $u \in \mathcal{M}'$. Note that x can be unbounded on \mathcal{H} . An operator x affiliated with \mathcal{M} is said to be *measurable with respect to (\mathcal{M}, τ)* , or simply *measurable* if for any $\varepsilon > 0$, there exists a projection $e \in \mathcal{M}$ such that

$$e(H) \subset \mathcal{D}(x) \text{ and } \tau(e^\perp) \leq \varepsilon,$$

where $e^\perp = 1 - e$ and $\mathcal{D}(x)$ denotes the domain of x . We denote by $L_0(\mathcal{M}, \tau)$, or simply $L_0(\mathcal{M})$ the family of measurable operators. For $x \in L_0(\mathcal{M}, \tau)$, we define the *distribution function* of x as

$$\lambda_s(x) := \tau(\mathbf{1}_{(s, \infty)}(|x|)), \quad s > 0,$$

where $\mathbf{1}_{(s, \infty)}(|x|)$ is the spectral projection of $|x|$ corresponding to the interval (s, ∞) , and define the *generalized singular numbers* of x as

$$\mu_t(x) := \inf\{s > 0 : \lambda_s(x) < t\}, \quad t > 0.$$

Similar to the classical case, for $0 < p, q < \infty$, the *noncommutative Lorentz space $L_{p,q}(\mathcal{M})$* is defined as the collection of all measurable operators x such that

$$\|x\|_{p,q} := \left(\int_0^\infty (t^{\frac{1}{p}} \mu_t(x))^q \frac{dt}{t} \right)^{\frac{1}{q}} < \infty.$$

Clearly, $L_{p,p}(\mathcal{M}) = L_p(\mathcal{M})$ with $\|\cdot\|_{p,p} = \|\cdot\|_p$. We may also define the *weak L_p -space $L_{p,\infty}(\mathcal{M})$* , $0 < p < \infty$, which consists of all measurable operators x such that

$$\|x\|_{p,\infty} := \sup_{t>0} t^{\frac{1}{p}} \mu_t(x) < \infty.$$

Like the classical L_p -spaces, noncommutative L_p -spaces behave well with respect to interpolation. Our reference for interpolation theory is [6]. Let $1 \leq p_0 \leq p_1 \leq \infty$, $1 \leq q \leq \infty$ and $0 < \theta < 1$. Then

$$(L_{p_0}(\mathcal{M}), L_{p_1}(\mathcal{M}))_\theta = L_{p_\theta}(\mathcal{M}) \text{ (with equal norms)}$$

and

$$(L_{p_0}(\mathcal{M}), L_{p_1}(\mathcal{M}))_{\theta, q} = L_{p_{\theta, q}}(\mathcal{M}) \text{ (with equal norms),} \quad (4.1)$$

where $1/p_{\theta} = (1-\theta)/p_0 + \theta/p_1$, $(\cdot, \cdot)_{\theta}$ and $(\cdot, \cdot)_{\theta, q}$ denote respectively the complex and real interpolation methods.

We formulate here some properties that we will use in this thesis. For the proofs we refer to [25, 61].

Lemma 4.1. *Let $1 < p, q < \infty$ and $1/p + 1/p' = 1, 1/q + 1/q' = 1$. Then we have*

$$(1) \mu_{s+t}(xy) \leq \mu_s(x)\mu_t(y) \text{ for all } s, t > 0 \text{ and } x, y \in L_0(\mathcal{M});$$

$$(2) \text{ for any } q < r \leq \infty \text{ and any } x \in L_{p, q}(\mathcal{M}),$$

$$\|x\|_{p, r} \lesssim_{p, q, r} \|x\|_{p, q}, \quad (4.2)$$

where the constant is $c_{p, q, r} = (q/p)^{\frac{1}{q} - \frac{1}{r}}$.

The next lemma is Hölder's inequality on noncommutative Lorentz space. We give a proof here for the convenience of the readers.

Lemma 4.2. *Let $0 < p_0, q_0 < \infty, 0 < p_1, q_1 \leq \infty$. Let p, q be such that $1/p = 1/p_0 + 1/p_1$ and $1/q = 1/q_0 + 1/q_1$. Let \mathcal{M} be a von Neumann algebra equipped with a n.s.f. trace τ . Then we have for any $x \in L_{p_0, q_0}(\mathcal{M}, \tau)$ and $y \in L_{p_1, q_1}(\mathcal{M}, \tau)$*

$$\|xy\|_{p, q} \lesssim_p \|x\|_{p_0, q_0} \|y\|_{p_1, q_1}, \quad (4.3)$$

where the constant is $c_p = 2^{\frac{1}{p}}$.

Proof. From Hölder's inequality on L_p -spaces of $(\mathbb{R}^+, \frac{dt}{t})$ and Lemma 4.1(1) it follows that

$$\begin{aligned} \|xy\|_{p, q} &= \left(\int_0^{\infty} (t^{\frac{1}{p}} \mu_t(xy))^q \frac{dt}{t} \right)^{\frac{1}{q}} \\ &= 2^{\frac{1}{p}} \left(\int_0^{\infty} (t^{\frac{1}{p}} \mu_{2t}(xy))^q \frac{dt}{t} \right)^{\frac{1}{q}} \\ &\leq 2^{\frac{1}{p}} \left(\int_0^{\infty} (t^{\frac{1}{p_0}} \mu_t(x) \cdot t^{\frac{1}{p_1}} \mu_t(y))^q \frac{dt}{t} \right)^{\frac{1}{q}} \\ &\leq 2^{\frac{1}{p}} \left(\int_0^{\infty} (t^{\frac{1}{p_0}} \mu_t(x))^{q_0} \frac{dt}{t} \right)^{\frac{1}{q_0}} \left(\int_0^{\infty} (t^{\frac{1}{p_1}} \mu_t(y))^{q_1} \frac{dt}{t} \right)^{\frac{1}{q_1}} \\ &= 2^{\frac{1}{p}} \|x\|_{p_0, q_0} \|y\|_{p_1, q_1}, \end{aligned}$$

for all $x \in L_{p_0, q_0}(\mathcal{M}, \tau)$ and $y \in L_{p_1, q_1}(\mathcal{M}, \tau)$. \square

We end this subsection with two examples.

Example 4.3. The usual (commutative) L_p -spaces are noncommutative L_p -spaces. Let $(\Omega, \mathcal{F}, \mu)$ be a σ -finite measure space. The family of essentially bounded functions on Ω , $L_{\infty}(\Omega)$, can be considered as the von Neumann algebra acting on the Hilbert space $L_2(\Omega)$ by identifying each $f \in L_{\infty}(\Omega)$ with M_f . Here $M_f : L_2(\Omega) \rightarrow L_2(\Omega)$ is the multiplication operator given by $M_f(g) = fg$. The map $f \mapsto M_f$ is an isometric *-homomorphism from $L_{\infty}(\Omega)$ into $B(L_2(\Omega))$.

In the von Neumann algebra $L_\infty(\Omega)$, M_f is positive iff f is a non-negative function. It is equipped with a *n.s.f.* trace \int given by

$$\int f := \int_\Omega f d\mu, \quad f \in L_\infty(\Omega)^+.$$

Then for $(L_\infty(\Omega), \int)$, the set $\mathcal{S} = \mathcal{S}(L_\infty(\Omega))$ consists of all functions f with finite-measure support. The noncommutative L_p -space $L_p(L_\infty(\Omega), \int)$ coincides with the usual L_p -space $L_p(\Omega, d\mu)$. However, we remark here is a minor difference between measurable operators with respect to $(L_\infty(\Omega), \int)$ and measurable functions on Ω . In fact, any measurable function f on Ω belongs to $L_0(L_\infty(\Omega), \int)$ iff it is bounded outside a set of finite measure.

Example 4.4. Let G be a discrete group with unit e . Denote by $(\delta_g)_{g \in G}$ the canonical basis of the Hilbert space $\ell_2(G)$, i.e., δ_g is the indicator function on g . Let $\lambda : G \rightarrow B(\ell_2(G))$ be the left regular representation. That is,

$$\lambda(g)f(h) := f(g^{-1}h), \quad g, h \in G, f \in \ell_2(G).$$

The *group von Neumann algebra* \widehat{G} is defined as the von Neumann subalgebra of $B(\ell_2(G))$ generated by all $\lambda(g), g \in G$. The $*$ -subalgebra $\mathbb{C}[G] := \{x = \sum_{\text{finite sum}} x_g \lambda(g) : x_g \in \mathbb{C}\}$ is weak*-dense in \widehat{G} . Note that $\lambda(g)^* = \lambda(g^{-1})$. There is a canonical normal faithful trace $\tau = \tau_G$ on \widehat{G} : $\tau(x) = \langle \delta_e, x \delta_e \rangle, x \in \widehat{G}$, where $\langle \cdot, \cdot \rangle$ is the inner product in $\ell_2(G)$ which is linear in second argument. Moreover, $\tau(1) = 1$. On (\widehat{G}, τ) one can construct the noncommutative L_p -spaces $L_p(\widehat{G}) = L_p(\widehat{G}, \tau), 0 < p \leq \infty$.

In this chapter we use \mathbb{F}_n to denote the free group on n generators with $n \in \mathbb{N} \cup \{\infty\}$, and $|\cdot| : \mathbb{F}_n \rightarrow \mathbb{N}$ is its natural length function. A function $\varphi : \mathbb{F}_n \rightarrow \mathbb{C}$ is said to be *radial* if $\varphi = \phi(|\cdot|)$ for some $\phi : \mathbb{N} \rightarrow \mathbb{C}$.

4.2 Main results

Let G be a discrete group with λ the left regular representation. For any function $\varphi : G \rightarrow \mathbb{C}$, we say that φ (or T_φ) is a *L_p -Fourier multiplier* if the map $T_\varphi : \sum a_g \lambda(g) \mapsto \sum \varphi(g) a_g \lambda(g)$ (or $\lambda(f) \mapsto \lambda(\varphi f)$) extends to a bounded map from $L_p(\widehat{G})$ to itself.

Our first result concerns the general discrete groups.

