دانشگاه تبریز
دانشکدهٔ فیزیک
گروه فیزیک نظری و اختر فیزیک

رساله

برای دریافت درجه دکتری در رشته
فیزیک گرایش نظری

عنوان

مطالعهٔ کدهای کوانتومی و کلاسیکی و درهمتنیدگی کوانتومی با استفاده از جبرهای نیم ـ ساده

استاد راهنما:

دکتر محمد علی جعفریزاده
دکتر حسین متولی

استاد مشاور:

دکترسید کمال الدین سید یعقوبی

پژوهشگر:

یحیی اکبری کوربلاغ

مهر ماه ۱۳۸۷

بِسمِ اللّهِ الرّحمنِ الرّحيم

تقدیم به:

پدر و مادر عزیزم

همسر مهربانم

و فرزندان دلبندم

یحیی اکبری کوربلاغ
مهر ماه ۱۳۸۷

به نام خدا

سپاس و ستایش پروردگار بی همتا را که به قلم قداست و به انسان کرامت بخشید و انسان را به زیور علم و معرفت بیاراست. اینک که در سایهٔ عنایات بیکران خداوندی دورهٔ دکتری را پشت سر نهاده و موفق به نگارش رسالهٔ این دوره شده‌ام،

از استاد راهنمای گرانمایه و بزرگوارم جناب آقای **دکتر محمد علی جعفریزاده** که در طول این دوره اندیشه‌ها و دیدگاه‌های علمی ایشان همواره چراغ راهم بود و از راهنمایی‌های ارزندهٔ ایشان بهره‌های فراوان بردم، با کمال ادب و احترام تشکر و قدردانی می‌نمایم.

از استاد راهنمای بزرگوارم جناب آقای **دکتر حسین متولی** به خاطر زحماتی که متحمل شدند تشکر و قدردانی می‌نمایم.

از استاد مشاور بزرگوارم جناب آقای **دکتر سید کمال الدین سید یعقوبی** که از هیچگونه همفکری و مشورت دریغ ننمودند سپاسگزاری می‌نمایم.

از اساتید ارجمند، آقایان **دکتر محمد رضا ابوالحسنی**، **دکتر رسول رکنی‌زاده** و **دکتر مهدی رضائی کرامتی** که زحمت داوری این رساله را تقبل و با دقت و حوصلهٔ فراوان رساله را مطالعه نمودند تشکر می‌نمایم.

از دوستان عزیزم در دورهٔ دکتری فیزیک نظری، آقایان دکتر سید جواد اخترشناس، دکتر مهدی میرزایی، دکتر مهدی رضائی کرامتی، دکتر صدیف احدپور، دکتر شهریار سلیمی، دکتر اسفندیار فیضی، دکتر قادر نجارباشی، دکتر ناصر کریمی و آقایان نقی بهزادی، کوروش آقایار، محمود مهدیان، احمد حشمتی، یوسف مظهری و خانم دکتر رحیمه صوفیانی، به دلیل روزهای خوبی که باهم داشتیم سپاسگزارم.

از مسئولین محترم دانشگاه تربیت معلم آذربایجان که فرصت ادامهٔ تحصیل را برایم فراهم آوردند و نیز از اساتید گرامی و کارکنان زحمتکش آن دانشگاه قدردانی می‌نمایم.

از مسئولین محترم، اساتید گرامی و کارکنان زحمتکش دانشگاه تبریز، خصوصاً دانشکدهٔ فیزیک آن دانشگاه، که در طول این دوره زحمات فراوانی را متقبل شده‌اند، تشکر می‌نمایم.

یحیی اکبری کوربلاغ

مهر ماه ۱۳۸۷

نام خانوادگی دانشجو: اکبری کوربلاغ　　　نام: یحیی

عنوان: مطالعهٔ کدهای کوانتومی و کلاسیکی و درهمتنیدگی کوانتومی با استفاده از جبرهای نیم ـ ساده

