بسم الله الرحمن الرحیم

جبرهای اندازه و کاربردها

دوفصلنامهٔ علمی دانشگاه قم

سال اول، شماره دوم، بهار و تابستان ۱۴۰۳، شماره پیاپی ۲

صاحب امتیاز: دانشگاه قم
مدیرمسئول: دکتر علیرضا باقری ثالث
سردبیر: دکتر مرتضی میرزائی ازندریانی

- در این دوفصلنامه، مقالاتی انتشار می‌یابند که مرتبط با آنالیز ریاضی و به‌ویژه در ارتباط با فضاهای اندازه باشند (فارسی همراه با چکیدهٔ مبسوط انگلیسی).
- مسئولیت مطالب هر مقاله بر عهدهٔ نویسنده است.
- نقل مطالب دوفصلنامه با ذکر منبع مانعی ندارد.
- دوفصلنامه در ویرایش، اختصار و اصلاح مقاله‌ها آزاد است.

نشانی: قم، بلوار الغدیر، دانشگاه قم، ساختمان مرکزی، دفتر دوفصلنامهٔ جبرهای اندازه و کاربردها.
کد پستی: ۳۷۱۶۱۴۶۶۱۱، تلفن: ۰۲۵-۳۲۱۰۳۳۶۰
Website: maa.qom.ac.ir ∗ Email: maa@qom.ac.ir

راهنمای نگارش مقاله

۱. مقاله باید پیش‌از این منتشر نشده باشد و نباید هم‌زمان به مجلهٔ دیگری ارسال شده باشد.

۲. پذیرش اولیهٔ مقاله منوط به نگارش مقاله در فایل نمونهٔ قرارگرفته در وبگاه مجله (قسمت راهنمای نویسندگان) و باتوجه‌به توضیحات ذکرشده در آن است. در ضمن، فایل LaTeX مقاله باید بدون خطا اجرا شود و هر دو فایل LaTeX و PDF مقاله، توسط نویسندهٔ محترم از طریق سامانهٔ مجله ارسال شوند.

۳. حداقل دو صفحهٔ اول مقاله باید به زبان انگلیسی نوشته شوند (چکیده و چکیدهٔ مبسوط انگلیسی).

۴. منابع مقاله باید مطابق استانداردهای مجله (که در فایل نمونه ذکر شده است) باشند.

۵. دوفصلنامه در رد یا قبول، ویرایش، اختصار و اصلاح مقاله‌ها آزاد است.

۶. درصورتی‌که مقاله بیش از یک نویسنده داشته باشد، محتوای مقاله باید مورد تأیید همهٔ نویسندگان باشد.

۷. نقل و اقتباس از مقاله‌های مجله با ذکر منبع آزاد است.

۸. در صورت استفاده از دستاوردهای پژوهشی دیگران یا بخشی از پژوهش‌های خود، ذکر منبع الزامی است.

جبرهای اندازه و کاربردها

فهرست مقالات

Measure Algebras and Applications

On the $L_p(G)$ spaces as topological lattice vector groups

Mohammad Ali Ranjbar[1], **Seyyed Hassan Myrnouri**[2]✉

1. Teacher and free researcher. Email: maaliranjbar@gmail.com
2. Corresponding Author, Department of Mathematics, Lahijan Branch, Islamic Azad University, Lahijan, Iran. Email: myrnouri@liau.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 31 December 2023
Received in revised form:
01 March 2024
Accepted: 15 June 2024
Published Online:
20 August 2024

Keywords:
ℓ-group,
Unital ℓ-group,
Order unit,
Locally compact group,
Haar measure,
Riesz algebra,
Topological lattice-ordered ring

2020 Mathematics Subject Classification: 06F20, 06F25

ABSTRACT

In this paper, we consider the $L_p(G)$ spaces with pointwise ordering as Riesz spaces and investigate some lattice group topologies on them. In many cases, these topologies which are called link topologies or positive filter topologies are not vector topologies in the sense that the scalar multiplication is not continuous with respect to them, but they have many useful properties.

Cite this article: Ranjbar, M.A., & Myrnouri, S.H. (2024). On the $L_p(G)$ spaces as topological lattice vector groups. *Measure Algebras and Applications*, 1(2), 1–13. http://doi.org/10.22091/MAA.2024.10266.1013

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10266.1013

Extended Abstract

Introduction

Ordered algebraic structures have been investigated by many mathematicians. In the last decades, many researchers introduced and investigated lattice topologies on the ordered algebraic structures [12], [19], [14], [23], [27] and [29]. In 1998, Gusic introduced the concept of an admissible subset of a 2-divisible lattice-ordered group H, which induces a topology on it. This topology is a group topology and also is locally solid. The Gusic topology investigated by Ranjbar and Pourgholamhossein in [23] and [27] and Yang in [29]. In [23], the authors introduced the concept of links as a generalization of admissible subsets of a lattice-ordered group. The topology induced by a link is Hausdorff. If the lattice-ordered group H is Archimedean with order unit, then the set of all order units is a link and called the strong link. It is a case that the lattice-ordered group is also an Archimedean Riesz space. However the link topology in an Archimedean Riesz space is not necessarily a vector topology. The authors in [24] showed that the link topology in an Archimedean Riesz space is a vector topology if and only if the link is the strong link. Although the link topology in a Riesz space is not a vector topology in general, it makes the Riesz space into a locally convex topological vector group [17]. The notion of topological vector group was defined and studied by Raikov in [25] and [26].

Positive filter topology on a lattice-ordered group is another lattice group topology which was introduced and investigated in [19] and [14]. A positive filter is a subset of the positive cone of an ℓ- group which induces the positive filter topology. Every link in an ℓ-group is a positive filter. In some cases, the positive filter topology and link topology on an ℓ-group are the same, which have been investigated by authors in [24].

In this work, we review the last researches about the introduction of lattice topologies on a Riesz space and we investigate some properties of these topologies on $L_p(G)$ $(0 < p < \infty)$ spaces, where G is a locally compact abelian group with the Haar measure. In fact, we consider $L_p(G)$ $(0 < p < \infty)$ as Riesz spaces with pointwise ordering in the sense of almost everywhere. The Riesz spaces $L_p(G)$ or $L_p(X, \Sigma, \mu)$ are very important in functional analysis. It is well known that for $1 \leq p$, $L_p(G)$ spaces are Banach lattices with respect to the integral norm. A famous theorem about the spaces $L_p(G)$ or more generally $L_p(X, \Sigma, \mu)$ is that every abstract L_p-space has a representation of the form $L_p(X, \Sigma, \mu)$ (see [1] for more details). Furthermore, as we shall see later, $L_p(G)$ is a locally convex topological vector group with respect to every link topology on it. We also see that some of the link topologies are finer than the integral norm topology on $L_p(G)$.

We show that if G is not discrete, then for every $0 < p < \infty$ and every neighborhood U of zero in G, there is an unbounded $f \in L_p(G)$ such that $supp(f)$ is contained in U. We also show that an $L_p(G)$ $(0 < p < \infty)$ does not contain an order unit unless G is finite. We introduce the notion of *completely positive* functions in an $L_p(G)$ and we show that the set of all completely positive functions is a link in $L_p(G)$ if G is σ-compact. A completely positive function is a real-valued measurable function on G which is far from zero almost everywhere.

It is well known that in $L_p(G)$ the pointwise multiplication is not closed in general. We introduce the concept of *p-ideal* subspace of an $L_p(G)$ which is closed under pointwise multiplication. More precisely, for $0 < p < \infty$, a function $f \in L_p(G)$ is p-ideal, if for every $g \in L_p(G)$, we have $f.g \in L_p(G)$. For instance, every characteristic function on a compact subset of G is a p-ideal of $L_p(G)$ for all $0 < p < \infty$. The set of all p-ideal functions is a linear subspace of $L_p(G)$ and we call it the p-ideal subspace of $L_p(G)$.

We show that this is an order-ideal of $L_p(G)$. We also show that the p-ideal subspace of an $L_p(G)$ with pointwise multiplication is a Riesz algebra. In addition, we give a link topology on the p-ideal subspace of $L_p(G)$ which makes it a topological lattice-ordered ring.

Conclusion

In this paper, the following concepts are presented:
1- A completely positive measurable function.
2- A p-ideal function in an $L_p(G)$.
3- A p-ideal subspace of an $L_p(G)$ and we denote it by $IL_p(G)$.
4- The link IP in $IL_p(G)$.

Also, the next theorems, propositions and corollaries are presented:
1- The Riesz space of $L_p(G)$ contains a strong link, if G is a finite group.
2- If G is a σ-compact locally compact abelian group, then the set of all completely positive functions in $L_p(G)$ is a link in $L_p(G)$ $(0 < p < \infty)$.
3- $IL_p(G)$ is a Riesz subspace and an order-ideal of $L_p(G)$. Furthermore, $IL_p(G)$ is closed under pointwise multiplication and is a Riesz algebra.
4- If G is σ-compact, then $IL_p(G)$ is a topological lattice-ordered ring with respect to some of the link topologies.

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۳-۱

بررسی فضاهای $L_p(G)$ به‌عنوان گروه‌های برداری مشبکه توپولوژیکی

محمدعلی رنجبر [۱] ، سید حسن میرنوری [۲]✉

۱. قم. آموزش‌وپرورش ناحیه چهارم. رایانامه: maaliranjbar@gmail. com
۲. نویسندهٔ مسئول، گروه ریاضی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. رایانامه: myrnouri@liau. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۰/۱۰
تاریخ بازنگری: ۱۴۰۲/۱۲/۱۱
تاریخ پذیرش: ۱۴۰۳/۳/۲۶
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
گروه مشبکه،
گروه مشبکهٔ یکانی،
یکّهٔ ترتیبی،
گروه فشردهٔ موضعی،
اندازهٔ هار،
جبر ریس،
حلقهٔ مشبکهٔ توپولوژیک

رده‌بندی ریاضی:
06F20, 06F25

چکیده

در این مقاله، فضاهای $L_p(G)$ را با رابطهٔ ترتیب نقطه‌ای به‌عنوان فضاهای ریس در نظر می‌گیریم و دسته‌ای از توپولوژی‌های گروهی (با عمل جمع) مشبکه‌ای را روی آن‌ها بررسی خواهیم کرد. این توپولوژی‌ها که توپولوژی‌های فیلتری مثبت و یا توپولوژی‌های زنجیره‌ای نام دارند، در بسیاری از مواقع توپولوژی برداری نیستند، بدین معنا که عمل ضرب اسکالر در آن‌ها پیوستهٔ توأم نیست، ولی بسیاری از ویژگی‌های مورد انتظار را دارند.

استناد: رنجبر، محمدعلی.، میرنوری، سید حسن. (۱۴۰۳). بررسی فضاهای $L_p(G)$ به‌عنوان گروه‌های برداری مشبکه توپولوژیکی. جبرهای اندازه و کاربردها، ۱(۲)، ۱۳-۱.

http://doi.org/10.22091/MAA.2024.10266.1013

ناشر: دانشگاه قم.

۱ مقدمه و پیش‌نیازها

ساختارهای جبری مرتب از اوایل قرن بیستم مورد توجه ریاضی‌دانان بزرگ جهان بوده است. همچنین رابطهٔ بین آن‌ها و MV -جبرها نیز به‌وسیلهٔ بسیاری از ریاضی‌دانان ازجمله موندیچی مورد بررسی قرار گرفته است، تا جایی که موندیچی نشان داد که رستهٔ گروه‌های مشبکهٔ یکانی با رستهٔ همهٔ MV -جبرها، یکریخت رسته‌ای است [۲۰]. یادآور می‌شویم که مفهوم MV -جبر، در سال ۱۹۵۸ میلادی توسط چانگ و به‌عنوان تعمیمی از مفهوم جبر بولی معرفی شد [۴]. می‌دانیم که در یک MV -جبر، مجموعهٔ همهٔ عناصر خودتوان، همراه با اعمال مشبکه، تشکیل یک جبر بولی می‌دهد [۵]. در دهه‌های اخیر، ساخت و بررسی توپولوژی‌ها بر روی گروه‌های مشبکه و فضاهای ریس مورد توجه بسیاری از پژوهشگران در ایران و جهان قرار گرفته است [۱۲]، [۱۹]، [۱۴]، [۲۳]، [۲۷]، [۲۸] و [۲۹]. این توپولوژی‌ها باید با اعمال جبری و اعمال مشبکه‌ای سازگار باشند. بدین معنا که عمل دوتایی جمع و عمل‌های دوتایی سوپریمم و اینفیمم تحت این توپولوژی‌ها پیوسته باشند. در این مقاله، پس از بیان خواص مقدماتی گروه‌های مشبکه، فضاهای ریس و فضاهای L_p، مختصری از پژوهش‌های نوین پیرامون ساخت توپولوژی‌های مشبکه‌ای در گروه‌های مشبکه و فضاهای ریس را بیان می‌کنیم. همچنین به تطبیق و بررسی این توپولوژی‌ها در یک فضای $L_p(G)$ می‌پردازیم که در آن G یک گروه فشردهٔ موضعی آبلی با اندازهٔ هار است. در انتها نیز یک سؤال بی‌پاسخ را در این خصوص مطرح خواهیم کرد. یک گروه مشبکه عبارت است از یک گروه جزئاً مرتب (یک گروه به‌همراه یک رابطهٔ ترتیب $\leq$ بر روی آن که تحت انتقال پایا است؛ بدین معنا که اگر $x \leq y$ ، آنگاه برای هر عنصر z در گروه، $x + z \leq y + z$) که هر زیرمجموعهٔ متناهی از آن، دارای سوپریمم و اینفیمم باشد. (سوپریمم مجموعهٔ دو عضوی x, y را با $x \vee y$ و اینفیمم آن را با $x \wedge y$ نمایش می‌دهیم). برای اطلاع از خواص گروه‌های جزئاً مرتب و گروه‌های مشبکه به [۱۰] و [۱۱] مراجعه نمایید. در اینجا ما گروه مشبکهٔ $(L, +, \leq)$ را همواره آبلی در نظر می‌گیریم و آن را به‌اختصار با L نمایش می‌دهیم و عضو خنثی نیز همواره با 0 نمایش داده می‌شود. همچنین مجموعهٔ همهٔ عناصر $x \in L$ که در رابطهٔ $x \leq 0$ صدق کنند، را با L^+ نمایش می‌دهیم که مجموعهٔ عناصر مثبت نامیده می‌شود.

تعریف ۱.۱. عنصر مثبت u در گروه مشبکهٔ L را یکّهٔ ترتیبی نامند، هرگاه برای هر $x \in L$، عدد طبیعی n یافت شود به‌طوری‌که $x \leq nu$. همچنین یک گروه مشبکهٔ یکانی یا ℓ -گروه یکانی، عبارت است از یک گروه مشبکه که دارای یکّهٔ ترتیبی باشد.

تعریف ۲.۱. اگر L, H گروه‌های مشبکه باشند، آنگاه همریختی گروهی $f : L \to H$ را یک همریختی مثبت گوییم اگر $f(L^+) \subseteq H^+$. همچنین f را همریختی گروه‌های مشبکه نامیم، اگر علاوه‌بر خواص بالا، داشته باشیم:

$$f(x \wedge y) = f(x) \wedge f(y)$$

و

$$f(x \vee y) = f(x) \vee f(y).$$

گزاره ۳.۱. [۶] در هر گروه مشبکهٔ آبلی L، برای هر $x, y \in L$ و هر عدد طبیعی n داریم:

$$n(x \vee y) = nx \vee ny, \quad n(x \wedge y) = nx \wedge ny.$$

لازم به توضیح است که هر گروه مشبکهٔ آبلی، نمایش‌پذیر است (ر.ک [۶]، گزاره ۶.۴۷) یعنی ℓ -زیرگروه حاصل‌ضربی از گروه‌های کاملاً مرتب است. حال، گزارهٔ بالا به‌طور مستقیم از گزاره ۱۰.۴۷ (در همین مرجع) نتیجه می‌شود. گروه مشبکهٔ L را ارشمیدسی [1] نامیم، اگر برای $x, y \in G$، هرگاه نامساوی $nx \leq y$ برای هر عدد طبیعی n برقرار باشد، آنگاه $x \leq 0$. زیرمجموعهٔ A از گروه مشبکهٔ G را جامد [2] نامیم هرگاه برای هر $a \in A$ و هر $x \in G$، اگر $|x| \leq |a|$، آنگاه $x \in A$ که در آن $|x| = x \vee (-x)$ قدرمطلق x نام دارد. فضای برداری حقیقی E به‌همراه رابطهٔ ترتیب جزئی $\leq$ یک فضای ریس نام دارد، هرگاه اولاً $(E, \leq)$ با عمل جمع، یک گروه مشبکه باشد و ثانیاً اگر $x, y \in E$ به‌طوری‌که $x \leq y$، آنگاه نامساوی $rx \leq ry$ برای هر عدد حقیقی مثبت r برقرار باشد. برای اطلاع از خواص مقدماتی مشبکه‌ها و فضاهای ریس به [۱] و [۵] مراجعه نمایید. یک جبر ریس عبارت است از یک جبر حقیقی مانند A همراه با یک رابطهٔ ترتیب جزئی $\leq$ که A به‌عنوان یک فضای برداری حقیقی، همراه با این رابطهٔ ترتیب، یک فضای ریس باشد و علاوه‌بر آن اگر $x, y \in A^+$ آنگاه $x.y \geq 0$ [۲۲]. گروه مشبکهٔ L به‌همراه توپولوژی τ را یک گروه مشبکهٔ توپولوژیک نامیم، هرگاه (L, τ) یک گروه توپولوژیک باشد و علاوه‌بر آن نگاشت‌های $(x, y) \to x \vee y$ و $(x, y) \to x \wedge y$ از $L \times L$ به L پیوسته باشند. در این حالت توپولوژی τ را توپولوژی گروهی مشبکه‌ای نامند. همچنین (L, τ) را گروه مشبکهٔ جامد موضعی نامیم اگر مبدأ دارای پایهٔ موضعی با عناصر جامد باشد. به همین

[1] Archimedean
[2] solid

ترتیب فضای ریس جامد موضعی تعریف می‌شود. لازم به توضیح است که $S \subseteq L$ را جامد نامند، اگر برای هر $x \in S$ و هر $y \in L$، اگر $|y| \leq |x|$، آنگاه $y \in S$.

فرض کنیم G یک گروه فشردهٔ موضعی آبلی باشد و μ اندازهٔ هار روی آن باشد. در این صورت برای هر $0 < p < \infty$، $L_p(G)$ را مجموعهٔ همهٔ توابع اندازه‌پذیر حقیقی مقدار روی G در نظر می‌گیریم که $\int_G |f|^p \, d\mu < \infty$. همان‌گونه که می‌دانیم $L_p(G)$ یک فضای برداری حقیقی است و با اعمال جمع نقطه‌ای و ضرب اسکالر، یک فضای برداری است. یادآور می‌شویم مفهوم تساوی در $L_p(G)$ با یک رابطهٔ هم‌ارزی تعریف می‌شود. مثلاً دو تابع $f, g \in L_p(G)$ را مساوی گوییم اگر تقریباًهمه‌جا مساوی باشند. یعنی

$$\mu\{x \in G : f(x) \neq g(x)\} = 0.$$

برای اطلاع از خواص مقدماتی گروه‌های فشردهٔ موضعی و توابع انتگرال‌پذیر به [۸] و [۹] مراجعه نمایید. حال برای هر $0 < p < \infty$، رابطهٔ ترتیب نقطه‌ای را به مفهوم تقریباًهمه‌جا بر روی $L_p(G)$ در نظر می‌گیریم. یعنی $f \leq g$ اگر و تنها اگر نامساوی $f(x) \leq g(x)$ تقریباًهمه‌جا برقرار باشد. برای هر $f, g \in L_p(G)$ می‌دانیم که $f \wedge g$ اندازه‌پذیر است و ثانیاً

$$\int_G |f \wedge g|^p \, d\mu \leq \int_G (|f| + |g|)^p \, d\mu < \infty.$$

بنابراین $L_p(G)$ با این رابطهٔ ترتیب، یک فضای ریس است. همچنین یک بررسی ساده نشان می‌دهد که $L_p(G)$ یک فضای ریس ارشمیدسی است. البته معمولاً به‌جای گروه فشردهٔ موضعی G، فضای اندازه (X, Σ, μ) را در نظر می‌گیرند و به همین ترتیب ثابت می‌شود که $L_p(X, \Sigma, \mu)$ یک فضای ریس ارشمیدسی است [۱].

فرض کنیم E یک فضای ریس و مجهز به نرم ریس N باشد (یعنی N یک نرم باشد به‌طوری‌که برای هر $x, y \in E$، نامساوی $|x| \leq |y|$، نامساوی $N(x) \leq N(y)$ را نتیجه دهد). فضای E را یک مشبکهٔ باناخ نامند، اگر E به‌همراه نرم ریس N یک فضای باناخ باشد. همچنین به‌ازای عدد حقیقی $p \leq 1$، نرم N را p- جمع‌پذیر نامند اگر تساوی

$$(N(x) + N(y))^p = (N(x))^p + (N(y))^p$$

برای هر $x, y \in E^+$ که $x \wedge y = 0$ برقرار باشد. مشبکهٔ باناخ (E, N) را یک فضای L_p مجرد نامند، اگر نرم ریس N، p- جمع‌پذیر باشد. ثابت شده است که برای هر فضای اندازهٔ (X, Σ, μ) و هر $p \leq 1$، فضای ریس $L_p(X, \Sigma, \mu)$ با نرم انتگرالی

$$\| f \|_p = \left(\int_X |f|^p \, d\mu \right)^{\frac{1}{p}}$$

یک مشبکهٔ باناخ و همچنین یک L_p- فضای مجرد است. یادآور می‌شویم که یک L_p- فضای مجرد عبارت است از یک مشبکهٔ باناخ که نرم آن اولاً یک نرم ریس و ثانیاً p- جمع‌پذیر باشد. قضیهٔ زیر که تلفیقی از قضایای کاکوتانی [۱] [۱۶]، بانبلاست [۲] [۳] و ناکانو [۳] [۲۱] است، نشان می‌دهد که حتی هر L_p- فضای مجرد، یکریخت مشبکه‌ای با یک فضا به شکل بالا است.

قضیه ۴.۱. ([۱]، قضیه ۳۳.۳. کاکوتانی- بانبلاست- ناکانو) برای هر $p \leq 1$، هر L_p- فضای مجرد، یکریخت مشبکه‌ای با یک مشبکهٔ باناخ $L_p(X, \Sigma, \mu)$ است.

ملاحظه ۵.۱. همان‌گونه که می‌بینیم مطالب ذکرشده در بالا فقط برای حالت‌هایی است که $p \leq 1$ و همان‌گونه که می‌دانیم، اگر $p < 1$ حتی ممکن است $\| \cdot \|_p$ یک نرم نباشد و در واقع نامساوی مثلثی ممکن است برقرار نباشد.

تعریف ۶.۱. فرض کنیم E یک فضای ریس باشد و $C \subseteq E^+$. C را یک زنجیره در E نامیم اگر شرایط زیر برقرار باشند.

۱) اگر $x, y \in C$، آنگاه $x \wedge y \in C$.

۲) اگر $x \leq y$ و $x \in C$، آنگاه $y \in C$.

۳) $0 \notin C$.

۴) $\inf(C) = 0$.

۵) اگر $x \in C$ آنگاه $rx \in C$ برای هر $0 < r \leq 1$.

همچنین $F \subseteq E$ را یک فیلتر مثبت نامند اگر خواص ۱و۲و ۵ فوق را داشته باشد.

[1] Kakutani
[2] Bohnenblust
[3] Nakano

تعریف ۷.۱. فرض کنیم Ω یک زنجیره در E باشد. برای هر $g \in E$ و $r \in \Omega$ مجموعهٔ زیر را در نظر می‌گیریم.

$$U_{g,r} = \{x \in G, r - |x - g| \in \Omega\}$$

گردایهٔ همهٔ مجموعه‌های به شکل $U_{g,r}$ $(r \in \Omega, g \in E)$ تشکیل یک توپولوژی روی E می‌دهد که آن را توپولوژی زنجیره‌ای القاشده با Ω یا Ω -توپولوژی گوییم.

ملاحظه ۸.۱. زنجیره‌ها در اصل روی گروه‌های مشبکه تعریف می‌شوند و خاصیت ۵ که در بالا ذکر شد، در گروه‌های مشبکه تعمیم داده می‌شود و بیان آن خارج از اهداف این مقاله است. برای اطلاع از خواص توپولوژی‌های زنجیره‌ای به [۲۳]، [۲۴] و [۲۷] مراجعه نمایید.

قضیهٔ زیر از قضیه ۴ در [۲۳] و نتیجه ۱۰.۲ در [۱۷] نتیجه می‌شود. ابتدا تعریف زیر را یادآور می‌شویم که برای اولین بار رایکوف در [۲۵] آن را معرفی کرد.

تعریف ۹.۱. یک فضای برداری X به‌همراه توپولوژی τ روی آن را یک گروه برداری توپولوژیک نامند اگر اولاً (X, τ) به‌همراه عمل جمع یک گروه توپولوژیک هاسدورف باشد و ثانیاً τ دارای یک پایهٔ موضعی متعادل [۱] در صفر باشد.

در برخی منابع در تعریف گروه برداری توپولوژیک، به‌جای متعادل موضعی بودن، شرط کلی‌تری را ارائه داده‌اند که عبارت است از اینکه برای هر اسکالر (حقیقی یا مختلط) α، نگاشت $x \mapsto \alpha x$ از X به X پیوسته باشد [۷] و [۱۸].

قضیه ۱۰.۱. اگر Ω یک زنجیره در E باشد، آنگاه E به‌همراه Ω- توپولوژی، یک گروه برداری توپولوژیک هاسدورف، جامد موضعی و محدب موضعی است.

فرض کنیم F یک فیلتر مثبت در فضای ریس E باشد، آنگاه برای هر $a \in F$ و برای هر $r \in F$ و هر عدد طبیعی n، مجموعهٔ زیر را در نظر می‌گیریم

$$N_{\frac{r}{n}}(a) = \{x \in E : n\,|x - a| \leq r\}.$$

گردایهٔ چنین مجموعه‌هایی، یک پایه برای یک توپولوژی روی E است. توپولوژی تولیدشده توسط این مجموعه‌ها را توپولوژی فیلتری مثبت نامند. البته مجموعه‌های به شکل $N_{\frac{r}{n}}(a)$ در این توپولوژی باز نیستند، بلکه هرکدام از آن‌ها حاوی یک همسایگی باز و مشمول در یک همسایگی بازند. در واقع پایهٔ توپولوژی در توپولوژی فیلتری مثبت، متشکل از مجموعه‌هایی به فرم زیر است

$$T_{\frac{r}{n}}(a) = \left\{x \in E : \exists k \in \mathbb{N}, N_{\frac{r}{k}}(x) \subseteq N_{\frac{r}{n}}(a)\right\}$$

که در آن $r \in F, a \in E$ و $n \in \mathbb{N}$ و می‌توان آن را یک گوی باز به مرکز a و شعاع $\frac{1}{n}r$ تصور کرد. البته این گفته بدین معنا نیست که توپولوژی فیلتری مثبت، توپولوژی متری است و ممکن است که این توپولوژی، مترپذیر نباشد. این توپولوژی را با τ_F نمایش می‌دهیم. برای اطلاع از ویژگی‌های توپولوژی فیلتری مثبت به [۱۴] و [۱۹] مراجعه نمایید. در زیر برخی از ویژگی‌های اساسی این توپولوژی و رابطهٔ آن با توپولوژی زنجیره‌ای بیان خواهند شد.

قضیه ۱۱.۱. ([۱۹]، قضیه ۵.۲) اگر F یک توپولوژی فیلتری مثبت در گروه مشبکهٔ G باشد، آنگاه (G, τ_F) یک گروه مشبکهٔ توپولوژیک است.

قضیه ۱۲.۱. ([۲۴]، قضیه ۵.۲). اگر F یک زنجیره در گروه مشبکهٔ L باشد، آنگاه توپولوژی زنجیره‌ای القاشده با F و توپولوژی τ_F یکسان‌اند.

البته همان‌گونه که پیش‌ازاین نیز بیان شد، در این تحقیق، نظر ما معطوف به فضای ریس $L_p(G)$ است و قضایای بالا را بر روی چنین فضایی اعمال می‌کنیم.

[1] balanced

۲ گروه‌های برداری مشبکه توپولوژیک

مثال ۱.۲. فرض کنیم G یک گروه فشردهٔ موضعی و $K \subseteq G$ فشرده باشد به‌طوری‌که $\mu(K) > ۰$ که در آن μ اندازهٔ هار روی G است. برای هر $۰ < p \leq \infty$ قرار می‌دهیم

$$L_p^+(G) = \{f \in L_p(G) : ۰ \leq f\}$$

و

$$P_K := \left\{f \in L_p^+(G) : f(x) > ۰, \forall x \in K\right\}.$$

اولاً با توجه به اینکه $\chi_K \in P_K$، لذا $P_K \neq \emptyset$. ثانیاً روشن است که اگر $f \leq g$ و $f \in P_K$، آنگاه $g \in P_K$. ثالثاً $f \wedge g \in P_K$ برای هر $f, g \in P_K$. همچنین برای هر $f \in P_K$ و برای هر عدد طبیعی n روشن است که $\frac{۱}{n} f \in P_K$. ازاینجا نتیجه می‌گیریم که $\inf\{f : f \in P_K\} = ۰$. بنابراین P_K یک زنجیره در $L_p(G)$ است. فرض کنیم $۱ \leq p$ و $\mu(K) = ۱$. می‌بینیم که برای هر عدد طبیعی n، $\frac{۱}{n}\chi_K \in P_K$. همچنین برای هر عدد طبیعی n و هر $f \in N_{\frac{\chi_K}{n}}(۰)$ داریم $n|f| \leq \chi_K$ و درنتیجه

$$n \parallel f \parallel_p \leq \parallel \chi_K \parallel^p = ۱.$$

بنابراین $N_{\frac{\chi_K}{n}}(۰) \subseteq \left\{f \in L_p : \parallel f \parallel_p \leq \frac{۱}{n}\right\}$. با توجه به اینکه $T_{\frac{\chi_K}{n}}(۰) \subseteq N_{\frac{\chi_K}{n}}(۰)$ بنابراین توپولوژی فیلتری مثبت روی $L_p(G)$ که با P_K القاء شده است، ظریف‌تر از توپولوژی حاصل از نرم $\parallel . \parallel_p$ است.

از مثال بالا می‌بینیم که برای هر زیرمجموعهٔ فشرده با اندازهٔ بزرگ‌تر از صفر در G، یک توپولوژی گروهی هاسدورف روی $L_p(G)$ ساخته می‌شود. حال این دو سؤال مطرح می‌شود. ۱) آیا ممکن است توپولوژی زنجیره‌ای روی فضای $L_p(G)$، یک توپولوژی برداری باشد؟ ۲) آیا هر زنجیره در $L_p(G)$، به‌صورت P_K است که در آن K یک زیرمجموعهٔ با اندازهٔ ناصفر در G است؟
برای پاسخ به سؤال اول ابتدا گزارهٔ زیر را یادآور می‌شویم.

گزاره ۲.۲. ([۲۴] گزاره ۷.۴) اگر G یک گروه فشردهٔ موضعی ناگسسته یا یک گروه نامتناهی با توپولوژی گسسته باشد، آنگاه $L_p(G)$ $(۱ \leq p < \infty)$ با رابطهٔ ترتیب نقطه‌ای، یکّهٔ ترتیبی ندارد.

لم ۳.۲. اگر گروه فشردهٔ موضعی G گسسته نباشد، آنگاه برای هر همسایگی صفر مانند U در G، تابع $f \in L_p(G)$ وجود دارد که اولاً بی‌کران است و ثانیاً $supp(f) \subseteq U$.

اثبات. فرض کنیم $U \subseteq G$ یک همسایگی صفر باشد. با استفاده از روشی که در برهان گزاره ۲.۲ به کار رفته است، یک دنبالهٔ تودرتو از همسایگی‌های باز و متقارن صفر مانند $(U_n)_n$ وجود دارد که $۲\mu(U_{n+۱}) \leq \mu(U_n)$ و $\overline{U_۱} \subseteq U$. برای نشان دادن این نکته، فرض کنیم $U_۱ \subseteq U$ یک همسایگی باز و متقارن صفر باشد که بستار آن نیز زیرمجموعهٔ U باشد. چون G گسسته نیست، عنصر $۰ \neq a \in U_۱$ وجود دارد و چون G هاسدورف است، لذا همسایگی باز و متقارن $U_۲$ از صفر وجود دارد که $U_۲ \cap a + U_۲ = \emptyset$. می‌توان $U_۲$ را طوری در نظر گرفت که $a + U_۲ \subseteq U_۱$ ، $U_۲$. بنابراین

$$۲\mu(U_۲) = \mu(U_۲) + \mu(a + U_۲) \leq \mu(U_۱).$$

به همین ترتیب همسایگی‌های باز $U_۳, U_۴, ...$ ساخته می‌شوند. می‌توان $U_۱$ را طوری در نظر گرفت که $\mu(U_۱) < \infty$. حال تابع حقیقی مقدار f را روی G به‌صورت زیر می‌سازیم. برای هر $x \in G \setminus U_۱$ قرار می‌دهیم $f(x) = ۰$. برای هر عدد طبیعی n و هر $x \in U_n \setminus U_{n+۱}$، قرار می‌دهیم $f(x) = n$. می‌بینیم تابع f بی‌کران است. همچنین داریم

$$۰ < \int_G f^p d\mu \leq (۱ + \frac{۲^p}{۲} + \frac{۳^p}{۴} + ... + \frac{n^p}{۲^{n-۱}} + ...)\mu(U_۱).$$

با توجه به اینکه سری $\Sigma_{n=۱}^{\infty} \frac{n^p}{۲^{n-۱}}$ برای هر $۰ < p$ همگراست، لذا انتگرال بالا متناهی است. □

نتیجه ۴.۲. فضای ریس $L_p(G)$ حاوی یک زنجیرهٔ قوی است اگر و تنها اگر G یک گروه متناهی باشد.

اثبات. فرض کنیم G یک گروه متناهی باشد. لذا هر تابع در $L_p(G)$ کران‌دار است و درنتیجه تابع ثابت ۱ یکّهٔ ترتیبی است. چون فضای ریس $L_p(G)$ ارشمیدسی است، لذا مجموعهٔ همهٔ یکّه‌های ترتیبی در آن، یک زنجیرهٔ قوی است. برعکس، فرض کنیم P یک زنجیرهٔ قوی در $L_p(G)$ باشد. لذا $L_p(G)$ حاوی یکّهٔ ترتیبی خواهد بود و طبق گزاره ۲.۲ G گسسته و متناهی است. □

مثال زیر نشان می‌دهد که زنجیره‌ها در $L_p(G)$ لزوماً به فرم P_K که در مثال ۱.۲ بیان شد نیستند.

مثال ۵.۲. فرض کنیم G یک گروه فشردهٔ موضعی ناگسسته و $\mathcal{K}$ مجموعهٔ همهٔ همسایگی‌های فشردهٔ صفر در G باشد (بنابراین با توجه به مفروضات، $0 < \mu(K) < \infty$ برای هر $K \in \mathcal{K}$). قرار می‌دهیم

$$C = \left\{ f \in L_p^+(G) : \exists K \in \mathcal{K}, K \subseteq pos(f) \right\}$$

که در آن $pos(f) = \{x \in G : f(x) > 0\}$. نشان می‌دهیم C یک زنجیره در $L_p(G)$ است. اگر $f, g \in L_p(G)$، آنگاه همسایگی‌های فشردهٔ K_1, K_2 از مبدأ وجود دارند که در شرایط بالا صدق می‌کنند. بنابراین $K_1 \cap K_2 \subseteq pos(f \wedge g)$ که نتیجه می‌دهد $f \wedge g \in C$. خواص ۲و ۳و ۴و ۵ زنجیره‌ها نیز به‌وضوح برقرارند.

تعریف ۶.۲. برای هر گروه فشرده موضعی G، تابع اندازه‌پذیر $f : G \to \mathbb{R}$ را کاملاً مثبت نامیم اگر برای هر زیرمجموعهٔ فشرده K از G، عدد $\epsilon > 0$ وجود داشته باشد که

$$\mu\left(f^{-1}(-\epsilon, \epsilon) \cap K\right) = 0.$$

به‌عبارت‌دیگر، تابع f کاملاً مثبت است اگر مقادیر این تابع بر هر زیرمجموعهٔ فشرده از G، تقریباًهمه‌جا دور از صفر باشند.

قضیه ۷.۲. اگر G یک گروه فشردهٔ موضعی و سیگما-فشرده باشد، آنگاه مجموعهٔ توابع کاملاً مثبت در $L_p(G)$ یک زنجیره در $L_p(G)$ است $(0 < p < \infty)$.

اثبات. مجموعهٔ همهٔ توابع کاملاً مثبت در $L_p(G)$ را با P نمایش می‌دهیم. ابتدا نشان می‌دهیم P تهی نیست. اگر $\mu(G) < \infty$ آنگاه روشن است که تابع ثابت ۱ در P است. فرض کنیم $\mu(G) = \infty$ ابتدا حالت $\frac{1}{2} < p < \infty$ را در نظر می‌گیریم. چون G سیگما-فشرده است، لذا یک دنباله از زیرمجموعه‌های باز پیش‌فشرده و ناتهی مانند $(U_n)_n$ وجود دارد (یعنی بستار هرکدام فشرده است) که تحت شمول صعودی است و $G = \cup_{n=1}^{\infty} U_n$ ([۹]، گزاره ۳۹.۴). برای هر n قرار می‌دهیم $K_n = \overline{U_n}$. بدون کاستن از کلیت برای هر $n > 1$ می‌توان فرض کرد $\mu(K_n \setminus K_{n-1}) > 0$. حال قرار می‌دهیم $f_1 = \frac{\chi_{K_1}}{\mu(K_1)}$ و برای هر عدد طبیعی $n > 1$ قرار می‌دهیم

$$f_n = \left(\chi_{K_n \setminus K_{n-1}}\right) \left(n^2 \mu(K_n)\right)^{-1}.$$

داریم:

$$\int_G f_1(x) d\mu(x) = \int_{K_1} f_1(x) d\mu(x) = 1$$

و همچنین برای هر $n > 1$ خواهیم داشت:

$$\int_G f_n(x) d\mu(x) = \int_{K_n \setminus K_{n-1}} f_n(x) d\mu(x) = \frac{\mu(K_n \setminus K_{n-1})}{n^2 \mu(K_n)} \leq \frac{1}{n^2}.$$

حال تابع حقیقی مقدار f روی G را چنین تعریف می‌کنیم

$$f(x) = \vee_{n=1}^{\infty} f_n(x).$$

با توجه به اینکه برای هر $x \in G$، دنبالهٔ $(f_n(x))_n$ کران‌دار است، لذا سوپریمم بالا برای هر $x \in G$ موجود است. بنابراین، تابع f یک تابع پله‌ای خواهد بود و مقادیر آن روی هرکدام از مجموعه‌های $K_1,\ K_2 \setminus K_1,\ K_3 \setminus K_2,\ K_4 \setminus K_3, \ldots$ ثابت و مثبت هستند و در هیچ نقطه‌ای صفر نیستند. لذا اگر قرار دهیم $K_0 = \emptyset$ خواهیم داشت:

$$\int_G |f(x)|^p \, d\mu(x) = \sum_{n=1}^{\infty} \int_{K_n \setminus K_{n-1}} f_n^p(x) d\mu(x) \leq \sum_{n=1}^{\infty} \frac{1}{n^{2p}} < \infty$$

که نامساوی آخر به این دلیل است که از ابتدا فرض کردیم $p > \frac{1}{2}$. اگر $0 < p \leq \frac{1}{2}$، آنگاه توابع f_n را به‌صورت

$$f_n = \left(\chi_{K_n \setminus K_{n-1}}\right)\left(n^k \mu(K_n)\right)^{-1}$$

تعریف می‌کنیم که در آن k عددی طبیعی است که $kp > 1$. همچنین تابع f را مانند قبل تعریف می‌کنیم و با قرار دادن در انتگرال بالا خواهیم داشت

$$\int_G |f(x)|^p \, d\mu(x) \leq \sum_{n=1}^{\infty} \frac{1}{n^{kp}} < \infty.$$

ازاین‌رو $f \in P$. ادعا می‌کنیم که f کاملاً مثبت است. فرض کنیم $K \subseteq G$ فشرده و دلخواه باشد. چون $K \subseteq \cup_{n=1}^{\infty} U_n$، لذا عدد طبیعی m وجود دارد که $K \subseteq \cup_{n=1}^{m} U_n$ و لذا $K \subseteq \cup_{n=1}^{m} K_n$. با توجه به نحوهٔ ساخت تابع f_m، می‌بینیم که مقادیر تابع f روی K بزرگ‌تر یا مساوی $\left(m^2 \mu(K_m)\right)^{-1}$ خواهند بود. حال کافی است عدد مثبت ϵ را طوری انتخاب کنیم که $\epsilon < \left(m^2 \mu(K_m)\right)^{-1}$. بنابراین

$$\mu\left(f^{-1}(-\epsilon, \epsilon) \cap K\right) = 0.$$

حال نشان می‌دهیم که P یک زنجیره است. روشن است که اگر $f, g \in P$، آنگاه $f \wedge g \in P$ و اگر $f \in P$ و $f \leq g$، آنگاه $g \in P$. برای نشان دادن اینکه $\inf(P) = 0$، فرض کنیم v یک کران پایین برای P باشد. لذا $v^+ = 0 \vee v$ کران پایین دیگری برای P است. بنابراین برای هر تابع $f \in P$ خواهیم داشت $v^+ \leq f$. با توجه به اینکه برای هر $f \in P$ و هر عدد طبیعی n، $\frac{1}{n} f \in P$، لذا نامساوی $v^+ \leq \frac{1}{n} f$ برای هر عدد طبیعی n برقرار است و این بدین معناست که $v^+ = 0$. درنتیجه $v \leq 0$. سایر ویژگی‌های زنجیره‌ها نیز به‌وضوح برقرارند. □

با توجه به اینکه عمل ضرب نقطه‌ای در $L_p(G)$ بسته نیست، لذا معمولاً ضرب‌های دیگری روی فضای $L_p(G)$ در نظر گرفته می‌شوند که آن را تبدیل به یک جبر کنند. به‌عنوان مثال ضرب پیچشی روی $L_1(G)$ که آن را به‌همراه نرم انتگرالی، به یک جبر باناخ مبدل می‌کند، کاربرد زیادی در جبر اندازه‌ها دارد. اما این ضرب فقط به ازای $p = 1$ روی $L_p(G)$ تعریف می‌شود. در اینجا سعی داریم به ضرب نقطه‌ای در $L_p(G)$ بازگردیم، ولی این ضرب را روی تمام فضا اعمال نمی‌کنیم و در این خصوص تعریف زیر را ارائه می‌دهیم.

تعریف ۸.۲. تابع $f \in L_p(G)$ $(0 < p < \infty)$ را یک تابع p- ایده‌آل نامیم، اگر برای هر $g \in L_p(G)$، $f.g \in L_p(G)$.
همچنین مجموعهٔ همهٔ توابع p- ایده‌آل در $L_p(G)$ را زیرفضای p- ایده‌آل $L_p(G)$ نامیم و با $IL_p(G)$ نمایش می‌دهیم.

روشن است که برای هر $0 < p < \infty$ و برای هر زیرمجموعهٔ فشردهٔ G مانند K، داریم $\chi_K \in IL_p(G)$. در زیر دلیل انتخاب این نام برای این توابع، با یک قضیه روشن می‌شود.

قضیه ۹.۲. الف) $IL_p(G)$ یک زیرفضای ریس و همچنین یک ایده‌آل ترتیبی در $L_p(G)$ است.
ب) $IL_p(G)$ با رابطهٔ ترتیب نقطه‌ای و ضرب نقطه‌ای، یک جبر ریس است.

اثبات. الف) اگر $f, g \in IL_p(G)$، آنگاه برای هر $h \in L_p(G)$ داریم $h.f, h.g \in L_p(G)$ و درنتیجه

$$h.(f + g) = h.f + h.g \in L_p(G).$$

سایر ویژگی‌های فضای برداری به‌وضوح برقرارند. حال فرض کنیم $f, g \in IL_p(G)$. اگر $h \in L_p(G)$ دلخواه باشد، آنگاه خواهیم داشت $|h.(f \wedge g)| \leq |h.f| \in L_p(G)$ که این نتیجه می‌دهد $f \wedge g \in L_p(G)$. بنابراین $IL_p(G)$ با رابطهٔ ترتیب نقطه‌ای یک فضای ریس است. همچنین روشن است که اگر $f \in IL_p(G)$ و $|g| \leq |f|$، آنگاه $g \in IL_p(G)$. بنابراین $IL_p(G)$ یک ایده‌آل ترتیبی در $L_p(G)$ است.

ب) برای دیدن اینکه $IL_p(G)$ یک جبر ریس است، کافی است ملاحظه کنیم که اگر $f, g \in IL_p(G)$ و $f \leq g$ آنگاه نامساوی $f.h \leq g.h$ برای هر $h \in (IL_p(G))^+$ برقرار است. □

مجموعهٔ توابع کاملاً مثبت در $IL_p(G)$ را با IP نمایش می‌دهیم. در قضیه ۷.۲ دیدیم که P یک زنجیره در $L_p(G)$ است، به شرط اینکه G سیگما-فشرده باشد. اگر G سیگما-فشرده باشد، خواص ۱و۲و۳و ۵ از زنجیره‌ها به‌وضوح برای IP نیز برقرارند. برهان اینکه $\inf(IP) = 0$، همانند برهان $\inf(P) = 0$ در قضیه ۷.۲ است و درنتیجه IP یک زنجیره در $IL_p(G)$ است.

نتیجه ۱۰.۲. اگر G سیگما-فشرده باشد، آنگاه زنجیرهٔ IP در $IL_p(G)$ نسبت به عمل ضرب بسته است.

گزاره ۱۱.۲. اگر G سیگما-فشرده باشد، آنگاه $IL_p(G)$ با توپولوژی زنجیره‌ای IP، یک حلقهٔ توپولوژیک است. بدین معنا که علاوه‌بر اینکه توپولوژی زنجیره‌ای IP یک توپولوژی گروهی روی $IL_p(G)$ است، عمل ضرب نقطه‌ای توابع نیز نسبت به این توپولوژی پیوسته است.

اثبات. نشان می‌دهیم که عمل ضرب برداری در صفر پیوسته است. با توجه به اینکه توپولوژی فیلتری مثبت که به‌وسیلهٔ IP القا شده است، با توپولوژی زنجیره‌ای القاشده به‌وسیلهٔ IP یکی است، کافی است که این پیوستگی در توپولوژی فیلتری مثبت ثابت شود. فرض کنیم $u \in IP$ دلخواه باشد. نشان می‌دهیم عناصر $v, w \in IP$ وجود دارند که $N_v(\circ).N_w(\circ) \subseteq N_u(\circ)$. قبل از برهان این ادعا، ابتدا به این نکته اشاره می‌کنیم که چون برای هر $u \in IP$، و هر $n \in \mathbf{N}$، داریم $\frac{1}{n}u \in IP$، لذا می‌توانیم تمام همسایگی‌های صفر در $IL_p(G)$ را در توپولوژی فیلتری مثبت به‌صورت $N_u(\circ)$ در نظر بگیریم. حال تابع v را برای هر $x \in G$ به‌صورت زیر تعریف می‌کنیم

$$v(x) = \min\{u(x), 1\}.$$

بنابراین تابع v نیز اندازه‌پذیر، کاملاً مثبت و در $IL_p(G)$ است و درنتیجه $v \in P$. چون برای هر $x \in G$، $v(x) \leq 1$، بنابراین $v^2 \leq v$. حال اگر $f, g \in N_v(\circ)$ آنگاه $|g| \leq v, |f| \leq v$، و خواهیم داشت

$$|fg| = |f|\,|g| \leq v^2 \leq v \leq u$$

که این نیز نتیجه می‌دهد $N_v(\circ).N_v(\circ) \subseteq N_u(\circ)$. □

ملاحظه ۱۲.۲. لازم به ذکر است که عمل ضرب اسکالر در $IL_p(G)$ نسبت به توپولوژی زنجیره‌ای IP پیوسته نیست، مگر آنکه G یک گروه متناهی باشد. لذا اگر G متناهی نباشد (حتی اگر فشرده باشد)، هیچ‌کدام از توپولوژی‌های زنجیره‌ای، فضای $IL_p(G)$ را به یک جبر توپولوژیک مبدل نمی‌کنند.

References

[1] Aliprantis, C.D., & Burkinshaw, O. (2003). Locally Solid Riesz Spaces with Applications to Economics. *Math Surveys and Monographs*, Volume 105, *American Math. Society*.

[2] Birkhoff, G. (1967). Lattice Theory. *A.M.S. Colloquium Publications*.

[3] Bohnenblust, H.F. (1940). On axiomatic characterization of L_p-spaces. *Duke Math. J*, 6, 627–640. DOI: https://doi.org/10.1215/S0012-7094-40-00648-2.

[4] Chang, C.C. (1958). Algebraic analysis of many valued logics. *Trans. Amer. Math. Soc*, 88, 467–490. DOI: https://doi.org/10.2307/1993227.

[5] Cignoli, R., Ottaviano, I.M.L.D., & Mundici, D. (2000). Algebraic Foundations of many-valued Reasoning. *Kluwer Academic Publ, Dordrecht*. DOI: https://doi.org/10.1007/978-94-015-9480-6.

[6] Darnel, M. (1995). Theory of lattice-ordered groups. *Marcel Dekker, New York*.

[7] Dominguez, X., & Tarieladze, V. (2008). Group topologies on vector spaces and character lifting properties. *Bol. Soc. Mat. Mexicana (3)*, 14, 21–34.

[8] Folland, G.B. (1994). A Course in Abstract Harmonic Analysis. *CRC Press*. DOI: https://doi.org/10.1201/b19172.

[9] Folland, G.B. (1999). Real Analysis: Modern Techniques and Their Applications. *Wiley, New York, second edition*.

[10] Glass, A.M.W. (1999). Partially Ordered Groups. *World Scientific Publishing Co. Pte. Ltd.*

[11] Goodearl, K.R. (1986). Partially Ordered Abelian Groups With Interpolation. *Amer. Mathematical Society (Mathematical Surveys and Monographs)*. DOI: https://doi.org/10.1090/surv/020.

[12] Gusic, I. (1998). A topology on lattice-ordered groups. *Proc Amer Math Soc*, 126(9), 2593–2597.

[13] Hahn, H. (1907). Uber die nichtarchimedischen Groben-systeme. *Sitz. ber. K. Akad. der Wiss., Math. Nat. KI. IIa*, 116, 601–655.

[14] Jordan, F., & Pajoohesh, H. (2018). Topologies on abelian lattice-ordered groups induced by a positive filter and completeness. *Algebra Universalis*, 79(62), 1–18. DOI: https://doi.org/10.1007/s00012-018-0543-7.

[15] Kadison, R.V. (1951). A representation theory for commutative topological algebra. *Mem. A M S, No. 7*.

[16] Kakutani, S. (1941). Concrete Representation of Abstract (L)-Spaces and the Mean Ergodic Theorem. *Ann. of Math*, 42, 523–537. DOI: https://doi.org/10.2307/1968915.

[17] Karamdoust, S., Myrnouri, H., & Pourgholamhossein, M. (2024). On the Boolean algebra induced by a unital ℓ-group. *Algebra Universalis*, 85, 16. DOI: https://doi.org/10.1007/s00012-024-00848-6.

[18] Kenderov, P. (1970). On topological vector groups. *Mat. Sb*, 10, 531–546. DOI: https://doi.org/10.1070/SM1970v010n04ABEH001679.

[19] Kopperman, R., Pajoohesh, H., & Richmond, T. (2011). Topologies arising from metrics valued in abelian ℓ-groups. *Algebra Universalis*, 65, 315–330. DOI: https://doi.org/10.1007/s00012-011-0132-5.

[20] Mundici, D. (1986). Interpretation of AF C*-algebras in Lukasiewicz sentential calculus. *J. Funct. Anal*, 65, 15–63. DOI: https://doi.org/10.1016/0022-1236(86)90015-7.

[21] Nakano, H. (1955). Semi-Ordered Linear Spaces. *Japan Society for the Promotion of Science*, Tokyo.

[22] Pagter. B. de. (1981). F-Algebras and Orthomorphisms. *Ph. D. Dissertation, Leiden*.

[23] Pourgholamhossein, M., & Ranjbar, M.A. (2019). On the topological mass Lattice Groups. *Positivity*, 23, 811–827. DOI: https://doi.org/10.1007/s11117-018-0639-5.

[24] Pourgholamhossein, M., & Ranjbar, M.A. (2022). Positive filters and links in an ℓ-group. *Quaestiones Mathematicae*, 45, 1297–1308. DOI: https://doi.org/10.2989/16073606.2021.1942287.

[25] Raikov, D.A. (1964). Free locally convex spaces for uniform spaces. *Mat. Sb. (N.S)*, 63(105), 582–590.

[26] Raikov, D.A. (1968). On B-complete topological vector groups. *Studia Math*, 31, 295–306.

[27] Ranjbar, M.A., & Pourgholamhossein, M. (2020). Filter and weak link topologies. *Algebra Universalis*, 81, 41. DOI: https://doi.org/10.1007/s00012-020-00670-w.

[28] Wu, S., Luan, W., & Yang, Y. (2020). Filter topologies on MV-algebras ll. *Soft Computing*, 24, 3173–3177. DOI: https://doi.org/10.1007/s00500-020-04682-5.

[29] Yang, Y. (2009). The C-topology on lattice-ordered groups. *Sci China Ser A*, 52(11), 2397–2403. DOI: https://doi.org/10.1007/s11425-009-0098-3.

Measure Algebras and Applications

Complete Magic Labeling of Vertices of the Complete Bipartite Graphs

Gholam Hassan Shirdel[1]✉, **Zahra Sadat Emamy**[2]

1. Corresponding Author, Department of Mathematics and Computer Sciences, Faculty of Science, University of Qom, Qom, Iran. Email: g.h.shirdel@qom.ac.ir
2. Master of Science from Department of Mathematics, Sharif University, Tehran, Iran. Email: Zahra_emamy@alum.sharif.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 17 March 2024
Received in revised form:
17 May 2024
Accepted: 17 June 2024
Published Online:
20 August 2024

Keywords:
Magic Graph,
Complete Magic Labeling of Vertices,
Complete Graph,
Complete Bipartite Graph

2020 Mathematics Subject Classification: 20F05, 05C05

ABSTRACT

In this paper, first, we explain the concept of magic graphs, and then we describe the complete magic labeling of the vertices of a graph. Also, some conditions that must be met so that this labeling can be done in complete bipartite graphs are stated.

Cite this article: Shirdel, G.H., & Emamy, Z.S. (2024). Complete Magic Labeling of Vertices of the Complete Bipartite Graphs. *Measure Algebras and Applications*, 1(2), 14–29. http://doi.org/10.22091/MAA.2024.10537.1017

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10537.1017

Extended Abstract

One of the useful operators in graphs is labeling. A labeling for a graph is a mapping in which elements of the graph are mapped to numbers. These numbers are usually positive or non-negative integers. If the domain of the map is the set of vertices, edges, or both, then the labeling is called vertices labeling, edge labeling, or complete labeling, respectively. In 1963, the concept of a magic graph was defined by Sedlacek. A graph is called magic if there exists a mapping from the graph to the set of positive integer numbers, so that firstly, for each different two edges, the values of the mapping are also different, and secondly for any arbitrary vertex of the graph, the sum of the mapping values of the edges that coincide with vertex should be equal to a specific number. Magic labelings are one-to-one mappings and cover with a constant sum property. A labeling is called edge-magic if the sum of the labels of the elements connected to an edge is a fixed number. This constant value is independent of edge selection. If the same property holds for an arbitrary vertex in the graph, then the labeling is called vertex-magic. In this paper, first, we defined the concept of complete magic labeling of vertices and unbalanced complete bipartite graphs. Then, we showed that complete graphs can have complete magic labeling of vertices. For those complete graphs that did not have the necessary conditions, we described how to construct the complete magic labeling of the vertices using the magic square. Also, we have described and explained the complete magic labeling techniques of vertices in the case of complete bipartite graphs. Now, we state the purpose of this paper with more details.

Consider the graph G = (V, E) a simple, finite and undirected graph. A labeling or valuation for a graph is a mapping in which elements (nodes and or edges) are mapped to numbers. These numbers are usually positive or non-negative integers. If the mapping domain is the set of vertices, the set of edges, or the set of their union, then labeling is called vertex labeling, edge labeling, or complete labeling, respectively. The concept of magic graph was first introduced in 1963 by Sedlacek. A graph G is called magic if there exists a mapping f from E(G) to the set of positive integers such that:

1. For both arbitrary edges $\mathbf{e_i}$ and $\mathbf{e_j}$ if $\mathbf{e_i} \neq \mathbf{e_j}$, then $\neq \mathbf{f}(\mathbf{e_i}) \neq \mathbf{f}(\mathbf{e_j})$.
2. For a predetermined fixed number λ and for any arbitrary vertex $\mathbf{v} \in \mathbf{V(G)}$, we have:

$$\sum_{\mathbf{e} \in \mathbf{E(G)}} \rho(\mathbf{v}, \mathbf{e}) f(e) = \lambda.$$

So that

$$\rho(\mathbf{v}, \mathbf{e}) = \begin{cases} \mathbf{1} & , \quad \textbf{If e is adjacent to node v} \\ \mathbf{0} & , \quad \textbf{otherwise} \end{cases}$$

Magic labels are one-to-one mappings and overlay with a constant sum property. A labeling is called edge-magic if the sum of the labels of the elements connected to an edge is a fixed number. This constant value is independent of edge selection. If the same property is true for an arbitrary vertex, then such a labeling is called a magic-vertex.

Vertices complete magic labeling of a complete bipartite graph

We show the set of vertices and edges of the graph $\mathbf{K_{m,n}}$ as follows:

V=$\{\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_m}, \mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_n}\}$, E=$\{\mathbf{x_i}\, \mathbf{y_j} : \mathbf{1} \leq \mathbf{i} \leq \mathbf{m}, \mathbf{1} \leq \mathbf{j} \leq \mathbf{n}\}$. There-

fore, we can show the complete vertices labeling of the graph $\mathbf{K_{m,n}}$ with a matrix as follows:

$$\begin{bmatrix} \mathbf{a_{00}} & \cdots & \mathbf{a_{0n}} \\ \vdots & \ddots & \vdots \\ \mathbf{a_{m0}} & \cdots & \mathbf{a_{mn}} \end{bmatrix}$$

$$\mathbf{a_{i,j}} = \begin{cases} \mathbf{f}(\mathbf{x_i}) & \mathbf{j = 0} \\ \mathbf{f}(\mathbf{y_j}) & \mathbf{i = 0} \\ \mathbf{f}(\mathbf{x_i y_j}) & \text{otherwise} \end{cases}$$

***Definition* 0.1.** *Graph $K_{m,n}$ is said to be unbalanced if $|m - n| > 1$.*

In the following theorem, we show that a complete bipartite unbalanced graph cannot have complete magic labeling of vertices.

***Theorem* 0.2.** *If $K_{m,n}$ is unbalanced, then it cannot have complete magic labeling of vertices.*

Constructing complete magic vertex labeling for graph $\mathbf{K_{m,n}}$

In this section, we want to present how to make a complete vertices magic labeling of graph $K_{m,n}$. Since this magic labeling is done by using the magic square, we first define the magic square.

***Definition* 0.3.** *A magic square with order n is a table $n \times n$ whose houses are filled with positive numbers $1, 2, \ldots, n^2$, so that the sum of the numbers of each row, each column or its diagonal is a fixed number.*

***Theorem* 0.4.** *For every $m > 1$, $K_{m,n}$ has complete vertices magic labeling with magic constant*

$$\frac{1}{2}\left[(m+1)^3 - (m+1)\right].$$

According to what was stated, it is possible to create a complete magic vertex labeling for complete bipartite graphs. This is an important achievement in the field of graph labeling.

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۲۹-۱۴

برچسب‌گذاری جادویی کامل رأسی گراف کامل دوبخشی

غلام حسن شیردل [۱]✉ ، **زهرا سادات امامی** [۲]

۱. نویسندهٔ مسئول، عضو هیئت‌علمی دانشگاه قم. رایانامه: g. h. shirdel@qom. ac. ir
۲. فارغ‌التحصیل کارشناسی ارشد دانشگاه صنعتی شریف. رایانامه: zahra_emamy@alum. sharif. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۲/۲۷
تاریخ بازنگری: ۱۴۰۳/۲/۲۸
تاریخ پذیرش: ۱۴۰۳/۳/۲۸
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
گراف جادویی،
برچسب‌گذاری جادویی کامل رأسی،
گراف کامل،
گراف دوبخشی کامل

رده‌بندی ریاضی:
20F05, 05C05

چکیده

در این مقاله، ابتدا مفهوم گراف‌های جادویی را بیان کرده و سپس برچسب‌گذاری جادویی کامل رأسی یک گراف را توصیف می‌کنیم و شرایطی که باید برقرار باشند تا این برچسب‌گذاری را بتوان در گراف‌های کامل دوبخشی انجام داد مطرح کرده و اثبات آن‌ها را ذکر می‌کنیم.

استناد: شیردل، غلام حسن.، امامی، زهرا سادات. (۱۴۰۳). برچسب‌گذاری جادویی کامل رأسی گراف کامل دوبخشی. جبرهای اندازه و کاربردها، ۱(۲)، ۲۹-۱۴.

http://doi.org/10.22091/MAA.2024.10537.1017

ناشر: دانشگاه قم.

۱ معرفی

گراف G را یک گراف ساده، متناهی و بدون جهت در نظر بگیرید [۱۱]. فرض کنید $V(G)$ مجموعهٔ رأس‌ها و $E(G)$ مجموعهٔ یال‌ها باشند به‌طوری‌که $|V(G)| = n$ و $|E(G)| = m$. یک برچسب‌گذاری [۱] یا ارزش‌گذاری [۲] برای یک گراف، نگاشتی است که در آن عناصری (رأس‌ها، یال‌ها و یا اجتماع آن‌ها) به اعدادی نگاشته می‌شوند. این اعداد معمولاً اعداد صحیح مثبت یا نامنفی هستند. اگر دامنهٔیک نگاشت به ترتیب مجموعهٔ رئوس، مجموعهٔ یال‌ها و یا مجموعهٔ $V(G) \cup E(G)$ گراف باشد، آنگاه برچسب‌گذاری را به ترتیب برچسب‌گذاری رأسی [۳]، برچسب‌گذاری یالی [۴] و یا برچسب‌گذاری کامل [۵] گویند. مفهوم گراف جادویی برای اولین بار در سال ۱۹۶۳ توسط سِدلِیسِک [۶] معرفی شد. گراف G را جادویی می‌نامند اگر نگاشت f از $E(G)$ به مجموعهٔ اعداد صحیح مثبت وجود داشته باشد به‌طوری‌که [۹]

۱. برای هر دو یال دلخواه e_i, e_j که $e_i \neq e_j$ داشته باشیم $f(e_i) \neq f(e_j)$.

۲. برای هر رأس دلخواه $v \in V(G)$ داشته باشیم $\sum_{e \in E(G)} \rho(v,e) f(e) = \lambda$.

اگر یال e مجاور با رأس v باشد، آنگاه $\rho(v,e) = ۱$ و در غیر این صورت برابر صفر است. برچسب‌گذاری‌های جادویی، نگاشت‌های یک‌به‌یک و پوشایی [۷] با ویژگی مجموع ثابت [۸] هستند. یک برچسب‌گذاری را یال-جادویی [۹] می‌نامند اگر مجموع برچسب‌های عناصر متصل به یک یال عدد ثابتی باشد، این مقدار ثابت مستقل از انتخاب یال است. اگر همین ویژگی برای یک رأس دلخواه در گراف برقرار باشد چنین برچسب‌گذاری را رأس-جادویی [۱۰] می‌نامند. گراف‌های جادویی که در آن برای هر یال $e \in E(G)$، $f(e)$ یک عدد اول منحصربه‌فرد باشد گراف‌های جادویی-اول [۱۱] نامیده می‌شوند، در واقع دامنه و برد تابع f برای چنین گراف‌هایی به‌صورت $f : E(G) \to \text{Prime positive integers}$ تعریف می‌شود. اِستِوارت [۱۲] در [۱۰] ثابت کرد، گراف دوبخشی $k_{۳,۳}$ یک گراف جادویی- اول با ثابت جادویی $k = ۱۳۹$ است. گراف جادویی G را فوق جادویی [۱۳] گویند اگر برچسب‌گذاری جادویی f وجود داشته باشد به‌طوری‌که مجموعهٔ $\{f(e) : e\}$ شامل اعداد صحیح متوالی باشد به‌عبارت‌دیگر تابع f به‌صورت $f : E(G) \to \text{Consecutive integers}$ تعریف می‌شود. در [۱۰] نشان داده شده است که گراف k_n زمانی که $n > ۵$ و $n \not\equiv ۰ \pmod 4$، یک گراف فوق جادویی است همچنین در مرجع [۱۰] اثبات شده است که گراف $k_{n,n}$ برای $n \geq ۳$ فوق جادویی است. نگاشت یک‌به‌یک و پوشای $f : V \cup E \to \{۱, ۲, \cdots, m+n\}$ را برچسب‌گذاری جادویی کامل رأسی [۱۴] برای گراف G گوییم اگر عدد ثابت k وجود داشته باشد به‌طوری‌که برای هر رأس دلخواه $u \in V(G)$ رابطه (۱.۱) برقرار باشد

$$f(u) + \sum_{v \in N(u)} f(uv) = k. \qquad (۱.۱)$$

در رابطه (۱.۱) مجموعهٔ $N(u)$ شامل همهٔ رئوسی است که بین آن‌ها و رأس u یالی در گراف G وجود داشته باشد. این نوع برچسب‌گذاری جادویی در سال ۲۰۰۲ توسط مَک دوگل [۱۵] و همکاران معرفی شد [۴]. در رابطه (۱.۱) اگر تابع f که برچسب یال‌ها را تعیین می‌کند به‌صورت $f : E(G) \to \{۱, ۲, \cdots, q\}$ تعریف شود چنین برچسب‌گذاری را کیو-یالی می‌نامند. برچسب‌گذاری کیو-یالی در سال ۲۰۱۲ برای اولین بار توسط ماریموثو [۱۶] معرفی شد[۵].

---

[1] Labeling
[2] Valuation
[3] Vertex-labeling
[4] Edge-labeling
[5] Total-labeling
[6] J.Sedlacek
[7] Bijection mapping
[8] Constant sum
[9] Edge magic
[10] Vertex magic
[11] Prime-magic
[12] B. M. Stewart
[13] Super magic
[14] Vertex magic total labeling
[15] J. A. MacDougall
[16] G. Marimuthu

۲ برچسب‌گذاری جادویی کامل رأسی گراف کامل دوبخشی

مجموعهٔ رئوس و یال‌های گراف دوبخشی $k_{m,n}$ را به‌صورت رابطه (۱.۲) نشان می‌دهیم:

$$\begin{aligned} V &= \{x_۱, x_۲, \cdots, x_m, y_۱, y_۲, \cdots, y_n\}, \\ E &= \{x_i y_j : ۱ \le i \le m, ۱ \le j \le n\} \end{aligned} \tag{۱.۲}$$

بنابراین برچسب‌گذاری کامل رأسی گراف $k_{m,n}$ را می‌توانیم با یک آرایهٔ $(m+۱) \times (n+۱)$ نشان دهیم:

$$\left[\begin{array}{c|cccc} a_{۰۰} & a_{۰۱} & a_{۰۲} & \cdots & a_{۰n} \\ \hline a_{۱۰} & a_{۱۱} & a_{۱۲} & \cdots & a_{۱n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m۰} & a_{m۱} & am۲ & \cdots & a_{mn} \end{array}\right]$$

که $a_{۰۰} = ۰$، $a_{i۰} = f(x_i)$، $a_{۰j} = f(y_j)$ و $a_{ij} = f(x_i y_j)$. آرایهٔ A را نمایش ماتریسی f گوییم. ویژگی جادویی بودن ایجاب می‌کند که مجموع هر سطر و هر ستون دلخواه به‌جز سطر و ستون صفرم باید برابر با مقدار جادویی k باشد و مقادیر موجود در عناصر ماتریس A جایگشت‌های متفاوت $\{۰, ۱, \cdots, mn+m+n\}$ هستند.

تعریف ۱.۲. گراف $k_{m,n}$ را نامتعادل [۱] گوییم اگر $| m-n | > ۱$ باشد.

در قضیه ۲.۲ نشان می‌دهیم که یک گراف نامتعادل دوبخشی کامل $k_{m,n}$ نمی‌تواند دارای برچسب‌گذاری جادویی کامل رأسی باشد.

قضیه ۲.۲ ([۴]). اگر $k_{m,n}$ نامتعادل باشد، نمی‌تواند دارای برچسب‌گذاری جادویی کامل رأسی باشد.

اثبات. بدون از دست دادن کلیت فرض می‌کنیم $m \le n$. فرض کنید $k_{m,n}$ دارای برچسب‌گذاری جادویی کامل با ثابت جادویی k باشد. برای این گراف $V = m+n$ و $E = mn$. بنابراین مجموعهٔ برچسب‌های $k_{m,n}$، $\{۱, ۲, \cdots, mn+m+n\}$ است. مجموع وزن‌های رئوس $\{x_۱, x_۲, \cdots, x_m\}$ حداقل به‌صورت زیر است:

$$mk \ge ۱ + ۲ + \cdots + (mn+m) = \frac{(mn+m)(mn+m+۱)}{۲} k \ge \frac{(n+۱)}{(mn+m+۱)} \tag{۲.۲}$$

به بیان دیگر، مجموع وزن‌های $\{y_۱, \cdots, y_n\}$ حداکثر به‌صورت زیر است:

$$\begin{aligned} nk &\le (m+۱) + (m+۲) + \cdots + (mn+m+n) \\ &= \frac{(mn+m+n)(mn+m+n+۱) - m(m+۱)}{۲} \\ &= \frac{(mn^۲ + ۲mn + n^۲ + n)}{۲} \\ k &\le \frac{(m+۱)}{(mn+۲m+n+۱)} \end{aligned} \tag{۳.۲}$$

با در نظر گرفتن (۲.۲) و (۳.۲) خواهیم داشت:

$$\begin{aligned} (n+۱)(mn+m+۱) &\le (mn+۲m+n+۱)(m+۱) \\ m &\ge n - ۲ + \frac{۲}{n+۲} \to m \ge n - ۱ \end{aligned}$$

ازآنجاکه فرض مسئله $m \le n$ بود پس یا $m = n$ و یا $m = n-۱$. روند اثبات برای حالت $n \le m$ کاملاً مشابه است. □

[1] Unbalanced

۱.۲ ساخت برچسب‌گذاری جادویی کامل رأسی برای گراف $k_{m,n}$

در این قسمت می‌خواهیم نحوهٔ ساخت برچسب‌گذاری جادویی کامل رأسی گراف $k_{m,n}$ را برای حالاتی که وجود آن توسط قضیه ۲.۲ رد نشده است؛ ارائه دهیم. ازآنجاکه با استفاده از مربع جادویی [1] این برچسب‌گذاری جادویی انجام می‌شود؛ در تعریف (۳.۲)، مفهوم مربع جادویی را توضیح داده‌ایم.

تعریف ۳.۲. مربع جادویی یا وفقی از مرتبهٔ n، جدولی $n \times n$ است که خانه‌های آن با اعداد مثبت $1, 2, \cdots, n^2$ به ترتیبی پر شده‌اند، که مجموع اعداد هر ردیف افقی، هر ستون عمودی و یا هر قطر آن عددی ثابت است

قضیه ۴.۲ (گراف $k_{m,m}$). برای هر $m > 1$، $k_{m,m}$ دارای برچسب‌گذاری جادویی کامل رأسی با ثابت جادویی $\frac{1}{2}[(m+1)^3-(m+1)]$ است.