Theorem 4.5. *Let $1 < p < \infty$ and $1/p^* := |1/2 - 1/p|$. Let G be any discrete group with the dual \widehat{G} . Then for any $\varphi \in \ell_{p^*, \infty}(G)$, we have*

$$\|T_\varphi : L_p(\widehat{G}) \rightarrow L_p(\widehat{G})\| \lesssim_p \|\varphi\|_{p^*, \infty}. \quad (4.4)$$

Remark 4.6. *In fact, one can show that for $1 < p \leq 2 \leq q < \infty$ and $1/r = 1/p - 1/q$, we have*

$$\|T_\varphi : L_p(\widehat{G}) \rightarrow L_q(\widehat{G})\| \lesssim_{p,q} \|\varphi\|_{r, \infty}. \quad (4.5)$$

Example 4.7. Let G be a finitely generated group with the unit e and a symmetric set S of generators. By saying symmetric we mean $x^{-1} \in S$ whenever $x \in S$. Then it has an *exponential growth*, i.e.,

$$\#\{x \in G : d(x, e) \leq n\} \leq a^n, \quad n \geq 1, \quad (4.6)$$

for some $a > 1$, where d is the word metric on G with respect to S and \sharp denotes the counting measure on G . Indeed, one can always choose a to be $\sharp S$. Then for any $\varphi : G \rightarrow \mathbb{C}$ such that $|\varphi(g)| \leq Ca^{-\frac{|g|}{p^*}}$, where $|g| := d(g, e)$ and $C > 0$ is a constant,

$$|\varphi(g)| \geq \alpha \text{ implies } |g| \leq -p^* \log_a \frac{\alpha}{C}, \quad \alpha > 0.$$

Therefore

$$\alpha^{p^*} \sharp\{g \in G : |\varphi(g)| \geq \alpha\} \leq \alpha^{p^*} a^{-p^* \log_a \frac{\alpha}{C}} \leq C^{p^*} < \infty, \quad \alpha > 0,$$

and we have $\varphi \in \ell_{p^*, \infty}(G)$, whence T_φ is a L_p -multiplier on $L_p(\widehat{G})$. For free group of N generators \mathbb{F}_N , we may choose S as the set consisting of N generators with their inverses and let $a = 2N$.

If moreover, G is of *polynomial growth*, i.e., the right hand side of (4.6) can be replaced by some polynomial $p(n)$, or equivalently, n^k for some $k > 0$, then a similar argument yields that for any $\varphi : G \rightarrow \mathbb{C}$ such that $|\varphi(g)| \leq C|g|^{-\frac{k}{p^*}}$, we have $\varphi \in \ell_{p^*, \infty}(G)$, and then T_φ is a L_p -multiplier on $L_p(\widehat{G})$.

Our second result concerns the free group \mathbb{F}_∞ .

Theorem 4.8. *Let $2 < p < \infty$. Suppose that φ is radial on \mathbb{F}_∞ , i.e., $\varphi(g) = \phi(|g|)$ for some $\phi : \mathbb{N} \rightarrow \mathbb{C}$. Then we have*

$$\|T_\varphi : L_p(\widehat{\mathbb{F}_\infty}) \rightarrow L_p(\widehat{\mathbb{F}_\infty})\| \leq \left(\sum_{n \geq 0} (1+n)^{\alpha_p} |\phi(n)|^2 \right)^{1/2}, \quad (4.7)$$

where $\alpha_p = \max\{2 - 6/p, 1 - 2/p\}$.

Corollary 4.9. *As a direct consequence, T_φ is a L_p -Fourier multiplier on $\widehat{\mathbb{F}_\infty}$ if there exists $\epsilon > 0$ such that*

$$\sup_{n \geq 0} n^{1 - \frac{1}{p} + \epsilon} |\phi(n)| < \infty, \quad 2 < p \leq 4, \quad (4.8)$$

or

$$\sup_{n \geq 0} n^{\frac{3}{2} - \frac{3}{p} + \epsilon} |\phi(n)| < \infty, \quad p \geq 4. \quad (4.9)$$

The inequalities (4.8) and (4.9) suggest that, if one aims to develop a Hörmander-Mikhlin type multiplier theorem on free group \mathbb{F}_∞ , the constant α (which is independent of p) appearing in

$$\sup_{n \geq 0} n^\alpha |\phi(n)| < \infty,$$

should not be larger than $3/2$ (observe (4.9) when $p \rightarrow \infty$). It covers the above result completely only if $\alpha \leq 1/2$ (observe (4.8) when $p \rightarrow 2^+$). Since $|\phi(n)| \leq |\phi(0)| + \sum_{m=1}^n |\phi(m) - \phi(m-1)|$, the Hörmander-Mikhlin type multiplier theorem should be related to the condition

$$\sup_{n \geq 1} n^\beta |\phi(n) - \phi(n-1)| < \infty,$$

with $\beta \leq 5/2$, and it covers (4.8) and (4.9) completely only if $\beta \leq 3/2$.

4.3 The proofs

Suppose $1 < p < 2$ and $1/p + 1/p' = 1$. Recall that the Hausdorff-Young inequality says that

$$\|\lambda(x)\|_{p'} \leq \|x\|_p. \quad (4.10)$$

Indeed, it is a consequence of the complex interpolation of the following two inequalities:

$$\|\lambda(x)\|_\infty \leq \|x\|_1 \text{ and } \|\lambda(x)\|_2 = \|x\|_2.$$

If we apply the real interpolation instead of the complex interpolation, one obtains

$$\|\lambda(x)\|_{p',p} \lesssim_p \|x\|_p. \quad (4.11)$$

The dual of (4.11) takes the form:

$$\|x\|_{p',p} \lesssim_p \|\lambda(x)\|_p. \quad (4.12)$$

Now we are ready to prove (4.4). One can use a similar argument to show (4.5), which is simpler than the proof of the boundedness of L_p - L_q Fourier multipliers on \mathbb{R} in [36].

Proof of Theorem 4.5. We only prove the case $1 < p < 2$, since the proof for $p > 2$ is similar. Note that $1/2 = 1/p^* + 1/p'$, then by (4.2), (4.3) and (4.12) we have

$$\|\lambda(\varphi f)\|_p \leq \|\lambda(\varphi f)\|_2 = \|\varphi f\|_2 \lesssim_p \|\varphi\|_{p^*,\infty} \|f\|_{p',2} \lesssim_p \|\varphi\|_{p^*,\infty} \|f\|_{p',p} \lesssim_p \|\varphi\|_{p^*,\infty} \|\lambda(f)\|_p.$$

□

To prove Theorem 4.8, we need *Haagerup's inequality*. For this, denote by S_n the set of all elements in \mathbb{F}_∞ with length n , i.e., $S_n = \{g \in \mathbb{F}_\infty : |g| = n\}$. We say that x is *supported on S_n* if $x = \sum_{g \in S_n} x_g \lambda(g)$. The Haagerup's inequality states that:

Lemma 4.10. [32, Lemma 1.4] *For any x supported on S_n , we have*

$$\|x\|_\infty \leq (n+1)\|x\|_2. \quad (4.13)$$

The following lemma can be found in [63].

Lemma 4.11. [63, Lemma 7] *For any x supported on S_n , we have*

$$\|x\|_4 \leq (n+1)^{\frac{1}{4}} \|x\|_2. \quad (4.14)$$

For any x supported on S_n , using (4.13), (4.14) and the trivial equality $\|x\|_2 = \|x\|_2$, we obtain by complex interpolation that

$$\|x\|_p \leq (n+1)^{\frac{1}{2} - \frac{1}{p}} \|x\|_2, \quad 2 < p \leq 4, \quad (4.15)$$

and

$$\|x\|_p \leq (n+1)^{1 - \frac{3}{p}} \|x\|_2, \quad p \geq 4. \quad (4.16)$$

From (4.13) and $\|x\|_2 = \|x\|_2$ one can obtain the estimate

$$\|x\|_p \leq (n+1)^{1 - \frac{2}{p}} \|x\|_2, \quad 2 < p < \infty.$$

It will give (4.7) with $\alpha_p = 2 - 4/p$ for all $2 < p < \infty$. So (4.13) is essential, while (4.14) improves the result slightly.

Proof of Theorem 4.8. It suffices to prove the estimate for all $x \in \text{span}\{\lambda(g) : g \in \mathbb{F}_\infty\}$. For any such x , we can write it as $x = \sum_{n \geq 0} x_n$ with x_n supported on S_n . Note that for $m \neq n$, x_m and x_n are orthogonal with respect to the inner product induced by the canonical tracial state τ on \mathbb{F}_∞ , so that we have

$$\sum_{n \geq 0} \|x_n\|_2^2 = \|x\|_2^2 \leq \|x\|_p^2, \quad p > 2. \quad (4.17)$$

By the triangle inequality and (4.15) we have for all $2 < p \leq 4$ that

$$\|T_\varphi(x)\|_p = \left\| \sum_{n \geq 0} \phi(n)x_n \right\|_p \leq \sum_{n \geq 0} |\phi(n)| \|x_n\|_p \leq \sum_{n \geq 0} |\phi(n)|(n+1)^{\frac{1}{2} - \frac{1}{p}} \|x_n\|_2.$$

From Cauchy-Schwarz inequality and (4.17), it follows that

$$\|T_\varphi(x)\|_p^2 \leq \sum_{n \geq 0} |\phi(n)|^2 (n+1)^{1 - \frac{2}{p}} \sum_{n \geq 0} \|x_n\|_2^2 \leq \sum_{n \geq 0} |\phi(n)|^2 (n+1)^{1 - \frac{2}{p}} \cdot \|x\|_p^2,$$

which finishes the proof for $2 < p \leq 4$. The proof for $p \geq 4$ follows similarly with (4.15) replaced by (4.16). \square

Chapter 5

Monotonicity of α - z Rényi relative entropies

In this chapter we study the joint convexity/concavity of the trace function

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s,$$

where $p, q, s \in \mathbb{R}$, A and B are positive definite matrices and K is any fixed invertible matrix. We will give full range of (p, q, s) for $\Psi_{p,q,s}$ to be jointly convex/concave for all K . As a consequence, we confirm a conjecture of Carlen, Frank and Lieb [10, Conjecture 4]. In particular, we confirm a weaker conjecture of Audenaert and Datta [2, Conjecture 1] and obtain the full range of (α, z) for α - z Rényi relative entropies to be monotone under completely positive trace preserving maps. We also give simpler proofs of many known results, including the concavity of $\Psi_{p,0,1/p}$ for $0 < p < 1$ which was firstly proved by Epstein [23] using complex analysis. The key is to reduce the problem to the joint convexity/concavity of trace function

$$\Psi_{p,1-p,1}(A, B) = \text{Tr} K^* A^p K B^{1-p},$$

for $-1 < p < 1$ using a variational method.

5.1 Introduction

The joint convexity/concavity of trace function

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s,$$

has played an important role in mathematical physics and quantum information. Its study can be traced back to the celebrated *Lieb's Concavity Theorem* [49], which states that $\Psi_{p,q,1}$ is jointly concave for all $0 \leq p, q \leq 1, p + q \leq 1$ and for all K . Using this, Lieb confirmed the Wigner-Yanase-Dyson Conjecture [72, 49]: *for $0 < p < 1$ and any self-adjoint K , the function*

$$S_p(\rho, K) := \frac{1}{2} \text{Tr}[\rho^p, K][\rho^{1-p}, K] = -\text{Tr} \rho K^2 + \text{Tr} \rho^p K \rho^{1-p} K,$$

is concave in ρ , where $[A, B] = AB - BA$. We refer to [72, 49] for more details about the skew information $-S_p(\rho, K)$.

Since then, a lot of work around the joint convexity/concavity of $\Psi_{p,q,s}$ has emerged [1, 5, 9, 12, 11, 23, 26, 33, 34], following [49]. Through this line of research many methods have been developed. Two main methods are the “analytic method” and the “variational method”. We refer to a very nice survey paper [10] for more historical information and the explanation of these two methods.

Another motivation to study the joint convexity/concavity of $\Psi_{p,q,s}$ comes from quantum information. Indeed, the joint convexity/concavity of $\Psi_{p,q,1/(p+q)}$ is closely related to the monotonicity of the α - z Rényi relative entropies, which has become a frontier topic recently. We shall recall this connection in Section 5.2. This is the motivation of the conjecture of Audenaert and Datta:

Conjecture 5.1. [2, Conjecture 1] If $1 \leq p \leq 2$, $-1 \leq q < 0$ and $(p, q) \neq (1, -1)$, then for any matrix K , the function

$$\Psi_{p,q,1/(p+q)}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^{\frac{1}{p+q}},$$

is jointly convex in (A, B) .

In this chapter we confirm a stronger conjecture of Carlen, Frank and Lieb:

Conjecture 5.2. [10, Conjecture 4] If $1 \leq p \leq 2$, $-1 \leq q < 0$, $(p, q) \neq (1, -1)$ and $s \geq \frac{1}{p+q}$, then for any matrix K , the function

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s,$$

is jointly convex in (A, B) .

As we mentioned earlier, in the history two main methods have been developed to study the convexity/concavity of trace functions $\Psi_{p,q,s}$: the analytic method and the variational method. The analytic method, which is the methodology employing the theory of Herglotz functions, was introduced firstly by Epstein [23]. The variational method was firstly introduced by Carlen and Lieb in [12]. Both of them have their own advantages, as in [10, Page 8] the authors wrote: “It appears that the analyticity method is especially useful for proving concavity and the variational method is more useful for proving convexity, but this is not meant to be an absolute distinction.” In this chapter we confirm Carlen-Frank-Lieb Conjecture by developing only the variational method.

The main value of this chapter is twofold. Firstly, we develop the variational method in a very simple way such that it is useful to prove both convexity and concavity, and it reduces the convexity/concavity of $\Psi_{p,q,s}$ to three very particular cases (see Remark 5.14). In this way we obtain the full range of (p, q, s) such that $\Psi_{p,q,s}$ is jointly convex/concave and confirm the Carlen-Frank-Lieb Conjecture. Secondly, such three very particular cases can be furthermore reduced to Lieb’s concavity result [49] of $\Psi_{p,1-p,1}$ for $0 < p \leq 1$ and Ando’s concavity result [1] of $\Psi_{p,1-p,1}$ for $-1 \leq p < 0$ in 1970s. In other words, from Lieb’s and Ando’s results (which admit many simple proofs) on

$$\Psi_{p,1-p,1}(A, B) = \text{Tr} K^* A^p K B^{1-p},$$

the subsequent results on joint convexity/concavity of $\Psi_{p,q,s}$ can be derived easily via our variational method. In this way the analytic method can be avoided.

We fix some notations in this chapter. We shall use \mathcal{H} to denote a finite-dimensional Hilbert space. We use $\mathcal{B}(\mathcal{H})$ to denote the family of bounded linear operators on \mathcal{H} , $\mathcal{P}(\mathcal{H})$

to denote the family of positive linear operators on \mathcal{H} (or n -by- n positive semi-definite matrices with $\dim \mathcal{H} = n$), and $\mathcal{D}(\mathcal{H})$ to denote the family of density operators, i.e., positive linear operators on \mathcal{H} with unit trace (or n -by- n positive semi-definite matrices having unit trace with $\dim \mathcal{H} = n$). Moreover, we use $\mathcal{B}(\mathcal{H})^\times$ (reps. $\mathcal{P}(\mathcal{H})^\times$ and $\mathcal{D}(\mathcal{H})^\times$) to denote the family of invertible operators in $\mathcal{B}(\mathcal{H})$ (resp. $\mathcal{P}(\mathcal{H})$ and $\mathcal{D}(\mathcal{H})$). We use Tr to denote the usual trace on matrix algebra and we use I to denote the identity matrix. For any matrix A we use $|A|$ to denote its modulus $(A^*A)^{\frac{1}{2}}$.

5.2 Background and main results

Given two probability density functions p and q on \mathbb{R} , the *relative entropy*, or the *Kullback-Leibler divergence* of p with respect to q is given by

$$S(p||q) := \int_{\mathbb{R}} p(x)(\log p(x) - \log q(x))dx. \quad (5.1)$$

For $\alpha \in (0, 1) \cup (1, \infty)$, the α -*Rényi relative entropy* of p with respect to q is defined as [62]

$$S_\alpha(p||q) := \frac{1}{\alpha - 1} \log \int_{\mathbb{R}} p(x)^\alpha q(x)^{1-\alpha} dx. \quad (5.2)$$

Both relative entropies have been generalized to quantum case, where the density functions are replaced by the density operators, and the integral is replaced by the trace, respectively.

Now for $\rho, \sigma \in \mathcal{D}(\mathcal{H})^\times$, a natural quantum analogue of (5.1), is the so-called *Umegaki relative entropy* [71]

$$D(\rho||\sigma) := \text{Tr} \rho (\log \rho - \log \sigma). \quad (5.3)$$

The quantum analogues of (5.2) might take various forms. One of the most important generalizations of (5.2) are the *quantum α -Rényi relative entropies*

$$D_\alpha(\rho||\sigma) := \frac{1}{\alpha - 1} \log \text{Tr}(\rho^\alpha \sigma^{1-\alpha}), \quad \alpha \in (0, 1) \cup (1, \infty).$$

It admits the Umegaki relative entropy $D(\rho||\sigma)$ as a limit case when $\alpha \rightarrow 1$.

Another generalization of (5.2), introduced by Müller-Lennert, Dupuis, Szehr, Fehr, Tomamichel [56] and Wilde, Winter, Yang [73], are the *sandwiched α -Rényi entropies*:

$$\tilde{D}_\alpha(\rho||\sigma) := \frac{1}{\alpha - 1} \log \text{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha, \quad \alpha \in (0, 1) \cup (1, \infty).$$

In recent years, Audenaert and Datta [2] introduced a new family of quantum Rényi relative entropies, unifying the α -Rényi relative entropy D_α and the sandwiched α -Rényi relative entropy \tilde{D}_α by using two parameters, called the α - z *Rényi relative entropies*:

$$D_{\alpha,z}(\rho||\sigma) := \frac{1}{\alpha - 1} \log \text{Tr}(\sigma^{\frac{1-\alpha}{2z}} \rho^\alpha \sigma^{\frac{1-\alpha}{2z}})^z, \quad \alpha \in (-\infty, 1) \cup (1, \infty), \quad z > 0. \quad (5.4)$$

Note that by taking $z = 1$ and $\alpha = z$, one recovers D_α and \tilde{D}_α , respectively. We comment here that the α - z Rényi relative entropies have appeared earlier in a paper by Jaksic, Ogata, Pautrat and Pillet [37].

Now we come back to the α - z Rényi relative entropies $D_{\alpha,z}$. They have the operational meaning only if they are monotone under completely positive trace preserving (CPTP) maps. That is,

$$D_{\alpha,z}(\mathcal{E}(\rho)||\mathcal{E}(\sigma)) \leq D_{\alpha,z}(\rho||\sigma), \quad (5.5)$$

for any CPTP map $\mathcal{E} : \mathcal{B}(\mathcal{H})^\times \rightarrow \mathcal{B}(\mathcal{H})^\times$, for all $\rho, \sigma \in \mathcal{D}(\mathcal{H})^\times$ and for any \mathcal{H} .

The inequality (5.5) is known as the *Data Processing Inequality* (DPI). Although DPI is thoroughly studied for D_α and \tilde{D}_α , it remained open that whether DPI holds for $D_{\alpha,z}$ for some range of (α, z) or not. It is well-known that DPI is essentially equivalent to the joint convexity/concavity of the trace functions inside the definition of $D_{\alpha,z}$.

Proposition 5.3. *Let $\alpha, z > 0$ and $\alpha \neq 1$. Set $p = \frac{\alpha}{z}$ and $q = \frac{1-\alpha}{z}$. Then $D_{\alpha,z}$ is monotone under all CPTP maps on $\mathcal{B}(\mathcal{H})^\times$ if and only if one of the following holds*

- (1) $\alpha < 1$ and $\Psi_{p,q,1/(p+q)}$ with $K = I$ is jointly concave;
- (2) $\alpha > 1$ and $\Psi_{p,q,1/(p+q)}$ with $K = I$ is jointly convex.

We will go back to its proof in the end of this section.