اثبات. $S = (s_{ij})$ را یک مربع جادویی از مرتبهٔ $m+1$ روی مجموعهٔ اعداد $1, \cdots, (m+1)^2$ در نظر بگیرید. فرض کنید سطرها و ستون‌های S با اعداد $0, 1, \cdots, m$ شماره‌گذاری شده‌اند. هر سطر و ستون S با اعداد $0, 1, \cdots, m$ شماره‌گذاری شده است. جمع عناصر هر سطر یا ستون این مربع جادویی برابر $\frac{1}{2}(m+1)(m^2+2m+2)$ است. ماتریس $A = (a_{ij})$ را با درایه‌های $a_{ij} = s_{ij} - 1$ تشکیل می‌دهیم ازآنجاکه مربع S جادویی است مجموع عناصر سطرها یا ستون‌های A برابر مقدار

$$k = \frac{1}{2}(m+1)(m^2+2m+2) - (m+1) \qquad (۴.۲)$$

است و درایه‌های ماتریس A از مجموعهٔ $\{0, \cdots, (m+1)^2 - 1\}$ انتخاب می‌شوند (برای مطالعهٔ نحوهٔ ساخت استاندارد مربع‌های جادویی از یک مرتبهٔ دلخواه به پیوست مراجعه کنید). بدون از دست دادن کلیت می‌توانیم سطرها و ستون‌های A را جایگشت دهیم تا درایهٔ $a_{00} = 0$ شود (این کار ممکن است باعث شود مجموع عناصر قطرها برابر با ثابت جادویی نباشد اما به این ویژگی در ساخت نیاز نداریم). با انجام این کار ماتریس A تبدیل به نمایش ماتریسی برچسب‌گذاری جادویی کامل رأسی f با ثابت k که در معادله (۴.۲) نشان داده شده است، می‌شود. □

در ادامه برچسب‌گذاری جادویی کامل رأسی را برای گراف $k_{m,m+1}$ (m فرد) می‌سازیم. این برچسب‌گذاری برای گراف $k_{1,2}$ به‌سادگی ساخته می‌شود. حالا فرض می‌کنیم $m = 2n - 1$ که $n > 1$. ساخت برچسب‌گذاری برای n داده‌شده با تعریف دو ماتریس $(2n-1 \times 2n)$ به نام‌های $A = (a_{ij})$ و $B = (b_{ij})$ انجام می‌شود. در ادامه با استفاده از ماتریس‌های A و B ماتریس $(2n \times 2n+1)$ به نام C را می‌سازیم و نشان می‌دهیم C نمایش ماتریسی برچسب‌گذاری جادویی کامل رأسی گراف است. برای سازگاری با تعریف نمایش ماتریسی برچسب‌گذاری جادویی کامل رأسی فرض می‌کنیم سطر اول و ستون اول ماتریس C با عدد صفر پر شده‌اند. درایه‌های ماتریس $A = (a_{ij})$ به‌صورت زیر تعریف می‌شوند:

$$a_{ij} = \begin{cases} m+1-j, & \text{if } \ i+j \ \text{ is odd}, \ \ j+i \le m+1 \\ & \text{or } \ i+j \text{ is even}, \quad j+i > m+1 \\ j-1, & \text{otherwise} \end{cases}$$

مجموع سطری و ستونی ماتریس A را می‌خواهیم محاسبه کنیم. اگر i زوج باشد قرار می‌دهیم $i = 2t$ و مجموع درایه‌های سطر i به‌صورت زیر است:

$$\begin{aligned} \sum_{j=1}^{2n} a_{ij} &= \sum_{k=1}^{n} a_{i,2k-1} + a_{i,2k} \\ &= \sum_{k=1}^{n-t} (a_{i,2k-1} + a_{i,2k}) + \sum_{k=n-t+1}^{n} (a_{i,2k-1} + a_{i,2k}) \\ &= \sum_{k=1}^{n-t} ((2n-2k+1) + (2k-1)) + \sum_{k=n-t+1}^{n} ((2k-2) + (2n-2k)) \end{aligned}$$

[1] Magic square

$$= \sum_{k=۱}^{n-t}(۲n) + \sum_{k=n-t+۱}^{n}(۲n-۲)$$
$$= ۲n^۲ - i$$

اگر i فرد باشد قرار می‌دهیم $i = ۲t+۱$:

$$\sum_{j=۱}^{۲n} a_{ij} = \sum_{k=۱}^{n} a_{i,۲k-۱} + a_{i,۲k}$$
$$= \sum_{k=۱}^{n-t} a_{i,۲k-۱} + \sum_{k=۱}^{n-t-۱} a_{i,۲k} + \sum_{k=n-t+۱}^{n} a_{i,۲k-۱} + \sum_{k=n-t}^{n} a_{i,۲k}$$
$$= \sum_{k=۱}^{n-t}(۲k-۲) + \sum_{k=۱}^{n-t-۱}(۲n-۲k) + \sum_{k=n-t+۱}^{n}(۲n-۲k+۱) + \sum_{k=n-t}^{n}(۲k-۱)$$
$$= ۲n^۲ - i.$$

در هر حالت، سطر i ام دارای مجموع $۲n^۲ - i$ است. مجموع ستونی ساده‌تر محاسبه می‌شود:
ستون j ام شامل n درایه برابر با $j-۱$ و $n-۱$ درایه برابر $۲n-j$ است. بنابراین برای هر j،

$$\sum_{i=۱}^{۲n-۱} a_{ij} = n(j-۱) + (n-۱)(۲n-j)$$
$$= ۲n^۲ - ۳n + j.$$

ستون‌های اول و آخر ماتریس B دارای مقادیر $۰, ۱, \ldots, ۲n-۳, ۲n-۲$ هستند پس

$$b_{۱j} = b_{mj} = m - i - ۱.$$

ستون دوم با مقادیر فرد $۱, ۲n-۷, \ldots, ۲n-۵$ شروع می‌شود و با مقادیر زوج $۰, ۲n-۴, \ldots, ۲n-۲$ ادامه می‌یابد و به $۲n-۳$ ختم می‌شود. ستون‌های دیگر همین ترکیب از اعداد را به‌صورت معکوس دارند بنابراین

$$b_{i,j} = b_{i+۱,j-۱}$$

(ذکر این نکته الزامی است که اندیس‌ها در mod (2n,2+1) محاسبه می‌شوند). در هر سطر B، در هر یک از ستون‌های ۲ تا $۲n-۱$ همهٔ اعداد مجموعهٔ $۰, ۱, \ldots, m-۲$ حضور دارند به‌جز

$$x_i = ۲n-۱-۲i \text{ is missing from row i, } i = ۱, ۲, \ldots, n-۱,$$

$$x_i = ۴n-۲-۲i \text{ is missing from row i, } i = n, n+۱, \ldots, ۲n-۱.$$

بنابراین مجموع سطری به‌صورت زیر است:

$$\sum_{j=۱}^{m} b_{ij} = ۲(۲n-i-۱) + \sum_{k=۰}^{۲n-۲} k - x_i$$
$$= ۲n^۲ + n - ۱ - ۲i - x_i$$

بنابراین

$$\sum_{j=۱}^{m} b_{ij} = ۲n^۲ - n$$

زمانی که

$$i \leq n-۱,$$

و

$$\sum_{j=۱}^{m} b_{ij} = ۲n^۲ - ۳n + ۱$$

زمانی که

$$i \geq n.$$

بنابراین هر ستون جایگشتی از اعداد $۲n-۲$, $\ldots$, ۱, ۰ است. جمع هر ستون به‌صورت زیر است:

$$\sum_{i=۱}^{۲n-۱} b_{ij} = ۲n^۲ - ۳n + ۱.$$

حال ماتریس $C_{۲n\times(۲n-۱)}$ را به‌صورت زیر می‌سازیم:

$$c_{۰۰} = ۰$$

$$c_{۰j} = ۴n^۲ + ۲n - j,$$

$$۱ \leq j \leq ۲n,$$

$$c_{i۰} = \begin{cases} i, & ۱ \leq i \leq n-۱ \\ ۴n^۲ - ۲n + i, & n \leq i \leq ۲n-۱, \\ a_{ij} + ۲nb_{ij} + n, & \text{otherwise.} \end{cases}$$

قضیه ۵.۲. ماتریس C نمایش ماتریسی برچسب‌گذاری جادویی کامل رأسی گراف $k_{۲n-۱,۲n}$ با ثابت جادویی $۴n^۳ + ۲n^۲$ است.

اثبات. لازم است نشان دهیم مجموع درایه‌های هر سطر و ستون ماتریس C (به‌جز احتمالاً سطر و ستون صفر) برابر $۴n^۳ + ۲n^۲$ است و هر عدد صحیح در بازهٔ صفر تا $v + e = ۴n^۲ + ۲n - ۱$ دقیقاً یک بار در C تکرار می‌شود (می‌دانیم عدد صفر در درایهٔ $(۰, ۰)$ ظاهر خواهد شد). مجموع سطری ماتریس C به‌صورت زیر است:

$$\sum_{j=۰}^{۲n} c_{ij} = c_{i۰} + \sum_{j=۱}^{۲n} a_{ij} + ۲n \sum_{j=۱}^{۲n} b_{ij} + ۲n^۲$$

$$= c_{i۰} + ۲n^۲ - i + ۲n \sum_{j=۱}^{۲n} b_{ij} + ۲n^۲$$

$$= ۴n^۳ + ۲n^۲$$

و مجموع ستونی ماتریس C به‌صورت زیر است:

$$\sum_{i=۰}^{۲n-۱} c_{ij} = c_{۰j} + \sum_{i=۱}^{۲n-۱} a_{ij} + ۲n \sum_{i=۱}^{۲n-۱} b_{ij} + n(۲n-۱)$$

$$= ۴n^۲ + ۲n - j + ۲n^۲ - ۳n + j + ۲n \left(\sum_{i=۱}^{۲n-۱} b_{ij} \right) + n(۲n-۱)$$

$$= ۴n^۲ + ۲n - j + ۲n^۲ - ۳n + j + ۲n(۲n^۲ - ۳n + ۱) + n(۲n-۱)$$

$$= ۴n^۳ + ۲n^۲$$

بنابراین مجموع همهٔ سطرها و ستون‌ها (به‌جز اولی) برابر $۴n^۳ + ۲n^۲$ است.
در نهایت، نشان می‌دهیم درایه‌های ماتریس C اعضای مجموعهٔ $۰, ۱, ۲, \ldots, ۴n^۲ - ۲n - ۱$ هستند که هر عضو دقیقاً یک بار در C ظاهر می‌شود. مجموعه‌های $۰, ۱, ۲, \ldots, n-۱$ و $۴n^۲ - n, ۴n^۲ - n + ۱, \ldots, ۴n^۲ + ۲n - ۱$ به ترتیب در اولین سطر و ستون C ظاهر می‌شوند. درایه‌های ماتریس A در بازهٔ بستهٔ $[۰, ۲n - ۱]$ و درایه‌های ماتریس B در بازهٔ $[۰, ۲n - ۲]$ قرار دارند. بنابراین درایه‌های ماتریس C (به‌جز سطر و ستون اول) در بازهٔ $[۱, ۴n^۲ - n - ۱] = [n, ۳n - ۱ + ۲n(۲n - ۲)]$ قرار دارند. در این بازه $۴n^۲ - ۲n$ عدد وجود دارد و فقط کافی است نشان دهیم درایه‌ها منحصربه‌فرد هستند. برای اثبات این موضوع باید نشان دهیم زوج‌های (a_{ij}, b_{ij}) یکتا هستند. اولین و آخرین ستون ماتریس A فقط شامل اعداد ۰ و $۲n - ۱$ هستند و اولین و آخرین ستون ماتریس B شامل اعداد $۰, ۱, \ldots, ۲n - ۲$ هستند و اثبات اینکه در این قسمت هیچ زوج تکراری وجود ندارد، ساده است. برای قسمت باقی‌ماندهٔ ماتریس A و ماتریس B توجه کنید که مقدار b_{ij} ها مستقل از انتخاب i و j مقدار ثابت است و درایه‌های ماتریس A همهٔ مقادیر $\{۱, ۲, \ldots, ۲n - ۲\}$ را اتخاذ می‌کنند. بنابراین همهٔ زوج‌ها متمایز هستند. درنتیجه هر عدد صحیح در بازهٔ $[۱, ۴n^۲ - ۲n - ۱]$ در ماتریس C دقیقاً یک بار ظاهر می‌شود. □

حال می‌خواهیم برچسب‌گذاری جادویی کامل رأسی را برای گراف $k_{m,m+۱}$ به ازای m زوج بررسی کنیم. در این حالت فرض می‌کنیم $m = ۲n$. بنابراین $V = ۴n + ۱$ و $E = ۴n^۲ + ۲n$ و یک برچسب‌گذاری کامل به $۴n^۲ + ۶n + ۱$ برچسب نیاز دارد.

قضیه ۶.۲. یک برچسب‌گذاری جادویی کامل رأسی برای گراف $k_{۲n,۲n+۱}$ با ثابت جادویی $(n + ۱)(۲n + ۱)^۲$ وجود دارد.

اثبات. ماتریس $C = (c_{ij})$ را که نمایش ماتریسی برچسب‌گذاری جادویی کامل رأسی گراف $k_{۲n,۲n+۱}$ است به‌صورت زیر می‌سازیم:

۱. سطر صفرم ماتریس C به‌صورت $\{۰, (۲n+۱)^۲, (۲n+۱)^۲ + ۱, \ldots, (۲n+۱)^۲ + ۲n\}$ است به‌عبارت‌دیگر $C_{۰۰} = ۰$ و $C_{۰j} = (۲n + ۱)^۲ + j - ۱$.

۲. به‌ازای $۱ \le i \le ۲n$، داریم $c_{i۰} = (۲n + ۲)i$.

۳. اگر $۱ \le i < n$ و $۱ \le j \le n + ۱$ یا $n + ۲ \le i \le ۲n$ و $n + ۲ \le j \le ۲n + ۱$، آنگاه:

$$c_{ij} = ۲n(۲n + ۲) - [j + (i - ۱)(۲n + ۲)].$$

۴. اگر $۱ \le i < n$ و $n + ۲ \le j \le ۲n + ۱$ یا اگر $n + ۱ < i \le ۲n$ و $۱ \le j \le n + ۱$، آنگاه:

$$c_{ij} = j + (i - ۱)(۲n + ۲).$$

۵. اگر $۱ \le j \le n + ۱$، آنگاه:

$$c_n, j = n(۲n + ۲) + ۲n - ۲j + ۳,$$
$$c_{n+۱,j} = (n - ۱)(۲n - ۲) + n + j$$

و اگر $n + ۲ \le j \le ۲n + ۱$، آنگاه:

$$c_{n,j} = (n - ۱)(۲n + ۲) + ۴n - ۲j + ۴,$$
$$c_{n+۱,j} = n(۲n + ۲) + j - n - ۱.$$

در واقع قسمت پنجم می‌تواند به‌صورت زیر بیان شود:
به‌جز درایهٔ $(۰, ۰)$ باقی درایه‌های سطرهای n، ۰ و $n + ۱$ ماتریس C از روی سطرهای ماتریس X که به شکل زیر است

$$\left[\begin{array}{ccccc|cccc} ۱ & ۲ & ۳ & \cdots & n+۱ & n+۲ & n+۳ & \cdots & ۲n+۱ \\ ۲n+۱ & ۲n-۱ & ۲n-۳ & \cdots & ۱ & ۲n & ۲n-۲ & \cdots & ۲ \\ n+۱ & n+۲ & n+۳ & \cdots & ۲n+۱ & ۱ & ۲ & \cdots & n \end{array}\right]$$

با اضافه کردن

$$\begin{bmatrix} (۲n+۱)^۲-۱ \\ n(۲n+۲) \\ (n-۱)(۲n+۲) \end{bmatrix}$$

به هرکدام از $n+۱$ ستون اول ماتریس X و اضافه کردن

$$\begin{bmatrix} (۲n+۱)^۲-۱ \\ (n-۱)(۲n+۲) \\ n(۲n+۲) \end{bmatrix}$$

به بقیهٔ ستون‌ها به دست می‌آید. □

به‌وضوح مشخص است که هر سطر X جایگشتی از $۱, ۲, \ldots, ۲n+۱$ است. بنابراین سطرهای n و $n+۱$ دقیقاً یک بار شامل عناصر مجموعهٔ $(n-۱)(۲n+۲)+۱, (n-۱)(۲n+۲)+۲, \ldots, (n+۱)(۲n+۲)$ است. زمانی که $۱ \le i < n$، سطرهای i و $۲n+۱-i$ شامل همهٔ اعداد زیر هستند:

$$t+(i-۱)(۲n+۲): \qquad ۱ \le t \le ۲n+۲$$
$$t+(۲n-i)(۲n+۲): \qquad ۱ \le t \le ۲n+۲$$

در این راستا خواهیم داشت:

$$c_{i۰} = ۲n+۲+(i-۱)(۲n+۲) = i(۲n+۲) \tag{۵.۲}$$

$$c_{۲n+۱-i,۰} = ۲n+۲+(۲n-i)(۲n+۲) \tag{۶.۲}$$

و بقیهٔ درایه‌ها از قسمت‌های (۳) و (۴) به دست می‌آیند. سطر صفرم ماتریس C طبق تعریف بالا به‌صورت
$[۰ \quad (۲n+۱)^۲ \quad (۲n+۱)^۲+۱ \quad \ldots \quad (۲n+۱)^۲+۲n]$ است. بنابراین دقیقاً شامل هر یک از اعضای مجموعهٔ $\{۰, ۱, \ldots, ۴n^۲+۶n+۱\}$ است.
از (۳) و (۴) داریم:

$$\begin{aligned} c_{ij}+c_{۲n+۱-i,j} &= j+(i-۱)(۲n+۲)+۲n(۲n+۲)-(j+(i-۱)(۲n+۲)) \\ &= ۲n(۲n+۲) \qquad ۱ \le i < n. \end{aligned}$$

جمع هر ستون ماتریس X برابر $۳n+۳$ است، پس

$$c_{n,j}+c_{n+۱,j}+c_{۰j} = (n+۱)(۸n+۱), \quad ۱ \le j \le ۲n+۱.$$

بنابراین مجموع ستون j ام ماتریس C به‌صورت زیر است:

$$\begin{aligned} \sum c_{ij}{}_{i=۰}^{۲n} &= (n-۱)۲n(۲n+۲)+c_{nj}+c_{n+۱,j}+c_{۰,j} \\ &= (n-۱)۲n(۲n+۲)+(n+۱)(۸n+۱) \\ &= (n+۱)(۲n+۱)^۲. \end{aligned}$$

مجموع سطر i ام ماتریس C، اگر $i \le n$، به‌صورت زیر محاسبه می‌شود

$$\begin{aligned} \textstyle\sum_{j=۰}^{۲n+۱} c_{ij} &= \textstyle\sum_{j=۱}^{۲n+۱} j + c_{i۰} + n(i-۱)(۲n+۲)+(n+۱)(۲n-i)(۲n+۲) \\ &= \binom{۲n+۲}{۲} + (۲n+۲)i + (۲n+۲) + n(i-۱) + (n+۱)(۲n-i) \\ &\qquad (n+۱)(۲n+۱)+۲(n+۱)n(۲n+۱) \\ &= (n+۱)(۲n+۱)^۲. \end{aligned}$$

حکم به طریق مشابه برای $i \ge n+۱$ به دست می‌آید.

۲.۲ طیف برچسب‌گذاری جادویی کامل رأسی گراف $k_{m,n}$

در این قسمت می‌خواهیم برای گراف‌های $k_{m,n}$ ای که طبق قضیه ۲.۲ می‌دانیم برای آن‌ها برچسب‌گذاری جادویی کامل رأسی وجود دارد مجموعهٔ مقادیر k را حساب کنیم[۵]. این مجموعه را طیف [۱] مسئلهٔ برچسب‌گذاری می‌گویند. فرض کنید گراف G دارای یک نگاشت برچسب‌گذاری جادویی کامل رأسی f است. مجموع برچسب‌های یال‌ها را با S_E نشان می‌دهیم و طبق تعریف داریم:

$$S_E = \sum_{x \in E(G)} f(x)$$

با شمارش مجموع برچسب‌ها در همهٔ رئوس خواهیم داشت:

$$S_E + \binom{v+e+۱}{۲} = vk \tag{۷.۲}$$

به‌وضوح

$$\sum_{i=۱}^{e} i \leq S_E \leq \sum_{i=v+۱}^{v+e} i \tag{۸.۲}$$

یا

$$\binom{e+۱}{۲} \leq S_E \leq \binom{e+۱}{۲} + ve. \tag{۹.۲}$$

فرمول‌های (۸.۲) و (۹.۲) می‌تواند کران‌هایی روی طیف برچسب‌گذاری کامل رأسی ایجاد کند. برای گراف $k_{m,m}$ با استفاده از فرمول‌های (۸.۲) و (۹.۲) خواهیم داشت:

$$\frac{۱}{۲}[(m+۱)^۳ - m^۲] \leq k \leq \frac{۱}{۲}[(m+۱)^۳ + m^۲] \tag{۱۰.۲}$$

ازآنجاکه $k_{m,m}$ یک گراف منظم است قضیهٔ دوگان ([۴]) را می‌توان به کار برد. بنابراین می‌توانیم نتیجه بگیریم یک برچسب‌گذاری جادویی کامل رأسی با ثابت جادویی $\frac{۱}{۲}[(m+۱)^۳ + x]$ برای $k_{m,m}$ وجود دارد اگر و تنها اگر $k = \frac{۱}{۲}[(m+۱)^۳ - x]$.

برای گراف $k_{۲,۲}$ از فرمول (۱۰.۲) نتیجه می‌گیریم $۱۲ \leq k \leq ۱۵$ و یک جستجوی کامل نشان می‌دهد برای هر عدد صحیح در بازهٔ $[۱۲, ۱۵]$ حداقل یک برچسب‌گذاری جادویی کامل رأسی وجود دارد. در حقیقت، دقیقاً پنج برچسب‌گذاری جادویی کامل در گراف $k_{۲,۲}$ وجود دارد. نمایش‌های ماتریسی آن‌ها به قرار زیر است:

$$\left[\begin{array}{cc|c} ۳ & ۷ & ۰ \\ ۴ & ۱ & ۸ \\ ۶ & ۵ & ۲ \end{array}\right] : k = ۱۳ \qquad \left[\begin{array}{cc|c} ۷ & ۵ & ۰ \\ ۳ & ۱ & ۸ \\ ۲ & ۶ & ۴ \end{array}\right] : k = ۱۲ \tag{۱۱.۲}$$

$$\left[\begin{array}{cc|c} ۲ & ۴ & ۰ \\ ۷ & ۳ & ۵ \\ ۶ & ۸ & ۱ \end{array}\right] : k = ۱۵ \qquad \left[\begin{array}{cc|c} ۳ & ۵ & ۰ \\ ۷ & ۱ & ۶ \\ ۴ & ۸ & ۲ \end{array}\right] : k = ۱۴ \qquad \left[\begin{array}{cc|c} ۶ & ۴ & ۰ \\ ۵ & ۱ & ۷ \\ ۲ & ۸ & ۳ \end{array}\right] : k = ۱۳ \tag{۱۲.۲}$$

برای گراف $k_{۳,۳}$ از فرمول (۱۰.۲) خواهیم داشت $۳۶ \leq k \leq ۲۸$ و k می‌تواند تمامی مقادیر این بازه را اتخاذ کند. ۳۵ برچسب‌گذاری جادویی کامل رأسی با $k = ۲۸$ وجود دارد. به‌ازای $k = ۳۶$ هفتاد و به‌ازای $k = ۳۵$ چهارصدوهفتادوهفت برچسب‌گذاری جادویی کامل رأسی وجود خواهند داشت. این‌که آیا برای هر مقدار مجاز k در فرمول (۱۰.۲) حداقل یک برچسب‌گذاری جادویی کامل رأسی وجود خواهد داشت یک مسئلهٔ باز است.

[1] Spectrum

در حالت $k_{m,m+1}$ می‌توانیم کران فرمول (۹.۲) را با استفاده از رویه‌ای مشابه اثبات قضیه ۲.۲ بهبود بخشیم، برای این کار S_1 جمع برچسب‌های رئوس مجموعهٔ m تایی و S_2 را جمع برچسب‌های رئوس مجموعهٔ $m+1$ تایی قرار می‌دهیم. مجدداً S_E را به‌عنوان مجموع برچسب یال‌ها نمایش می‌دهیم. هر یال مجاور با دقیقاً یکی از رئوس هر دو مجموعه است، بر این اساس خواهیم داشت:

$$km = S_1 + S_E \quad \geq 1 + 2 + \ldots + (m + m(m+1)) \tag{۱۳.۲}$$

بنابراین

$$k \geq \frac{1}{2}(m+1)^2(m+2). \tag{۱۴.۲}$$

از طرفی خواهیم داشت:

$$\begin{aligned} k(m+1) &= S_2 + S_E \\ &\leq (m+1) + (m+2) + \ldots + ((2m+1) + m(m+1)), \\ k &\leq \frac{1}{2}(m+1)(m^2 + 4m + 2) \end{aligned} \tag{۱۵.۲}$$

برای گراف $k_{1,2}$، خواهیم داشت $6 \leq k \leq 7$ و برای هر دو مقدار، برچسب‌گذاری جادویی کامل رأسی وجود دارد. به‌عبارت‌دیگر

$$\left[\begin{array}{cc|c} 3 & 5 & 0 \\ \hline 4 & 2 & 1 \end{array}\right] : k = 7 \qquad \left[\begin{array}{cc|c} 5 & 4 & 0 \\ \hline 1 & 2 & 3 \end{array}\right] : k = 6 \tag{۱۶.۲}$$

اگرچه برای گراف $k_{2,3}$ مقادیر مجاز k بازهٔ $[18, 21]$ است اما فقط برای $k = 18, 19, 20$ می‌توان برچسب‌گذاری جادویی کامل رأسی پیدا کرد. نمایش ماتریسی این برچسب‌گذاری‌ها به قرار زیر است:

$$\left[\begin{array}{ccc|c} 8 & 9 & 11 & 0 \\ \hline 1 & 6 & 5 & 7 \\ 10 & 4 & 3 & 2 \end{array}\right] : k = 19 \qquad \left[\begin{array}{ccc|c} 9 & 10 & 11 & 0 \\ \hline 1 & 6 & 4 & 7 \\ 8 & 2 & 3 & 5 \end{array}\right] : k = 18 \tag{۱۷.۲}$$

$$\left[\begin{array}{ccc|c} 6 & 9 & 11 & 0 \\ \hline 4 & 8 & 7 & 1 \\ 10 & 3 & 2 & 5 \end{array}\right] : k = 20 \qquad \left[\begin{array}{ccc|c} 8 & 9 & 11 & 0 \\ \hline 1 & 7 & 6 & 5 \\ 10 & 3 & 2 & 4 \end{array}\right] : k = 19 \tag{۱۸.۲}$$

برای گراف $k_{2,3}$ برای همهٔ مقادیر k که $40 \leq k \leq 46$ برچسب‌گذاری جادویی کامل وجود دارد. در این رابطه یک مسئلهٔ باز به قرار زیر است:

برای کدام مقادیر k که در روابط (۱۴.۲) و (۱۵.۲) صدق می‌کنند برچسب‌گذاری جادویی کامل رأسی وجود دارد؟

۳ برچسب‌گذاری جادویی-اول گراف $k_{n,n}$

گراف‌های جادویی که در آن برای هر یال $e \in E(G)$، $f(e)$ یک عدد اول منحصربه‌فرد باشد گراف‌های جادویی-اول [1] نامیده می‌شوند در واقع دامنه و برد تابع f برای چنین گراف‌هایی به‌صورت $f : E(G) \to$ Prime positive integers تعریف می‌شود. اِستِوارت در [۱۰] ثابت کرد $k_{3,3}$ یک گراف جادویی- اول با ثابت جادویی $k = 139$ است. کوچک‌ترین مقدار ثابت جادویی k برای گراف جادویی- اول $k_{n,n}$، $n \geq 3$ چقدر است؟ سِدلِیسِک نشان داد کوچک‌ترین مقدار k برای گراف جادویی- اول $k_{3,3}$ برابر ۵۳ است [۹]. در این بخش می‌خواهیم برچسب‌گذاری جادویی-اول گراف کامل دوبخشی $k_{4,4}$ را توصیف کنیم [۱]. ازآنجاکه توزیع اعداد اول، توزیعی نامنظم است؛ ارائهٔ یک قضیهٔ کلی برای پیدا کردن کوچک‌ترین مقدار k برای گراف‌های جادویی-اول $k_{n,n}$، $(n \geq 5)$ تاکنون حل نشده است و در واقع یک مسئلهٔ باز است.

[1] Prime-magic

قضیه ۱.۳. کوچک‌ترین مقدار k برای گراف جادویی-اول $k_{۴,۴}$ برابر ۱۱۴ است.

اثبات. $A = (f(e_{ij}))$ نمایش ماتریسی برچسب‌گذاری گراف $k_{۴,۴}$ است، درایه‌های A از اعداد اول تشکیل شده‌اند و f برچسب‌گذاری جادویی گراف $k_{۴,۴}$ است. قرار دهید $S = \sum_{i=۱}^{۴} f(e_{ij})$ که e_{ij} یال متصل‌کنندهٔ رأس i و رأس j در گراف $k_{۴,۴}$ است. به‌وضوح $S \geq ۴۳۸$، زیرا $k \equiv ۰ \pmod 2$ و $S = ۴k$. اولین مقدار S ای که در شرط بالا صدق می‌کند $S = ۴۴۰$ است. بنابراین $k = ۱۱۰ \equiv -۱ \pmod 3$، لذا هر چهارتایی از اعداد اول (که $f(e_{ij}) \neq ۲$) باید دارای دو مقدار همنهشت با -۱ در پیمانهٔ ۳ باشد و عدد دیگر با -۱ در پیمانهٔ ۳ همنهشت است. از طرفی هر چهارتایی از اعداد اول که $f(e_{ij}) \neq ۲, ۳$، یا همهٔ مقادیر آن‌ها در پیمانهٔ ۳ همنهشت با -۱ باشد و یا اینکه یکی از این مقادیر در پیمانهٔ ۳ همنهشت با -۱ بوده و سه مقدار دیگر در پیمانهٔ ۳ همنهشت با ۱ باشند. بنابراین ماتریسی با درایه‌های $-۱, ۱, ۰$ وجود خواهد داشت که مجموع هر سطر و هر ستون ماتریس در پیمانهٔ ۳ همنهشت با -۱ است. بااین‌وجود، مجموع ۳ عدد اول و همچنین مجموع ۱۰ عدد اول در پیمانهٔ ۳ همنهشت با $+۱$ است و مجموع ۵ عدد اول در پیمانهٔ ۳ همنهشت با -۱ است که باعث به وجود آمدن ماتریس زیر می‌شوند و $S > ۴۴$ خواهد شد که این یک تناقض است.

$$\begin{bmatrix} ۰ & ۱ & -۱ & -۱ \\ ۱ & -۱ & ۱ & ۱ \\ -۱ & ۱ & ۱ & ۱ \\ -۱ & ۱ & ۱ & ۱ \end{bmatrix}$$

اکنون حالت $k = ۱۱۲ \equiv ۱ \pmod 3$ را بحث می‌کنیم، در این حالت هر چهارتایی از اعداد $f(e_{ij}) \neq ۲$ و $f(e_{۱۱}) = ۳$ باید شامل دو مقدار $+۱$ و یک مقدار همنهشت با -۱ در پیمانهٔ ۳ باشند و هر چهارتایی از اعداد $f(e_{ij}) \neq ۲, ۳$ یا همگی در پیمانهٔ ۳ همنهشت با ۱ هستند و یا سه عدد از آن‌ها همنهشت با -۱ و دیگری همنهشت با ۱ در پیمانهٔ ۳ هستند.

$$\begin{bmatrix} ۰ & -۱ & ۱ & ۱ \\ -۱ & ۱ & -۱ & -۱ \\ ۱ & -۱ & -۱ & -۱ \\ ۱ & -۱ & -۱ & -۱ \end{bmatrix}$$

جمع هر سه عدد اول و مجموع هر پنج عدد اول همنهشت با ۱ در پیمانهٔ ۳ است و جمع هر ۱۰ عدد اول معادل با -۱ در پیمانهٔ ۳ بزرگ‌تر از ۴۴۸ است. این بدان معنی است که برای $k = ۱۱۲$ هیچ گراف جادویی اول $k_{۴,۴}$ وجود ندارد.

مشابه بالا می‌توان برای $k = ۱۱۴$ نشان داد که دقیقاً دو ماتریس با درایه‌های $-۱, +۱, ۰$ وجود دارند.

الف) $\begin{bmatrix} ۰ & ۱ & ۱ & ۱ \\ ۱ & -۱ & ۱ & -۱ \\ ۱ & ۱ & -۱ & -۱ \\ ۱ & -۱ & -۱ & ۱ \end{bmatrix}$ ب) $\begin{bmatrix} ۰ & -۱ & -۱ & -۱ \\ -۱ & ۱ & -۱ & ۱ \\ -۱ & ۱ & ۱ & -۱ \\ -۱ & -۱ & ۱ & ۱ \end{bmatrix}$

برای ماتریس (الف) به تناقض خواهیم رسید ولی برای ماتریس (ب) به یک ماتریس متشکل از اعداد اول متمایز خواهیم رسید و این نشان می‌دهد عدد ۱۱۴ کمترین مقدار ممکن برای k است

$$\begin{bmatrix} ۳ & ۱۱ & ۴۷ & ۵۳ \\ ۲۳ & ۳۷ & ۴۱ & ۱۳ \\ ۲۹ & ۶۱ & ۷ & ۱۷ \\ ۵۹ & ۵ & ۱۹ & ۳۱ \end{bmatrix}.$$

□

۴ نتیجه‌گیری و پیشنهادها

در این مقاله، ابتدا مفهوم برچسب‌گذاری جادویی کامل رأسی را برای یک گراف دلخواه تعریف کردیم. سپس نشان دادیم که یک گراف کامل دوبخشی نامتعادل نمی‌تواند دارای برچسب‌گذاری جادویی کامل رأسی باشد و برای آن دسته از گراف‌های کامل دوبخشی که در شرط قضیه ۲.۲ قرار ندارند با استفاده از مربع جادویی، نحوهٔ ساخت برچسب‌گذاری جادویی کامل رأسی را نشان دادیم و مجموعهٔ طیف (مجموعهٔ مقادیر k) آن‌ها را محاسبه کردیم. در نهایت، برچسب‌گذاری جادویی-اول گراف $k_{n,n}$ را مورد بررسی قرار داده و نشان دادیم که به ازای $n = ۴$

یک برچسب‌گذاری جادویی-اول برای گراف $k_{n,n}$ وجود دارد. برای $n \geq ۵$ مسئلهٔ وجود برچسب‌گذاری جادویی کامل گراف $k_{n,n}$ یک مسئلهٔ باز است و مطالعه و بررسی این مسئله توصیه می‌شود.

ضمیمه (نحوهٔ ساخت مربع جادویی)

یک مربع جادویی از مرتبهٔ n، مربعی با n سطر و n ستون است به‌طوری‌که مجموع اعداد سطرها، ستون‌ها و قطرهای آن مقداری ثابت به نام ثابت جادویی است که با $\mu(A)$ یا به‌طور مختصر با μ نشان داده می‌شود. برای ساخت یک مربع جادویی A از مرتبه n باید یک دستگاه معادلات به‌صورت زیر حل نمود

$$A = \begin{bmatrix} a_{۱۱} & \cdots & a_{۱n} \\ \vdots & \ddots & \vdots \\ a_{n۱} & \cdots & a_{nn} \end{bmatrix}$$

$$\sum_{i=۱}^{n} a_{ij} = \mu \qquad j = ۱, ۲, ۳, \ldots, n$$

$$\sum_{j=۱}^{n} a_{ij} = \mu \qquad i = ۱, ۲, ۳, \ldots, n$$

$$\sum_{i=j} a_{ij} = \mu$$

$$\sum_{\mathbf{i=n,\ j=۱}} a_{ij} = \mu$$

$$\sum_{\mathbf{i=۱,\ j=n}} a_{ij} = \mu$$

$$(a_{۱,\mathbf{n}} + a_{۲,\mathbf{n-۱}} + a_{۳,\mathbf{n-۲}} + \ldots + a_{\mathbf{n-۱},۲} + a_{\mathbf{n},۱} = \mu)$$

مثال :

$$\mathbf{A} = \begin{bmatrix} \mathbf{a_{۱۱}} & \mathbf{a_{۱۲}} & \mathbf{a_{۱۳}} \\ \mathbf{a_{۲۱}} & \mathbf{a_{۲۲}} & \mathbf{a_{۲۳}} \\ \mathbf{a_{۳۱}} & \mathbf{a_{۳۲}} & \mathbf{a_{۳۳}} \end{bmatrix}$$

$$\mathbf{a_{۱۱} + a_{۱۲} + a_{۱۳} = ۱۵}$$

$$\mathbf{a_{۲۱} + a_{۲۲} + a_{۲۳} = ۱۵}$$

$$\mathbf{a_{۳۱} + a_{۳۲} + a_{۳۳} = ۱۵}$$

$$\mathbf{a_{۱۱} + a_{۲۱} + a_{۳۱} = ۱۵}$$

$$\mathbf{a_{۱۲} + a_{۲۲} + a_{۳۲} = ۱۵}$$

$$\mathbf{a_{۱۳} + a_{۲۳} + a_{۳۳} = ۱۵}$$

$$\mathbf{a_{۱۱} + a_{۲۲} + a_{۳۳} = ۱۵}$$

$$\mathbf{a_{۱۳} + a_{۲۲} + a_{۳۱} = ۱۵}$$

یک جواب این دستگاه معادلات عبارت است از

$$A = \begin{bmatrix} ۸ & ۱ & ۶ \\ ۳ & ۵ & ۷ \\ ۴ & ۹ & ۲ \end{bmatrix}.$$

References

[1] Baca, M., & Hollander, I. (1990). Prime-magic labeling of $k_{n,n}$. *Journal of Franklin Inst*, 327, 923–926. DOI: https://doi.org/10.1016/0016-0032(90)90069-U.

[2] Freyberg, B. (2023). Face-magic labelings of some gridded graphs. *Communications in Combinatorics and Optimization*, 8, 595–601. DOI: https://doi.org/10.22049/CCO.2023.28208.1478.

[3] Inpoonjai, Ph., & Jiarasuksakun, T. (2018). Balanced Degree-Magic Labelings of Complete Bipartite Graphs under Binary Operations. *Iranian Journal of Mathematical Sciences and Informatics*, 13, 1–13. DOI: https://doi.org/10.7508/ijmsi.2018.13.001.

[4] MacDougall, J.A., Gray, I.D., Simpson, R.J., & Wallis, W.D. (2003). Vertex-Magic Total Labelings of Complete Bipartite Graphs. *Ars Combinatoria*, 69, 1–12.

[5] Marimuthu, G., & Balakrishnan, M. (2012). E-super vertex magic labelings of graphs. *Discrete Appl. Math*, 160, 1766–1774. DOI: https://doi.org/10.1016/j.dam.2012.03.016.

[6] Marimuthu, G., & Stalin K. (2016). Mixed cycle-E-super magic decomposition of complete bipartite graphs. *Journal of Algorithms and Computation*, 47, 37–52.

[7] Mejia, M. (2022). Vertex-Magic Total Labeling on G-sun Graphs. *In BSU Honors Program Theses and Projects. Item 554*.

[8] Rikio, I. & et al. (2024). Recent studies on the super edge-magic deficiency of graphs. *Theory and Applications of Graphs*, Vol. 11, Iss. 1, Article 1. DOI: https://doi.org/10.20429/tag.2024.110101.

[9] Sedláček, J. (1976). On magic graphs. *Mathematica Slovaca*, 26, 329–335.

[10] Stewart, B.M. (1966). Magic graphs. *Canadian Journal of Mathematics*, 18, 1031–1059. DOI: https://doi.org/10.4153/CJM-1966-104-7.

[11] West, D.B. (2001). Introduction to Graph Theory. *Prentice-Hall*.

[12] Zeen El Deen, M.R., & et al. (2024). Super Edge Magic Harmonious Labeling for Certain Graphs. *Frontiers in Scientific Research and Technology*, 8, 47–56. DOI: https://doi.org/10.21608/FSRT.2023.248393.1114.

Measure Algebras and Applications

Local sequence entropy of dynamical systems

Amir Assari[1]

1. Department of Mathematics, Jundi-Shapur University of Technology, Dezful, Iran.
Email: amirassari@jsu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 11 March 2024
Received in revised form:
05 May 2024
Accepted: 18 June 2024
Published Online:
20 August 2024

Keywords:
Entropy,
Finitely ergodic map,
Local entropy,
Sequence entropy

2020 Mathematics Subject Classification:
28D20, 37A35

ABSTRACT

In this paper, we present a local approach to sequence entropy of compact dynamical systems. We show that, given any continuous map on a compact metric space with finitely many ergodic measures and any increasing sequence of natural numbers, there is a local sequence entropy map, in the sense that, its integral with respect to any invariant measure results in the corresponding sequence entropy.

Cite this article: Assari, A. (2024). Local sequence entropy of dynamical systems. *Measure Algebras and Applications*, 1(2), 30–40. http://doi.org/10.22091/MAA.2024.10505.1016

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10505.1016

Extended Abstract

Introduction

The concept of sequence entropy was introduced by Kushnirenko [6]. This invariant could distinguish between automorphisms with zero entropy. Let $(X, \mathcal{B}, \mu)$ be a probability space and $T : X \to X$ be a measurable map preserving μ. Let also, $\Gamma = \{t_i\}_{i\geq 1}$ be a sequence of increasing positive integers (if T is invertible, then the sequence may consist of arbitrary integers). The sequence entropy of T with respect to ξ is defined by

$$h_{\mu,\Gamma}(T, \xi) = \lim \sup_{n\to\infty} \frac{1}{n} H_\mu(\bigvee_{i=0}^{n-1} T^{-t_i}\xi),$$

where $H_\mu(\eta) = -\sum_{A\in\eta} \mu(A) \log \mu(A)$ is the usual Shannon entropy of a partition η. Finally, the metric sequence entropy of T (with respect to Γ) is defined by

$$h_{\mu,\Gamma}(T) = \sup_{\xi} h_{\mu,\Gamma}(T, \xi),$$

where the supremum is taken over all finite partitions of X. Clearly if we set $\Gamma = \{i\}_{i=1}^{\infty}$, then we will have the usual metric entropy. In [8], Newton proved that the sequence entropy of an ergodic automorphism with finite positive entropy is a multiple of the metric entropy of the system. The relationship between sequence entropy and generators was also studied by Rokhlin [16]. The special case of aperiodic automorphisms has also been studied in [8]. One may find a comparison between some results in classical Kolmogorov entropy and sequence entropy in [1]. Comprehensive discussions and results on sequence entropy of dynamical systems may be found in [4, 5]. There are also other concepts of entropy based on sequences of integers that generalize Kolmogorov entropy [21, 22]. There are several local approaches to the concept of entropy in dynamical systems [3, 6, 9, 9–12, 16]. This motivates us to extend the local theory of entropy of dynamical systems to the sequence entropy case. In the present paper, for finitely ergodic dynamical systems, we follow the definition of sequence entropy in a local manner. Given any sequence Γ, we define a local entropy J_Γ which all sequence entropies $h_{\mu,\Gamma}(T)$ with μ, as an invariant measure, are extracted from J_Γ. In the rest of the paper, if $T : X \to X$ is a continuous map on a compact metric space, then we denote by $M(X, T)$ and $E(X, T)$ the set of all T-invariant and T-ergodic probability measures on X respectively. In 1970, Newton presented the relationship between the sequence entropy and Kolmogorov entropy. We first recall the following definition.

***Definition* 0.1.** *([8]) Given an increasing sequence of integers $\Gamma = \{t_i\}_{i=1}^{n}$ let*

$$S_\Gamma(n, k) = \text{card} \bigcup_{i=1}^{n} \{t_i, t_i + 1, ..., t_i + k\},$$

and define

$$K(\Gamma) = \lim_{k\to\infty} \left(\limsup_{n\to\infty} \frac{S_\Gamma(n, k)}{n} \right).$$

The following theorem states the relationship between sequence entropy and Kolmogorov entropy for invertible ergodic systems.

***Theorem* 0.2.** *([8]) Let $T : X \to X$ be an invertible map preserving an ergodic measure μ. Then*

(i) $h_{\mu,\Gamma}(T) = 0$ *if* $K(\Gamma) = 0$.

(ii) $h_{\mu,\Gamma}(T) = K(\Gamma)h_\mu(T)$ *if* $0 < h_\mu(T) < \infty$.

(iii) $h_{\mu,\Gamma}(T) = 0$ *if* $0 < K(\Gamma) < \infty$ *and* $h_\mu(T) = 0$.

(iv) $h_{\mu,\Gamma}(T) = \infty$ *if* $0 < K(\Gamma) \leq \infty$ *and* $h_\mu(T) = \infty$.

In Section 2, we present some results on sequence entropy. In Section 3, we present a local approach to the sequence entropy of compact dynamical systems. We assign a map to any compact dynamical system which can be used to extract the sequence entropy by integrating it with respect to any invariant measure. In Section 4, we give some concluding remarks.

Conclusion

In this paper, the following definitions and results are given:

***Definition* 0.3.** *For $x \in X$ and $A \subseteq X$, the average visit time of x in A is defined as follows:*

$$\omega(x, A) := \limsup_{n\to\infty} \frac{1}{n} |\{0 \leq j \leq n-1, T^j(x) \in A\}|,$$

where $|\cdot|$ stands for the cardinality of a set.

***Definition* 0.4.** *Let ξ be a partition and $x \in X$. We define $\Omega(x, \xi)$ as follows:*

$$\Omega(x, \xi) := \sum_{A\in\xi} \phi(\omega(x, A)),$$

where $\phi(t) = -t \log t$ for $t > 0$ and $\phi(0) = 0$. If η is another partition of X, then the conditional version of the previous quantity is defined as follows:

$$\Omega(x, \xi|\eta) := \sum_{A\in\xi, B\in\eta} \omega(x, B)\phi\left(\frac{\omega(x, A \cap B)}{\omega(x, B)}\right).$$

***Definition* 0.5.** *Let $\Gamma = \{t_i\}_{i\geq 1}$ be an increasing sequence of positive integers, and ξ be a finite partition of X. The Γ-local entropy map of T with respect to ξ is defined as follows:*

$$J_\Gamma(x, \xi) := \limsup_{n\to\infty} \frac{1}{n} \Omega(x, \bigvee_{i=1}^{n} T^{-t_i}\xi).$$

For $\Gamma = \{i\}_{i=1}^{\infty}$, we simply write $J_\Gamma = J$.

***Lemma* 0.6.** *For any $x \in X$ and partitions ξ and η, we have*

$$\Omega(x, \xi \vee \eta) \geq \Omega(x, \xi) + \Omega(x, \eta|\xi).$$

***Lemma* 0.7.** *For any $x \in X$ and Borel partitions ξ, η, if $\xi < \eta$, then $\Omega(x, \xi) \leq \Omega(x, \eta)$.*

The following theorem is our main result.

***Theorem* 0.8.** *Let $T : X \to X$ be a continuous finitely ergodic map on a compact metric space and $\Gamma = \{t_i\}_{i\geq 1}$ be an increasing sequence of positive integers. Then, for every T-invariant Borel probability measure μ we have*

$$\sup_{\xi} \int_X J_\Gamma(x,\xi)d\mu(x) = h_{\mu,\Gamma}(T),$$

where the supremum is taken over all finite Borel partitions of X.

The following properties are proved in [1].

***Proposition* 0.9.** *(i) Let $\Gamma = \{t_i\}_{i\geq 1}$ be a sequence of integers and $k \in \mathbb{N}$. If $T : X \to X$ is a map preserving the measure μ and ξ is a finite partition of X, then*

$$h_{\mu,\Gamma}(T,\xi) = h_{\mu,\sigma^k(\Gamma)}(T,\xi),$$

where $\sigma : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ is the shift map. In particular,

$$h_{\mu,\Gamma}(T) = h_{\mu,\sigma^k(\Gamma)}(T).$$

(ii) Let $\Gamma = \{k^n\}_{n\geq 1}$ and ξ be a partition of X. If T is a map preserving the measure μ, then

$$h_{\mu,\Gamma}(T,\xi) = h_{\mu,\Gamma}(T^{k^m},\xi)$$

for any $m \in \mathbb{N}$. In particular,

$$h_{\mu,\Gamma}(T) = h_{\mu,\Gamma}(T^{k^m}).$$

The following proposition is the local version of Proposition 0.9.

***Proposition* 0.10.** *Let $T : X \to X$ be a compact dynamical system, preserving a Borel probability measure μ and ξ be a Borel partition of X.*

(i) Given any sequence of positive integers $\Gamma = \{t_i\}_{i\geq 1}$, we have $J_\Gamma(x,\xi) = J_{\sigma^k(\Gamma)}(x,\xi)$ for μ-almost every $x \in X$.

(ii) If $\Gamma = \{k^n\}_{n\geq 1}$, then, for any $m \in \mathbb{N}$ we have $J_\Gamma^T(x,\xi) = J_\Gamma^{T^{k^m}}(x,\xi)$ for μ-almost every $x \in X$, where J_Γ^T and $J_\Gamma^{T^{k^m}}$ are the Γ-local entropy maps corresponding to T and T^{k^m}, respectively.

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۴۰-۳۰

آنتروپی دنباله‌ای موضعی دستگاه‌های دینامیکی

امیر عصاری [۱]

۱. گروه ریاضی، دانشکده علوم پایه، دانشگاه صنعتی جندی‌شاپور دزفول، ایران. رایانامه: amirassari@jsu. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۲/۲۱
تاریخ بازنگری: ۱۴۰۳/۲/۱۶
تاریخ پذیرش: ۱۴۰۳/۳/۲۹
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
آنتروپی،
آنتروپی موضعی،
آنتروپی دنباله‌ای،
توابع به‌طور متناهی ارگودیک

رده‌بندی ریاضی:
28D20, 37A35

چکیده

در این مقاله، رویکردی موضعی برای آنتروپی دنباله‌ای دستگاه‌های دینامیکی فشرده ارائه می‌کنیم. نشان می‌دهیم که متناظر با هر تابع پیوسته روی یک فضای متریک فشرده با تعداد متناهی اندازهٔ ارگودیک و هر دنبالهٔ صعودی از اعداد طبیعی، یک تابع آنتروپی دنبالهٔ موضعی وجود دارد، به این معنا که انتگرال آن نسبت به هر اندازهٔ پایا منجر به آنتروپی دنباله‌ای متناظر می‌شود.

استناد: عصاری، امیر. (۱۴۰۳). آنتروپی دنباله‌ای موضعی دستگاه‌های دینامیکی. جبرهای اندازه و کاربردها، ۱(۲)، ۴۰-۳۰.
http://doi.org/10.22091/MAA.2024.10505.1016

ناشر: دانشگاه قم.

۱ مقدمه

مفهوم آنتروپی دنباله‌ای دستگاه‌های دینامیکی توسط کوشنیرنکو [۶] معرفی شد. به کمک این کمیت پایا می‌توان بین اتومورفیسم‌هایی با آنتروپی صفر تمایز قائل شد. فرض کنید $(X,\mathcal{B},\mu)$ یک فضای احتمال بوده و $T:X\to X$ یک تابع حافظ اندازهٔ μ باشد. همچنین، فرض کنید $\Gamma=\{t_i\}_{i\geq 1}$ دنباله‌ای صعودی از اعداد مثبت باشد (اگر T وارون‌پذیر باشد، آنگاه این دنباله می‌تواند مشتمل بر اعداد صحیح نیز باشد). آنتروپی دنباله‌ای T نسبت به افراز اندازه‌پذیر ξ به‌صورت زیر تعریف می‌شود:

$$h_{\mu,\Gamma}(T,\xi)=\lim_{n\to\infty}\sup\frac{1}{n}H_\mu(\bigvee_{i=0}^{n-1}T^{-t_i}\xi),$$

که در آن $H_\mu(\eta)=-\sum_{A\in\eta}\mu(A)\log\mu(A)$ آنتروپی شانون معمول نسبت به افراز η است. در نهایت، آنتروپی دنباله‌ای T (نسبت به Γ) به‌صورت

$$h_{\mu,\Gamma}(T)=\sup_{\xi}h_{\mu,\Gamma}(T,\xi),$$

تعریف می‌شود که در آن سوپریمم بر روی کلیهٔ افرازهای اندازه‌پذیر و متناهی X گرفته می‌شود. بدیهی است که اگر قرار دهیم $\Gamma=\{i\}_{i=1}^{\infty}$ آنگاه به آنتروپی کولموگوروف T خواهیم رسید. در [۸]، نیوتن ثابت کرد که آنتروپی دنباله‌ای یک اتومورفیسم ارگودیک با آنتروپی مثبت متناهی مضرب آنتروپی متریک دستگاه است. رابطهٔ بین آنتروپی دنباله‌ای و مولدها نیز توسط روخلین [۱۶] مورد بررسی قرار گرفت. مورد خاص اتومورفیسم‌های متناوب نیز در [۸] بررسی شده است. می‌توان مقایسه‌ای بین برخی از خواص آنتروپی کلموگروف کلاسیک و آنتروپی دنباله‌ای در [۱] یافت. مباحث و نتایج جامع در مورد آنتروپی دنباله‌ای دستگاه‌های دینامیکی را می‌توان در [۴، ۵] یافت. همچنین مفاهیم دیگری از آنتروپی بر اساس دنباله‌های اعداد صحیح وجود دارند که آنتروپی کلموگروف [۲۱، ۲۲] را تعمیم می‌دهند. چندین رویکرد موضعی برای مفهوم آنتروپی در دستگاه‌های دینامیکی وجود دارند [۳، ۶، ۹، ۹–۱۲، ۱۶]. این به ما انگیزه می‌دهد تا نظریهٔ موضعی آنتروپی دستگاه‌های دینامیکی را به حالت آنتروپی دنباله‌ای گسترش دهیم. در مقالهٔ حاضر، تعریف آنتروپی دنباله‌ای را به‌صورت موضعی دنبال می‌کنیم. متناظر با هر دنبالهٔ Γ، یک آنتروپی موضعی J_Γ تعریف می‌کنیم که تمام آنتروپی‌های دنبالهٔ $h_{\mu,\Gamma}(T)$ با μ، به‌عنوان یک اندازهٔ ثابت، از J_Γ استخراج می‌شوند. در ادامهٔ مقاله، اگر $T:X\to X$ یک تابع پیوسته بر یک فضای متریک فشرده باشد، آنگاه مجموعهٔ اندازه‌های احتمال T-پایا و T-ارگودیک را به‌ترتیب با $M(X,T)$ و $E(X,T)$ نشان می‌دهیم. در بخش ۲، برخی از نتایج مهم در مورد آنتروپی دنباله‌ای را ارائه می‌کنیم. در بخش ۳، یک رویکرد موضعی به آنتروپی دنباله‌ای دستگاه‌های دینامیکی فشرده ارائه می‌کنیم. یک تابع را به هر دستگاه دینامیکی فشرده متناظر می‌کنیم که می‌توان از آن برای استخراج کلیهٔ آنتروپی‌های دنباله‌ای متناظر با هر اندازهٔ پایای احتمال استفاده نمود. در بخش ۴، چند نکتهٔ پایانی را بیان می‌کنیم.

۲ نتایجی در باب آنتروپی دنباله‌ای

در این بخش، مفاهیم مقدماتی و پیش‌نیازهای مورد استفاده در بخش بعدی این مقاله را از نظر می‌گذرانیم. در سرتاسر این مقاله، X یک فضای متریک فشرده و $T:X\to X$ یک تابع پیوسته است. تحت این شرایط، زوج (X,T) را یک دستگاه دینامیکی فشرده می‌نامیم. روشن است که X به‌طور طبیعی به σ-جبر بورل $\mathcal{B}_X$ مجهز است. در این بخش ابتدا برخی از خصوصیات آنتروپی دنباله‌ای را بررسی می‌کنیم و سپس برخی از نتایج را تعمیم می‌دهیم. فرض کنید $T:X\to X$ یک دستگاه دینامیکی فشرده باشد، به‌عنوان مثال، X یک فضای متریک فشرده و T پیوسته باشد. فرض کنید $\Gamma=\{t_i\}_{i\geq 1}$ نیز یک دنبالهٔ صعودی از اعداد صحیح مثبت باشد. گزارهٔ زیر با اصلاح ساده‌ای از اثبات قضیه ۳۸ [۲۲] به دست می‌آید. بنابراین از ارائهٔ جزئیات استدلال خودداری می‌کنیم.

گزاره ۱.۲. فرض کنید $T:X\to X$ تابعی پیوسته بر فضای متریک فشردهٔ X باشد. فرض کنید $\{\xi_n\}_{n\geq 1}$ دنباله‌ای از افرازهای متناهی اندازه‌پذیر باشد به‌گونه‌ای که $\operatorname{diam}(\xi_n)\to 0$. در این صورت برای هر $\mu\in M(X,T)$، داریم

$$h_{\mu,\Gamma}(T)=\lim_{n\to\infty}h_{\mu,\Gamma}(T,\xi_n).$$

گزارهٔ زیر نیز برقرار است.

گزاره ۲.۲. برای هر افراز متناهی اندازه‌پذیر ξ نگاشت $\mu\longmapsto h_{\mu,\Gamma}(T,\xi)$ آفین است.

در سال ۱۹۷۰، نیوتن رابطهٔ بین آنتروپی دنباله‌ای و آنتروپی کولموگروف را ارائه کرد. ابتدا تعریف زیر را یادآوری می‌کنیم.

تعریف ۳.۲. ([۸]) متناظر با هر دنبالهٔ صعودی از اعداد صحیح مانند $\Gamma = \{t_i\}_{i=1}^{n}$ قرار دهید

$$S_\Gamma(n,k) = \text{card} \bigcup_{i=1}^{n} \{t_i, t_i+1, ..., t_i+k\},$$

و همچنین

$$K(\Gamma) = \lim_{k\to\infty} \left(\limsup_{n\to\infty} \frac{S_\Gamma(n,k)}{n} \right).$$

قضیهٔ زیر رابطهٔ بین آنتروپی دنباله‌ای و آنتروپی کولموگوروف را برای توابع وارون‌پذیر بیان می‌کند.

قضیه ۴.۲. ([۸]) فرض کنید $T : X \to X$ تابعی وارون‌پذیر و حافظ اندازهٔ احتمال μ باشد. در این صورت:

۱. $h_{\mu,\Gamma}(T) = 0$ هرگاه $K(\Gamma) = 0$.

۲. $h_{\mu,\Gamma}(T) = K(\Gamma)h_\mu(T)$ هرگاه $0 < h_\mu(T) < \infty$.

۳. $h_{\mu,\Gamma}(T) = 0$ هرگاه $0 < K(\Gamma) < \infty$ و $h_\mu(T) = 0$.

۴. $h_{\mu,\Gamma}(T) = \infty$ هرگاه $0 < K(\Gamma) \leq \infty$ و $h_\mu(T) = \infty$.

۳ آنتروپی دنباله‌ای موضعی

در این بخش، رویکردی موضعی به آنتروپی دنباله‌ای دستگاه‌های دینامیکی فشرده ارائه می‌دهیم. در این راستا، از مراجع [۱۶، ۱۷] ایده گرفته‌ایم.

تعریف ۱.۳. برای $x \in X$ و $A \subseteq X$، متوسط زمان ملاقات x در A به‌صورت زیر تعریف می‌شود:

$$\omega(x,A) := \limsup_{n\to\infty} \frac{1}{n} |\{0 \leq j \leq n-1, T^j(x) \in A\}|,$$

که در آن $|\cdot|$ نشان‌دهندهٔ تعداد اعضای یک مجموعه است.

تعریف ۲.۳. فرض کنید ξ افرازی اندازه‌پذیر از X بوده و $x \in X$. قرار دهید:

$$\Omega(x,\xi) := \sum_{A\in\xi} \phi(\omega(x,A)),$$

که در آن $\phi(t) = -t\log t$ برای $t > 0$ و همچنین $\phi(0) = 0$. اگر η افرازی دیگر از X باشد، آنگاه نسخهٔ شرطی کمیت اخیر را به‌صورت زیر تعریف می‌کنیم:

$$\Omega(x,\xi|\eta) := \sum_{A\in\xi, B\in\eta} \omega(x,B)\phi\left(\frac{\omega(x,A\cap B)}{\omega(x,B)}\right).$$

تعریف ۳.۳. فرض کنید $\Gamma = \{t_i\}_{i\geq 1}$ دنباله‌ای صعودی از اعداد طبیعی بوده و ξ افرازی اندازه‌پذیر از X باشد. Γ- آنتروپی موضعی تابع T نسبت به ξ را به‌صورت زیر تعریف می‌کنیم:

$$J_\Gamma(x,\xi) := \limsup_{n\to\infty} \frac{1}{n}\Omega(x, \bigvee_{i=1}^{n} T^{-t_i}\xi).$$

برای $\Gamma = \{i\}_{i=1}^{\infty}$ به‌سادگی می‌نویسیم $J_\Gamma = J$.

لم ۴.۳. برای هر $x \in X$ و افرازهای اندازه‌پذیر ξ و η داریم:

$$\Omega(x,\xi\vee\eta) \geq \Omega(x,\xi) + \Omega(x,\eta|\xi).$$

اثبات: فرض کنید ξ و η دو افراز اندازه‌پذیر X باشند به‌گونه‌ای که $\xi < \eta$. بدون کاسته‌شدن از کلیت، می‌توان فرض کرد که برای A در ξ و η داریم $\omega(x, A) \neq 0$. در این صورت

$$\begin{aligned}
\Omega(x, \xi \vee \eta) &= -\sum_{A\in\xi, B\in\eta} \omega(x, A\cap B)\log\omega(x, A\cap B) \\
&= -\sum_{A\in\xi, B\in\eta} \omega(x, A\cap B)\log\left(\frac{\omega(x, A\cap B)}{\omega(x, A)}.\omega(x, A)\right) \\
&= -\sum_{A\in\xi, B\in\eta} \omega(x, A\cap B)\log\left(\frac{\omega(x, A\cap B)}{\omega(x, A)}\right) \qquad (۱.۳) \\
&\quad -\sum_{A\in\xi, B\in\eta} \omega(x, A\cap B).\log\omega(x, A) \\
&= \Omega(x, \eta|\xi) - \sum_{A\in\xi, B\in\eta} \omega(x, A\cap B).\log\omega(x, A). \qquad (۲.۳)
\end{aligned}$$

به‌سادگی می‌توان دید که برای هر $A \in \xi$،

$$\sum_{B\in\eta} \omega(x, A\cap B) \geq \omega(x, A). \qquad (۳.۳)$$

از ضرب طرفین رابطه (۳.۳) در $-\log\omega(x, A)$ و سپس جمع‌بندی بر اعضای $A \in \xi$ خواهیم داشت

$$\begin{aligned}
-\sum_{A\in\xi, B\in\eta} \omega(x, A\cap B)\log\omega(x, A) &\geq -\sum_{A\in\xi} \omega(x, A)\log\omega(x, A) \\
&= \Omega(x, \xi).
\end{aligned}$$

از ترکیب رابطهٔ اخیر با رابطه (۳.۳) حکم اثبات می‌شود. □

لم ۵.۳. برای هر $x \in X$ و افرازهای اندازه‌پذیر ξ و η، اگر $\xi < \eta$، آنگاه $\Omega(x, \xi) \leq \Omega(x, \eta)$.

اثبات. با به‌کارگیری لم ۴.۳ داریم

$$\Omega(x, \eta) = \Omega(x, \xi \vee \eta) \geq \Omega(x, \xi \vee \eta) \geq \Omega(x, \xi) + \Omega(x, \eta|\xi) \geq \Omega(x, \xi). \quad \square$$

اکنون، در قضیهٔ بعد نشان می‌دهیم که J_Γ در واقع یک نگاشت آنتروپی دنباله‌ای موضعی است.

قضیه ۶.۳. فرض کنید $T : X \to X$ تابعی پیوسته بر فضای متریک فشردهٔ X بوده به‌گونه‌ای که $|E(X, T)| < +\infty$ و $\Gamma = \{t_i\}_{i\geq 1}$ دنباله‌ای صعودی از اعداد طبیعی باشد. در این صورت، برای هر اندازهٔ بورل T-پایای μ داریم

$$\sup_\xi \int_X J_\Gamma(x, \xi)d\mu(x) = h_{\mu,\Gamma}(T),$$

که در آن سوپریمم بر کلیهٔ افرازهای اندازه‌پذیر X گرفته می‌شود.

اثبات. فرض کنید ξ افرازی اندازه‌پذیر از X باشد. ابتدا فرض کنید $\mu \in E(X, T)$. در این صورت، برای هر مجموعهٔ اندازه‌پذیر $A \subseteq X$، و با به‌کارگیری قضیهٔ ارگودیک بیرخوف، نتیجه می‌گیریم که برای تقریباً هر $x \in X$ داریم $\omega(x, A) = \mu(A)$. بنابراین، برای تقریباً هر $x \in X$ خواهیم داشت $\Omega(x, \xi) = H_\mu(\xi)$. به‌طور مشابه، برای هر $n \in \mathbb{N}$، مجموعهٔ $D_n \subseteq X$ موجود است به‌گونه‌ای که $\mu(D_n) = 1$ و برای هر $x \in D_n$،

$$\Omega(x, \bigvee_{i=1}^n T^{-t_i}\xi) = H_\mu(\bigvee_{i=1}^n T^{-t_i}\xi).$$

قرار دهید $D = \bigcap_{n=1}^\infty D_n$، در این صورت $\mu(D) = 1$ و برای هر $x \in D$ داریم $J_\Gamma(x, \xi) = h_{\mu,\Gamma}(T, \xi)$. انتگرال‌گیری از طرفین رابطهٔ اخیر منجر به نتیجهٔ مورد نظر برای اندازه‌های ارگودیک می‌شود. اکنون فرض کنید $\mu \in M(X, T)$. چون مجموعهٔ

اندازه‌های ارگودیک متناهی است، پس اندازه‌های $\mu_1, \mu_2, \cdots, \mu_k \in E(X,T)$ و اعداد $0 \leq \lambda_i \leq 1$ $(1 \leq i \leq k)$ موجودند به‌گونه‌ای $\sum_{i=1}^{k} \lambda_i = 1$ و $\mu = \sum_{i=1}^{k} \lambda_i \mu_i$. اکنون به کمک گزاره ۲.۲ و برقراری حکم برای اندازه‌های ارگودیک، داریم

$$\int_X J_\Gamma(x,\xi) d\mu(x) = \sum_{i=1}^{k} \lambda_i \int_X J_\Gamma(x,\xi) d\mu_i(x) = \sum_{i=1}^{k} \lambda_i h_{\mu_i}(T,\xi) = h_\mu(T,\xi). \quad (۴.۳)$$

در نهایت، حکم با سوپریمم‌گیری از رابطهٔ اخیر بر کلیهٔ افرازهای اندازه‌پذیر به دست می‌آید. □

ویژگی‌های زیر در مرجع [۱] ثابت شده‌اند.

گزاره ۷.۳. ۱. فرض کنید $\Gamma = \{t_i\}_{i\geq 1}$ دنباله‌ای صعودی از اعداد صحیح بوده و $k \in \mathbb{N}$. اگر $T : X \to X$ تابعی حافظ اندازهٔ μ بوده و ξ افرازی اندازه‌پذیر از X باشد، آنگاه

$$h_{\mu,\Gamma}(T,\xi) = h_{\mu,\sigma^k(\Gamma)}(T,\xi),$$

که در آن $\sigma : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ نگاشت انتقال است. به‌طور خاص،

$$h_{\mu,\Gamma}(T) = h_{\mu,\sigma^k(\Gamma)}(T).$$

۲. فرض کنید $\Gamma = \{k^n\}_{n\geq 1}$ و ξ افرازی اندازه‌پذیر از X باشد. اگر T تابعی حافظ اندازهٔ μ باشد، آنگاه برای هر $m \in \mathbb{N}$،

$$h_{\mu,\Gamma}(T,\xi) = h_{\mu,\Gamma}(T^{k^m},\xi),$$

و به‌طور خاص

$$h_{\mu,\Gamma}(T) = h_{\mu,\Gamma}(T^{k^m}).$$

گزارهٔ بعدی نسخهٔ موضعی از گزاره ۷.۳ است.

گزاره ۸.۳. فرض کنید $T : X \to X$ یک دستگاه دینامیکی فشرده باشد که حافظ اندازهٔ μ است و به‌علاوه، ξ افرازی اندازه‌پذیر از X باشد.

۱. اگر $\Gamma = \{t_i\}_{i\geq 1}$ دنباله‌ای از اعداد طبیعی باشد، آنگاه برای تقریباً هر $x \in X$ داریم $J_\Gamma(x,\xi) = J_{\sigma^k(\Gamma)}(x,\xi)$.

۲. اگر $\Gamma = \{k^n\}_{n\geq 1}$ آنگاه برای هر $m \in \mathbb{N}$ رابطهٔ $J_\Gamma^T(x,\xi) = J_\Gamma^{T^{k^m}}(x,\xi)$ برای تقریباً هر $x \in X$ برقرار است، که در آن J_Γ^T و $J_\Gamma^{T^{k^m}}$ به‌ترتیب نگاشت‌های Γ- آنتروپی موضعی متناظر با T و T^{k^m} هستند.

اثبات. ۱. توجه کنید که برای $n \in \mathbb{N}$ داریم $\bigvee_{i=k+1}^{n} T^{-t_i}\xi < \bigvee_{i=1}^{n} T^{-t_i}\xi$. بنابراین، طبق لم ۵.۳ داریم

$$\Omega(x, \bigvee_{i=k+1}^{n} T^{-t_i}\xi) \leq \Omega(x, \bigvee_{i=1}^{n} T^{-t_i}\xi).$$

با تقسیم رابطهٔ اخیر بر n و میل دادن n به بی‌نهایت، خواهیم داشت

$$J_{\sigma^k(\Gamma)}(x,\xi) \leq J_\Gamma(x,\xi),$$

و یا به‌طور معادل

$$J_\Gamma(x,\xi) - J_{\sigma^k(\Gamma)}(x,\xi) \geq 0. \quad (۵.۳)$$

از طرف دیگر، با به‌کارگیری رابطه (۴.۳) و گزاره ۷.۳ خواهیم داشت

$$\int_X (J_\Gamma(x,\xi) - J_{\sigma^k(\Gamma)}(x,\xi)) d\mu(x) = h_{\mu,\Gamma}(T,\xi) - h_{\mu,\sigma^k(\Gamma)}(T,\xi) = 0. \quad (۶.۳)$$

نتیجه از روابط (۵.۲) و (۶.۲) حاصل می‌شود.

۲. ابتدا توجه کنید که $k^m\Gamma = \{k^{n+m}\}_{n\geq 1} = \sigma^m(\Gamma)$. همچنین، به‌سادگی مشاهده می‌شود که اگر ξ افرازی از X باشد، آنگاه

$$J^T_{\sigma^m(\Gamma)}(x,\xi) = J^T_{k^m\Gamma}(x,\xi) = J^{T^{k^m}}_{\Gamma}(x,\xi).$$

بنابراین، با توجه به قسمت ۱، داریم $J^{T^{k^m}}_{\Gamma}(x,\xi) \leq J^T_{\Gamma}(x,\xi)$ و یا به‌طور معادل

$$J^T_{\Gamma}(x,\xi) - J^{T^{k^m}}_{\Gamma}(x,\xi) \geq 0. \tag{۷.۳}$$

از طرف دیگر، با به‌کارگیری (۴.۳) و قسمت ۲ از گزاره ۷.۳ خواهیم داشت

$$\int_X (J^T_{\Gamma}(x,\xi) - J^{T^{k^m}}_{\Gamma}(x,\xi))d\mu(x) = h_{\mu,\Gamma}(T,\xi) - h_{\mu,\Gamma}(T^{k^m},\xi) = 0. \tag{۸.۳}$$

در نهایت، حکم از روابط (۷.۳) و (۸.۳) به دست می‌آید. □

۴ نتیجه‌گیری

در این مقاله، رویکردی موضعی به مفهوم آنتروپی دنباله‌ای دستگاه‌های دینامیکی فشرده با تعداد متناهی اندازهٔ ارگودیک ارائه شده است. متناظر با هر دنبالهٔ صعودی $\Gamma = \{t_i\}_{i\geq 1}$ از اعداد صحیح مثبت، یک تابع J_Γ تعریف کردیم که در واقع یک تابع آنتروپی دنبالهٔ موضعی است، به این معنا که انتگرال J_Γ نسبت به هر اندازهٔ پایای μ به $h_{\mu,\Gamma}(T)$ منجر می‌شود. توجه داشته باشید که مطالعهٔ موضعی آنتروپی دستگاه‌های دینامیکی ممکن است در اندازه‌گیری اطلاعات تولیدشده توسط یک دستگاه در ناحیهٔ خاصی از فضا به‌جای کل فضا اعمال شود. برای مثال، این رویکرد برای تعریف محتوای اطلاعاتی یک ساختار مولکولی، با استفاده از آنتروپی موضعی به کار گرفته می‌شود.

References

[1] Balibrea, F., Jiménéz Lopéz, V., & Cánovas, J.S. (1999). Some results on entropy and sequence entropy. *International Journal of Bifurcation and Chaos*, 9, 1731–1742. DOI: https://doi.org/10.1142/s0218127499001218.

[2] Barreira, L., Pesin, Ya., & Schemling, J. (1997). On a general concept of multifractality: Multifractal spectra for dimensions, entropies, and Lyapunov exponents. Multifractal rigidity. *Chaos*, 7, 27–38. DOI: https://doi.org/10.1063/1.166232.

[3] Brin, M., & Katok, A. (1983). On local entropy in geometric dynamics. 30–38, *New York, Springer-Verlag*, (Lecture Notes in Mathematics 1007). DOI: https://doi.org/10.1007/bfb0061408.

[4] Cánovas, J.S. (2007). Topological sequence entropy and topological dynamics of interval maps. *Dyn. Contin. Discrete Impuls. Syst. Ser. A Math. Anal*, 14, 47–54.

[5] Cánovas, J.S., & Jiménez López, V. (2002). Computing explicitly topological sequence entropy: the unimodal case. *Ann. Inst. Fourier, Grenoble*, 52, 1093–1133. DOI: https://doi.org/10.5802/aif.1913.

[6] Kushnirenko, A.G. (1967). On Metric invariants of entropy type. *Russ. Math. Surv*, 22, 53–61. DOI: https://doi.org/10.1070/rm1967v022n05abeh001225.

[7] McMillan, B. (1953). The basic theorems of information theory. *Ann. Math. Statist*, 24, 196–219. DOI: https://doi.org/10.1214/aoms/1177729028.

[8] Newton, D. (1970). On Sequence entropy II. *Math. Syst. Th*, 4, 126–128. DOI: https://doi.org/10.1007/bf01691096.

[9] Pesin, Ya. (1977). Characteristic Lyapunov exponents and smooth ergodic theory. *Russian Math. Surveys*, 32, 54–114. DOI: https://doi.org/10.1070/rm1977v032n04abeh001639.

[10] Pesin, Ya., & Weiss, H. (1997). A multifractal analysis of equilibrium measures for conformal expanding maps and Moran-like geometric constructions. J. Stat. Phys, 86, 233–275. DOI: https://doi.org/10.1007/bf02180206.

[11] Pesin, Ya., & Weiss, H. (1997). The multifractal analysis of Gibbs measures: Motivation, mathematical foundation, and examples. *Chaos*, 7, 89–106. DOI: https://doi.org/10.1063/1.166242.

[12] Rahimi, M. (2015). A local approach to g-entropy. *Kybernetika*, 51, 231–245. DOI: https://doi.org/10.14736/kyb-2015-2-0231.

[13] Rahimi, M., & Assari, A. (2020). Mutual Entropy Map for Continuous Systems on Compact Metric Spaces. *Mathematical Analysis and Convex Optimization*, 1, 49–55. DOI: https://doi.org/10.29252/maco.1.1.6.

[14] Rahimi, M., & Assari, A. (2021). On local metric pressure of dynamical systems. *Periodica Mathematica Hungarica*, 82, 223–230. DOI: https://doi.org/10.1007/s10998-020-00355-w.

[15] Rahimi, M., Assari, A., & Ramezani, F. (2016). A local approach to Yager entropy of dynamical systems. *International Journal of Fuzzy Systems*, 18, 98–102. DOI: https://doi.org/10.1007/s40815-015-0062-z.

[16] Rahimi, M., & Mohammadi Anjedani, M. (2018). A local view on the Hudetz correction of the Yager entropy of dynamical systems. *International Journal of General Systems*, 48, 321–333. DOI: https://doi.org/10.1080/03081079.2018.1552688.

[17] Rahimi, M., & Shakouri, A. (2019). On Hudetz entropy localization. *Fuzzy Sets and Systems*, 367, 96–106. DOI: https://doi.org/10.1016/j.fss.2018.11.005.

[18] Rokhlin, V.A. (1959). Entropy of metric automorphism. *Dokl. Akad. Nauk. SSSR*, 124, 980–983.

[19] Takens, F., & Verbitski, E. (1999). Multifractal Analysis of Local Entropies for Expansive Homeomorphisms with Specification. *Commun. Math. Phys*, 203, 593–612. DOI: https://doi.org/10.1007/s002200050627.

[20] Walters, P. (1982). An introduction to ergodic theory. *Springer-Verlag*. DOI: https://doi.org/10.1007/springerreference_60354.

[21] Zhao, Y., & Pesin, Y. (2015). Scaled entropy for dynamical systems. *J. Stat. Phys*, 158, 447–475. DOI: https://doi.org/10.1007/s10955-014-1133-5.

[22] Zhao, Y., & Pesin, Y. (2016). Errutum to: Scaled entropy for dynamical systems. *J. Stat. Phys*, 162, 1654–1660. DOI: https://doi.org/10.1007/s10955-016-1451-x.

Measure Algebras and Applications

Increasing the efficiency of the key generation algorithm for NTRU with the help of the norm field

Reza Alimoradi[1]✉, **Mohammad Hossein Noorallahzadeh**[2], **Ahmad Gholami**[3]

1. Corresponding Author, University of Qom, Qom, Iran. Email: r.alimoradi@qom.ac.ir
2. University of Qom, Qom, Iran. Email: mh.noorallahzadeh@stu.qom.ac.ir
3. University of Qom, Qom, Iran. Email: a.gholami@qom.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 09 February 2024
Received in revised form:
16 April 2024
Accepted: 19 June 2024
Published Online:
20 August 2024

Keywords:
Post-quantum cryptographic schemes,
Lattice-based cryptographic schemes,
NTRU-based cryptographic schemes,
Algorithms based on soft field

2020 Mathematics Subject Classification: 20F05, 05C05

ABSTRACT

Conceptually, a signature scheme consists of three steps: private key generation, signature, and authentication. Private key generation in NTRU-based signature schemes on a typical laptop (Intel Core i7-6567U 3.30 GHz) takes a long time (more than one second), while signature and verification take much less time (for example, a thousandths of a second). The current paper deals with providing solutions to reduce the time of private key generation. In this paper, the previous methods are studied and then a new method based on the norm field is introduced and it is shown that the execution time is significantly reduced by using it.

Cite this article: Alimoradi, R., Noorallahzadeh, M.H., & Gholami, A. (2024). Increasing the efficiency of the key generation algorithm for NTRU with the help of the norm field. *Measure Algebras and Applications*, 1(2), 41–70. http://doi.org/10.22091/MAA.2024.10396.1014

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10396.1014

Extended Abstract

Introduction

NTRU lattices have emerged as a specialized subset of general lattices, offering distinct advantages that have garnered significant attention in the realm of cryptography. Their efficient implementation of common lattice algorithms has positioned them as a favorable choice for employment in asymmetric cryptographic schemes, particularly those involving public key encryption and digital signatures. Within NTRU-based schemes, fundamental components such as keys and ciphertexts are represented as polynomials, reflecting the inherent algebraic structure of NTRU lattices.