Then from some known results on joint convexity and joint concavity of $\Psi_{p,q,1/(p+q)}$ with $K = I$, Audenaert and Datta obtained DPI for $D_{\alpha,z}$ for some—but not full—range of (α, z) [2, Theorem 1]. By saying full we mean necessary and sufficient conditions on (α, z) . It is then natural to ask whether DPI holds for the remaining range of (α, z) . This motivated Audenaert and Datta to raise the following conjecture:

Conjecture 5.4. [2, Conjecture 1] *If $1 \leq p \leq 2$, $-1 \leq q < 0$ and $(p, q) \neq (1, -1)$, then for any $K \in \mathcal{B}(\mathcal{H})^\times$ and any \mathcal{H} ,*

$$\Psi_{p,q,1/(p+q)}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^{\frac{1}{p+q}}, \quad A, B \in \mathcal{P}(\mathcal{H})^\times,$$

is jointly convex.

We cheat a little bit here, since their original form of conjecture concerns the convexity of $\mathcal{P}(\mathcal{H}) \ni A \mapsto \text{Tr}(A^{\frac{q}{2}} K^* A^p K A^{\frac{q}{2}})^{\frac{1}{p+q}}$. However, by doubling dimension, a standard argument shows that they are equivalent. See the discussions after [10, Conjecture 1] for example.

More generally, consider the joint convexity/concavity of trace functions

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s,$$

for $A, B \in \mathcal{P}(\mathcal{H})^\times$, $K \in \mathcal{B}(\mathcal{H})^\times$ and $p, q, s \in \mathbb{R}$. Note that $\Psi_{q,p,s}(B, A) = \Psi_{p,q,s}(A, B)$ with K replaced by K^* , and $\Psi_{-p,-q,-s}(A, B) = \Psi_{p,q,s}(A, B)$ with K replaced by $(K^{-1})^*$. So in the sequel, we may assume that $p \geq q$ and $s > 0$.

The knowledge of joint convexity/concavity of $\Psi_{p,q,s}$ before the survey paper [10] is summarized in the following proposition:

Proposition 5.5. *Fix $K \in \mathcal{B}(\mathcal{H})^\times$.*

- (1) *If $0 \leq q \leq p \leq 1$ and $0 < s \leq \frac{1}{p+q}$, then $\Psi_{p,q,s}$ is jointly concave.*
- (2) *If $-1 \leq q \leq p \leq 0$ and $s > 0$, then $\Psi_{p,q,s}$ is jointly convex.*
- (3) *If $-1 \leq q \leq 0$, $1 \leq p < 2$, $(p, q) \neq (1, -1)$ and $s \geq \min\{\frac{1}{p-1}, \frac{1}{q+1}\}$, then $\Psi_{p,q,s}$ is jointly convex. If $p = 2$, $-1 \leq q \leq 0$ and $s \geq \frac{1}{q+2}$, then $\Psi_{p,q,s}$ is jointly convex.*

The proofs of (1)(2) for full range are due to Hiai [34, Theorem 2.1]. The proofs of (3) are due to Frank and Lieb [26, Proposition 3], and Carlen, Frank and Lieb [9]. For more details of history on these results, see the discussions after [10, Theorem 2]. We only comment here that the case for $s = 1$, which was firstly studied in the history, is due to Lieb [49] for $0 \leq q \leq p \leq 1$ with $p + q \leq 1$, as well as for $-1 \leq q \leq 0$, and due to Ando [1] for $-1 \leq q \leq 0$, $1 \leq p < 2$, with $p + q \geq 1$. Their work played an important role in the development of matrix analysis.

The following proposition gives necessary conditions for $\Psi_{p,q,s}$ to be jointly convex or jointly concave.

Proposition 5.6. *Let $p \geq q$ and $s > 0$. Suppose that $(p, q) \neq (0, 0)$.*

- (1) *If $\Psi_{p,q,s}$ is jointly concave for $\mathcal{H} = \mathbb{C}^2$ and $K = I$, then $0 \leq q \leq p \leq 1$ and $0 < s \leq \frac{1}{p+q}$.*
- (2) *If $\Psi_{p,q,s}$ is jointly convex for $\mathcal{H} = \mathbb{C}^4$ and $K = I$, then either $-1 \leq q \leq p \leq 0$ and $s > 0$ or $-1 \leq q \leq 0$, $1 \leq p \leq 2$, $(p, q) \neq (1, -1)$ and $s \geq \frac{1}{p+q}$.*

From the above two propositions, Carlen, Frank and Lieb conjectured [10] that:

Conjecture 5.7. [10, Conjecture 4] *If $1 \leq p \leq 2$, $-1 \leq q < 0$, $(p, q) \neq (1, -1)$ and $s \geq \frac{1}{p+q}$, then for any $K \in \mathcal{B}(\mathcal{H})^\times$ and any \mathcal{H}*

$$\Psi_{p,q,s}(A, B) = \text{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s, \quad A, B \in \mathcal{P}(\mathcal{H})^\times,$$

is jointly convex.

Partial results of Conjecture 5.7 have been known, as pointed out in Proposition 5.5 (3). The main result of this chapter is to prove Conjecture 5.7, which, together with Proposition 5.5 (1)(2) and Proposition 5.6, will give the full range of (p, q, s) for $\Psi_{p,q,s}$ to be jointly convex or jointly concave:

Theorem 5.8. *Fix $K \in \mathcal{B}(\mathcal{H})^\times$. Suppose that $p \geq q$ and $s > 0$. Then $\Psi_{p,q,s}$ is*

- (1) *jointly concave if $0 \leq q \leq p \leq 1$ and $0 < s \leq \frac{1}{p+q}$;*
- (2) *jointly convex if $-1 \leq q \leq p \leq 0$ and $s > 0$;*
- (3) *jointly convex if $-1 \leq q \leq 0$, $1 \leq p \leq 2$, $(p, q) \neq (-1, 1)$ and $s \geq \frac{1}{p+q}$.*

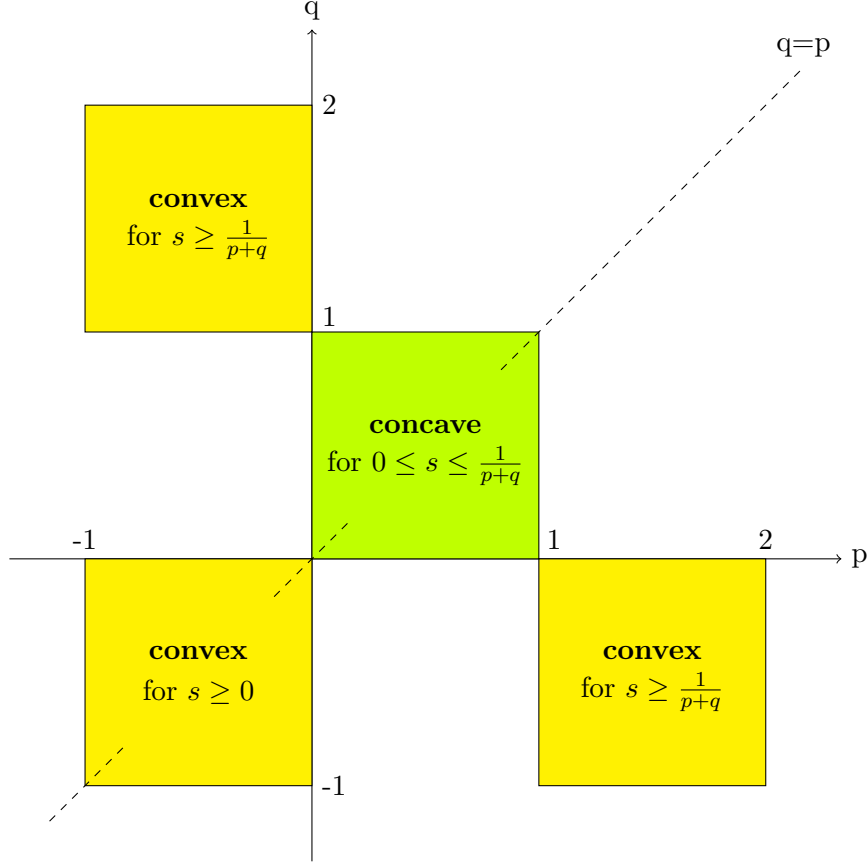
The Figure 5.1 summarizes the joint convexity/concavity of $\Psi_{p,q,s}$ for all (p, q, s) . Note that $(1, -1)$ and $(-1, 1)$ donot belong to the area of convexity.

As a corollary of Proposition 5.6 and Theorem 5.8 we have

Corollary 5.9. *The α -z Rényi relative entropy $D_{\alpha,z}$ is monotone under CPTP maps on $\mathcal{B}(\mathcal{H})^\times$ for all \mathcal{H} if and only if one of the following holds*

- (1) $0 < \alpha < 1$ and $z \geq \max\{\alpha, 1 - \alpha\}$;
- (2) $1 < \alpha \leq 2$ and $\frac{\alpha}{2} \leq z \leq \alpha$;
- (3) $2 \leq \alpha < \infty$ and $\alpha - 1 \leq z \leq \alpha$.

Now we close this section with the proof of Proposition 5.3. It comes from [10], which follows from a well-known argument of Lindblad [50] and Uhlmann [70].

Figure 5.1: Joint convexity/concavity of $\Psi_{p,q,s}$

Proof of Proposition 5.3. We use Ψ to denote $\Psi_{p,q,1/(p+q)}$ with $K = I$. We only prove here that when $\alpha > 1$, $D_{\alpha,z}$ is monotone under CPTP maps on $\mathcal{B}(\mathcal{H})^\times$ for all \mathcal{H} if and only if Ψ is jointly convex, since the proof for $\alpha < 1$ is similar. Note that when $\alpha > 1$, $D_{\alpha,z}$ is monotone under CPTP maps if and only if

$$\Psi(\mathcal{E}(\rho) || \mathcal{E}(\sigma)) \leq \Psi(\rho || \sigma),$$

for all CPTP maps $\mathcal{E} : \mathcal{B}(\mathcal{H})^\times \rightarrow \mathcal{B}(\mathcal{H})^\times$ and density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})^\times$, with \mathcal{H} being any finite dimensional Hilbert space.

To show the “if” part, take any CPTP map $\mathcal{E} : \mathcal{B}(\mathcal{H})^\times \rightarrow \mathcal{B}(\mathcal{H})^\times$. We can write it as

$$\mathcal{E}(\gamma) = \text{Tr}_2 U(\gamma \otimes \delta) U^*,$$

where $\delta \in \mathcal{B}(\mathcal{H}')$, U is unitary on $\mathcal{H} \otimes \mathcal{H}'$, and \mathcal{H}' is a Hilbert space such that $N' := \dim \mathcal{H}' \leq (\dim \mathcal{H})^2$. Tr_2 denotes the usual partial trace over \mathcal{H}' . For a proof, see for example [51, Lemma 5]. It originates in Stinespring’s Theorem [69]. Let du denote the normalized Haar measure on the group of all unitaries on \mathcal{H}' , then

$$\mathcal{E}(\gamma) \otimes \frac{I_{\mathcal{H}'}}{N'} = \int (I_{\mathcal{H}} \otimes u) U(\gamma \otimes \delta) U^* (I_{\mathcal{H}} \otimes u^*) du. \quad (5.6)$$

By the tensor property of Ψ , we have

$$\Psi(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = \Psi \left(\mathcal{E}(\rho) \otimes \frac{I_{\mathcal{H}'}}{N'}, \mathcal{E}(\sigma) \otimes \frac{I_{\mathcal{H}'}}{N'} \right).$$

From the joint convexity of Ψ and (5.6) it follows that

$$\Psi(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \int \Psi((I_{\mathcal{H}} \otimes u)U(\rho \otimes \delta)U^*(I_{\mathcal{H}} \otimes u^*), (I_{\mathcal{H}} \otimes u)U(\sigma \otimes \delta)U^*(I_{\mathcal{H}} \otimes u^*))du.$$

By the unitary invariance and tensor property of Ψ we obtain that

$$\Psi(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \Psi(\rho, \sigma),$$

as desired.

To show the “only if” part, for any $\rho_1, \rho_2, \sigma_1, \sigma_2 \in \mathcal{P}(\mathcal{H})^\times$ and any $0 < \lambda < 1$, define

$$\rho = \begin{pmatrix} \lambda\rho_1 & 0 \\ 0 & (1-\lambda)\rho_2 \end{pmatrix} \text{ and } \sigma = \begin{pmatrix} \lambda\sigma_1 & 0 \\ 0 & (1-\lambda)\sigma_2 \end{pmatrix},$$

in $\mathcal{P}(\mathcal{H} \oplus \mathcal{H})^\times$. Since the map

$$\mathcal{E} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{2} \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix},$$

defines a CPTP map on $\mathcal{B}(\mathcal{H} \oplus \mathcal{H})^\times$, we obtain from the monotonicity of Ψ that

$$\Psi(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \Psi(\rho, \sigma),$$

which is nothing but

$$\Psi(\lambda\rho_1 + (1-\lambda)\rho_2, \lambda\sigma_1 + (1-\lambda)\sigma_2) \leq \lambda\Psi(\rho_1, \sigma_1) + (1-\lambda)\Psi(\rho_2, \sigma_2).$$

This finishes the proof of the joint convexity of Ψ . □

5.3 The proofs

This section is devoted to the proof of Theorem 5.8. The following classical results will serve as building blocks to achieve the joint convexity/concavity of $\Psi_{p,q,s}$. The concavity result is due to Lieb [49] and the convexity is due to Ando [1]. They have been extensively studied and have many simple proofs, see for example [58].

Lemma 5.10. *For any $K \in \mathcal{B}(\mathcal{H})^\times$, the function $\Psi_{p,1-p,1}(A, B) = \text{Tr}K^*A^pB^{1-p}$ is*

- (1) *jointly concave if $0 < p < 1$;*
- (2) *jointly convex if $-1 < p < 0$.*

Theorem 5.8 will be reduced to Lemma 5.10 in three steps, based on the following variational method. This method is the key of the proof and originates in [12]. One can compare it with the other known variational methods in [10].

Theorem 5.11. *For $r_i > 0, i = 0, 1, 2$ such that $\frac{1}{r_0} = \frac{1}{r_1} + \frac{1}{r_2}$, we have for any $X, Y \in \mathcal{B}(\mathcal{H})^\times$ that*

$$\text{Tr}|XY|^{r_0} = \min_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{r_0}{r_1} \text{Tr}|XZ|^{r_1} + \frac{r_0}{r_2} \text{Tr}|Z^{-1}Y|^{r_2} \right\}, \quad (5.7)$$

and

$$\text{Tr}|XY|^{r_1} = \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{r_1}{r_0} \text{Tr}|XZ|^{r_0} - \frac{r_1}{r_2} \text{Tr}|Y^{-1}Z|^{r_2} \right\}. \quad (5.8)$$

Proof. For $0 < p < \infty$ define $\|\cdot\|_p$ as $\|A\|_p^p := \text{Tr}|A|^p$ for any matrix A . For any $Z \in \mathcal{B}(\mathcal{H})^\times$, we have by Hölder's inequality that

$$\text{Tr}|XY|^{r_0} \leq \|XZ\|_{r_1}^{r_0} \|Z^{-1}Y\|_{r_2}^{r_0} = [\text{Tr}|XZ|^{r_1}]^{\frac{r_0}{r_1}} [\text{Tr}|Z^{-1}Y|^{r_2}]^{\frac{r_0}{r_2}}.$$

Then from the Young's inequality for numbers (or AM-GM inequality): $x^\alpha y^\beta \leq \alpha x + \beta y$ for positive x, y and positive α, β such that $\alpha + \beta = 1$, it follows that

$$\text{Tr}|XY|^{r_0} \leq [\text{Tr}|XZ|^{r_1}]^{\frac{r_0}{r_1}} [\text{Tr}|Z^{-1}Y|^{r_2}]^{\frac{r_0}{r_2}} \leq \frac{r_0}{r_1} \text{Tr}|XZ|^{r_1} + \frac{r_0}{r_2} \text{Tr}|Z^{-1}Y|^{r_2}. \quad (5.9)$$

Exchanging Y and Z , we have

$$\text{Tr}|XY|^{r_1} \geq \frac{r_1}{r_0} \text{Tr}|XZ|^{r_0} - \frac{r_1}{r_2} \text{Tr}|Y^{-1}Z|^{r_2}. \quad (5.10)$$

To prove (5.7), let $Y^*X^* = U|Y^*X^*|$ be the polar decomposition of Y^*X^* , then $XYU = |Y^*X^*|$. Set $Z := YU|Y^*X^*|^{-\frac{r_1}{r_1+r_2}}$, then we have

$$XZ = XYU|Y^*X^*|^{-\frac{r_1}{r_1+r_2}} = |Y^*X^*|^{\frac{r_2}{r_1+r_2}}, \quad Z^{-1}Y = |Y^*X^*|^{\frac{r_1}{r_1+r_2}}U^*.$$

Using the facts that $\|\cdot\|_p$ is unitarily invariant and $\|A\|_p = \|A^*\|_p$ for all A , we have

$$\text{Tr}|XZ|^{r_1} = \text{Tr}|Y^*X^*|^{\frac{r_1 r_2}{r_1+r_2}} = \text{Tr}|XY|^{\frac{r_1 r_2}{r_1+r_2}} = \text{Tr}|XY|^{r_0},$$

and

$$\text{Tr}|Z^{-1}Y|^{r_2} = \text{Tr}|Y^*X^*|^{\frac{r_1 r_2}{r_1+r_2}} = \text{Tr}|XY|^{\frac{r_1 r_2}{r_1+r_2}} = \text{Tr}|XY|^{r_0}.$$

Hence $\frac{r_0}{r_1} \text{Tr}|XZ|^{r_1} + \frac{r_0}{r_2} \text{Tr}|Z^{-1}Y|^{r_2} = \text{Tr}|XY|^{r_0}$, which proves (5.7).

Now we prove (5.8) in a similar way. Let U be as above and choose Z to be $YU|Y^*X^*|^{\frac{r_1}{r_2}}$, then

$$XZ = XYU|Y^*X^*|^{\frac{r_1}{r_2}} = |Y^*X^*|^{\frac{r_1+r_2}{r_2}}, \quad Y^{-1}Z = U|Y^*X^*|^{\frac{r_1}{r_2}}.$$

It follows that

$$\text{Tr}|XZ|^{r_0} = \text{Tr}|Y^*X^*|^{\frac{r_1+r_2}{r_0 r_2}} = \text{Tr}|Y^*X^*|^{r_1} = \text{Tr}|XY|^{r_1},$$

and

$$\text{Tr}|Y^{-1}Z|^{r_2} = \text{Tr}|Y^*X^*|^{r_1} = \text{Tr}|XY|^{r_1}.$$

Hence $\text{Tr}|XY|^{r_1} = \frac{r_1}{r_0} \text{Tr}|XZ|^{r_0} - \frac{r_1}{r_2} \text{Tr}|Y^{-1}Z|^{r_2}$. This proves (5.8). \square

Remark 5.12. *It is possible to generalize this variational method to the infinite dimensional case or to more general norm functions, which is beyond the aim of this chapter. It is also possible to apply this variational method to the trace functions with $n \geq 3$ variables. Indeed, let $r_j > 0, j = 0, 1, \dots, n$ such that $\frac{1}{r_0} = \sum_{j=1}^n \frac{1}{r_j}$. Then we have for $X_1, \dots, X_n \in \mathcal{B}(\mathcal{H})^\times$ that*

$$\begin{aligned} & \text{Tr}|X_1 \cdots X_n|^{r_0} \\ &= \min \left\{ \frac{r_0}{r_1} \text{Tr}|X_1 Z_1|^{r_1} + \sum_{j=2}^{n-1} \frac{r_0}{r_j} \text{Tr}|Z_{j-1}^{-1} X_j Z_j|^{r_j} + \frac{r_0}{r_n} \text{Tr}|Z_{n-1}^{-1} X_n|^{r_n} \right\}, \end{aligned} \quad (5.11)$$

and

$$\begin{aligned} & \operatorname{Tr}|X_1 \cdots X_n|^{r_1} \\ &= \max \left\{ \frac{r_1}{r_0} \operatorname{Tr}|X_1 Z_1|^{r_0} - \sum_{j=2}^{n-1} \frac{r_1}{r_j} \operatorname{Tr}|Z_j^{-1} X_j^{-1} Z_{j-1}|^{r_j} - \frac{r_1}{r_n} \operatorname{Tr}|X_n^{-1} Z_{n-1}|^{r_n} \right\}, \end{aligned} \quad (5.12)$$

where \max and \min run over all $Z_1, \dots, Z_{n-1} \in \mathcal{B}(\mathcal{H})^\times$. The proof is similar to the two variables case. We only explain here when \min is achieved for (5.11). Let $X_n^* \cdots X_1^* = U|X_n^* \cdots X_1^*|$ be the polar decomposition of $X_n^* \cdots X_1^*$. Then set

$$Z_j := X_{j+1} \cdots X_n U|X_n^* \cdots X_1^*|^{\alpha_j}, \quad \alpha_j = \sum_{k=1}^j \frac{r_0}{r_k} - 1$$

for $1 \leq j \leq n-1$. One can check that

$$\operatorname{Tr}|X_1 \cdots X_n|^{r_0} = \frac{r_0}{r_1} \operatorname{Tr}|X_1 Z_1|^{r_1} + \sum_{j=2}^{n-1} \frac{r_0}{r_j} \operatorname{Tr}|Z_{j-1}^{-1} X_j Z_j|^{r_j} + \frac{r_0}{r_n} \operatorname{Tr}|Z_{n-1}^{-1} X_n|^{r_n}.$$

Now we are ready to prove Theorem 5.8 with three steps of reductions. Note that the **Step 1** already suffices to finish the proof of Theorem 5.8 and confirm Conjectures 5.4 and 5.7.