Notably, the private key utilized in certain NTRU-based schemes is characterized by a polynomial of low degree with exceedingly small coefficients, while the public key is represented by a polynomial with large coefficients. This distinction effectively establishes short and long bases within the lattice structure, contributing to the security and efficiency of NTRU-based cryptographic systems. The unique properties of NTRU lattices have not only facilitated the development of robust cryptographic solutions but have also sparked further exploration and research in the field, holding promise for continued advancements in secure communication and data protection. Several lattice-based encryption schemes usually require solving the NTRU equation to generate keys:

$$fG-gF=q \bmod x^n+1$$

where f and g are constants, and the objective is to calculate F and G for the equation. It should be noted that the polynomials are in

$$\mathbb{Z}[x]/\left(x^n+1\right).$$

Conceptually, a signature scheme consists of three stages: key generation, signing, and verification. In the context of NTRU-based signature schemes, the process of private key generation typically consumes a significant amount of time, especially when executed on standard computing hardware such as a regular laptop (Intel Core i7-6567U 3.30 GHz), where the generation process may exceed one second. Conversely, the signing and verification stages exhibit notably lower time requirements, often on the order of milliseconds.

The current paper delves into the challenge of mitigating the time-intensive nature of private key generation in NTRU-based signature schemes. It thoroughly examines existing methods and their associated limitations, paving the way for the introduction of a novel approach rooted in the realm of number fields. This innovative method showcases a remarkable reduction in the execution time required for private key generation, presenting a compelling avenue for enhancing the overall efficiency and practicality of NTRU-based signature schemes.

The introduction of asymmetric encryption systems by Diffie and Hellman in 1976 marked a significant milestone in the evolution of cryptography. At the core of asymmetric systems lies the concept of employing a set of information along with a one-way function for encryption, which in isolation does not provide sufficient data for decryption. For the decryption process, an additional finite set of information, known as the "private key," is indispensable, while the set of information required for encryption is termed the "public key."

The prevalent one-way function in asymmetric encryption, rooted in discrete logarithm and exponentiation, serves as the cornerstone for well-known asymmetric encryption systems such as ElGamal,

ECC, and RSA. These systems hinge on number theory problems that, with the emergence of quantum computing, are susceptible to resolution. In response to this vulnerability, extensive research has been directed toward exploring the complexity of lattice problems, aiming to identify alternative approaches for asymmetric encryption that do not rely on lattice-based foundations. Notably, the NTRU encryption system, a highly efficient lattice-based system, derives its resilience from the formidable challenge of solving the Shortest Vector Problem (SVP) within lattices, presenting a compelling avenue for robust encryption in the face of advancing cryptographic landscapes. This paper also delves into the mathematical prerequisites needed for the study. Specifically, it includes a review of lattice concepts, gathering essential concepts from NTRU lattices, studying number fields and related concepts, reviewing Karatsuba multiplication (used in the paper), and finally examining ring structures.

A real-valued V module over R, which functions as a module over a set closed under addition and scalar multiplication, transforms into a lattice when it is bounded by a finite set of real numbers. The defining characteristic of a lattice lies in the presence of a bounded set of real numbers that can be added to the set, establishing its fundamental structure.

In our pursuit of optimizing computations on polynomial rings, particularly in the context of solving the NTRU equation, we have strategically employed number fields to enhance efficiency and performance. This strategic utilization of number fields carries significant practical implications, particularly for the post-quantum Falcon signature algorithm. Notably, our optimizations enable the complete utilization of the Falcon signature algorithm on small microcontrollers or even smart cards, with the algorithm requiring a mere 32 kilobytes of RAM to operate effectively. This level of resource efficiency extends to the implementation of long-term secure NTRU lattices (degree $n = 1024$), showcasing that all signature operations, including signature generation, verification, and key pair generation, can be seamlessly executed on such resource-constrained hardware environments. This breakthrough paves the way for the widespread deployment of robust cryptographic solutions in diverse computing environments, from embedded systems to IoT devices, without compromising on security or performance.
We also list several open questions below:

Non-cyclotomic polynomials: In our description, we covered cyclotomic polynomials as a covering module. This approach can be extended to other modules. In fact, for any module

$$\varphi = \varphi'(x^d)$$

for some $d > 1$, the use of a "number field" can divide the degree by d for the purposes of calculating residuals and solving the NTRU equation.

Even if φ is not irreducible in $Q[x]$, i.e., if $Q[x]/(\varphi)$ is not actually a field, the general case remains a problem for further investigation. However, the use of reducible modules in NTRU lattices is generally not recommended.

While our achievements in memory management are indeed significant, the challenge of effectively handling large integers remains a prominent concern that warrants continued exploration. From the perspective of implementation complexity, the prospect of eliminating large integers, for instance by conducting all operations in the Residue Number System (RNS), without adversely impacting the execution time and memory requirements of our algorithms, presents an intriguing area for further investigation and potential optimization. This pursuit holds the promise of streamlining computational processes and resource utilization, contributing to enhanced efficiency across a spectrum of cryptographic applications.

In addition to addressing the management of large integers, it is imperative to explore potential ap-

plications of the method proposed in this paper to enhance the efficiency of other encryption algorithms. Just as we have demonstrated a constructive application of a number field in this work, distinct from the approach in a previous study, there is merit in investigating a constructive application of lattice tracking, as opposed to a different reference. This comparative exploration can shed light on the adaptability and versatility of our proposed methodology within the broader landscape of encryption and security protocols.

Furthermore, leveraging the method outlined in this paper to enhance attacks on a specific field or even on field tracking holds the potential to yield valuable insights, opening up new possibilities for specialized analysis applications in the realm of cryptography and security. These potential directions for further exploration underscore the multifaceted implications of the research presented in this paper, offering promising avenues for continued advancements in cryptographic techniques and their practical applications. This comprehensive approach to exploring the broader implications of our work sets the stage for future breakthroughs in the field of cryptography and computational security, paving the way for innovative solutions and heightened resilience in the face of evolving security challenges.

Conclusion

We presented the use of the norm field to optimize some computations on polynomial loops, especially the results and solutions of the NTRU equation. The second practical result is that Falcon's post-quantum signature algorithm is fully usable on small microcontrollers or even smart cards since 32 KB of RAM are required to run our algorithm even for a long-term secure NTRU network (degree $n = 1024$). Enough.: All operations related to signatures (signature generation, verification, and key pair generation) can be placed on such limited hardware.

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۷۰-۴۱

افزایش کارآمدی الگوریتم تولید کلید مشبکه‌های NTRU به کمک نرم میدان

رضا علیمرادی [۱]✉ ، محمدحسین نوراله زاده [۲] ، احمد غلامی [۳]

۱. نویسندهٔ مسئول، دانشگاه قم، قم، ایران. رایانامه: r. alimoradi@qom. ac. ir
۲. دانشگاه قم، قم، ایران. رایانامه: mh. noorallahzadeh@stu. qom. ac. ir
۳. دانشگاه قم، قم، ایران. رایانامه: a. gholami@qom. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۱/۲۰
تاریخ بازنگری: ۱۴۰۳/۱/۲۸
تاریخ پذیرش: ۱۴۰۳/۳/۳۰
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
طرح‌های رمزنگاری پساکوانتومی،
طرح‌های رمزنگاری مشبکهٔ مبنا،
طرح‌های رمزنگاری مبتنی بر NTRU،
الگوریتم‌های مبتنی بر نرم میدان

رده‌بندی ریاضی:
20F05, 05C05

چکیده

در طراحی بسیاری از طرح‌های نامتقارن مانند کلید عمومی و امضای دیجیتال از مشبکه‌های NTRU استفاده می‌کنند. به‌صورت مفهومی یک طرح امضا از سه مرحله تشکیل می‌شود: تولید کلید خصوصی، امضا و تصدیق. برای تولید کلید خصوصی در طرح‌های امضای مبتنی بر NTRU در یک لپ‌تاپ معمولی (Intel Core i7-6567U 3.30 GHz) زمان زیادی صرف می‌شود (بیش از یک ثانیه) درحالی‌که امضا و تصدیق به‌مراتب زمان کمتری نیاز دارند (برای مثال یک‌هزارم ثانیه). مقالهٔ فعلی به ارائهٔ راهکارهایی برای کاهش زمان مرحلهٔ تولید کلید خصوصی می‌پردازد. در این مقاله، روش‌های قبلی مورد مطالعه قرار می‌گیرند و سپس یک روش جدید مبتنی بر نرم میدان معرفی می‌گردد و نشان داده می‌شود که با استفاده از آن، زمان اجرا به‌طور قابل ملاحظه‌ای کاهش پیدا می‌کند.

استناد: علیمرادی، رضا.، نوراله زاده، محمدحسین.، غلامی، احمد. (۱۴۰۳). افزایش کارآمدی الگوریتم تولید کلید مشبکه‌های NTRU به کمک نرم میدان. جبرهای اندازه و کاربردها، ۱(۲)، ۷۰-۴۱.

http://doi.org/10.22091/MAA.2024.10396.1014

ناشر: دانشگاه قم.

۱ مقدمه

مشبکه‌های NTRU حالت خاصی از مشبکه‌های عمومی هستند. بسیاری از الگوریتم‌های رایج در نظریهٔ مشبکه‌ها زمانی که برای مشبکه‌های NTRU استفاده می‌شوند، به‌صورت بسیار کارآمدتری قابل پیاده‌سازی هستند. در عمل برای طراحی بسیاری از طرح‌های نامتقارن مانند کلید عمومی و امضای دیجیتال از این مشبکه‌ها استفاده می‌شود. در طرح‌های مبتنی بر NTRU عناصر اصلی مانند کلید، متن رمزی و ... از نوع چندجمله‌ای هستند. به‌طور خاص، کلید خصوصی مورد استفاده در برخی از طرح‌های مبتنی بر NTRU یک یا دو چندجمله‌ای با ضرایب بسیار کوچک، و کلید عمومی یک یا دو چندجمله‌ای با ضرایب بزرگ است که این‌ها را می‌توان به‌عنوان پایه‌های کوتاه و بلند در یک مشبکه در نظر گرفت. تعدادی از طرح‌های رمزنگاری مبتنی بر مشبکه، معمولاً برای تولید کلید، مستلزم حل معادلهٔ NTRU هستند:

$$fG-gF=q \bmod x^n+1.$$

در اینجا f و g ثابت بوده و هدف، محاسبهٔ F و G برای معادله است. لازم به ذکر است که چندجمله‌ای‌ها در $\mathbb{Z}[x]/\left(x^n+1\right)$ قرار دارند. در این مقاله به بررسی و مطالعهٔ پیش‌نیازهای ریاضی مورد نیاز نیز خواهیم پرداخت. به‌طور خاص:

- مروری بر مفاهیم مشبکه خواهیم داشت،
- مفاهیم مورد نیاز از مشبکه‌های NTRU را گردآوری می‌کنیم،
- نرم میدان و مفاهیم مرتبط با آن را مورد مطالعه قرار می‌دهیم،
- مروری بر ضرب کاراتسوبا خواهیم داشت (در مقاله مورد استفاده قرار گرفته است)،
- و در نهایت برج حلقه‌ها را بررسی می‌کنیم.

سامانه‌های رمزنگاری نامتقارن در سال ۱۹۷۶ توسط "دیفی" و "هلمن" با ارائه در مقاله [۹] معرفی شدند. یک سامانهٔ نامتقارن بر این مفهوم بنانهاده شده است که مجموعه‌ای متناهی از اطلاعات به انضمام یک تابع یک‌طرفه برای رمزنگاری اطلاعات مورد استفاده قرار می‌گیرد ولی این اطلاعات برای رمزگشایی کافی نیست و برای رمزگشایی داده‌های رمزشده به مجموعهٔ متناهی دیگری از اطلاعات نیاز است. به مجموعهٔ اطلاعات لازم برای رمزگذاری، "کلید عمومی" و به مجموعهٔ اطلاعات مورد نیاز برای رمزگشایی "کلید خصوصی" گفته می‌شود. تابع یک‌طرفهٔ پرکاربرد در رمزگذاری نامتقارن تجزیهٔ اعداد و لگاریتم گسسته است که اساس سامانه‌های رمزنگاری نامتقارن مانند ElGamal، ECC، RSA را تشکیل می‌دهد. این سامانه‌ها بر پایهٔ مسائل نظریهٔ اعداد استوارند که با بهبود قدرت و توسعهٔ محاسبات کوانتوم، قابل‌حل هستند. تحقیقات روی دشواری مسائل مشبکه، دانشمندان را به دستیابی نامزد دیگری برای رمزنگاری نامتقارن، امیدوار می‌کند؛ که چیزی جز رمزنگاری مبتنی بر مشبکه نیست. ازجمله مسائل دشوار در مشبکه که در این مقاله معرفی خواهند شد؛ می‌توان به مسائل کوتاه‌ترین بردار[۱] و نزدیک‌ترین بردار[۲] اشاره کرد. یکی از سامانه‌های فوق‌العاده کارآمد مبتنی بر مشبکه، سامانهٔ رمزنگاری NTRU است که به آن خواهیم پرداخت. این سامانه، امنیت خود را از سختی مسئلهٔ SVP اخذ می‌کند.

در ادامه مقدمات ریاضی لازم بیان می‌گردد: یک فضای برداری V روی اعداد حقیقی R، مجموعه‌ای از بردارها است که نسبت به اعمال جمع و ضرب بسته است. یک مشبکه شبیه به فضای برداری است که در آن به ضرب بردارها با اعداد صحیح محدود شده‌ایم.

۱.۱ تعاریف بنیادی مشبکه و ویژگی‌های آن

تعریف ۱.۱. اگر $v_1, v_2, \ldots, v_n$ مجموعه‌ای از بردارهای مستقل خطی باشد، مشبکهٔ L تولیدشده توسط آن، مجموعهٔ تمام ترکیبات خطی از $v_1, v_2, \ldots, v_n$ است که ضرایب اعداد صحیح هستند:

$$L = L\left(v_1, v_2, \ldots, v_n\right) = \left\{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \ : a_i \in Z\right\}.$$

مجموعهٔ $v_1, v_2, \ldots, v_n$، پایه و n را بعد مشبکهٔ L می‌نامند.

گزاره ۲.۱. اگر $V = \{v_1, v_2, \ldots, v_n\}$ و $W = \{w_1, w_2, \ldots, w_n\}$ پایه‌هایی برای مشبکهٔ L باشند، آنگاه $W = AV$، که A ماتریسی با درایه‌های صحیح است و $|\det(A)| = 1$.

[1] Shortest Vector Problem (SVP)
[2] Closest Vector Problem (CVP)

اثبات. ازآنجاکه $w_i \in L$، داریم

$$w_۱ = a_{۱۱}v_۱ + a_{۱۲}v_۲ + \dots a_{۱n}v_n$$
$$w_۲ = a_{۲۱}v_۱ + a_{۲۲}v_۲ + \dots a_{۲n}v_n$$
$$\vdots$$
$$w_n = a_{n۱}v_۱ + a_{n۲}v_۲ + \dots a_{nn}v_n \ .$$

این درحالی است که $a_{ij} \in Z$. به‌عبارت‌دیگر

$$\begin{pmatrix} w_۱ \\ w_۲ \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} a_{۱۱} & a_{۱۲} & \dots & a_{۱n} \\ a_{۲۱} & a_{۲۲} & \dots & a_{۲n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n۱} & a_{n۲} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} v_۱ \\ v_۲ \\ \vdots \\ v_n \end{pmatrix} .$$

ماتریس $\begin{pmatrix} a_{۱۱} & a_{۱۲} & \dots & a_{۱n} \\ a_{۲۱} & a_{۲۲} & \dots & a_{۲n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n۱} & a_{n۲} & \dots & a_{nn} \end{pmatrix}$ را A می‌نامیم. درنتیجه $W = AV$ که درایه‌های A صحیح هستند. ازطرفی می‌توان نتیجه گرفت که درایه‌های $A^{-۱}$ نیز صحیح هستند؛ زیرا می‌دانیم ماتریس B موجود است که $V = BW$ و چون $W = AV$، داریم $V = A^{-۱}W$. در نهایت وارون‌پذیری W، تساوی $B = A^{-۱}$ را نتیجه می‌دهد. به‌عبارت‌دیگر $A^{-۱}$ ماتریسی صحیح است. ازطرفی می‌دانیم $\det\left(A^{-۱}\right) \det\left(A\right) = ۱$، پس می‌توان گفت $|\det\left(A\right)| = ۱$. درنتیجه حکم به دست می‌آید. □

تعریف ۳.۱. ماتریس‌هایی با ویژگی فوق، درایه‌هایی صحیح همراه با قدر مطلق دترمینان برابر ۱، را ماتریس‌های یونی مادولار[1] می‌نامند.

تعریف ۴.۱. فرض کنید L مشبکهٔ n بعدی با پایهٔ $\{v_۱, v_۲, \dots, v_n\}$ باشد، دامنهٔ اصلی مشبکهٔ L منسوب به این پایه را، مجموعهٔ زیر در نظر می‌گیریم

$$F\left(v_۱, v_۲, \dots, v_n\right) = \{t_۱v_۱ + t_۲v_۲ + \dots t_nv_n \ : ۰ \leq t_i < ۱\} \ .$$

مثالی از مشبکهٔ ۲ بعدی و دامنهٔ اصلی آن در شکل ۱ آورده شده است.

گزاره ۵.۱. اگر $L \subseteq R^n$ مشبکه‌ای n بعدی و F دامنهٔ اصلی آن باشد، آنگاه هر بردار $w \in R^n$ نمایش منحصربه‌فردی به‌صورت $w = t + a$ دارد که $t \in F$ و $a \in L$.

اثبات. اگر $\{v_۱, v_۲, \dots, v_n\}$ را به‌عنوان پایه برای مشبکهٔ L در نظر بگیریم؛ می‌توان w را به‌صورت ترکیب خطی از آن‌ها نوشت

$$w = b_۱v_۱ + b_۲v_۲ + \dots + b_nv_n.$$

ازطرفی می‌توان نوشت $b_i = t_i + a_i$ که $۰ \leq t_i < ۱$ و $a_i \in Z$ (برای هر $۱ \leq i \leq n$). پس می‌توان t را برابر $t_۱ + t_۲ + \dots + t_n$ و a را برابر $a_۱ + a_۲ + \dots + a_n$ در نظر گرفت. برای اثبات منحصربه‌فردی نمایش $w = t + a$، فرض می‌کنیم $w = t + a = t' + a'$؛ که $t, t' \in F$ و $a, a' \in L$. ازآنجاکه $t \in F$ داریم $t = t_۱v_۱ + t_۲v_۲ + \dots t_nv_n$ که $۰ \leq t_i < ۱$. به همین ترتیب $t' = t'_۱v_۱ + t'_۲v_۲ + \dots + t'_nv_n$ که $۰ \leq t'_i < ۱$. ازآنجاکه $a \in L$ داریم $a = a_۱v_۱ + a_۲v_۲ + \dots + a_nv_n$ که $a_i \in Z$. به همین ترتیب $a' = a'_۱v_۱ + a'_۲v_۲ + \dots + a'_nv_n$ که $a'_i \in Z$. درنتیجه داریم

$$w = (t_۱ + a_۱)\, v_۱ + \dots + (t_n + a_n)\, v_n = \left(t'_۱ + a'_۱\right) v_۱ + \dots \left(t'_n + a'_n\right) v_n \ .$$

ازطرفی به دلیل استقلال $\{v_۱, v_۲, \dots, v_n\}$، داریم $t_i + a_i = t'_i + a'_i$ (برای هر $۱ \leq i \leq n$). درنتیجه

$$t_i - t'_i = a'_i - a_i \ .$$

پس هر دو طرف تساوی صفر خواهند شد که در نهایت؛ یکتایی نمایش w را نتیجه می‌دهد. □

[1] Uni Modular

تعریف ۶.۱. فرض کنید L مشبکهٔ n بعدی و F دامنهٔ اصلی آن باشد، حجم F را که با $Vol\,(F)$ نمایش می‌دهند، دترمینان L می‌نامیم.

گزاره ۷.۱ (نامساوی هادامارد). فرض کنید L مشبکه‌ای n بعدی باشد. برای هر پایهٔ $\{v_۱, v_۲, \ldots, v_n\}$ و دامنهٔ اصلی F، داریم

$$\det(L) = Vol\,(F) \leq ||v_۱||\,||v_۲|| \ldots ||v_n||$$

و اگر پایه‌ها متعامد باشند، نامساوی بالا تبدیل به تساوی خواهد شد.

گزاره ۸.۱. اگر $L \subseteq R^n$ مشبکه‌ای با بعد n، $\{v_۱, v_۲, \ldots, v_n\}$ پایهٔ آن و همچنین F دامنهٔ اصلی L منسوب به این پایه باشد، داریم

$$Vol\,(F) = |\det(V)|\,;$$

درحالی‌که درایه‌های V (ماتریس $n \times n$)، در سطر i ام معادل با درایه‌های v_i است.

اثبات. بنابر تعریف انتگرال، داریم

$$Vol\,(F) = \int_F dx_۱\, dx_۲ \ldots dx_n\,,$$

به‌طوری‌که $X = (x_۱, x_۲, \ldots, x_n) \in F$. ازآنجاکه $X = tV$؛ می‌توان نوشت $t \in C_n$

$$\begin{aligned}
&\int_F dx_۱\, dx_۲ \ldots dx_n \\
&= \int_{C_n V} dx_۱\, dx_۲ \ldots dx_n \\
&= \int_{C_n} |\det(V)|\, dt_۱\, dt_۲ \ldots dt_n \\
&= |\det(V)| \int_{C_n} dt_۱\, dt_۲ \ldots dt_n \\
&= |\det(V)|\,,
\end{aligned}$$

درنتیجه حکم به دست می‌آید. □

نتیجه ۹.۱. اگر $L \subseteq R^n$ مشبکه‌ای با بعد n باشد، آنگاه تمام دامنه‌های اصلی L (منسوب به هر پایهٔ دلخواه)، حجم یکسانی دارند. به‌عبارت‌دیگر؛ مقدار $\det(L)$ پایا است.

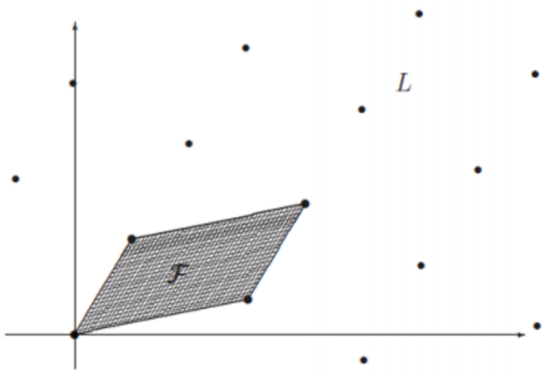
اثبات. اگر $\{v_۱, v_۲, \ldots, v_n\}$ و $\{w_۱, w_۲, \ldots, w_n\}$ دو پایه برای مشبکهٔ L باشند؛ باید نشان دهیم

$$|\det(V)| = |\det(W)|\,,$$

درحالی‌که V ماتریسی با سطرهای v_i و W ماتریسی با سطرهای w_i است. با توجه به گزاره ۲.۱، داریم $V = AW$ که $|\det(A)| = ۱$. خواهیم داشت

$$\begin{aligned}
|\det(V)| &= |\det(AW)| \\
&= |\det(A)\det(W)| \\
&= |\det(A)|\,|\det(W)| \\
&= |\det(W)|
\end{aligned}$$

درنتیجه حکم به دست می‌آید. □



شکل ۱: مشبکهٔ ۲-بعدی L و دامنهٔ اصلی آن.

۲.۱ مسائل دشوار در مشبکه

مسائل محاسباتی بنیادی در مشبکه‌ها، عبارت‌اند از پیدا کردن کوتاه‌ترین بردار ناصفر در مشبکه و یافتن نزدیک‌ترین بردار در مشبکه نسبت به برداری دلخواه.

مسئلهٔ کوتاه‌ترین بردار: مطلوب یافتن بردار ناصفر v در مشبکهٔ L است که $||v||$ کمترین مقدار ممکن باشد.

مسئلهٔ نزدیک‌ترین بردار: مطلوب یافتن بردار $v \in L$ است که نسبت به بردار داده‌شده $w \in R^n$ نزدیک‌ترین باشد. به‌عبارت‌دیگر؛ به‌ازای هر $a \in L$، داشته باشیم $||w - v|| \leq ||w - a||$.

هر دو مسئلهٔ SVP و CVP ازلحاظ محاسباتی بسیار دشوار هستند. به‌خصوص وقتی بعد مشبکه افزایش می‌یابد. از طرف دیگر؛ جواب‌های تخمینی برای این مسائل، کاربردهای بسیاری در مباحث ریاضیات کاربردی و محض دارند. لازم به ذکر است که مسئلهٔ SVP حالت خاصی از مسئلهٔ CVP است.

ازجمله مسائل دیگر در مشبکه، می‌توان به مسئلهٔ کوتاه‌ترین پایه[۱]، مسئلهٔ تقریب کوتاه‌ترین بردار[۲] و مسئلهٔ تقریب نزدیک‌ترین بردار[۳] اشاره کرد.

مسئلهٔ کوتاه‌ترین پایه: مطلوب یافتن کوتاه‌ترین پایهٔ $\{v_1, v_2, \ldots, v_n\}$ برای مشبکهٔ L است. نسخه‌های متفاوتی از SBP موجود هستند که هر یک وابسته به تعریف «اندازهٔ پایه» است.

مسئلهٔ تقریب کوتاه‌ترین بردار: فرض کنید مشبکهٔ L دارای بعد L باشد، مطلوب یافتن بردار $v \in L$ است که $||v|| < f(n)\,||v_{shortest}||$. روشن است که؛ بسته به انتخاب $f(n)$، جواب می‌تواند متفاوت باشد.

مسئلهٔ تقریب نزدیک‌ترین بردار: فرض کنید w بردار دلخواهی در R^n باشد. مطلوب یافتن بردار $u \in L$ است که به‌ازای هر $v \in L$، داشته باشیم $||w - u|| \leq \gamma\,||w - v||$.

۳.۱ تقریب‌هایی از اندازهٔ کوتاه‌ترین بردار در مشبکه

با توجه به اهمیت مسئلهٔ SVP؛ در این بخش به اندازهٔ کوتاه‌ترین بردار در مشبکه می‌پردازیم. چنان‌که با استفاده از قضایایی چون هرمیت[۴] و مینکوفسکی[۵]، کران بالایی برای جواب مسئلهٔ SVP به دست می‌آوریم. این کران وابسته به بعد و دترمینان مشبکه است.

قضیه ۱.۱۰ (هرمیت). هر مشبکهٔ L با بعد n، شامل بردار ناصفر $v \in L$ است که

$$||v|| \leq \sqrt{n}\det(L)^{\frac{1}{n}}\ .$$

تعریف ۱.۱۱. برای n داده‌شده، ثابت هرمیت γ_n، کوچکترین مقداری است که مشبکهٔ n بعدی L شامل بردار ناصفر v است که $||v||^2 \leq \gamma_n \det(L)^{\frac{2}{n}}$.

[1] Shortest Basis Problem(SBP)
[2] Approximate Shortest Vector Problem (appr. SVP)
[3] ApproximateClosest Vector Problem (appr. CVP or γ -CVP)
[4] Hermit
[5] Minkowski

بنابر قضیه ۱۰.۱، $\gamma_n \leq n$. مقدار دقیق γ_n برای $1 \leq n \leq 8$ و $n = 24$ به دست آمده است

$$\gamma_2^2 = \frac{4}{3}\ ,\ \gamma_3^3 = 2\ ,\ \gamma_4^4 = 4\ ,\ \gamma_5^5 = 8$$
$$\gamma_6^6 = \frac{64}{3},\ \gamma_7^7 = 64\ ,\ \gamma_8^8 = 256\ ,\ \gamma_{24} = 4.$$

روشن است که در سامانه‌های رمزی، مطلوب یافتن γ_nای با n بزرگ است. برای مقادیر بزرگ n، کران‌های زیر به دست آمده‌اند

$$\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e}\ ; \pi = 3/14159\ldots,\ e = 2/71828.$$

تذکر ۱۲.۱. صورت‌های دیگری از قضیه ۱۰.۱ موجودند که با تعداد بردارهای بیشتری سروکار دارند. به‌عنوان مثال؛ می‌توان ثابت کرد پایهٔ $\{v_1, v_2, \ldots, v_n\}$ برای مشبکهٔ n بعدی L وجود دارد که

$$||v_1||\ ||v_2|| \ldots ||v_n|| \leq n^{\frac{n}{2}} \det(L)\ .$$

تعریف ۱۳.۱. نسبت هادامارد پایهٔ $V = \{v_1, v_2, \ldots, v_n\}$ برای مشبکهٔ L برابر مقدار

$$H(V) = \frac{\det(L)}{||v_1||\ ||v_2|| \ldots ||v_n||}$$

تعریف می‌شود. داریم $0 < H(V) \leq 1$ و هنگامی که بردارها متعامد باشند، این مقدار برابر ۱ می‌شود. (معکوس نسبت هادامارد را **نقص تعامد** گویند.)

برای اثبات قضیهٔ هرمیت، نتیجه‌ای از قضیهٔ مینکوفسکی مورد استفاده قرار می‌گیرد. برای شرح قضیهٔ مینکوفسکی احتیاج به تعاریف زیر داریم.

تعریف ۱۴.۱. برای هر $a \in R^n$ و $r > 0$، گوی بسته به مرکز a و شعاع r را

$$B_r(a) = \{x \in R^n\ : ||x - a|| \leq R\}$$

تعریف می‌کنیم.

تعریف ۱۵.۱. اگر S زیرمجموعه‌ای از R^n باشد؛
الف) S را کران‌دار گویند، هرگاه طول بردارهای S کران‌دار باشد؛ یعنی $r > 0$ موجود باشد که S داخل گوی $B_r(0)$ باشد.
ب) S متقارن است، اگر برای هر $a \in S$، $-a$ نیز متعلق به S باشد.
ج) S محدب است، اگر به‌ازای $a, b \in S$، سرتاسر خط واصل a و b نیز متعلق به S باشد.
د) S بسته است، هرگاه به‌ازای هر $a \in R^n$ و $r > 0$ که $B_r(a)$ شامل حداقل یک نقطه از S باشد، داشته باشیم $a \in S$.

قضیه ۱۶.۱ (مینکوفسکی). اگر $L \in R^n$ مشبکه‌ای n بعدی و $S \in R^n$ مجموعهٔ کران‌دار، محدب و متقارن باشد که $Vol(S) > 2^n \det(L)$، آنگاه S شامل حداقل یک بردار ناصفر از مشبکهٔ L خواهد شد. به‌علاوه؛ اگر S بسته و نامساوی فوق مختار به تساوی نیز شود، حکم همچنان برقرار است.

اثبات. برای اثبات، فرض می‌کنیم $L \in R^n$ مشبکهٔ n بعدی و همچنین S ابرمکعب در R^n به مرکز صفر با طول اضلاع $2B$ باشد. به‌عبارت‌دیگر؛

$$S = \{(x_1, x_2, \ldots, x_n) \in R^n\ :\ -B \leq x_i \leq B\}\ .$$

روشن است که S مجموعه‌ای کران‌دار، بسته، محدب و متقارن است. ازآنجاکه $Vol(S) = (2B)^n$، قرار می‌دهیم $B = \det(L)^{\frac{1}{n}}$ تا شرط $2^n \det(L) \leq Vol(S)$ برقرار شود. حال قضیه ۱۶.۱ را برای $0 \neq a \in S \cap L$ به کار می‌بریم

$$||a|| = \sqrt{a_1^2 + \cdots + a_n^2} \leq \sqrt{n}B = \sqrt{n}\det(L)^{\frac{1}{n}}\ .$$

درنتیجه حکم به دست می‌آید. □

این امکان وجود دارد که ثابت ظاهرشده در قضیه ۱۰.۱ را با به‌کارگیری قضیه ۱۶.۱ برای یک ابرکره، بهبود بخشید. به‌منظور انجام این کار؛ نیاز به دانستن حجم یک گوی در R^n داریم.

تعریف ۱۷.۱. تابع $\Gamma(s)$ برای $s > 0$ برابر است با

$$\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}.$$

گزاره ۱۸.۱ (تقریب استرلینگ). برای مقادیر بزرگ s، تابع $\Gamma(1+s)^{\frac{1}{s}}$ به‌طور تقریبی برابر $\frac{s}{e}$ است.

قضیه ۱۹.۱. اگر $B_r(a)$ گوی به شعاع r در R^n باشد، آنگاه داریم

$$Vol(B_r(a)) = \frac{\pi^{\frac{n}{2}} R^n}{\Gamma\left(1+\frac{n}{2}\right)}.$$

تذکر ۲۰.۱. هنگامی که n مقداری بزرگ باشد، بنابر گزاره ۱۸.۱، خواهیم داشت

$$Vol(B_r(a))^{\frac{1}{n}} = \sqrt{\frac{2\pi e}{n}} r.$$

دوباره قضیه ۱۶.۱ را در نظر می‌گیریم، این بار مجموعهٔ S را گوی $B_r(0)$ قرار می‌دهیم و r را طوری انتخاب می‌کنیم که

$$2^n \det(L) \leq Vol(S) \tag{1.1}$$

پس می‌توان اطمینان حاصل کرد که $B_r(0)$ شامل حداقل یک بردار ناصفر مشبکهٔ L است. با فرض بزرگ بودن n، بنابر تذکر ۲۰.۱ داریم

$$Vol(B_r(0))^{\frac{1}{n}} = \sqrt{\frac{2\pi e}{n}} r.$$

ازطرفی شرط (۱.۲) ایجاب می‌کند

$$\sqrt{\frac{2n}{\pi e}} \det(L)^{\frac{1}{n}} \leq r.$$

پس می‌توان نتیجه گرفت $v \in L$ موجود است که داخل این گوی قرار می‌گیرد. به‌عبارت‌دیگر

$$||v|| \leq \sqrt{\frac{2n}{\pi e}} \det(L)^{\frac{1}{n}}.$$

مشاهده می‌شود که کران بهتری نسبت به قضیه ۱۰.۱ به دست آوردیم. اگرچه کران واقعی برای اندازهٔ کوتاه‌ترین بردار در مشبکه مجهول است، اما وقتی n بزرگ باشد؛ می‌توان اندازهٔ آن را با آرگومان‌های احتمالاتی تخمین زد. فرض کنید $B_r(0)$ گویی بزرگ به مرکز صفر باشد، آنگاه تعداد نقاط مشبکهٔ L در $B_r(0)$ به‌طور تقریبی برابر است با

$$\frac{Vol(B_r(0))}{Vol(F)}.$$

حال اگر این تعداد برابر یک باشد، داریم $Vol(F) = Vol(B_r(0))$، که بنابر تذکر ۲۰.۱ به دست می‌آید

$$r \approx \sqrt{\frac{n}{2\pi e}} \det(L)^{\frac{1}{n}}.$$

تعریف ۲۱.۱. فرض کنید L مشبکهٔ تصادفی n بعدی باشد، طول کوتاه‌ترین بردار ناصفر مورد انتظار گوسی در L به‌طور تقریبی برابر است با

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}} \det(L)^{\frac{1}{n}}.$$

به‌طور دقیق‌تر؛ اگر $\epsilon > 0$ ثابت باشد، آنگاه برای تمام nهای به‌قدر کافی بزرگ و مشبکه‌های تصادفی n بعدی، داریم

$$(1-\epsilon)\sigma(L) \leq ||v_{shortest}|| \leq (1+\epsilon)\sigma(L).$$

تذکر ۲۲.۱. برای nهای کوچک، بهتر است فرمول دقیق $B_r(\circ)$ استفاده شود. پس به‌منظور دستیابی به طول کوتاه‌ترین بردار مورد انتظار گوسی، خواهیم داشت

$$\begin{aligned} & Vol\left(B_r(\circ)\right) = Vol\left(F\right) \\ \Longrightarrow \quad & \frac{\pi^{\frac{n}{2}} r^n}{\Gamma\left(1+\frac{n}{2}\right)} = \det\left(L\right) \\ \Longrightarrow \quad & r = \frac{\Gamma\left(1+\frac{n}{2}\right)^{\frac{1}{n}}}{\sqrt{\pi}} \det(L)^{\frac{1}{n}} \\ \Longrightarrow \quad & \sigma\left(L\right) = \frac{\Gamma\left(1+\frac{n}{2}\right)^{\frac{1}{n}}}{\sqrt{\pi}} \det(L)^{\frac{1}{n}}. \end{aligned}$$

به‌طور مثال؛ برای $n = 6$، مقدار تقریبی $\sigma\left(L\right)$ برابر است با $0.5927 \det(L)^{\frac{1}{6}}$، درحالی‌که مقدار دقیق آن برابر است با $0.7605 \det(L)^{\frac{1}{6}}$؛ که باهم متفاوت‌اند. اما اگر $n = 100$، مقدار تقریبی $\sigma\left(L\right)$ برابر است با $2.4420 \det(L)^{\frac{1}{100}}$، درحالی‌که مقدار دقیق آن برابر است با $2.4900 \det(L)^{\frac{1}{100}}$؛ که تفاوت ناچیزی دارند.

۴.۱ پایه‌های مطلوب در مشبکه

برای شروع؛ مشبکهٔ $L\left(v_1, v_2, \ldots, v_n\right)$ را به قسمی تجسم کنید که v_iها دوبه‌دو متعامد باشند. آنگاه مسئلهٔ SVP نه‌تنها دشوار نیست، بلکه بسیار ساده به جواب نهایی می‌رسد؛ زیرا اگر $v_1, v_2, \ldots, v_n$ دوبه‌دو متعامد باشند، برای هر مجموعهٔ ضرایب دلخواه $a_1, a_2, \ldots, a_n \in Z$، داریم

$$||a_1 v_1 + a_2 v_2 + \cdots + a_n v_n||^2 = a_1^2||v_1||^2 + a_2^2||v_2||^2 + \ldots a_n^2||v_n||^2.$$

با فرض اینکه برای هر $1 \leq j \leq n$؛ v_j کوتاه‌ترین بردار پایه باشد، خواهیم داشت

$$||a_1 v_1 + a_2 v_2 + \cdots + a_n v_n||^2 \geq ||v_j||^2 \left(a_1^2 + a_2^2 + \cdots + a_n^2\right) \geq ||v_j||^2.$$

به‌عبارت‌دیگر؛ نرم هیچ ترکیب خطی از v_iها نمی‌تواند از نرم v_j کمتر باشد. اما ازآنجاکه در مورد مشبکه‌های با بعد بالا، دستیابی به پایه‌های کاملاً متعامد بعید است، هدف خود را به یافتن پایه‌های شبه‌متعامد و تاحدامکان کوتاه، تقلیل می‌دهیم. به بیانی دیگر؛ سعی بر افزایش مقدار نسبت هادامارد تا نزدیکی آن به ۱، داریم. زیرا دترمینان مشبکه، مقداری پایاست.

۵.۱ مفهوم کاهش مشبکه

اشاره کردیم که مشبکه و خصوصاً حل مسائلی مثل CVP و SVP به دلیل کاربرد بسیار گسترده در شاخه‌های مختلف علوم محض و کاربردی، برای بیش از ۱۵۰ سال، مورد توجه ریاضیدانان بوده و با کارهای «مینکوفسکی» و «هرمیت» در ابتدای قرن بیستم به اوج بالندگی رسید. با ظهور کامپیوترها به‌عنوان ابزارهای سریع محاسبات، جستجو به دنبال الگوریتم‌هایی که لااقل بتواند تقریبی (حتی نه‌چندان خوب) از کوتاه‌ترین یا نزدیک‌ترین بردار یک مشبکه با پایه‌های مفروض به دست بیاورد در دستور کار بسیاری از پژوهشگران قرار گرفت. الگوریتم‌هایی که قادر به ارائهٔ پایه‌های مطلوب برای مشبکه باشند. تا اینکه در سال ۱۹۸۲ برادران «لنسترا»[1] به همراه نابغهٔ مجارستانی «لواش»[2]، چنین الگوریتمی را معروف به **الگوریتم LLL** ارائه کردند [۲۱]؛ الگوریتمی که بعداً مشخص شد که به‌طرز عجیب و ناشناخته‌ای بهتر از کرانی که برای آن اثبات شده عمل می‌کند.

۱.۵.۱ الگوریتم LLL

کاری که ابداع‌کنندگان الگوریتم LLL انجام دادند، تعریف هوشمندانه‌ای از پایه‌های کاهش‌یافته[3] و ارائهٔ الگوریتمی کارآمد با زمان چندجمله‌ای برای محاسبهٔ چنین پایه‌هایی بود.

[1] Lenstra
[2] Lov'asz
[3] Reduced Basis

تعریف ۲۳.۱ (پایهٔ کاهش‌یافتهٔ LLL). در یک مشبکه، پایه‌های کاهش‌یافتهٔ LLL، پایه‌هایی تقریباً متعامد، همراه با بردارهایی با نرم نسبتاً کوچک هستند؛ فرض کنید $\{v_1, v_2, \ldots, v_n\}$ پایهٔ مشبکهٔ L و $\{v_1^*, v_2^*, \ldots, v_n^*\}$ پایهٔ متعامد متناظر آن (به‌دست‌آمده از الگوریتم گرام-اشمیت) باشد. در اینجا پایهٔ کاهش‌یافتهٔ $\{v_1, v_2, \ldots, v_n\}$ از یک مشبکه مثل L، با شرایط زیر تعریف می‌شود.

۱-شرط اندازه) باید برای هر $1 \leq j < i \leq n$ داشته باشیم $\left|\frac{\langle v_i, v_j^* \rangle}{||v_j^*||^2}\right| \leq \frac{1}{2}$ و این یعنی در فرآیند گرام-اشمیت، $|\mu_{i,j}| \leq \frac{1}{2}$. به‌عبارت‌دیگر زاویهٔ هر بردار v_i با v_j^* قبل از خودش بیشتر از ۶۰ درجه است؛ زیرا شرط فوق معادل است با

$$2\left|\langle v_i, v_j^* \rangle\right| \leq ||v_j^*||^2.$$

بنابر تعریف v_j^* داریم

$$||v_j^*||^2 \leq ||v_j||\ ||v_j^*||,$$

اما ازآنجاکه v_jهای قبل از v_i به ترتیب اندازه مرتب شده‌اند، داریم

$$||v_j||\ ||v_j^*|| \leq ||v_i||\ ||v_j^*||,$$

درنتیجه

$$2\left|\langle v_i, v_j^* \rangle\right| \leq ||v_i||\ ||v_j^*||\ .$$

۲- شرط لواش) باید برای هر $1 \leq i \leq n$ داشته باشیم $||v_i^*||^2 \geq \left(\frac{3}{4} - \mu_{i,j-1}^2\right) ||v_{i-1}^*||^2$.

حال به شرط الگوریتم LLL می‌پردازیم؛ این الگوریتم، بردارهای پایه و نامتعامد $\{v_1, v_2, \ldots, v_n\}$ را به‌عنوان ورودی از مشبکهٔ L گرفته و پایه‌های جدید $\{v_1', v_2', \ldots, v_n'\}$ را به قسمی تولید می‌کند که

۱. $Span\left(\{v_1, v_2, \ldots, v_n\}\right) = Span\left(\{v_1', v_2', \ldots, v_n'\}\right)$

۲. v_i'ها در هر دو شرط **اندازه** و **لواش** صدق کنند.

```
[1]   Input a basis {v_1, ..., v_n} for a lattice L
[2]   Set k = 2
[3]   Set v_1* = v_1
[4]   Loop while k ≤ n
[5]       Loop j = 1, 2, 3, ..., k − 1
[6]           Set v_k = v_k − ⌊μ_{k,j}⌉ v_j*  [Size Reduction]
[7]       End j Loop
[8]       If ||v_k*||^2 ≥ (3/4 − μ_{k,k−1}^2) ||v_{k−1}*||^2  [Lov'asz Condition]
[9]           Set k = k + 1
[10]      Else
[11]          Swap v_{k−1} and v_k  [Swap Step]
[12]          Set k = max(k − 1, 2)
[13]      End If
[14]  End k Loop
[15]  Return LLL reduced basis {v_1, ..., v_n}
```

Note: At each step, $v_1^*, \ldots, v_k^*$ is the orthogonal set of vectors obtained by applying Gram-Schmidt to the current values of $v_1, \ldots, v_k$ and $\mu_{i,j}$ is the associated quantity $\left(v_i\ .v_j^*\right) / \left|\left|v_j^*\right|\right|^2$.

۶.۱ سامانه‌های رمزنگاری نامتقارن مبتنی بر مشبکه

در خلال سال‌های ۶۱۹۹ تا ۱۹۹۸، با اثبات آن‌که حل مسائل SVP و CVP در مشبکه‌های تصادفی مسائلی مشکل هستند، روزنهٔ امیدی برای پیاده‌سازی سامانه‌های رمزنگاری نامتقارن جدید و مبتنی بر دشواری حل این مسائل در مشبکه گشوده شد. از بین سامانه‌های رمزنگاری کلید عمومی مبتنی بر مشبکه، سامانهٔ NTRU، که رسماً در سال ۱۹۹۸ معرفی شد [۱۹] توانست نهایتاً با اصلاحات زیاد اعتماد عمومی را جلب کرده و پس از استانداردسازی با عنوان IEEE P1363.1، به صنعت راه پیدا کند [۲۸]. سامانهٔ رمز NTRU را می‌توان اولین سامانهٔ عملی دانست که امنیت خود را بر اساس حل مسئلهٔ SVP می‌داند. در مقایسه با سامانه‌های رمزی شناخته‌شده‌ای مثل RSA یا ECC، بزرگ‌ترین مزیت این سامانهٔ رمز سرعت بسیار بالا و هزینه پیاده‌سازی پایین است. چراکه در این سامانه، عملیات محاسباتی با پیچیدگی $O(N)^{۲}$ انجام می‌گیرد و N حداکثر ۹ بیتی است.

۱.۶.۱ سامانهٔ رمزی NTRU

سامانهٔ رمزنگاری کلید عمومی NTRU برای اولین بار به‌طور غیررسمی در خلال نشست‌های جانبی اجلاس Crypto96، توسط ریاضیدان‌هایی از دانشگاه براون به نام‌های هافشتین[۱]، ژیل پایفر[۲] و جوزف سیلورمن[۳] معرفی و دو سال بعد جزییات آن به‌صورت رسمی در [۱۹] منتشر شد. در خلال یک دهه، علی‌رغم حملات مؤثری که علیه NTRU طراحی شد، تمامی این حملات با اصلاحات جزئی خنثی شدند. درحال‌حاضر هستهٔ NTRU نفوذناپذیر تلقی می‌شود. در اردیبهشت‌ماه سال ۱۳۸۸، IEEE نیز اولین نسخهٔ این سامانهٔ رمزنگاری کلید عمومی را با شناسه P1363.1 استانداردسازی و منتشر نمود که این خود دلیلی بر اعتماد عمومی و استقبال صنعت از این سامانهٔ سریع و بهینه است. اخیراً شرکت‌هایی مثل Intel، Cisco، Motorola، NXP، Sony و IBM در به‌کارگیری این الگوریتم در محصولات خود با شرکتی به همین نام (Ntru: Security Innovation)، همکاری خود را آغاز کرده‌اند.

۲.۶.۱ نمادها و عملگرها

عملیات پایه در سامانهٔ رمز NTRU، در حلقهٔ $R = \frac{Z[x]}{x^N - ۱}$ انجام می‌گیرد که در آن N عددی اول است. R شامل چندجمله‌ای‌هایی با درجهٔ $N - ۱$ است که ضرایب صحیح هستند. همچنین حلقه‌های چندجمله‌ای $R_p = \frac{Z_p[x]}{x^N - ۱}$ و $R_q = \frac{Z_q[x]}{x^N - ۱}$ که چندجمله‌ای‌هایی از درجهٔ $N - ۱$ با ضرایب صحیح به پیمانهٔ p و q، نیز در این سامانه مورد استفاده قرار می‌گیرند. اعداد p و q نسبت به هم اولند و q بسیار بزرگ‌تر از p است (به‌طور معمول $p = ۳$).

تعریف ۲۴.۱. برای هر عدد صحیح مثبت $d_۱$، $d_۲$، $\Gamma(d_۱, d_۲)$ را تعریف می‌کنیم؛ تمام چندجمله‌ای‌های متعلق به حلقهٔ R که دارای $d_۱$ ضریب ۱ و $d_۲$ ضریب -۱ است و بقیهٔ ضرایب صفر هستند. به این‌چنین چندجمله‌ای، چندجمله‌ای سه‌گانه گویند.

تعریف ۲۵.۱. فرض کنید a و b دو چندجمله‌ای از درجهٔ $N - ۱$ باشند، به‌طوری‌که

$$a = \sum_{j=۰}^{N-۱} a_j x^j \ , \quad b = \sum_{j=۰}^{N-۱} b_j x^j.$$

تعریف می‌کنیم

$$c = a * b = \sum_{i=۰}^{N-۱} c_i x^i; \quad c_i = \sum_{j=۰}^{N-۱} a_j b_{i-j}.$$

تعریف ۲۶.۱. فرض کنید a و b دو چندجمله‌ای از درجهٔ $N - ۱$ باشند، (a, b) را برداری $۲N$تایی تعریف می‌کنیم که N درایهٔ اول آن ضرایب چندجمله‌ای a و N درایهٔ دوم ضرایب چندجمله‌ای b باشد.

۳.۶.۱ عملکرد سامانهٔ NTRU

بر اساس تعاریف قسمت قبل، سامانهٔ NTRU را می‌توان به‌صورت زیر توصیف نمود:

[1] J. Hoffstein
[2] J. Pipher
[3] J. Silverman

- **کلید خصوصی:** دو چندجمله‌ای $f \in \Gamma(d_f, d_f - ۱)$ و $g \in \Gamma(d_g, d_g)$ به‌صورت تصادفی تولید می‌شوند. پس از انتخاب f و g، با استفاده از **الگوریتم تعمیم‌یافتهٔ اقلیدسی**، وارون f روی حلقه‌های R_p و R_q محاسبه شده و به‌ترتیب F_p و F_q نامیده می‌شوند. احتمال آن‌که چندجمله‌ای f روی این حلقه‌ها وارون‌پذیر باشد، بسیار بالا است. اما در غیر این صورت می‌توان چندجمله‌ای f جدیدی تولید کرد.

- **کلید عمومی:** کلید عمومی سامانهٔ NTRU، چندجمله‌ای h است که به‌صورت زیر محاسبه می‌شود

$$h = F_q * g \ (mod\, q)\,.$$

لازم به ذکر است که مقادیر d_g، d_f، q، p، N و d_r نیز به‌صورت عمومی منتشر می‌شوند. (مقدار d_r در قسمت رمزنگاری به کار می‌رود.)

- **رمزنگاری:** در فرایند رمزنگاری، سامانهٔ رمز ابتدا یک چندجمله‌ای تصادفی $r \in \Gamma(d_r, d_r)$ انتخاب کرده و پیام ورودی را در قالب یک چندجمله‌ای $m \in R$ با ضرایبی بین $\frac{p}{۲}$ و $-\frac{p}{۲}$ تبدیل می‌کند. متن رمزشده به‌صورت زیر محاسبه و ارسال می‌شود

$$e = p.h * r + m \ (mod\, q)\,.$$

- **رمزگشایی:** گیرنده برای محاسبهٔ چندجمله‌ای m، با در اختیار داشتن چندجمله‌ای e به‌صورت زیر عمل می‌کند

$$f * e = f * (p.h * r + m) \ (mod\, q) \Longrightarrow f * e = p.f * h * r + f * m \ (mod\, q)\,.$$

با جایگذاری h خواهیم داشت

$$e * f = p.f * F_q * g * r + f * m \ (mod\, q)$$

$$\Longrightarrow f * e = p.g * r + f * m \ (mod\, q)\,.$$

ازآنجاکه چندجمله‌ای‌های r، g، f و m دارای ضرایب کوچک هستند و همچنین مقدار p می‌توان مطمئن بود که ضرایب چندجمله‌ای فوق در بازه $\left[-\frac{q}{۲}, \frac{q}{۲}\right)$ واقع می‌شوند (احتمال عدم وقوع این پیشامد برای سامانه‌ای با پارامترهای $d_r = ۱۸$، $d_g = ۲۰$، $d_f = ۶۱$، $q = ۱۲۸$، $P = ۳$، $N = ۱۶۷$ چیزی نزدیک به $۱۰^{-۵}$ است). پس داریم

$$f * g = p.g * r + f * m.$$

در ادامه؛ گیرنده مقدار $f * e * F_p \ (mod\, p)$ را محاسبه می‌کند

$$\begin{aligned} f * e * F_p = p.g * r * F_p + m * f * F_p \ (mod\, p) \\ \Longrightarrow \ f * e * F_p = m * f * F_p \ (mod\, p) \\ \Longrightarrow \ f * e * F_p = m \ (mod\, p)\,. \end{aligned}$$

اما می‌دانیم ضرایب چندجمله‌ای m بین $-\frac{p}{۲}$ و $\frac{p}{۲}$ قرار دارند؛ پس نتیجه می‌شود

$$f * e * F_p = m.$$

۴.۶.۱ مشبکه و امنیت سامانهٔ NTRU

بنابر آنچه گفته شد؛ به‌منظور حمله بر سامانهٔ رمزی NTRU، می‌بایست با استفاده از کلید عمومی h، کلیدهای خصوصی f و g را به دست آورد. به‌عبارت‌دیگر؛ یافتن بردار (f, g) هدف حمله‌کننده به این سامانه است. نشان خواهیم داد؛ سامانهٔ رمزی NTRU، سامانهٔ مبتنی بر مشبکه بوده و حمله به این سامانه، معادل با حل مسئلهٔ SVP است. می‌توان کلید عمومی h را به‌صورت چندجمله‌ای

$h(x) = h_0 + h_1 x + \dots h_{N-1} x^{N-1}$ در نظر گرفت. مشبکهٔ منتسب به h را با L_h^{NTRU} نمایش داده که توسط ماتریس

$$M_h^{NTRU} = \begin{pmatrix} 1 & 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & 1 & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & 1 & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & q & \dots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & q \end{pmatrix}_{2N \times 2N}$$

تولید می‌شود.

گزاره ۲۷.۱. با فرض اینکه $f(x) * h(x) = g(x) \, (mod\, q)$، $u(x)$ متعلق به R موجود است که $f(x) * h(x) = g(x) + qu(x)$ آنگاه $M_h^{NTRU} = (f, g)$. $(f, -u)$.

اثبات. با توجه به تعریف ماتریس M_h^{NTRU} و تساوی $f(x) * h(x) = g(x) + qu(x)$ حکم ثابت می‌شود. □

نتیجه ۲۸.۱. بردار (f, g) متعلق به مشبکهٔ L_h^{NTRU} است.

گزاره ۲۹.۱. فرض کنید (N, p, q, d_f, d_g, d_r) پارامترهای سامانهٔ رمزی $NTRU$ باشد و

$$d_f = d_g = d_r = \frac{N}{3},\ q \approx 2N,$$

آنگاه (f, g) برداری کوتاه در مشبکهٔ L_h^{NTRU} خواهد بود.

اثبات. با توجه به آن‌که $f \in \Gamma(d_f, d_f - 1)$ و $g \in \Gamma(d_g, d_g)$، داریم

$$||(f, g)|| \approx \sqrt{2d_f + 2d_g} = \sqrt{\frac{4N}{3}}.$$

ازطرفی؛ شهود گوسی پیش‌بینی می‌کند که

$$\sigma(L) \approx \sqrt{\frac{N}{2\pi e}}$$

$$\Longrightarrow \frac{||(f, g)||}{\sigma(L)} \approx \frac{2/39}{\sqrt{N}}.$$

پس $||(f, g)||$ برای Nهای نسبتاً بزرگ بسیار کمتر از میانگین تخمین‌زده‌شده توسط شهود گوسی است. پس می‌توان نتیجه گرفت که بردار (f, g)، کوتاه‌ترین بردار در مشبکهٔ L_h^{NTRU} است. □

با در نظر گرفتن گزارهٔ فوق، می‌توان دریافت که سامانهٔ رمزنگاری کلید عمومی NTRU امنیت خود را از سختی مسئلهٔ SVP به عاریه گرفته است. در جدول ۲، می‌توان پارامترهای سامانهٔ NTRU را در سطوح مختلف امنیت مقایسه کرد. همچنین جدول ۳، پارامترهای این سامانه را به طور کامل معرفی می‌کند.

جدول ۱: سامانهٔ رمزنگاری NTRU

Public Parameter Creation	
A trusted party chooses public parameters (N, p, q, d) with N and p prime, $\gcd(p, q) = \gcd(N, q) = 1$, and $q > (6d+1)\,p$.	
Alice	Bob
Key Creation	
Choose private $f \in T(d+1, d)$ that is invertible in R_q and R_p. Choose private $g \in T(d, d)$. Compute F_q, the inverse of f in R_q. Compute F_p, the inverse of f in R_p. Publish the public key $h = F_q * g$.	
Encryption	
	Choose plaintext $m \in R_p$. Choose a random $r \in T(d, d)$. Use Alice's public key h to compute $e \equiv prh + m \pmod q$. Send ciphertext e to Alice.
Decryption	
Compute $f * e \equiv pg * r + f * m \pmod q$ Centerlift to $a \in R$ and compute $m \equiv F_p * a \pmod p$	

جدول ۲: پارامترهای سامانه NTRU در سطوح مختلف امنیت

	N	p	Q
امنیت پایین	۱۶۷	۳	۱۲۸
امنیت استاندارد	۲۵۱	۳	۱۲۸
امنیت بالا	۳۴۷	۳	۱۲۸
امنیت فوق بالا	۵۰۳	۳	۲۵۶

جدول ۳: پارامترهای سامانه NTRU

	N	p	q	d_f	d_g	d_r
NTRU167:3	۱۶۷	۳	۱۲۸	۶۱	۲۰	۱۸
NTRU251:3	۲۵۱	۳	۱۲۸	۵۰	۲۴	۱۶
NTRU503:3	۵۰۳	۳	۲۵۶	۲۱۶	۷۲	۵۵
NTRU167:2	۱۶۷	۲	۱۲۷	۴۵	۳۵	۱۸
NTRU251:2	۲۵۱	۲	۱۲۷	۳۵	۳۵	۲۲
NTRU503:2	۵۰۳	۲	۲۵۳	۱۵۵	۱۰۰	۶۵

۲ معرفی

مشبکه‌های NTRU دسته‌ای از مشبکه‌های دارای دریچه هستند که توسط [۱۹] به‌عنوان اساس طراحی الگوریتم رمزگذاری نامتقارن NTRUEncrypt معرفی شدند. برای یک چندجمله‌ای مونیک $\phi \in \mathbb{Z}[x]$ از درجهٔ n، مشبکه توسط دو چندجمله‌ای "کوتاه" f و g در مد ϕ ایجاد می‌شود. ضرایب f و g اعداد صحیح بسیار کوچکی هستند (در NTRUEncrypt، آن‌ها به $\{-۱, ۰, ۱\}$ محدود می‌شوند). چندجمله‌ای f و g مخفی هستند، اما نسبت بین آن‌ها

$$h = \frac{g}{f} \bmod \phi \bmod q \tag{۱.۲}$$

عدد صحیح کوچک q، مقداری عمومی و آشکار است. چندجمله‌ای f طوری انتخاب می‌شود که در مد ϕ و q معکوس‌پذیر باشد. Q لزوماً اول نیست. مشبکه‌های NTRU ویژگی‌های عملکردی خوبی را ارائه می‌دهند؛ آن‌ها در چندین طرح نامتقارن دیگر مورد استفادهٔ مجدد قرار گرفته‌اند. برخی از این طرح‌ها نیاز دارند که دریچهٔ مشبکه کامل باشد، به این معنی که فراتر از دانستن f و g، مالک کلید خصوصی باید دو چندجمله‌ای کوتاه دیگر F و G را نیز بداند که معادلهٔ NTRU زیر را تکمیل می‌کنند:

$$fG - gF = q \tag{۲.۲}$$

به‌عنوان مثال در طرح امضا NTRUSign [۱۸]، یک طرح رمزگذاری مبتنی بر هویت [۱۰]، طرح امضا Falcon [۱۳] و طرح رمزگذاری مبتنی بر هویت سلسله مراتبی LATTE [۴] به یک دریچهٔ کامل NTRU نیاز است. یافتن کوتاه‌ترین راه‌حل (برای یک نرم داده‌شده) مسئله‌ای سخت است. بااین‌حال، محاسبهٔ راه‌حلی که برای اجرای یک الگوریتم بر اساس مشبکه‌های کامل NTRU به اندازهٔ کافی کوتاه باشد، امکان‌پذیر است. به‌این‌ترتیب حل معادلهٔ NTRU بخشی از فرآیند تولید کلید محسوب می‌شود. درحالی‌که معادلهٔ NTRU ساده به نظر می‌رسد، حل آن به شیوه‌ای کارآمد مسئله‌ای بدیهی نیست. الگوریتم‌های موجود برای یافتن یک جواب [۱۸، ۲۶] در بعد n، به‌ترتیب دارای پیچیدگی زمانی و حافظهٔ حداقل از درجهٔ سه و دو هستند. برای اندازهٔ پارامترهای متداول، این در عمل یعنی نیاز به چندین مگابایت RAM که در یک کامپیوتر معمولی در حدود ۲ ثانیه زمان خواهد برد. این مانع از پیاده‌سازی در بسیاری از سامانه‌های محدود و تعبیه‌شده می‌شود. می‌توان استدلال کرد که توانایی پیاده‌سازی تولید کلید در یک دستگاه تعبیه شده چندان مهم نیست زیرا می‌توان آن را به‌صورت خارجی تولید کرد و کلید را در دستگاه کپی نمود، اما نگه‌داشتن کلید خصوصی در یک دستگاه مقاوم در برابر دست‌کاری برای چرخه عمر کامل آن اغلب برای امنیت و انطباق (به‌عنوان مثال با استاندارد FIPS 140-2 [۱۲]) مطلوب است. در این مقاله، نشان می‌دهیم که چگونه می‌توانیم از نرم میدان در حلقه‌های چندجمله‌ای، برای دستیابی به عملکردی بسیار بهبودیافته در حل معادلهٔ NTRU استفاده کنیم. این به ما اجازه می‌دهد تا دو الگوریتم جدید را برمبنای نرم میدان معرفی نماییم، که پیچیدگی (زمان و حافظه) بهتری را نسبت به الگوریتم‌های موجود با عوامل شبه‌خطی برحسب n (دقیقاً، حداقل $O(n/\log n)$) ارائه می‌دهد. به‌عنوان یک محصول جانبی، ما یک الگوریتم بهبودیافته را برای محاسبهٔ برآیندهای چندجمله‌ای، زمانی که یکی از چندجمله‌ای‌ها سیکلوتومیک باشد، توسعه دادیم. (به بخش ۳ مراجعه کنید). جدول ۴ پیچیدگی مجانبی به‌دست‌آمده توسط روش جدید ما را با روش‌های شناخته‌شدهٔ موجود مقایسه می‌کند. ما حل‌کنندهٔ کلاسیک NTRU مبتنی بر نتیجه و نیز الگوریتم جدید خود را، با بهینه‌سازی و ابزارهای مشابه پیاده‌سازی کردیم. این مسئله امکان اندازه‌گیری مستقیم ارتقای عملکرد روش ما را فراهم کرد، که تجزیه‌وتحلیل مجانبی را تائید نمود: برای یک درجهٔ معمولی ($n = ۱۰۲۴$)، روش جدید سریع‌تر و کوچک‌تر از الگوریتم‌های کلاسیک است، هر دو با یک ضریب ۱۰۰ یا بیشتر.

۱.۲ روش

الگوریتم ما به استفادهٔ مکرر از پارادایم تصویر-کن-سپس-بالا-ببر متکی است، یک پارادایم معروف در نظریهٔ اعداد الگوریتمی و تحلیل رمزی، که شامل تصویر کردن مسئله بر روی یک زیرمجموعه است که در آن آسان‌تر می‌شود، قبل از اینکه راه‌حل را به مجموعهٔ اصلی ببریم. ما بر استفاده از وجود برج‌های میدان و برج‌های حلقه تکیه می‌کنیم. به‌عنوان مثال، برج میدان‌های زیر را در نظر بگیریم:

$$\mathbb{K}_\ell / \mathbb{K}_{\ell-۱} / \ldots / \mathbb{K}_۱ / \mathbb{K}_۰ = \mathbb{Q}$$

که در آن $\forall i$ ، $\mathbb{K}_i = \mathbb{Q}[x] / \left(x^{۲^i}+۱\right)$ ، و برج حلقه‌های مرتبط (که حلقه‌هایی از اعداد صحیح از میدان‌های مربوطه هستند) با $n = ۲^\ell$:

$$\mathbb{Z}[x] / (x^n+۱) \not\supseteq \mathbb{Z}[x] / \left(x^{n/۲}+۱\right) \not\supseteq \cdots \supseteq \mathbb{Z}[x] / \left(x^۲+۱\right) \not\supseteq \mathbb{Z}.$$

می‌دانیم که نرم میدان می‌تواند هر عنصر $f \in \mathbb{Z}[x]/(x^n+1)$ را بر روی حلقهٔ کوچک‌تری از برج خود ترسیم کند. این واقعیت در حمله "NTRU بیش‌ازحد کشیده‌شده" [۱] مورد استفاده قرار می‌گیرد، جایی که مسائل به یک حلقهٔ کوچک‌تر نگاشته می‌شوند، سپس حل شده و جواب به حلقهٔ اصلی برمی‌گردد. بااین‌حال، چیزی که در این آثار مورد استفاده قرار نمی‌گیرد، این واقعیت است که نرم میدان با برج‌های میدان‌ها به‌خوبی بازی می‌کند: برای یک برج از توسعه‌های میدان $\mathbb{L}/\mathbb{K}/\mathbb{J}$ و $f \in \mathbb{L}$ ، داریم $\mathrm{N}_{\mathbb{K}/\mathbb{J}} \circ \mathrm{N}_{\mathbb{L}/\mathbb{K}}(f) = \mathrm{N}_{\mathbb{L}/\mathbb{J}}(f)$ (که در آن N نرم میدان را نشان می‌دهد). این واقعیت در قلب الگوریتم‌های ما قرار دارد. ما ابتدا به‌طور مکرر از نرم میدان برای تصویر کردن معادلاتی بر روی $\mathbb{Z}$ استفاده می‌کنیم که در اصل بر روی $\mathbb{Z}[x]/(x^n+1)$ تعریف شده‌اند؛ این مرحلهٔ نزول است. در این مرحله معلوم می‌شود که این معادلات را بر روی $\mathbb{Z}$ خیلی سریع‌تر می‌توان حل کرد. سپس از ویژگی‌های نرم میدان برای برگرداندن جواب‌هایمان به $\mathbb{Z}[x]/(x^n+1)$ استفاده می‌کنیم؛ این مرحلهٔ بلند کردن است. این اصل ساده به ما این امکان را می‌دهد که نسبت به الگوریتم‌های کلاسیک، حداقل از مرتبهٔ $\tilde{O}(n)$ بهبود به دست آوریم. ما چند ترفند مضاعف مانند تنبلی حافظه، استفاده از سامانه‌های اعداد باقیمانده، و یا این واقعیت که در میدان‌های سیکلوتومیک، مزدوج‌های گالوایی یک عنصر در نمایش FFT یا NTT، محاسبهٔ ساده و سرراستی دارد را نیز استفاده می‌کنیم. این روش‌ها پیاده‌سازی ما را سریع‌تر و از نظر حافظه کارآمدتر می‌کنند.

جدول ۴: مقایسهٔ روش جدید ما برای حل معادلهٔ NTRU با روش‌های موجود. B نشان‌دهندهٔ کران بالایی در $\log||f||$، $\log||g||$ است. تگ $[K]$ نشان می‌دهد که الگوریتم Karatsuba برای ضرب اعداد صحیح بزرگ استفاده شده است و $[SS]$ نشان می‌دهد که الگوریتم شونهاگ-استراسن استفاده شده است.

Method	Time complexity	Space complexity
Resultant [18]	$\tilde{O}(n(n2+B))$	$O(n2B)$
HNF [26]	$\tilde{O}(n3B)$	$O(n2B)$
TowerSolverR (Algorithm 4)	$O((nB)\log 2(3)\log n)$ $[K]$	$O(n(B+\log n)\log n)$
	$\tilde{O}(nB)$ $[SS]$	

۲.۲ کاربردها

الگوریتم‌های جدید ما حداقل چهار طرح مبتنی بر مشبکهٔ موجود را تحت تأثیر قرار می‌دهند.

NTRUSign. اولین طرحی که مستلزم حل این معادله در تولید کلید است، NTRUSign [۱۸] است. اگرچه در شکل فعلی، این طرح به دلایلی مستقل از تولید کلید، ناامن است.

Falcon. در طرح امضای فالکون [۱۳]، پرهزینه‌ترین بخش تولید کلید شامل حل یک معادلهٔ NTRU است. بدون روش‌های ما، برای داشتن بالاترین سطح امنیتی، در حدود ۲۳۳ کلاک پردازنده در یک لپ‌تاپ نسبتاً جدید و ۳ مگابایت حافظه نیاز است که این مسئله، کاربرد آن در دستگاه‌های تعبیه‌شده را محدود می‌کند. با توجه به اینکه ما ازلحاظ سرعت و حافظه، بهبودی از مرتبهٔ ۱۰۰ را به دست می‌آوریم، به‌طور قابل توجهی محدودهٔ دستگاه‌هایی را که می‌توان Falcon را به‌طور کامل روی آن‌ها پیاده‌سازی کرد، افزایش خواهیم داد.

DLP. مرحلهٔ راه‌اندازی طرح رمزگذاری مبتنی بر هویت DLP [۱۰] با تولید کلید فالکون یکسان است. بنابراین، آنچه در بالا ذکر شد اینجا نیز صادق است.

LATTE. اخیراً کمپبل و گرووز [۴] LATTE را معرفی کردند؛ یک طرح رمزگذاری مبتنی بر هویت سلسله مراتبی که اساساً [۱۰] را با ساختمان درختان بونسایِ [۵] ترکیب می‌کند. در هر استخراج یک کلید مخفی، LATTE باید یک معادلهٔ تعمیم‌یافتهٔ NTRU را حل کند. به‌طور دقیق‌تر، برای $f_1,\ldots,f_k \in \mathbb{Z}[x]/(\phi)$ این طرح نیاز دارد تا $F_1,\ldots,F_k \in \mathbb{Z}[x]/(\phi)$ را محاسبه نماید به‌طوری‌که:

$$\sum f_i F_i = q$$

و k ممکن است در عمل برابر با ۳ یا ۴ باشد (به [۴]، اسلاید ۲۳] مراجعه کنید). روش ما را می‌توان به‌سادگی برای حل این نوع معادله گسترش داد. تأثیر این روش‌ها بر روی LATTE حتی مهم‌تر از تأثیر آن‌ها روی طرح‌های فوق‌الذکر است، زیرا ممکن است یک مرجع نیاز به انجام استخراج‌های زیادی داشته باشد (معمولاً یک‌بار برای هر کاربر و برای هر دورهٔ تمدید کلید). برای اطلاع از مشخصات کامل‌تر LATTE به [۹] مراجعه نمایید.

الگوریتم‌های ما در تولید کلید طرح‌های دیگری همچون BAT [۱۴]، و مشتقات فالکون مانند ModFalcon [۷] و Mitaka [۱۱] مورد استفاده قرار گرفته‌اند.

۳.۲ کارهای مرتبط

معادلهٔ NTRU برای اولین بار در [۱۸] معرفی و حل شد.
روش دیگری برای حل معادلهٔ NTRU توسط Stehlé و Steinfeld [۲۶] با استفاده از فرم نرمال هرمیت پیشنهاد شد. کارآمدترین الگوریتم ازلحاظ فضا برای محاسبهٔ HNF مربوط به Miciancio و Warinschi است [۲۲]؛ بااین‌حال، مانند روش مبتنی بر نتایج، دارای پیچیدگی فضای درجهٔ دوم و پیچیدگی‌های زمانی شبه‌مکعبی / شبه-درجه-سه است و مشکل استفاده از RAM را حل نمی‌کند.
استفاده‌ای که ما از نرم میدان انجام می‌دهیم یادآور حمله "NTRU بیش‌ازحد کشیده‌شده" توسط [۱] است، با این تفاوت که این آثار، تحلیل رمزنگاری بوده و تنها یک‌بار از نرم میدان استفاده می‌کنند، درحالی‌که در کار ما به‌طور مکرر از آن استفاده می‌شود و ساختارهای رمزنگاری را بهبود می‌بخشد.

۴.۲ نقشهٔ راه

در بخش ۲، نمادها را معرفی می‌کنیم و الگوریتم کلاسیک مبتنی-بر-نتیجه را یادآوری می‌کنیم؛ ما همچنین برخی از ابزارهای ریاضی شناخته‌شده را که در الگوریتم جدید خود استفاده خواهیم کرد، توضیح می‌دهیم. در بخش ۳، یک روش جدید برای محاسبهٔ موارد خاص از نتایج را ارائه می‌کنیم؛ الگوریتم جدید ما مبتنی بر این روش بوده و در بخش ۴ توضیح داده شده است، همچنین نشان می‌دهیم که چگونه می‌توان آن را به‌عنوان یک بهینه‌سازی الگوریتم کلاسیک مبتنی-بر-نتیجه مشاهده کرد. مسائل پیاده‌سازی در بخش ۵ مورد بحث قرار گرفته‌اند.

۳ مقدمات

حلقهٔ اعداد صحیح و میدان‌های اعداد گویا، حقیقی و مختلط را با $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ نشان می‌دهیم. برای $a>0, b>1$، ما لگاریتم a در مبنای b را با $\log_b a$ نشان می‌دهیم، و قرارداد می‌کنیم $\log a=\log_2 a$. برای عدد صحیح $r>0$، حلقهٔ اعداد صحیح به پیمانهٔ r را با $\mathbb{Z}_r$ نشان می‌دهیم.

۱.۳ حلقه‌ها و میدان‌های چندجمله‌ای

فرض کنید $\mathbb{Z}[x]$ حلقهٔ چندجمله‌ای‌ها با ضرایب صحیح باشد (ازاین‌پس آن‌ها را چندجمله‌ای‌های انتگرالی خواهیم نامید). فرض کنید ϕ یک چندجمله‌ای انتگرالی مونیک غیرصفر از درجهٔ $n\geq 1$ باشد (یعنی $\phi=x^n+\sum_{i=0}^{n-1}\phi_i x^i$). تقسیم اقلیدسی هر چندجمله‌ای انتگرالی بر ϕ به‌خوبی تعریف شده است و باقیمانده‌ای یکتا از درجهٔ کمتر از n را خواهد داد؛ بنابراین می‌توانیم $\mathbb{Z}[x]/(\phi)$، حلقهٔ چندجمله‌ای‌های انتگرالی به پیمانهٔ ϕ را تعریف کنیم. به‌طور مشابه، ما $\mathbb{Z}_r[x]/(\phi)$ و $\mathbb{Q}[x]/(\phi)$,$\mathbb{C}[x]/(\phi)$ را تعریف می‌کنیم. وقتی ϕ در $\mathbb{Z}[x]$ تحویل‌ناپذیر باشد، در $\mathbb{Q}[x]$ نیز تحویل‌ناپذیر بوده و $\mathbb{Q}[x]/(\phi)$ یک میدان است. در این مقاله، روی چندجمله‌ای‌های به پیمانهٔ ϕ که در $\mathbb{Q}[x]$ تحویل‌ناپذیر هستند کار خواهیم کرد؛ اما در حالت کلی، $\mathbb{C}[x]/(\phi)$ و $\mathbb{Z}_r[x]/(\phi)$ میدان نیستند.

۲.۳ ماتریس‌ها و بردارها

درحالی‌که هدف استفاده از حلقه‌های چندجمله‌ای برای نشان دادن مشبکه‌ها، اجتناب از محاسبات مربوط به ماتریس‌ها و بردارها است، ما همچنان از چنین اشیاء جبری در برخی برهان‌ها استفاده خواهیم کرد. ماتریس‌ها را با حروف بزرگ پررنگ (مثلاً $\mathbf{B}$) و بردارها را با حروف کوچک پررنگ (مثلاً $\mathbf{v}$) نشان خواهیم داد. ما بردارها را به‌صورت ردیفی نمایش می‌دهیم. p-نرم یک بردار v را با $\|\mathbf{v}\|_p$ نشان می‌دهیم و طبق قرارداد، $\|\mathbf{v}\|=\|\mathbf{v}\|_2$. یادآوری می‌کنیم که برای $\mathbf{v}\in\mathbb{C}^n$ و $0<r\leq p\leq\infty$، و با قرارداد کردن اینکه $1/\infty=0$ داریم:

$$\|\mathbf{v}\|_p\leq\|\mathbf{v}\|_r\leq n^{\left(\frac{1}{r}-\frac{1}{p}\right)}\|\mathbf{v}\|_p \tag{۱.۳}$$

برای یک چندجمله‌ای $f \in \mathbb{C}[x]/(\phi)$، که در آن ϕ یک چندجمله‌ای مونیک از درجهٔ n است، $\mathcal{C}_\phi(f)$ ماتریسی $n \times n$ را نشان می‌دهد که ردیف jام آن از ضرایب $x^{j-1} f \bmod \phi$ تشکیل شده است:

$$\mathcal{C}_\phi(f) = \begin{bmatrix} f \bmod \phi \\ xf \bmod \phi \\ \cdots \\ x^{n-1} f \bmod \phi \end{bmatrix} \tag{۲.۳}$$

هنگامی‌که ϕ از زمینهٔ بحث مشخص باشد، ما این ماتریس را به‌صورت ساده با $\mathcal{C}(f)$ نمایش می‌دهیم. می‌توان بررسی کرد که وقتی $\phi = x^n + 1$، ماتریس $\mathcal{C}_\phi(f)$ یک ماتریس چرخشی است. عملگر $f \in \mathbb{C}[x]/(\phi) \mapsto \mathcal{C}(f)$ یک هم‌ریختی حلقه بر روی تصویرش است. به‌طور خاص، برای همهٔ $f, g \in \mathbb{C}[x]/(\phi)$، داریم:

$$\begin{aligned} \mathcal{C}(f+g) &= \mathcal{C}(f) + \mathcal{C}(g) \\ \mathcal{C}(fg) &= \mathcal{C}(f)\,\mathcal{C}(g) \end{aligned} \tag{۳.۳}$$

۳.۳ ضرب سریع اعداد صحیح

روش‌های ما، زمانی که برای حل معادلهٔ NTRU به کار می‌روند، مستلزم استفاده از اعداد صحیح بزرگ هستند. هزینه‌های محاسباتی مجانبی، به پیچیدگی زمانی ضرب دو عدد صحیح بزرگ بستگی دارد. هنگامی‌که اندازهٔ بیتی این دو عدد صحیح با b محدود شود، آن پیچیدگی را با $\mathcal{M}(b)$ نشان می‌دهیم:

- اگر از الگوریتم Karatsuba استفاده کنیم، $\mathcal{M}(b) = O\left(b^{\log_2(3)}\right) \approx O\left(b^{1.585}\right)$؛
- با الگوریتم شونهاگ-استراسن [۲۴]، $\mathcal{M}(b) = \Theta(b \cdot \log b \cdot \log\log b)$.

الگوریتم کاراتسوبا برای مقادیر «کوچک» b کارآمدتر است، درحالی‌که شونهاگ-استراسن به‌طور مجانبی بهتر است. هنگام ارائهٔ پیچیدگی‌های زمانی برای الگوریتم‌های ارتقاءیافتهٔ خود، هر دو روش را در نظر می‌گیریم. باید توجه داشت که پیچیدگی مجانبی، فقط برای پارامترهای "به‌اندازهٔ کافی بزرگ" تخمین معقولی از عملکرد را به دست می‌دهد. در پیاده‌سازی‌های خود متوجه شدیم که برای پارامترهای معمولی (درجهٔ n حداکثر تا ۱۰۲۴)، گلوگاه عملکردی، ضرب عدد صحیح نیست، بلکه کاهش Babai است که مستلزم انجام عملیات اعشاری است.

۴.۳ چندجمله‌ای‌های سیکلوتومیک

اکثر الگوریتم‌های رمزنگاری مبتنی بر مشبکه که از حلقه‌های چندجمله‌ای برای نمایش مشبکه‌های ساختاریافته استفاده می‌کنند، به چندجمله‌ای‌های سیکلوتومیک متکی هستند (البته به‌استثنای برخی موارد قابل توجه مانند [۳، ۲۵]). چندجمله‌ای‌های سیکلوتومیک دارای برخی ویژگی‌ها هستند که آن‌ها را برای استفاده از نرم میدان ایده‌آل می‌کند.

تعریف ۱.۳. برای یک عدد صحیح $m \geq 1$، m-امین چندجمله‌ای سیکلوتومیک به‌صورت زیر است:

$$\Phi_m = \prod_{\substack{0 < k < m \\ \gcd(k,m) = 1}} \left(x - e^{2i\pi(k/m)}\right) \tag{۴.۳}$$

چندجمله‌ای‌های سیکلوتومیک دارای ویژگی‌های شناخته‌شدهٔ زیر هستند:

- آن‌ها در $\mathbb{Z}[x]$ بوده و در $\mathbb{Q}[x]$ تحویل‌ناپذیر هستند.
- درجهٔ Φ_m، $\varphi(m)$ است، که φ تابع اویلر را نشان می‌دهد: $\varphi(m) = |\mathbb{Z}_m^\times|$.
- اگر $n = 2^\ell$، آنگاه $\Phi_{2n} = x^n + 1$.

- اگر p یک عامل اول m باشد، آنگاه:

$$\Phi_{\mathrm{mp}}\ (x)=\Phi_m\left(x^P\right) \tag{۵.۳}$$

ازآنجایی‌که چندجمله‌ای‌های سیکلوتومیک تحویل‌ناپذیر هستند، $\mathbb{Q}[x]/\left(\Phi_m\right)$ برای همهٔ $m\geq ۱$ یک میدان است؛ ما آن‌ها را میدان‌های سیکلوتومیک می‌نامیم.

۵.۳ نرم میدان

نرم میدان ابزار اصلی‌ای است که ما در الگوریتم‌های خود استفاده می‌کنیم، و همین دلیل کارایی آن‌ها است. در این بخش، ما تعریف و همچنین چند ویژگی آن را یادآوری می‌کنیم.

تعریف ۲.۳ (نرم میدان). فرض کنید $\mathbb{K}$ یک میدان عددی باشد، و $\mathbb{L}$ یک توسیع گالوایی از $\mathbb{K}$ باشد. گروه گالوایِ توسیع میدان $\mathbb{L}/\mathbb{K}$ را با $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ نشان می‌دهیم.
نرم میدان $\mathrm{N}_{\mathbb{L}/\mathbb{K}}:\mathbb{L}\to\mathbb{K}$ نگاشتی است که برای هر $f\in\mathbb{L}$ توسط حاصل‌ضرب مزدوج‌های گالوا f تعریف می‌شود:

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(f)=\prod_{\mathrm{g}\in\mathrm{Gal}(\mathbb{L}/\mathbb{K})}\mathrm{g}(f) \tag{۶.۳}$$

به‌طور معادل، $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(f)$ را می‌توان به‌عنوان دترمینان نگاشت $\mathbb{K}$-خطی $\psi_f:a\in\mathrm{L}\mapsto fa$ تعریف کرد.

از این تعریف مشخص است که نرم میدان یک مورفیسم ضربی است. علاوه‌بر این، نرم میدان با ترکیب سازگار است: برای یک برجِ توسیع‌های $\mathbb{L}/\mathbb{K}/\mathbb{J}$، رابطهٔ $\mathrm{N}_{\mathbb{L}/\mathbb{K}}\circ\mathrm{N}_{\mathbb{K}/\mathbb{J}}(f)=\mathrm{N}_{\mathbb{L}/\mathbb{J}}(f)$ برقرار است. برای اختصار، $\mathbb{K}$ و $\mathbb{L}$ را می‌توان زمانی که از متن بحث روشن باشد، از زیرنویس حذف نمود. به‌عنوان مثال، وقتی $f\in\mathbb{L}$ و $\mathbb{K}$ بزرگ‌ترین زیرمیدان سره و یکتای $\mathbb{L}$ است، آنگاه داریم $\mathrm{N}(f)=\mathrm{N}_{\mathbb{L}/\mathbb{K}}(f)$. به‌علاوه، اگر $f\in\mathbb{L}$ و $\mathbb{L}$ بر بالای یک برج میدان قرار بگیرد که از متن بحث مشخص باشد، آنگاه می‌توانیم i مرتبه ترکیب N را با $\mathrm{N}^i(f)$ نمایش دهیم. برای مثال، اگر برج میدان زیر را در نظر بگیریم:

$$\mathrm{Q}[x]/\left(x^n+۱\right)/\mathrm{Q}[x]/\left(x^{n/۲}+۱\right)/\ldots/\mathrm{Q}[x]/\left(x^۲+۱\right)/\mathbb{Q} \tag{۷.۳}$$

که در آن $n=۲^\ell$، آنگاه $\mathrm{N}^i(f)$ چندجمله‌ای $f\in\mathbb{Q}[x]/\left(x^n+۱\right)$ را به $\mathbb{Q}[x]/\left(x^{n/(۲^i)}+۱\right)$ می‌فرستد.
حالت توسیع‌های سیکلوتومیک. برای توسیع‌های سیکلوتومیک، نرم میدان را می‌توان به شکلی که برای ما راحت باشد بیان نمود. فرض کنید $m,n>۰$، اعدادی صحیح باشند به‌طوری‌که $n|m,\ \mathbb{L}=\mathbb{Q}[x]/\left(\Phi_m\right)$ و $\mathbb{K}=\mathbb{Q}[y]/\left(\Phi_n\right)$. مورفیسم $y\mapsto x^{m/n}$ یک توسیع میدان $\mathbb{L}/\mathbb{K}$ را تعریف می‌کند. سپس مزدوج‌های گالوای $\mathrm{g}_a(f)$ از $f\in\mathbb{L}$ به شکل:

$$\mathrm{g}_a(f)(x)=f\left(x^a\right) \tag{۸.۳}$$

خواهند بود؛ برای مجموعهٔ $a\in\mathbb{Z}_m$ که در رابطهٔ $a=۱\bmod n$ صادق باشند. این یک روش ساده و کارآمد برای محاسبهٔ نرم $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(f)=\prod_a\mathrm{g}_a(f)$ به‌ویژه در FFT یا NTT را ارائه می‌دهد. به‌ویژه در حالت خاصی که $n=۲^\ell$، $\mathbb{L}=\mathbb{Q}[x]/\left(\Phi_{۲n}\right)$ و $\mathbb{K}=\mathbb{Q}[y]/\left(\Phi_n\right)$، بیان نرم میدان بسیار ساده است. هر $f\in\mathbb{L}$ را می‌توان به ضرایبی از درجه‌های زوج و فرد تفکیک کرد:

$$f=f_e\left(x^۲\right)+xf_o\left(x^۲\right) \tag{۹.۳}$$

که در آن $f_o,f_e\in\mathbb{K}$. ازآنجاکه $\psi_f:a\in\mathbb{L}\mapsto fa$، داریم

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(f)=\det{}_{\mathbb{K}}\left(\psi_f\right)=\det\begin{bmatrix}f_e & f_o\\ yf_o & f_e\end{bmatrix}=f_e^۲-yf_o^۲ \tag{۱۰.۳}$$

۶.۳ تبدیل فوریهٔ سریع و تبدیل نظریهٔ اعدادی

تبدیل فوریهٔ سریع، و شکل دیگر آن یعنی تبدیل نظریهٔ اعدادی، ابزارهای قدرتمندی هستند که امکان محاسبات کارآمد را در حلقه‌های چندجمله‌ای فراهم می‌کنند. زمانی که عملوندها از نمایش FFT یا NTT استفاده می‌کنند، نرم میدان، به‌ویژه، می‌تواند بسیار ساده و سریع ارزیابی شود. بیشتر افزایش سرعت‌های به‌دست‌آمده توسط روش‌های ما، از تعامل بین نرم میدان و FFT/NTT حاصل می‌شود.

فرض کنید $\phi \in \mathbb{Q}[x]$ یک چندجمله‌ای مونیک از درجهٔ n، با n ریشهٔ متمایز $(\gamma_j)_{0 \le j < n}$ روی $\mathbb{C}$ باشد. برای $f \in \mathbb{C}[x]/(\phi)$، تبدیل فوریهٔ آن $\hat{f}$ به‌صورت زیر تعریف می‌شود:

$$\hat{f} = (f(\gamma_j))_{0 \le j < n} \tag{۱۱.۳}$$

تبدیل فوریه یک ایزومورفیسم بین $\mathbb{C}[x]/(\phi)$ و $\mathbb{C}^n$ است. بنابراین، برای $f, g \in \mathbb{C}[x]/(\phi)$، تبدیل فوریهٔ $f+g$ و fg را می‌توان به‌ترتیب با جمع و ضرب $\hat{f}$ و $\hat{g}$ محاسبه نمود.

تبدیل فوریهٔ سریع (یا FFT) یک الگوریتم شناخته‌شده برای محاسبهٔ تبدیل فوریهٔ f در حالت خاص $\phi = x^n + 1$ با $n = 2^\ell$ است [۱۵، ۸]. FFT دارای پیچیدگی زمانی $O(n \log n)$ عملیات در $\mathbb{C}$ است؛ تبدیل معکوس را نیز می‌توان با همین کارآمدی محاسبه کرد. به‌طور خاص، FFT امکان محاسبهٔ حاصل‌ضرب دو چندجمله‌ای به پیمانهٔ ϕ با پیچیدگی $O(n \log n)$ را فراهم می‌کند. FFT را می‌توان به پیمانه‌های دیگر، به‌ویژه چندجمله‌ای‌های سیکلوتومیک گسترش داد.

تبدیل نظریهٔ اعدادی (یا NTT)، آنالوگ تبدیل فوریه بر روی میدان متناهی $\mathbb{Z}_r$ برای یک عدد اول r است. تا زمانی که ϕ روی $\mathbb{Z}_r$ تقسیم شود، NTT خوش‌تعریف است؛ وقتی $\phi = x^n + 1$، کافی است داشته باشیم $r = 1 \bmod 2n$. مشابه حالت FFT، NTT را می‌توان در $O(n \log n)$ عملیات ابتدایی در $\mathbb{Z}_r$ برای برخی پیمانه‌ها، به‌ویژه چندجمله‌ای‌های سیکلوتومیک محاسبه کرد.

۷.۳ کاهش بابایی

قبل از اینکه نشان دهیم چگونه می‌توان معادلهٔ NTRU را حل کرد، آخرین ابزاری که نقش مهمی در این فرآیند بازی می‌کند را معرفی می‌کنیم: کاهش بابایی، یا بهتر است بگوییم تعمیمی از آن. این کاهش، یک جواب معادلهٔ NTRU را به جواب دیگری با چندجمله‌ای‌های کوتاه‌تر تبدیل می‌کند. ابتدا الحاق را تعریف می‌کنیم.

تعریف ۳.۳ (الحاق). فرض کنید $\phi \in \mathbb{Q}[x]$ مونیک با ریشه‌های متمایز (γ_j) روی $\mathbb{C}$ باشد. برای $f \in \mathbb{C}[x]/(\phi)$، ما الحاق آن f^* را به‌عنوان چندجمله‌ای منحصربه‌فردی در $\mathbb{C}[x]/(\phi)$ تعریف می‌کنیم که برای هر γ_j:

$$f^*(\gamma_j) = \overline{f(\gamma_j)} \tag{۱۲.۳}$$

که در آن $\overline{\cdot}$ نشان‌دهندهٔ مزدوج عدد مختلط است.

وجود و یکتایی به‌راحتی با توجه به این نکته به دست می‌آید که در نمایش FFT، محاسبهٔ الحاق، معادل جایگزینی هر ضریب فوریه با مزدوج آن است. اگر $f \in \mathbb{R}[x]/(\phi)$، آنگاه خواهیم داشت $f^* \in \mathbb{R}[x]/(\phi)$. در واقع، اگر γ ریشهٔ ϕ باشد، $\overline{\gamma}$ نیز ریشهٔ ϕ است، و $\overline{f(\gamma)} = f(\overline{\gamma})$. بنابراین، $f^*(\overline{\gamma}) = \overline{f^*(\gamma)}$ برای همهٔ ریشه‌های γ از ϕ. این خاصیت فقط با چندجمله‌ای‌های حقیقی به دست می‌آید، یعنی چندجمله‌ای‌هایی که ضرایب مختلط آن‌ها همهٔ اعداد حقیقی هستند. الحاق به ما امکان می‌دهد Reduce (الگوریتم ۱) را تعریف کنیم، که تعمیمی مستقیم از الگوریتم نزدیک‌ترین صفحه بابای [۲] بر روی $\mathbb{Z}[x]/(\phi)$-پیمانه‌ها است. برای ورودی‌های $f, g, F, G \in \mathbb{Z}[x]/(\phi)$، الگوریتم Reduce، F' و G' را با اندازه‌های نزدیک به حداقل محاسبه می‌کند به‌طوری‌که $fG - gF = fG' - gF'$. این نکته را ذکر می‌کنیم که گونه‌هایی از این الگوریتم قبلاً در کارهای قبلی ارائه شده‌اند، برای مثال [۱۸].

Algorithm 1 $Reduce_\phi(f, g, F, G)$

Require: $f, g, F, G \in \mathbb{Z}[x]/(\phi)$

Ensure: $F', G' \in \mathbb{Z}[x]/(\phi)$ such that $fG' - gF' = fG - gF \bmod \phi$

do

  $k \leftarrow \left\lfloor \frac{Ff^* + Gg^*}{ff^* + 9g^*} \right\rceil$

  $(F, G) \leftarrow (F - kf, G - kg)$

while $k \neq 0$

return F, G

ممکن است چند بار تکرار نیاز باشد، به‌خصوص اگر k با دقت کمی محاسبه شده باشد. در واقع، در عمل، ضرایب چندجمله‌ای‌های F, G می‌توانند قبل از کاهش، بسیار بزرگ باشند، و بنابراین محاسبهٔ k با دقت پایین (مثلاً با استفاده از مقادیر double در زبان برنامه‌نویسی C) نسبت به تقریب‌های ضرایب چندجمله‌ای کارآمدتر است: این امکانِ استفاده از نمایش FFT را فراهم می‌کند، جایی‌که ضرب‌های چندجمله‌ای و الحاق به‌راحتی محاسبه می‌شوند. سپس هر تکرار، یک مقدار تقریبی از k با ضرایب کوچک (با مقیاس‌بندی) را به دست می‌دهد. البته، استفاده از حساب اعشاری یعنی فرد ممکن است در یک حلقهٔ بی‌نهایت گیر بیافتد، اما این به‌راحتی با خروج از الگوریتم به‌محض توقف کاهش نرم (F, G) خنثی می‌شود.

به این نکته اشاره می‌کنیم که محاسبهٔ k، تقسیم چندجمله‌ای‌ها به پیمانهٔ ϕ را شامل می‌شود. در نمایش FFT، تقسیم به‌سادگی، عضوبه‌عضو اعمال می‌شود. ازآنجایی‌که ϕ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است، در اینجا هیچ تقسیم بر صفری رخ نمی‌دهد. بااین‌حال، در عمل، استفاده از مقادیر تقریبی با دقت پایین ممکن است (به‌ندرت) موقعیت‌هایی را به همراه داشته باشد که تقسیم بر صفر رخ دهد. همان‌طور که در بخش ۱.۵ توضیح داده خواهد شد، در تولید زوج کلید برای یک الگوریتم رمزنگاری، خطاهای گاه‌وبیگاه به‌راحتی قابل تحمل است. در این مقاله، ما از الگوریتم ۱ در چندجا استفاده می‌کنیم؛ هربار با چندجمله‌ای‌های f, g, F, G که در معادلهٔ NTRU (۲.۲) صدق می‌کنند. در این مورد، به‌طور غیررسمی، الگوریتم ۱ دو چندجمله‌ای F' و G' را به‌گونه‌ای محاسبه می‌کند که نرم (F', G') در حدود $O(\sqrt{n})$ بزرگ‌تر از (f, g) باشد.

۴ الگوریتم ارتقاءیافته برای حل معادلهٔ NTRU

این بخش روش و الگوریتم جدیدی را برای حل معادلهٔ NTRU ارائه می‌دهد (۲.۲). این الگوریتم از کاربرد بازگشتی نرم میدان در خود حل‌کنندهٔ NTRU کلاسیک ناشی می‌شود. ما ابتدا طرح کلی و شهود روش خود را در بخش ۱.۴ ارائه خواهیم کرد. در بخش ۲.۴، ما یک الگوریتم بازگشتی را بر اساس مشاهدات خود ارائه می‌دهیم، و در بخش ۳.۴، یک الگوریتم تکرارشوندهٔ کمی کندتر، اما از نظر حافظه کارآمدتر را معرفی می‌کنیم. در نهایت، در بخش ۴.۴، تحلیل‌هایی را برای زمان و حافظهٔ مورد نیاز الگوریتم ارائه خواهیم کرد.

۱.۴ طرح کلی

فرض کنید $m, p > 0$ اعداد صحیح باشند، $\mathbb{L}=\mathbb{Q}[x]/(\Phi_{pm})$, $\mathbb{K}=\mathbb{Q}[y]/(\Phi_m)$ و $\mathrm{N}=\mathrm{N}_{\mathbb{L}/\mathbb{K}}$. فرض کنید که یک عدد صحیح مفروض q و دو چندجمله‌ای $f, g \in \mathbb{Z}[x]/(\Phi_{pm})$ داشته باشیم، و می‌خواهیم $F, G \in \mathbb{Z}[x]/(\Phi_{pm})$ را پیدا کنیم به‌طوری‌که

$$fG - gF = q \tag{۱.۴}$$

از طرف دیگر، فرض کنید برای $\mathrm{N}(f), \mathrm{N}(g)$ که در حلقهٔ کوچک‌تر $\mathbb{Z}[y]/(\Phi_m)$ قرار دارند، می‌دانیم $F', G' \in \mathbb{Z}[y]/(\Phi_m)$ به‌گونه‌ای که:

$$\mathrm{N}(f)G' - \mathrm{N}(g)F' = q \tag{۲.۴}$$

ما ادعا می‌کنیم که می‌توانیم از راه‌حل‌های F', G' برای استنباط راه‌حل‌های F, G استفاده کنیم. در واقع، به یاد می‌آوریم که

$$N(f) = \prod_{g \in Gal(\mathbb{L}/\mathbb{K})} g(f) = ff^{\times}$$

که در آن $f^{\times} = \Pi_{\mathrm{g} \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \mathrm{g}(f)$ نشان‌دهندهٔ حاصل‌ضرب تمام مزدوج‌های گالوای f به‌جز خودش بوده، و ما یک برابری مشابه برای g نیز داریم. سپس

$$ff^{\times}G'(x^p) - gg^{\times}F'(x^p) = q \tag{۳.۴}$$

که یک برابری در حلقهٔ بزرگ‌تر $\mathbb{Z}[x]/(\Phi_{pm})$ است. از این معادلهٔ آخر، نتیجه می‌شود که $F = g^{\times}F'(x^p)$ و $G = f^{\times}G'(x^P)$ راه‌حل‌هایی معتبر برای معادلهٔ NTRU هستند. از این مشاهدات، اکنون می‌توانیم طرح کلی الگوریتم‌های خود را برای حل معادلهٔ NTRU ارائه دهیم:

(i) از نرم میدان برای تصویر کردن آن به یک زیرحلقهٔ کوچک‌تر استفاده کنید،

(ii) معادله را در حلقهٔ کوچک‌تر حل کنید،

(iii) برای صعود جواب‌ها به حلقهٔ اصلی.

بااین‌حال، و برخلاف حمله NTRU بیش‌ازحد کشیده‌شده [۱]، ما مراحل تصویر کردن و صعود را تنها یک‌بار انجام نمی‌دهیم، بلکه به‌طور مکرر آن‌ها را تکرار خواهیم کرد. به بیان دقیق‌تر:

- f, g را روی یک زیرحلقهٔ کوچک‌تر تصویر می‌کنیم تا زمانی که به حلقهٔ اعداد صحیح $\mathbb{Z}$ برسیم؛ ما آن را مرحلهٔ نزول می‌نامیم.
- هنگامی که جواب‌ها را در $\mathbb{Z}$ به دست آوریم، با صعود آن‌ها به‌طور مکرر تا رسیدن به حلقهٔ اصلی ادامه می‌دهیم؛ ما این را مرحلهٔ صعود می‌نامیم.

تصویر کردن‌ها و صعود مکرر، کلید کارایی الگوریتم ما هستند: یک‌بار اجرای آن‌ها فقط از مرتبهٔ $O(1)$ بهبود ایجاد می‌کند، اما نشان خواهیم داد که ازلحاظ نظری، تکرار آن‌ها اجازه می‌دهد تا از مرتبه‌های بزرگ‌تر از $\tilde{O}(n)$ بهبود به دست آوریم، و در عمل این بهبود برای یک مقدار معمولی $n = ۱۰۲۴$، از مرتبهٔ ۱۰۰ خواهد بود. روال اجرای دو الگوریتم ما در شکل ۱ خلاصه شده است. فاز نزول در ستون میانی، و فاز صعود در ستون سمت راست نشان داده شده است.

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/\left(x^n+1\right) & \ni & f, g & \rightarrow & F, G \\
\subsetneq & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/\left(x^{n/2}+1\right) & \ni & \mathrm{N}(f), \mathrm{N}(g) & \rightarrow & F^{[1]}, G^{[1]} \\
\subsetneq & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/\left(x^{n/4}+1\right) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & \rightarrow & F^{[2]}, G^{[2]} \\
\subsetneq & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\subsetneq & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^{\ell}(f), \mathrm{N}^{\ell}(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
$$

شکل ۱. طرح کلی الگوریتمهای ۴ و ۵ برای حل (۲).

۲.۴ یک الگوریتم بازگشتی

در حالت خاص $\phi = x^n + ۱$ با $n = ۲^{\ell}$، می‌توانیم این فرمول‌ها را با $p = ۲$ اعمال کنیم، و سپس این کار را به‌طور مکرر روی $\phi' = x^{n/۲} + ۱$ تکرار نماییم. با این کار TowerSolverR (الگوریتم ۲) به دست می‌آید.

Algorithm 2 $\mathrm{TowerSolverR}_{n,q}(f, g)$

Require: $f, g \in \mathbb{Z}[x]/(x^n + 1)$ with n a power of two
Ensure: Polynomials F, G such that (2.2) is verified

if $n = 1$ **then**
  Compute $u, v \in \mathbb{Z}$ such that $uf - vg = GCD(f, g)$
  if $\delta = GCD(f, g)$ is not a divisor of q **then**
    abort
  $(F, G) \leftarrow (vq/\delta, uq/\delta)$
  return (F, G)
else
  $f' \leftarrow N(f)$ ▷ $f', g', F', G' \in \mathbb{Z}[x]/\left(x^{n/2} + 1\right)$
  $g' \leftarrow N(g)$
  $(F', G') \leftarrow TowerSolverR_{\frac{n}{2},q}(f', g')$
  $F \leftarrow g^{\times}(x) F'\left(x^2\right)$ ▷ $F, G \in \mathbb{Z}[x]/(x^n+1)$
  $G \leftarrow f^{\times}(x) G'\left(x^2\right)$
  $Reduce(f, g, F, G)$
 return (F, G)

توضیح غیررسمی در مورد اینکه چرا الگوریتم TowerSolverR از فضای بسیار کمتری نسبت به حل‌کنندهٔ کلاسیک (ResultantSolver) استفاده می‌کند این است که در هر مرحلهٔ بازگشت، اندازهٔ هر یک از ضرایب تقریباً دو برابر می‌شود، اما درجه نصف می‌شود، بنابراین تنها به تعداد نصف ضرایب قبل، ضریب برای ذخیره وجود خواهد داشت. این الگوریتم بر کاهش بابای (Reduce) تکیه دارد تا ضرایب محاسبه‌شدهٔ جدید (F,G) را به اندازه‌ای مشابه ضرایب (f,g) برای این سطح بازگشتی بازگرداند. یک تحلیل رسمی پیچیدگی فضا در لم ۱.۵ ارائه شده است.

صحت. اگر الگوریتم یک جواب را خروجی دهد (خاتمه در زیر نشان داده شده است)، درستی الگوریتم ۲ فوراً نتیجه می‌شود. در واقع، صحت در عمیق‌ترین سطح بازگشتی واضح است، و اگر الگوریتم برای $(f,g)\in\mathbb{Z}[x]/\left(x^{n/2}+1\right)$ صحیح باشد، به ما اطمینان می‌دهد که برای $(f,g)\in\mathbb{Z}[x]/\left(x^{n}+1\right)$ نیز صحیح خواهد بود.

۵ تحلیل پیچیدگی

اکنون به‌طور تفصیلی پیچیدگی TowerSolverR را مطالعه می‌کنیم. برای سادگی، در نظر می‌گیریم که $q=1$: معادلهٔ NTRU برای $q>1$ به‌راحتی، ابتدا با حل آن برای $q=1$ و مقیاس کردن خروجی (F,G) با عامل q حل می‌شود.

لم ۱.۵ (تحلیل پیچیدگی فضا). فرض کنید $q=1$ و نرم‌های اقلیدسی f,g دارای کران باشند: $\log\|f\|,\log\|g\|\leq B$ همچنین می‌دانیم که $\ell=\log n$. در نهایت فرض کنید:

$$\beta=\left(\frac{f^\star}{ff^\star+gg^*},\frac{g^\star}{ff^\star+gg^*}\right) \tag{۱.۵}$$

اگر $\beta=O(n\|(f,g)\|)$، آنگاه الگوریتم ۲ (*TowerSolverR*) در فضای $O(n\ell(B+\ell))$ اجرا می‌شود.

اثبات. واضح است که ما برج بازگشتی زیر را داریم:

$$\text{TowerSolverR}_{n,q}(f,g)\to\text{TowerSolverR}_{n/2,q}(\,\mathrm{N}(f),\mathrm{N}(g))\to\ldots\text{TowerSolverR}_{1,q}\left(\,\mathrm{N}^\ell(f),\mathrm{N}^\ell(g)\right)\cdots\to$$

اکنون فضای مورد نیاز متغیرهای داخلی را محدود کردیم.

۱. از (۱.۳)، هر $\mathrm{N}^i(g)$، $O(n(B+\ell))$ بیت می‌گیرد.

۲. اکنون نرم (اقلیدسی) (F,G) را محدود کردیم. ابتدا نرم آن را پس از کاهش در نظر می‌گیریم. با توجه به $V=\mathrm{Span}((f,g))$، بردار (F,G) می‌تواند به‌طور منحصربه‌فرد بر روی $V\oplus V^\perp$ تجزیه شود:

$$(F,G)=\left(\tilde{F},\tilde{G}\right)+\left(\breve{F},\breve{G}\right)$$

که در آن $(\tilde{F},\tilde{G})\in V^\perp$ و $(\breve{F},\breve{G})\in V$.

- در [۱۰]، لم ۳] نشان داده شده است که $\|(\tilde{F},\tilde{G})\|=\beta$. با فرض، مشخص می‌شود که $\|(\tilde{F},\tilde{G})\|=O(n\|(f,g)\|)$.
- ما $\|(\tilde{F},\tilde{F}G)\|$ را محدود کردیم: پس از کاهش (F,G) با استفاده از الگوریتم ۱، نابرابری مثلث تضمین می‌کند که

$$\|(\breve{F},\breve{G})\|\leq n/2\|(f,g)\|.$$

نتیجه می‌شود که

$$\|\,(F,G)\,\|^2=\|(\tilde{F},\tilde{G})\|^2+\|(\breve{F},\breve{G})\|^2=O\left(n^2\|\,(f,g)\,\|^2\right) \tag{۲.۵}$$

و بنابراین (F,G) را می‌توان در فضای $O(n(B+\ell))$ ذخیره کرد. البته، ما همچنین باید (F,G) را زمانی که از $F',G',f^\times,g^\times$ محاسبه می‌شود و هنوز کاهش نیافته است، کنترل کنیم. بنابراین خواهیم داشت:

$$\|F\|\leq\sqrt{\frac{n}{2}}\,\|F'\|\,\|g\|\quad\text{and}\quad\|G\|\leq\sqrt{\frac{n}{2}}\,\|G'\|\,\|f\|.$$

□

دربارهٔ لم۳. نسخهٔ قبلی این اثر نسخه‌ای از لم ۱.۵ را ارائه کرد که به شرط $\beta=\|(\tilde{F},\tilde{G})\|$ نیازی نداشت. بااین‌حال، اثبات، حاوی کران بالایی اشتباه برای β بود. این نسخهٔ به‌روزشده با اضافه کردن شرط $\beta=O(n\|(f,g)\|)$ این مورد را تصحیح می‌کند. این اثبات را تمام می‌کند و همچنین آن را بسیار ساده‌تر می‌کند. نقطهٔ ضعف آشکار این است که گزارهٔ اثبات‌شده کلیت کمتری دارد. بااین‌حال، این محدودیت را می‌توان به‌طور پیشگیرانه بررسی کرد که امکان نمونه‌گیری مجدد (f,g) را در زمانی که اجازه داریم، می‌دهد. یک استدلال ابتکاری در [۱۰] بیان می‌کند که وقتی ضرایب f، g بر اساس گاوسی نمونه‌برداری می‌شوند، می‌توانیم به‌طور متوسط انتظار داشته باشیم $(\beta=O(1/\|(f,g)\|)$. ما از توماس اسپیتاو برای اشاره به کران بالای اشتباه روی $\|(\tilde{F},\tilde{G})\|$ سپاسگزاریم.

لم ۲.۵ (تحلیل پیچیدگی زمانی). با شرایط لم ۱.۵، پیچیدگی‌های زمانی الگوریتم ۲ (*TowerSolverR*) عبارت‌اند از:

- $\tilde{O}(nB)$ برای الگوریتم ۲ با *Schönhage-Strassen*،
- $O\left((nB)^{\log_2(3)}\ell\right)$ برای الگوریتم ۲ با *Karatsuba*

توجه می‌کنیم که درحالی‌که پیچیدگی‌های داده‌شده با شونهاگ-اشتراسن بسیار بهتر از کاراتسوبا هستند، اما گمراه‌کننده هستند زیرا $\tilde{O}$ عوامل ثابت و لگاریتمی را پنهان می‌کند که در عمل قابل چشم‌پوشی نیستند. پیچیدگی‌های ارائه‌شده با *Karatsuba*، زمان‌های اجرایی را که ما برای مقادیر معمولی n و B مشاهده می‌کنیم، با دقت بیشتری منعکس می‌کند. در الگوریتم ۲، صعود پرهزینه‌ترین بخش به‌عنوان هر مرحلهٔ جداگانه است، کمی گران‌تر از فرود. سپس پیچیدگی زمانی آن $\sum_{0\le i<\ell} R_i$ است که به اثبات الگوریتم ۲ پایان می‌دهد.

حالت کلی برای q. تحلیل فوق شرایطی را پوشش می‌دهد که در آن سمت راست معادلهٔ NTRU، $q=1$ است. در حالت کلی، ممکن است مقدار دیگری از q را هدف قرار دهیم، معمولاً یک عدد صحیح کوچک. این کار با ضرب مقادیر در q در نقطه‌ای از فاز صعود انجام می‌شود. در توضیح الگوریتم TowerSolverR، این ضرب درست بعد از GCD انجام شد، اما بعدازآن نیز می‌توان آن را انجام داد. در هر صورت، ضرب در q اندازهٔ ضرایب چندجمله‌ای را به‌صورت $\log q$ افزایش می‌دهد (از نظر بیتی) و کاهش Babai در عمل این بیت‌ها را جذب می‌کند. در بدترین حالت، بیت‌های $\log q$ تا آخرین مرحله باقی می‌مانند، که به معنای فضای سربار حداکثر بیت‌های $O(n\log q)$ است.
احتمال شکست. در نسخهٔ قبلی این کار، ما به اشتباه بیان کردیم که الگوریتم ۲ راه‌حلی برای معادلهٔ NTRU (۲.۲) با ورودی‌های (f,g) پیدا می‌کند، اگر و فقط اگر چنین راه‌حلی وجود داشته باشد. این لزوماً درست نیست؛ الگوریتم‌های ۱ و ۲ راه‌حلی را پیدا می‌کنند اگر و فقط اگر $q|\gcd(\mathrm{N}(f),\mathrm{N}(g))$. بااین‌حال، (۲.۲) ممکن است چنین راه‌حلی را بپذیرد حتی اگر $q\nmid\gcd(\mathrm{N}(f),\mathrm{N}(g))$.
به‌عنوان مثال، در حلقهٔ $\mathbb{Z}[x]/\left(x^4+1\right)$، عناصر حلقه را در نظر بگیرید:

$$(f,g,F,G)=\left(x-2,9x^3+x^2,x,x^2+2x+4\right).$$

می‌توان بررسی کرد که $fG-gF=1$، درحالی‌که $\mathrm{N}(f)=17$ و $\mathrm{N}(g)=17386$.
کیفیت خروجی. یک مفهوم مهم کیفیت جواب‌ها (F,G) است، برای مثال در نرم اقلیدسی یا در نرم گرام اشمیت (همان‌طور که در [۱۰، ۱۶] تعریف شده است). برای هر یک از این معیارها، الگوریتم‌های ما جواب‌هایی با کیفیتی مشابه با الگوریتم‌های موجود خروجی می‌دهند.
در واقع، مجموعهٔ جواب‌ها به شکل $\{(F_0+rf,G_0+rg)\mid r\in\mathbb{Z}[x]/(x^n+1)\}$ است، که در آن (F_0,G_0) یک جفت جواب دلخواه را نشان می‌دهد. برای هر عنصر در این مجموعه، الگوریتم ۱ همان جواب را خروجی می‌دهد، بنابراین نرم اقلیدسی خروجی برای الگوریتم‌های ۱ و ۲ یکسان خواهد بود.
از سوی دیگر، برای یک ورودی ثابت (f,g)، همهٔ جواب‌های معادلهٔ NTRU دارای نرم گرام اشمیت یکسان هستند (به‌عنوان مثال [۱۰]، لم ۳] را ببینید).

۶ نتیجه‌گیری و مسائل باز

ما استفاده از نرم میدان را برای بهینه‌سازی برخی از محاسبات روی حلقه‌های چندجمله‌ای، به‌ویژه نتیجه‌ها و حل معادلهٔ NTRU ارائه کردیم. نتیجه عملی دومی این است که الگوریتم امضای پساکوانتومی فالکون به‌طور کامل بر روی میکروکنترلرهای کوچک یا حتی کارت‌های هوشمند قابل استفاده است، زیرا ۳۲ کیلوبایت RAM برای اجرای الگوریتم ما حتی برای یک شبکهٔ NTRU با امنیتی طولانی‌مدت (درجه $n=1024$)، کافی است. تمام عملیات مربوط به امضاها (تولید امضا، تأیید، و تولید زوج کلید) می‌توانند بر روی چنین سخت‌افزارهای

محدودی قرار گیرند.

در زیر تعدادی از سؤالات باز را فهرست می‌کنیم.

چندجمله‌ای‌های غیر سیکلوتومیک. در توصیف خود، مورد چندجمله‌ای سیکلوتومیک را به‌عنوان مدول پوشش دادیم. این روش را می‌توان به مدول‌های دیگر گسترش داد. در واقع، برای هر مدول $\phi=\phi^{'}\left(x^{d}\right)$ برای مقدار $d>1$، استفاده از "نرم میدان" می‌تواند درجه را بر d برای اهداف محاسبهٔ برآیندها و حل معادلهٔ NTRU تقسیم کند. حتی اگر ϕ در $\mathbb{Q}[x]$ تقلیل‌ناپذیر نباشد، یعنی اگر $\mathbb{Q}[x]/(\phi)$ در واقع یک فیلد نباشد، صادق است. شرح حالت کلی همچنان به‌عنوان مسئله برای بررسی باقی مانده است. بااین‌حال، استفاده از مدول‌های کاهش‌پذیر در شبکه‌های NTRU معمولاً توصیه نمی‌شود.

اعداد صحیح بزرگ. درحالی‌که دستاوردهای ما، از نظر حافظه، قابل توجه است، ما هنوز باید اعداد صحیح بزرگ را مدیریت کنیم. از نقطه‌نظر پیچیدگی پیاده‌سازی، خلاص شدن از شر اعداد صحیح، برای مثال با انجام تمام عملیات در RNS، بدون تأثیر منفی بر زمان اجرا و نیازهای حافظهٔ الگوریتم‌های ما، جالب خواهد بود.

کاربردهای دیگر برای ساختارهای رمزنگاری. به نظر می‌رسد که بررسی اینکه آیا روش ذکرشده در این مقاله می‌تواند کارایی سایر الگوریتم‌های رمزنگاری را بهبود بخشند، ارزشمند باشد. علاوه‌بر این، درست همان‌طور که در این مقاله یک کاربرد سازنده از نرم میدان (در مقابل [۱]) ارائه کردیم، به نظر می‌رسد که، کاربرد سازندهٔ ردیابی (در مقابل [۶]) بسیار جالب خواهد بود. در پایان، [۲۰] نشان داد که دیدگاه جبری در مورد [۱] ضروری نیست. این سؤال را مطرح می‌کند که آیا در مورد این کار ارائه‌شده در این مقاله همچنین است؟

کاربردهای مختص تحلیل. به نظر می‌رسد که استفاده از روش ارائه‌شده در این مقاله برای بهبود حملات بر اساس نرم میدان [۱] یا حتی بر روی ردیابی میدان [۶] ارزشمند باشد.

References

[1] Albrecht, M., Bai, S., & Ducas, L. (2016). A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and graded encoding schemes. *In Annual International Cryptology Conference, Berlin, Heidelberg: Springer Berlin Heidelberg*, 9814, 153–178. DOI: https://doi.org/10.1007/978-3-662-53018-4_6.

[2] Babai, L. (1986). On Lovász'lattice reduction and the nearest lattice point problem. *Combinatorica*, 6, 1–13. DOI: https://doi.org/10.1007/BF02579403.

[3] Bernstein, D.J., Chuengsatiansup, C., Lange, T., & van Vredendaal, C. (2016). NTRU Prime. *Tech. rep., National Institute of Standards and Technology*.

[4] Campbell, P., & Groves, M. (2017). Practical post-quantum hierarchical identity-based encryption. *16th IMA International Conference on Cryptography and Coding*.

[5] Cash, D., Hofheinz, D., Kiltz, E., & Peikert, C. (2010). Bonsai trees, or how to delegate a lattice basis. *In: Gilbert, H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg*. DOI: https://doi.org/10.1007/978-3-642-13190-5_27.

[6] Cheon, J.H., Jeong, J., & Lee, C. (2016). An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low level encoding of zero. *LMS Journal of Computation and Mathematics*, 19, 255–266. DOI: https://doi.org/10.1112/S1461157016000371.

[7] Chuengsatiansup, C., Prest, T., Stehlé, D., Wallet, A., & Xagawa, K. (2020). ModFalcon: Compact signatures based on module-NTRU lattices. *In: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 853–866. DOI: https://doi.org/10.1145/3320269.3384758.

[8] Cooley, J.W., & Tukey, J.W. (1965). An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, 19, 297–301.

[9] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22, 644–654. DOI: https://doi.org/https://doi.org/10.1109/TIT.1976.1055638.

[10] Ducas, L., Lyubashevsky, V., & Prest, T. (2014). Efficient identity-based encryption over NTRU lattices. *In Advances in Cryptology–ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014, Proceedings, Part II, 20, 22–41*. DOI: https://doi.org/10.1007/978-3-662-45608-8_2.

[11] Espitau, T., Fouque, P.A., Gérard, F., Rossi, M., Takahashi, A., Tibouchi, M., Wallet, A., & Yu, Y. (2022). Mitaka: A simpler, parallelizable, maskable variant of Falcon. *In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cham: Springer International Publishing*, 222–253. DOI: https://doi.org/10.1007/978-3-031-07082-2_9.

[12] FIPS. (2001). NIST: Security Requirements for Cryptographic Modules.

[13] Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., & Zhang, Z. (2017). Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU (tech. rep.).

[14] Fouque, P.A., Kirchner, P., Pornin, T., & Yu, Y. (2022). Bat: Small and Fast KEM over NTRU Lattices. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 240–265. DOI: https://doi.org/10.46586/tches.v2022.i2.240-265.

[15] Gentleman, W.M., & Sande, G. (1966). Fast Fourier transforms: for fun and profit. *In Proceedings of the November 7-10, fall joint computer conference*, 563–578.

[16] Gentry, C., Peikert, C., & Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. *In Proceedings of the fortieth annual ACM symposium on Theory of computing*, 197–206. DOI: https://doi.org/10.1145/1374376.1374407.

[17] Harvey, D., & Van Der Hoeven, J. (2021). Integer multiplication in time O(nlog n). *Annals of Mathematics*, 193, 563–617. DOI: https://doi.org/10.4007/annals.2021.193.2.4.

[18] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., & Whyte, W. (2003). NTRUSIGN: Digital signatures using the NTRU lattice. *In Cryptographers' track at the RSA conference, Berlin, Heidelberg: Springer Berlin Heidelberg*, 122–140. DOI: https://doi.org/https://doi.org/10.1007/3-540-36563-X_9.

[19] Hoffstein, J., Pipher, J., & Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. *In International algorithmic number theory symposium, Berlin, Heidelberg: Springer Berlin Heidelberg*, 267–288. DOI: https://doi.org/https://doi.org/10.1007/BFb0054868.

[20] Kirchner, P., & Fouque, P.A. (2017). Revisiting lattice attacks on overstretched NTRU parameters. *In Annual International Conference on the Theory and Applications of Cryptographic*

Techniques, Cham: Springer International Publishing, 3–26. DOI: https://doi.org/10.1007/978-3-319-56620-7_1.

[21] Lenstra, A.K., Lenstra, H.W., & Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(ARTICLE), 515–534. DOI: https://doi.org/10.1007/BF01457454.

[22] Micciancio, D., & Warinschi, B. (2001). A Linear Space Algorithm for Computing the Hermite Normal Form. *In Proceedings of the 2001 international symposium on Symbolic and algebraic computation*, 231–236. DOI: https://doi.org/10.1145/384101.384133.

[23] NIST. (2016). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process.

[24] Schönhage, A., & Strassen, V. (1971). Fast multiplication of large numbers. *Computing*, 7, 281–292. DOI: https://doi.org/10.1007/BF02242355.

[25] Smart, N.P., Albrecht, M.R., Lindell, Y., Orsini, E., Osheter, V., Paterson, K., & Peer, G. (2017). Lima: A PQC encryption scheme. *National Institute of Standards and Technology*.

[26] Stehle, D. & Steinfeld, R. (2013). Making NTRUEnrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. *Cryptology ePrint Archive, Report 2013/004*.

[27] Von Zur Gathen, J., & Gerhard, J. (2013). Modern Computer Algebra (3. Ed.). *Cambridge University Press*.

[28] Working Group of the C/MM Committee. (2009). *IEEE P1363. 1 Standard Specifications for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices*.

[29] Zhao, R.K., McCarthy, S., Steinfeld, R., Sakzad, A., & O'Neill, M. (2023). Quantum-safe HIBE: does it cost a Latte?. *IEEE Transactions on Information Forensics and Security*. DOI: https://eprint.iacr.org/2021/222.

Measure Algebras and Applications

A^{**}-biprojectivity of Banach algebras based on maximal ideal space

Amir Sahami[1], **Mehdi Rostami**[2]✉

1. Department of Mathematics, Faculty of Basic Science, Ilam University, P.O. Box 69315-516 Ilam, Iran. Email: a.sahami@ilam.ac.ir
2. Corresponding Author, Department of Mathematics and Computer Science, Amirkabir University of Technology (Tehran Polytechnic), Iran. Email: mross@aut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 28 December 2023
Received in revised form:
17 April 2024
Accepted: 20 June 2024
Published Online:
20 August 2024

Keywords:
Banach algebra,
φ-A^{**}-biprojective,
φ-inner amenable,
Group algebra,
Measure algebra

2020 Mathematics Subject Classification:
43A20, 46M10

ABSTRACT

In this paper, we continue the study of A^{**}-biprojectivity of Banach algebras, was introduced in [19], and the relation between this new notion and φ-amenability of Banach algebras is investigated. A^{**}-biprojectivity of Segal algebras and lower triangular matrix algebras is studied. Also, we introduce the notion of φ-A^{**}-biprojectivity of Banach algebras. Some examples indicate that this notion is weaker than A^{**}-biprojectivity. We obtain the relation between this notion and φ-amenability and φ-inner amenability. Finally, we investigate this new notion on certain Banach algebras such as group algebras, measure algebras, and lower triangular Banach algebras.

Cite this article: Sahami, A., & Rostami, M. (2024). A^{**}-biprojectivity of Banach algebras based on maximal ideal space. *Measure Algebras and Applications*, 1(2), 71–84. http://doi.org/10.22091/MAA.2024.10255.1012

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10255.1012

Extended Abstract

Introduction

The concept of amenability (for discrete groups) originated by J. von Neumann in 1929, as, a discrete group is amenable if it admits a finitely additive left invariant probability measure. After that formally, it was introduced for all locally compact groups by M.M. Day. This concept was later extended to Banach algebras by B. E. Johnson in 1972 and has since grown into a fascinating area of research with applications in diverse fields, such as abstract harmonic analysis, operator algebras, and ergodic theory. In fact, a Banach algebra A is said to be amenable if the first cohomology group of A with coefficients in every dual Banach A-bimodule X^* is trivial. This notion has been considered as an important cohomological notion for Banach algebras by many mathematicians. After that many researchers studied the properties of this notion and the relation with many other cohomological notions. In 2006 Ghahramani et al. introduced the concept of approximate amenability as a notion weaker than amenability and improved the results related to amenability. A Banach algebra A is called approximately amenable if every continuous derivation from A into every dual Banach A-bimodule is approximately inner. They presented many examples to indicate that approximate amenability is different from amenability. In 2008, Kaniuth, Lau and Pym by inspiration of left amenability of F-algebras, was done by Lau [12], introduced φ-amenability of Banach algebras. This notion was studied by many authors and it was proved that φ-amenability has a near relation to the existence of a bounded approximate identity for $\ker\varphi$. A net (e_α) in A is an approximate identity for A if $\|ae_\alpha - a\| \to a$ and $\|e_\alpha a - a\| \to a$, for all $a \in A$. Helemskii in the 1980s defined biprojective Banach algebras as an important tool in homological notions and investigated any hereditary properties of this concept, interested readers are referred to his comprehensive book [3]. A Banach algebra A is called biprojective if there exists a bounded A-bimodule morphism $\rho\colon A \to A\widehat{\otimes}A$ such that $\pi_A \circ \rho(a) = a$. After that, some other weaker or stronger notions were defined and investigated. For example, Zhang in 1999 [23] introduced approximate biprojective Banach algebras. Sahami and Pourabbas in 2014 [22] by inspiration of φ-amenability introduced φ-biprojective Banach algebras and studied some properties of this notion. After that extensive research was done on this notion for some Banach algebras such as group algebras, measure algebras, semigroup algebras and Lipschitz algebras. A Banach algebra A is called φ-biprojective if there exists a continuous module morphism $\rho : A \to A\widehat{\otimes}A$ such that $\varphi \circ \pi_A \circ \rho(a) = \varphi(a)$, for all $a \in A$, where φ is a nonzero bounded multiplicative linear functional on A. The authors, in [19], introduced the notion of A^{**}-biprojective Banach algebras and found the relation between this notion with some other cohomological notions. Also, A^{**}-biprojectivity of certain Banach algebras such as Lipschitz algebras and triangular Banach algebras had been studied. In this paper, we investigate the relation between A^{**}-biprojectivity and φ-amenability. After that we define the notion of φ-A^{**}-biprojective Banach algebras and we obtain the relation between this notion and some other cohomological notions. Also, we study φ-A^{**}-biprojectivity of Banach algebras associated to a locally compact group.

Conclusion

In this paper, the following definitions are stated:

***Definition* 0.1.** *A Banach algebra A is called biprojective if there exists a bounded A-bimodule morphism $\rho\colon A \to A\widehat{\otimes}A$ such that $\pi_A \circ \rho(a) = a$.*

***Definition* 0.2.** *A Banach algebra A is called left φ-amenable if there exists a bounded net (m_α) in A such that*

$$am_\alpha - \varphi(a)m_\alpha \to 0, \qquad \varphi(m_\alpha) \to 1,$$

for all $a \in A$.

***Definition* 0.3.** *A Banach algebra A is called A^{**}-biprojective if there exists bounded A-module morphism $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ such that for all $a \in A$*

$$\pi_{A^{**}} \circ \rho(a) = \kappa_A(a).$$

***Definition* 0.4.** *Let A be a Banach algebra and $\varphi \in \Delta(A)$. A is called φ-A^{**}-biprojective if there exists a net $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ such that for all $a \in A$*

$$\widetilde{\varphi} \circ \pi_{A^{**}} \circ \rho(a) = \varphi(a).$$

Also, the next theorems and corollaries are presented:

***Theorem* 0.5.** *Let A be a Banach algebra with a left approximate identity. If A is A^{**}-biprojective, then A is left φ-amenable.*

***Corollary* 0.6.** *Let G be a locally compact group. If $S^1(G)$ is $S^1(G)^{**}$-biprojective, then G is amenable.*

***Lemma* 0.7.** *Let $|I| \geq 1$ be an index set with the smallest element. Then $LO(I, A)$ is not $LO(I, A)^{**}$-biprojective.*

***Theorem* 0.8.** *Let A be a Banach algebra and $\varphi \in \Delta(A)$. If A is φ-inner amenable and φ-A^{**}-biprojective, then A is left and right φ-amenable.*

***Theorem* 0.9.** *Let G be a locally compact group and $\varphi \in \Delta(L^1(G))$. The algebra $L^1(G)$ is φ-$L^1(G)^{**}$-biprojective if and only if G is amenable.*

***Theorem* 0.10.** *Let G be a locally compact group and $\varphi \in \Delta(M(G))$. The algebra $M(G)$ is φ-$M(G)^{**}$-biprojective if and only if G is amenable and discrete.*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۸۴-۷۱

A^{**} -دوتصویری جبرهای باناخ بر پایه فضای ایده‌آل ماکسیمال

امیر سهامی [۱] ، مهدی رستمی [۲]✉

۱. دانشکده علوم ریاضی، دانشگاه ایلام، ایلام، ایران. رایانامه: a. sahami@ilam. ac. ir
۲. نویسندهٔ مسئول، دانشکده ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران. رایانامه: mross@aut. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۰/۷
تاریخ بازنگری: ۱۴۰۳/۱/۲۹
تاریخ پذیرش: ۱۴۰۳/۳/۳۱
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
جبر باناخ،
A^{**}-φ- دوتصویر،
میانگین‌پذیر داخلی،
جبر گروهی،
جبر اندازه

رده‌بندی ریاضی:
43A20, 46M10

چکیده

در این مقاله، مطالعهٔ جبرهای باناخ A^{**} -دوتصویر را که در منبع [۱۹] معرفی شدند، ادامه می‌دهیم و ارتباط آن‌ها را با مفهوم φ -میانگین‌پذیری بررسی می‌کنیم. A^{**} -دوتصویری جبرهای سگال و جبرهای ماتریسی پایین مثلثی را مطالعه می‌کنیم. همچنین، مفهوم جبرهای باناخ A^{**}-φ -دوتصویر را معرفی می‌کنیم و رابطهٔ بین این مفهوم و φ -میانگین‌پذیری و φ -میانگین‌پذیری داخلی را به دست می‌آوریم. در نهایت، این مفهوم جدید، برای جبرهای باناخ خاص مانند جبرهای گروهی، جبرهای اندازه و جبرهای باناخ پایین مثلثی بررسی می‌شود.

استناد: سهامی، امیر.، رستمی، مهدی. (۱۴۰۳). A^{**} -دوتصویری جبرهای باناخ بر پایه فضای ایده‌آل ماکسیمال. جبرهای اندازه و کاربردها، ۱(۲)، ۸۴-۷۱.

http://doi.org/10.22091/MAA.2024.10255.1012

ناشر: دانشگاه قم.

۱ مقدمه

مفهوم میانگین‌پذیری (برای گروه‌های گسسته) توسط ج. فون نویمان در سال ۱۹۲۹ آغاز شد، که در آن، یک گروه گسسته میانگین‌پذیر است هرگاه یک اندازهٔ احتمال جمعی پایای چپ موجود باشد. پس‌از آن م. م. دی این مفهوم را به‌طور رسمی برای تمام گروه‌های فشردهٔ موضعی معرفی کرد. بعدها این مفهوم توسط ب. ا. جانسون در سال ۱۹۷۲ برای جبرهای باناخ توسیع داده شد و ازآن‌پس به‌عنوان یک موضوع تحقیقاتی جالب مورد توجه قرار گرفت و کاربردهای فراوانی در شاخه‌های مختلف ازجمله آنالیز هارمونیک مجرد، جبر عملگرها و نظریهٔ ارگودیک پیدا کرد. در واقع، جبر باناخ A میانگین‌پذیر گفته می‌شود هرگاه اولین گروه همانستگی A با ضرایب در هر A -دومدول باناخ دوگان X^* بدیهی باشد. این مفهوم بعدها به‌عنوان یک خاصیت همانستگی مهم برای جبرهای باناخ مورد توجه بسیاری از ریاضیدانان قرار گرفت. پس‌از آن تحقیقات بسیاری در مورد خواص این مفهوم و ارتباط آن با بسیاری از مفاهیم دیگر همانستگی مورد مطالعه قرار گرفت. در سال ۲۰۰۶ قهرمانی و همکاران مفهوم ضعیف‌تر میانگین‌پذیری تقریبی را معرفی کردند و توانستند بسیاری از نتایج مربوط به میانگین‌پذیری را تعمیم دهند. جبر باناخ A میانگین‌پذیر تقریبی نامیده می‌شود هرگاه هر اشتقاق پیوسته از A به توی هر A -دومدول باناخ دوگان درونی تقریبی باشد. آن‌ها با ذکر مثال‌های متعدد نشان دادند که این مفهوم با مفهوم میانگین‌پذیری متفاوت است. در سال ۲۰۰۸ کانیوث، لائو و پیم مفهوم φ -میانگین‌پذیری جبرهای باناخ را معرفی کردند که این تعریف با الهام از تعریف میانگین‌پذیری چپ F -جبرها که قبلاً توسط لائو [۱۲] انجام شده بود شکل گرفت. این مفهوم مورد توجه بسیاری قرار گرفت و ثابت شد که φ -میانگین‌پذیری رابطهٔ نزدیکی با وجود یکهٔ تقریبی کران‌دار برای $\ker\varphi$ دارد. تور (e_α) در A را یکهٔ تقریبی گوییم هرگاه برای هر $a\in A$، $\|ae_\alpha-a\|\to 0$ و $\|e_\alpha a-a\|\to 0$.
هلمسکی در دهه ۱۹۸۰ جبرهای باناخ دوتصویر را تعریف کرد که تا به اکنون به‌عنوان یکی از ابزارهای مهم در همانستگی جبرهای باناخ شناخته می‌شود. در واقع، جبر باناخ A دوتصویر نامیده می‌شود هرگاه همریختی A -دومدولی پیوسته $\rho : A\to A\widehat{\otimes}A$ وجود داشته باشد به‌طوری‌که $\pi_A\circ\rho=id_A$. پس‌از آن مفاهیم دیگری که قوی‌تر یا ضعیف‌تر از این مفهوم بودند نیز تعریف و مورد بررسی قرار گرفتند. به‌عنوان مثال، ژانگ در سال ۱۹۹۹ [۲۳] جبرهای باناخ دوتصویر تقریبی را معرفی کرد. سهامی و پورعباس در سال ۲۰۱۴ [۲۲] با الهام از تعریف φ -میانگین‌پذیری مفهوم جبرهای باناخ φ -دوتصویر را معرفی کردند و خواص آن را مورد بررسی قرار دادند. پس‌از آن نیز تحقیقات گسترده‌ای روی این مفهوم برای بسیاری از جبرها ازجمله جبر گروهی، جبر اندازه، جبر نیم‌گروهی و جبرهای لیپشیتزی انجام پذیرفت. جبر باناخ A، φ -دوتصویر نامیده می‌شود هرگاه همریختی A -مدولی پیوسته $\rho : A\to A\widehat{\otimes}A$ موجود باشد به‌طوری‌که $\varphi\circ\pi_A\circ\rho(a)=\varphi(a)$، که در آن φ یک تابعک خطی ضربی کران‌دار ناصفر روی A است. نویسندگان در [۱۹] مفهوم جبرهای باناخ A^{**} -دوتصویر را معرفی کردند و رابطهٔ آن را با برخی از مفاهیم همانستگی مطالعه کردند. همچنین A^{**} -دوتصویری برخی از جبرهای باناخ ازجمله جبرهای لیپشیتزی و جبرهای مثلثی را بررسی کردند. در این مقاله ارتباط بین A^{**} -دوتصویری و φ -میانگین‌پذیری را بررسی می‌کنیم. سپس جبرهای باناخ φ-A^{**}- دوتصویر را تعریف می‌کنیم و ارتباط آن را با برخی دیگر از مفاهیم همانستگی به دست می‌آوریم. همچنین این مفهوم را برای جبرهای وابسته به یک گروه فشردهٔ موضعی مطالعه می‌کنیم.

۲ تعاریف و مقدمات

فرض کنید A یک جبر باناخ و X یک A -دومدول باناخ باشد. در این صورت فضای دوگان X یعنی X^* با اعمال مدولی زیر یک A -دومدول باناخ است:

$$(a\cdot f)(x)=f(x\cdot a),\ (f\cdot a)(x)=f(a\cdot x)\qquad (a\in A, x\in X, f\in X^*).$$

اگر $A\widehat{\otimes}A$ فضای حاصلضرب تانسوری تصویری باشد در این صورت $A\widehat{\otimes}A$ یک باناخ A- دومدول با اعمال مدولی زیر است:

$$a\cdot(b\otimes c)=ab\otimes c,\ (b\otimes c)\cdot a=b\otimes ca\qquad (a,b,c\in A)$$

بنابراین $(A\widehat{\otimes}A)^*$ با اعمال مدولی زیر یک باناخ A- دومدول است:

$$\begin{aligned}&(a\cdot f)(b\otimes c)=f(b\otimes ca),\\ &(f\cdot a)(b\otimes c)=f(ab\otimes c)\qquad (a,b,c\in A, f\in(A\hat{\otimes}A)^*).\end{aligned}$$

به‌طور مشابه می‌توان $(A\widehat{\otimes}A)^{**}$ را به‌عنوان یک باناخ A -دومدول در نظر گرفت. به یک تابعک خطی ضربی ناصفر روی جبر باناخ A یک مشخصه گفته می‌شود و مجموعهٔ تمام مشخصه‌های روی A را با نماد $\Delta(A)$ نمایش می‌دهیم. در سرتاسر این مقاله، $\kappa_A : A\to A^{**}$

نشانندهٔ طبیعی و $\pi_A : A\hat{\otimes}A \to A$ نگاشت ضربی است که به‌صورت زیر تعریف می‌شود:

$$\pi_A(a \otimes b) = ab \qquad (a, b \in A).$$

آرنز در سال ۱۹۵۱ دو ضرب روی دوگان دوم یک جبر باناخ تعریف کرد تا بتواند آن را تبدیل به یک جبر باناخ کند. در واقع این ضرب‌ها توسیع ضرب معمولی روی جبر هستند. به این ضرب‌ها ضرب آرنز اول و دوم گفته می‌شود که به ترتیب با نمادهای $\square$ و $\Diamond$ نمایش داده می‌شوند و به‌صورت زیر تعریف می‌شوند:

$$\langle F\square G, f\rangle = \langle F, G \cdot f\rangle, \qquad \langle F\Diamond G, f\rangle = \langle G, f \cdot F\rangle,$$

و

$$\langle G \cdot f, a\rangle = \langle G, f \cdot a\rangle, \qquad \langle f \cdot F, a\rangle = \langle F, a \cdot f\rangle,$$

و

$$\langle f \cdot a, b\rangle = \langle f, ab\rangle, \qquad \langle a \cdot f, b\rangle = \langle f, ba\rangle,$$

که در آن $F, G \in A^{**}$، $f \in A^*$ و $a, b \in A$.

دقت شود که اگر A یک جبر باناخ باشد و $\varphi \in \Delta(A)$، آنگاه توسیع یکتایی از φ به A^{**} موجود است که آن را با $\widetilde{\varphi}$ نمایش می‌دهیم. در واقع برای هر $F \in A^{**}$ قرار می‌دهیم

$$\widetilde{\varphi}(F) = F(\varphi).$$

۳ نتایج اصلی

ابتدا تعریف جبرهای باناخ A^{**}-دوتصویر را ارائه می‌دهیم. برای جزئیات بیشتر به منبع [۱۹] مراجعه شود.

تعریف ۱.۳. جبر باناخ A را A^{**}-دوتصویر نامیم هرگاه همریختی پیوسته A-دومدولی $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ موجود باشد به‌طوری‌که به ازای هر $a \in A$

$$\pi_{A^{**}} \circ \rho(a) = \kappa_A(a)$$

که در آن $\pi_{A^{**}} : A^{**}\widehat{\otimes}A^{**} \to A^{**}$ عملگر ضربی با ضابطهٔ $\pi_{A^{**}}(F \otimes G) = F\square G$ است.

در قضیهٔ زیر به بررسی رابطهٔ بین A^{**}-دوتصویری جبر باناخ A با φ-میانگین‌پذیری می‌پردازیم.

تعریف ۲.۳. فرض کنیم A یک جبر باناخ باشد و $\varphi \in \Delta(A)$. گوییم A، φ-میانگین‌پذیر چپ است هرگاه تور کران‌دار (m_α) در A موجود باشد به‌طوری‌که برای هر $a \in A$

$$am_\alpha - \varphi(a)m_\alpha \to ۰, \qquad \varphi(m_\alpha) \to ۱.$$

تور (e_α) را یکهٔ تقریبی چپ جبر باناخ A گوییم هرگاه برای هر $a \in A$، $e_\alpha a \to a$. یکهٔ تقریبی (e_α) را کران‌دار گوییم هرگاه $K > ۰$ وجود داشته باشد که $\|e_\alpha\| \leq K$. به‌طور مشابه یکهٔ تقریبی راست کران‌دار نیز تعریف می‌شود. جبر باناخ A دارای یکهٔ تقریبی کران‌دار است هرگاه دارای یکهٔ تقریبی چپ کران‌دار و راست کران‌دار باشد.

قضیه ۳.۳. فرض کنیم A یک جبر باناخ با یکهٔ تقریبی چپ (راست) باشد و $\varphi \in \Delta(A)$. اگر A، A^{**}-دوتصویر باشد، آنگاه A، φ-میانگین‌پذیر چپ (راست) است.

اثبات. ازآنجاکه جبر A، A^{**}-دوتصویر است لذا طبق تعریف عملگر خطی $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ موجود است به‌طوری‌که برای هر $a, b \in A$ داریم:

$$\pi_{A^{**}} \circ \rho(a) = \kappa_A(a), \qquad \rho(ab) = \rho(a) \cdot b = a \cdot \rho(b).$$

طبق [۲، لم ۱.۷] نگاشت

$$\Psi : A^{**}\widehat{\otimes}A^{**} \to (A\widehat{\otimes}A)^{**}$$

موجود است به‌طوری‌که برای هر $a,b\in A$ و $n\in A^{**}\widehat{\otimes}A^{**}$ در شرایط زیر صدق می‌کند:

الف) $\Psi(\kappa_A(a)\otimes\kappa_A(b))=\kappa_{A\widehat{\otimes}A}(a\otimes b)$

ب) $\Psi(n)\cdot a=\Psi(n\cdot a)$

پ) $a\cdot\Psi(n)=\Psi(a\cdot n)$

ت) $\pi_A^{**}(\Psi(n))=\pi_{A^{**}}(n)$.

نگاشت $\theta:A\to(A\widehat{\otimes}\frac{A}{\ker\varphi})^{**}$ را به‌صورت زیر تعریف می‌کنیم:

$$\theta(a)=(id_A\otimes q)^{**}\circ\Psi\circ\rho(a),$$

که در آن $id_A:A\to A$ نگاشت همانی و $q:A\to\frac{A}{\ker\varphi}$ نگاشت خارج‌قسمتی است. دقت کنیم که نگاشت $id_A\otimes q$ یک همریختی A -مدولی است و درنتیجه $(id_A\otimes q)^{**}$ نیز یک A -مدولی همریختی است. چون A دارای یکهٔ تقریبی چپ است لذا $\overline{A\ker\varphi}=\ker\varphi$. پس برای هر $k\in\ker\varphi$ دنباله‌های $\{a_n\}$ در A و $\{k_n\}$ در $\ker\varphi$ وجود دارند که $k=\lim_{n\to\infty}a_nk_n$. ازآنجاکه برای هر $k\in\ker\varphi$، $q(k)=0$ لذا داریم

$$\begin{aligned}\theta(k)=\theta(\lim_{n\to\infty}a_nk_n)&=\lim_{n\to\infty}\theta(a_nk_n)\\&=\lim_{n\to\infty}(id_A\otimes q)^{**}\circ\Psi\circ\rho(a_nk_n)\\&=\lim_{n\to\infty}(id_A\otimes q)^{**}\circ\Psi\circ\rho(a_n)k_n=0.\end{aligned}$$

درنتیجه نگاشت θ یک A- مدول همریختی چپ کران‌دار $\widetilde{\theta}:\frac{A}{\ker\varphi}\to(A\widehat{\otimes}\frac{A}{\ker\varphi})^{**}$ القا می‌کند. عنصر $a_0\in A$ را طوری انتخاب می‌کنیم که $\varphi(a_0)=1$. تعریف می‌کنیم

$$\mathbf{m}=\widetilde{\theta}(a_0+\ker\varphi).$$

همان‌طور که می‌دانیم $\frac{A}{\ker\varphi}\cong\mathbb{C}$ و درنتیجه $\mathbf{m}\in A^{**}$. به‌آسانی می‌توان دید که برای هر $a\in A$ داریم

$$\begin{aligned}a\mathbf{m}=a\widetilde{\theta}(a_0+\ker\varphi)&=\widetilde{\theta}(aa_0+\ker\varphi)\\&=\widetilde{\theta}(\varphi(a)a_0+\ker\varphi)\\&=\varphi(a)\widetilde{\theta}(a_0+\ker\varphi)\\&=\varphi(a)\mathbf{m}.\end{aligned}$$

همچنین ازآنجاکه $\widetilde{\varphi}\circ\pi_A^{**}=\widetilde{\varphi}\circ(id_A\otimes q)^{**}$ نتیجه می‌گیریم که

$$\begin{aligned}\widetilde{\varphi}(\mathbf{m})=\widetilde{\varphi}\circ\widetilde{\theta}(a_0+\ker\varphi)&=\widetilde{\varphi}\circ\theta(a_0)\\&=\widetilde{\varphi}\circ(id_A\circ q)^{**}\circ\Psi\circ\rho(a_0)\\&=\widetilde{\varphi}\circ\pi_A^{**}\circ\Psi\circ\rho(a_0)\\&=\widetilde{\varphi}\circ\pi_{A^{**}}\circ\rho(a_0)\\&=\varphi(a_0)=1.\end{aligned}$$

بنابراین A، φ- میانگین‌پذیر چپ است. اثبات میانگین‌پذیری راست A نیز به‌طور مشابه انجام می‌شود. □

تعریف ۴.۳. برای گروه فشردهٔ موضعی G زیرفضای خطی $S(G)$ از جبر گروهی $L^1(G)$ را یک جبر سگال روی G نامیم هرگاه

الف) $S(G)$ زیرمجموعهٔ چگال در $L^1(G)$ است.

ب) $S(G)$ با نرم $\|\cdot\|_{S(G)}$ یک فضای باناخ باشد و برای هر $f\in S(G)$ داشته باشیم $\|f\|_{L^1(G)}\leq\|f\|_{S(G)}$.

ج) برای هر $f\in S(G)$ و $y\in G$ داشته باشیم $L_y(f)\in S(G)$ و نگاشت $y\mapsto L_y(f)$ از G به توی $S(G)$ پیوسته باشد که در آن $L_y(f)(x)=f(y^{-1}x)$.

د) برای هر $f\in S(G)$ و $y\in G$ داشته باشیم $\|L_y(f)\|_{S(G)}=\|f\|_{S(G)}$.

برای جزییات بیشتر دربارهٔ جبرهای سگال روی گروه‌های فشردهٔ موضعی به [۱۸] مراجعه شود.

تعریف ۵.۳. فرض کنید G یک گروه فشردهٔ موضعی باشد. گروه G را میانگین‌پذیر نامیم هرگاه دارای میانگین پایای چپ باشد. یعنی عملگر خطی و کران‌دار $T : L^\infty(G) \to \mathbb{C}$ موجود باشد به‌طوری‌که $\|T\| = T(1) = 1$ و برای هر $f \in L^\infty(G)$

$$T(L_x f) = T(f)$$

که در آن $L_x f$ نگاشت انتقال چپ $L_x f(y) = f(x^{-1}y)$ است. به‌عنوان مثالی از گروه‌های میانگین‌پذیر می‌توان به گروه‌های آبلی و گروه‌های فشرده اشاره کرد. برای مطالعهٔ بیشتر به منابع [۱۶] و [۱۷] مراجعه شود.

نتیجه ۶.۳. فرض کنیم G یک گروه فشردهٔ موضعی است. اگر $S(G)$، $S(G)^{**}$ -دوتصویر باشد، آنگاه G میانگین‌پذیر است.

اثبات. می‌دانیم که $S(G)$ همواره دارای یکهٔ تقریبی چپ است. از قضیه ۱.۲ نتیجه می‌شود که اگر $S(G)$، $S(G)^{**}$ -دوتصویر باشد، آنگاه $S(G)$، φ- میانگین‌پذیر چپ است و طبق [۱، قضیه ۲.۳] نتیجه می‌شود که G میانگین‌پذیر است. □

نتیجه ۷.۳. فرض کنیم A یک جبر باناخ با یکهٔ تقریبی چپ و راست باشد و $\varphi \in \Delta(A)$. اگر A، A^{**}- دوتصویر باشد، آنگاه A، φ- جانسون میانگین‌پذیر است.

اثبات. اثبات نتیجهٔ مستقیم قضیه ۱.۲ و [۲۲، قضیه ۲.۲] است. □

فرض کنیم I یک مجموعهٔ جهت‌دار کلی با کوچک‌ترین عضو باشد. $LO(I)$ را مجموعهٔ تمام ماتریس‌های $I \times I$ پایین مثلثی با عناصر در $\mathbb{C}$ در نظر می‌گیریم، یعنی

$$LO(I) = \{[a_{ij}]_{i,j\in I} : \ a_{ij} \in \mathbb{C}, a_{ij} = 0 \text{ برای هر } i < j\}.$$

$LO(I)$ با ضرب ماتریسی و نرم $\|[a_{ij}]\| = \sum_{i,j\in I} \|a_{ij}\|$ تشکیل جبر باناخ می‌دهد.

قضیه ۸.۳. اگر $|I| > 1$ و I دارای کوچک‌ترین عضو باشد، آنگاه $LO(I)$، $LO(I)^{**}$- دوتصویر نیست.