Step 1: In the first step we reduce the joint convexity/concavity of $\Psi_{p,q,s}$ to the convexity/concavity of

$$\Upsilon_{p,s}(A) := \operatorname{Tr}(K^* A^p K)^s, \quad A \in \mathcal{P}(\mathcal{H})^\times,$$

for all $K \in \mathcal{B}(\mathcal{H})^\times$, which has already been thoroughly studied.

Theorem 5.13. *For any $K \in \mathcal{B}(\mathcal{H})^\times$, the function $\Upsilon_{p,s}(A) = \operatorname{Tr}(K^* A^p K)^s$ is*

- (1) *concave if $0 < p \leq 1$ and $0 < s \leq \frac{1}{p}$;*
- (2) *convex if $-1 \leq p \leq 0$ and $s > 0$;*
- (3) *convex if $1 \leq p \leq 2$ and $s \geq \frac{1}{p}$.*

The proofs of (1) and (2) are due to Hiai [33, Theorem 4.1]. The proof of (3) is due to Carlen and Lieb [12, Theorem 1.1]. Again, see the discussions after Proposition 5 in [10] for more historical information. We only comment here that the proof of concavity for $0 < p \leq 1$ with $s = \frac{1}{p}$ is due to Epstein [23]. His analytic method is nowadays developed as an important tool in matrix analysis, in particular to deal with concavity (rather than convexity) of trace functions. We will give a simpler proof of this theorem later, without using Epstein's analytic approach.

Proof of Theorem 5.8 given Theorem 5.13. Before proceeding with the proof note first that

$$\Psi_{p,q,s}(A, B) = \operatorname{Tr}(B^{\frac{q}{2}} K^* A^p K B^{\frac{q}{2}})^s = \operatorname{Tr}|A^{\frac{p}{2}} K B^{\frac{q}{2}}|^{2s}.$$

We shall use an easy fact that the joint convexity (resp. joint concavity) is stable under taking \sup/\max (resp. \inf/\min).

(1) If $q = 0$, then the claim reduces to Theorem 5.13 (1). To show the case $0 < q \leq p \leq 1$ and $0 \leq s \leq \frac{1}{p+q}$, set $\lambda := s(p+q) \in (0, 1]$ and we apply (5.7) to $(r_0, r_1, r_2) = (2s, \frac{2\lambda}{p}, \frac{2\lambda}{q})$ and $(X, Y) = (A^{\frac{p}{2}}K, B^{\frac{q}{2}})$:

$$\Psi_{p,q,s}(A, B) = \min_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{p}{p+q} \text{Tr} |A^{\frac{p}{2}} K Z|^{\frac{2\lambda}{p}} + \frac{q}{p+q} \text{Tr} |Z^{-1} B^{\frac{q}{2}}|^{\frac{2\lambda}{q}} \right\} \quad (5.13)$$

Since $0 < \frac{\lambda}{p} \leq \frac{1}{p}$ and $0 < \frac{\lambda}{q} \leq \frac{1}{q}$, from Theorem 5.13 (1) it follows that the maps

$$A \mapsto \frac{p}{p+q} \text{Tr} |A^{\frac{p}{2}} K Z|^{\frac{2\lambda}{p}} = \frac{p}{p+q} \text{Tr} (Z^* K^* A^p K Z)^{\frac{\lambda}{p}}$$

and

$$B \mapsto \frac{q}{p+q} \text{Tr} |Z^{-1} B^{\frac{q}{2}}|^{\frac{2\lambda}{q}} = \frac{q}{p+q} \text{Tr} (Z^{-1} B^q (Z^{-1})^*)^{\frac{\lambda}{q}}$$

are both concave. Hence they are both jointly concave in (A, B) and so is $\Psi_{p,q,s}$ by (5.13).

(2) If $p = 0$, then the claim reduces to Theorem 5.13 (2). Suppose $-1 \leq q \leq p < 0$ and $s > 0$, then we apply (5.8) to $(r_0, r_1, r_2) = (2t, 2s, \frac{2}{-q})$ with $\frac{1}{t} = \frac{1}{s} - q$ and $(X, Y) = (A^{\frac{p}{2}}K, B^{\frac{q}{2}})$:

$$\Psi_{p,q,s}(A, B) = \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{s}{t} \text{Tr} |A^{\frac{p}{2}} K Z|^{2t} + sq \text{Tr} |B^{-\frac{q}{2}} Z|^{\frac{2}{-q}} \right\}. \quad (5.14)$$

Note that $t > 0$, $sq < 0$ and $0 < -q \leq 1$. By Theorem 5.13 (1) and (2), the maps

$$A \mapsto \frac{s}{t} \text{Tr} |A^{\frac{p}{2}} K Z|^{2t} = \frac{s}{t} \text{Tr} (Z^* K^* A^p K Z)^t$$

and

$$B \mapsto sq \text{Tr} |B^{-\frac{q}{2}} Z|^{\frac{2}{-q}} = sq \text{Tr} (Z^* B^{-q} Z)^{\frac{1}{-q}}$$

are both convex. Hence they are both jointly convex in (A, B) and so is $\Psi_{p,q,s}$ by (5.14).

(3) If $q = 0$, then the claim reduces to Theorem 5.13 (3). Suppose $-1 \leq q < 0$, $1 \leq p \leq 2$, $(p, q) \neq (1, -1)$ and $s \geq \frac{1}{p+q}$, then we apply (5.8) to $(r_0, r_1, r_2) = (2t, 2s, \frac{2}{-q})$ with $\frac{1}{t} = \frac{1}{s} - q$ and $(X, Y) = (A^{\frac{p}{2}}K, B^{\frac{q}{2}})$:

$$\Psi_{p,q,s}(A, B) = \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{s}{t} \text{Tr} |A^{\frac{p}{2}} K Z|^{2t} + sq \text{Tr} |B^{-\frac{q}{2}} Z|^{\frac{2}{-q}} \right\}. \quad (5.15)$$

Since $sq < 0$, $0 < -q \leq 1$ and $t = \frac{1}{s-1-q} \geq \frac{1}{p}$, we have by Theorem 5.13 (1) and (3) that the maps

$$A \mapsto \frac{s}{t} \text{Tr} |A^{\frac{p}{2}} K Z|^{2t} = \frac{s}{t} \text{Tr} (Z^* K^* A^p K Z)^t$$

and

$$B \mapsto sq \text{Tr} |B^{-\frac{q}{2}} Z|^{\frac{2}{-q}} = sq \text{Tr} (Z^* B^{-q} Z)^{\frac{1}{-q}}$$

are both convex. Hence they are both jointly convex in (A, B) and so is $\Psi_{p,q,s}$ by (5.15). \square

Step 2: In our second step we reduce Theorem 5.13 to three particular cases.

Remark 5.14. To prove Theorem 5.8 we may require fewer conditions on the convexity/concavity of $\Upsilon_{p,s}$. Namely, we only need that

(1) $\Upsilon_{p,1/p}$ is concave when $0 < p \leq 1$ (Epstein [23]);

(2) $\Upsilon_{p,s}$ is convex when $-1 \leq p < 0$ and $0 < s \leq 1$ (Hiai [33]);

(3) $\Upsilon_{p,1/p}$ is convex when $1 \leq p \leq 2$ (Carlen and Lieb [12]).

Indeed, from the variational formula (5.7) it follows that when $0 < p \leq 1$, $0 < s < \frac{1}{p}$ and $\frac{1}{s} = p + \frac{1}{t}$:

$$\mathrm{Tr}(K^* A^p K)^s = \min_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ s p \mathrm{Tr}(Z^* A^p Z)^{\frac{1}{p}} + \frac{s}{t} \mathrm{Tr}(K^* (Z^{-1})^* Z^{-1} K)^t \right\}.$$

Then the concavity of $\Upsilon_{p,1/p}$ gives the concavity of $\Upsilon_{p,s}$.

When $-1 \leq p < 0$ and $s > 1$, by the variational formula (5.8) we have

$$\mathrm{Tr}(K^* A^p K)^s = \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ s \mathrm{Tr} Z^* A^p Z - (s-1) \mathrm{Tr}(Z^* (K^{-1})^* K^{-1} Z)^{\frac{s}{s-1}} \right\}.$$

Then the convexity of $\Upsilon_{p,1}$ implies the convexity of $\Upsilon_{p,s}$.

When $1 \leq p \leq 2$, $s < \frac{1}{p}$ and $p = \frac{1}{s} + \frac{1}{t}$, we have by the variational formula (5.8)

$$\mathrm{Tr}(K^* A^p K)^s = \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ s p \mathrm{Tr}(Z^* A^p Z)^{\frac{1}{p}} - \frac{s}{t} \mathrm{Tr}(Z^* (K^{-1})^* K^{-1} Z)^t \right\}.$$

Then the convexity of $\Upsilon_{p,1/p}$ implies the convexity of $\Upsilon_{p,s}$.