اثبات. به برهان خلف فرض کنیم $LO(I)$، $LO(I)^{**}$- دوتصویر باشد. ازآنجاکه جبر $\mathbb{C}$ دارای عنصر همانی است لذا $LO(I)$ یکهٔ تقریبی دارد. نگاشت $\psi : LO(I) \to \mathbb{C}$ را با ضابطهٔ

$$\psi([a_{ij}]) = a_{i_0 i_0}$$

تعریف می‌کنیم که در آن i_0 کوچک‌ترین عنصر I است. به‌وضوح ψ یک مشخصه روی $LO(I)$ است. طبق قضیه ۱.۲ جبر $LO(I)$، ψ- میانگین‌پذیر چپ است. ایده‌آل بستهٔ

$$J = \left\{ \begin{bmatrix} a_{i_0 i_0} & 0 & \cdots & 0 & \cdots \\ a_{kk'} & 0 & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{ss'} & 0 & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} : \ a_{i_0 i_0}, a_{kk'}, a_{ss'}, \cdots \in \mathbb{C} \right\}$$

در $LO(I)$ را در نظر می‌گیریم. در این صورت $\psi|_J \neq 0$. درنتیجه بنابر [۱۰، لم ۳.۱] ایده‌آل J نیز $\psi|_J$- میانگین‌پذیر چپ است. پس تور کران‌دار $(m_\alpha) \subseteq J$ وجود دارد که برای هر $j \in J$

$$jm_\alpha - \psi(j)m_\alpha \to 0, \ \ \psi(m_\alpha) = 1.$$

از طرف دیگر برای هر $j_1, j_2 \in J$ رابطهٔ $j_1 j_2 = \psi(j_2)j_1$ برقرار است. بنابراین می‌توان نتیجه گرفت که برای هر $j \in J$، $j - \psi(j)m_\alpha \to 0$. حال با در نظر گرفتن عنصر

$$\mathbf{j} = \begin{bmatrix} 0 & 0 & \cdots & 0 & \cdots \\ 1 & 0 & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

به این نتیجه می‌رسیم که $\mathbf{j} = \mathbf{j} - \psi(\mathbf{j})m_\alpha \to 0$ و به تناقض می‌رسیم. □

در ادامه مفهوم A^{**} -دوتصویری وابسته به یک مشخصه را بیان می‌کنیم.

تعریف ۹.۳. فرض کنیم A یک جبر باناخ باشد و $\varphi \in \Delta(A)$. گوییم A، φ-A^{**} -دوتصویر است هرگاه همریختی پیوسته A -دومدولی $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ موجود باشد به‌طوری‌که به ازای هر $a \in A$

$$\widetilde{\varphi} \circ \pi_{A^{**}} \circ \rho(a) = \varphi(a).$$

به‌وضوح اگر A، A^{**} -دوتصویر باشد، آنگاه φ-A^{**} -دوتصویر است. در ادامه با ذکر مثالی نشان می‌دهیم که عکس این مطلب لزوماً برقرار نیست. فرض کنیم S یک نیم‌گروه باشد و $\ell^1(S)$ مجموعهٔ تمام توابع مختلط مقدار $f : S \to \mathbb{C}$ باشد به‌طوری‌که $\|f\|_1 = \sum_{s\in S} |f(s)| < \infty$. برای هر $f, g \in \ell^1(S)$ ضرب پیچشی f و g به‌صورت زیر تعریف می‌شود

$$(f * g)(r) = \sum_{st=r} f(s)g(t) \qquad (r \in S),$$

و در حالتی که هیچ عضوی مانند s و t یافت نشود که $st = r$ آنگاه $\sum_{st=r} f(s)g(t) = 0$. در این صورت $(\ell^1(S), *, \|\cdot\|_1)$ یک جبر باناخ است که آن را جبر نیم‌گروهی وابسته به S می‌نامیم.

مثال ۱۰.۳. مجموعهٔ اعداد طبیعی $\mathbb{N}$ همراه با عمل

$$m \cdot n = \max\{m, n\}$$

تشکیل یک نیم‌گروه می‌دهد که آن را با نماد $\mathbb{N}_{\max}$ نمایش می‌دهیم. در این صورت جبر نیم‌گروهی $A = \ell^1(\mathbb{N}_{\max})$، A^{**} -دوتصویر نیست. زیرا در غیر این صورت همریختی پیوسته A -دومدولی $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ وجود دارد به‌طوری‌که به ازای هر $a \in A$

$$\pi_{A^{**}} \circ \rho(a) = \kappa_A(a).$$

اگر قرار دهیم $m = \rho(\delta_1)$، آنگاه برای هر $a \in A$ داریم

$$\begin{aligned} a\Psi(m) &= \Psi(am) = \Psi(a\rho(\delta_1)) \\ &= \Psi(\rho(a\delta_1)) = \Psi(\rho(\delta_1 a)) \\ &= \Psi(\rho(\delta_1)a) = \Psi(m)a. \end{aligned}$$

همچنین

$$\begin{aligned} \pi_A^{**}(\Psi(m))a &= \pi_A^{**}(\Psi \circ \rho(\delta_1))a \\ &= \pi_{A^{**}} \circ \rho(\delta_1)a \\ &= \kappa_A(\delta_1)a \\ &= \kappa_A(a). \end{aligned}$$

نتیجه می‌شود که $\Psi(m)$ یک قطر مجازی برای A است و بنابراین A میانگین‌پذیر است. لذا باید $E(\mathbb{N}_{\max}) = E(\mathbb{N})$ مجموعه‌ای متناهی باشد که یک تناقض است. حال ادعا می‌کنیم A، φ-A^{**} -دوتصویر است. همان‌طور که می‌دانیم $\Delta(A) = \{\varphi_n : n \in \mathbb{N}\} \cup \{\varphi_\infty\}$ که در آن

$$\varphi_n(f) = \sum_{i=1}^{n} f(i), \qquad \varphi_\infty(f) = \sum_{i=1}^{\infty} f(i).$$

برای هر $n \in \mathbb{N}$ نگاشت $\rho_n : A \to A^{**}\widehat{\otimes}A^{**}$ را به‌صورت زیر تعریف می‌کنیم:

$$\rho_n(a) = a\mathbf{m} \otimes \mathbf{m}$$

که در آن $\mathbf{m} = \kappa_A(\delta_{n+1} - \delta_n)$. ازآنجاکه $a\mathbf{m} = \varphi_n(a)\mathbf{m}$ بنابراین ρ_n یک همریختی A -مدولی پیوسته است و داریم:

$$\begin{aligned}\widetilde{\varphi_n} \circ \pi_{A^{**}} \circ \rho(a) &= \widetilde{\varphi_n} \circ \pi_{A^{**}}(a\mathbf{m} \otimes \mathbf{m}) \\ &= \widetilde{\varphi_n}(a\mathbf{mm}) \\ &= \varphi(a)\widetilde{\varphi_n}(\mathbf{m}) \\ &= \varphi_n(a).\end{aligned}$$

بنابراین A، φ_n-A^{**} -دوتصویر است. همچنین، اگر قرار دهیم

$$\mathbf{M} = w^* - \lim_n \kappa_A(\delta_n) \in A^{**},$$

به‌راحتی دیده می‌شود ازآنجاکه $a\mathbf{M} = \mathbf{M}a = \varphi_\infty(a)\mathbf{M}$، لذا نگاشت $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ با ضابطهٔ

$$\rho(a) = a\mathbf{M} \otimes \mathbf{M}$$

یک همریختی A -مدولی پیوسته است و داریم:

$$\widetilde{\varphi_\infty} \circ \pi_{A^{**}} \circ \rho(a) = \widetilde{\varphi_\infty}(a\mathbf{M^2}) = \varphi_\infty(a).$$

نتیجه می‌گیریم که A، φ_∞-A^{**} -دوتصویر است.

لائو در سال ۱۹۸۸ کلاس F -جبرها را معرفی کرد [۱۲]. در واقع یک F -جبر یک جبر باناخ است که پیش دوگان یک W^* -جبر M باشد به‌طوری‌که عنصر همانی M یک تابعک خطی ضربی روی A باشد. برای اولین بار لائو میانگین‌پذیری چپ F -جبرها را تعریف و به مطالعهٔ خواص آن پرداخت. نصر اصفهانی در سال ۲۰۰۱ [۱۴] مفهوم میانگین‌پذیری داخلی را برای F -جبرها تعریف کرد و نتایج بسیاری در مورد جبرهای مختلف به دست آورد. یکی از این نتایج این بود که جبر گروهی $L^1(G)$ همواره میانگین‌پذیر داخلی است. جباری در سال ۲۰۱۱ در [۶] مفهوم φ -میانگین‌پذیر داخلی را برای جبرهای باناخ معرفی کرد.

تعریف ۱۱.۳. فرض کنیم A یک جبر باناخ باشد و $\varphi \in \Delta(A)$. جبر A را φ -میانگین‌پذیر داخلی گوییم هرگاه تور کران‌دار (a_α) در A موجود باشد به‌طوری‌که برای هر $a \in A$

$$aa_\alpha - a_\alpha a \to 0, \qquad \varphi(a_\alpha) \to 1.$$

در گزارهٔ زیر به بررسی رابطهٔ بین φ -میانگین‌پذیری و φ-A^{**} -دوتصویری جبرهای باناخ می‌پردازیم.

قضیه ۱۲.۳. فرض کنیم A یک جبر باناخ باشد و $\varphi \in \Delta(A)$ و A، φ-A^{**} -دوتصویر باشد. اگر A، φ -میانگین‌پذیر داخلی باشد، آنگاه A، φ -میانگین‌پذیر چپ و راست است.

اثبات. چون A، φ -میانگین‌پذیر داخلی است لذا تور کران‌دار (a_α) در A وجود دارد به‌طوری‌که برای هر $a \in A$

$$aa_\alpha - a_\alpha a \to 0, \qquad \varphi(a_\alpha) \to 1.$$

قرار می‌دهیم $m_\alpha = \rho(a_\alpha)$ و نگاشت $T : A^{**}\widehat{\otimes}A^{**} \to A^{**}$ را به‌صورت زیر تعریف می‌کنیم:

$$T(F \otimes G) = \widetilde{\varphi}(G)F.$$

اگر $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ نگاشت مدنظر در تعریف φ-A^{**} -دوتصویری باشد، با در نظر گرفتن $N_\alpha = T \circ \rho(a_\alpha)$ خواهیم داشت:

$$\begin{aligned}aN_\alpha - \varphi(a)N_\alpha &= aT \circ \rho(a_\alpha) - \varphi(a)T \circ \rho(a_\alpha) \\ &= T \circ \rho(aa_\alpha) - T \circ \rho(a_\alpha a) \\ &= T \circ \rho(aa_\alpha - a_\alpha a) \to 0.\end{aligned}$$

همچنین ازآنجاکه $\widetilde{\varphi} \circ T = \widetilde{\varphi} \circ \pi_{A^{**}}$ به این نتیجه می‌رسیم که

$$\widetilde{\varphi} \circ T \circ \rho(a_\alpha) = \widetilde{\varphi} \circ \pi_{A^{**}} \circ \rho(a_\alpha) = \varphi(a_\alpha) \to 1.$$

پس A، φ -میانگین‌پذیر چپ است. با استدلال مشابه می‌توان ثابت کرد A، φ -میانگین‌پذیر راست است. □

در ادامه با ذکر مثالی نشان می‌دهیم که در لم قبل شرط φ -میانگین‌پذیری داخلی ضروری است.

مثال ۱۳.۳. فرض کنیم $A = C([۰, ۱])$ فضای تمام توابع پیوسته بر $[۰, ۱]$ با نرم زیر باشد:

$$\|f\|_\infty = \sup\{|f(x)| : x \in [۰, ۱]\}.$$

فضای A همراه با ضرب

$$f \cdot g = g(۰)f,$$

تشکیل جبر باناخ می‌دهد. به‌راحتی می‌توان دید که $\Delta(A)$ یک مجموعهٔ تک عضوی است؛ در واقع $\phi(f) = f(۰)$ تنها مشخصه روی $C([۰, ۱])$ است. ادعا می‌کنیم که جبر A، ϕ -میانگین‌پذیر نیست اما A^{**}-ϕ -دوتصویر است. برای اثبات این ادعا، به برهان خلف اگر A، ϕ -میانگین‌پذیر باشد، آنگاه تور (f_α) در A وجود دارد که

$$f \cdot f_\alpha - \phi(f)f_\alpha \to ۰ \qquad \phi(f_\alpha) = ۱.$$

درنتیجه

$$\phi(f_\alpha)f - \phi(f)f_\alpha = f - \phi(f)f_\alpha \to ۰.$$

بنابراین برای هر $f \in \ker\phi$ می‌توان نتیجه گرفت که $f = ۰$ و لذا $\phi(f)f_\alpha \to f = ۰$ و این بدین معنی است که $\ker\phi = \{۰\}$. ازآنجاکه $\dim(\frac{A}{\ker\phi}) = ۱$ پس $\dim(A) = ۱$ و این یک تناقض است. برای اثبات ادعای دوم نگاشت $\rho : A \to A^{**}\widehat{\otimes}A^{**}$ را به‌صورت زیر تعریف می‌کنیم:

$$\rho(f) = \kappa_A(f) \otimes \kappa_A(۱).$$

در این صورت ρ یک همریختی A -مدولی پیوسته است و داریم:

$$\begin{aligned}\widetilde{\varphi} \circ \pi_{A^{**}} \circ \rho(f) &= \widetilde{\varphi} \circ \pi_{A^{**}}(\kappa_A(f) \otimes \kappa_A(۱)) \\ &= \widetilde{\varphi}(\kappa_A(f \cdot ۱)) \\ &= \phi(f)\phi(۱) \\ &= \phi(f).\end{aligned}$$

پس نتیجه می‌گیریم که A، A^{**}-$\widetilde{\phi}$ -دوتصویر است.

نتیجه ۱۴.۳. فرض کنیم A یک جبر باناخ جابجایی و A^{**}-φ -دوتصویر باشد. در این صورت A، φ -میانگین‌پذیر چپ و راست است.

نتیجه ۱۵.۳. فرض کنیم A یک جبر باناخ دارای یکهٔ تقریبی کران‌دار و A^{**}-φ -دوتصویر باشد. در این صورت A، φ -میانگین‌پذیر چپ و راست است.

در ادامه قصد داریم A^{**}-φ -دوتصویری جبر گروهی را مورد بررسی قرار دهیم. فرض کنید G یک گروه فشردهٔ موضعی با اندازهٔ هار چپ $d\lambda$ و $L^۱(G)$ جبر گروهی وابسته به گروه G با نرم $\|\cdot\|_۱$ و ضرب پیچشی باشد [۴]. همچنین فرض کنید $L^\infty(G)$ جبر توابع کران‌دار اساسی با نرم $\|\cdot\|_\infty$ و $M(G)$ جبر اندازهٔ گروه G باشد [۴]. اگر $\widehat{G}$ مجموعهٔ همهٔ همریختی‌های پیوسته $\xi : G \to \mathbb{T}$ باشد، در این صورت

$$\Delta(L^۱(G)) = \{\varphi_\xi : \xi \in \widehat{G}\},$$

که در آن

$$\varphi_\xi(f) = \int_G \overline{\xi(x)}f(x)d\lambda(x).$$

به مرجع [۴، قضیه ۲۳.۷] مراجعه کنید.

قضیه ۱۶.۳. فرض کنید G یک گروه فشردهٔ موضعی باشد. جبر گروهی $L^۱(G)$، $L^۱(G)^{**}$-φ -دوتصویر است اگر و فقط اگر G یک گروه میانگین‌پذیر باشد.

اثبات. ازآنجاکه $L^1(G)$ همواره دارای یکهٔ تقریبی کران‌دار است درنتیجه $L^1(G)$، φ -میانگین‌پذیر داخلی است و طبق قضیه ۱۲.۳ $L^1(G)$، φ -میانگین‌پذیر چپ است. بنابراین G میانگین‌پذیر است.

برعکس، فرض کنیم G یک گروه میانگین‌پذیر باشد. پس $L^1(G)$، φ -میانگین‌پذیر چپ و راست است. لذا M_1 و M_2 در $L^1(G)^{**}$ وجود دارند که برای هر $a \in L^1(G)$

$$aM_1 = \varphi(a)M_1, \qquad \widetilde{\varphi}(M_1) = 1$$

و

$$M_2 a = \varphi(a)M_2, \qquad \widetilde{\varphi}(M_2) = 1.$$

نگاشت $\rho : L^1(G) \to L^1(G)^{**}\widehat{\otimes}L^1(G)^{**}$ را تعریف می‌کنیم:

$$\rho(a) = aM_1 \otimes M_2.$$

در این صورت داریم:

$$\widetilde{\varphi} \circ \pi_{A^{**}} \circ \rho(a) = \widetilde{\varphi}(aM_1M_2) = \varphi(a).$$

همچنین

$$\rho(ab) = abM_1 \otimes M_2 = \varphi(ab)M_1 \otimes M_2 = \varphi(a)\varphi(b)M_1 \otimes M_2 = a\rho(b),$$

و

$$\begin{aligned}\rho(ab) &= abM_1 \otimes M_2 = \varphi(ab)M_1 \otimes M_2 \\ &= \varphi(a)\varphi(b)M_1 \otimes M_2 = \varphi(a)M_1 \otimes M_2 b \\ &= \rho(a)b.\end{aligned}$$

این ثابت می‌کند که $L^1(G)$، φ-$L^1(G)^{**}$ -دوتصویر است. □

نتیجه ۱۷.۳. فرض کنید G یک گروه فشردهٔ موضعی باشد. جبر اندازهٔ $M(G)$، φ-$M(G)^{**}$ -دوتصویر است اگر و فقط اگر G یک گروه میانگین‌پذیر و گسسته باشد.

اثبات. اگر $M(G)$، φ-$M(G)^{**}$ -دوتصویر باشد، چون $M(G)$ یکدار است بنابر نتیجه ۱۵.۳ $M(G)$، φ -میانگین‌پذیر چپ است و بنابراین طبق [۱۳، نتیجه ۲.۵] G میانگین‌پذیر و گسسته است. برای حالت برعکس، اگر G میانگین‌پذیر و گسسته باشد، آنگاه $M(G) = \ell^1(G)$ و درنتیجه قضیه ۱۶.۳ اثبات را تکمیل می‌کند. □

References

[1] Alaghmandan, M., Nasr-Isfahani, R., & Nemati, M. (2010). Character amenability and contractibility of abstract Segal algebras. *Bull. Austral. Math. Soc*, 82, 274–281. DOI: http://dx.doi.org/10.1017/S0004972710000286.

[2] Ghahramani, F., Loy, R.J., & Willis, G.A. (1996). Amenability and weak amenability of second conjugate Banach algebras. *Proc. Amer. Math. Soc*, 124, 1489–1497. DOI: https://doi.org/10.1090/s0002-9939-96-03177-2.

[3] Helemskii, A.Ya. (1989). The Homology of Banach and Topological Algebras. *Kluwer Academic Publishers, Holland*. DOI: https://doi.org/10.1007/978-94-009-2354-6.

[4] Hewitt. E., & Ross, K.A. (1970). Abstract Harmonic Analysis I, *Springer, Berlin*.

[5] Hu, Z., Monfared, M.S., & Traynor, T. (2009). On character amenable Banach algebras. *Studia Math*, 193, 53–78.

[6] Jabbari, A., Mehdi Abad, T., & Zaman Abadi, M. (2011). On ϕ-inner amenable Banach algebras. *Colloq. Math*, 122, 1–10. DOI: https://doi.org/10.4064/cm122-1-1.

[7] Javanshiri, H., & Nemati, M. (2018). Invariant ϕ-means for abstract Segal algebras related to locally compact groups. *Bull. Belg. Math. Soc. Simon Stevin*, 25, 687–698. DOI: http://dx.doi.org/10.36045/bbms/1547780429.

[8] Johnson, B.E. (1972). Cohomology in Banach algebras. *Mem. Amer. Math. Soc*, 127.

[9] Johnson, B.E. (1972). Approximate diagonals and cohomology of certain annihilator Banach algebras. *Amer. J. Math*, 94, 685–698. DOI: https://doi.org/10.2307/2373751.

[10] Kaniuth, E., Lau, A.T., & Pym, J. (2008). On ϕ-amenability of Banach algebras. *Math. Proc. Cambridge Philos. Soc*, 144, 85–96. DOI: https://doi.org/10.1017/S0305004107000874.

[11] Kaniuth, E., Lau, A.T., & Pym, J. (2008). On character amenability of Banach algebras. *J. Math. Anal. Appl*, 344, 942–955. DOI: https://doi.org/10.1016/j.jmaa.2008.03.037.

[12] Lau, A.T. (1983). Analysis on a class of Banach algebras with applications to harmonic analysis on locally compact groups and semigroups. *Fund. Math*, 118, 161–175. DOI: https://doi.org/10.4064/FM-118-3-161-175.

[13] Monfared, M.S. (2008). Character amenability of Banach algebras. *Math. Proc. Camb. Philos. Soc*, 144, 697–706. DOI: https://doi.org/10.1017/S0305004108001126.

[14] Nasr-Isfahani, R. (2001). Inner amenability of Lau algebras. *Arch. Math*, (Brno) 37, 45–55.

[15] Nasr Isfahani, R., & Soltani Renani, S. (2011). Character contractibility of Banach algebras and homological properties of Banach modules. *Studia Math*, 202, 205–225.

[16] Paterson, A.L.T. (1988). Amenability. *Math. Surveys Monogr, vol. 29, Amer. Math. Soc, Providence, RI*.

[17] Pier, J.P. (1984). Amenability of Locally Compact Groups. *Pure Appl. Math. (N. Y.), John Wiley & Sons, Inc., New York. A Wiley-Interscience Publication*.

[18] Reiter, H. (1971). L^1-algebras and Segal algebras. *Lecture Notes in Mathematics, 231 Springer*. DOI: https://doi.org/10.1007/BFb0060759.

[19] Rostami, M., & Sahami, A. (2023). A^{**}-biprojectivity of Banach algebras. *Measure Algebras and Applications*, 1(1), 128–140. DOI: http://doi.org/10.22091/MAA.2023.9829.1011.

[20] Runde, V. (2002). Lectures on Amenability, Lecture Notes in Mathematics (Volume 1774). *Springer Verlag, Berlin-Heidelberg-New York*. DOI: https://doi.org/10.1007/b82937.

[21] Sahami, A. (2019). On left ϕ-biprojectivity and left ϕ-biflatness of certain Banach algebras. *Politehn. Univ. Bucharest Sci. Bull. Ser. A*, 81, 97–106.

[22] Sahami, A., & Pourabbas, A. (2013). On ϕ-biflat and ϕ-biprojective Banach algebras. *Bull. Belg. Math. Soc. Simon Stevin*, 20, 789–801. DOI: https://doi.org/10.36045/bbms/1385390764.

[23] Zhang, Y. (1999). Nilpotent ideals in a class of Banach algebras. *Proc. Amer. Math. Soc*, 127, 3237–3242. DOI: http://dx.doi.org/10.1090/S0002-9939-99-04896-0.

Measure Algebras and Applications

Is the space of Holder functions predual of L^1?

Azin Golbaharan[1]

1. Kharazmi University, Tehran, Iran. Email: golbaharan@khu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 01 March 2024
Received in revised form:
07 May 2024
Accepted: 21 June 2024
Published Online:
20 August 2024

Keywords:
Lipschitz function,
Little Lipschitz space,
Holder function space,
$\mathrm{L}^1(\mu)$

2020 Mathematics Subject Classification:
47B33, 46J10

ABSTRACT

Let (X, d) be a compact pointed metric space. In this paper, we investigate the condition on the underlying metric space (X, d) which implies that the little Lipschitz space on (X, d) is predual of $\mathrm{L}^1(\mu)$. Then, we conclude that the space of Holder functions on every compact pointed space, and for each $0 < \alpha < 1$ is not predual of $\mathrm{L}^1(\mu)$.

Cite this article: Golbaharan, A. (2024). Is the space of Holder functions predual of L^1?. *Measure Algebras and Applications*, 1(2), 85–91. http://doi.org/10.22091/MAA.2024.10469.1015

Publisher: University of Qom
DOI: 10.22091/MAA.2024.10469.1015

Extended Abstract

Introduction

A metric space (X, d) is pointed if it carries a distinguished element or base point e. Let (X, d_X) and (Y, d_Y) be metric spaces. A map $f : X \to Y$ is Lipschitz if

$$\mathbf{L}(f) = \sup_{\substack{x,x' \in X \\ x \neq x'}} \frac{d_Y(f(x), f(x'))}{d_X(x, x')} < \infty. \tag{0.1}$$

Suppose that (X, d) is a compact pointed metric space. The collection of all Lipschitz functions $f : X \to \mathbb{C}$ with $f(e) = 0$ is called Lipschitz space and is denoted by $\mathrm{Lip}_0(X)$. The usual norm on $\mathrm{Lip}_0(X)$ is defined by (0.1) which gives a Banach space. The little Lipschitz space, $\mathrm{lip}_0(X)$, is the closed subspace of $\mathrm{Lip}_0(X)$ consists of all functions $f : X \to \mathbb{C}$ such that

$$\lim_{d(x,x') \to 0} \frac{|f(x) - f(x')|}{d(x, x')} = 0.$$

We say that $\mathrm{lip}_0(X)$ separates the points of X uniformly if there exists a constant $c > 1$ such that for every $x, y \in X$, some $f \in \mathrm{lip}_0(X)$ satisfies $\mathbf{L}(f) \leq c$ and $|f(x) - f(y)| = d(x, y)$. In the general case, it is possible that $\mathrm{lip}_0(X)$ does not separate points of X uniformly. For each constant $0 < \alpha < 1$ and metric space (X, d), we denote by X^α the same set together with the metric d^α and call it Holder metric space. The Holder space, $\mathrm{lip}_0(X^\alpha)$ separates the points of X uniformly.

Let (X, d) be a metric space. A molecule of X is a function $m : X \to \mathbb{C}$ which is supported on a finite set and which satisfies $\sum_{x \in X} m(x) = 0$. For $x, y \in X$ define the molecule m_{xy} by $m_{xy} = \chi_x - \chi_y$. We denote the set of molecules on X by æ(X) and give it the norm

$$\|m\|_{\mathrm{AE}} = \inf \left\{ \sum_{i=1}^{k} |a_i| d(x_i, y_i) : m = \sum_{i=1}^{k} a_i m_{x_i y_i} \right\}$$

and we let $AE(X)$ be the completion of the space of molecules on X.

We examine the condition on the underlying metric space (X, d) which implies that $\mathrm{lip}_0(X^\alpha)^* = \mathrm{L}^1(\mu)$ for some measure μ on X. Then we conclude that the space of Holder functions on every compact pointed space is not predual of $\mathrm{L}^1(\mu)$.

Conclusion

In this paper, the next theorem and corollary are presented:

***Theorem* 0.1.** *Let (X, d) be a compact pointed metric space. The little Lipschitz space, $\mathrm{lip}_0(X)$ is predual of $\mathrm{L}^1(\mu)$ and $\frac{1}{d(x,e)} m_{xe}$ is an extreme point of the closed unit ball of $\mathrm{lip}_0(X)*$ for all $x \in X \setminus \{e\}$ if and only if for each $x, y \in X$, $d(x, y) = d(x, e) + d(e, y)$.*

***Corollary* 0.2.** *The space of Holder functions on a compact pointed metric space with at least two distinct points of base point is not predual of L^1.*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۹۱-۸۵

آیا فضای توابع هلدر پیش‌دوگان L^1 است؟

آذین گل‌بهاران [۱]

۱. دانشگاه خوارزمی، تهران، ایران. رایانامه: golbaharan@khu. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۲/۱۱
تاریخ بازنگری: ۱۴۰۳/۲/۱۸
تاریخ پذیرش: ۱۴۰۳/۴/۱
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
تابع لیپ‌شیتس،
فضای لیپ‌شیتس کوچک،
فضای توابع هلدر،
$\mathrm{L}^1(\mu)$

رده‌بندی ریاضی:
47B33, 46J10

چکیده

فرض کنیم (X,d) یک فضای متریک فشرده شامل یک نقطهٔ پایه‌ای باشد. در این مقاله بررسی می‌کنیم تحت چه شرطی روی فضای متریک زمینهٔ (X,d) فضای لیپ‌شیتس کوچک، $\mathrm{lip}_0(X)$، پیش‌دوگان $\mathrm{L}^1(\mu)$ است. سپس نتیجه می‌گیریم فضای توابع هلدر بر هر فضای متریک فشردهٔ نقطه‌ای و هر $0 < \alpha < 1$، پیش‌دوگان $\mathrm{L}^1(\mu)$ نیست.

استناد: گل‌بهاران، آذین. (۱۴۰۳). آیا فضای توابع هلدر پیش‌دوگان L^1 است؟. جبرهای اندازه و کاربردها، ۱(۲)، ۹۱-۸۵.
http://doi.org/10.22091/MAA.2024.10469.1015

ناشر: دانشگاه قم.

۱ مقدمه

اگر فضای متریک (X,d) حاوی یک نقطهٔ متمایز باشد آن را فضای متریک نقطه‌ای گوییم و نقطهٔ متمایز آن را نقطهٔ پایه‌ای نامیم. فرض کنیم (X,d_X) و (Y,d_Y) فضاهای متریک باشند. تابع $f:X\to Y$ را لیپ‌شیتس نامیم هرگاه

$$\mathbf{L}(f)=\sup_{\substack{x,x'\in X\\ x\neq x'}}\frac{d_Y(f(x),f(x'))}{d_X(x,x')}<\infty. \tag{۱.۱}$$

فرض کنیم (X,d) یک فضای متریک نقطه‌ای با نقطهٔ پایه‌ای e باشد. گردایهٔ تمام توابع لیپ‌شیتس $f:X\to\mathbb{C}$ را که $f(e)=0$ فضای لیپ‌شیتس نامیده و با نماد $\mathrm{Lip}_0(X)$ نمایش می‌دهیم. تابع $\mathbf{L}(\cdot)$ در (۱.۱)، یک نرم روی $\mathrm{Lip}_0(X)$ تعریف می‌کند که آن را تبدیل به یک فضای باناخ می‌کند. فضای لیپ‌شیتس کوچک، $\mathrm{lip}_0(X)$، زیرفضای بستهٔ $\mathrm{Lip}_0(X)$ متشکل از همهٔ توابع $f:X\to\mathbb{C}$ است که

$$\lim_{d(x,x')\to 0}\frac{|f(x)-f(x')|}{d(x,x')}=0.$$

گوییم فضای لیپ‌شیتس کوچک نقاط X را به‌طور یکنواخت جدا می‌کند هرگاه ثابت $c>1$ یافت شود که به‌ازای هر $x,y\in X$، تابع $f\in\mathrm{lip}_0(X)$، با خاصیت $\mathbf{L}(f)\leq c$ و $|f(x)-f(y)|=d(x,y)$ موجود باشد. در حالت کلی ممکن است فضای لیپ‌شیتس کوچک نقاط X را جدا نکند. به‌عنوان نمونه به‌ازای فضای متریک $X=[0,1]$ مجهز به متر اقلیدسی، $\mathrm{lip}_0(X)$ فقط شامل تابع ثابت صفر خواهد بود. به‌ازای ثابت $0<\alpha<1$ و فضای متریک (X,d) ساختار (X,d^α) مجدداً یک فضای متریک است که آن را فضای هلدر می‌نامیم و به‌اختصار با X^α نمایش می‌دهیم. به‌علاوه $\mathrm{lip}_0(X^\alpha)$ فضای توابع هلدر نامیده می‌شود و همواره نقاط X را به‌طور یکنواخت جدا می‌کند. تابع اسکالر-مقدار m روی فضای متریک (X,d) که دارای تکیه‌گاه متناهی است و $\sum_{x\in X}m(x)=0$، یک ملکول نام دارد. فضای همهٔ ملکول‌های روی X را با $\mathrm{æ}(X)$ نمایش می‌دهیم و نرم زیر را روی آن در نظر می‌گیریم.

$$\|m\|_{\mathrm{AE}}=\inf\left\{\sum_{i=1}^{k}|a_i|d(x_i,y_i):m=\sum_{i=1}^{k}a_i m_{x_iy_i}\right\}$$

که در آن به‌ازای هر $x,y\in X$، $m_{xy}=\chi_x-\chi_y$. فضای ارنس-ایلز، $\mathrm{AE}(X)$، عبارت است از کامل‌شدهٔ فضای نرم‌دار $(\mathrm{æ}(X),\|\cdot\|_{\mathrm{AE}})$. درصورتی‌که (X,d) یک فضای متریک نقطه‌ای فشرده باشد و $\mathrm{lip}_0(X)$ نقاط X را به‌طور یکنواخت جدا کند، $\mathrm{lip}_0(X)^*=\mathrm{AE}(X)$ (قضیه ۳.۳.۳ در [۱]). یک فضای باناخ، پیش‌دوگان $\mathrm{L}^1(\mu)$ نامیده می‌شود، هرگاه بین دوگان نرمی آن و $\mathrm{L}^1(\mu)$، یک عملگر خطی، پوشا و طول‌پا موجود باشد. می‌دانیم که فضای $\mathrm{L}^1(\mu)$ پیش‌دوگان یگانه ندارد و از دیرباز این پرسش که آیا یک فضای باناخ معین پیش‌دوگان $\mathrm{L}^1(\mu)$ است، موضوع پژوهش‌های ریاضی متعددی بوده است. در این مقاله نخست در قضیه‌ای ارتباط بین پاسخ این پرسش دربارهٔ فضای لیپ‌شیتس کوچک و ساختار فضای متریک زمینه را بیان می‌کنیم. سپس نتیجه می‌گیریم فضای توابع هلدر بر هر فضای متریک نقطه‌ای فشرده پیش‌دوگان $\mathrm{L}^1(\mu)$ نیست.

۲ نتایج اصلی

در خلال اثبات قضیهٔ اصلی، به نکته‌ای که در گزارهٔ زیر مطرح می‌شود نیاز داریم.

ملاحظه ۱.۲. اگر f نقطهٔ اکستریم گوی یکهٔ $\mathrm{L}^1(\mu)$ باشد، آنگاه تکیه‌گاه f یک اتم در فضای اندازهٔ (X,μ) است. زیرا در غیر این صورت $E\subset\mathrm{supp}(f)$ یافت می‌شود که $0<\mu(E)<\mu(\mathrm{supp}(f))$ و با در نظر گرفتن $t=\int_E|f|d\mu\in(0,1)$، داریم $\|\frac{1}{t}f\chi_E\|_1=1$ و $\|\frac{1}{1-t}f\chi_{\mathrm{supp}(f)\setminus E}\|_1=1$. به‌علاوه $f=t(\frac{1}{t}f\chi_E)+(1-t)(\frac{1}{t}f\chi_E)$ که با اکستریم بودن f در تناقض است.

اکنون می‌توانیم قضیهٔ اصلی مقاله را به شرح زیر ارائه دهیم.

قضیه ۲.۲. فرض کنیم (X,d) یک فضای متریک فشرده و e نقطهٔ پایه‌ای آن باشد. فضای لیپ‌شیتس کوچک، $\mathrm{lip}_0(X)$، پیش‌دوگان $\mathrm{L}^1(\mu)$ و برای همهٔ نقاط $x\in X\setminus\{e\}$، $\frac{1}{d(x,e)}m_{xe}$ نقطهٔ اکستریم گوی یکهٔ $\mathrm{lip}_0(X)^*$ است اگر و تنها اگر به‌ازای هر دو نقطهٔ متمایز $x,y\in X$، $d(x,y)=d(x,e)+d(e,y)$.

اثبات. ابتدا فرض کنیم μ یک اندازهٔ مثبت روی X و

$$T : \mathrm{lip}_{۰}(X)^{*} \to \mathrm{L}^{۱}(\mu)$$

یکریختی طول‌پا باشد. به‌علاوه فرض کنیم

$$\left\{ \frac{۱}{d(x,e)} m_{xe} : x \in X, x \neq e \right\} \subseteq \mathrm{ext}(\mathrm{lip}_{۰}(X)^{*}).$$

به‌ازای هر $x \in X$ چون T یکریختی طول‌پا است و $\frac{۱}{d(x,e)} m_{xe} \in \mathrm{ext}(\mathrm{lip}_{۰}(X)^{*})$ داریم $T(\frac{۱}{d(x,e)} m_{xe}) \in \mathrm{ext}(\mathrm{L}^{۱}(\mu))$. بنابر ملاحظه ۱.۲ تکیه‌گاه $T(m_{xe})$ یک اتم در فضای اندازهٔ (X, μ) است و ازآنجاکه $\|T(\frac{۱}{d(x,e)} m_{xe})\|_{۱} = ۱$، اتم $E_x \subseteq X$ وجود دارد که

$$T(\frac{۱}{d(x,e)} m_{xe}) = \frac{۱}{\mu(E_x)} \chi_{E_x} \ (a.e.).$$

روشن است که چون T یکریختی است، به‌ازای هر $x, y \in X$، اگر $x \neq y$، آنگاه E_x و E_y متمایز و درنتیجه مجزا هستند. به‌این‌ترتیب به‌ازای هر دو نقطهٔ متمایز $x, y \in X \setminus \{e\}$،

$$\begin{aligned} d(x,y) &= \|m_{xy}\|_{\mathrm{AE}} \\ &= \|T(m_{xy})\|_{۱} \\ &= \|T(m_{xe}) - T(m_{ey})\|_{۱} \\ &= \|\frac{d(x,e)}{\mu(E_x)} \chi_{E_x} - \frac{d(y,e)}{\mu(E_y)} \chi_{E_y}\|_{۱} \\ &= \int_X |\frac{d(x,e)}{\mu(E_x)} \chi_{E_x} - \frac{d(y,e)}{\mu(E_y)} \chi_{E_y}| d\mu \\ &= \int_X \frac{d(x,e)}{\mu(E_x)} \chi_{E_x} + \frac{d(y,e)}{\mu(E_y)} \chi_{E_y} d\mu \\ &= d(x,e) + d(e,y). \end{aligned}$$

برعکس، فرض کنیم

$$d(x,y) = d(x,e) + d(e,y) \qquad (x, y \in X, \ x \neq y).$$

اندازهٔ μ را روی X به‌صورت زیر تعریف می‌کنیم

$$\mu : P(X) \to [۰, \infty]; \qquad \mu(E) = \begin{cases} \sum_{x \in E} d(x,e) & E \neq \emptyset \\ ۰ & E = \emptyset \end{cases}$$

به‌ازای هر $m \in \mathfrak{ae}(X)$ بنابر تعریف، $z_{۱}, \cdots, z_n \in \mathbb{C} \setminus \{۰\}$ وجود دارند که $m(X) = \{z_{۱}, \cdots, z_n\} \cup \{۰\}$ و $z_{۱} + \cdots + z_n = ۰$. به‌علاوه، اگر به‌ازای هر $i \in \{۱, \cdots, n\}$ قرار دهیم $E_i = m^{-۱}(z_i)$ داریم $\cup_{i=۱}^{n} E_i$ زیرمجموعهٔ متناهی X است و $m = \sum_{i=۱}^{n} z_i \chi_{E_i}$. بنابراین

$$\begin{aligned} \|m\|_{۱} &= \int_X |m| d\mu = \sum_{i=۱}^{n} |z_i| \mu(E_i) \\ &= \sum_{i=۱}^{n} |z_i| (\sum_{x \in E_i} d(x,e)) = \sum_{i=۱}^{n} \sum_{x \in E_i} |z_i| d(x,e) \end{aligned}$$

و از طرف دیگر

$$m = \sum_{i=1}^{n} z_i \chi_{E_i} = \sum_{i=1}^{n} z_i \sum_{x \in E_i} \chi_x = \sum_{i=1}^{n} \sum_{x \in E_i} z_i m_{xe}$$

لذا

$$\|m\|_{\mathrm{AE}} \leq \sum_{i=1}^{n} \sum_{x \in E_i} |z_i| d(x,e) \leq \|m\|_1. \tag{۱.۲}$$

برای اثبات نامساوی بالا در جهت عکس، $\epsilon > 0$ را دلخواه در نظر بگیریم. بنابر تعریف نرم $\|.\|_{\mathrm{AE}}$، برای $m \in \mathfrak{ae}(X)$ نقاط $q_k, \cdots, q_1, p_k, \cdots, p_1$ در X و اعداد $a_k, \cdots, a_1$ در $\mathbb{C}$ یافت می‌شوند که $m = \sum_{i=1}^{k} a_i m_{p_i q_i}$ و

$$\sum_{i=1}^{k} |a_i| d(p_i, q_i) < \|m\|_{\mathrm{AE}} + \epsilon.$$

سپس خواهیم داشت

$$\begin{aligned}
\|m\|_1 &= \int_X |\sum_{i=1}^{k} a_i m_{p_i q_i}| d\mu \\
&\leq \sum_{i=1}^{k} |a_i| \int_X |m_{p_i q_i}| d\mu \\
&= \sum_{i=1}^{k} |a_i| \int_X \chi_{p_i} + \chi_{q_i} d\mu \\
&\leq \sum_{i=1}^{k} |a_i| (\mu(\{p_i\}) + \mu(\{q_i\})) \\
&\leq \sum_{i=1}^{k} |a_i| (d(p_i, e) + d(q_i, e)) \\
&= \sum_{i=1}^{k} |a_i| d(p_i, q_i) \\
&< \|m\|_{\mathrm{AE}} + \epsilon.
\end{aligned}$$

به‌این‌ترتیب نتیجه می‌گیریم

$$\|m\|_1 \leq \|m\|_{\mathrm{AE}}. \tag{۲.۲}$$

بر اساس (۱.۲) و (۲.۲)، نگاشت همانی $I : \mathfrak{ae}(X) \to \mathrm{L}^1(\mu)$ یک عملگر خطی طول‌پا و به‌ویژه پیوستهٔ یکنواخت است. لذا دارای یک گسترش پیوسته به کامل‌شدهٔ $\mathfrak{ae}(X)$ یعنی $\mathrm{AE}(X)$ است که آن را با $\tilde{I}$ نمایش می‌دهیم. عملگر $\tilde{I}$ خاصیت طول‌پایی را حفظ می‌کند، زیرا به‌ازای هر $m \in \mathrm{AE}(X)$ دنباله‌ای از اعضای $\mathfrak{ae}(X)$ مانند $\{m_i\}_{i \in \mathbb{N}}$ موجود است که نسبت به نرم $\|.\|_{\mathrm{AE}}$ به m میل می‌کند و خواهیم داشت

$$\begin{aligned}
\|m\|_{\mathrm{AE}} = \lim_{i \to \infty} \|m_i\|_{\mathrm{AE}} &= \lim_{i \to \infty} \|\tilde{I}(m_i)\|_1 \\
&= \| \lim_{i \to \infty} \tilde{I}(m_i)\|_1 = \|\tilde{I}(m)\|_1.
\end{aligned}$$

توجه کنیم که طول‌پایی $\tilde{I}$ بسته بودن برد آن را ایجاب می‌کند در ادامه نشان می‌دهیم $\tilde{I}$ پوشا نیز هست. به‌ازای هر $E \subseteq X$ با شرط $\mu(E) < \infty$ داریم $\sum_{x \in E} d(x,e) = \mu(E) < \infty$، لذا مجموعهٔ E حداکثر شمارش‌پذیر است. پس می‌توان نوشت

$E = \{x_n : n \in \mathbb{N}\}$ که $\sum_{n\in\mathbb{N}} d(x_n, e) = \mu(E) < \infty$. بنابراین در فضای $\mathrm{AE}(X)$ سری $\sum_{n\in\mathbb{N}} m_{x_n e}$ همگرای مطلق و درنتیجه همگرا است، لذا $\chi_E = \sum_{n\in\mathbb{N}} m_{x_n e}$ متعلق به $\mathrm{AE}(X)$ است. به‌ویژه

$$\tilde{I}(\chi_E) = \tilde{I}(\sum_{n\in\mathbb{N}} m_{x_n e}) = \sum_{n\in\mathbb{N}} \tilde{I}(m_{x_n e}) = \sum_{n\in\mathbb{N}} I(m_{x_n e}) = \sum_{n\in\mathbb{N}} m_{x_n e} = \chi_E$$

بنابراین زیرفضای توابع پله‌ای که در $\mathrm{L}^1(\mu)$ چگال است مشمول در زیرفضای بستهٔ $\tilde{I}(\mathrm{AE}(X))$ از $\mathrm{L}^1(\mu)$ است که پوشایی $\tilde{I}$ را ایجاب می‌کند. در انتها به‌ازای هر $x_\circ \in X \setminus \{e\}$ داریم $r_{x_\circ} = d(x_\circ, e) > 0$ و درنتیجه $B(x_\circ, r_{x_\circ}) \cap X = \{x_\circ\}$ و درنتیجه $\chi_{x_\circ} \in \mathrm{lip}_\circ(X)$ به‌علاوه با به کار بردن قضیه ۳.۳۱ در [۱] برای تابع $f_{x_\circ} = d(x_\circ, e)\chi_{x_\circ}$ نتیجه می‌گیریم $\frac{1}{d(x_\circ,e)} m_{x_\circ e}$ یک نقطهٔ اکستریم از گوی یکهٔ $\mathrm{lip}_\circ(X)^* = \mathrm{AE}(X)$ است. □

پاسخ به پرسش اصلی مقاله در نتیجهٔ زیر بیان می‌شود.

نتیجه ۳.۲. فضای توابع هلدر روی یک فضای متریک نقطه‌ای فشرده با حداقل دو نقطهٔ متمایز از نقطهٔ پایه‌ای، پیش‌دوگان $\mathrm{L}^1(\mu)$ نیست.

اثبات. فرض خلف بگیریم فضای توابع هلدر روی فضای متریک نقطه‌ای فشرده (X, d)، که حداقل دو نقطهٔ متمایز از نقطهٔ پایه‌ای دارد، پیش‌دوگان $\mathrm{L}^1(\mu)$ است. توجه کنیم که با یک بررسی مقدماتی چون $0 < \alpha < 1$، به‌ازای هر سه نقطهٔ متمایز $x, y, z \in X$، داریم

$$d(x, z)^\alpha < d(x, y)^\alpha + d(y, z)^\alpha.$$

ازاین‌رو از گزاره ۳.۳۴ در [۱] و قضیه ۳.۳۹ در [۱] نتیجه می‌گیریم

$$\left\{ \frac{1}{d(x, e)} m_{xe} : x \in X, x \neq e \right\} \subseteq \mathrm{ext}(\mathrm{lip}_\circ(X^\alpha)^*).$$

لذا بنابر قضیهٔ بالا،

$$d(x, y)^\alpha = d(x, e)^\alpha + d(e, y)^\alpha \qquad (x, y \in X,\ x \neq y),$$

که ایجاب می‌کند $d(x, e) = 0$ یا $d(y, e) = 0$. در واقع نتیجه می‌گیریم X، حداکثر یک نقطهٔ متمایز از e دارد که با فرض در تناقض است. □

با به کار بردن نتیجه ۳.۳۲ در [۱] به‌جای قضیه ۳.۳۹ در [۱] در برهان نتیجهٔ اخیر، نتیجهٔ زیر حاصل می‌شود.

نتیجه ۴.۲. اگر X یک فضای متریک نقطه‌ای فشرده با حداقل دو نقطهٔ متمایز از نقطهٔ پایه‌ای و قطر حداکثر دو باشد، آنگاه $\mathrm{lip}_\circ(X)$ پیش‌دوگان $\mathrm{L}^1(\mu)$ است اگر و تنها اگر

$$d(x, y) = d(x, e) + d(e, y) \qquad (x, y \in X,\ x \neq y).$$

References

[1] Weaver, N. (2018). Lipschitz Algebras (Second Edition). *World Scientific, Singapore*.

Measure Algebras and Applications

Characterization of frames in terms of R-duals in separable Hilbert spaces

Farkhondeh Takhteh[1]

1. Persian Gulf University, Bushehr, Iran. Email: f.takhteh@pgu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 24 March 2024
Received in revised form:
26 May 2024
Accepted: 21 June 2024
Published Online:
20 August 2024

Keywords:
Hilbert space,
Frame,
R-dual,
Riesz basis

2020 Mathematics Subject Classification:
42C15

ABSTRACT

In this paper, we consider the concept of R-duality with respect to Riesz bases. In particular, we study the concept of R-duality with respect to Riesz bases, constructed by anti-linear operators, for Bessel sequences. Using these anti-linear operators, we give some characterizations for frames and Riesz bases.

Cite this article: Takhteh, F. (2024). Characterization of frames in terms of R-duals in separable Hilbert spaces. *Measure Algebras and Applications*, 1(2), 92–103. http://doi.org/10.22091/maa.2024.10714.1019

Publisher: University of Qom
DOI: 10.22091/maa.2024.10714.1019

Extended Abstract

Introduction

Let $\mathcal{H}$ be a separable Hilbert space. A sequence $\{f_i\}_{i=1}^{\infty}$ in $\mathcal{H}$ is a frame for $\mathcal{H}$ if there exist constants $0 < A \leq B < \infty$ such that

$$A\|f\|^2 \leq \sum_{i=1}^{\infty} |\langle f, f_i\rangle|^2 \leq B\|f\|^2, \quad \forall f \in \mathcal{H}.$$

If only the right-hand side inequality is required, it is called a Bessel sequence. It is called a tight frame if there is a constant $A > 0$ such that

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

It is called a Parseval frame if $A = 1$. It is called a frame sequence if it is a frame for its closed linear span.

Two Bessel sequences $\{f_i\}_{i=1}^{\infty}$ and $\{g_i\}_{i=1}^{\infty}$ are called dual frames if

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

A sequence $\{f_i\}_{i=1}^{\infty}$ in $\mathcal{H}$ is called a Riesz sequence for $\mathcal{H}$ if there exist constants $0 < A \leq B < \infty$ such that

$$A\sum_{i=1}^{\infty} |c_i|^2 \leq \Big\| \sum_{i=1}^{\infty} c_i f_i \Big\|^2 \leq B\sum_{i=1}^{\infty} |c_i|^2,$$

for all $\{c_i\}_{i=1}^{\infty} \in \ell^2(\mathbb{N})$, where A and B are called Riesz bounds. It is called a Riesz basis for $\mathcal{H}$ if $\overline{span\{f_i\}_{i=1}^{\infty}} = \mathcal{H}$.

If $\{f_i\}_{i=1}^{\infty}$ is a Riesz basis, it is well known that $\{f_i\}_{i=1}^{\infty}$ has a unique dual Riesz basis. In the other words, there exists a unique Riesz basis $\{\tilde{f}_i\}_{i=1}^{\infty}$ such that

$$\langle f_i, \tilde{f}_j\rangle = \delta_{i,j}, \quad i, j \in \mathbb{N}.$$

If $\{f_i\}_{i=1}^{\infty}$ has Riesz bounds A, B, then the dual Riesz sequence has bounds $\frac{1}{B}, \frac{1}{A}$.

Frames in Hilbert spaces were introduced by Duffin and Schaeffer [6] in 1952, when they were studying some problems in nonharmonic Fourier series. Frames were popularized after the work of Daubechies, Grossmann and Meyer [5] where the theory of frames was related to wavelets and Gabor systems. Indeed, after this work, frames were studied widely and deeply, particularly in the more specialized context of wavelet frames and Gabor frames, which are two key tools in signal processing, image processing, data compression, and sampling.

Let g be a function in $L^2(\mathbb{R})$ and a, b be two positive constants. The collection $\{E_{mb}T_{na}g\}_{m,n\in\mathbb{Z}}$ where $E_{mb}f(x) = e^{2\pi imbx}f(x)$ and $T_{na}f(x) = f(x - na)$ is called a Gabor frame in $L^2(\mathbb{R})$ if it is a frame for the Hilbert space $L^2(\mathbb{R})$.

Gabor frames, introduced by D. Gabor in 1946, have been extensively studied. One of the most important results for Gabor frames is the Ron-Shen duality principle that precisely characterizes Gabor frames. It states that for every $g \in L^2(\mathbb{R})$ and $a, b > 0$ with $ab \leq 1$, $\{E_{mb}T_{na}g\}_{m,n\in\mathbb{Z}}$ is a frame with bounds A, B for $L^2(\mathbb{R})$ if and only if $\{\frac{1}{\sqrt{ab}}E_{\frac{m}{a}}T_{\frac{n}{b}}g\}_{m,n\in\mathbb{Z}}$ is a Riesz sequence with bounds A, B.

For generalization of the duality principle from Gabor frames to abstract frame theory, the concept of R-duality with respect to orthonormal bases is defined as follows:
Let $(e_j)_{j\in\mathbb{N}}$ and $(h_i)_{i\in\mathbb{N}}$ be orthonormal bases for a separable Hilbert space $\mathcal{H}$. Let $(f_i)_{i\in\mathbb{N}}$ be a sequence such that for every $j \in \mathbb{N}$, $\sum_{i\in\mathbb{N}} |\langle f_i, e_j\rangle|^2 < \infty$ and

$$\omega_j^f = \sum_{i\in\mathbb{N}} \langle f_i, e_j\rangle h_i.$$

The sequence $(\omega_j^f)_{j\in\mathbb{N}}$ is called the R-dual sequence of $(f_i)_{i\in\mathbb{N}}$ with respect to $(e_j)_{j\in\mathbb{N}}$ and $(h_i)_{i\in\mathbb{N}}$.

The R-duality with respect to orthonormal bases is discussed in several papers. In this paper, first, we consider the concept of R-duality with respect to Riesz bases. In particular, for the Bessel sequences, we define the concept of R-duality concerning Riesz bases using an anti-linear map. Using this anti-linear map, we give characterizations of frames and Riesz bases. Also, we give characterizations of frames and Riesz bases in terms of their R-dual sequences with respect to Riesz bases. We show the relation of the R-dual sequence of the sum of Bessel sequences and the sum of the R-dual sequence with respect to Riesz bases. Also, we give some characterizations for sums of frames and sums of Riesz bases. In addition, we generalize some of the results in [2].

Conclusion

The main results of this paper are:

***Definition* 0.1.** *Let $(f_i)_{i\in I}$ be a Bessel sequence for $\mathcal{H}$ and $(h_i)_{i\in I}$ be a Riesz basis. Define the anti-linear operator $M : \mathcal{H} \to \mathcal{H}$ by*

$$M(f) = \sum_{i\in I} \langle f_i, f\rangle h_i. \qquad (0.3)$$

M is a well-defined and bounded anti-linear operator on $\mathcal{H}$. Its adjoint M^* is an anti-linear operator and

$$M^* f = \sum_{i\in I} \langle h_i, f\rangle f_i.$$

***Theorem* 0.2.** *Let $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$ be Riesz bases for $\mathcal{H}$, $(f_i)_{i\in I}$ be a sequence such that $\sum_{i\in I} |\langle f_i, e_j\rangle|^2 < \infty$ for every $j \in I$ and $(\omega_j^f)_{j\in I}$ be the R-dual sequence of $(f_i)_{i\in I}$ with respect to $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$. Then $(f_i)_{i\in I}$ is a frame in $\mathcal{H}$ if and only if $(\omega_j^f)_{j\in I}$ is a Riesz sequence in $\mathcal{H}$.*

***Theorem* 0.3.** *Let $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$ be Riesz bases for $\mathcal{H}$, $(f_i)_{i\in I}$ be a sequence such that $\sum_{i\in I} |\langle f_i, e_j\rangle|^2 < \infty$ for every $j \in I$ and $(\omega_j^f)_{j\in I}$ be the R-dual sequence of $(f_i)_{i\in I}$ with respect to $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$. Then, the following statements are equivalent:*

1. *$(f_i)_{i\in I}$ is a Riesz basis in $\mathcal{H}$.*
2. *$(\omega_j^f)_{j\in I}$ is a Riesz basis in $\mathcal{H}$.*

***Proposition* 0.4.** *Let $(f_i)_{i\in I}$ and $(g_i)_{i\in I}$ be Bessel sequences for $\mathcal{H}$ and $(\omega_j^f)_{j\in I}$ and $(\omega_j^g)_{j\in I}$ be the R-dual sequences of $(f_i)_{i\in I}$ and $(g_i)_{i\in I}$ with respect to Riesz bases $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$, respectively. Then $(\omega_j^f + \omega_j^g)_{j\in I}$ is the R-dual sequence of $(f_i + g_i)_{i\in I}$ with respect to Riesz bases $(e_j)_{j\in I}$ and $(h_i)_{i\in I}$.*

***Corollary* 0.5.** *With the assumptions of Proposition 0.4,*

1. $(f_i + g_i)_{i\in I}$ *is a frame if and only if* $(\omega_j^f + \omega_j^g)_{j\in I}$ *is a Riesz sequence.*
2. $(f_i + g_i)_{i\in I}$ *is a Riesz basis if and only if* $(\omega_j^f + \omega_j^g)_{j\in I}$ *is a Riesz basis.*

***Example* 0.6.** *Let* $\mathcal{H}$ *be a separable Hilbert space and let* $\{e_i\}_{i=1}^{\infty}$ *be an orthonormal basis for* $\mathcal{H}$*. Define* $T : \mathcal{H} \to \mathcal{H}$ *as follows:*

$$T(e_j) = \begin{cases} 2e_j, & j = 2k, \\ e_j, & j = 2k+1. \end{cases}$$

It is easy to see that for each $x \in \mathcal{H}$

$$\|x\| \leq \|Tx\| \leq 2\|x\|. \tag{0.4}$$

Also, $\overline{span\{T(e_i)\}_{i\in I}} = \mathcal{H}$*. Thus,* $\{f_i\}_{i\in I} = \{T(e_i)\}_{i\in I}$ *is a Riesz basis for* $\mathcal{H}$*.*
Consider the following Riesz bases:

$$\{z_i\}_{i\in I} = \{e_1, 3e_2, e_3, e_4, ...\},$$

and

$$\{h_i\}_{i\in I} = \{2e_1, e_2, e_3, e_4, ...\}.$$

A simple calculation implies that the R-dual of $\{f_i\}_{i\in I}$ *with respect to* $\{z_i\}_{i\in I}$ *and* $\{h_i\}_{i\in I}$ *is*

$$\{\omega_j^f\}_{j\in I} = \{2e_1, 6e_2, e_3, 2e_4, e_5, 2e_6, e_7, 2e_8, ...\},$$

which is a Riesz basis for $\mathcal{H}$*.*

***Lemma* 0.7.** *Let* $(f_i)_{i\in I}$ *be a Bessel sequence for* $\mathcal{H}$ *with the synthesis operator* T_f*. Let* $(\omega_j^f)_{j\in I}$ *be the R-dual of* $(f_i)_{i\in I}$ *with respect to Riesz bases* $(e_i)_{i\in I}$ *and* $(h_i)_{i\in I}$*. Then* $h \in (span\{\omega_j^f : j \in I\})^{\perp}$ *if and only if* $(\langle h_i, h\rangle)_{i\in I} \in ker T_f$*.*

***Proposition* 0.8.** *Let* $(f_i)_{i\in I}$ *be a frame sequence for* $\mathcal{H}$*,* $(e_i)_{i\in I}$ *be a Riesz basis and* $(h_i)_{i\in I}$ *be an orthonormal basis for* $\mathcal{H}$*. Let* $(\omega_j^f)_{j\in I}$ *be the R-dual of* $(f_i)_{i\in I}$ *with respect to Riesz bases* $(e_i)_{i\in I}$ *and* $(h_j)_{j\in I}$*. Then* $(\omega_j^f)_{j\in I}$ *is a frame sequence for* $\mathcal{H}$*.*

***Proposition* 0.9.** *Let* $(f_i)_{i\in I}$ *be a Bessel sequence with bound* A_1 *and frame operator* S_f *and* M *be defined as (0.3). Let* $(e_i)_{i\in I}$ *and* $(h_i)_{i\in I}$ *be Riesz bases for* $\mathcal{H}$*. Then the following statements hold.*

1. *If* $(e_i)_{i\in I}$ *is an orthonormal basis for* $\mathcal{H}$ *and* S_ω *is the frame operator of* $(\omega_j^f)_{j\in I}$*, then* $MM^* = S_\omega$*.*
2. *If* $(h_i)_{i\in I}$ *is an orthonormal basis for* $\mathcal{H}$*, then*
   (a) $M^*M = S_f$*.*
   (b) $\left\|\sum_{j\in I} \overline{a_j}\omega_j^f\right\|^2 = \sum_{i\in I} |\langle f, f_i\rangle|^2$*, where* $f = \sum_{j\in I} a_j e_j$*.*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۰۳-۹۲

ساختارسازی قاب‌ها برحسب R-دوگان‌ها در فضاهای هیلبرت جدایی‌پذیر

فرخنده تخته [۱]

۱. گروه ریاضی، دانشگاه خلیج‌فارس، بوشهر، ایران. رایانامه: f. takhteh@pgu. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۱/۵
تاریخ بازنگری: ۱۴۰۳/۳/۶
تاریخ پذیرش: ۱۴۰۳/۴/۱
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
فضای هیلبرت،
قاب،
R-دوگان،
پایهٔ ریس

رده‌بندی ریاضی:
42C15

چکیده

در این مقاله، R-دوگان‌ها نسبت به پایه‌های ریس را در فضاهای هیلبرت مورد مطالعه قرار می‌دهیم. به‌ویژه، برای دنباله‌های بسل با استفاده از یک عملگر مزدوج‌خطی مفهوم R-دوگان‌ها را مورد بررسی قرار می‌دهیم و نتایج و ساختارسازی‌هایی را برای قاب‌ها، پایه‌های ریس و دنباله‌های ریس برحسب R-دوگان‌ها به دست می‌آوریم.

استناد: تخته، فرخنده. (۱۴۰۳). ساختارسازی قاب‌ها برحسب R-دوگان‌ها در فضاهای هیلبرت جدایی‌پذیر. جبرهای اندازه و کاربردها، ۱(۲)، ۱۰۳-۹۲.

http://doi.org/10.22091/maa.2024.10714.1019

ناشر: دانشگاه قم.

۱ مقدمه

فرض کنیم g یک تابع در $L^۲(\mathbb{R})$ و a, b دو عدد مثبت باشند. در این صورت، خانوادهٔ $\{E_{mb}T_{na}g\}_{m,n\in\mathbb{Z}}$ که در آن $E_{mb}f(x) = e^{۲\pi imbx}f(x)$ و $T_{na}f(x) = f(x-na)$ یک قاب گابور نامیده می‌شود اگر آن یک قاب برای فضای هیلبرت $L^۲(\mathbb{R})$ باشد.

قاب‌های گابور در سال ۱۹۴۶ توسط **گابور** [1] در مرجع [۹] معرفی شدند و به‌طور وسیع مورد مطالعه قرار گرفتند، برای نمونه مراجع [۷، ۱۰] را مشاهده کنید.

یکی از نتایج مهم در مورد قاب‌های گابور، اصل دوگانی **رن- شن** [2] است (مرجع [۱۱] را ملاحظه کنید) که دقیقاً قاب‌های گابور را ساختارسازی می‌کند. در واقع، بیان می‌کند که اگر $g \in L^۲(\mathbb{R})$، $a, b > ۰$ با $ab \leq ۱$، در این صورت $\{E_{mb}T_{na}g\}_{m,n\in\mathbb{Z}}$ یک قاب با کران‌های A, B برای $L^۲(\mathbb{R})$ است اگر و فقط اگر $\{\frac{۱}{\sqrt{ab}}E_{\frac{m}{a}}T_{\frac{n}{b}}g\}_{m,n\in\mathbb{Z}}$ یک دنبالهٔ ریس با کران‌های A, B باشد.

برای تعمیم این اصل از قاب‌های گابور در $L^۲(\mathbb{R})$ به قاب‌ها در فضای هیلبرت $\mathcal{H}$، مفهوم یک R-دوگان نسبت به پایه‌های متعامدیکه در [۲] معرفی شد.

فرض کنیم $\{e_j\}_{j\in\mathbb{N}}$ و $\{h_i\}_{i\in\mathbb{N}}$ پایه‌های متعامدیکه برای فضای هیلبرت $\mathcal{H}$ باشند. همچنین فرض کنیم $\{f_i\}_{i\in\mathbb{N}}$ یک دنباله در $\mathcal{H}$ باشد به‌طوری‌که به‌ازای هر $j \in \mathbb{N}$، داشته باشیم $\sum_{i\in\mathbb{N}}|\langle f_i, e_j\rangle|^۲ < \infty$. در این صورت تعریف می‌کنیم $\omega_j^f := \sum_{i\in\mathbb{N}}\langle f_i, e_j\rangle h_i$ و دنبالهٔ $\{\omega_j^f\}_{j\in\mathbb{N}}$ یک R-دوگان $\{f_i\}_{i\in\mathbb{N}}$ نسبت به پایه‌های متعامدیکه $\{e_j\}_{j\in\mathbb{N}}$ و $\{h_i\}_{i\in\mathbb{N}}$ نامیده می‌شود.

مفهوم R-دوگانی نسبت به پایه‌های متعامدیکه در مقالات زیادی مورد توجه قرار گرفته است، مقالات [۲]، [۲]، [۳]، [۴]، [۱۲] و [۱۳] را ملاحظه کنید.

در این مقاله روی مفهوم R-دوگان‌ها نسبت به پایه‌های ریس تمرکز می‌کنیم. به‌ویژه برای دنباله‌های بسل، با استفاده از یک عملگر مزدوج‌خطی (تعریف‌شده در مرجع [۱۳]) دنبالهٔ R-دوگان آن را تعریف می‌کنیم. با استفاده از تکنیک‌های نظریهٔ عملگرها نتایجی را در مورد R-دوگان‌ها به دست می‌آوریم.

۲ تعاریف و مقدمات

در این بخش، مفاهیم و قضایای مورد نیاز را یادآوری می‌کنیم.

تعریف ۱.۲. فرض کنیم $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند. فرض کنیم $\{f_i\}_{i\in I}$ دنباله‌ای در $\mathcal{H}$ باشد به‌طوری‌که برای هر $j \in I$، داشته باشیم $\sum_{i\in I}|\langle f_i, e_j\rangle|^۲ < \infty$. در این صورت، تعریف می‌کنیم $\omega_j^f := \sum_{i\in I}\langle f_i, e_j\rangle h_i$ دنبالهٔ $\{\omega_j^f\}_{j\in I}$ را یک R-دوگان $\{f_i\}_{i\in I}$ نسبت به پایه‌های ریس $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ می‌نامیم.

تعریف ۲.۲. فرض کنید $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل در $\mathcal{H}$ و $\{h_i\}_{i\in I}$ یک پایهٔ ریس باشد. در این صورت، عملگر مزدوج‌خطی $M : \mathcal{H} \to \mathcal{H}$ را به‌صورت

$$M(f) = \sum_{i\in I}\langle f_i, f\rangle h_i \qquad (۱.۲)$$

تعریف می‌کنیم. این عملگر خوش‌تعریف و کران‌دار است. الحاقی M یعنی M^* یک عملگر مزدوج‌خطی به‌صورت زیر است:

$$M^*f = \sum_{i\in I}\langle h_i, f\rangle f_i.$$

ملاحظه ۳.۲. فرض کنیم $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل، $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند. در این صورت، اگر M عملگر تعریف‌شده در (۱.۲) باشد، آنگاه $M(e_j) = \sum_{i\in I}\langle f_i, e_j\rangle h_i$، لذا $\omega_j^f = M(e_j)$ پس $\{M(e_j)\}_{j\in I}$، یک R-دوگان $\{f_i\}_{i\in I}$ نسبت به $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ است.

قضیهٔ زیر، الگوریتمی را معرفی می‌کند که $\{f_i\}_{i\in I}$ را برحسب یک R-دوگانش نسبت به پایه‌های ریس نمایش دهد (مراجع [۲، ۱۵] را ملاحظه کنید).

[1] Gabor
[2] Ron-Shen

قضیه ۴.۲. فرض کنیم $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند و $\{f_i\}_{i\in I}$ دنباله‌ای در $\mathcal{H}$ باشد به‌طوری‌که برای هر $j \in I$ داشته باشیم $\sum_{i\in I} |\langle f_i, e_j\rangle|^2 < \infty$. در این صورت، شرایط زیر برقرار هستند:

(الف) برای هر $i \in I$ داریم:

$$f_i = \sum_{j\in I} \langle \omega_j^f, \widetilde{h_i}\rangle \widetilde{e_j},$$

که در آن، $\{\widetilde{e_j}\}_{j\in I}$ و $\{\widetilde{h_i}\}_{i\in I}$ به‌ترتیب دوگان‌های کانونی $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ هستند.

(ب) $\{f_i\}_{i\in I}$ یک R-دوگان $\{\omega_j^f\}_{j\in I}$ نسبت به $\{\widetilde{h_i}\}_{i\in I}$ و $\{\widetilde{e_j}\}_{j\in I}$ است.

قضیه ۵.۲. فرض کنیم $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل با کران A باشد، $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند و M را عملگر تعریف‌شده در (۱.۰) در نظر می‌گیریم. فرض کنیم $\{\omega_j^f\}_{j\in I}$ یک R-دوگان $\{f_i\}_{i\in I}$ نسبت به $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ باشد. در این صورت، $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ بسل در $\mathcal{H}$ است. علاوه‌بر این، گزاره‌های زیر معادل هستند:

(۱) $R(M)$ (برد M) بسته است و M یک‌به‌یک است.

(۲) M از پایین کران‌دار است.

(۳) $\{f_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ است.

قضیه ۶.۲. فرض کنیم $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل و $\{h_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ باشد. در این صورت، عملگر مزدوج‌خطی $M : \mathcal{H} \to \mathcal{H}$ (تعریف‌شده در (۱.۰)) وارون‌پذیر است اگر و فقط اگر $\{f_i\}_{i\in I}$ یک پایهٔ ریس باشد.

۳ نتایج اصلی

قضیهٔ زیر یک ساختارسازی برای قاب برحسب R-دوگان آن نسبت به پایه‌های ریس ارائه می‌دهد.

قضیه ۱.۳. فرض کنید $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند و $\{f_i\}_{i\in I}$ دنباله‌ای باشد به‌طوری‌که برای هر $j \in I$ داشته باشیم $\sum_{i\in I} |\langle f_i, e_j\rangle|^2 < \infty$. همچنین فرض کنید $\{\omega_j^f\}_{j\in I}$ دنبالهٔ R-دوگان $\{f_i\}_{i\in I}$ نسبت به پایه‌های ریس $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ باشد. در این صورت $\{f_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ است اگر و فقط اگر $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ ریس برای $\mathcal{H}$ باشد.

اثبات. فرض کنید $\{f_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ باشد و M عملگر مزدوج‌خطی (۱.۰) باشد. در این صورت بنابر قضیه ۵.۲، M یک عملگر مزدوج‌خطی از پایین کران‌دار است. پس اعداد ثابت مثبت A_1 و A_2 وجود دارند به‌طوری‌که

$$A_1\|f\|^2 \le \|M(f)\|^2 \le A_2\|f\|^2 \quad \forall f \in \mathcal{H}.$$

فرض کنید $0 < A_1' \le A_2'$ کران‌های ریس برای $\{e_j\}_{j\in I}$ و $\mathcal{F}$ یک زیرمجموعهٔ متناهی از I باشد. بنابراین خواهیم داشت:

$$\begin{aligned}\left\|\sum_{j\in\mathcal{F}} a_j\omega_j^f\right\|^2 = \left\|\sum_{j\in\mathcal{F}} a_j M(e_j)\right\|^2 &= \left\|M\Big(\sum_{j\in\mathcal{F}} \overline{a_j} e_j\Big)\right\|^2 \\ &\le A_2\left\|\sum_{j\in\mathcal{F}} \overline{a_j} e_j\right\|^2 \\ &\le A_2A_2'\sum_{j\in\mathcal{F}} |a_j|^2\end{aligned}$$

درنتیجه $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ ریس برای $\mathcal{H}$ است (A_1A_1' کران پایین است).

برعکس، فرض کنید $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ ریس با کران‌های ریس $0 < A_1 \leq A_2$ برای $\mathcal{H}$ باشد. همچنین فرض کنید $0 < B_1 \leq B_2$ و $0 < C_1 \leq C_2$ به‌ترتیب کران‌های ریس برای $\{e_i\}_{i\in I}$ و $\{h_i\}_{i\in I}$ باشند. اگر $f \in span\{e_k\}_{k\in I}$، آنگاه زیرمجموعهٔ متناهی F از I و ثابت‌های $\{c_j : j \in F\}$ موجود هستند به‌طوری‌که $f = \sum_{j\in F} c_j e_j$. بنابراین خواهیم داشت:

$$\begin{aligned}
\sum_{i\in I} |\langle f_i, f\rangle|^2 = \sum_{i\in I} \left|\sum_{j\in F} \langle f_i, c_j e_j\rangle\right|^2 &\leq \frac{1}{C_1} \left\|\sum_{i\in I}\sum_{j\in F} \langle f_i, c_j e_j\rangle h_i\right\|^2 \\
&= \frac{1}{C_1} \left\|\sum_{j\in F} \overline{c_j} \sum_{i\in I} \langle f_i, e_j\rangle h_i\right\|^2 \\
&= \frac{1}{C_1} \left\|\sum_{j\in F} \overline{c_j}\omega_j^f\right\|^2 \\
&\leq \frac{A_2}{C_1} \sum_{j\in F} |c_j|^2 \\
&\leq \frac{A_2}{B_1 C_1} \left\|\sum_{j\in F} c_j e_j\right\|^2 = \frac{A_2}{B_1 C_1}\|f\|^2.
\end{aligned}$$

با اثباتی مشابه خواهیم داشت:

$$\sum_{i\in I} |\langle f_i, f\rangle|^2 \geq \frac{A_1}{B_2 C_2}\|f\|^2.$$

چون $\mathcal{H} = \overline{span\{e_k\}_{k\in I}}$ نتیجه می‌شود $\{f_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ است. □

قضیه ۲.۳. فرض کنید $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ دو پایهٔ ریس برای $\mathcal{H}$ باشند و $\{f_i\}_{i\in I}$ دنباله‌ای در $\mathcal{H}$ باشد به‌طوری‌که برای هر $j \in I$، $\sum_{i\in I} |\langle f_i, e_j\rangle|^2 < \infty$. همچنین فرض کنید $\{\omega_j^f\}_{j\in I}$ دنبالهٔ R-دوگان $\{f_i\}_{i\in I}$ نسبت به $\{h_i\}_{i\in I}$ و $\{e_j\}_{j\in I}$ باشد. در این صورت عبارت‌های زیر معادل هستند:

۱. $\{f_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است.

۲. $\{\omega_j^f\}_{j\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است.

اثبات. (۱) $\Leftarrow$ (۲). فرض کنید $\{f_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ باشد. بنابر قضیه ۱.۳، $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ ریس برای $\mathcal{H}$ است. برای کامل شدن برهان، کافی است ثابت کنیم $\{\omega_j^f\}_{j\in I}$ در $\mathcal{H}$ کامل است. برای این منظور فرض کنید، $h \in \mathcal{H}$ و برای هر $j \in I$ داشته باشیم $\langle h, \omega_j^f\rangle = 0$. حال برای هر $j \in I$ خواهیم داشت:

$$0 = \langle h, \omega_j^f\rangle = \left\langle h, \sum_{i\in I} \langle f_i, e_j\rangle h_i\right\rangle = \left\langle e_j, \sum_{i\in I} \langle h_i, h\rangle f_i\right\rangle.$$

چون $\{e_i\}_{i\in I}$ در $\mathcal{H}$ کامل است، پس $\sum_{i\in I} \langle h_i, h\rangle f_i = 0$. اما $\{f_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است، درنتیجه برای هر $i \in I$، $\langle h_i, h\rangle = 0$. از کامل بودن $\{h_i\}_{i\in I}$ نتیجه می‌شود $h = 0$.

(۲) $\Leftarrow$ (۱). فرض کنید $\{\omega_j^f\}_{j\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ باشد. بنابر قضیه ۱.۳، $\{f_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ است. برای کامل کردن برهان، کافی است نشان دهیم اگر $\{c_i\}_{i\in I} \in \ell^2(I)$ و $\sum_{i\in I} c_i f_i = 0$، آنگاه برای هر $i \in I$ داریم $c_i = 0$. ازآنجایی‌که $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ است، پس $\{\omega_j^f\}_{j\in I}$ نیز یک دنبالهٔ بسل برای $\mathcal{H}$ است. بنابر ملاحظه ۳.۲، $\{f_i\}_{i\in I} = \{M_1(\widetilde{h_i})\}_{i\in I}$ که $M_1 : \mathcal{H} \to \mathcal{H}$ به‌صورت زیر است:

$$M_1(g) = \sum_{j\in I} \langle \omega_j^f, g\rangle \widetilde{e_j}. \tag{۱.۳}$$

از پیوستگی M_1 نتیجه می‌شود

$$\sum_{i\in I} c_i f_i = M_1\left(\sum_{i\in I} \overline{c_i}\widetilde{h_i}\right) = 0.$$

بنابر قضیه ۶.۲، M_1 یک عملگر وارون‌پذیر است. بنابراین $\sum_{i\in I} \overline{c_i}\widetilde{h_i} = 0$. حال چون $\{\widetilde{h_i}\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است، برای هر $i \in I$ نتیجه می‌شود $c_i = 0$. □

ملاحظه ۳.۳. در قضیه ۲.۳، اگر $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل باشد، می‌توانیم برهان ساده‌تری برای آن ارائه دهیم. چون $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ است، $\{\omega_j^f\}_{j\in I}$ نیز یک دنبالهٔ بسل برای $\mathcal{H}$ است. فرض کنید M_1 عملگر مزدوج‌خطی تعریف‌شده در (۱.۳) باشد. برای هر $g \in \mathcal{H}$ خواهیم داشت:

$$M_1(g) = \sum_{j\in I}\langle \omega_j^f, g\rangle \widetilde{e_j} = \sum_{j\in I}\langle M(e_j), g\rangle \widetilde{e_j} = \sum_{j\in I}\langle M^*(g), e_j\rangle \widetilde{e_j} = M^*(g).$$

درنتیجه $M_1 = M^*$. بنابر قضیه ۶.۲، $\{f_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است اگر و فقط اگر M_1 یک عملگر وارون‌پذیر باشد. چون $M_1 = M^*$ وارون‌پذیری M_1 و M باهم معادل هستند. بازهم بنابر قضیه ۶.۲، وارون‌پذیری M معادل با این است که $\{\omega_j^f\}_{j\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است.

مثال ۴.۳. فرض کنید $\{e_i\}_{i\in I}$ یک پایهٔ متعامدیکه برای $\mathcal{H}$ باشد. عملگر $T : \mathcal{H} \to \mathcal{H}$ را به‌صورت زیر تعریف می‌کنیم:

$$T(e_j) = \begin{cases} 2e_j, & j = 2k, \\ e_j, & j = 2k+1 \end{cases}$$

برای هر $x \in \mathcal{H}$ رابطهٔ زیر برقرار است:

$$\|x\| \le \|Tx\| \le 2\|x\|. \qquad (2.3)$$

همچنین $\overline{span\{T(e_i)\}_{i\in I}} = \mathcal{H}$. پس دنبالهٔ $\{f_i\}_{i\in I} = \{T(e_i)\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است. اکنون پایه‌های ریس

$$\{z_i\}_{i\in I} = \{e_1, 3e_2, e_3, e_4, ...\}$$

و

$$\{h_i\}_{i\in I} = \{2e_1, e_2, e_3, e_4, ...\}$$

را در نظر بگیرید. با انجام محاسبات ساده‌ای می‌توان دید که دنبالهٔ R-دوگان $\{f_i\}_{i\in I}$ برحسب $\{z_i\}_{i\in I}$ و $\{h_i\}_{i\in I}$ دنبالهٔ

$$\{\omega_j^f\}_{j\in I} = \{2e_1, 6e_2, e_3, 2e_4, e_5, 2e_6, e_7, 2e_8, ...\}$$

است که یک پایهٔ ریس برای $\mathcal{H}$ است.

گزاره ۵.۳. فرض کنید $\{f_i\}_{i\in I}$ و $\{g_i\}_{i\in I}$ دو دنبالهٔ بسل برای $\mathcal{H}$ باشند و $\{\omega_j^f\}_{j\in I}$ و $\{\omega_j^g\}_{j\in I}$ به‌ترتیب R-دوگان‌های $\{f_i\}_{i\in I}$ و $\{g_i\}_{i\in I}$ نسبت به پایه‌های ریس $\{e_j\}_{j\in I}$ $\{h_i\}_{i\in I}$ باشند. در این صورت $\{\omega_j^f + \omega_j^g\}_{j\in I}$ R-دوگان $\{f_i + g_i\}_{i\in I}$ نسبت به پایه‌های ریس $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ است.

اثبات. $\{f_i + g_i\}_{i\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ است. زیرا کافی است ثابت کنیم عملگر ترکیب آن یک عملگر خطی کران‌دار از $\ell^2(I)$ به $\mathcal{H}$ است. برای این منظور فرض کنید A و B به‌ترتیب کران‌های بسل برای $\{f_i\}_{i\in I}$ و $\{g_i\}_{i\in I}$ باشند. برای هر $\{c_k\} \in \ell^2(I)$ خواهیم داشت:

$$\begin{aligned} \left\|\sum_{k\in I} c_k(f_k + g_k)\right\| &= \left\|\sum_{k\in I} c_k f_k + \sum_{k\in I} c_k g_k\right\| \\ &\le \left\|\sum_{k\in I} c_k f_k\right\| + \left\|\sum_{k\in I} c_k g_k\right\| \\ &\le (\sqrt{A} + \sqrt{B})\left(\sum_{k\in I} |c_k|^2\right)^{\frac{1}{2}}. \end{aligned}$$

بنابراین $\{f_i + g_i\}_{i\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ است.
حال برای هر $j \in I$ خواهیم داشت:

$$\sum_{i\in I}\langle f_i + g_i, e_j\rangle h_i = \sum_{i\in I}\langle f_i, e_j\rangle h_i + \sum_{i\in I}\langle g_i, e_j\rangle h_i = \omega_j^f + \omega_j^g.$$

درنتیجه حکم ثابت می‌شود. □

نتیجه ۶.۳. با فرض‌های گزاره ۵.۳، نتایج زیر برقرار هستند:

(۱) $\{f_i + g_i\}_{i\in I}$ یک قاب برای $\mathcal{H}$ است اگر و فقط اگر $\{\omega_j^f + \omega_j^g\}_{j\in I}$ یک دنبالهٔ ریس برای $\mathcal{H}$ باشد.

(۲) $\{f_i + g_i\}_{i\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است اگر و فقط اگر $\{\omega_j^f + \omega_j^g\}_{j\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ باشد.

گزاره ۷.۳. فرض کنید $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل با کران A_1 و عملگر قاب S_f باشد. همچنین فرض کنید $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ پایه‌های ریس برای $\mathcal{H}$ باشند و عملگر M به‌صورت (۱.۰) تعریف شود. اگر $\{\omega_j^f\}_{j\in I}$ R-دوگان دنبالهٔ $\{f_i\}_{i\in I}$ نسبت به $\{e_j\}_{j\in I}$ و $\{h_j\}_{j\in I}$ باشد، در این صورت عبارت‌های زیر برقرار هستند:

(۱) اگر $\{e_j\}_{j\in I}$ یک پایهٔ متعامدیکه برای $\mathcal{H}$ باشد و S_ω عملگر قاب $\{\omega_j^f\}_{j\in I}$ باشد، آنگاه $MM^* = S_\omega$.

(۲) اگر $\{h_i\}_{i\in I}$ یک پایهٔ متعامدیکه برای $\mathcal{H}$ باشد، آنگاه $M^*M = S_f$ و با فرض $f = \sum_{j\in I} a_j e_j$ خواهیم داشت:

$$\left\|\sum_{j\in I}\overline{a_j}\omega_j^f\right\|^2 = \sum_{i\in I}|\langle f, f_i\rangle|^2.$$

اثبات. برای هر $f \in \mathcal{H}$، داریم:

$$\begin{aligned} S_\omega(f) = \sum_{j\in I}\langle f, \omega_j^f\rangle\omega_j^f &= \sum_{j\in I}\langle f, M(e_j)\rangle M(e_j) \\ &= M\left(\sum_{j\in I}\langle M(e_j), f\rangle e_j\right) \\ &= M\left(\sum_{j\in I}\langle M^*f, e_j\rangle e_j\right) = MM^*f. \end{aligned}$$

برای هر $f \in \mathcal{H}$، داریم:

$$\begin{aligned} M^*M(f) &= \sum_{l\in I}\left\langle h_l, \sum_{i\in I}\langle f_i, f\rangle h_i\right\rangle f_l = \sum_{l\in I}\sum_{i\in I}\langle h_l, h_i\rangle\langle f, f_i\rangle f_l \\ &= \sum_{i\in I}\langle f, f_i\rangle f_i = S(f). \end{aligned}$$

بنابراین برای هر $f \in \mathcal{H}$، رابطهٔ زیر برقرار است:

$$\langle M^*M(f), f\rangle = \langle S(f), f\rangle.$$

درنتیجه

$$\|M(f)\|^2 = \langle S(f), f\rangle = \sum_{i\in I}|\langle f, f_i\rangle|^2.$$

اکنون اگر $f = \sum_{j\in I} a_j e_j$، پیوستگی M نتیجه می‌دهد:

$$\begin{aligned}\left\|\sum_{j\in I} \overline{a_j}\omega_j^f\right\|^2 &= \left\|\sum_{j\in I} \overline{a_j} M(e_j)\right\|^2 = \left\|M\left(\sum_{j\in I} a_j e_j\right)\right\|^2 = \|M(f)\|^2 \\ &= \sum_{i\in I} |\langle f, f_i\rangle|^2.\end{aligned}$$

□

لم ۸.۳. فرض کنید $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ با عملگر ترکیب T_f باشد. همچنین فرض کنید $\{\omega_j^f\}_{j\in I}$ R-دوگان دنبالهٔ $\{f_i\}_{i\in I}$ نسبت به پایه‌های ریس $\{e_j\}_{j\in I}$ و $\{h_i\}_{i\in I}$ باشد. در این صورت $h \in (span\{\omega_j^f : j \in I\})^\perp$ اگر و فقط اگر داشته باشیم $\{\langle h_i, h\rangle\}_{i\in I} \in kerT_f$.

اثبات. برای هر $j \in I$، خواهیم داشت:

$$0 = \langle h, \omega_j^f\rangle = \langle h, M(e_j)\rangle = \langle e_j, M^*(h)\rangle = \left\langle e_j, \sum_{i\in I}\langle h_i, h\rangle f_i\right\rangle.$$

چون $\{e_j\}_{j\in I}$ یک پایهٔ ریس برای $\mathcal{H}$ است، پس $\overline{span\{e_i\}_{i\in I}} = \mathcal{H}$. درنتیجه $\left\langle e_j, \sum_{i\in I}\langle h_i, h\rangle f_i\right\rangle = 0$ اگر و فقط اگر $\sum_{i\in I}\langle h_i, h\rangle f_i = 0$ و از این نتیجه می‌شود $(\langle h_i, h\rangle)_{i\in I} \in kerT_f$. □

گزاره ۹.۳. فرض کنید $\{f_i\}_{i\in I}$ یک دنبالهٔ قاب، $\{e_j\}_{j\in I}$ یک پایهٔ ریس و $\{h_i\}_{i\in I}$ یک پایهٔ متعامدیکه برای $\mathcal{H}$ باشند. اگر $\{\omega_j^f\}_{j\in I}$ دنبالهٔ R-دوگان دنبالهٔ $\{f_i\}_{i\in I}$ نسبت به $\{e_j\}_{j\in I}$ و $\{h_j\}_{j\in I}$ باشد، آنگاه $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ قاب برای $\mathcal{H}$ است.

اثبات. چون $\{f_i\}_{i\in I}$ یک دنبالهٔ بسل نیز برای $\mathcal{H}$ هست، پس بنابر قضیه ۵.۲، $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ بسل برای $\mathcal{H}$ است. فرض کنید $f \in \overline{span(\omega_j^f)_{j\in I}}$. چون $\{h_i\}_{i\in I}$ یک پایهٔ متعامدیکه برای $\mathcal{H}$ است، پس بنابر لم ۸.۳ داریم $\{\langle h_i, f\rangle\}_{i\in I} \in kerT_f{}^\perp$. فرض کنید D_1 یک کران پایین قاب برای $\{f_i\}_{i\in I}$ و B_1 کران پایین ریس برای $\{e_j\}_{j\in I}$ باشد. در این صورت خواهیم داشت:

$$\begin{aligned}\sum_{j\in I} |\langle \omega_j^f, f\rangle|^2 &= \sum_{j\in I} |\langle M(e_j), f\rangle|^2 = \sum_{j\in I} |\langle M^*(f), e_j\rangle|^2 \\ &\geq B_1\|M^*(f)\|^2 = B_1\left\|\sum_{i\in I}\langle h_i, f\rangle f_i\right\|^2 \\ &\geq B_1 D_1 \sum_{i\in I} |\langle h_i, f\rangle|^2 = B_1 D_1 \|f\|^2.\end{aligned}$$

بنابراین $\{\omega_j^f\}_{j\in I}$ یک دنبالهٔ قاب برای $\mathcal{H}$ است. □

References

[1] Casazza, P., Kutyniok, G., & Lammers, M.C. (2004). Duality principles in frame theory. *J. Fourier Anal. Appl*, 10, 383–408. DOI: https://doi.org/10.1007/s00041-004-3024-7.

[2] Casazza, P., Kutyniok, G., & Lammers, M.C. (2005). Duality principle, localization of frames, and Gabor theory, Optics and photonics. *International Society for Optics and Photonics*. DOI: https://doi.org/10.1117/12.615440.

[3] Christensen, O., Kim, H.O., & Kim, R.Y. (2011). On the duality principle by Casazza, Kutyniok, and Lammers. *J. Fourier Anal. Appl*, 17, 640–655. DOI: https://doi.org/10.1007/s00041-010-9151-4.

[4] Chuang, Z., & Zhao, J. (2015). On equivalent conditions of two sequences to be R-dual. *Journal of Inequalities and Applications*, 10, 1–8. DOI: https://doi.org/10.1186/s13660-014-0529-8.

[5] Daubechies, I., Grossmann, A., & Meyer, Y. (1986). Painless nonorthogonal expansions. *J. Math. Phys*, 27, 1271–1286. DOI: https://doi.org/10.1063/1.527388.

[6] Duffin, R.J., & Schaeffer, A.C. (1952). A class of nonharmonic Fourier series. *Trans. Am. Math. Soc*, 72, 341–366. DOI: https://doi.org/10.2307/1990760.

[7] Feichtinger, H.G., & Grochenig, K. (1997). Gabor frames and Time-Frequency Analysis of Distributions. *Journal of Functional Analysis*, 146, 464–495. DOI: https://doi.org/10.1006/jfan.1996.3078.

[8] Folland, G.B. (1994). A Course in Abstract Harmonic Analysis. *CRC Press*. DOI: https://doi.org/10.1201/b19172.

[9] Gabor, D. (1946). Theory of communications. *J. Inst. Elec. Eng*, 93, 429–457.

[10] Gröchenig, K. (2001). Foundation of time-frequency analysis. *Birkhäuser, Boston*. DOI: https://doi.org/10.1007/978-1-4612-0003-1.

[11] Ron, A., & Shen, Z. (1997). Weyl-Heisenberg frames and Riesz bases in $L_2(\mathbb{R})$. *Duke Math. J*, 89, 237–282. DOI: https://doi.org/10.1215/S0012-7094-97-08913-4.

[12] Stoeva, D.T., & Christensen, O. (2015). On R-duals and the duality principle in Gabor analysis. *J. Fourier Anal. Appl*, 21, 383–400. DOI: https://doi.org/10.1007/s00041-014-9376-8.

[13] Takhteh, F. (2023). Some results on R-duals in Hilbert spaces. *Measure Algebras and Applications*, 1(1), 13–21. DOI: http://doi.org/10.22091/MAA.2023.9523.1008.

[14] Wexler, J., & Raz, S. (1990). Discrete Gabor expansions. *Signal Proc*, 21, 207–220. DOI: https://doi.org/10.1016/0165-1684(90)90087-F.

[15] Xiao, X.M., & Zhu, Y.C. (2009). Duality principle of frames in Banach spaces. *Acta. Math. Sci. Ser. A. Chin*, 29, 94–102.

Measure Algebras and Applications

Scalable g-frames and piecewise scalable frames in Hilbert spaces

Mohammad Reza Farmani[1]✉, **Amir Khosravi**[2]

1. Corresponding Author, Faculty of Mathematical Sciences and Computer, Kharazmi University, 599 Taleghani Ave., Tehran 15618, Iran. Email: mr.farmanis@gmail.com
2. Faculty of Mathematical Sciences and Computer, Kharazmi University, 599 Taleghani Ave., Tehran 15618, Iran. Email: khosravi@khu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 03 April 2024
Received in revised form:
16 June 2024
Accepted: 22 June 2024
Published Online:
20 August 2024

Keywords:
G-frame,
Scalable frame,
Piecewise scalable frame,
Orthogonal projection

2020 Mathematics Subject Classification:
42C15

ABSTRACT

In this paper, we generalize the concept of scalability to g-frames, introduce scalable g-frames, obtain some characterizations for them, and demonstrate that scalability is stable under unitary operators and isomorphisms between two Hilbert spaces. In addition, we consider and study the piecewise scalability of frames in Hilbert spaces. In particular, we present some necessary and sufficient conditions for the piecewise scalability of frames in H, and we will extend this concept to the tensor product of Hilbert spaces.

Cite this article: Farmani, M.R., & Khosravi, A. (2024). Scalable g-frames and piecewise scalable frames in Hilbert spaces. *Measure Algebras and Applications*, 1(2), 104–118. http://doi.org/10.22091/maa.2024.10904.1021

Publisher: University of Qom
DOI: 10.22091/maa.2024.10904.1021

Extended Abstract

Introduction

Hilbert space frames were originally introduced by Duffin and Schaeffer to deal with some problems in non-harmonic Fourier analysis [9], [8]. Frames can be viewed as redundant bases which are generalizations of Riesz bases [2], [4], [6], [1], [12],[14]. This redundancy property sometimes is extremely important in some applications such as signal and image processing, data compression, and sampling theory.

In recent years, in [13], Kutyniok et al. introduced scalable frames and provided characterizations for them. Here, we extended this concept to g-frames and applied some of their results to g-frames. We also consider the Paley-Wiener perturbation of g-frames and obtain some results for scaling operators that preserve the g-frame property. Moreover, we achieve some results regarding preserving the g-frame property of a g-frame and its Paley Wiener perturbations.
We recover by the formula

$$f = S^{-1}S(f) = \sum_{j\in J}\langle f, f_j\rangle S^{-1}f_j = \sum_{j\in J}\langle f, S^{-\frac{1}{2}}f_j\rangle S^{-\frac{1}{2}}f_j, \qquad (f \in H).$$

It follows that $\{S^{-\frac{1}{2}}f_j\}_{j\in J}$ is a Parseval frame. This requires inverting the frame operator which might be difficult.

Since a frame is $A-$tight if and only if $Sf = Af$ for all $f \in H$, Parseval frames are the most desirable since $S = I$. So we want to alter a frame in a simple manner to make it Parseval.

Conclusion

In this paper, the following definitions and results are stated:

***Definition* 0.1.** *A g-frame $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ for H with respect to $\{H_j : j \in J\}$ is scalable, if there exist scalars $c_j \geq 0$, $j \in J$, such that $\{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ is a Parseval g-frame. If, in addition, $c_j > 0$, for all $j \in J$, then $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ is said to be positively scalable. If there exists $\delta > 0$, such that $c_j \geq \delta$, for all $j \in J$, then $\{\Lambda_j \in B(H, H_j) : j \in J\}$ is referred to as strictly scalable.*

***Remark* 0.2.** *We note that we can define scalability for every sequence $\{x_i : i \in I\}$ and also for scaling constants $\{c_i : i \in I\} \subseteq \mathbb{C}$, but in frame theory we deal with frames and try to get a reconstruction formula. Also since for every sequence $C = \{c_i : i \in I\} \subseteq \mathbb{C}$*

$$S_C(x) = S_{|C|}(x),$$

for each $x \in H$, then $\{c_i x_i : i \in I\}$ is a frame (Parseval frame) if and only if $\{|c_i|x_i : i \in I\}$ is a frame (Parseval frame). Hence we consider $c_i \geq 0$ for each $i \in I$.

***Proposition* 0.3.** *Let $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ be a g-frame with frame operator S_Λ, analysis operator T^*_Λ, $\{c_j\}_{j\in J} \subseteq \mathbb{R}^+$ and $\Gamma = \{c_j\Lambda_j \in B(H, H_j) : j \in J\}$. Then the following conditions are equivalent:*

(i) Γ *is a g-frame.*
(ii) $ranT_\Lambda^* \subset domD_c$ *and* $D|_{ranT_\Lambda^*}$ *is* ICR.
Moreover, in this case, the g-frame operator of the g-frame Γ *is given by*

$$S_\Gamma = \overline{T_\Lambda D_c} D_c T_\Lambda^*,$$

where $\overline{T_\Lambda D_c}$ *denotes the closure of the operator* $T_\Lambda D_c$.

***Proposition* 0.4.** *Let* $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ *be a g-frame for* H. *Then* $\Gamma = \{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ *is a g-frame if and only if* $D|_{ranT_\Lambda^*}$ *is a bounded* ICR*-operator.*

***Proposition* 0.5.** *Let* $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ *be a g-frame with frame operator* S_Λ *and analysis operator* T_Λ^*. *Consequently, the following conditions are equivalent:*

(i) Λ *is (positively, strictly) scalable.*

(ii) There exists a non-negative (positive, strictly positive, respectively) diagonal operator D *in* $\oplus_{j\in J} H_j$ *such that*

$$\overline{T_\Lambda D}(DT_\Lambda^*) = I_H.$$

We provide a highly useful implication of Proposition 2.2, which shows that scalability is stable under unitary transformations.

***Corollary* 0.6.** *Let* H *and* K *be Hilbert spaces,* $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ *be a g-frame and* $U \in B(K, H)$ *be an isomorphism, i.e.,* $UU^* = I_H$ *and* $U^*U = I_K$. *Then* Λ *is scalable if and only if* $\Lambda U = \{\Lambda_j U \in B(K, H_j) : j \in J\}$ *is scalable*

***Definition* 0.7.** *Let* $\{x_i : i \in I\} \subseteq H$ *be a frame for* H. *We say that* $\{x_i : i \in I\}$ *is a piecewise scalable frame if there exist orthogonal projections* $P_1, ..., P_m$ *on* H, *which are mutually orthogonal,* $\sum_{j=1}^m P_j = I$ *and scaling constants* $\{a_i^1, ..., a_i^m : i \in I\} \subseteq \mathbb{R}^{\geq 0}$ *such that* $\{a_i^1 P_1(x_i) + ... + a_i^m P_m(x_i) : i \in I\}$ *is a Parseval frame. Sometimes we call it* $\mathcal{P}$*-piecewise, if* $\mathcal{P} := \{P_1, ..., P_m\}$.

Throughout the paper, for every $j \in [m]$, we take $H_j = P_j(H)$. Note that the scalable frames are piecewise scalable. It is not difficult to find piecewise scalable frames which are not scalable. For more details, see [4].

***Theorem* 0.8.** $X = \{x_i : i \in I\} \subseteq H$ *is piecewise scalable with orthogonal projections* $P_1, ..., P_m$ *and scaling constants* $\{a_i^j : i \in I, j \in [m]\}$ *if and only if* $\{P_j x_i : i \in I\}$ *is a scalable frame for* H_j *with scaling constants* $\{a_i^j : i \in I\}$, *for each* $j \in [m]$ *and for every* $x \in H$,

$$\sum_{i\in I} \sum_{k\neq j,k,j=1}^{m} a_i^j a_i^k Re[\langle x, P_j x_i\rangle \overline{\langle x, P_k x_i\rangle}] = 0.$$

***Corollary* 0.9.** *Let* $X = \{x_i : i \in I\}$ *be a piecewise scalable frame with projections* $P_1, ..., P_m$. *Then the sequence* $\{P_j x_i : i \in I, j \in [m]\}$ *is a scalable frame for* H.

***Proposition* 0.10.** *Let* $X = \{x_i : i \in I\}$ *be a frame for* H. *If there exist orthogonal projections* $P_1, ..., P_m$ *on* H *which are mutually orthogonal* $\sum_{j\in[m]} P_j = I$ *and a partition* $P = \{\sigma_1, \sigma_2, ..., \sigma_m\}$ *of* I *such that* $\{P_j x_i : i \in \sigma_j\}$ *is a scalable frame for* H_j, *for each* $j \in [m]$, *then* X *is piecewise scalable.*

***Theorem* 0.11.** *Let $\{x_i : i \in I\} \subseteq H$ be a frame for H and P_j be an orthogonal projection on H for each $j \in [m]$ with $\sum_{j=1}^{m} P_j = I$. Then the following statements are equivalent:*
(1) $\{x_i : i \in I\}$ is a piecewise scalable frame for H with scaling constants $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$.
(2) $\sum_{1 \leq k \neq j \leq m} T_k^* D_k D_j T_j = 0$, where D_j is a diagonal operator on $\ell_2(I)$ with diagonal elements $\{a_i^j : i \in I\}$ for each $j \in [m]$.

***Theorem* 0.12.** *Let H and K be two separable Hilbert spaces. Then $X = \{x_i : i \in I\}$ is a piecewise scalable frame for H if and only if $UX = \{Ux_i : i \in I\}$ is a piecewise scalable frame for K, for every unitary operator $U : H \to K$.*

***Proposition* 0.13.** *Let $X = \{x_i : i \in I\}$ be a frame for finite-dimensional Hilbert space H. If X is piecewise scalable with orthogonal projections $P_1, ..., P_m$ on H and scaling constants $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$, then*

$$dimH = \sum_{j \in [m]} dimH_j = \sum_{j \in [m]} \sum_{i \in I} (a_i^j)^2 \|P_j(x_i)\|^2.$$

***Proposition* 0.14.** *Let $\chi = \{x_i : i \in I\}$ be a piecewise scalable unit norm frame for a finite dimensional Hilbert space H with orthogonal projections $P_1, ..., P_m$ and scaling constants $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$. Then*
(i) $\sum_{i \in I} \min\{(a_i^j)^2 : j \in [m]\} \leq dim(H)$,
(ii) $dim(H) \leq \sum_{i \in I} \max\{(a_i^j)^2 : j \in [m]\}$.

***Theorem* 0.15.** *Let $\chi = \{x_i : i \in I\} \subseteq H$ be a frame for H and $\{y_j : j \in J\}$ be an A-tight frame for K. Then, χ is a piecewise scalable frame for H with orthogonal projections $P_1, ..., P_m$ and constants $\{a_i^1, ..., a_i^m : i \in I\}$ if and only if $\{x_i \otimes y_j : i \in I, j \in J\}$ is a piecewise scalable frame for $H \otimes K$ with orthogonal projections $P_1^{'} = P_1 \otimes I_K, ..., P_m^{'} = P_m \otimes I_K$ and constants $\{\frac{1}{\sqrt{A}} a_i^1, ..., \frac{1}{\sqrt{A}} a_i^m : i \in I\}$.*

***Corollary* 0.16.** *Let $\{x_i : i \in I\}$ be a λ-tight frame for H. Then $\{y_j : j \in J\}$ is a piecewise scalable frame for K with orthogonal projections $Q_1, ..., Q_m$ and constants $\{b_j^1, ..., b_j^m : j \in J\}$ if and only if $\{x_i \otimes y_j : i \in I, j \in J\}$ is a piecewise scalable frame for $H \otimes K$ with orthogonal projections $I_H \otimes Q_1, ..., I_H \otimes Q_m$ and constants $\{\frac{1}{\sqrt{\lambda}} b_j^1, ..., \frac{1}{\sqrt{\lambda}} b_j^m : j \in J\}$.*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۱۸-۱۰۴

G-قاب‌های مقیاس‌پذیر و قاب‌های تکه‌ای مقیاس‌پذیر روی فضاهای هیلبرت

محمدرضا فرمانی [۱]✉، امیر خسروی [۲]

۱. نویسندهٔ مسئول، گروه ریاضی، دانشگاه خوارزمی، تهران، ایران. رایانامه: mr.farmanis@gmail.com
۲. گروه ریاضی، دانشگاه خوارزمی، تهران، ایران. رایانامه: khosravi@khu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۱/۱۵
تاریخ بازنگری: ۱۴۰۳/۳/۲۷
تاریخ پذیرش: ۱۴۰۳/۴/۲
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
$g-$ قاب،
قاب مقیاس‌پذیر،
قاب تکه‌ای مقیاس‌پذیر،
تصویر متعامد

رده‌بندی ریاضی:
42C15

چکیده

در این مقاله، مفهوم مقیاس‌پذیری قاب‌ها را به $g-$قاب‌ها تعمیم خواهیم داد و برخی از نتایج آن‌ها را در $g-$ قاب‌ها ارائه می‌کنیم. علاوه‌بر این، با یافتن شرایط خاص، این نوع $g-$قاب‌ها را دسته‌بندی خواهیم کرد. سرانجام نشان خواهیم داد که مقیاس‌پذیری تحت عملگرهای یکانی و یکریختی‌های بین دو فضای هیلبرت ناوردا است. علاوه‌بر این، قاب‌های تکه‌ای مقیاس‌پذیر را روی فضاهای هیلبرت دلخواه تعریف می‌نماییم و برخی از نتایج را در فضاهای هیلبرت دلخواه و در فضاهای هیلبرت با بعد متناهی تعمیم می‌دهیم. در ادامه یک شرط لازم و کافی برای مشخصه‌سازی قاب‌های تکه‌ای مقیاس‌پذیر ارائه می‌دهیم. نهایتاً، شرایطی که موجب می‌شود این مفهوم در فضای حاصلضرب تانسوری فضاهای هیلبرت دلخواه برقرار شود، را مورد مطالعه قرار می‌دهیم.

استناد: فرمانی، محمدرضا.، خسروی، امیر. (۱۴۰۳). G-قاب‌های مقیاس‌پذیر و قاب‌های تکه‌ای مقیاس‌پذیر روی فضاهای هیلبرت. جبرهای اندازه و کاربردها، ۱(۲)، ۱۱۸-۱۰۴.

http://doi.org/10.22091/maa.2024.10904.1021

ناشر: دانشگاه قم.

۱ تاریخچه و تعاریف

قاب‌ها در فضاهای هیلبرت برای اولین بار توسط دافین و شفر در حل برخی از مسائل آنالیز هارمونیک غیرهمساز معرفی و مورد استفاده قرار گرفتند [۹]، [۸]. قاب‌ها، در حقیقت توسیع‌یافتهٔ پایه‌های فضاهای برداری هستند، که می‌توان آن را به پایه‌های ریس تعمیم داد. مراجع [۲]، [۴]، [۶]، [۱]، [۱۲]، [۱۴] را ببینید. از خاصیت قاب‌ها در حل برخی از مسائل کاربردی مانند پردازش سیگنال و تصویر، فشرده‌سازی داده‌ها و نظریهٔ نمونه‌گیری که دارای اهمیت بسیاری است، مورد استفاده قرار می‌گیرد. در سال‌های اخیر، قاب‌های پارسوال و $g-$قاب‌های پارسوال در بسیاری از مسائل مخابرات نقش بسزا و سودمندی ایفا می‌کنند. لذا کوتینیوک، کاسازا و همکارانش در [۱۳] قاب‌های مقیاس‌پذیر را معرفی کردند و برخی از خواص آن‌ها را مورد بررسی قرار دادند. ما نیز در این مقاله، مفهوم مقیاس‌پذیری را به $g-$قاب‌ها تعمیم خواهیم داد و برخی از نتایج آن‌ها را در $g-$ قاب‌ها ارائه می‌کنیم. علاوه‌بر این، با یافتن شرایط خاص، این نوع $g-$قاب‌ها را دسته‌بندی خواهیم کرد. سرانجام نشان خواهیم داد که مقیاس‌پذیری تحت عملگرهای یکانی و یکریختی‌های بین دو فضای هیلبرت ناوردا است. ابتدا تعاریف و قضایایی از مقیاس‌پذیری $g-$قاب‌ها را ارائه می‌دهیم. با استفاده از فرمول بازسازی قاب‌ها خواهیم داشت:

$$f = S^{-1}S(f) = \sum_{j\in J}\langle f, f_j\rangle S^{-1}f_j = \sum_{j\in J}\langle f, S^{-\frac{1}{2}}f_j\rangle S^{-\frac{1}{2}}f_j, \qquad (f \in H).$$

که در این صورت $\{S^{-\frac{1}{2}}f_j\}_{j\in J}$ یک قاب پارسوال است. یکی از راه‌هایی که بتوانیم یک قاب را به‌سادگی تجزیه‌وتحلیل کنیم این است که از فرمول بازسازی استفاده نماییم و برای این کار در برخی از مسائل نیازمند به دست آوردن وارون عملگر قاب هستیم، در مواردی به دست آوردن آن ما را دچار مشکل می‌کند. لذا با قرار دادن ضرایبی در عناصر قاب، آن را به یک قاب پارسوال (قاب $A-$تنگ) تبدیل می‌نماییم زیرا می‌دانیم که یک قاب $A-$تنگ است اگر و تنها اگر به‌ازای هر $f \in H$، $Sf = Af$ و یا در حالت مطلوب‌تر آن، قاب پارسوال است زیرا $S = I$. به همین دلیل مفهوم مقیاس‌پذیری قاب‌ها به وجود آمد.

تعریف ۱.۱. یک $g-$قاب $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ در H را نسبت به $\{H_j : j \in J\}$، $g-$قاب مقیاس‌پذیر گویند، اگر به‌ازای هر $j \in J$ $c_j \geq 0$ وجود داشته باشد به‌طوری‌که $\{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ به یک $g-$قاب پارسوال تبدیل شود. علاوه‌بر این، اگر به‌ازای هر $j \in J$ $c_j > 0$، آن را $g-$قاب مقیاس‌پذیر مثبت گویند. درصورتی‌که $\delta > 0$ ای موجود باشد که به‌ازای هر $j \in J$ $c_j \geq \delta$، $\{\Lambda_j \in B(H, H_j) : j \in J\}$ را $g-$ قاب مقیاس‌پذیر اکیداً مثبت نامند.

تذکر ۲.۱. توجه شود که تعریف مقیاس‌پذیری را می‌توان برای هر دنباله مانند $\{x_i : i \in I\}$ با ضرایبی از $\{c_i : i \in I\} \subseteq \mathbb{C}$ بیان نمود، ولی بنابر تعریف عملگر قاب، به‌ازای هر دنبالهٔ $C = \{c_i : i \in I\} \subseteq \mathbb{C}$ داریم

$$S_C(x) = S_{|C|}(x), \qquad (x \in H).$$

درنتیجه $\{c_ix_i : i \in I\}$ یک قاب (قاب پارسوال) است اگر و تنها اگر $\{|c_i|x_i : i \in I\}$ یک قاب (قاب پارسوال) باشد. بنابراین به‌ازای هر $i \in I$، فرض می‌کنیم $c_i \geq 0$.

مثال ۳.۱. فرض کنیم H یک فضای هیلبرت جدایی‌پذیر و $\{f_j : j \in J\}$ قابی مقیاس‌پذیر در H باشد. فرض کنیم Λ_{f_j} تابعک القایی توسط f_j باشد، یعنی

$$\Lambda_{f_j}f = \langle f, f_j\rangle, \qquad (f \in H).$$

به‌آسانی می‌توان بررسی کرد که $\{\Lambda_{f_j} : j \in J\}$، $g-$ قاب مقیاس‌پذیر نسبت به $\mathbb{C}$ است.

واضح است که مقیاس‌پذیری مثبت و اکیداً مثبت برای $g-$قاب‌های با تعداد متناهی عضو معادل هستند. علاوه‌بر این، هر ضریب $g-$قاب مانند $\{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ از $g-$قاب $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$ به‌طوری‌که $|J| < \infty$ و ضرایب مثبت c_j، نیز $g-$قاب است. در حالت نامتناهی این امر ممکن است اتفاق نیفتد. فرض کنیم $\{e_j : j \in J\}$ پایهٔ متعامد $\oplus_{j\in J}H_j$ باشد. عملگر قطری

$$D = D_c : \oplus_{j\in J}H_j \to \oplus_{j\in J}H_j$$

متناظر با دنبالهٔ اسکالری $c = \{c_j\}_{j\in J}$ را به‌صورت زیر تعریف می‌کنیم:

$$D_c\{x_j\}_{j\in J} = \{c_jx_j\}_{j\in J}, \qquad \{x_j\}_{j\in J} \in domD_c,$$

که در آن

$$domD_c := \{\{x_j\}_{j\in J} \in \oplus_{j\in J} H_j : \{c_j x_j\}_{j\in J} \in \oplus_{j\in J} H_j\},$$

یک عملگر خوش‌تعریف است. عملگر D_c خودالحاق است اگر و تنها اگر به‌ازای هر $j \in J$، $c_j \in \mathbb{R}$. دامنه، هسته و برد عملگر خطی T را به‌ترتیب با نمادهای $domT$، $kerT$ و $ranT$ نمایش می‌دهیم. علاوه‌بر این، عملگری خطی، یک‌به‌یک و با برد بسته T بین دو فضای H و K را به‌اختصار با نماد ICR (یا $ICR-$عملگر) نمایش می‌دهیم. به‌عبارت‌دیگر، $\delta > 0$ وجود داشته باشد، به‌طوری‌که به‌ازای هر $x \in domT$، $\|Tx\| \geq \delta\|x\|$. می‌دانیم که عملگر تحلیل هر $g-$قاب، یک عملگر ICR است. همچنین، اگر عملگر D_c از پایین کران‌دار باشد، آنگاه D_c یک یکریختی [1] است.

لم ۴.۱. فرض کنیم $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$قاب و $\{c_j\}_{j\in J} \subseteq \mathbb{R}^+$.
آ) اگر $D_c\Lambda$، $g-$قاب پارسوال باشد، آنگاه به‌ازای هر $x \in H$

$$x = \sum_{j\in J} c_j^2 \Lambda_j^* \Lambda_j(x).$$

ب) اگر $\{c_j^2\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$دوگان Λ باشد، آنگاه Λ مقیاس‌پذیر است.

اثبات. آ) فرض کنیم $x \in H$. چون $\{c_j\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$قاب پارسوال است، در این صورت

$$x = \sum_{j\in J} (c_j\Lambda_j)^*(c_j\Lambda_j)(x) = \sum_{j\in J} c_j^2 \Lambda_j^*\Lambda_j(x).$$

ب) اگر $x \in H$، آنگاه

$$x = \sum_{j\in J} (c_j^2\Lambda_j)^*\Lambda_j(x) = \sum_{j\in J} (c_j\Lambda_j)^*(c_j\Lambda_j)(x).$$

بنابراین $g-$قاب $\{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ یک قاب پارسوال و لذا Λ مقیاس‌پذیر است.

□

تذکر ۵.۱. توجه داشته باشید، Λ، $g-$قاب مقیاس‌پذیر با دنبالهٔ اسکالری $c = \{c_j\}_{j\in J}$ است اگر و تنها اگر $\{c_j^2\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$ دوگان Λ باشد وقتی‌که $c = \{c_j\}_{j\in J}$ کران‌دار باشد.

در گزارهٔ بعدی رابطهٔ بین عملگر قاب، عملگر تحلیل و قطری با مقیاس‌پذیری $g-$قاب را بیان می‌کنیم.

گزاره ۶.۱. فرض کنیم $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$قاب با عملگر قاب S_Λ، عملگر تحلیل T_Λ^*، $\{c_j\}_{j\in J} \subseteq \mathbb{R}^+$ و $\Gamma := \{c_j\Lambda_j \in B(H, H_j) : j \in J\}$. در این صورت، احکام زیر هم‌ارزند.
آ) Γ، $g-$قاب است.
ب) $ranT_\Lambda^* \subset domD_c$ و $D|_{ranT_\Lambda^*}$، عملگر ICR است.
در این حالت، عملگر $g-$قاب Γ از رابطهٔ زیر به دست می‌آید

$$S_\Gamma = \overline{T_\Lambda D_c} D_c T_\Lambda^*,$$

که در آن $\overline{T_\Lambda D_c}$ نماد بستار عملگر $T_\Lambda D_c$ است.

اثبات. (ب $\Rightarrow$ آ) فرض کنیم Γ، $g-$قاب باشد. آنگاه برای هر $f \in H$

$$T_\Gamma^* f = \{(c_j\Lambda_j)(f)\}_{j\in J} = D_c\{\Lambda_j f\}_{j\in J} = D_c T_\Lambda^* f.$$

درنتیجه $T_\Gamma^* = D_c T_\Lambda^*$. همچنین

$$S_\Gamma = T_\Gamma T_\Gamma^* = (D_c T_\Lambda^*)^* D_c T_\Lambda^*,$$

[1] isomorphism

چون روی $dom(D_c)$ رابطهٔ $(D_cT_\Lambda^*)^* = T_\Lambda D_c$ برقرار است. از سوی دیگر، $dom(D_c)$ در $\oplus H_j$ چگال است و $(D_cT_\Lambda^*)^*$ عملگری کران‌دار است، پس $T_\Gamma^* = D_cT_\Lambda^*$ کران‌دار است. درنتیجه $(D_cT_\Lambda^*)^*$ بستار $T_\Lambda D_c$ است. بنابراین

$$S_\Gamma = \overline{T_\Lambda D_c} D_c T_\Lambda^*.$$

(آ $\Rightarrow$ ب) فرض کنیم، $ranT_\Lambda^* \subseteq domD_c$ و $D_c|_{ranT_\Lambda^*}$، ICR–عملگر باشد. چون Λ، g–قاب است، بنابراین T_Λ^*، ICR است. به‌خصوص، با برد بسته است. بنابر قضیهٔ گراف بسته $D_c|_{ranT_\Lambda^*}$ عملگر کران‌دار است و چون $D_c|_{ranT_\Lambda^*}$، ICR–عملگر است، می‌توان نتیجه گرفت که ثابت‌های $A', B' > ۰$ وجود دارند به‌طوری‌که

$$A'\|g\| \leq \|D_cg\| \leq B'\|g\|, \qquad (g \in ranT_\Lambda^*).$$

اگر A، B کران‌های $g-$ قاب $\{\Lambda_j \in B(H, H_j) : j \in J\}$ باشند، آنگاه

$$A\|f\|^۲ \leq \|T_\Lambda^* f\|^۲ \leq B\|f\|^۲, \qquad (f \in H).$$

درنتیجه به‌ازای هر $f \in H$ داریم:

$$\begin{aligned} AA'^۲\|f\|^۲ &\leq A'^۲\|T_\Lambda^* f\|^۲ \leq \|D_cT_\Lambda^*(f)\|^۲ \\ &\leq B'^۲\|T_\Lambda^* f\|^۲ \leq BB'^۲\|f\|^۲, \qquad (f \in H). \end{aligned}$$

لذا

$$AA'^۲\|f\|^۲ \leq \|T_\Gamma^*(f)\|^۲ \leq BB'^۲\|f\|^۲, \qquad (f \in H).$$

و به دنبال آن Γ، g–قاب است. علاوه‌بر این

$$S_\Gamma = (D_cT_\Lambda^*)^*(D_cT_\Lambda^*) = \overline{T_\Lambda D_c} D_c T_\Lambda^*.$$

□

گزاره ۷.۱. فرض کنید $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$، یک g–قاب در H نسبت به $\{H_j : j \in J\}$ باشد. در این صورت $\Gamma = \{c_j\Lambda_j \in B(H, H_j) : j \in J\}$ یک g–قاب است اگر و تنها اگر $D_c|_{ranT_\Lambda^*}$ یک عملگر ICR کران‌دار باشد.

اثبات. فرض کنیم Λ، $g-$ قاب با کران‌های $A, B > ۰$ باشد. درنتیجه برای هر $f \in H$

$$\sqrt{A}\|f\| \leq \|T_\Lambda^* f\| \leq \sqrt{B}\|f\|.$$

اگر Γ، g–قاب با کران‌های $A', B' > ۰$ باشد، آنگاه به‌ازای هر $f \in H$

$$\sqrt{A'}\|f\| \leq \|T_\Gamma^* f\| = \|D_cT_\Lambda^*(f)\| \leq \sqrt{B'}\|f\|.$$

پس برای هر $f \in H$

$$\begin{aligned} \frac{\sqrt{A'}}{\sqrt{B}}\|T_\Lambda^*(f)\| &\leq \sqrt{A'}\|f\| \leq \|D_cT_\Lambda^*(f)\| \\ &\leq \frac{\sqrt{B'}}{\sqrt{A}}\|T_\Lambda^*(f)\|, \end{aligned}$$

بنابراین $D|_{ranT_\Lambda^*}$ یک عملگر ICR کران‌دار است.

برعکس، اگر $D|_{ranT_\Lambda^*}$، $ICR-$ عملگر کران‌دار باشد، آنگاه ثابت‌های $A'', B'' > ۰$ وجود دارند به‌طوری‌که به‌ازای هر $f \in H$

$$A''\|T_\Lambda^*(f)\| \leq \|D_cT_\Lambda^*(f)\| = \|T_\Gamma^*(f)\| \leq B''\|T_\Lambda^* f\|.$$

درنتیجه

$$\begin{aligned} A''\sqrt{A'}\|f\| &\leq A''\|T_\Lambda^*(f)\| \leq \|T_\Gamma^*(f)\| \\ &\leq B''\|T_\Lambda^*(f)\| \leq B''\sqrt{B'}\|f\|, \end{aligned}$$

و نتیجه به دست می‌آید. □

ما اکنون یک شرط هم‌ارز به‌ظاهر بدیهی را برای مقیاس‌پذیری بیان می‌کنیم، که بیان و اثبات آن در حالت کلی در فضاهای هیلبرت دلخواه تفکیک‌پذیر آسان نیست.

گزاره ۸.۱. فرض کنیم $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$ قاب با عملگر قاب S_Λ و عملگر تحلیل T_Λ^* باشد. در این صورت، گزاره‌های زیر هم‌ارز هستند.

آ) Λ، $g-$قاب مقیاس‌پذیر (مثبت، اکیداً مثبت) است.

ب) عملگر قطری نامنفی (مثبت، اکیداً مثبت) D در $\oplus_{j\in J}H_j$ وجود دارد به‌طوری‌که

$$\overline{T_\Lambda D}(DT_\Lambda^*) = I_H.$$

اثبات. (ب $\Rightarrow$ آ) فرض کنیم Λ $g-$قاب مقیاس‌پذیر با دنبالهٔ اسکالرهای $\{c_j\}_{j\in J} \subset \mathbb{R}^+$ باشد. بنابراین $\Gamma = \{c_j\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$قاب پارسوال است. درنتیجه، بنابر گزاره ۶.۱، $ranT_\Lambda^* \subset domD_c$ و $S_\Gamma = \overline{T_\Lambda D_c}(D_cT_\Lambda^*)$ عملگر $g-$قاب Γ است. چون عملگر $g-$قاب پارسوال، عملگر همانی است، پس

$$\overline{T_\Lambda D_c}(D_cT_\Lambda^*) = I_H.$$

(آ $\Rightarrow$ ب) فرض کنیم، D عملگری قطری نامنفی در $\oplus_{j\in J}H_j$ باشد، به‌طوری‌که

$$\overline{T_\Lambda D_c}(D_cT_\Lambda^*) = I_H.$$

آنگاه DT_Λ^* روی H قابل تعریف است. به‌خصوص، $ranT_\Lambda^* \subset domD$. می‌دانیم که چون Λ یک $g-$قاب است پس T_Λ^* عملگری کران‌دار و از پایین نیز کران‌دار است همچنین D عملگری کران‌دار و $D\mid_{ranT_\Lambda^*}$ از پایین کران‌دار است پس DT_Λ^* عملگری کران‌دار است و از پایین کران‌دار است.

از سوی دیگر

$$\|x\|^2 = \langle x, x\rangle = \langle (T_\Lambda D)^*(DT_\Lambda^*)x, x\rangle = \|DT_\Lambda^*x\|^2, \qquad (x \in H).$$

پس DT_Λ^* ایزومتری است. درنتیجه DT_Λ^* عملگری ICR است.

فرض کنیم $\{c_j\}_{j\in J}$ دنبالهٔ اسکالری نامنفی باشد، به‌طوری‌که $D = D_c$. از گزاره ۶.۱ نتیجه می‌شود که $\Gamma = \{c_j\Lambda_j\}_{j\in J}$، $g-$ قاب با عملگر قاب $S_\Gamma = I_H$ است. درنتیجه g $\Gamma-$قاب پارسوال است.

اثبات‌های مثبت و اکیداً مقیاس‌پذیری Λ به‌طور مشابه است. □

یک نتیجهٔ بسیار مفید از گزاره ۶.۱ ارائه می‌دهیم، که نشان می‌دهد مقیاس‌پذیری تحت تبدیلات یکانی پایا است.

نتیجه ۹.۱. فرض کنیم H و K دو فضای هیلبرت و $\Lambda = \{\Lambda_j \in B(H, H_j) : j \in J\}$، $g-$قاب باشد و $U \in B(K, H)$ عملگری یکانی باشد، یعنی $UU^* = I_H$ و $U^*U = I_K$. آنگاه Λ $g-$قاب مقیاس‌پذیر است اگر و تنها اگر $\Lambda U = \{\Lambda_jU \in B(K, H_j) : j \in J\}$ $g-$قاب مقیاس‌پذیر باشد.

اثبات. فرض کنیم Λ یک $g-$قاب مقیاس‌پذیر در H با عملگر قطری D باشد. چون عملگر تحلیل ΛU، $T_{\Lambda U}^* = T_\Lambda^*U$ است، لذا داریم:

$$\begin{aligned} \overline{(T_{\Lambda U}D)}(DT_{\Lambda U}^*) &= \overline{(U^*T_\Lambda D)}(DT_\Lambda^*U) \\ &= U^*\overline{(T_\Lambda D)}(DT_\Lambda^*)U \\ &= U^*U \\ &= I_K. \end{aligned}$$

درنتیجه ΛU مقیاس‌پذیر است.

برعکس، کافی است توجه کنیم که اگر U یک یکریختی باشد، آنگاه U^* یک یکریختی است و چون $\Lambda = (\Lambda U)U^*$، به‌این‌ترتیب حکم به دست می‌آید. □

۲ قاب‌های تکه‌ای مقیاس‌پذیر در فضاهای هیلبرت

کاسازا و همکارانش برای اولین بار مفهوم قاب‌های تکه‌ای مقیاس‌پذیر را روی فضاهای $\mathbb{R}^n$ در مقاله [۴] تعریف نموده‌اند و برخی از نتایج را در این فضا به دست آوردند. ما نیز در این بخش تلاش کرده‌ایم این مفهوم را روی فضاهای هیلبرت دلخواه تعریف نماییم و تعدادی از این نتایج را در فضاهای هیلبرت دلخواه، به‌خصوص در فضاهای هیلبرت با بعد متناهی تعمیم دهیم و در ادامه یک شرط لازم و کافی برای مشخصه‌سازی قاب‌های تکه‌ای مقیاس‌پذیر ارائه می‌دهیم. نهایتاً، شرایطی را که موجب می‌شود این مفهوم در فضای حاصلضرب تانسوری فضاهای هیلبرت دلخواه برقرار شود را مورد مطالعه قرار می‌دهیم. اکنون تعریف قاب تکه‌ای مقیاس‌پذیر برای تعداد متناهی عملگر تصویر متعامد $P_1, ..., P_m$ که در آن $m \geq 2$ را بیان می‌کنیم.

تعریف ۱.۲. فرض کنید $\{x_i : i \in I\}$ یک قاب در H باشد. آن را قاب تکه‌ای مقیاس‌پذیر گویند، هرگاه عملگرهای تصویر متعامد $P_1, ..., P_m$ روی H وجود داشته باشند به‌طوری‌که $\sum_{j=1}^{m} P_j = I$ ، و زیرمجموعه‌ای از ضرایب

$$\{a_i^1, ..., a_i^m : i \in I\} \subseteq \mathbb{R}^{\geq 0}$$

موجود باشند، به‌طوری‌که

$$\{a_i^1 P_1(x_i) + ... + a_i^m P_m(x_i) : i \in I\}$$

یک قاب پارسوال روی H باشد. گاهی آن را $\mathcal{P}$-مقیاس‌پذیر [1] گویند هرگاه $\mathcal{P} := \{P_1, ..., P_m\}$.

در کل این بخش، به‌ازای هر $j \in [m]$، قرار می‌دهیم $H_j = P_j(H)$. مشاهده می‌شود قاب‌های مقیاس‌پذیر، تکه‌ای مقیاس‌پذیر هستند. درحالی‌که مثال‌هایی در مقاله [۴]، با جزئیات بیشتر زده شده است، که نشان می‌دهد عکس آن برقرار نیست.

نتیجهٔ اصلی این بخش را در ادامه ارائه خواهیم نمود.

قضیه ۲.۲. $X = \{x_i : i \in I\} \subseteq H$ تکه‌ای مقیاس‌پذیر با تصویر متعامد $P_1, ..., P_m$ و ضرایب مقیاس $\{a_i^j : i \in I, j \in [m]\}$ است اگر و تنها اگر به‌ازای هر $j \in [m]$، $\{P_j x_i : i \in I\}$ قاب مقیاس‌پذیر در H_j با ضرایب مقیاس $\{a_i^j : i \in I\}$ باشد و به‌ازای هر $x \in H$

$$\sum_{i \in I} \sum_{k \neq j, k, j=1}^{m} a_i^j a_i^k Re[\langle x, P_j x_i \rangle \overline{\langle x, P_k x_i \rangle}] = 0.$$

اثبات. $\Rightarrow$) فرض کنیم $\{x_i : i \in I\}$ قاب تکه‌ای مقیاس‌پذیر با تصاویر متعامد $P_1, ..., P_m$ و ضرایب مقیاس $\{a_i^j : i \in I, j \in [m]\}$ روی H باشد. در این صورت $\{a_i^1 P_1 x_i + ... + a_i^m P_m x_i : i \in I\}$ قاب پارسوال روی H است. چون تصویر متعامد یک قاب (قاب پارسوال)، یک قاب (قاب پارسوال) است و به‌ازای هر $j \in [m]$، خواهیم داشت:

$$P_j(a_i^1 P_1 x_i + ... + a_i^j P_j x_i + ... + a_i^m P_m x_i) = a_i^j P_j x_i,$$

بنابراین به‌ازای هر $j \in [m]$، $\{a_i^j P_j x_i : i \in I\}$ قاب پارسوال است.

[1] $\mathcal{P}-$piecewise

همچنین به‌ازای هر $x \in H$، داریم:

$$\begin{aligned}\|x\|^2 &= \sum_{i\in I} |\sum_{j=1}^{m} \langle x, a_i^j P_j(x_i)\rangle|^2 \\ &= \sum_{i\in I}\sum_{j=1}^{m} |\langle x, a_i^j P_j(x_i)\rangle|^2 + 2\sum_{i\in I}\sum_{1\le j<k\le m} a_i^j a_i^k Re\Big(\langle x, P_j x_i\rangle\overline{\langle x, P_k x_i\rangle}\Big) \\ &= \sum_{j=1}^{m}\sum_{i\in I} |\langle x, a_i^j P_j(x_i)\rangle|^2 + 2\sum_{i\in I}\sum_{1\le j<k\le m} a_i^j a_i^k Re\Big(\langle x, P_j x_i\rangle\overline{\langle x, P_k x_i\rangle}\Big) \\ &= \sum_{j=1}^{m} \|P_j x\|^2 + 2\sum_{i\in I}\sum_{1\le j<k\le m} a_i^j a_i^k Re\Big(\langle x, P_j x_i\rangle\overline{\langle x, P_k x_i\rangle}\Big).\end{aligned}$$

درنتیجه

$$\sum_{i\in I}\sum_{1\le j<k\le m} a_i^j a_i^k Re\Big(\langle x, P_j x_i\rangle\overline{\langle x, P_k x_i\rangle}\Big) = 0.$$

$\Leftarrow$) فرض کنیم $x \in H$. با توجه به روند اثبات فوق، خواهیم داشت:

$$\begin{aligned}\sum_{i\in I}\Big|\sum_{j=1}^{m}\langle x, a_i^j P_j x_i\rangle\Big|^2 &= \sum_{j=1}^{m}\|P_j(x)\|^2 + 2Re\Big(\sum_{i\in I}\sum_{1\le j<k\le m}\langle x, a_i^j P_j x_i\rangle\overline{\langle x, a_i^k P_k x_i\rangle}\Big) \\ &= \|x\|^2,\end{aligned}$$

به‌این‌ترتیب اثبات کامل می‌شود. □

نتیجه ۳.۲. فرض کنید $X = \{x_i : i \in I\}$ قاب تکه‌ای مقیاس‌پذیر با تصاویر متعامد $P_1, ..., P_m$ باشد. آنگاه دنبالهٔ $\{P_j x_i : i \in I, j \in [m]\}$ قاب مقیاس‌پذیر H است.

اثبات. بنابر مفروضات، ضرایب ثابت $\{a_i^1, ..., a_i^m : i \in I\}$ وجود دارند، به‌طوری‌که $\{\sum_{j=1}^m a_i^j P_j x_i : i \in I\}$ یک قاب پارسوال H است و بنابر قضیه ۲.۲

$$\sum_{j=1}^{m}\sum_{i\in I} |\langle x, a_i^j P_j x_i\rangle|^2 = \|x\|^2.$$

درنتیجه دنبالهٔ $\{P_j x_i : j \in [m], i \in I\}$ قاب مقیاس‌پذیر H است. □

اکنون فرع ۲.۳، در مرجع [۴] را به فضاهای هیلبرت دلخواه تعمیم می‌دهیم.

گزاره ۴.۲. فرض کنید $X = \{x_i : i \in I\}$ یک قاب H باشد. اگر تصاویر متعامد $P_1, ..., P_m$ روی H موجود باشند به‌طوری‌که $\sum_{j\in[m]} P_j = I$، و یک افراز $P = \{\sigma_1, \sigma_2, ..., \sigma_m\}$ از I باشد که به‌ازای هر $j \in [m]$ $\{P_j x_i : i \in \sigma_j\}$ قاب مقیاس‌پذیر H_j باشد، آنگاه X قاب تکه‌ای مقیاس‌پذیر است.

اثبات. فرض کنید به‌ازای هر $j \in [m]$، $\{a_i^j : i \in \sigma_j\} \subseteq \mathbb{R}^{\ge 0}$. $\{a_i^j P_j(x_i) : i \in \sigma_j\}$ یک قاب پارسوال H_j است. در این صورت به‌ازای هر $i \in I \setminus \sigma_j$ قرار می‌دهیم $a_i^j = 0$ و به‌ازای هر $j \in [m]$، دنبالهٔ $\{a_i^j P_j x_i : i \in I\}$ یک قاب پارسوال H_j است. اکنون به‌ازای هر $i \in I$، $j \ne k,\ j, k \in [m]$ خواهیم داشت

$$a_i^j a_i^k = 0.$$

بنابر قضیه ۲.۲، نتیجه به دست خواهد آمد. □

اکنون به‌ازای هر $j \in [m]$ فرض کنید T_j عملگر تحلیل $\{P_j x_i : i \in I\}$ باشد. در این صورت T_j روی H قابل توسیع است هرگاه به‌ازای هر $k \ne j$، روی H_k داشته باشیم $T_j = 0$.

قضیه ۵.۲. فرض کنید $\{x_i : i \in I\} \subseteq H$ یک قاب H و به‌ازای هر $j \in [m]$، P_j تصویر متعامد روی H باشد. آنگاه احکام زیر معادل هستند:
(۱) $\{x_i : i \in I\}$ قاب تکه‌ای مقیاس‌پذیر H با ضرایب مقیاس $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$ است.
(۲) $\{a_i^j : i \in I\}$ به‌ازای هر $j \in [m]$، D_j عملگر قطری روی $\ell^2(I)$ با عناصر قطری $\sum_{1 \le k \ne j \le m} T_k^* D_k D_j T_j = 0$ است.

اثبات. می‌دانیم که عملگر تحلیل $\{a_i^j P_j(x_i) : i \in I, j \in [m]\}$ به‌صورت $T = \sum_{j=1}^m D_j T_j$ است. درنتیجه $T^* = \sum_{j=1}^m T_j^* D_j$ و

$$\begin{aligned} T^*T &= \left(\sum_{k=1}^m T_k^* D_k\right)\left(\sum_{j=1}^m D_j T_j\right) \\ &= \sum_{j=1}^m T_j^* D_j^2 T_j + \sum_{1 \le k \ne j \le m} T_k^* D_k D_j T_j. \end{aligned}$$

(۲) $\Rightarrow$ (۱) چون $\{a_i^j P_j(x_i) : i \in I, j \in [m]\}$ یک قاب پارسوال روی H است، آنگاه

$$\begin{aligned} S &= I_H = \sum_{j=1}^m T_j^* D_j^2 T_j + \sum_{1 \le k \ne j \le m} T_k^* D_k D_j T_j \\ &= \sum_{j=1}^m I_{P_j(H)} + \sum_{1 \le k \ne j \le m} T_k^* D_k D_j T_j. \end{aligned}$$

درنتیجه $\sum_{1 \le k \ne j \le m} T_k^* D_k D_j T_j = 0$.
(۱) $\Rightarrow$ (۲) به‌وضوح اگر $S = I_H$، نتیجه به دست می‌آید. □

در قضیهٔ بعدی نشان خواهیم داد که خاصیت تکه‌ای مقیاس‌پذیر قاب‌ها تحت عملگرهای یکانی روی فضاهای هیلبرت حفظ می‌شود.

قضیه ۶.۲. فرض کنید H و K دو فضای هیلبرت جدایی‌پذیر باشند. آنگاه $X = \{x_i : i \in I\}$ یک قاب تکه‌ای مقیاس‌پذیر H است اگر و تنها اگر به‌ازای هر عملگر یکانی $U : H \to K$، $UX = \{Ux_i : i \in I\}$ یک قاب تکه‌ای مقیاس‌پذیر K باشد.

اثبات. فرض کنید $X = \{x_i : i \in I\} \subseteq H$ یک قاب تکه‌ای مقیاس‌پذیر H با تصاویر متعامد $P_1, P_2, ..., P_m$ با ضرایب ثابت $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$ و عملگر یکانی دلخواه $U : H \to K$ باشد. اگر به‌ازای هر $j \in [m]$، $Q_j = UP_jU^*$، در این صورت $Q_j^* = Q_j^2 = Q_j$. درنتیجه هر Q_j یک تصویر متعامد روی K است. به‌ازای هر $y \in K$ داریم:

$$\begin{aligned} \sum_{i \in I}\sum_{j \in [m]} |\langle y, a_i^j Q_j(Ux_i)\rangle|^2 &= \sum_{i \in I}\sum_{j \in [m]} |\langle U^*y, a_i^j P_j(x_i)\rangle|^2 \\ &= \|U^*(y)\|^2 = \|y\|^2, \end{aligned}$$

درنتیجه UX قاب تکه‌ای مقیاس‌پذیر است.
برعکس، می‌دانیم که اگر U یکریختی باشد، آنگاه U^* نیز یکریختی است لذا کافی است قرار دهیم $X = U^*(UX)$. □

دنبالهٔ $X = \{x_i : i \in I\}$ را یک قاب با نرم برابر گویند، هرگاه به‌ازای هر $j, k \in I$، $\|x_j\| = \|x_k\|$. X را یک قاب با نرم واحد نامند، هرگاه به‌ازای هر $j \in I$، $\|x_j\| = 1$.

گزاره ۷.۲. فرض کنید $X = \{x_i : i \in I\}$ یک قاب فضای هیلبرت H با بعد متناهی باشد. اگر X قاب تکه‌ای مقیاس‌پذیر با تصاویر متعامد $P_1, ..., P_m$ و ضرایب ثابت $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$ باشد، آنگاه

$$dimH = \sum_{j \in [m]} dimH_j = \sum_{j \in [m]}\sum_{i \in I} (a_i^j)^2 \|P_j(x_i)\|^2.$$

اثبات. می‌دانیم که اگر H یک فضای هیلبرت با بعد متناهی و $\{f_i : i \in I\}$ قاب پارسوال H باشد، آنگاه

$$\sum_{i\in I} \|f_i\|^2 = dim(H).$$

همچنین اگر $\{g_i : i \in I\}$ قاب پارسوال و $P : H \to H$ تصویر متعامد روی H باشد، آنگاه $\{P(g_i) : i \in I\}$ قاب پارسوال $K = P(H)$ است. زیرا به‌ازای هر $j \in [m]$ داریم:

$$\left\{ P_j(\sum_{j\in[m]} a_i^k P_k(x_i)) : i \in I \right\} = \{a_i^j P_j(x_i) : i \in I\}$$

قاب پارسوال $H_j = P_j(H)$ است. بنابراین

$$\sum_{i\in I} \|a_i^j P_j(x_i)\|^2 = dim(H_j).$$

درنتیجه

$$\sum_{j\in[m]} \sum_{i\in I} \|a_i^j P_j(x_i)\|^2 = \sum_{j\in[m]} dimH_j = dim(H).$$

□

قضیه ۸.۲. فرض کنید $X = \{x_i : i \in I\}$ یک قاب تکه‌ای مقیاس‌پذیر با نرم واحد فضای هیلبرت با بعد متناهی H باشد به‌طوری‌که با تصاویر متعامد $P_1, ..., P_m$ و ضرایب ثابت $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$ باشد. آنگاه

الف) $\sum_{i\in I} \min\{(a_i^j)^2 : j \in [m]\} \le dim(H)$

ب) $dim(H) \le \sum_{i\in I} \max\{(a_i^j)^2 : j \in [m]\}$.

اثبات. به‌ازای هر $i \in I$ قرار می‌دهیم

$$c_i = \min\{(a_i^j)^2 : j \in [m]\}$$

و

$$\ell_i = \max\{(a_i^j)^2 : j \in [m]\}.$$

الف) چون به‌ازای هر $j \in [m]$ $\{a_i^j P_j(x_i) : i \in I\}$ قاب پارسوال H_j است، لذا

$$\sum_{k\in I} (a_i^j)^2 \|P_j(x_i)\|^2 = dimH_j.$$

چون به‌ازای هر $i \in I$، $j \in [m]$

$$1 = \|x_i\|^2 = \sum_{j\in[m]} \|P_j(x_i)\|^2, \quad dimH = \sum_{j\in[m]} dimH_j,$$

آنگاه

$$\sum_{i\in I} c_i \le \sum_{i\in I} \sum_{j\in[m]} (a_i^j)^2 \|P_j(x_i)\|^2 \le \sum_{i\in I} l_i$$

و اثبات کامل می‌شود. □

ا.خسروی و ب.خسروی در مقاله [۱۱]، نشان دادند که حاصلضرب تانسوری دو قاب دلخواه در فضای هیلبرت، یک قاب است. در ادامه یک شرط لازم و کافی تکه‌ای مقیاس‌پذیر در حاصلضرب تانسوری قاب‌ها را بیان و اثبات می‌کنیم.

قضیه ۹.۲. فرض کنید $X = \{x_i : i \in I\} \subseteq H$ قاب H و $\{y_j : j \in J\}$ یک قاب $A-$تنگ K باشد. آنگاه X یک قاب تکه‌ای مقیاس‌پذیر H با تصاویر متعامد $P_1, ..., P_m$ و ضرایب مقیاس $\{a_i^1, a_i^2, ..., a_i^m : i \in I\}$ است اگر و تنها اگر $\{x_i \otimes y_j : i \in I, j \in J\}$ یک قاب تکه‌ای مقیاس‌پذیر $H \otimes K$ با تصاویر متعامد $P_1' = P_1 \otimes I_K, ..., P_m' = P_m \otimes I_K$ با ضرایب مقیاس $\left\{ \frac{1}{\sqrt{A}} a_i^1, ..., \frac{1}{\sqrt{A}} a_i^m : i \in I \right\}$ باشد.

اثبات. ($\Rightarrow$) چون $\{y_j : j \in J\}$ یک قاب $A-$تنگ است. پس $\{\frac{1}{\sqrt{A}}y_j : j \in J\}$ و همچنین $\{\sum_{j=1}^{m} a_i^j P_j(x_i) : i \in I\}$ قاب‌های پارسوال H هستند. در این صورت نتایج به‌دست‌آمده در [۱۱] ایجاب می‌کند که

$$\left\{\sum_{l=1}^{m} a_i^l P_l(x_i) \otimes \frac{1}{\sqrt{A}} y_j : i \in I, j \in J\right\}$$

یک قاب پارسوال در $H \otimes K$ باشد. بنابراین

$$\left\{\sum_{l=1}^{m} \frac{1}{\sqrt{A}} a_i^l P_l'(x_i \otimes y_j) : i \in I, j \in J\right\}$$

قاب پارسوال در $H \otimes K$ است. درنتیجه $\{x_i \otimes y_j : i \in I, j \in J\}$ یک قاب تکه‌ای مقیاس‌پذیر $H \otimes K$ است.
($\Leftarrow$) فرض کنید $x \in H$ و $y \neq 0$ در K باشد. بنابراین

$$\begin{aligned} \|x\|^2\|y\|^2 &= \|x \otimes y\|^2 = \sum_{l=1}^{m} \sum_{i\in I} \sum_{j\in J} \frac{1}{A}(a_i^l)^2 |\langle x, P_l(x_i)\rangle|^2 |\langle y, y_j\rangle|^2 \\ &= \|y\|^2 \sum_{l=1}^{m} \sum_{i\in I} (a_i^l)^2 |\langle x, P_l(x_i)\rangle|^2. \end{aligned}$$

درنتیجه

$$\|x\|^2 = \sum_{l=1}^{m} \sum_{i\in I} (a_i^l)^2 |\langle x, P_l(x_i)\rangle|^2.$$

□

اثبات نتیجهٔ زیر شبیه اثبات فوق است.

نتیجه ۱۰.۲. فرض کنید $\{x_i : i \in I\}$ یک قاب λ-تنگ H باشد. در این صورت $\{y_j : j \in J\}$ قاب تکه‌ای مقیاس‌پذیر K با تصاویر متعامد $Q_1, ..., Q_m$ و با ضرایب مقیاس $\{b_j^1, ..., b_j^m : j \in J\}$ است اگر و تنها اگر $\{x_i \otimes y_j : i \in I, j \in J\}$ یک قاب تکه‌ای مقیاس‌پذیر $H \otimes K$ با تصاویر متعامد $I_H \otimes Q_1, ..., I_H \otimes Q_m$ و ضرایب مقیاس $\left\{\frac{1}{\sqrt{\lambda}} b_j^1, ..., \frac{1}{\sqrt{\lambda}} b_j^m : j \in J\right\}$ باشد.

References

[1] Asgari, M.S., & Khosravi, A. (2005). Frames and bases of subspaces in Hilbert spaces. *J. Math. Anal. Appl*, 308, 541–553. DOI: https://doi.org/10.1016/j.jmaa.2004.11.036.

[2] Cahill, J., & Chen, X. (2013). A note on scalable frames. *Proceedings of the 10th International Conference on Sampling Theory and Applications*, 93–96.

[3] Casazza, P., Carli, L., & Tran, T. (2024). Piecewise scalable frames. *Linear Algebra and its Applications*, 694, 262–282. DOI: https://doi.org/10.1016/j.laa.2024.04.008.

[4] Casazza, P., & Chen, X. (2017). Frame scalings: A condition number approach. *Linear Algebra and its Applications*, 523, 152–168. DOI: https://doi.org/10.1016/j.laa.2017.02.020.

[5] Casazza, P., & Kutyniok, G. (2004). Frames of subspaces. *Contemp. Math. Amer. Math. Soc*, 345, 87–113.

[6] Casazza, P.G., & Kutyniok, G. (2013). Finite Frames: Theory and Applications. *Birkhauser, New York*. DOI: https://doi.org/10.1007/978-0-8176-8373-3.

[7] Christensen, O. (2008). Frames and Bases. *Birkhauser, Boston*. DOI: https://doi.org/10.1007/978-0-8176-4678-3.

[8] Daubechies, I., Grossmann, A., & Meyer, Y. (1986). Painless nonorthogonal expansions. *J. Math. Phys*, 27, 1271–1286. DOI: https://doi.org/10.1063/1.527388.

[9] Duffin, R.J., & Schaeffer, A.C. (1952). A class of nonharmonic Fourier series. *Trans. Am. Math. Soc*, 72, 341–366. DOI: https://doi.org/10.2307/1990760.

[10] Khosravi, A., & Farmani, M.R. (2024). Piecewise scalable frames in Hilbert spaces. *International Journal of Wavelets, Multiresolution and Information Processing*, 22(3), 2350052. DOI: https://doi.org/10.1142/S0219691323500522.

[11] Khosravi, A., & Khosravi, B. (2007). Frames and bases in tensor product of Hilbert spaces and Hilbert C^*-modules. *Proc. Math. Sci*, 117, 1–12. DOI: https://doi.org/10.1007/s12044-007-0001-5.

[12] Khosravi, A., & Mirzaee Azandaryani, M. (2014). Approximate duality of g-frames in Hilbert spaces. *Acta Math. Sci*, 34, 639–652. DOI: https://doi.org/10.1016/S0252-9602(14)60036-9.

[13] Kutyniok, G., Okoudjou, K.A., & Philipp, F. (2013). Scalable frames. *Linear Algebra and its Applications*, 438, 2225–2238. DOI: https://doi.org/10.1016/j.laa.2012.10.046.

[14] Sun, W. (2006). G-frames and g-Riesz bases. *J. Math. Anal. Appl*, 322, 437–452. DOI: https://doi.org/10.1016/j.jmaa.2005.09.039.

Measure Algebras and Applications

The structure of invariant and ergodic states for C^*-dynamical systems

Mohammad Nekoufar[1]

1. Department of Mathematics, Andimeshk Branch, Islamic Azad University, Andimeshk, Iran.
Email: mrnekoufar@iauandimeshk.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 31 March 2024
Received in revised form:
13 June 2024
Accepted: 24 June 2024
Published Online:
20 August 2024

Keywords:
C^*-dynamical system,
The lift of a C^*-dynamical system,
Invariant state,
Ergodic state

2020 Mathematics Subject Classification:
37A35

ABSTRACT

In this paper, the invariant and ergodic states corresponding to a C^*-dynamical system are introduced and the structures of these sets are studied. To do this, we use the concept of the lift of a C^*-dynamical system.

Cite this article: Nekoufar, M. (2024). The structure of invariant and ergodic states for C^*-dynamical systems. *Measure Algebras and Applications*, 1(2), 119–129. http://doi.org/10.22091/maa.2024.10781.1020

Publisher: University of Qom
DOI: 10.22091/maa.2024.10781.1020

Extended Abstract

Introduction

C^*-dynamical systems are introduced and studied as a generalization of classical dynamical systems. In particular, ergodic theory as an approach with analysis taste to dynamical systems is studied in the framework of C^*-dynamical systems [1–4, 7, 8, 11].

The concepts like invariant measures [18], Birkhoff ergodic theorem [5] and von-Neumann ergodic theorem [16, 17] are formulated and studied for C^*-dynamical systems. Also, there are some other concepts such as the entropy, in classical dynamical systems [4, 19], which are extended to C^*-dynamical systems. They generalize the corresponding concepts in the classical case.

In the classical ergodic theory for dynamical systems, invariant and ergodic measures play very important roles. These measures are applied in the formulation of ergodic theorems [5, 16–18], the introduction of entropy [4, 19] and pressure [13, 19, 21] for dynamical systems. They are also applied in the thermodynamic formalism of dynamical systems [14].

In the theory of C^*-dynamical systems, the concepts of state and invariant state correspond to probability and invariant measures for classical dynamical systems. They are applied to define the entropy of a C^*-dynamical system [6].

In this paper, the concept of ergodic state is given and then, using the concept of a lift map, the structure of invariant states is studied and connected to ergodic states.

Conclusion

In this paper, the following definitions and results are applied. One may see [10] for more discussions.

***Definition* 0.1.** *Let A be a C^*-algebra with the unit element $1 \in A$. For $a \in A$, the spectrum of a is defined by*

$$spec(a) := \{\lambda \in \mathbb{C} : \lambda \cdot 1 - a \ \textit{is not invertible}\}.$$

The spectral radius of a is also defined by

$$r(a) := \sup\{|\lambda| : \lambda \in spec(a)\}.$$

***Theorem* 0.2.** *We have the following properties:*

1. *If A is a unital C^*-algebra, then for any $a \in A$, the set $spec(a)$ is non-empty and compact.*
2. *For every $a \in A$, we have $r(a) \leq ||a||$. Indeed*
$$r(a) = \lim_{n\to\infty} ||a^n||^{\frac{1}{n}}.$$
3. *If $a^* = a$, then $r(a) = ||a||$.*

***Definition* 0.3.** *Let A and B be two C^*-algebras on $\mathbb{C}$. The set of all non-zero homomorphisms $\phi : A \to B$ is denoted by $Hom(A, B)$. Recall that $\phi : A \to B$ is a homomorphism if*

1. *ϕ is linear.*

2. $\forall a, b \in A \ : \ \phi(ab) = \phi(a)\phi(b)$.