Before the last step of reduction, we need the following well-known lemma.

Lemma 5.15. *Let X, Y be two convex subsets of vector spaces and let $f : X \times Y \rightarrow \mathbb{R}$ a function. If f is jointly convex on $X \times Y$, then $x \mapsto \inf_{y \in Y} f(x, y)$ is convex. Similarly, if f is jointly concave on $X \times Y$, then $x \mapsto \sup_{y \in Y} f(x, y)$ is concave.*

Proof. We only prove the convexity here. The proof of the concavity case is similar. For any $x_1, x_2 \in X$ and any $0 < \lambda < 1$, set $x := \lambda x_1 + (1 - \lambda)x_2$. Then for any $\epsilon > 0$ and $i = 1, 2$, there exists $y_i \in Y$ such that $f(x_i, y_i) \leq \inf_{y \in Y} f(x_i, y) + \epsilon$. By the joint convexity of f , we have

$$\begin{aligned} \inf_{y \in Y} f(x, y) &\leq f(x, \lambda y_1 + (1 - \lambda)y_2) \\ &\leq \lambda f(x_1, y_1) + (1 - \lambda)f(x_2, y_2) \\ &\leq \lambda \inf_{y \in Y} f(x_1, y) + (1 - \lambda) \inf_{y \in Y} f(x_2, y) + \epsilon. \end{aligned}$$

Then the proof finishes by letting $\epsilon \rightarrow 0^+$. □

Step 3: In the last step, we reduce Theorem 5.8 to Lemma 5.10.

Proof of Theorem 5.13 given Lemma 5.10. It suffices to prove (1)-(3) in Remark 5.14. The proof is inspired by the proof of (2) in [10]. Let us recall it first. If $s = 1$, the convexity of $\Upsilon_{p,1}$ follows from the operator convexity of $A \mapsto A^p$. If $s < 1$, by (5.7) we have

$$\begin{aligned} \mathrm{Tr}(K^* A^p K)^s &= \min_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ s \mathrm{Tr} |A^{\frac{p}{2}} K Z|^2 + (1 - s) \mathrm{Tr} |Z^{-1}|^{\frac{2s}{1-s}} \right\} \\ &= \min_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ s \mathrm{Tr} K^* A^p K Z + (1 - s) \mathrm{Tr} Z^{\frac{s}{s-1}} \right\} \\ &= \min_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ s \mathrm{Tr} K^* A^p K Z^{1-p} + (1 - s) \mathrm{Tr} Z^{\frac{s(1-p)}{s-1}} \right\}. \end{aligned}$$

Since $\frac{s(1-p)}{s-1} < 0$, the function $t \mapsto t^{\frac{s(1-p)}{s-1}}$ is convex. Thus it is well-known that $Z \mapsto \text{Tr} Z^{\frac{s(1-p)}{s-1}}$ is convex (see for example [8, Theorem 2.10]). This, together with Ando's convexity result (Lemma 5.10 (2)) and Lemma 5.15, yields the convexity of $\Upsilon_{p,s}$.

Now we prove (1). There is nothing to prove when $p = 1$. For $0 < p < 1$, by (5.8), we have

$$\begin{aligned} \text{Tr}(K^* A^p K)^{\frac{1}{p}} &= \max_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} |A^{\frac{p}{2}} K Z|^2 - \frac{1-p}{p} \text{Tr} |Z|^{\frac{2}{1-p}} \right\} \\ &= \max_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} K^* A^p K Z - \frac{1-p}{p} \text{Tr} Z^{\frac{1}{1-p}} \right\} \\ &= \max_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} K^* A^p K Z^{1-p} - \frac{1-p}{p} \text{Tr} Z \right\}. \end{aligned}$$

Then by Lieb's concavity result (Lemma 5.10 (1)) and Lemma 5.15, $\Upsilon_{p,1/p}$ is concave.

(3) can be shown similarly. Indeed, the case $p = 1$ is trivial. For $1 < p \leq 2$, we have by (5.7)

$$\begin{aligned} \text{Tr}(K^* A^p K)^{\frac{1}{p}} &= \min_{Z \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} |A^{\frac{p}{2}} K Z|^2 + \frac{p-1}{p} \text{Tr} |Z^{-1}|^{\frac{1}{1-p}} \right\} \\ &= \min_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} K^* A^p K Z + \frac{p-1}{p} \text{Tr} Z^{\frac{1}{1-p}} \right\} \\ &= \min_{Z \in \mathcal{P}(\mathcal{H})^\times} \left\{ \frac{1}{p} \text{Tr} K^* A^p K Z^{1-p} + \frac{p-1}{p} \text{Tr} Z \right\}. \end{aligned}$$

Then by Ando's convexity result (Lemma 5.10 (2)) and Lemma 5.15, $\Upsilon_{p,1/p}$ is convex. \square

Remark 5.16. Although the variational methods of (5.7) and (5.8) admit analogues (5.11) and (5.12) of $n(\geq 3)$ variables, the joint convexity/concavity of

$$\mathcal{P}(\mathcal{H})^\times \times \cdots \times \mathcal{P}(\mathcal{H})^\times \ni (A_1, \dots, A_n) \mapsto \text{Tr}(A_n^{\frac{pn}{2}} K_{n-1}^* \cdots K_1^* A_1^{p_1} K_1 \cdots K_{n-1} A_n^{\frac{pn}{2}})^s$$

can not be derived directly from Theorem 5.13 because of the appearance of the term $\text{Tr} |Z_{j-1}^{-1} X_j Z_j|^{r_j}$. For example, we have

$$\text{Tr} |X_1 X_2 X_3|^{r_0} = \min_{Z_1, Z_2 \in \mathcal{B}(\mathcal{H})^\times} \left\{ \frac{r_0}{r_1} \text{Tr} |X_1 Z_1|^{r_1} + \frac{r_0}{r_2} \text{Tr} |Z_1^{-1} X_2 Z_2|^{r_2} + \frac{r_0}{r_3} \text{Tr} |Z_2^{-1} X_3|^{r_3} \right\}. \quad (5.16)$$

To obtain the joint concavity of

$$\mathcal{P}(\mathcal{H})^\times \times \mathcal{P}(\mathcal{H})^\times \times \mathcal{P}(\mathcal{H})^\times \ni (A_1, A_2, A_3) \mapsto \text{Tr}(A_3^{\frac{p_3}{2}} K_2^* A_2^{\frac{p_2}{2}} K_1^* A_1^{p_1} K_1 A_2^{\frac{p_2}{2}} K_2 A_3^{\frac{p_3}{2}})^s,$$

via the variational method (5.16), the concavity of the function of the form

$$\mathcal{P}(\mathcal{H})^\times \ni A_2 \mapsto \text{Tr} |Y_1 A_2^{\frac{p_2}{2}} Y_2|^{r_2} = \text{Tr}(Y_2^* A_2^{\frac{p_2}{2}} Y_1^* Y_1 A_2^{\frac{p_2}{2}} Y_2)^{\frac{r_2}{2}}$$

is required. Unfortunately, little is known for general $Y_1^* Y_1$. Indeed, Carlen, Frank and Lieb proved that [9, Corollary 3.3] for $p, q, r \in \mathbb{R} \setminus \{0\}$, the function

$$(A, B, C) \mapsto \text{Tr} C^{\frac{r}{2}} B^{\frac{q}{2}} A^p B^{\frac{q}{2}} C^{\frac{r}{2}}$$

is never concave, and it is convex if and only if $q = 2$, $p, r < 0$ and $-1 \leq p + r < 0$.

Bibliography

- [1] T. Ando. Concavity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra Appl.*, 26:203–241, 1979.
- [2] K. M. R. Audenaert and N. Datta. α - z -Rényi relative entropies. *J. Math. Phys.*, 56(2):022202, 16, 2015.
- [3] T. Banica, U. Franz, and A. Skalski. Idempotent states and the inner linearity property. *Bull. Pol. Acad. Sci. Math.*, 60(2):123–132, 2012.
- [4] E. Bédos, G. J. Murphy, and L. Tuset. Co-amenability of compact quantum groups. *Journal of Geometry and Physics*, 40(2):129–153, 2001.
- [5] T. N. Bekjan. On joint convexity of trace functions. *Linear algebra and its applications*, 390:321–327, 2004.
- [6] J. Bergh and J. Löfström. *Interpolation spaces. An introduction*. Springer-Verlag, Berlin-New York, 1976. Grundlehren der Mathematischen Wissenschaften, No. 223.
- [7] W. Böge. Über die Charakterisierung unendlich teilbarer Wahrscheinlichkeitsverteilungen. *J. Reine Angew. Math.*, 201:150–156, 1959.
- [8] E. A. Carlen. Trace inequalities and quantum entropy: an introductory course. *Entropy and the quantum*, 529:73–140, 2010.
- [9] E. A. Carlen, R. L. Frank, and E. H. Lieb. Some operator and trace function convexity theorems. *Linear Algebra Appl.*, 490:174–185, 2016.
- [10] E. A. Carlen, R. L. Frank, and E. H. Lieb. Inequalities for quantum divergences and the Audenaert–Datta conjecture. *Journal of Physics A: Mathematical and Theoretical*, 51(48):483001, 2018.
- [11] E. A. Carlen and E. H. Lieb. A Minkowski type trace inequality and strong subadditivity of quantum entropy. In *Differential operators and spectral theory*, volume 189 of *Amer. Math. Soc. Transl. Ser. 2*, pages 59–68. Amer. Math. Soc., Providence, RI, 1999.
- [12] E. A. Carlen and E. H. Lieb. A Minkowski type trace inequality and strong subadditivity of quantum entropy. II. Convexity and concavity. *Lett. Math. Phys.*, 83(2):107–126, 2008.
- [13] M. Caspers. The L^p -Fourier transform on locally compact quantum groups. *J. Operator Theory*, 69(1):161–193, 2013.