Additionally, if $\phi(a^*) = \phi(a)^*$, then ϕ is called a $*$-homomorphism. Finally, if $B = \mathbb{C}$, then we write $\Omega(A) = Hom(A, \mathbb{C})$.

***Remark* 0.4.** *If A and B are two C^*-algebras and $\rho : A \to B$ is a $*$-homomorphism, then $||\rho|| \leq 1$, that is $||\rho(a)|| \leq ||a||$, for all $a \in A$.*

***Remark* 0.5.** *Let A be a commutative unital C^*-algebra and $\phi \in \Omega(A)$. Then,*

1. $\forall a \in A$, $\phi(a) \in spec(a)$.
2. $||\phi|| = 1$.
3. $\forall a \in A$, $\phi(a^*) = \phi(a)^*$.

Let A^* be the dual of A, equipped by weak-star topology. Then, $\Omega(A) \subset A^*$. In this case, we have the following proposition.

***Proposition* 0.6.** *If A is a commutative unital C^*-algebra, then $\Omega(A)$ is compact in weak-star topology on the unit ball of A^*.*

***Lemma* 0.7.** *Let $a \in A$. The evaluation map $\hat{a} : \Omega(A) \to \mathbb{C}$ defined by $\hat{a}(\phi) := \phi(a)$ is continuous with the range $spec(a)$.*

***Theorem* 0.8.** *Let A be a commutative unital C^*-algebra. Then, the map $\Phi : A \to C(\Omega(A))$ defined by $\Phi(a) := \hat{a}$ is an isometric $*$-isomorphism from A to $C(\Omega(A))$. In other words, $A \cong C(\Omega(A))$.*

C^*-dynamical systems and invariant and ergodic states

In this section, invariant and ergodic states for a C^*-dynamical system are introduced and the structure of these sets is studied.

***Definition* 0.9.** *Let A be a C^*-algebra on $\mathbb{C}$. By a C^*-dynamical system on A, we mean a map $\alpha : A \to A$ such that,*

1. *α is linear.*
2. *For every $a \in A$, we have $\alpha(a^*) = \alpha(a)^*$.*
3. *For every $a, b \in A$, we have $\alpha(ab) = \alpha(a)\alpha(b)$.*

***Definition* 0.10.** *Let A be a C^*-algebra on $\mathbb{C}$. A function $\omega : A \to \mathbb{C}$ is called a state, if*

1. *ω is linear.*
2. *ω is positive, i.e., for every $a \in A$ we have $\omega(aa^*) \geq 0$.*
3. *$||\omega||_{\text{op}} = 1$, where $|| \cdot ||_{\text{op}}$ is the operator norm of ω.*

The collection of all of states on a C^*-algebra A is denoted by $S(A)$.

***Definition* 0.11.** *Let $\alpha : A \to A$ be a C^*-dynamical system. A state $\omega : A \to \mathbb{C}$ is called α-invariant if $\omega \circ \alpha = \omega$. The collection of all α-invariant states is denoted by $S(A, \alpha)$.*

***Remark* 0.12.** *Let A^* be the dual of the C^*-algebra A. Then $S(A)$ and $S(A,\alpha)$ are weak* compact convex subsets of the unit ball of A^*.*

***Definition* 0.13.** *An α-invariant state ω is called α-ergodic, if for any $a \in A$, the relation $\alpha(a) = a$ implies $\hat{a} = c$, where c is a constant.*

The collection of all α-ergodic states is denoted by $S_e(A,\alpha)$. It is obvious that, $S_e(A,\alpha) \subset S(A,\alpha) \subset S(A)$.

We have the following theorem.

***Theorem* 0.14.** *Let $\omega \in S(A)$. Then, there exists a unique positive probability measure μ_ω on Borel subsets of $\Omega(A)$ such that*

$$g(\omega) = \int_{\Omega(A)} g d\mu_\omega, \qquad \forall g \in C(\Omega(A)).$$

***Corollary* 0.15.** *The map $I : S(A) \to M_1(\Omega(A))$ defined by $I(\omega) := \mu_\omega$ is affine and bijective. So, there is a one-to-one correspondence between the elements of $S(A)$ and $M_1(\Omega(A))$.*

***Definition* 0.16.** *Let $\Phi : A \to C(\Omega(A))$ be the isomorphism as in Theorem 0.8. For a C^*-dynamical system $\alpha : A \to A$, the lift map $\tilde{\alpha} : C(\Omega(A)) \to C(\Omega(A))$ is defined by $\tilde{\alpha} := \Phi \circ \alpha \circ \Phi^{-1}$.*

***Definition* 0.17.** *Let $\alpha : A \to A$ be a C^*-dynamical system and $\tilde{\alpha}$ be the corresponding lift map. The collection of all probability measures μ on Borel σ-algebra of $\Omega(A)$ such that*

$$\int_{\Omega(A)} \tilde{\alpha}(g) d\mu = \int_{\Omega(A)} g d\mu, \qquad \forall g \in C(\Omega(A))$$

is denoted by $M(A,\tilde{\alpha})$. Also, the collection of all measures $\mu \in M(A,\tilde{\alpha})$ such that, given any $g \in C(\Omega(A))$, the equality $\tilde{\alpha}(g) = g$ implies $g = c$, μ.a.e, where c is a constant, is denoted by $E(A,\tilde{\alpha})$.

***Lemma* 0.18.** *1. $\omega \in S(A,\alpha)$ if and only if $\mu_\omega \in M(A,\tilde{\alpha})$.*

2. $\omega \in S_e(A,\alpha)$ if and only if $\mu_\omega \in E(A,\tilde{\alpha})$.

Note that, applying the proof of Theorem 6.10 in [20], one may easily see that, the set of extreme points of $M(A,\tilde{\alpha})$ is $E(A,\tilde{\alpha})$. We have the following theorem for the states.

***Theorem* 0.19.** *The set of extreme points of $S(A,\alpha)$ is $S_e(A,\alpha)$.*

***Theorem* 0.20.** *(Choquet) Suppose that Y is a compact convex metrizable subset of a locally convex space E, and that $x_0 \in Y$. Then there exists a probability measure τ on Y which represents x_0 and is supported by the extreme points of Y, i.e., $\Phi(x_0) = \int_Y \Phi d\tau$ for every continuous linear functional Φ on E, and $\tau(ext(Y)) = 1$.*

See [8] for a proof of Choquet's theorem.

The following result is a direct consequence of Choquet's theorem [8].

***Corollary* 0.21.** *For any $\omega \in S(A,\alpha)$, there exists a unique probability measure σ on Borel sets of $S(A,\alpha)$ such that $\sigma(S_e(A,\alpha)) = 1$ and*

$$\int_{\Omega(A)} f d\mu_\omega = \int_{S_e(A,\alpha)} \left(\int_\Omega f d\mu_\nu \right) d\sigma(\nu).$$

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۲۹-۱۱۹

ساختار حالت‌های پایا و ارگودیک برای C^*-دستگاه‌های دینامیکی

محمد نکوفر [۱]

۱. گروه ریاضی، واحد اندیمشک، دانشگاه آزاد اسلامی، اندیمشک، ایران. رایانامه: mrnekoufar@iauandimeshk. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۱/۱۲
تاریخ بازنگری: ۱۴۰۳/۳/۲۴
تاریخ پذیرش: ۱۴۰۳/۴/۴
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
C^*-دستگاه دینامیکی،
بالابر متناظر با یک C^*-دستگاه دینامیکی،
حالت پایا،
حالت ارگودیک

رده‌بندی ریاضی:
37A35

چکیده

در این مقاله به معرفی حالت‌های پایا و ارگودیک متناظر با یک C^*-دستگاه دینامیکی پرداخته و ساختار این مجموعه‌ها را مطالعه می‌نماییم. برای این کار از مفهوم بالابر متناظر با یک C^*-دستگاه دینامیکی استفاده می‌نماییم.

استناد: نکوفر، محمد. (۱۴۰۳). ساختار حالت‌های پایا و ارگودیک برای C^*-دستگاه‌های دینامیکی. جبرهای اندازه و کاربردها، ۱(۲)، ۱۲۹-۱۱۹.

http://doi.org/10.22091/maa.2024.10781.1020

ناشر: دانشگاه قم.

۱ مقدمه

C^*-دستگاه‌های دینامیکی به‌عنوان تعمیمی از دستگاه‌های دینامیکی کلاسیک معرفی شده و مورد مطالعه قرار گرفته‌اند [۱–۴، ۷، ۸، ۱۱]. به‌طور خاص، نظریهٔ ارگودیک به‌عنوان رویکردی با طعم آنالیز به دستگاه‌های دینامیکی، در چارچوب C^*-دستگاه‌های دینامیکی نیز مورد توجه قرار گرفته‌اند. مفاهیمی مانند اندازهٔ پایا [۱۸] و قضایای ارگودیگ بیرخوف [۵] و فون نیومن [۱۶، ۱۷] برای C^*- دستگاه‌های دینامیکی نیز مورد مطالعه قرار گرفته‌اند. به‌علاوه، مفاهیمی مانند آنتروپی دستگاه‌های دینامیکی [۴، ۱۹] نیز برای C^*- دستگاه‌های دینامیکی تعریف شده و مورد مطالعه قرار گرفته‌اند. این مفاهیم، تعمیمی از مفاهیم متناظر با آن‌ها در نظریهٔ دستگاه‌های دینامیکی هستند. در نظریهٔ کلاسیک ارگودیک برای دستگاه‌های دینامیکی، اندازه‌های پایا و ارگودیک نقش بسیار مهمی بازی می‌کنند. این اندازه‌ها در فرمول‌بندی قضایای ارگودیک [۵، ۱۶–۱۸]، معرفی مفهوم آنتروپی [۴، ۱۹] و فشار توپولوژیک [۱۳، ۱۹، ۲۱] و همچنین صورت‌بندی ترمودینامیکی دستگاه‌های دینامیکی [۱۴] نقش مهمی بازی می‌کنند. در نظریهٔ C^*-دستگاه‌های دینامیکی، مفهوم حالت و حالت‌های پایا متناظر با اندازه‌های پایا معرفی شده و به کمک آن‌ها، مفهوم آنتروپی یک C^*-دستگاه دینامیکی معرفی شده و مورد مطالعه قرار گرفته است [۶].
در این مقاله، ضمن معرفی مفهوم حالت ارگودیک، به کمک نگاشت بالابر، ساختار مجموعهٔ حالت‌های پایا و ارتباط آن‌ها با حالت‌های ارگودیک را مورد مطالعه قرار می‌دهیم.

۲ مفاهیم مقدماتی

در این بخش به معرفی و یادآوری مفاهیم مقدماتی مورد استفاده در این مقاله می‌پردازیم. در تمام این مقاله، A یک C^*-جبر بر $\mathbb{C}$ است و $* : A \to A$ همان عمل بازگشت است. برای دیدن بحث مفصل‌تر در مورد مفاهیم مقدماتی این بخش می‌توان به مرجع [۶] مراجعه‌کرد.

تعریف ۱.۲. فرض کنیم A یک C^*-جبر بر $\mathbb{C}$ با عنصر واحد $\mathbb{1} \in A$ باشد. برای هر $a \in A$، طیف a عبارت است از:

$$Spec(a) := \{\lambda \in \mathbb{C} \mid \text{وارون‌پذیر نیست } \lambda.\mathbb{1} - a\}.$$

شعاع طیفی a نیز عبارت است از

$$r(a) := \sup\{|\lambda| \mid \lambda \in Spec(a)\}.$$

خواص زیر برقرارند.

قضیه ۲.۲. اگر A یک C^*-جبر دارای واحد باشد، آنگاه

۱. برای هر $a \in A$، $Spec(a)$ ناتهی و فشرده است.

۲. برای هر $a \in A$ داریم $r(a) \leq ||a||$.

۳. اگر $a = a^*$، آنگاه $r(a) = ||a||$.

تعریف ۳.۲. فرض کنیم A و B، C^*-جبرهایی بر $\mathbb{C}$ باشند. مجموعهٔ کلیهٔ هومومرفیسم‌های غیرصفر $\varphi : A \to B$ را با $Hom(A, B)$ نمایش می‌دهیم. یادآور می‌شویم که $\varphi : A \to B$ را یک هومومرفیسم می‌نامیم هرگاه:

۱. φ خطی باشد.

۲. برای هر $a, b \in A$ داشته باشیم، $\varphi(ab) = \varphi(a)\varphi(b)$.

به‌علاوه اگر $\varphi(a^*) = \varphi(a)^*$، آنگاه φ را یک $*$-هومومرفیسم می‌نامیم. در نهایت، اگر $B = \mathbb{C}$، آنگاه می‌نویسیم

$$\Omega(A) = Hom(A, \mathbb{C}).$$

تذکر ۴.۲. اگر A و B دو C^*-جبر بوده و $\varphi : A \to B$ یک $*$-هومومرفیسم باشد، آنگاه $||\varphi|| \leq 1$ یعنی

$$\forall a \in A : \qquad ||\varphi|| \leq ||a||.$$

تذکر ۵.۲. فرض کنیم A یک C^*-جبر جابه‌جایی و یکدار بوده و $\varphi \in \Omega(A)$. آنگاه

۱. $\forall a \in A : \ \varphi(a) \in Spec(a)$.

۲. $||\varphi|| = ۱$.

۳. $\forall a \in A : \ \varphi(a^*) = \overline{\varphi(a)}$.

فرض کنیم A^* دوگان A، مجهز به توپولوژی ضعیف-ستاره باشد. در این صورت $\Omega(A) \subseteq A^*$ و در این حالت گزارهٔ زیر را داریم.

گزاره ۶.۲. اگر A یک C^*-جبر جابه‌جایی یکدار باشد، آنگاه $\Omega(A)$ نسبت به توپولوژی ضعیف-ستاره بر گوی واحد A^*، فشرده است.

لم ۷.۲. فرض کنیم $a \in A$. نگاشت مقداردهی $\widehat{a} : \Omega(A) \to \mathbb{C}$ با ضابطهٔ $\widehat{a}(\varphi) := \varphi(a)$ پیوسته است و برد آن $Spec(a)$ است.

قضیه ۸.۲. فرض کنیم A یک C^*-جبر جابه‌جایی و یکدار باشد. در این صورت تابع

$$\Phi : A \to C(\Omega(A)) \qquad , \qquad a \mapsto \widehat{a}$$

یک $*$-ایزومورفیسم طول‌پا از A بر $C(\Omega(A))$ است. به‌عبارت‌دیگر $A \cong C(\Omega(A))$.

۳ C^*-دستگاه‌های دینامیکی و حالت‌های پایا و ارگودیک

در این بخش حالت‌های پایا و ارگودیک را برای C^*-دستگاه‌های دینامیکی معرفی کرده و ساختار این مجموعه‌ها را مورد مطالعه قرار می‌دهیم.

تعریف ۱.۳. فرض کنیم A یک C^*-جبر بر $\mathbb{C}$ باشد. منظور از یک C^*-دستگاه دینامیکی بر A، تابعی مانند $\alpha : A \to A$ است به‌گونه‌ای که:

۱. α خطی است.

۲. برای هر $a \in A$، داریم $\alpha(a^*) = \alpha(a)^*$.

۳. برای هر $a, b \in A$ داریم $\alpha(ab) = \alpha(a)\alpha(b)$.

تعریف ۲.۳. فرض کنیم A یک C^*-جبر بر $\mathbb{C}$ باشد. تابع $\omega : A \to \mathbb{C}$ را یک تابع حالت نامیم هرگاه:

۱. ω خطی است.

۲. ω مثبت باشد، یعنی برای هر $a \in A$ داشته باشیم:

$$\omega(aa^*) \geq ۰$$

۳. $||\omega||_{op} = ۱$، که در آن $||.||_{op}$ همان نرم ω به‌عنوان یک تابعک خطی است.

مجموعهٔ متشکل از کلیهٔ حالت‌های C^*-جبر A را با نماد $S(A)$ نمایش می‌دهیم.

تعریف ۳.۳. فرض کنیم $\alpha : A \to A$ یک C^*-دستگاه دینامیکی باشد. حالت $\omega : A \to \mathbb{C}$ را یک α-پایا می‌نامیم هرگاه داشته باشیم $\omega \circ \alpha = \omega$. مجموعهٔ کلیهٔ حالت‌های α-پایا را با نماد $S(A, \alpha)$ نمایش می‌دهیم.

تذکر ۴.۳. فرض کنیم A^* دوگان C^*-جبر A باشد و B_{A^*} گوی واحد در A^* باشد. با در نظر گرفتن توپولوژی ضعیف-ستاره بر A^* و با توجه به قضیهٔ باناخ-آلاقلو، گوی واحد B_{A^*} نسبت به توپولوژی ضعیف-ستاره فشرده است. به‌علاوه روشن است که

$$S(A, \alpha), S(A) \subseteq B_{A^*}$$

به‌سادگی می‌توان دید که $S(A)$ و $S(A, \alpha)$ زیرمجموعه‌های بسته و محدبی از B_{A^*} هستند و در نتیجه فشرده نیز هستند.

تعریف ۵.۳. حالت α-پایای ω را α-ارگودیک نامیم هرگاه برای هر $a \in A$، از رابطهٔ $\alpha(a) = a$ نتیجه بگیریم که $\widehat{a} = cte$ ثابت است. مجموعهٔ متشکل از کلیهٔ حالت‌های ارگودیک α را با نماد $S_e(A, \alpha)$ نمایش می‌دهیم.

قضیهٔ زیر به هر حالت بر C^*-جبر A یک اندازه نظیر می‌کند.

قضیه ۶.۳. فرض کنیم $\omega \in S(A)$ در این صورت اندازهٔ مثبت احتمال یکتای μ_ω بر σ-جبر بورل $\Omega(A)$ موجود است به‌گونه‌ای که

$$\forall\, g \in C(\Omega(A)) : \qquad g(\omega) = \int_{\Omega(A)} g\, d\mu_\omega$$

اثبات. فرض کنیم $\omega \in S(A)$. تابعک خطی $L_\omega : C(\Omega(A)) \to \mathbb{C}$ را به‌صورت $L_\omega(g) := g(\omega)$ تعریف می‌کنیم. روشن است که L_ω خطی است و به‌علاوه

$$||L_\omega||_{op} = \sup_{||g||=1} |L_\omega(g)| = \sup_{||g||=1} |g(\omega)| \leq 1.$$

بنابراین L_ω عملگری کران‌دار است و درنتیجه $L_\omega \in (C(\Omega(A)))^*$. اکنون طبق قضیهٔ نمایش ریس، اندازهٔ یکتای μ_ω بر σ-جبر بورل $C(\Omega(A))$ موجود است به‌گونه‌ای که:

$$\forall\ \in C(\Omega(A)) : \qquad g(\omega) = L_\omega(g) = \int_{\Omega(A)} g\, d\mu_\omega.$$

روشن است که اگر $g \geq 0$، آنگاه $L_\omega(g) \geq 0$ و درنتیجه μ_ω اندازه‌ای مثبت است. □

نتیجه ۷.۳. نگاشت $I : S(A) \longrightarrow M_1(\Omega(A))$ با ضابطهٔ $w \longmapsto \mu_w$ آفین و دوسویی است. بنابراین یک تناظر یک‌به‌یک آفین بین عناصر $S(A)$ و اعضای $M_1(\Omega(A))$ برقرار است.

اثبات. برای هر $a \in A$ و هر $w, w' \in S(A)$ داریم:

$$(\lambda w + (L_\lambda)w')(a) = \lambda w(a) + (1-\lambda)w'(a)$$

یا به‌طور معادل

$$\int_{\Omega(A)} \hat{a} d\mu_{\lambda w+(1-\lambda)w'} = \lambda \int_{\Omega(A)} \hat{a} d\mu_w + (1-\lambda) \int_{\Omega(A)} \hat{a} d\mu_{w'} = \int_{\Omega(A)} \hat{a} d(\lambda\mu_w + (1-\lambda)\mu_{w'})$$

رابطهٔ فوق نتیجه می‌دهد که

$$\mu_{\lambda w+(1-\lambda)w'} = \lambda\mu_w + (1-\lambda)\mu_{w'}$$

که آفین بودن I را نشان می‌دهد. به‌علاوه، I یک‌به‌یک است، چرا که اگر $w, w' \in S(A)$ و $w \neq w'$ آنگاه عنصر $a \in A$ موجود است به‌گونه‌ای که $w(a) \neq w(a')$. پس $\int_{\Omega(A)} \hat{a} d\mu_w \neq \int_{\Omega(A)} \hat{a} d\mu_{w'}$ و درنتیجه $\mu_w \neq \mu_{w'}$.

پوشایی I نیز نتیجهٔ مستقیمی از پوشایی $\Phi \to C(\Omega(A))$ است. □

تعریف ۸.۳. فرض کنید $\Phi : A \to C(\Omega(A))$ ایزومورفیسم مربوط به قضیه ۸.۲ باشد. برای C^*- دستگاه دینامیکی $\alpha : A \to A$ نگاشت بالابر $\widetilde{\alpha}: C(\Omega(A)) \to C(\Omega(A))$ را به‌صورت زیر تعریف می‌کنیم:

$$\widetilde{\alpha} := \Phi \circ \alpha \circ \Phi^{-1}.$$

تعریف ۹.۳. فرض کنید $A \to A$ یک C^*-دستگاه دینامیکی بوده و $\widetilde{\alpha}$ نگاشت بالابر متناظر آن باشد. مجموعهٔ متشکل از کلیهٔ اندازه‌های احتمال $\mu : \mathcal{B}_{C(\Omega(A))} \to [0, 1]$ با این خاصیت که

$$\forall g \in C(\Omega)) : \int_{\Omega(A)} \widetilde{\alpha}\ (g) d\mu = \int_{\Omega(A)} g d\mu$$

را با نماد $M(A, \widetilde{\alpha})$ نمایش می‌دهیم. به‌علاوه، مجموعهٔ کلیهٔ اعضای $\mu \in M(A, \widetilde{\alpha})$ که در آن برای هر $g \in C(\Omega(A))$، رابطهٔ $\widetilde{\alpha}\ (g) = g$ نتیجه دهد $g = c$ ثابت برای μ- تقریباً هر g در $C(\Omega(A))$، را با نماد $E(A, \widetilde{\alpha})$ نمایش می‌دهیم.

نتیجه ۱۰.۳. چون برای هر $w \in S(A)$ داریم

$$C(\overline{\Omega(A)})^{L^1(\mu_w)} = L^1(\mu_w)$$

آنگاه رابطهٔ

$$\int_{\Omega(A)} g d\mu_w = g(w)$$

برای هر تابع اندازه‌پذیر و کران‌دار g بر $C(\Omega(A))$ نیز برقرار خواهد بود.

لم ۱۱.۳. ۱. $w \in S(A,\alpha)$ اگر و تنها اگر $\mu_w \in M(A,\widetilde{\alpha})$.
۲. $w \in S_e(A,\alpha)$ اگر و تنها اگر $\mu_w \in E(A,\widetilde{\alpha})$.

اثبات. ۱. فرض کنید $w \in S(A,\alpha)$. به‌علاوه فرض کنید $g \in C(\Omega(A))$. عنصر $a \in A$ را چنان در نظر بگیرید که $g = \hat{a} = \Phi(a)$. در این صورت

$$\begin{aligned}\int_{\Omega(A)} \widetilde{\alpha}\,(g) d\mu_w &= \int_{\Omega(A)} \widetilde{\alpha}\,(\Phi(a)) d\mu_w = \int_{\Omega(A)} \Phi(\alpha(a)) d\mu_w = \int_{\Omega(A)} \widehat{\alpha(a)} d\mu_w \\ &= \widehat{\alpha(a)}(w) = (w\circ\alpha)(a) = w(a) = \hat{a}(w) = \int_{\Omega(A)} g d\mu_w.\end{aligned}$$

بنابراین $\mu_w \in M(A,\widetilde{\alpha})$.
برعکس فرض کنید $\mu_w \in M(A,\widetilde{\alpha})$. برای هر $a \in A$ داریم:

$$\int \widetilde{\alpha}\,(\hat{a}) d\mu_w = \int \hat{a} d\mu_w$$

یا به‌طور معادل:

$$\int_{\Omega(A)} \widetilde{\alpha}\,(\Phi(a)) d\mu_w = \int_{\Omega(A)} \hat{a} d\mu_w$$

و درنتیجه

$$\begin{aligned}(wo\alpha)(a) &= \widehat{\alpha(a)}(w) = \int_{\Omega(A)} \widehat{\alpha(a)} d\mu_w = \int_{\Omega(A)} \Phi(\alpha(a)) d\mu_w \\ &= \int_{\Omega(A)} \widetilde{\alpha}\,(\Phi(a)) d\mu_w = \int_{\Omega(A)} \hat{a} d\mu_w = w(a).\end{aligned}$$

به‌عبارت‌دیگر $w \circ \alpha = w$ پس $w \in S(A,\alpha)$.
۲. فرض کنید $w \in S_e(A,\alpha)$. به‌علاوه فرض کنید $g \in C(\Omega(A))$ به‌گونه‌ای باشد که $\widetilde{\alpha}\,(g) = g$. عضو $a \in A$ را طوری در نظر بگیرید که $\hat{a} = \Phi(a) = g$. پس $\Phi\alpha\Phi^{-1}(g) = g$ و درنتیجه $\alpha\Phi^{-1}(g) = \Phi^{-1}(g)$ و یا $\alpha(a) = a$. حال چون $w \in S_e(A,\alpha)$ پس $\hat{a} = g$ ثابت است μ_w-تقریباً همه‌جا. بنابراین $\mu_w \in E(A,\widetilde{\alpha})$. با برعکس کردن روند اثبات اخیر برعکس حکم نیز ثابت می‌شود. □

نتیجه ۱۲.۳. به کمک روش اثبات قضیه ۱۰.۶ در مرجع [۲۰] به‌سادگی می‌توان نشان داد که $ext(M(A,\widetilde{\alpha})) = E(A,\widetilde{\alpha})$.

قضیهٔ زیر نیز برای حالت‌ها برقرار است.

قضیه ۱۳.۳. داریم $ext(S(A,\alpha)) = S_e(A,\alpha)$.

اثبات. حکم با توجه به آفین بودن نگاشت $I : S(A) \to M_1(\Omega(A))$ و لم ۱۱.۳ برقرار است. □

قضیه ۱۴.۳. (قضیهٔ شوکه) فرض‌کنید Y یک زیرمجموعهٔ فشردهٔ متریک‌پذیر محدب از فضای موضعاً محدب E باشد و $x_\circ \in Y$. در این صورت اندازهٔ احتمال σ بر زیرمجموعه‌های بورل Y موجود است به‌گونه‌ای که $\sigma(ext(Y)) = 1$ و برای هر تابعک خطی Φ بر E داریم $\Phi(x_\circ) = \int_Y \Phi d\sigma$.

نتیجهٔ زیر از قضیهٔ شوکه [۸] به دست می‌آید:

نتیجه ۱۵.۳. برای هر $w \in S(A,\alpha)$، اندازهٔ احتمال σ بر زیرمجموعهٔ بورل $S(A,\alpha)$ موجود است به‌گونه‌ای که $\sigma(S_e(A,\alpha)) = ۱$ و برای هر تابع کران‌دار $f : \Omega(A) \to \mathbb{R}$ داریم:

$$\int_{\Omega(A)} f d\mu_w = \int_{S_e(A,\alpha)} \left(\int_{\Omega(A)} S d\mu_v \right) d\sigma(\nu).$$

اثبات. کافیست قضیهٔ شوکه را برای $E = A^*$ و $Y = S(A,\alpha)$ و تابعک خطی $\Phi : E \to \mathbb{C}$ با ضابطهٔ $\Phi(w) = \int_{\Omega(A)} f d\mu_w$، که در آن f تابعی کران‌دار است، در نظر بگیریم. □

References

[1] Abadie, B., & Dykema, K. (2009). Unique ergodicity of free shifts and some other automorphisms of C^*-algebras. *J. Operator Theory*, 61, 279–294.

[2] Accardi, L., & Mukhamedov, F. (2009). A note on noncommutative unique ergodicity and weighted means. *Linear Algebra Appl*, 430, 782–790. DOI: https://doi.org/10.1016/j.laa.2008.09.029.

[3] Austin, T., Eisner, T., & Tao, T. (2011). Nonconventional ergodic averages and multiple recurrence for von Neumann dynamical systems. *Pacific J. Math*, 250, 1–60. DOI: https://doi.org/10.2140/pjm.2011.250.1.

[4] Beyers, C., Duvenhage, R., & Stroh, A. (2010). The Szemeredi property in ergodic W^*-dynamical systems. *J. Operator Theory*, 64, 35–67.

[5] Birkhoff, G.D. (1931). Proof of the ergodic theorem. *Proc. Natl. Acad. Sci*, 17, 656–660. DOI: https://doi.org/10.1073/pnas.17.2.656.

[6] Connes, A., Narnhofer, H., & Thirring, W. (1987). Dynamical entropy of C^*-Algebras and von Neumann algebras. *Commun. Math. Phys*, 112, 691–719. DOI: https://doi.org/10.1007/BF01225381.

[7] Fidaleo, F. (2009). An ergodic theorem for quantum diagonal measures. *Infin. Dimens. Anal. Quantum Probab. Relat. Top*, 12, 307–320. DOI: https://doi.org/10.1142/S0219025709003665.

[8] Fidaleo, F. (2009). On strong ergodic properties of quantum dynamical systems. *Infin. Dimens. Anal. Quantum Probab. Relat. Top*, 12, 551–564. DOI: https://doi.org/10.1142/S0219025709003884.

[9] Kolmogorov, A.N. (1958). New metric invariant of transitive dynamical systems and endomorphisms of Lebesgue spaces. *Doklady of Russian Academy of Sciences*, 119, 851–864.

[10] Murphy, G.J. (1990). C^*-Algebras and Operator Theory. *Academic Press, Inc*. DOI: https://doi.org/10.1016/C2009-0-22289-6.

[11] Niculescu, C.P., Stroh, A., & Zsido, L. (2003). Noncommutative extensions of classical and multiple recurrence theorems. *J. Operator Theory*, 50, 3–52.

[12] Phelps, R. (2001). Lectures on Choquet's Theorem. *Springer-Verlag Berlin, Heidelberg (originally published by Van Nostrand, Princeton, 1966)*. DOI: https://doi.org/10.1007/b76887.

[13] Ruelle, D. (1973). Statistical mechanics on a compact set with $\mathbb{Z}^\nu$-action satisfying expansiveness and specification. *Trans. Amer. Math. Soc*, 185, 237–251. DOI: https://doi.org/10.2307/1996437.

[14] Ruelle, D. (2004). Thermodynamic formalism. *Cambridge Mathematical Library. Cambridge University Press, second edition, The mathematical structures of equilibrium statistical mechanics*. DOI: https://doi.org/10.1017/CBO9780511617546.

[15] Sinai, Ya.G. (1959). On the notion of entropy of a dynamical system. *Doklady of Russian Academy of Sciences*, 124, 768–771. DOI: https://doi.org/10.1007/978-0-387-87870-6_1.

[16] Von Neumann, J. (1932). Proof of the Quasi-ergodic Hypothesis. *Proc. Natl. Acad. Sci*, 18, 70–82. DOI: https://doi.org/10.1073/pnas.18.1.70.

[17] Von Neumann, J. (1932). Physical Applications of the Ergodic Hypothesis. *Proc. Natl. Acad. Sci*, 18, 263–266. DOI: https://doi.org/10.1073/pnas.18.3.263.

[18] Von Neumann, J. (1999). Invariant measures. *American Mathematical Society*, ISBN 978-0-8218-0912-9.

[19] Walters, P. (1975). A variational principle for the pressure of continuous transformations. *Amer. J. Math*, 97, 937–971. DOI: https://doi.org/10.2307/2373682.

[20] Walters, P. (1982). An Introduction to Ergodic Theory. *Springer-Verlag*.

[21] Walters, P. (1986). Relative pressure, relative equilibrium states, compensation functions and many-to-one codes between subshifts. *Trans. Amer. Math. Soc*, 296, 1–31. DOI: https://doi.org/10.2307/2000558.

Measure Algebras and Applications

Invariant measures of action of amenable groups and their entropy

AliReza Alehafttan[1]✉, **Hossein Kasiri**[2], **Mehran Hosseinzadeh Dizaj**[3]

1. Corresponding Author, Department of Mathematics, Jundi-Shapur University of Technology, Dezful, Iran. Email: a.r.alehafttan@jsu.ac.ir
2. Department of Mathematics, Jundi-Shapur University of Technology, Dezful, Iran. Email: hossein_kasiry@jsu.ac.ir
3. Department of Electrical Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran. Email: meh.hosseinzadehdizaj@iauctb.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 12 April 2024
Received in revised form: 17 June 2024
Accepted: 26 June 2024
Published Online: 20 August 2024

Keywords:
Amenable group,
Følner sequence,
Information function,
Entropy

2020 Mathematics Subject Classification: 37A35

ABSTRACT

In this article, with the help of the concept of diagonal measure, we define an information function for the amenable group action on a compact metric space and then obtain the entropy of the group action from it. In other words, we show that the integral of the defined information function will be equal to the entropy of the amenable group action.

Cite this article: Alehafttan, A.R., Kasiri, H., & Hosseinzadeh Dizaj, M. (2024). Invariant measures of action of amenable groups and their entropy. *Measure Algebras and Applications*, 1(2), 130–141. http://doi.org/10.22091/maa.2024.10600.1018

Publisher: University of Qom

DOI: 10.22091/maa.2024.10600.1018

Extended Abstract

Introduction

In the classical ergodic theory, the concept of entropy is defined for measure-preserving $\mathbb{Z}$-actions. The definition of entropy is stated via different approaches, but with the same origin [1, 3, 4, 12–14, 17, 19].

Entropy of $\mathbb{Z}$-actions is generalized to actions of general amenable groups. To have a nice entropy theory for actions of amenable groups, the concept of Følner sequence is applied. A Følner sequence, for an action, is a sequence of finite sets that exhaust the space and do not move too much when acted on by any group element.

Many classical results for $\mathbb{Z}$-actions, such as Shannon-McMillan-Brieman theorem [2, 6, 17], Ergodic theorems [21, 23–25] and Rokhlin-Sinai results [16], are generalized for actions of general amenable groups.

Traditionally, the entropy of an action is a non-negative extended real number which is invariant under isomorphism. For $\mathbb{Z}$-actions it is replaced by linear operators on Banach spaces [12, 13].

In this paper, we introduce a function corresponding to the action of an amenable group, which contains the entropy of the group's action. In other words, the entropy of the group action is obtained by integrating this function, which we call the information function. With the help of information functions, entropy operators can be introduced, and a spectral approach to the concept of entropy of the action of a group is presented.

Conclusion

In this paper, the following definitions and results are applied.

***Definition* 0.1.** *Suppose that G is a topological group acting on a probability space $(X, \mathcal{B}, \mu)$ such that the action $G \times X \to X$ is measurable. The measure μ is called G-invariant if $\mu(gA) = \mu(A)$ for any $g \in G$.*

***Definition* 0.2.** *An invariant measure μ is called ergodic if, for any measurable set A we have*

$$\forall g \in A, \quad gA = A \Longrightarrow \mu(A) = 0 \quad or \quad \mu(A) = 1.$$

The collection of all probability measures on $\mathcal{B}$ is denoted by $M(X)$ and the collection of all G-invariant measures on $\mathcal{B}$ is denoted by $M(G, X)$. We also write $E(G, X)$ for the collection of all ergodic measures.

It is known that $M(X)$, equipped by the weak* topology, is a compact metrizable space [22]. The proof of the following theorem is similar to [22] Theorem 6.10.

***Theorem* 0.3.** *Suppose that G acts on a metric space X and μ is a G-invariant measure on β_X, the σ-algebra of Borel sets of X, then*

1. *$M(G, X)$ is a compact subset of $M(X)$;*
2. *$M(G, X)$ is convex;*

3. *$ext(M(G,X)) = E(G,X)$, i.e., the collection of ergodic measures equals the extreme points of the collection of G-invariant measures.*

In the following, we recall the Choquet's representation theorem.

***Theorem* 0.4.** *(Phelps [8]) Suppose that Y is a compact convex metrizable subset of a locally convex space E, and that $x_0 \in Y$. Then there exists a probability measure τ on Y which represents x_0 and is supported by the extreme points of Y, i.e., $\Psi(x_0) = \int_Y \Psi d\tau$ for every continuous linear functional Ψ on E, and $\tau(ext(Y)) = 1$.*

Let $\mu \in M(G,X)$ and $f : X \to \mathbb{R}$ be a bounded measurable function. Since we know that $E(G,X)$ agrees with the set of extreme points of $M(X,\phi)$, applying Choquet's representation theorem for $Y = M(G,X)$ and $\Psi(\mu) = \int_X f d\mu$, we will have the following corollary:

***Corollary* 0.5.** *Suppose that G is a topological group acting continuously on the compact metric space X. Then for each $\mu \in M(G,X)$ there is a unique measure $\tau = \tau_\mu$ on the Borel subsets of the compact metrizable space $M(G,X)$ such that $\tau_\mu(E(G,X)) = 1$ and*

$$\int_X f(x)d\mu(x) = \int_{E(G,X)} \left(\int_X f(x)dm(x) \right) d\tau_\mu(m)$$

for every bounded measurable function $f : X \to \mathbb{R}$.

Under the assumptions of Corollary 0.5, we write $\mu = \int_{E(G,X)} m d\tau_\mu(m)$ and it is called the ergodic decomposition of μ.

Suppose that G is a countable and discrete group. There are many equivalent formulations for the concept of amenability. In the discrete case, one of the convenient definitions of amenability for discrete groups is as follows:

A dicrete group G is amenable if for any finite set $K \subset G$ and $\delta > 0$ there is a finite set $F \subset G$ such that

$$\forall k \in K \quad |F \Delta kF| < \delta |F|.$$

Such a set F is called (K,δ)-invariant.

A sequence $\{F_n\}_{n\geq 1}$ of finite subsets of G is called a Følner sequence if for any K and $\delta > 0$, F_n is (K,δ)-invariant, for all large enough n. Without loss of generality, we may assume that $|F_n| \geq n$.

Assume that G acts from the left on a measure space $(X, \mathcal{B}, \mu)$ with $\mu(X) = 1$. Let also μ preserve the action of G on X. We have the following mean ergodic theorem for amenable groups. It may easily be proved by the same method applied for $\mathbb{Z}$-actions.

***Theorem* 0.6.** *If G is amenable and acts ergodically on $(X, \mathcal{B}, \mu)$, then for any $f \in L^1(\mu)$, and Følner sequence $\{F_n\}_{n\geq 1}$,*

$$A(F_n, f)(x)_{n\to\infty} \longrightarrow \int_X f d\mu \quad in \quad L^1(\mu)$$

where

$$A(F_n, f)(x) := \frac{1}{|F|} \sum_{g\in F} f(gx).$$

The pointwise version of Theorem 0.6 does not necessarily hold for any given Følner sequence [5]. The following definition is introduced in [18].

***Definition* 0.7.** *(A. Shulman) A sequence of sets $\{F_n\}_{n\geq 1}$ is said to be tempered if for some $c > 0$ and all $n \in \mathbb{N}$,*

$$|\bigcup_{k\leq n} {F_k}^{-1}F_{n+1}| \leq c|F_{n+1}|.$$

A version of the maximal ergodic theorem was proved for tempered sequences [20]. We also have the following for tempered Følner sequences [5].

***Theorem* 0.8.** *(Pointwise ergodic theorem) Let G be an amenable group acting on a measure space $(X, \mathcal{B}, \mu)$, and let $\{F_n\}_{n\geq 1}$ be a tempered Følner sequence. Then for any $f \in L^1(\mu)$,*

$$\lim_{n\to\infty} A(F_n, f)(x) = \int_X f d\mu \quad a.e.$$

A space $(X, \mathcal{B}, \mu)$ on which acts, together with a partition $\mathcal{P}$ of X, is called a process.

If $x \in X$ and $\mathcal{P}$ is a partition, then we denote the unique element of $\mathcal{P}$ containing x by $\mathcal{P}(x)$. If also, $F \subset G$ we set

$$\mathcal{P}^F := \bigvee_{g\in F} g^{-1}\mathcal{P}$$

where $\bigvee$ denotes the joint operation on the set of finite partitions.
We recall the definition of the entropy of a process.

***Definition* 0.9.** *For any $F \subset G$ and $\epsilon > 0$, we set*

$$b(F, \epsilon, \mathcal{P}) := \min\{|\mathcal{C}| : \mathcal{C} \subset \mathcal{P}^F, \mu(\cup\mathcal{C}) > 1 - \epsilon\}.$$

Then the entropy $h_\mu(\mathcal{P})$ is defined as

$$h_\mu(\mathcal{P}) := \lim_{\epsilon\to\infty} \liminf_{n\to\infty} \frac{\log b(F_n, \epsilon, \mathcal{P})}{|F_n|}$$

where $\{F_n\}_{n\geq 1}$ is a Følner sequence for G.

The following is a generalized version of the Shannon-McMillan-Breiman theorem [5].

***Theorem* 0.10.** *Let $\mathcal{P}$ be a finite partition, and assume that G is an amenable group acting ergodically on a measure space $(X, \mathcal{B}, \mu)$. Let $h_\mu(\mathcal{P})$ denote the entropy of this process. Assume that $\{F_n\}_{n\geq 1}$ is a tempered sequence of Følner sets. Then for almost every x,*

$$\frac{-\log(\mu(\mathcal{P}^{F_n}(x)))}{|F_n|} \longrightarrow h_\mu(\mathcal{P}) \quad as \quad n \to \infty.$$

Information kernel for action of amenable groups

In the rest of the paper, let X be a metric space and β_X be the σ-algebra of all Borel partitions. Let G be an amenable group acting on the space (X, β_X), $\mu \in M(G, X)$ and $\mathcal{P}$ be a measurable partition of X. Let also $\{F_n\}_{n\geq 1}$ be a tempered Følner sequence of G. We may assume that $|F_{n+1}| \geq |F_n|$.

***Definition* 0.11.** *For $x, y \in X$ and $n \in \mathbb{N}$, we set*

$$\tau_n(x, y; \mathcal{P}) := \limsup_{m\to\infty} \frac{1}{|F_m|} card(\{g \in F_m : y \in g^{-1}\mathcal{P}^{F_n}(x)\})$$

and

$$\tau_n^*(x, y; \mathcal{P}) := \begin{cases} -\frac{1}{|F_n|}\log \tau_n(x, y; \mathcal{P}) & : \tau_n(x, y; \mathcal{P}) \neq 0 \\ 0 & : \tau_n(x, y; \mathcal{P}) = 0 \end{cases}$$

***Remark* 0.12.** *For $x, y \in X$ and a partition $\mathcal{P}$, the sequence $\{\tau_n^*(x, y; \mathcal{P})\}_{n\geq 1}$ is increasing.*

Note that, the previous remark holds because of the following reason:
Let $k \leq n$. The partition $\mathcal{P}^{F_n}$ is finer than $\mathcal{P}^{F_k}$ therefore, if $x \in X$, then $\mathcal{P}^{F_n}(x) \subset \mathcal{P}^{F_k}(x)$ and consequently $g^{-1}\mathcal{P}^{F_n}(x) \subset g^{-1}\mathcal{P}^{F_k}(x)$ for any $g \in G$. Now, for $m \in \mathbb{N}$ we have

$$\{g \in F_m : y \in g^{-1}\mathcal{P}^{F_n}\} \subset \{g \in F_m : y \in g^{-1}\mathcal{P}^{F_k}\}$$

which easily results in $\tau_n(x, y; \mathcal{P}) \leq \tau_k(x, y; \mathcal{P})$, therefore $\tau_k^*(x, y; \mathcal{P}) \leq \tau_n^*(x, y; \mathcal{P})$.

By Remark 0.12, $\lim_{n\to\infty} \tau_n^*(x, y; \mathcal{P})$ exists as an extended real non-negative number. So, we may have the following definition:

***Definition* 0.13.** *For $x, y \in X$ and the partition $\mathcal{P}$ of X, set*

$$I_G(x, y) := \lim_{n\to\infty} \tau_n^*(x, y; \mathcal{P}).$$

The function $I_G : X \times X \to [0, +\infty]$ is called the information kernel of G-action on X.

Before we mention our first main result, we need to note that, when G is an amenable countably infinite discrete group, for any finite measurable partition $\mathcal{P}$ of X and any $\mu \in M(G, X)$, one has the equality

$$h_\mu(\mathcal{P}) = \int_{E(G,X)} h_m(\mathcal{P}) d\tau_\mu(m) \tag{0.1}$$

where $\mu = \int_{E(G,X)} m d\tau_\mu(m)$ is the ergodic decomposition of μ. One can deduce (0.1) from [7] Propositions 5.3.2 and 5.3.5, and the proof in the case $G = \mathbb{Z}$ in [22] Theorem 8.4. (i).

***Definition* 0.14.** *Let $\mu \in M(G, X)$ and $\mu = \int_{E(G,X)} m d\tau(m)$ be the ergodic decomposition of μ. Then the diagonal measure of μ is defined by*

$$diag(\mu)(D) = \int_{M(G,X)} (m \times m)(D) d\tau(m) = \int_{E(G,X)} (m \times m)(D) d\tau(m).$$

The following theorem is our main result.

***Theorem* 0.15.** *Given any partition $\mathcal{P}$, $h_\mu(\mathcal{P}) < +\infty$ if and only if $I_G \in L^1(X \times X, \mu \times \mu)$; moreover, under the previous condition we have*

$$||I_G||_{L^1(X\times X, \mu\times\mu)} = h_\mu(\mathcal{P}).$$

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۴۱-۱۳۰

اندازه‌های پایای عمل گروه‌های میانگین‌پذیر و آنتروپی آن‌ها

علی‌رضا آل هفت تن [۱]✉ ، حسین کثیری [۲] ، مهران حسین زاده دیزج [۳]

۱. نویسندهٔ مسئول، گروه ریاضی، دانشگاه صنعتی جندی شاپور دزفول، ایران. رایانامه: a. r. alehafttan@jsu. ac. ir
۲. گروه ریاضی، دانشکده علوم پایه، دانشگاه صنعتی جندی شاپور دزفول، ایران. رایانامه: hossein_kasiry@jsu. ac. ir
۳. گروه مهندسی برق، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: meh. hosseinzadehdizaj@iauctb. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۱/۲۴
تاریخ بازنگری: ۱۴۰۳/۳/۲۸
تاریخ پذیرش: ۱۴۰۳/۴/۶
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
گروه میانگین‌پذیر،
دنبالهٔ فولنر،
تابع اطلاعات،
آنتروپی

رده‌بندی ریاضی:
37A35

چکیده

در این مقاله، به کمک مفهوم اندازهٔ قطری، یک تابع اطلاعات برای عمل گروه میانگین‌پذیر بر یک فضای متریک فشرده تعریف کرده و سپس آنتروپی عمل گروه را از آن به دست می‌آوریم. به‌عبارت‌دیگر، نشان می‌دهیم که انتگرال از تابع اطلاعات تعریف‌شده نسبت به اندازهٔ قطری برابر با آنتروپی عمل گروه میانگین‌پذیر خواهد شد.

استناد: آل هفت تن، علی‌رضا.، کثیری، حسین.، حسین زاده دیزج ، مهران. (۱۴۰۳). اندازه‌های پایای عمل گروه‌های میانگین‌پذیر و آنتروپی آن‌ها. جبرهای اندازه و کاربردها، ۱(۲)، ۱۴۱-۱۳۰.

http://doi.org/10.22091/maa.2024.10600.1018

ناشر: دانشگاه قم.

۱ مقدمه

مفهوم آنتروپی در نظریهٔ ارگودیک، با رویکردهای مختلفی مورد مطالعه قرار گرفته است [۱، ۳، ۴، ۱۲–۱۴، ۱۷، ۱۹]. در نظریهٔ کلاسیک ارگودیک، این مفهوم برای عمل $\mathbb{Z}$ بر یک فضای اندازه، که اندازهٔ موجود روی فضا را حفظ می‌کند، تعریف می‌شود. این مفهوم برای اعمال گروه‌های میانگین‌پذیر تعمیم پیدا می‌کند. بدین منظور نیازمند دنبالهٔ فولنر می‌باشیم. یک دنبالهٔ فولنر برای یک عمل گروه، جایگزینی است برای دنبالهٔ اعداد طبیعی که در تعریف آنتروپی عمل $\mathbb{Z}$ در نظریهٔ کلاسیک ارگودیک مورد استفاده قرار می‌گیرد.
قضایای کلاسیک زیادی در نظریهٔ کلاسیک ارگودیک، برای عمل گروه‌های میانگین‌پذیر تعمیم یافته‌اند. به‌طور مثال، قضیهٔ شانون-مک میلان-بریمن [۲، ۶، ۱۷]، قضایای ارگودیک [۲۱، ۲۳–۲۵] و قضایای روخلین-سینای [۱۶]، برای عمل گروه‌های میانگین‌پذیر تعمیم یافته‌اند. به‌طور سنتی، آنتروپی، یک عدد نامنفی حقیقی است که تحت یکریختی پایاست. برای عمل گروه $\mathbb{Z}$، این عدد با عملگر فضای خطی بر فضاهای باناخ جایگزین شده است [۱۲، ۱۳]. در این مقاله به معرفی تابعی متناظر با عمل یک گروه میانگین‌پذیر می‌پردازیم که در درون خود، آنتروپی عمل گروه را نهفته دارد. به‌عبارت‌دیگر، آنتروپی عمل گروه با انتگرال‌گیری از این تابع، که به آن تابع اطلاعات می‌گوییم، به دست می‌آید. به کمک توابع اطلاعات می‌توان عملگرهای آنتروپی را معرفی کرده و رویکردی طیفی به مفهوم آنتروپی عمل یک گروه ارائه داد.

۲ پیش‌نیازها

در این بخش، پیش‌نیازهایی را که در ادامهٔ مقاله مورد استفاده قرار می‌گیرند، از نظر خواهیم گذراند.

تعریف ۱.۲. فرض کنیم G گروهی توپولوژیک باشد که بر فضای احتمال (X, β, μ) عمل می‌کند به‌گونه‌ای که این عمل به‌عنوان تابعی از $G \times X$ به X، اندازه‌پذیر است. در این صورت اندازهٔ μ را G-پایا نامیم هرگاه داشته باشیم

$$\forall A \in \beta, \quad \forall g \in G \quad : \quad \mu(gA) = \mu(A).$$

تعریف ۲.۲. اندازهٔ G-پایای μ را ارگودیک می‌نامیم هرگاه برای هر مجموعهٔ اندازه‌پذیر A در X داشته باشیم

$$\forall g \in A \quad : \quad gA = A \Longrightarrow \mu(A) = ۰ \quad \text{یا} \quad \mu(A) = ۱.$$

مجموعهٔ کلیهٔ اندازه‌های احتمال بر X را با $M(X)$ و مجموعهٔ همهٔ اندازه‌های G-پایا بر X را با $M(G, X)$ نمایش می‌دهیم. به‌علاوه، مجموعهٔ تمام اندازه‌های ارگودیک را با $E(G, X)$ نشان خواهیم داد.
روشن است که $M(X)$ مجهز به توپولوژی ضعیف-ستاره بوده و نسبت به این توپولوژی فشرده و متریک‌پذیر است [۲۲].
اثبات قضیهٔ زیر مشابه اثبات قضیه ۶.۱۰ از مرجع [۲۲] است.

قضیه ۳.۲. فرض کنیم G گروهی توپولوژیک باشد که بر فضای متریک فشرده X عمل می‌کند و μ نیز اندازه‌ای G-پایا بر مجموعه‌های بورل X باشد. در این صورت

۱. $M(G, X)$ زیرمجموعه‌ای فشرده از $M(X)$ است.

۲. $M(G, X)$ محدب است.

۳. مجموعهٔ نقاط گوشه‌ای $M(G, X)$ برابر $E(G, X)$ است.

قضیهٔ زیر به قضیهٔ شوکه [۸] معروف است.

قضیه ۴.۲. فرض کنیم Y یک زیرمجموعهٔ فشرده و محدب و متریک‌پذیر از یک فضای برداری محدب موضعی E بوده و $x_۰ \in Y$. در این صورت اندازهٔ احتمال τ بر زیرمجموعه‌های بورل Y موجود است به‌گونه‌ای که $\tau(ext(Y)) = ۱$ و برای هر تابعک خطی پیوسته $\psi : E \longrightarrow \mathbb{R}$ داریم

$$\psi(x_۰) = \int_Y \psi \, d\tau.$$

قضیه ۵.۲. فرض کنیم G یک گروه توپولوژیک با عمل پیوسته بر فضای متریک فشرده X باشد. در این صورت برای هر $\mu \in M(G,X)$، اندازهٔ احتمال یکتای $\tau = \tau_\mu$ بر زیرمجموعه‌های بورل $M(G,X)$ موجود است به‌گونه‌ای که $\tau(E(G,X)) = ۱$ و به‌علاوه برای هر تابع اندازه‌پذیر و کران‌دار $f : X \longrightarrow \mathbb{R}$ داریم

$$\int_X f(x)\, d\mu(x) = \int_{E(G,X)} \left(\int_X f(x)\, dm(x) \right) d\mu(m).$$

اثبات. فرض کنیم $\mu \in M(G,X)$ و $f : X \longrightarrow \mathbb{R}$ تابعی اندازه‌پذیر و کران‌دار باشد. چون $E(G,X) = ext(M(G,X))$، حکم از به‌کارگیری قضیهٔ شوکه برای $Y = M(G,X)$ و تابعک $\psi = \int_X f\, d\mu$ به دست می‌آید. □

تحت شرایط قضیه ۵.۲ می‌نویسیم $\mu = \int_{E(G,X)} m\, d\tau(m)$ و آن را تجزیهٔ ارگودیک μ می‌نامیم.

فرض کنیم G یک گروه گسستهٔ شمارش‌پذیر باشد. فرمول‌بندی‌های معادل زیادی برای مفهوم میانگین‌پذیری وجود دارد. در حالت گسسته، تعریف معادل زیر را داریم.

تعریف ۶.۲. گروه توپولوژیک گسستهٔ G را میانگین‌پذیر می‌نامیم هرگاه برای هر زیرمجموعهٔ متناهی $K \subset G$ و هر $\delta > ۰$، زیرمجموعهٔ متناهی $F \subset G$ موجود باشد به‌گونه‌ای که

$$\forall k \in K \quad : \quad | F \Delta kF | < \delta \, | F | .$$

چنین مجموعه‌ای مانند تعریف ۶.۲ را (K,δ)-پایا می‌نامیم.

دنبالهٔ $\{F_n\}_{n\in\mathbb{N}}$ از زیرمجموعه‌های متناهی G را دنبالهٔ فولنر نامیم، هرگاه برای هر K و هر $\delta > ۰$ و به‌ازای هر n به قدر کافی بزرگ، F_n، (K,δ)-پایا باشد. بدون کاستن از کلیت، می‌توان فرض کرد $| F_n | \geqslant n$.

فرض کنیم G از چپ بر فضای احتمال (X,β,μ) عمل کند. به‌علاوه فرض کنیم μ حافظ عمل G باشد. قضیهٔ ارگودیک میانگین زیر، به‌سادگی برای عمل $\mathbb{Z}$ بر X ثابت می‌شود.

قضیه ۷.۲. اگر G میانگین‌پذیر بوده و به‌طور ارگودیک بر (X,β,μ) عمل کند، آنگاه برای هر $f \in L^۱(\mu)$ و هر دنبالهٔ فولنر $\{F_n\}_{n\in\mathbb{N}}$ داریم

$$A(F_n, f)(x) \underset{n\to\infty}{\longrightarrow} \int_X f\, d\mu,$$

در $L^۱(\mu)$ که در آن

$$A(F_n, f)(x) = \frac{۱}{| F |} \sum_{g\in F} f(g(x)).$$

تذکر ۸.۲. همگرایی نقطه‌ای لزوماً در قضیه ۷.۲ برقرار نیست.

تعریف ۹.۲. ([۱۸]) دنبالهٔ فولنر $\{F_n\}_{n\in\mathbb{N}}$ از زیرمجموعهٔ G را تعدیل‌شده نامیم، هرگاه برای عددی مانند $c > ۰$ و هر $n \in \mathbb{N}$ داشته باشیم

$$| \bigcup_{k\leqslant n} F_k^{-۱} F_{n+۱} | \leqslant c \, | F_{n+۱} | .$$

قضیهٔ زیر برای دنباله‌های فولنر تعدیل‌شده برقرار است.

قضیه ۱۰.۲. (قضیهٔ ارگودیک نقطه‌ای) فرض کنیم G گروهی توپولوژیک و میانگین‌پذیر باشد که بر فضای اندازهٔ (X,β,μ) عمل می‌کند. به‌علاوه فرض کنید $\{F_n\}_{n\in\mathbb{N}}$ دنبالهٔ فولنر و تعدیل‌شده باشد. در این صورت برای هر $f \in L^۱(\mu)$ داریم

$$\lim_{n\to\infty} A(F_n, f)(x) = \int_X f\, d\mu.$$

تذکر ۱۱.۲. اگر P افرازی اندازه‌پذیر از (X,β,μ) بوده و $x \in X$، آنگاه عضو یکتا از P که شامل x است را با $P(x)$ نمایش می‌دهیم. به‌علاوه اگر $F \subset G$، قرار می‌دهیم

$$P^F = \bigvee_{g\in F} g^{-۱} P,$$

که در آن $\vee$ به معنای تلفیق افرازها است، یعنی؛

$$P \vee Q = \{A \cap B \quad : \quad A \in P \quad , \quad B \in Q\}.$$

تعریف ۱۲.۲. برای هر $F \subset G$ و هر $\varepsilon > ۰$ قرار می‌دهیم

$$b(F,\varepsilon,P) := min\left\{ \mid C \mid \quad : \quad C \subset P^F \quad , \quad \mu(\bigcup C) > ۱ - \varepsilon \right\}.$$

اکنون آنتروپی افراز P نسبت به μ به صورت زیر تعریف می‌شود

$$h_\mu(P) := \lim_{\varepsilon \to ۰} \lim_{n \to \infty} \frac{\log(b(F,\varepsilon,P))}{\mid F_n \mid},$$

که در آن $\{F_n\}_{n\in\mathbb{N}}$ دنبالهٔ فولنر در G است.

قضیهٔ زیر تعمیمی از قضیهٔ شانون-مک میلان-بریمن است [۵].

قضیه ۱۳.۲. فرض کنید $\mathcal{P}$ افرازی متناهی از X بوده و G گروهی میانگین‌پذیر باشد که به‌طور ارگودیک بر فضای اندازهٔ (X,β,μ) عمل می‌کند. فرض کنید $\{F_n\}_{n\geqslant ۱}$ دنبالهٔ فولنری تعدیل‌شده باشد. در این صورت برای تقریباً هر $x \in X$ داریم:

$$\lim_{n\to\infty} \frac{-\log \mu(\mathcal{P}^{F_n}(x))}{|F_n|} = h_\mu(\mathcal{P}).$$

۳ هستهٔ آنتروپی برای عمل گروه‌های میانگین‌پذیر

در این قسمت به معرفی مفهوم هستهٔ آنتروپی برای عمل یک گروه میانگین‌پذیر می‌پردازیم. در ادامهٔ این مقاله، فرض کنید X یک فضای متریک و σ-جبر بورل باشد. به‌علاوه فرض کنید G گروه میانگین‌پذیر باشد که بر (X,β_X) عمل می‌کند و $\mathcal{P}$ نیز افرازی اندازه‌پذیر از X باشد. همچنین $\mu \in M(G,X)$ و $\{F_n\}_{n\geqslant ۱}$ دنباله‌ای فولنر و تعدیل‌شده در G باشد به‌گونه‌ای که $|F_{n+۱}| \geqslant |F_n|$.

تعریف ۱.۳. برای $x,y \in X$ و $n \in \mathbb{N}$، قرار می‌دهیم

$$\tau_n(x,y,\mathcal{P}) = \limsup_{m\to\infty} \frac{۱}{|F_m|} |\{g \in F_m : y \in g^{-۱}\mathcal{P}^{F_n}(x)\}|,$$

و

$$\tau_n^*(x,y,\mathcal{P}) = \begin{cases} -\frac{۱}{|F_n|}\log \tau_n(x,y,\mathcal{P}) & \tau_n(x,y,\mathcal{P}) \neq ۰ \\ ۰ & \tau_n(x,y,\mathcal{P}) = ۰ \end{cases}.$$

به‌سادگی می‌توان دید که دنبالهٔ $\{\tau_n^*(x,y,\mathcal{P})\}_{n\geq ۱}$ صعودی است، بنابراین حد آن به‌عنوان یک عدد حقیقی تعمیم‌یافته موجود است. بنابراین تعریف زیر بامعنا است.

تعریف ۲.۳. برای $x,y \in X$ و افراز $\mathcal{P}$ از X قرار دهید

$$I_G(x,y) = \lim_{n\to\infty} \tau_n^*(x,y,\mathcal{P}).$$

تابع $I_G : X \times X \to [۰,\infty]$ را تابع اطلاعات عمل G بر X می‌نامیم.

قبل از بیان و اثبات مهم‌ترین خاصیت تابع اطلاعات I_G، مفهوم اندازهٔ قطری را مطرح می‌کنیم.

تعریف ۳.۳. فرض کنید $\mu \in M(G,X)$ و $\mu = \int_{E(G,X)} m d\tau(m)$ تجزیهٔ ارگودیک μ باشد. در این صورت اندازهٔ قطری μ به این صورت تعریف می‌شود

$$diag(\mu)(D) = \int_{M(G,X)} (m\times m)(D) d\tau(m) = \int_{E(G,X)} (m\times m)(D) d\tau(m).$$

توجه کنید که اندازهٔ قطری بر فضای حاصلضربی $X \times X$ تعریف می‌شود. همچنین به‌طور خاص، اگر $\mu \in E(G,X)$، آنگاه $diag(\mu) = \mu \times \mu$. اکنون آماده‌ایم تا قضیهٔ اصلی مقاله را بیان و اثبات کنیم.

قضیه ۴.۳. برای افراز $\mathcal{P}$، $h_\mu(\mathcal{P}) < \infty$ اگر و تنها اگر $I_G \in L^1(X \times X, \mu \times \mu)$. به‌علاوه تحت فرض فوق داریم

$$||I_G||_{L^1(X\times X, diag(\mu))} = h_\mu(\mathcal{P}).$$

اثبات. ابتدا فرض کنید $\mu \in E(G, X)$. در این صورت $diag(\mu) = \mu \times \mu$. فرض کنید $x, y \in X$ و $n \in \mathbb{N}$. در این صورت برای تقریباً هر $y \in X$ با توجه به قضیه ۱۳.۲ داریم:

$$\begin{aligned}
\tau_n(x, y, \mathcal{P}) &= \limsup_{k\to\infty} \frac{1}{|F_k|} |\{g \in F_k : y \in g^{-1}\mathcal{P}^{F_n}(x)\}| \\
&= \limsup_{k\to\infty} \frac{1}{|F_k|} \sum_{g\in F_k} \chi_{g^{-1}\mathcal{P}^{F_n}(x)}(y) \\
&= \limsup_{k\to\infty} \frac{1}{|F_k|} \sum_{g\in F_k} \chi_{\mathcal{P}^{F_n}(x)}(gy) \\
&= \limsup_{k\to\infty} A(F_k, \chi_{\mathcal{P}^{F_n}(x)}(y) \\
&= \int_X \chi_{\mathcal{P}^{F_n}(x)}(y) d\mu(y) \\
&= \mu(\mathcal{P}^{F_n}(x)).
\end{aligned}$$

پس برای تقریباً هر $y \in X$ داریم:

$$\tau_n^*(x, y, \mathcal{P}) = -\frac{\log \mu(\mathcal{P}^{F_n}(x))}{|F_n|}.$$

ازاین‌رو برای تقریباً هر $x, y \in X$ داریم:

$$\lim_{n\to\infty} \tau_n^*(x, y, \mathcal{P}) = h_\mu(\mathcal{P}).$$

بنابراین برای تقریباً هر $x, y \in X$

$$I_G(x, y) = h_\mu(\mathcal{P}).$$

رابطهٔ فوق به‌سادگی نتیجه می‌دهد که

$$||I_G||_{L^1(X\times X, diag(\mu))} = ||I_G||_{L^1(X\times X, \mu\times\mu)} = h_\mu(\mathcal{P}). \quad (۱)$$

اکنون در حالت کلی فرض کنید $\mu \in M(X, G)$ و $\mu = \int_{E(G,X)} m d\tau(m)$ تجزیهٔ ارگودیک μ باشد. در این صورت اندازهٔ قطری μ عبارت است از:

$$diag(\mu) = \int_{E(G,X)} m \times m d\tau(m).$$

اکنون با توجه به رابطه (۱) و قضیهٔ ژاکوب (مرجع [۲۲]) داریم:

$$\begin{aligned}
||I_G||_{L^1(X\times X, diag(\mu))} &= \int_{X\times X} I_G d(diag(\mu)) \\
&= \int_{E(G,X)} \left(\int_{X\times X} I_G dm \times m \right) d\tau(m) \\
&= \int_{E(G,X)} h_m(\mathcal{P}) d\tau(m) = h_\mu(\mathcal{P}).
\end{aligned}$$

و اثبات کامل می‌شود. □

References

[1] Adler, R.L., Konheim, A.G., & McAndrew, M.H. (1965). Topological entropy. *Trans. Amer. Math. Soc*, 114, 309–319. DOI: https://doi.org/10.1090/S0002-9947-1965-0175106-9.

[2] Bowen, R. (1979). Invariant measures for Markov maps of the interval. *Comm. Math. Physics*, 69, 1–14. DOI: https://doi.org/10.1007/BF01941319.

[3] Brin, M., & Katok, A. (1983). On local entropy in geometric dynamics. 30–38, *New York, Springer-Verlag*, (Lecture Notes in Mathematics 1007). DOI: https://doi.org/10.1007/bfb0061408.

[4] Kolmogorov, A.N. (1958). New metric invariant of transitive dynamical systems and endomorphisms of Lebesgue spaces. *Doklady of Russian Academy of Sciences*, 119, 861–864.

[5] Lindenstrauss, E. (2001). Pointwise theorems for amenable groups. *Invent. math*, 146, 259–295. DOI: https://doi.org/10.1007/s002220100162.

[6] McMillan, B. (1953). The basic theorems of information theory. *Ann. Math. Statist*, 24, 196–219. DOI: https://doi.org/10.1214/aoms/1177729028.

[7] Ollagnier, J.M. (1985). Ergodic Theory and Statistical Mechanics. *Springer Berlin, Heidelberg*. DOI: https://doi.org/10.1007/BFb0101575.

[8] Phelps, R. (2001). Lectures on Choquet's Theorem. *Springer-Verlag Berlin, Heidelberg (originally published by Van Nostrand, Princeton, 1966)*. DOI: https://doi.org/10.1007/b76887.

[9] Rahimi, M., & Assari, A. (2020). Mutual Entropy Map for Continuous Systems on Compact Metric Spaces. *Mathematical Analysis and Convex Optimization*, 1, 49–55. DOI: https://doi.org/10.29252/maco.1.1.6.

[10] Rahimi, M., & Assari, A. (2021). On local metric pressure of dynamical systems. *Periodica Mathematica Hungarica*, 82, 223–230. DOI: https://doi.org/10.1007/s10998-020-00355-w.

[11] Rahimi, M., Assari, A., & Ramezani, F. (2016). A local approach to Yager entropy of dynamical systems. *International Journal of Fuzzy Systems*, 18, 98–102. DOI: https://doi.org/10.1007/s40815-015-0062-z.

[12] Rahimi, M., & Riazi, A. (2012). Entropy operator for continuous dynamical systems of finite topological entropy. *Bulletin of the Iranian Mathematical Society*, 38, 883–892.

[13] Rahimi, M., & Riazi, A. (2012). Entropy functional for continuous systems of finite entropy. *Acta Mathematica Scientia*, 32B, 775–782. DOI: https://doi.org/10.1016/S0252-9602(12)60057-5.

[14] Rathie, P.N. (1970). On a Generalized Entropy and a Coding Theorem. *J. Appl. Probl*, 7, 124–133. DOI: https://doi.org/10.2307/3212154.

[15] Réyni, A. (1961). On Measures of Entropy and Information. *Proc. 4th Berk. Symp. Math Statist. and Probl., University of California Press*, Vol. 1, 547–561.

[16] Rokhlin, V.A., & Sinai, Ya.G. (1961). The structure and properties of invariant measurable partitions. *Dokl. Akad. Nauk SSSR*, 141, 1038–1041.

[17] Shannon, C. (1948). A mathematical theory of communication. *Bell Syst. Tech. Journal*, 27, 379–423. DOI: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[18] Shulman, A. (1988). Maximal ergodic theorems on groups. *Dept. Lit. NIINTI, No. 2184*.

[19] Sinai, Ya.G. (1959). On the notion of entropy of a dynamical system. *Doklady of Russian Academy of Sciences*, 124, 768–771. DOI: https://doi.org/10.1007/978-0-387-87870-6_1.

[20] Tempelman, A. (1992). Ergodic theorems for group actions, informational and thermodynamical aspects. *Springer Dordrecht*. DOI: https://doi.org/10.1007/978-94-017-1460-0.

[21] Von Neumann, J. (1932). Proof of the Quasi-ergodic Hypothesis. *Proc. Natl. Acad. Sci*, 18, 70–82. DOI: https://doi.org/10.1073/pnas.18.1.70.

[22] Walters, P. (1982). An introduction to ergodic theory. *Springer-Verlag*. DOI: https://doi.org/10.1007/springerreference_60354.

[23] Wiener, N. (1939). The ergodic theorem. *Duke Math. J*, 5, 1–18. DOI: https://doi.org/10.1215/S0012-7094-39-00501-6.

[24] Yosida, K. (1938). Mean ergodic theorem in Banach spaces. *Proc. Imp. Acad*, 14, 292–294. DOI: https://doi.org/10.3792/pia/1195579607.

[25] Yosida, K., & Kakutani, S. (1939). Birkhoff‘s ergodic theorem and the maximal ergodic theorem. *Proc. Imp. Acad*, 15, 165–168. DOI: https://doi.org/10.3792/pia/1195579375.

Measure Algebras and Applications

Topological groups with three relative commutativity degrees

Seyyed Ali Moosavi[1]

1. Department of Mathematics, University of Qom, Qom, Iran. Email: s.a.mousavi@qom.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 20 April 2024
Received in revised form:
22 June 2024
Accepted: 29 June 2024
Published Online:
20 August 2024

Keywords:
Commutativity degree,
Relative commutativity degree,
Topological group,
Compact group,
Closed subgroup

2020 Mathematics Subject Classification:
20P05, 20D60, 28A60

ABSTRACT

Suppose that G is a compact Hausdorff topological group and H is a closed subgroup of G. The relative commutativity degree of H in G, denoted by $\Pr(H, G)$, represents the probability that an element of H commutes with an element of G. Let $\mathcal{D}(G)$ be the set of all relative commutativity degrees of subgroups of G. In this paper, we will study the structure of topological groups that have exactly three relative commutativity degrees for their subgroups. In particular, we will show that for such groups, the centralizer of every non-central element is a maximal abelian subgroup. We will also provide examples of groups that have three relative commutativity degrees.

Cite this article: Moosavi, S.A. (2024). Topological groups with three relative commutativity degrees. *Measure Algebras and Applications*, 1(2), 142–153. http://doi.org/10.22091/maa.2024.11077.1022

Publisher: University of Qom
DOI: 10.22091/maa.2024.11077.1022

Extended Abstract

Introduction

Suppose that G is a finite group and we define

$$C = \{(x, y) \in G \times G \mid xy = yx\}. \tag{1.1}$$

The commutativity degree of the finite group G, denoted by $\Pr(G)$, is defined as

$$\Pr(G) = \frac{|C|}{|G|^2}.$$

The commutativity degree represents the probability that two randomly selected elements of G commute. Suppose that H is a subgroup of G. The concept of relative commutativity degree of the subgroup, as a generalization of commutativity degree, was defined in [3] as

$$\Pr(H, G) = \frac{|\{(x, y) \in H \times G \mid xy = yx\}|}{|H||G|}.$$

These concepts have been the basis for extensive research on finite groups, for example in [2, 4, 6, 8]. As the above definitions show, the cardinalities of the sets play a crucial role in these definitions, therefore these definitions are not directly applicable to infinite groups.

To address this issue, one can employ the notion of measure in the definitions. For the first time, Gustafson in [6] defined the notion of commutativity degree in the more general way for a compact topological group, and established several properties similar to the finite case. In [5, 9], similar approaches have been used to study the concept of the relative commutativity degree.

Suppose that G is a compact Hausdorff topological group, and μ is the unique probability Haar measure on G (note that μ is actually the left Haar measure with the normalization condition $\mu(G) = 1$, and for any x in G, we have $\mu(xE) = \mu(E)$). On the product space $G \times G$, we consider the product measure $\mu \times \mu$. For each subgroup H of non-zero measure and every Borel subset D of G, we set

$$\mu_H(D) := \frac{\mu(H \cap D)}{\mu(H)}.$$

It can be easily observed that μ_H is the normalized Haar measure on H and μ_G will be the same as the measure μ. In [7], the relative commutativity degree of the subgroup H, denoted by $\Pr(H, G)$, is defined as follows:

$$\Pr(H, G) := \mu_H \times \mu(C) = \int_{G \times G} \chi_C(x, y)\, d\mu_H(x)\, d\mu(y)$$

where C is the set defined in equation (1.1) and χ_C is the characteristic function on C. The relative commutativity degree of the subgroup can be defined in a more general way when $H \leq K \leq G$ as:

$$\Pr(H, K) := \mu_H \times \mu_K(C) = \int_{G \times G} \chi_C(x, y)\, d\mu_H(x)\, d\mu_K(y).$$

In particular, $\Pr(H, H)$ is the same as $\Pr(H)$. We define

$$\mathcal{D}(G) = \{\Pr(H, G) \quad | \quad H \leq G\},$$

which means that $\mathcal{D}(G)$ is the set of all relative commutativity degrees of the subgroups of G. For finite groups, the study of groups whose set $\mathcal{D}(G)$ has a specific number of elements has been of great interest to many researchers. One can refer to [1, 3] for example.

In this paper, we will study the structure of compact topological groups whose set $\mathcal{D}(G)$ has exactly three elements. First, we will show that there is no group whose set $\mathcal{D}(G)$ is a set of two elements, and then we will examine the groups with three relative commutativity degrees. Also, the set $\mathcal{D}(G)$ will be computed for a class of groups with this property. We will observe that many properties will be similar to the results obtained in the finite case.

Conclusion

In this paper, the following results have been obtained:

***Lemma* 0.1.** *Suppose that $H \leq K \leq G$, then for every x in G we have*

$$\frac{\mu(C_K(x))}{\mu(K)} \leq \frac{\mu(C_H(x))}{\mu(H)}.$$

***Lemma* 0.2.** *Suppose that $H \leq K \leq G$, then we have $\Pr(H,G) \leq \Pr(K,G)$ and the equality holds if and only if for every x in G we have $K = HC_K(x)$.*

***Lemma* 0.3.** *Suppose that G is a non-abelian group and $x \in G \setminus Z(G)$. Then*

$$\Pr(\langle x \rangle, G) \notin \{1, \Pr(G)\}.$$

***Corollary* 0.4.** *Suppose that G is a non-abelian group, then $|\mathcal{D}(G)| \neq 2$.*

***Lemma* 0.5.** *Suppose that G is a non-abelian group and $\mathcal{D}(G) = \{1, d, \Pr(G)\}$. If H is a subgroup of G such that $\Pr(H,G) = d$, then H is abelian.*

***Theorem* 0.6.** *Suppose that G is a group such that $|\mathcal{D}(G)| = 3$. Then for every $x \in G \setminus Z(G)$, the subgroup $C_G(x)$ is a maximal abelian subgroup of G.*

***Theorem* 0.7.** *Suppose that G is a group such that $|\mathcal{D}(G)| = 3$ and $\mathcal{D}(G) = \{1, d, \Pr(G)\}$. If H is a subgroup of G such that $\Pr(H,G) = d$, $x \in H \setminus Z(G)$ and $M = C_G(x)$, then*

$$\mathcal{D}(G) = \left\{1, \frac{\mu(Z)}{\mu(M)} + \mu(M \setminus Z), \Pr(G)\right\},$$

where $Z = M \cap Z(G)$.

***Example* 0.8.** *Let*

$$G_1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Then G_1 with the usual multiplication of complex numbers and the usual topology of complex numbers is a compact topological group. Let p be an odd prime number and consider $G = G_1 \times D_{2p}$, where D_{2p} is the dihedral group of order $2p$ given by

$$D_{2p} = \langle a, b | a^p = b^2 = id, bab = a^{-1} \rangle = \{id, a, \cdots, a^{p-1}, b, ab, \cdots, a^{p-1}b\}.$$

By computing commutativity degrees of subgroups of G we have

$$\mathcal{D}(G) = \left\{1, \frac{p+1}{2p}, \frac{p+3}{4p}\right\}.$$

So G is a group whose $\mathcal{D}(G)$ has exactly three elements.

***Remark* 0.9.** *By comparing the results obtained in this article and [1], it is observed that all these theorems also hold in the finite case. Since every finite group with the discrete topology is a compact topological group, one can consider the proof of these theorems in the finite case as a special case of this article. However, since in the finite case, the finiteness of the order of the group is an effective tool, one can obtain more results regarding the structure of these groups, as can be seen in [1].*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۵۳-۱۴۲

گروه‌های توپولوژیک با سه درجه جابه‌جایی نسبی

سید علی موسوی [۱]

۱. گروه ریاضی، دانشکده علوم پایه، دانشگاه قم، قم، ایران. رایانامه: s. a. mousavi@qom. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۲/۱
تاریخ بازنگری: ۱۴۰۳/۴/۲
تاریخ پذیرش: ۱۴۰۳/۴/۹
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
درجهٔ جابه‌جایی،
درجهٔ جابه‌جایی نسبی،
گروه توپولوژیک،
گروه فشرده،
زیرگروه بسته

رده‌بندی ریاضی:
20P05, 20D60, 28A60

چکیده

فرض کنید G یک گروه توپولوژیک فشردهٔ هاسدورف و H زیرگروهی بسته از G باشد. درجهٔ جابه‌جایی نسبی H در G که با نماد $\Pr(H,G)$ نمایش داده می‌شود، احتمال جابه‌جایی یک عضو H با یک عضو G را نشان می‌دهد. فرض کنید $\mathcal{D}(G)$ مجموعهٔ تمام درجات نسبی زیرگروه‌های G باشد. در این مقاله به بررسی گروه‌هایی خواهیم پرداخت که دارای دقیقاً سه درجهٔ جابه‌جایی نسبی برای زیرگروه‌های خود هستند. به‌ویژه نشان خواهیم داد که برای چنین گروه‌هایی مرکزساز هر عضو غیرمرکزی یک زیرگروه ماکسیمال آبلی خواهد بود. همچنین مثال‌هایی از گروه‌هایی که دارای سه درجهٔ جابه‌جایی نسبی هستند را معرفی خواهیم کرد.

استناد: موسوی، سید علی. (۱۴۰۳). گروه‌های توپولوژیک با سه درجه جابه‌جایی نسبی. جبرهای اندازه و کاربردها، ۱(۲)، ۱۵۳-۱۴۲.
http://doi.org/10.22091/maa.2024.11077.1022

ناشر: دانشگاه قم.

۱ مقدمه

فرض کنید G یک گروه متناهی باشد و قرار می‌دهیم

$$C = \{(x, y) \in G \times G \mid xy = yx\}. \tag{۱.۱}$$

درجهٔ جابه‌جایی گروه متناهی G که با نماد $\Pr(G)$ نمایش داده می‌شود به‌صورت زیر تعریف می‌شود

$$\Pr(G) = \frac{|C|}{|G|^2}.$$

درجهٔ جابه‌جایی احتمال جابه‌جا شدن دو عضو از G که به‌صورت تصادفی انتخاب شده باشند را نشان می‌دهد. فرض کنید که H زیرگروهی از G باشد. مفهوم درجهٔ جابه‌جایی نسبی زیرگروه به‌عنوان تعمیمی از درجهٔ جابه‌جایی در [۳] به‌صورت زیر تعریف شد

$$\Pr(H, G) = \frac{|\{(x, y) \in H \times G \mid xy = yx\}|}{|H||G|}.$$

مفاهیم فوق زمینهٔ تحقیقات زیادی در گروه‌های متناهی بوده که برای نمونه می‌توان به [۲، ۴، ۶، ۸] مراجعه کرد. همان‌طور که در تعاریف فوق مشخص است تعداد اعضای مجموعه‌ها نقش اساسی در تعاریف فوق دارند که باعث می‌شوند تعاریف فوق در حالت گروه‌های نامتناهی قابل بیان نباشند. جهت رفع این مشکل می‌توان مفهوم اندازه را در تعاریف فوق به کار گرفت.

اولین بار گوستافسون در [۶] درجهٔ جابه‌جایی را در حالت کلی‌تر برای یک گروه توپولوژیک فشرده تعریف کرد و با استفاده از آن چند خاصیت مشابه حالت متناهی را برای این گروه‌ها ثابت کرد. در [۵، ۹] با رویکرد مشابهی مفاهیم درجهٔ جابه‌جایی نسبی مورد بررسی قرار گرفته است.

فرض کنید G یک گروه توپولوژیک فشرده و هاسدورف باشد و فرض کنید μ اندازهٔ احتمال منحصربه‌فرد G باشد (توجه کنید که μ در حقیقت اندازهٔ هار چپ است که شرط نرمال‌سازی $\mu(G) = ۱$ روی آن لحاظ شده است. همچنین به‌ازای هر x از گروه G داریم $\mu(xE) = \mu(E)$). روی فضای $G \times G$ اندازهٔ حاصل‌ضرب $\mu \times \mu$ را در نظر می‌گیریم. به‌ازای هر زیرگروه H از اندازهٔ غیرصفر و هر زیرمجموعهٔ بورل D از G قرار می‌دهیم

$$\mu_H(D) := \frac{\mu(H \cap D)}{\mu(H)},$$

در این صورت به‌راحتی می‌توان مشاهده کرد که μ_H اندازهٔ هار نرمال‌شده روی H است و μ_G همان اندازهٔ μ خواهد بود. در [۷] درجهٔ جابه‌جایی نسبی زیرگروه H که با نماد $\Pr(H, G)$ نمایش داده می‌شود، به‌صورت زیر تعریف شده است

$$\Pr(H, G) := \mu_H \times \mu(C) = \int_{G \times G} \chi_C(x, y) d\mu_H(x) d\mu(y), \tag{۲.۱}$$

که C همان مجموعهٔ تعریف‌شده در رابطه (۱.۱) و χ_C تابع مشخصه روی C است. درجهٔ جابه‌جایی نسبی زیرگروه را می‌توان در حالت کلی‌تر برای وقتی که $H \leq K \leq G$، به‌صورت زیر تعریف کرد

$$\Pr(H, K) := \mu_H \times \mu_K(C) = \int_{G \times G} \chi_C(x, y) d\mu_H(x) d\mu_K(y), \tag{۳.۱}$$

به‌ویژه $\Pr(H, H)$ همان $\Pr(H)$ خواهد بود. قرار می‌دهیم

$$\mathcal{D}(G) = \{\Pr(H, G) \quad | \quad H \leq G\},$$

یعنی $\mathcal{D}(G)$ مجموعهٔ تمام درجات نسبی زیرگروه‌های G است. در گروه‌های متناهی بررسی گروه‌هایی که مجموعهٔ $\mathcal{D}(G)$ آن‌ها دارای تعداد مشخصی عضو است مورد توجه محققان زیادی بوده است. برای نمونه می‌توان به [۱، ۳] مراجعه کرد.

در این مقاله به بررسی ساختار گروه‌های توپولوژیک فشرده‌ای خواهیم پرداخت که مجموعهٔ $\mathcal{D}(G)$ آن‌ها دقیقاً دارای سه عضو است. در ابتدا نشان خواهیم داد که هیچ گروهی وجود ندارد که مجموعهٔ $\mathcal{D}(G)$ آن یک مجموعهٔ دو عضوی باشد و سپس گروه‌های با سه درجهٔ جابه‌جایی نسبی را بررسی خواهیم کرد. همچنین رده‌ای از گروه‌ها که چنین ویژگی دارند را معرفی خواهیم کرد. مشاهده خواهیم کرد که بسیاری از ویژگی‌ها با نتایج به‌دست‌آمده در حالت متناهی مشابه خواهد بود.

۲ احکام و قضایای مقدماتی

در این بخش به بیان احکام و قضایای مقدماتی خواهیم پرداخت که در مقاله مورد استفاده قرار خواهند گرفت. در سراسر مقاله همواره منظور از گروه G، یک گروه توپولوژیک هاسدورف با اندازهٔ احتمال μ است و زیرگروه H همواره زیرگروهی بسته از اندازهٔ غیرصفر در نظر گرفته می‌شود و μ_H همان اندازهٔ تعریف‌شده در بخش مقدمه است. مرکزساز عضو x در G را با نماد $C_G(x)$ نشان داده و برای مرکز گروه از نماد $Z(G)$ استفاده می‌کنیم. همچنین $|G : H|$ نشان‌دهندهٔ شاخص زیرگروه H در گروه G خواهد بود. در ابتدا چند لم مربوط به گروه‌ها را بیان می‌کنیم.

قضیه ۱.۲ (حکم ۵.۳.۱ از [۱۰]). فرض کنید G یک گروه باشد و H و K زیرگروه‌هایی از G باشند به‌طوری‌که $K \leq H \leq G$. در این صورت داریم

$$|G : K| = |G : H||H : K|.$$

قضیه ۲.۲ (حکم ۱۱.۳.۱ از [۱۰]). فرض کنید G یک گروه باشد و H و K زیرگروه‌هایی از G باشند. در این صورت داریم

$$|G : H \cap K| \leq |G : H||G : K|,$$

و تساوی اتفاق می‌افتد اگر و تنها اگر $G = HK$.

لم ۳.۲ (لم ۲.۲ از [۹]). فرض کنید G یک گروه و H زیرگروهی از G باشد. در این صورت

$$\mu(H) = \begin{cases} \frac{1}{|G:H|} & \text{اگر } |G : H| < \infty \\ 0 & \text{اگر } |G : H| = \infty \end{cases}.$$

لم ۴.۲. فرض کنید H زیرگروهی از G باشد. در این صورت داریم

$$\Pr(H, G) = \frac{1}{\mu(H)} \int_G \mu(C_H(y)) d\mu(y) = \frac{1}{\mu(H)} \int_H \mu(C_G(x)) d\mu(x). \quad (۱.۲)$$

اثبات. به لم ۳.۳ از [۷] مراجعه شود. □

قضیه ۵.۲ (قضیه ۲.۴ از [۷]). فرض کنید G یک گروه غیرآبلی و H زیرگروهی از آن باشد. اگر $H \subseteq Z(G)$، آنگاه $\Pr(H, G) = 1$.

۳ نتایج اصلی

در این بخش به بررسی گروه‌هایی خواهیم پرداخت که دارای دقیقاً سه درجهٔ جابه‌جایی نسبی هستند. در ابتدا به اثبات یک لم خواهیم پرداخت که در نتایج بعدی مورد استفاده قرار خواهد گرفت.

لم ۱.۳. فرض کنید $H \leq K \leq G$، در این صورت به‌ازای هر x از G داریم

$$\frac{\mu(C_K(x))}{\mu(K)} \leq \frac{\mu(C_H(x))}{\mu(H)}.$$

اثبات. رابطهٔ فوق معادل با این است که

$$\mu(H)\mu(C_K(x)) \leq \mu(K)\mu(C_H(x)).$$

اگر $|G : C_K(x)| = \infty$ آنگاه $\mu(C_K(x)) = 0$ و در این حالت حکم برقرار است. پس فرض کنید $|G : C_K(x)| \neq \infty$. چون $C_H(x) = H \cap C_K(x)$، با توجه به قضایای ۱.۲ و ۲.۲ می‌توان نوشت

$$|K : H||H : C_H(x)| = |K : C_H(x)| \leq |K : H||K : C_K(x)|, \quad (۱.۳)$$

و در این رابطه تساوی برقرار است اگر و تنها اگر به‌ازای هر x داشته باشیم $K = HC_K(x)$. با ضرب طرفین رابطهٔ فوق در $|G : K|$ خواهیم داشت

$$|G : K||K : H||H : C_H(x)| \leq |G : K||K : H||K : C_K(x)|,$$

که نتیجه می‌دهد

$$|G : H||H : C_H(x)| \leq |K : H||G : C_K(x)|.$$

این رابطه معادل با این است که

$$|G : C_H(x)| \leq |K : H||G : C_K(x)|.$$

حال اگر طرفین رابطهٔ بالا را دوباره در $|G : K|$ ضرب کنیم داریم

$$|G : K||G : C_H(x)| \leq |G : H||G : C_K(x)|,$$

و با معکوس کردن دوطرف نتیجه می‌شود

$$\frac{۱}{|G : H|}\frac{۱}{|G : C_K(x)|} \leq \frac{۱}{|G : K|}\frac{۱}{|G : C_H(x)|},$$

که با توجه به لم ۳.۲ همان نتیجهٔ مورد نظر است. همچنین با توجه به اینکه نامساوی فوق معادل با رابطه (۱.۳) است لذا تساوی برقرار است اگر و تنها اگر به‌ازای هر x از G داشته باشیم $K = HC_K(x)$. □

لم ۲.۳. فرض کنید $H \leq K \leq G$، در این صورت داریم $\Pr(H, G) \leq \Pr(K, G)$ و تساوی برقرار است اگر و تنها اگر به‌ازای هر x از G داشته باشیم $K = HC_K(x)$.

اثبات. با توجه به لم ۱.۳ داریم

$$\frac{\mu(C_K(x))}{\mu(K)} \leq \frac{\mu(C_H(x))}{\mu(H)},$$

و تساوی برقرار است اگر و تنها اگر به‌ازای هر x از G داشته باشیم $K = HC_K(x)$. از ترکیب رابطهٔ فوق و لم ۴.۲ خواهیم داشت

$$\begin{aligned}\Pr(K, G) &= \frac{۱}{\mu(H)}\int_G \mu(C_K(y))d\mu(y)\\ &= \int_G \frac{\mu(C_K(y))}{\mu(K)}d\mu(y)\\ &\leq \int_G \frac{\mu(C_H(y))}{\mu(H)}d\mu(y) = \Pr(H, G),\end{aligned}$$

و نامساوی مورد نظر ثابت شد. همچنین تساوی برقرار است اگر و تنها اگر به‌ازای هر x از G داشته باشیم $K = HC_K(x)$. □

لم ۳.۳. فرض کنید G یک گروه غیرآبلی باشد و $x \in G \setminus Z(G)$. در این صورت

$$\Pr(\langle x\rangle, G) \notin \{۱, \Pr(G)\}.$$

اثبات. ابتدا توجه می‌کنیم که چون x یک عضو غیرمرکزی است لذا $\langle x\rangle$ زیرمجموعهٔ مرکز گروه نیست و درنتیجه $\Pr(\langle x\rangle, G) \neq ۱$. حال فرض کنید $\Pr(\langle x\rangle, G) = \Pr(G)$، در این صورت با توجه به لم ۲.۳ به‌ازای هر عضو y از G داریم $G = \langle x\rangle C_G(y)$. به‌ویژه اگر قرار دهیم $y = x$ خواهیم داشت $G = \langle x\rangle C_G(x) = C_G(x)$ که نتیجه می‌دهد $x \in Z(G)$ که متناقض با فرض است. بنابراین $\Pr(\langle x\rangle, G) \neq \Pr(G)$ و حکم ثابت شد. □

از لم فوق نتیجهٔ زیر را خواهیم داشت که نشان می‌دهد هیچ گروه غیرآبلی دارای دو درجهٔ جابه‌جایی نسبی نیست.

نتیجه ۴.۳. فرض کنید G یک گروه غیرآبلی باشد، در این صورت $|\mathcal{D}(G)| \neq ۲$.

لم ۵.۳. فرض کنید G گروهی غیرآبلی باشد و $\mathcal{D}(G) = \{1, d, \Pr(G)\}$. اگر H زیرگروهی از G باشد به‌طوری‌که $\Pr(H, G) = d$، در این صورت H آبلی است.

اثبات. فرض کنید H غیرآبلی باشد و $h \in H \setminus Z(H)$، در این صورت با توجه به لم ۳.۳ داریم $\Pr(\langle h\rangle, G) \neq \Pr(G)$ و چون h مرکزی هم نیست پس $\Pr(\langle h\rangle, G) \neq 1$. بنابراین $\Pr(\langle h\rangle, G) = \Pr(H, G)$. حال لم ۲.۳ نتیجه می‌دهد که به‌ازای هر عضو x از G داریم $H = \langle h\rangle C_H(x)$. به‌ویژه اگر x را با خود h جایگزین کنیم خواهیم داشت $H = C_H(h)$ که نشان می‌دهد $h \in Z(H)$ که متناقض با فرض است. □

قضیه ۶.۳. فرض کنید G یک گروه باشد به‌طوری‌که $|\mathcal{D}(G)| = 3$. در این صورت به‌ازای هر $x \in G \setminus Z(G)$، زیرگروه $C_G(x)$ یک زیرگروه ماکسیمال آبلی از G است.

اثبات. فرض کنید $\mathcal{D}(G) = \{1, d, \Pr(G)\}$ و $x \in G \setminus Z(G)$ اگر $C_G(x)$ یک گروه غیرآبلی باشد آنگاه با توجه به لم ۳.۳ داریم $\Pr(C_G(x), G) \neq d$ و چون $C_G(x)$ مرکزی نیست لذا $\Pr(C_G(x), G) \neq 1$، بنابراین $\Pr(C_G(x), G) = \Pr(G)$. حال لم ۲.۳ نتیجه می‌دهد که به‌ازای هر عضو g از G داریم $G = C_G(x)C_G(g)$. به‌ویژه با قرار دادن $g = x$ خواهیم داشت $G = C_G(x)C_G(x) = C_G(x)$ که نشان می‌دهد $x \in Z(G)$ که متناقض با فرض است. لذا $C_G(x)$ آبلی است. اگر $C_G(x)$ ماکسیمال نباشد آنگاه زیرگروهی مانند M موجود است که $C_G(x) < M < G$. اگر M غیرآبلی باشد آنگاه مشابه برهان قسمت اول، نتیجه می‌شود که $G = MC_G(x)$ که به این معنی است که $G = M$ که تناقض است. پس M آبلی است و درنتیجه $M = C_G(x)$ که بازهم تناقض است. بنابراین $C_G(x)$ ماکسیمال است. □

قضیه ۷.۳. فرض کنید G گروهی باشد که $|\mathcal{D}(G)| = 3$ و $\mathcal{D}(G) = \{1, d, \Pr(G)\}$. اگر H زیرگروهی از G باشد به‌طوری‌که $\Pr(H, G) = d$، $x \in H \setminus Z(G)$ و $M = C_G(x)$، آنگاه

$$\mathcal{D}(G) = \left\{1, \frac{\mu(Z)}{\mu(M)} + \mu(M \setminus Z), \Pr(G)\right\},$$

که در آن $Z = M \cap Z(G)$.

اثبات. با توجه به قضیه ۶.۳، M یک زیرگروه آبلی است. قرار دهید $Z = M \cap Z(G)$. به‌ازای هر $y \in Z$ داریم $C_G(y) = G$ و درنتیجه $\mu(C_G(y)) = 1$. اگر $y \in M \setminus Z$ چون M آبلی ماکسیمال است لذا $C_G(y) = M$. لذا با توجه به تعریف داریم

$$\begin{aligned}
\Pr(M, G) &= \frac{1}{\mu(M)} \int_M \mu(C_G(y)) d\mu(y) \\
&= \frac{1}{\mu(M)} \left(\int_Z \mu(C_G(y)) d\mu(y) + \int_{M\setminus Z} \mu(C_G(y)) d\mu(y) \right) \\
&= \frac{1}{\mu(M)} \left(\int_Z d\mu(y) + \int_{M\setminus Z} \mu(M) d\mu(y) \right) \\
&= \frac{\mu(Z)}{\mu(M)} + \mu(M \setminus Z).
\end{aligned}$$

□

مثال ۸.۳. فرض کنید $G_1 = \{z \in \mathbb{C} \mid |z| = 1\}$، در این صورت G_1 با ضرب معمولی اعداد مختلط و توپولوژی معمولی اعداد مختلط، یک گروه توپولوژیک فشرده است. فرض کنید p یک عدد اول فرد باشد و قرار می‌دهیم $G = G_1 \times D_{2p}$، که در آن D_{2p} گروه دووجهی از مرتبهٔ $2p$ است و اعضای آن به‌صورت زیر است

$$D_{2p} = \langle a, b | a^p = b^2 = id, bab = a^{-1}\rangle = \{id, a, \cdots, a^{p-1}, b, ab, \cdots, a^{p-1}b\}.$$

در این مثال نشان خواهیم داد که

$$\mathcal{D}(G) = \left\{1, \frac{p+1}{2p}, \frac{p+3}{4p}\right\}.$$

برای بررسی این موضوع توجه می‌کنیم که زیرگروه‌های غیرمرکزی G به‌صورت زیر هستند

$$H_۱ = G_۱ \times \langle a \rangle, H_۲ = G_۱ \times \langle a^i b \rangle, \quad i = ۰, \cdots, p-۱.$$

ابتدا برای زیرگروه $H = H_۱$ درجهٔ جابه‌جایی نسبی را محاسبه می‌کنیم. فرض کنید

$$K_۱ = \{(g, id) \mid g \in G_۱\}, \quad K_۲ = \{(g, y) \mid g \in G_۱, y \in \{a, \cdots, a^{p-۱}\}\}.$$

در این صورت واضح است که هر عضو (g, id) از $K_۱$ یک عضو مرکزی است و درنتیجه $C_G(g, id) = G$. همچنین برای هر عضو (g, a^i) از $K_۲$ داریم $C_G(g, a^i) = H$. بنابراین

$$\begin{aligned}
\Pr(H, G) &= \frac{۱}{\mu(H)} \int_H \mu(C_G(y)) d\mu(y) \\
&= \frac{۱}{\mu(H)} \left(\int_{K_۱} \mu(C_G(y)) d\mu(y) + \int_{K_۲} \mu(C_G(y)) d\mu(y) \right) \\
&= \frac{۱}{\mu(H)} \left(\int_{K_۱} d\mu(y) + \int_{K_۲} \mu(H) d\mu(y)) \right) \\
&= \frac{۱}{\mu(H)} \left(\mu(K_۱) + \mu(K_۲)\mu(H) \right).
\end{aligned}$$

اما با توجه به تعاریف مجموعه‌های $K_۱$ و $K_۲$ و لم ۳.۲ واضح است که $\mu(K_۱) = \frac{۱}{۲p}$، $\mu(K_۲) = \frac{p-۱}{۲p}$ و $\mu(H) = \frac{۱}{۲}$. بنابراین داریم

$$\Pr(H, G) = ۲(\frac{۱}{۲p} + \frac{p-۱}{۲p} \cdot \frac{۱}{۲}) = \frac{۱}{p} + \frac{p-۱}{۲p} = \frac{p+۱}{۲p}.$$

حال فرض کنید $۱ \leq i \leq p-۱$ و $H = G_۱ \times \langle a^i b \rangle$ و قرار دهید

$$K_۱ = \{(g, id) \mid g \in G_۱\}, \quad K_۲ = \{(g, a^i b) \mid g \in G_۱\}.$$

در این صورت بازهم با توجه به لم ۳.۲ واضح است که $\mu(K_۱) = \mu(K_۲) = \frac{۱}{۲p}$ و $\mu(H) = \frac{۱}{p}$. همچنین مانند قسمت قبل همهٔ اعضای $K_۱$ مرکزی هستند و مرکزساز آن‌ها برابر کل گروه است و برای اعضای $K_۲$ داریم $C_G(g, a^i b) = H$. بنابراین داریم

$$\begin{aligned}
\Pr(H, G) &= \frac{۱}{\mu(H)} \int_H \mu(C_G(y)) d\mu(y) \\
&= \frac{۱}{\mu(H)} \left(\int_{K_۱} \mu(C_G(y)) d\mu(y) + \int_{K_۲} \mu(C_G(y)) d\mu(y) \right) \\
&= \frac{۱}{\mu(H)} \left(\int_{K_۱} d\mu(y) + \int_{K_۲} \mu(H) d\mu(y)) \right) \\
&= \frac{۱}{\mu(H)} \left(\mu(K_۱) + \mu(K_۲)\mu(H) \right) \\
&= p \left(\frac{۱}{۲p} + \frac{۱}{۲p} \cdot \frac{۱}{p} \right) \\
&= \frac{۱}{۲} + \frac{۱}{۲p} = \frac{p+۱}{۲p}.
\end{aligned}$$

مشاهده می‌شود که برای هر زیرگروه به شکل $H = G_۱ \times \langle a^i b \rangle$ درجهٔ جابه‌جایی زیرگروه با حالت قبل یکسان بوده و برابر $\frac{p+۱}{۲p}$ است. لذا برای تمام زیرگروه‌های غیرمرکزی G فقط یک درجهٔ جابه‌جایی نسبی داریم. همچنین با توجه به قضیه ۵.۲ واضح است که برای زیرگروه‌های مرکزی داریم $\Pr(H, G) = ۱$. حال به محاسبهٔ درجهٔ جابه‌جایی گروه G می‌پردازیم. قرار می‌دهیم

$$K_۱ = G_۱ \times id, K_۲ = G_۱ \times \langle a \rangle,$$

و

$$H_i = G_1 \times \langle a^i b \rangle, \quad i = 1, \cdots, p-1.$$

در این صورت واضح است که

$$\mu(K_1) = \frac{1}{2p}, \mu(K_2) = \frac{1}{2}, \mu(K_2 \setminus K_1) = \frac{p-1}{2p}, \mu(H_i) = \frac{1}{p}, \mu(H_i \setminus K_1) = \frac{1}{2p},$$

بنابراین داریم (توجه کنید که $\mu(G) = 1$)

$$\begin{aligned}
\Pr(G,G) &= \frac{1}{\mu(G)} \int_G \mu(C_G(y)) d\mu(y) = \int_G \mu(C_G(y)) d\mu(y) \\
&= \left(\int_{K_1} \mu(C_G(y)) d\mu(y) + \int_{K_2 \setminus K_1} \mu(C_G(y)) d\mu(y) + \sum_{i=0}^{p-1} \int_{H_i \setminus K_1} \mu(C_G(y)) d\mu(y) \right) \\
&= \left(\int_{K_1} d\mu(y) + \int_{K_2 \setminus K_1} \mu(K_2) d\mu(y) + \sum_{i=0}^{p-1} \int_{H_i \setminus K_1} \mu(H_i) d\mu(y) \right) \\
&= \left(\mu(K_1) + \mu(K_2 \setminus K_1)\mu(K_2) + \sum_{i=0}^{p-1} \mu(H_i \setminus K_1)\mu(H_i) \right) \\
&= \left(\frac{1}{2p} + \frac{p-1}{2p}\frac{1}{2} + \sum_{i=0}^{p-1} \frac{1}{2p}\frac{1}{p} \right) \\
&= \left(\frac{1}{2p} + \frac{p-1}{4p} + \frac{1}{2p} \right) \\
&= \frac{p+3}{4p}.
\end{aligned}$$

پس

$$\mathcal{D}(G) = \left\{ 1, \frac{p+1}{2p}, \frac{p+3}{4p} \right\},$$

و لذا G یک گروه با سه درجهٔ جابه‌جایی نسبی است.

ملاحظه ۹.۳. با مقایسهٔ نتایج به‌دست‌آمده در این مقاله و [۱] مشاهده می‌شود که همهٔ این احکام در حالت متناهی هم برقرار هستند، در حقیقت چون هر گروه متناهی با توپولوژی گسسته یک گروه توپولوژیک فشرده است می‌توان برهان این احکام در حالت متناهی را به‌عنوان حالت خاصی از این مقاله در نظر گرفت. البته با توجه به اینکه در حالت متناهی، مرتبهٔ متناهی بودن گروه یک ابزار کارآمد است لذا همان‌طور که در [۱] دیده می‌شود می‌توان نتایج بیشتری در مورد ساختار این گروه‌ها به دست آورد.

References

[1] Barzgar, R., Erfanian, A., & Farrokhi DG, M. (2013). Finite groups with three relative commutativity degrees. *Bulletin of the Iranian Mathematical Society*, 39(2), 271–280.

[2] Erdos, P., & Turan, P. (1968). On some problems of a statistical group-theory. *Acta Math. Acad. Sci. Hung*, 19, 413–435. DOI: https://doi.org/10.1007/BF01894517.

[3] Erfanian, A., & Farrokhi DG, M. (2015). Finite groups with four relative commutativity degrees. *Algebra Colloquium*, 22(3), 449–458. DOI: https://doi.org/10.1142/S1005386715000401.

[4] Erfanian, A., Rezaei, R., & Lescot, P. (2007). On the relative commutativity degree of a subgroup of a finite group. *Communications in Algebra*, 35, 4183–4197. DOI: https://doi.org/10.1080/00927870701545044.

[5] Erfanian, A., & Russo, F. (2008). Probability of mutually commuting n-tuples in some classes of compact groups. *Bulletin of the Iranian Mathematical Society*, 34(2), 27–37.

[6] Gustafson, W.H. (1973). What is the probability that two group elements commute?. *Amer. Math. Monthly*, 80, 1031–1304. DOI: https://doi.org/10.1080/00029890.1973.11993437.

[7] Moosavi, S.A. (2023). Relative commutativity degree for some topological groups. *Measure Algebras and Applications*, 1(1), 1–12. DOI: http://doi.org/10.22091/MAA.2023.9447.1004.

[8] Nath, R.K., & Yadav, M.K. (2015). Some results on relative commutativity degree. *Rendiconti del Circolo Matematico di Palermo (1952-)*, 64, 229–239. DOI: https://doi.org/10.1007/s12215-015-0194-x.

[9] Rezaei, R., & Russo, F.G. (2011). Bounds for the relative n-th nilpotency degree in compact groups. *Asian-European Journal of Mathematics*, 4, 495–506. DOI: https://doi.org/10.1142/S1793557111000411.

[10] Robinson, D. (1996). A Course in the Theory of Groups. *Germany: Springer New York*. DOI: https://doi.org/10.1007/978-1-4419-8594-1.

Measure Algebras and Applications

Tensor products for α-duals of g-frames and fusion frames in Hilbert C^*-modules

Fatemeh Zamani Mirarkoulaei[1]

1. Department of Mathematics, Kharazmi University, Tehran, Iran. Email: std_zamani243@khu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 21 April 2024
Received in revised form:
23 June 2024
Accepted: 01 July 2024
Published Online:
20 August 2024

Keywords:
Hilbert C^*-module,
G-frame,
Fusion frame,
α-dual,
Tensor product

2020 Mathematics Subject Classification:
42C15

ABSTRACT

In this paper, we show that the tensor product of a finite number of α-duals for standard g-frames (resp. standard fusion frames) is an α-dual for the tensor product of the standard g-frames (resp. the standard fusion frames) in the tensor product of Hilbert C^*-modules.

Cite this article: Zamani Mirarkoulaei, F. (2024). Tensor products for α-duals of g-frames and fusion frames in Hilbert C^*-modules. *Measure Algebras and Applications*, 1(2), 154–164. http://doi.org/10.22091/maa.2024.11097.1023

Publisher: University of Qom
DOI: 10.22091/maa.2024.11097.1023

Extended Abstract

Introduction

Let $\mathcal{H}$ be a Hilbert space and let I be a finite or countable index set. A family $\mathcal{F} = \{f_i\}_{i\in I} \subseteq \mathcal{H}$ is a frame for $\mathcal{H}$, if there exist $0 < A_{\mathcal{F}} \leq B_{\mathcal{F}} < \infty$, such that

$$A_{\mathcal{F}}\|f\|^2 \leq \sum_{i\in I} |\langle f, f_i\rangle|^2 \leq B_{\mathcal{F}}\|f\|^2,$$

for each $f \in \mathcal{H}$. The sequence $\mathcal{F}$ is called a *Bessel sequence* if only the second inequality is required (see [4]).

For each $i \in I$, let $\mathcal{H}_i$ be a Hilbert space and let $L(\mathcal{H}, \mathcal{H}_i)$ be the set of all bounded operators from $\mathcal{H}$ into $\mathcal{H}_i$. We call $\Lambda = \{\Lambda_i \in L(\mathcal{H}, \mathcal{H}_i) : i \in I\}$ a *g-frame* for $\mathcal{H}$ with respect to $\{\mathcal{H}_i : i \in I\}$ if there exist two positive constants A and B such that

$$A\|f\|^2 \leq \sum_{i\in I} \|\Lambda_i f\|^2 \leq B\|f\|^2,$$

for each $f \in \mathcal{H}$. If only the second inequality is required, we call it a *g-Bessel sequence* with upper bound B (see [13]).

Another important generalization of frames is the fusion frame introduced in [2].

Let $\{W_i\}_{i\in I}$ be a family of closed subspaces of a Hilbert space $\mathcal{H}$, and $\{\omega_i\}_{i\in I}$ be a family of weights, i.e., $\omega_i > 0$ for each $i \in I$. Then $\mathcal{W} = \{(W_i, \omega_i)\}_{i\in I}$ is a *fusion frame*, if there are two positive numbers A and B such that for each $f \in \mathcal{H}$,

$$A\|f\|^2 \leq \sum_{i\in I} \omega_i^2\|\pi_{W_i}(f)\|^2 \leq B\|f\|^2,$$

where π_{W_i} is the orthogonal projection onto the subspace W_i. If only the right-hand inequality is required, then $\mathcal{W}$ is called a *Bessel fusion sequence*.

It is easy to see that if $\mathcal{W} = \{(W_i, \omega_i)\}_{i\in I}$ is a Bessel fusion sequence, then the operator $S_{\mathcal{W}}$ defined on $\mathcal{H}$ by $S_{\mathcal{W}}f = \sum_{i\in I} \omega_i^2\pi_{W_i}f$ is well-defined, bounded and positive. Also, if $\mathcal{W}$ is a fusion frame, then $S_{\mathcal{W}}$ is invertible.

Note that $\mathcal{W} = \{(W_i, \omega_i)\}_{i\in I}$ is a fusion frame if and only if $\Lambda_{\mathcal{W}} := \{\omega_i\pi_{W_i}\}_{i\in I}$ is a g-frame.

Tensor products of g-frames and fusion frames in Hilbert spaces were considered in [7] and α-duals of g-frames and fusion frames in Hilbert spaces were studied in [1, 12].

Hilbert C^*-modules are generalizations of Hilbert spaces by allowing the inner product to take values in a C^*-algebra rather than in the field of complex numbers.

Let $\mathfrak{A}$ be a unital C^*-algebra and suppose that E is a left $\mathfrak{A}$-module such that the linear structures of $\mathfrak{A}$ and E are compatible. Then E is called a pre-Hilbert $\mathfrak{A}$-module if E is equipped with an $\mathfrak{A}$-valued inner product $\langle\cdot,\cdot\rangle : E \times E \longrightarrow \mathfrak{A}$, such that

(i) $\langle\alpha x + \beta y, z\rangle = \alpha\langle x, z\rangle + \beta\langle y, z\rangle$, for each $\alpha, \beta \in \mathbb{C}$ and $x, y, z \in E$;

(ii) $\langle ax, y\rangle = a\langle x, y\rangle$, for each $a \in \mathfrak{A}$ and $x, y \in E$;

(iii) $\langle x, y\rangle = \langle y, x\rangle^*$, for each $x, y \in E$;

(iv) $\langle x, x\rangle \geq 0$, for each $x \in E$ and if $\langle x, x\rangle = 0$, then $x = 0$.

For each $x \in E$, we define $\|x\| = \|\langle x, x\rangle\|^{\frac{1}{2}}$. If E is complete with $\|.\|$, it is called a *Hilbert* $\mathfrak{A}$*-module* or a *Hilbert* C^**-module* over $\mathfrak{A}$.

Let E be a Hilbert $\mathfrak{A}$-module. A family $\mathcal{F} = \{f_i\}_{i\in I} \subseteq E$ is a *frame* for E, if there exist real constants $0 < A_{\mathcal{F}} \leq B_{\mathcal{F}} < \infty$, such that for each $x \in E$,

$$A_{\mathcal{F}}\langle x, x\rangle \leq \sum_{i\in I}\langle x, f_i\rangle\langle f_i, x\rangle \leq B_{\mathcal{F}}\langle x, x\rangle.$$

If the second inequality is required, $\mathcal{F}$ is a *Bessel sequence*. If the series $\sum_{i\in I}\langle x, f_i\rangle\langle f_i, x\rangle$ is convergent with respect to the norm, then $\mathcal{F}$ is called a *standard frame* (see [5]).

A closed submodule M of E is *orthogonally complemented* if $E = M \oplus M^{\perp}$. In this case $\pi_M \in \mathfrak{L}_{\mathfrak{A}}(E, M)$, where $\pi_M : E \longrightarrow M$ is the projection onto M.
Suppose that $\{\omega_i : i \in I\} \subseteq \mathfrak{A}$ is a family of weights, i.e., each ω_i is a positive, invertible element from the center of $\mathfrak{A}$, and $\{W_i : i \in I\}$ is a family of orthogonally complemented submodules of E. Then $\{(W_i, \omega_i)\}_{i\in I}$ is a *fusion frame* if there exist positive numbers A and B such that

$$A.\langle x, x\rangle \leq \sum_{i\in I}\omega_i^2\langle \pi_{W_i}(x), \pi_{W_i}(x)\rangle \leq B.\langle x, x\rangle,$$

for each $x \in E$. If we only require to have the upper bound, then $\{(W_i, \omega_i)\}_{i\in I}$ is called a *Bessel fusion sequence* with upper bound B.

Let $\{E_i\}_{i\in I}$ be a sequence of Hilbert $\mathfrak{A}$–modules. A sequence $\Lambda = \{\Lambda_i \in \mathfrak{L}(E, E_i) : i \in I\}$ is called a *g-frame* for E with respect to $\{E_i : i \in I\}$ if there exist real constants $A, B > 0$ such that for each $x \in E$,

$$A.\langle x, x\rangle \leq \sum_{i\in I}\langle \Lambda_i x, \Lambda_i x\rangle \leq B.\langle x, x\rangle.$$

If only the second-hand inequality is required, then Λ is called a *g-Bessel sequence*. Standard g-frames and fusion frames are defined similar to frames.

If $W = \{(W_i, \omega_i)\}_{i\in I}$ is a standard Bessel fusion sequence, then the operator $S_W : E \longrightarrow E$ which is defined by $S_W x = \sum_{i\in I}{\omega_i}^2\pi_{W_i}x$ is adjointable and called the *operator* of W. For a standard g-Bessel sequence Λ, the operator $S_\Lambda : E \longrightarrow E$ which is defined by $S_\Lambda(x) = \sum_{i\in I}\Lambda_i^*\Lambda_i(x)$ is adjointable and it is called the *operator* of Λ. If Λ is a standard (A, B) g-frame, then $A.Id_E \leq S_\Lambda \leq B.Id_E$. For more results about fusion frames and g-frames in Hilbert C^*-modules, see [6, 11].

In this paper, all C^*-algebras are unital and Hilbert C^*-modules are finitely or countably generated. All fusion frames, g-frames and Bessel sequences are standard.

Throughout this paper I and I_k, for each $1 \leq k \leq n$, are subsets of $\mathbb{N}$. $\mathfrak{A}_k$ is a unital C^*-algebra, E, E_k and $E_{i(k)}$ are finitely or countably generated Hilbert C^*-modules, for each $k \in \{1, \ldots, n\}$ and $i(k) \in I_k$.

Recall that if $\mathfrak{A}_k$ is a C^*-algebra, for each $1 \leq k \leq n$, then $\otimes_{k=1}^n\mathfrak{A}_k$ is a C^*-algebra with the spatial norm and for each $a_k \in \mathfrak{A}_k$, we have $\|a_1 \otimes \ldots \otimes a_n\| = \Pi_{k=1}^n\|a_k\|$. The multiplication and involution on simple tensors are defined by $(\otimes_{k=1}^n a_k)(\otimes_{k=1}^n b_k) = \otimes_{k=1}^n(a_k b_k)$ and $(\otimes_{k=1}^n a_k)^* = \otimes_{k=1}^n a_k^*$, respectively.

Now, if E_k is a Hilbert $\mathfrak{A}_k$-module, for each $1 \leq k \leq n$, then the (Hilbert C^*-module) tensor product $\otimes_{k=1}^n E_k = E_1 \otimes \ldots \otimes E_n$ is a Hilbert $(\otimes_{k=1}^n\mathfrak{A}_k)$-module. The module action and inner product for simple tensors are defined by

$$\begin{aligned}(\otimes_{k=1}^n a_k)(\otimes_{k=1}^n x_k) &= (a_1x_1) \otimes \ldots \otimes (a_nx_n)\\ &= \otimes_{k=1}^n(a_kx_k),\end{aligned}$$

and

$$\begin{aligned} & \langle \otimes_{k=1}^{n} x_k, \otimes_{k=1}^{n} y_k \rangle \\ = \; & \langle x_1, y_1 \rangle \otimes \ldots \otimes \langle x_n, y_n \rangle \\ = \; & \otimes_{k=1}^{n} \langle x_k, y_k \rangle, \end{aligned}$$

respectively, where $a_k \in \mathfrak{A}_k$ and $x_k, y_k \in E_k$. For more results, see [8].

In this paper $\Phi^{(k)} = \{\Lambda_{i(k)} \in \mathfrak{L}_{\mathfrak{A}_k}(E_k, E_{i(k)})\}_{i(k)\in I_k}$, $\Psi^{(k)} = \{\Gamma_{i(k)} \in \mathfrak{L}_{\mathfrak{A}_k}(E_k, E_{i(k)}) : i(k) \in I_k\}$, $\mathcal{W}^{(k)} = \{(W_{i(k)}, \omega_{i(k)})\}_{i(k)\in I_k}$ $\mathcal{V}^{(k)} = \{(V_{i(k)}, \upsilon_{i(k)}) : i(k) \in I_k\}$, where $W_{i(k)}$ and $V_{i(k)}$ are orthogonally complemented submodules of E_k and $\omega_{i(k)}$ and $\upsilon_{i(k)}$ are weights in $\mathfrak{A}_k$, for each $1 \leq k \leq n$. $\otimes_{k=1}^{n} \Phi^{(k)}$ and $\otimes_{k=1}^{n} \mathcal{W}^{(k)}$ are

$$\{\Lambda_{i(1)} \otimes \ldots \otimes \Lambda_{i(n)} \in \mathfrak{L}_{(\mathfrak{A}_1 \otimes \ldots \otimes \mathfrak{A}_n)}(\otimes_{k=1}^{n} E_k, E_{i(1)} \otimes \ldots \otimes E_{i(n)}), (i(1), \ldots, i(n)) \in (I_1 \times \ldots \times I_n)\},$$

$$\{(W_{i(1)} \otimes \ldots \otimes W_{i(n)}, \omega_{i(1)} \otimes \ldots \otimes \omega_{i(n)}) : (i(1), \ldots, i(n)) \in (I_1 \times \ldots \times I_n)\}.$$

Tensor products of g-frames and fusion frames in Hilbert C^*-modules were studied in [9]. Here, we consider the tensor product of α-duals in Hilbert C^*-modules. Indeed, some obtained results in [12] are generalized to Hilbert C^*-modules.

Conclusion

In the present paper, the following definitions and theorems are stated:

***Definition* 0.1.** *Let $\alpha \in \mathbb{Z}$ and let $\Lambda = \{\Lambda_i \in \mathfrak{L}(E, E_i) : i \in I\}$ be a g-frame. A g-frame $\Gamma = \{\Gamma_i \in \mathfrak{L}(E, E_i) : i \in I\}$ is called an α-dual of $\{\Lambda_i\}_{i\in I}$ if $\sum_{i\in I} \Lambda_i^* \Gamma_i f = S_\Lambda^\alpha f$, for each $f \in E$.*

***Theorem* 0.2.** *Suppose that $\Phi^{(k)}$'s and $\Psi^{(k)}$'s are g-frames. If $\Psi^{(k)}$ is an α-dual of $\Phi^{(k)}$, for each $k \in \{1, \ldots, n\}$, then $\otimes_{k=1}^{n} \Psi^{(k)}$ is an α-dual of $\otimes_{k=1}^{n} \Phi^{(k)}$.*

***Definition* 0.3.** *Let $\alpha \in \mathbb{Z}$ and $\mathcal{W} = \{(W_i, \omega_i)\}_{i\in I}$ and $\mathcal{V} = \{(V_i, \upsilon_i)\}_{i\in I}$ be two fusion frames for E. Then, $\mathcal{V}$ is called an α-dual of $\mathcal{W}$ if $\sum_{i\in I} \upsilon_i \omega_i \pi_{W_i} \pi_{V_i} f = S_\mathcal{W}^\alpha f$, for each $f \in E$.*

***Theorem* 0.4.** *Suppose that $\mathcal{W}^{(k)}$'s and $\mathcal{V}^{(k)}$'s are fusion frames. If $\mathcal{V}^{(k)}$ is an α-dual of $\mathcal{W}^{(k)}$, for each $k \in \{1, \ldots, n\}$, then $\otimes_{k=1}^{n} \mathcal{V}^{(k)}$ is an α-dual of $\otimes_{k=1}^{n} \mathcal{W}^{(k)}$.*

جبرهای اندازه و کاربردها
سال ۱۴۰۳، دوره ۱، شماره ۲، ص ۱۶۴-۱۵۴

حاصل‌ضرب‌های تانسوری برای α-دوگان‌های g-قاب‌ها و قاب‌های مخلوط در C^*-مدول‌های هیلبرت

فاطمه زمانی میرارکلائی [۱]

۱. گروه ریاضی، دانشگاه خوارزمی، تهران، ایران. رایانامه: std_zamani243@khu. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت: ۱۴۰۳/۲/۲
تاریخ بازنگری: ۱۴۰۳/۴/۳
تاریخ پذیرش: ۱۴۰۳/۴/۱۱
تاریخ انتشار: ۱۴۰۳/۵/۳۰

کلمات کلیدی:
C^*-مدول هیلبرت،
g-قاب،
قاب مخلوط،
α-دوگان،
حاصل‌ضرب تانسوری

رده‌بندی ریاضی:
42C15

چکیده

در این مقاله، نشان می‌دهیم که حاصل‌ضرب تانسوری تعداد متناهی از α-دوگان‌های g-قاب‌های استاندارد (قاب‌های مخلوط استاندارد) یک α-دوگان برای حاصل‌ضرب تانسوری g-قاب‌ها (قاب‌های مخلوط) در فضای حاصل‌ضرب تانسوری C^*-مدول‌های هیلبرت است.

استناد: زمانی میرارکلائی، فاطمه. (۱۴۰۳). حاصل‌ضرب‌های تانسوری برای α-دوگان‌های g-قاب‌ها و قاب‌های مخلوط در C^*-مدول‌های هیلبرت. جبرهای اندازه و کاربردها، ۱(۲)، ۱۶۴-۱۵۴.

http://doi.org/10.22091/maa.2024.11097.1023

ناشر: دانشگاه قم.

۱ مقدمه

در سال ۱۹۵۲، دافین و شیفر که در حال بررسی چند مسئلهٔ اساسی در مورد سری‌های فوریهٔ غیرهارمونیک بودند، احساس نیاز به معرفی مفهومی کردند و آن را یک قاب فضای هیلبرت نامیدند ([۴]). اما ارزش قاب‌ها در فضاهای هیلبرت پس از چاپ مقالهٔ دوبچیز، گراسمان و مِیِر ([۳]) در سال ۱۹۸۶ بیش‌ازپیش مشخص شد.

تعریف ۱.۱. فرض کنیم H یک فضای هیلبرت جدایی‌پذیر باشد. دنبالهٔ $\mathcal{F} = \{f_i\}_{i\in I}$ یک قاب گسسته برای H نامیده می‌شود اگر دو عدد مثبت $A_{\mathcal{F}}$ و $B_{\mathcal{F}}$ وجود داشته باشند به‌طوری‌که برای هر $f \in H$ داشته باشیم:

$$A_{\mathcal{F}}\|f\|^2 \leq \sum_{i\in I} |\langle f, f_i\rangle|^2 \leq B_{\mathcal{F}}\|f\|^2.$$

قاب‌های تعمیم‌یافته یا g-قاب‌ها به‌عنوان یکی از تعمیم‌های مهم قاب‌ها در [۱۳] معرفی شدند.

تعریف ۲.۱. فرض کنیم به‌ازای هر $i \in I$، H_i یک فضای هیلبرت باشد. دنبالهٔ $\Lambda = \{\Lambda_i \in L(H, H_i) : i \in I\}$ یک g-قاب برای H نسبت به $\{H_i\}_{i\in I}$ نامیده می‌شود اگر دو عدد مثبت A و B موجود باشند به‌طوری‌که برای هر $f \in H$، نامساوی زیر برقرار باشد:

$$A\|f\|^2 \leq \sum_{i\in I} \|\Lambda_i f\|^2 \leq B\|f\|^2.$$

در این حالت Λ را یک (A, B) g-قاب می‌نامیم.
A و B کران‌های g-قاب نامیده می‌شوند (A را یک کران پایین و B را یک کران بالا می‌نامیم). اگر در تعریف فوق Λ در نامساوی سمت راست صدق کند، آنگاه Λ را یک g-دنبالهٔ بسل می‌نامیم.

C^*-مدول‌های هیلبرت، تعمیم‌هایی از فضاهای هیلبرت هستند که همانند فضاهای هیلبرت دارای یک ضرب داخلی هستند با این تفاوت که ضرب داخلی دو عضو از یک C^*-مدول هیلبرت عضوی از یک C^*-جبر است و اگر این C^*-جبر میدان اعداد مختلط باشد، آنگاه این C^*-مدول هیلبرت، یک فضای هیلبرت خواهد بود.

تعریف ۳.۱. فرض کنیم $\mathfrak{A}$ یک C^*-جبر و E یک $\mathfrak{A}$-مدول چپ باشد. E را یک پیش C^*-مدول هیلبرت گوییم اگر ضرب داخلی $\mathfrak{A}$-مقدار $\langle .,. \rangle : E \times E \to \mathfrak{A}$ موجود باشد به‌طوری‌که به‌ازای هر $x, y, z \in E$ ، $\alpha, \beta \in \mathbb{C}$ و $a \in \mathfrak{A}$ داشته باشیم:

(آ) $\langle \alpha x + \beta y, z\rangle = \alpha\langle x, z\rangle + \beta\langle y, z\rangle$؛

(ب) $\langle ax, y\rangle = a\langle x, y\rangle$؛

(پ) $\langle x, y\rangle^* = \langle y, x\rangle$؛

(ت) $\langle x, x\rangle \geq 0$ و اگر $\langle x, x\rangle = 0$، آنگاه $x = 0$.

برای هر $x \in E$، تعریف می‌کنیم $\|x\| := \|\langle x, x\rangle\|^{\frac{1}{2}}$. اگر E با این نرم کامل باشد، آنگاه E را یک $\mathfrak{A}$-مدول هیلبرت یا یک C^*-مدول هیلبرت روی $\mathfrak{A}$ می‌نامیم. برای هر $a \in \mathfrak{A}$، داریم $|a| = (a^*a)^{\frac{1}{2}}$ و اینک برای هر $x \in E$ تعریف می‌کنیم $|x| := \langle x, x\rangle^{\frac{1}{2}}$.

تعریف ۴.۱. فرض کنیم E و F دو C^*-مدول هیلبرت باشند. عملگر $T : E \to F$ را الحاقی‌پذیر گوییم اگر یک عملگر $T^* : F \to E$ موجود باشد به‌طوری‌که به‌ازای هر $x \in E$ و $y \in F$ تساوی زیر برقرار باشد

$$\langle T(x), y\rangle = \langle x, T^*(y)\rangle.$$

عملگر T^* را الحاقی T می‌نامیم.

هر عملگر الحاقی‌پذیر مانند T کران‌دار و خطی است (یعنی به‌ازای هر $a \in \mathfrak{A}$ و $x \in E$ داریم $T(ax) = aT(x)$). مجموعهٔ تمام عملگرهای الحاقی‌پذیر از E به F را با $\mathfrak{L}(E, F)$ یا با $\mathfrak{L}_{\mathfrak{A}}(E, F)$ نمایش می‌دهیم. دقت شود که $\mathfrak{L}(E, E)$ یک C^*-جبر است که آن را با $\mathfrak{L}(E)$ نشان می‌دهیم.

تعریف ۵.۱. فرض کنیم $\mathfrak{A}$ یک C^*-جبر باشد.

(آ) $\mathfrak{A}$-مدول هیلبرت E را به‌طور متناهی تولیدشده گوییم اگر زیرمجموعهٔ متناهی $\{x_1, \cdots, x_n\} \subseteq E$ موجود باشد به‌طوری‌که هر $x \in E$ را بتوان به‌صورت یک ترکیب $\mathfrak{A}$-خطی مانند $x = \sum_{i=1}^{n} a_i x_i$ ، $a_i \in \mathfrak{A}$ نوشت.

(ب) $\mathfrak{A}$-مدول هیلبرت E را به‌طور شمارا تولیدشده گوییم اگر زیرمجموعهٔ شمارایی مانند $\{x_i\}_{i\in I}$ موجود باشد به‌طوری‌که هر $x \in E$، در بستار غلاف $\mathfrak{A}$-خطی $\{x_i\}_{i\in I}$ باشد.

برای مطالعهٔ بیشتر در مورد C^*-مدول‌های هیلبرت به [۸] رجوع کنید.
قاب‌ها و g-قاب‌ها در C^*-مدول‌های هیلبرت به‌ترتیب در [۵] و [۶] معرفی شدند. همچنین قاب‌های مخلوط در C^*-مدول‌های هیلبرت نیز در [۶] معرفی شده‌اند.

تعریف ۶.۱. فرض کنیم E یک C^*-مدول هیلبرت باشد. دنبالهٔ $\{f_i\}_{i\in I} \subseteq E$ را یک قاب برای E گوییم اگر دو عدد مثبت A و B موجود باشند به‌طوری‌که به‌ازای هر $x \in E$، نامساوی زیر برقرار باشد:

$$A\langle x, x\rangle \leq \sum_{i\in I} \langle x, f_i\rangle\langle f_i, x\rangle \leq B\langle x, x\rangle.$$

در این حالت $\{f_i\}_{i\in I}$ را یک (A, B)-قاب می‌نامیم.

A و B را کران‌های قاب می‌نامیم (A را یک کران پایین و B را یک کران بالا گوییم). اگر نامساوی سمت راست برقرار باشد $\{f_i\}_{i\in I}$ را یک دنبالهٔ بسل می‌نامیم. اگر به‌ازای هر $x \in E$، سری $\sum_{i\in I}\langle x, f_i\rangle\langle f_i, x\rangle$ با نرم همگرا باشد، آنگاه قاب را استاندارد گوییم.

تعریف ۷.۱. فرض کنیم $\{E_i\}_{i\in I}$ دنباله‌ای از C^*-مدول‌های هیلبرت باشد. دنبالهٔ $\Lambda = \{\Lambda_i \in \mathfrak{L}(E, E_i) : i \in I\}$ یک g-قاب برای E نسبت به $\{E_i\}_{i\in I}$ نامیده می‌شود اگر دو عدد مثبت A و B موجود باشند به‌طوری‌که به‌ازای هر $x \in E$، نامساوی زیر برقرار باشد

$$A\langle x, x\rangle \leq \sum_{i\in I} \langle \Lambda_i x, \Lambda_i x\rangle \leq B\langle x, x\rangle.$$

در این حالت Λ را یک g-قاب (A, B) می‌نامیم. A و B را کران‌های g-قاب می‌نامیم. g-قاب Λ را استاندارد گوییم اگر برای هر $x \in E$، سری $\sum_{i\in I}\langle \Lambda_i x, \Lambda_i x\rangle$ با نرم همگرا باشد. همچنین اگر نامساوی سمت راست برقرار باشد، آنگاه Λ را یک g-دنبالهٔ بسل می‌نامیم.

تعریف ۸.۱. فرض کنیم $\{\omega_i : i \in I\} \subseteq \mathfrak{A}$ خانواده‌ای از وزن‌ها باشد یعنی هر ω_i یک عضو مثبت و وارون‌پذیر در مرکز $\mathfrak{A}$ باشد و $\{W_i : i \in I\}$ خانواده‌ای از زیرمدول‌های به‌طور متعامد مکمل‌دار در E باشد. در این صورت $\{(W_i, \omega_i)\}_{i\in I}$ را یک قاب مخلوط می‌نامیم اگر اعداد A و B موجود باشند به‌طوری‌که برای هر $x \in E$ داشته باشیم:

$$A.\langle x, x\rangle \leq \sum_{i\in I} \omega_i^2 \langle \pi_{W_i}(x), \pi_{W_i}(x)\rangle \leq B.\langle x, x\rangle.$$

اگر $W = \{(W_i, \omega_i)\}_{i\in I}$ یک قاب مخلوط باشد، آنگاه عملگر

$$S_W : E \longrightarrow E, \quad S_W x = \sum_{i\in I} \omega_i{}^2 \pi_{W_i} x$$

الحاقی‌پذیر است. همچنین اگر Λ یک g-دنبالهٔ بسل باشد، آنگاه

$$S_\Lambda : E \longrightarrow E, \quad S_\Lambda(x) = \sum_{i\in I} \Lambda_i^* \Lambda_i(x)$$

الحاقی‌پذیر است. برای مطالعهٔ بیشتر مراجع [۱۰، ۱۱] را مطالعه نمایید.

۲ نتایج اصلی

حاصل‌ضرب‌های تانسوری g-قاب‌ها و قاب‌های مخلوط برای فضاهای هیلبرت در مقاله [۷] و برای C^*-مدول‌های هیلبرت در مقاله [۹] بررسی شدند. همچنین α-دوگان‌های g-قاب‌ها و قاب‌های مخلوط برای فضاهای هیلبرت در [۱، ۱۲] مورد مطالعه قرار گرفتند.

در این مقاله، با استفاده از نتایج به‌دست‌آمده در مقالات فوق، نتایج مشابهی در مورد α-دوگان‌ها در C^*-مدول‌های هیلبرت به دست می‌آوریم.

در این مقاله I و I_k (برای $1 \leq k \leq n$) زیرمجموعه‌هایی از $\mathbb{N}$ هستند. $\mathfrak{A}_k$ یک C^*-جبر یکدار است، E، E_k و $E_{i(k)}$ C^*-مدول‌های هیلبرت به‌طور متناهی یا شمارا تولیدشده هستند (برای $k \in \{1, \ldots, n\}$ و $i(k) \in I_k$).
$\Phi^{(k)} = \{\Lambda_{i(k)} \in \mathfrak{L}_{\mathfrak{A}_k}(E_k, E_{i(k)})\}_{i(k)\in I_k}$، $\Psi^{(k)} = \{\Gamma_{i(k)} \in \mathfrak{L}_{\mathfrak{A}_k}(E_k, E_{i(k)}) : i(k) \in I_k\}$،
$\mathcal{W}^{(k)} = \{(W_{i(k)}, \omega_{i(k)})\}_{i(k)\in I_k}$ و $\mathcal{V}^{(k)} = \{(V_{i(k)}, \upsilon_{i(k)}) : i(k) \in I_k\}$، که در آن‌ها $W_{i(k)}$ و $V_{i(k)}$ زیرمدول‌های به‌طور متعامد مکمل‌دار در E_k هستند و $\omega_{i(k)}$ و $\upsilon_{i(k)}$ وزن‌هایی در $\mathfrak{A}_k$ هستند. $\otimes_{k=1}^n \Phi^{(k)}$ و $\otimes_{k=1}^n \mathcal{W}^{(k)}$ به‌صورت زیر تعریف می‌شوند:

$$\{\Lambda_{i(1)} \otimes \ldots \otimes \Lambda_{i(n)} \in \mathfrak{L}_{(\mathfrak{A}_1 \otimes \ldots \otimes \mathfrak{A}_n)}(\otimes_{k=1}^n E_k, E_{i(1)} \otimes \ldots \otimes E_{i(n)}), (i(1), \ldots, i(n)) \in (I_1 \times \ldots \times I_n)\},$$

$$\{(W_{i(1)} \otimes \ldots \otimes W_{i(n)}, \omega_{i(1)} \otimes \ldots \otimes \omega_{i(n)}) : (i(1), \ldots, i(n)) \in (I_1 \times \ldots \times I_n)\}.$$

یادآوری می‌کنیم که اگر $\mathfrak{A}_k$ یک C^*-جبر باشد، آنگاه $\otimes_{k=1}^n \mathfrak{A}_k$ یک C^*-جبر است و برای هر $a_k \in \mathfrak{A}_k$ داریم $\|a_1 \otimes \ldots \otimes a_n\| = \Pi_{k=1}^n \|a_k\|$. ضرب و برگشت روی تانسورهای ساده به‌صورت زیر تعریف می‌شوند

$$(\otimes_{k=1}^n a_k)(\otimes_{k=1}^n b_k) = \otimes_{k=1}^n (a_k b_k)$$

و

$$(\otimes_{k=1}^n a_k)^* = \otimes_{k=1}^n a_k^*.$$

اکنون اگر E_k یک C^*-مدول هیلبرت باشد (برای $1 \leq k \leq n$)، آنگاه حاصل‌ضرب تانسوری $E_1 \otimes \ldots \otimes E_n = \otimes_{k=1}^n E_k$ یک $(\otimes_{k=1}^n \mathfrak{A}_k)$-مدول هیلبرت است. اعمال مدولی و ضرب داخلی به صورت زیر تعریف می‌شوند:

$$\begin{aligned}(\otimes_{k=1}^n a_k)(\otimes_{k=1}^n x_k) &= (a_1 x_1) \otimes \ldots \otimes (a_n x_n) \\ &= \otimes_{k=1}^n (a_k x_k),\end{aligned}$$

و

$$\langle \otimes_{k=1}^n x_k, \otimes_{k=1}^n y_k \rangle = \langle x_1, y_1 \rangle \otimes \ldots \otimes \langle x_n, y_n \rangle = \otimes_{k=1}^n \langle x_k, y_k \rangle.$$

تعریف ۱.۲. فرض کنیم $\alpha \in \mathbb{Z}$ و $\Lambda = \{\Lambda_i \in \mathfrak{L}(E, E_i) : i \in I\}$ یک g-قاب باشد. g-قاب $\Gamma = \{\Gamma_i \in \mathfrak{L}(E, E_i) : i \in I\}$ یک α-دوگان $\{\Lambda_i\}_{i\in I}$ نامیده می‌شود اگر برای هر $f \in E$ داشته باشیم:

$$\sum_{i\in I} \Lambda_i^* \Gamma_i f = S_\Lambda^\alpha f.$$

قضیه ۲.۲. فرض کنیم $\Phi^{(k)}$ها و $\Psi^{(k)}$ها g-قاب باشند. اگر $\Psi^{(k)}$ یک α-دوگان برای $\Phi^{(k)}$ باشد (به‌ازای هر $k \in \{1, \ldots, n\}$)، آنگاه $\otimes_{k=1}^n \Psi^{(k)}$ یک α-دوگان برای $\otimes_{k=1}^n \Phi^{(k)}$ است.

اثبات. کافی است قضیه را برای $n = 2$ ثابت کنیم. فرض کنیم B_1 و B_2 کران‌های بالا برای $\Phi^{(1)}$ و $\Phi^{(2)}$ باشند، $I_1 := \{i_{11}, \ldots, i_{1p}, \ldots\}$ و $I_2 := \{i_{21}, \ldots, i_{2q}, \ldots\}$. سپس برای $x \in E_1$ و $y \in E_2$ تعریف می‌کنیم $S_{1p}x = \sum_{r=1}^p \Lambda_{i_{1r}}^* \Lambda_{i_{1r}} x$ و $S_{2q}y = \sum_{t=1}^q \Lambda_{i_{2t}}^* \Lambda_{i_{2t}} y$. اکنون برای هر $p, q \in \mathbb{N}$ داریم $\|S_{1p}\| \leq \|S_{\Phi^{(1)}}\|$ و $\|S_{2q}\| \leq \|S_{\Phi^{(2)}}\|$ و چون $\Phi^{(1)}$ و $\Phi^{(2)}$ g-قاب‌های استاندارد هستند، پس برای $k \in \{1, 2\}$ خواهیم داشت $0 \leq S_{\Phi^{(k)}} \leq B_k . Id_{E_k}$ درنتیجه

$$\circ \leq S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}} \leq B_1 B_2 . Id_{(E_1 \otimes E_2)}.$$

لذا از لم ۱.۴ در [۸]، برای هر $z \in E_1 \otimes E_2$ و $p, q \in \mathbb{N}$ داریم

$$\langle (S_{1p} \otimes S_{2q})z, z\rangle \leq \langle (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z, z\rangle \leq B_1 B_2 . \langle z, z\rangle. \qquad (1.2)$$

همچنین به‌سادگی می‌توان مشاهده کرد که برای هر $z = \sum_{l=1}^{m} x_l \otimes y_l \in E_1 \otimes_{alg} E_2$ داریم

$$\lim_{p,q} (S_{1p} \otimes S_{2q})z = (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z.$$

اینک اگر $z \in E_1 \otimes E_2$، آنگاه با انتخاب مناسب یک $z_\circ \in E_1 \otimes_{alg} E_2$ و با استفاده از نامساوی

$$\begin{aligned} & \|(S_{1p} \otimes S_{2q})z - (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z\| \\ \leq\ & \|S_{\Phi^{(1)}}\| \|S_{\Phi^{(2)}}\| \|z - z_\circ\| \\ +\ & \|(S_{1p} \otimes S_{2q})z_\circ - (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z_\circ\| \\ +\ & B_1 B_2 \|z - z_\circ\|, \end{aligned}$$

خواهیم داشت

$$\lim_{p,q} (S_{1p} \otimes S_{2q})z = (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z.$$

این رابطه نشان می‌دهد سری $\sum_{(i(1),i(2))\in I_1 \times I_2} \langle (\Lambda_{i(1)} \otimes \Lambda_{i(2)})z, (\Lambda_{i(1)} \otimes \Lambda_{i(2)})z\rangle$ با نرم همگرا است و با استفاده از (۱.۲)، داریم

$$\sum_{(i(1),i(2))\in I_1 \times I_2} \langle (\Lambda_{i(1)} \otimes \Lambda_{i(2)})z, (\Lambda_{i(1)} \otimes \Lambda_{i(2)})z\rangle$$

$$= \langle (S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})z, z\rangle \leq B_1 B_2 . \langle z, z\rangle. \qquad (2.2)$$

این نشان می‌دهد $\Phi^{(1)} \otimes \Phi^{(2)}$ یک g-دنبالهٔ بسل استاندارد با کران $B_1 B_2$ است.

حال فرض کنیم $\Phi^{(1)}$ و $\Phi^{(2)}$، g-قاب‌های استاندارد با کران‌های پایین A_1 و A_2 باشند. چون

$$\begin{aligned} & A_1 A_2 . Id_{E_1 \otimes E_2} \\ \leq\ & (\|S^{-1}_{\Phi^{(1)}}\|^{-1} \|S^{-1}_{\Phi^{(2)}}\|^{-1}) . Id_{E_1 \otimes E_2} \\ =\ & \|(S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}})^{-1}\|^{-1} . Id_{E_1 \otimes E_2} \\ \leq\ & S_{\Phi^{(1)}} \otimes S_{\Phi^{(2)}}, \end{aligned}$$

با استفاده از (۱.۲) و (۲.۲)، به دست می‌آوریم که $\otimes_{k=1}^{2} \Phi^{(k)}$ یک g-قاب استاندارد با کران پایین $A_1 A_2$ است.

به‌طور مشابه می‌توان نشان داد که $\otimes_{k=1}^{2} \Psi^{(k)}$ یک g-قاب استاندارد است.

پس تا اینجا نشان دادیم که $\otimes_{k=1}^{n} \Phi^{(k)}$ و $\otimes_{k=1}^{n} \Psi^{(k)}$ g-قاب‌های استاندارد هستند. همچنین از رابطه (۲.۲) به دست می‌آوریم که $\otimes_{k=1}^{n} S_{\Phi^{(k)}} = S_{\otimes_{k=1}^{n} \Phi^{(k)}}$ بنابراین برای هر $m \in \mathbb{N}$ داریم

$$\otimes_{k=1}^{n} S^{m}_{\Phi^{(k)}} = (\otimes_{k=1}^{n} S_{\Phi^{(k)}})^{m} = S^{m}_{\otimes_{k=1}^{n} \Phi^{(k)}},$$

و

$$\otimes_{k=1}^{n} S^{-1}_{\Phi^{(k)}} = (\otimes_{k=1}^{n} S_{\Phi^{(k)}})^{-1} = S^{-1}_{\otimes_{k=1}^{n} \Phi^{(k)}}.$$

لذا برای هر $\alpha \in \mathbb{Z}$ خواهیم داشت

$$\otimes_{k=1}^{n} S^{\alpha}_{\Phi^{(k)}} = (\otimes_{k=1}^{n} S_{\Phi^{(k)}})^{\alpha} = S^{\alpha}_{\otimes_{k=1}^{n} \Phi^{(k)}}.$$

پس برای هر $\otimes_{k=1}^n f_{i(k)} \in \otimes_{k=1}^n E_k$ داریم:

$$\begin{aligned}&\sum_{(i(1),\ldots,i(n))\in(I_1\times\ldots\times I_n)} (\Lambda_{i(1)}\otimes\ldots\otimes\Lambda_{i(n)})^*(\Gamma_{i(1)}\otimes\ldots\otimes\Gamma_{i(n)})(\otimes_{k=1}^n f_{i(k)})\\ =\ & \otimes_{k=1}^n S^\alpha_{\Phi^{(k)}}(\otimes_{k=1}^n f_{i(k)}) = (\otimes_{k=1}^n S_{\Phi^{(k)}})^\alpha(\otimes_{k=1}^n f_{i(k)})\\ =\ & S^\alpha_{\otimes_{k=1}^n \Phi^{(k)}}(\otimes_{k=1}^n f_{i(k)}).\end{aligned}$$

این رابطه نشان می‌دهد که $\otimes_{k=1}^n \Psi^{(k)}$ یک $\otimes_{k=1}^n \Phi^{(k)}$ یک α-دوگان برای است. □

تعریف ۳.۲. فرض کنیم $\alpha \in \mathbb{Z}$ و $\mathcal{W} = \{(W_i, \omega_i)\}_{i\in I}$ یک قاب مخلوط باشد. قاب مخلوط $\mathcal{V} = \{(V_i, \upsilon_i)\}_{i\in I}$ یک α-دوگان $\mathcal{W}$ نامیده می‌شود اگر برای هر $f \in E$ داشته باشیم $\sum_{i\in I} \upsilon_i\omega_i\pi_{W_i}\pi_{V_i} f = S^\alpha_{\mathcal{W}} f$.

قضیه ۴.۲. فرض کنیم $\mathcal{W}^{(k)}$ها و $\mathcal{V}^{(k)}$ها قاب‌های مخلوط باشند. اگر $\mathcal{V}^{(k)}$ یک α-دوگان برای $\mathcal{W}^{(k)}$ باشد (به‌ازای هر $k \in \{1, \ldots, n\}$)، آنگاه $\otimes_{k=1}^n \mathcal{V}^{(k)}$ یک α-دوگان برای $\otimes_{k=1}^n \mathcal{W}^{(k)}$ است.

اثبات. نتیجه از قضیه ۲.۲ و با استفاده از این حقیقت به دست می‌آید که $\Phi^{(k)} := \{\omega_{i(k)}\pi_{W_{i(k)}}\}_{i(k)\in I_k}$ یک g-قاب استاندارد است (برای هر $1 \le k \le n$) اگر و فقط اگر $\otimes_{k=1}^n \Phi^{(k)} = \{(\omega_{i(1)}\otimes\ldots\otimes\omega_{i(n)})\pi_{(W_{i(1)}\otimes\ldots\otimes W_{i(n)})}\}_{(i(1),\ldots,i(n))\in(I_1\times\ldots\times I_n)}$ یک g-قاب استاندارد باشد ([۹]). □

References

[1] Abdollahpour, M.R., & Najati, A. (2011). G-frames and Hilbert-Schmidt operators. *Bull. Iranian Math. Soc*, 4, 141–155.

[2] Casazza, P., & Kutyniok, G. (2004). Frames of subspaces. *Contemp. Math. Amer. Math. Soc*, 345, 87–113.

[3] Daubechies, I., Grossmann, A., & Meyer, Y. (1986). Painless nonorthogonal expansions. *J. Math. Phys*, 27, 1271–1283. DOI: https://doi.org/10.1063/1.527388.

[4] Duffin, R.J., & Schaeffer, A.C. (1952). A class of nonharmonic Fourier series. *Trans. Amer. Math. Soc*, 72, 341–366. DOI: https://doi.org/10.2307/1990760.

[5] Frank, M., & Larson, D.R. (2002). Frames in Hilbert C^*-modules and C^*-algebras. *J. Operator Theory*, 48, 273–314.

[6] Khosravi, A., & Khosravi, B. (2008). Fusion frames and g-frames in Hilbert C^*-modules. *Int. J. Wavelets Multiresolut. Inf. Process*, 6, 433–446. DOI: https://doi.org/10.1142/S0219691308002458.

[7] Khosravi, A., & Mirzaee Azandaryani, M. (2012). Fusion frames and g-frames in tensor product and direct sum of Hilbert spaces. *Appl. Anal. Discrete Math*, 6, 287–303. DOI: https://doi.org/10.2298/AADM120619014K.

[8] Lance, E.C. (1995). Hilbert C^*-modules: A Toolkit for Operator Algebraists. *Cambridge University Press, Cambridge*.

[9] Mirzaee Azandaryani, M. (2016). Bessel multipliers on the tensor product of Hilbert C^*-modules. *Int. J. Industrial Mathematics*, 8(1), 9–16.

[10] Mirzaee Azandaryani, M. (2018). Invertibility of multipliers in Hilbert C^*-modules. *Filomat*, 32(17), 6073–6085. DOI: https://doi.org/10.2298/FIL1817073M.

[11] Mirzaee Azandaryani, M. (2023). The stability of duals and approximate duals of frames and generalized frames under the action of bounded operators. *Measure Algebras and Applications*, 1(1), 36–52. DOI: http://doi.org/10.22091/MAA.2023.9513.1007.

[12] Mirzaee Azandaryani, M., & Pourgholamhossein, M. (2023). Duality and α-duality of g-frames and fusion frames in Hilbert spaces. *Mathematical Analysis & Convex Optimization*, 4, 1–6. DOI: http://doi.org/10.22034/maco.4.2.1.

[13] Sun, W. (2006). G-frames and g-Riesz bases. *J. Math. Anal. Appl*, 322, 437–452. DOI: https://doi.org/10.1016/j.jmaa.2005.09.039.

Measure Algebras and Applications

Table of Contents

Measure Algebras and Applications

Scientific Biannual Journal at the University of Qom

Vol 1. Issue 2. Spring & Summer (August 2024).

Publisher: University of Qom

Director in Charge: Alireza Bagheri Salec (Ph.D)

Editor in Chief: Morteza Mirzaee Azandaryani (Ph.D)

- ”Measure Algebras and Applications” (MAA) presents papers that treat mathematical analysis, especially the ones related to measure spaces (in Persian with English Extended Abstract).
- The authors are fully responsible for the content of their papers.
- The content of MAA is open to be cited on the condition that the source is mentioned.
- MAA is free to edit, summarize and revise the papers.

Address: University of Qom, Qom, Iran.

Tel: 00982532103360

Website: maa.qom.ac.ir ∗ Email: maa@qom.ac.ir