-
- [14] M. Caspers and M. De La Salle. Schur and Fourier multipliers of an amenable group acting on non-commutative L^p -spaces. *Transactions of the American Mathematical Society*, 367(10):6997–7013, 2015.
- [15] M. Caspers, J. Parcet, M. Perrin, and É. Ricard. Noncommutative de Leeuw theorems. In *Forum of Mathematics, Sigma*, volume 3. Cambridge University Press, 2015.
- [16] Y. A. Chapovsky and L. I. Vainerman. Compact quantum hypergroups. *J. Operator Theory*, 41(2):261–289, 1999.
- [17] T. Cooney. A Hausdorff-Young inequality for locally compact quantum groups. *Internat. J. Math.*, 21(12):1619–1632, 2010.
- [18] I. Csiszár. Generalized cutoff rates and Rényi’s information measures. *IEEE Transactions on information theory*, 41(1):26–34, 1995.
- [19] B. Das, U. Franz, and X. Wang. Invariant Markov semigroups on quantum homogeneous spaces. *arXiv:1901.00791*, 2019.
- [20] L. Delvaux and A. Van Daele. Algebraic quantum hypergroups. *Adv. Math.*, 226(2):1134–1167, 2011.
- [21] L. Delvaux and A. Van Daele. Algebraic quantum hypergroups II. Constructions and examples. *Internat. J. Math.*, 22(3):407–434, 2011.
- [22] J. Dixmier. Formes linéaires sur un anneau d’opérateurs. *Bull. Soc. Math. France*, 81:9–39, 1953.
- [23] H. Epstein. Remarks on two theorems of E. Lieb. *Comm. Math. Phys.*, 31:317–325, 1973.
- [24] S. A. Evdokimov, I. N. Ponomarenko, and A. M. Vershik. Algebras in Plancherel duality and algebraic combinatorics. *Functional Analysis and Its Applications*, 31(4):252–261, 1997.
- [25] T. Fack and H. Kosaki. Generalized s -numbers of τ -measurable operators. *Pacific J. Math.*, 123(2):269–300, 1986.
- [26] R. L. Frank and E. H. Lieb. Monotonicity of a relative Rényi entropy. *J. Math. Phys.*, 54(12):122201, 5, 2013.
- [27] U. Franz and R. Gohm. Random walks on finite quantum groups. In *Quantum independent increment processes. II*, volume 1866 of *Lecture Notes in Math.*, pages 1–32. Springer, Berlin, 2006.
- [28] U. Franz and A. Skalski. A new characterisation of idempotent states on finite and compact quantum groups. *C. R. Math. Acad. Sci. Paris*, 347(17-18):991–996, 2009.
- [29] U. Franz and A. Skalski. On idempotent states on quantum groups. *J. Algebra*, 322(5):1774–1802, 2009.
- [30] U. Franz, A. Skalski, and R. Tomatsu. Idempotent states on compact quantum groups and their classification on $U_q(2)$, $SU_q(2)$, and $SO_q(3)$. *J. Noncommut. Geom.*, 7(1):221–254, 2013.

- [31] A. M. González-Pérez, M. Junge, and J. Parcet. Smooth Fourier multipliers in group algebras via Sobolev dimension. *Ann. Sci. École Norm. Sup.*, 50:879–925, 2017.
- [32] U. Haagerup. An example of a non nuclear c^* -algebra, which has the metric approximation property. *Inventiones mathematicae*, 50(3):279–293, 1978.
- [33] F. Hiai. Concavity of certain matrix trace and norm functions. *Linear Algebra Appl.*, 439(5):1568–1589, 2013.
- [34] F. Hiai. Concavity of certain matrix trace and norm functions. II. *Linear Algebra Appl.*, 496:193–220, 2016.
- [35] F. Hiai and D. Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in mathematical physics*, 143(1):99–114, 1991.
- [36] L. Hörmander. Estimates for translation invariant operators in L^p spaces. *Acta Math.*, 104:93–140, 1960.
- [37] V. Jaksic, Y. Ogata, Y. Pautrat, and C. Pillet. Entropic fluctuations in quantum statistical mechanics. an introduction. In *Quantum Theory from Small to Large Scales: Lecture Notes of the Les Houches Summer School: Volume 95, August 2010*. Oxford University Press, 2012.
- [38] M. Junge, T. Mei, and J. Parcet. Smooth Fourier multipliers on group von Neumann algebras. *Geometric and Functional Analysis*, 24(6):1913–1980, 2014.
- [39] M. Junge, T. Mei, and J. Parcet. Noncommutative Riesz transforms–dimension free bounds and Fourier multipliers. *Journal of the European Mathematical Society*, 20(3), 2018.
- [40] M. Kalantar, M. Neufang, and Z. Ruan. Poisson boundaries over locally compact quantum groups. *Internat. J. Math.*, 24(3):1350023, 21, 2013.
- [41] A. A. Kalyuzhnyi. Conditional expectations on compact quantum groups and new examples of quantum hypergroups. *Methods Funct. Anal. Topology*, 7(4):49–68, 2001.
- [42] P. Kasprzak and P. M. Sołtan. The lattice of idempotent states on a locally compact quantum group. *ArXiv e-prints*, February 2018.
- [43] Y. Kawada and K. Itô. On the probability distribution on a compact group. I. *Proc. Phys.-Math. Soc. Japan (3)*, 22:977–998, 1940.
- [44] S. V. Kerov. Duality of finite-dimensional $*$ -algebras. *Vestnik Leningrad. Univ.*, (7 Mat. Meh. Astronom. Vyp. 2):23–29, 170, 1974.
- [45] S. Kullback. A lower bound for discrimination information in terms of variation (corresp.). *IEEE transactions on Information Theory*, 13(1):126–127, 1967.
- [46] S. Kullback and R. A. Leibler. On information and sufficiency. *The annals of mathematical statistics*, 22(1):79–86, 1951.
- [47] R. A. Kunze. L_p Fourier transforms on locally compact unimodular groups. *Trans. Amer. Math. Soc.*, 89:519–540, 1958.
- [48] J. Kustermans and S. Vaes. Locally compact quantum groups. *Ann. Sci. École Norm. Sup. (4)*, 33(6):837–934, 2000.

-
- [49] E. H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Advances in Math.*, 11:267–288, 1973.
- [50] G. Lindblad. Expectations and entropy inequalities for finite quantum systems. *Comm. Math. Phys.*, 39:111–119, 1974.
- [51] G. Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40(2):147–151, 1975.
- [52] A. Maes and A. Van Daele. Notes on compact quantum groups. *Nieuw Arch. Wisk. (4)*, 16(1-2):73–112, 1998.
- [53] J. P. McCarthy. Random Walks on Finite Quantum Groups: Diaconis-Shahshahani Theory for Quantum Groups. *arxiv:math/1709.09357*, September 2017.
- [54] M. Mosonyi and F. Hiai. On the quantum Rényi relative entropies and related capacity formulas. *IEEE Trans. Inform. Theory*, 57(4):2474–2487, 2011.
- [55] M. Mosonyi and T. Ogawa. Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. *Comm. Math. Phys.*, 334(3):1617–1648, 2015.
- [56] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On quantum Rényi entropies: a new generalization and some properties. *J. Math. Phys.*, 54(12):122203, 20, 2013.
- [57] S. Neuwirth and É. Ricard. Transfer of Fourier multipliers into Schur multipliers and sumsets in a discrete group. *Canadian Journal of Mathematics*, 63(5):1161–1187, 2011.
- [58] I. Nikoufar, A. Ebadian, and G. M. Eshaghi. The simplest proof of Lieb concavity theorem. *Adv. Math.*, 248:531–533, 2013.
- [59] A. Pal. A counterexample on idempotent states on a compact quantum group. *Lett. Math. Phys.*, 37(1):75–77, 1996.
- [60] K. R. Parthasarathy. Infinitely divisible representations and positive definite functions on a compact group. *Comm. Math. Phys.*, 16:148–156, 1970.
- [61] G. Pisier and Q. Xu. Non-commutative L^p -spaces. In *Handbook of the geometry of Banach spaces, Vol. 2*, pages 1459–1517. North-Holland, Amsterdam, 2003.
- [62] A. Rényi. On measures of entropy and information. In *Proc. 4th Berkeley Sympos. Math. Statist. and Prob., Vol. I*, pages 547–561. Univ. California Press, Berkeley, Calif., 1961.
- [63] É. Ricard and Q. Xu. A noncommutative martingale convexity inequality. *Ann. Probab.*, 44(2):867–882, 2016.
- [64] P. Salmi. Idempotent states on locally compact groups and quantum groups. In *Algebraic methods in functional analysis*, pages 155–170. Springer, 2014.
- [65] L. Schmetterer. On Poisson laws and related questions. pages 169–185, 1972.
- [66] I. E. Segal. A non-commutative extension of abstract integration. *Ann. of Math. (2)*, 57:401–457, 1953.

-
- [67] Y. Sekine. An example of finite-dimensional Kac algebras of Kac-Paljutkin type. *Proc. Amer. Math. Soc.*, 124(4):1139–1147, 1996.
- [68] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.
- [69] W. F. Stinespring. Positive functions on C^* -algebras. *Proc. Amer. Math. Soc.*, 6:211–216, 1955.
- [70] A. Uhlmann. Endlich-dimensionale Dichtematrizen. II. *Wiss. Z. Karl-Marx-Univ. Leipzig Math.-Natur. Reihe*, 22:139–177, 1973.
- [71] H. Umegaki. Conditional expectation in an operator algebra. IV. Entropy and information. *Kodai Math. Sem. Rep.*, 14:59–85, 1962.
- [72] E. P. Wigner and Mutsuo M. Yanase. Information contents of distributions. *Proc. Nat. Acad. Sci. U.S.A.*, 49:910–918, 1963.
- [73] M. M. Wilde, A. Winter, and D. Yang. Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. *Comm. Math. Phys.*, 331(2):593–622, 2014.
- [74] S. L. Woronowicz. Compact quantum groups. In *Symétries quantiques (Les Houches, 1995)*, pages 845–884. North-Holland, Amsterdam, 1998.
- [75] H. Zhang. Carlen-Frank-Lieb conjecture and monotonicity of α - z Rényi relative entropy. *arXiv:1811.01205*, 2018.
- [76] H. Zhang. Idempotent states on Sekine quantum groups. *Communications in Algebra*, 0(0):1–19, 2019.
- [77] H. Zhang. Infinitely divisible states on finite quantum groups. *Mathematische Zeitschrift*, 2019.