استاد راهنما: دکتر محمد علی جعفریزاده
دکتر حسین متولی

استاد مشاور: دکترسید کمال الدین سید یعقوبی

مقطع تحصیلی: دکتری　　رشته: فیزیک　　گرایش: نظری　　دانشگاه تبریز

دانشکدهٔ فیزیک　　تاریخ فارغ‌التحصیلی: مهر ماه ۱۳۸۷　　تعداد صفحه: ۱۰۵

کلید واژه‌ها: کد پایدارساز، شِمای همبسته، جبر نیم ـ ساده، شاهد درهمتنیدگی

چکیده

نظریهٔ کدگذاری از مباحث مهم محاسبات و اطلاعات کلاسیکی و کوانتومی است که پردازش، ذخیره سازی و انتقال مطمئن اطلاعات را ممکن می‌سازد. اطلاعات کوانتومی در حالت‌های درهمتنیدهٔ سیستم‌های کوانتومی ذخیره و حمل می‌شوند. از آنجا که این حالت‌ها در برابر واهمدوسی بسیار حساس و آسیب پذیر اند، وجود کدهای کوانتومی ضرورت اساسی دارد. یک ردهٔ بسیار مهم از کدهای کوانتومی که با کدهای کلاسیکی نیز ارتباط نزدیکی دارد، کدهای پایدارساز کوانتومی‌اند. هر چند کدهای پایدارساز دوتایی به خوبی مطالعه شده‌اند، اما مبحث کدهای پایدارساز غیر دوتایی هنوز نوپا است و مسائل حل نشدهٔ بسیاری را پیش روی خود دارد. در این رساله برای ابعادی که توان صحیحی از عدد دو اند، کدهای پایدارسازی با ماتریس‌های دیراک ساخته‌ایم. تشخیص حالت‌های کوانتومی درهمتنیده از حالت‌های کوانتومی جداپذیر در مبحث کدها نیز اهمیت اساسی دارد. از اینرو، از روش بهینه سازی محدب که کاربرد روز افزونی در مباحث محاسبات و اطلاعات کوانتومی پیدا می کند، استفاده کرده و چندین شاهد درهمتنیدگی پایدارساز و غیر پایدارساز ساخته‌ایم.

فهرست مطالب

۳ نتایج و بحث ۴۹

مقدمه

عصری که در آن به سر می‌بریم عصر اطلاعات است و انسان امروزی نیاز روزافزونی به سرعت و دقت در تولید، ذخیره‌سازی، انتقال و بازیابی اطلاعات دارد. وجود نوفه در کانال‌های ارتباطی اجتناب‌ناپذیر است. از اینرو برای انتقال مطمئن اطلاعات، مسئلهٔ کدگذاری و کدگشایی اهمیت پیدا می‌کند. در صورت ساخت رایانه‌های کوانتومی، کدهای کوانتومی جزء جداناپذیر آنها خواهد بود. نظریهٔ کدگذاری از مباحث مهم محاسبات و اطلاعات کلاسیکی و کوانتومی است که مورد توجه دانشمندان فیزیک، ریاضی و علوم ارتباطات است.

ایدهٔ اساسی کدها، اعم از کلاسیکی و کوانتومی، این است که برای حفظ یک پیام در برابر آثار نوفه، باید با افزودن اطلاعات زائد آن را کدگذاری کرد. چنانچه بخشی از اطلاعات پیام کدگذاری شده در اثر نوفه مخدوش شود، وجود این اطلاعات زائد سبب خواهد شد که پیام اصلی را بتوان به طور کامل بازیابی کرد. در کدهای کلاسیکی، اطلاعات زائد لازم را از طریق تکثیر اطلاعات پیام اصلی ایجاد می‌کنند اما این روش در کدهای کوانتومی کارایی ندارد زیرا بنا بر قضیهٔ «تکثیر ـ ممنوع»[۱] حالت‌های کوانتومی دلخواه تکثیرناپذیرند.

در هر مبحثی از علم و فناوری که نیاز به پردازش، ذخیره‌سازی و انتقال مطمئن اطلاعات باشد، نظریهٔ کدگذاری نیز کاربرد دارد. از جملهٔ کاربردهای کدهای کلاسیکی می‌توان به این موارد اشاره کرد: رایانه‌های کلاسیکی، تبادل اطلاعات میان کاوشگرهای فضایی و ایستگاه‌های زمینی، لوح‌های فشرده، تلفن‌های همراه، اینترنت، شماره‌گذاری بین‌المللی کتاب‌ها و شماره‌گذاری کارت‌های اعتباری و چک‌های بانکی.

زمانی که شور[۲] در سال ۱۹۹۴ الگوریتم زمان ـ چندجمله‌ای خود برای تجزیهٔ عددهای صحیح بزرگ روی رایانه‌های کوانتومی را ارائه داد، محاسبات و اطلاعات کوانتومی نیز به گونه‌ای چشمگیر مورد توجه قرار گرفت. اطلاعات کوانتومی در «حالت‌های درهمتنیدهٔ»[۳] سیستم‌های کوانتومی ذخیره می‌شوند. اما این حالت‌ها در برابر «واهمدوسی»[۴] ناشی از برهم‌کنش سیستم کوانتومی با محیط و «عدم دقت»[۵] ناشی از پیوسته بودن عمل‌های کوانتومی، بسیار آسیب‌پذیرند. از اینرو کدهای کوانتومی یک جزء اجتناب‌ناپذیر در بسیاری از زمینه‌های محاسبات

[۱] no-cloning theorem
[۲] Shor
[۳] entangled states
[۴] decoherence
[۵] inaccuracy

و اطلاعات کوانتومی است.

با توجه به این که اطلاعات کوانتومی در حالت‌های درهمتنیده ذخیره می‌شوند، تشخیص حالت‌های کوانتومی درهمتنیده از حالت‌های کوانتومی جداپذیر در مبحث کدها نیز از اهمیت خاصی برخوردار است. یکی از رهیافت‌های این مسئله، استفاده از شاهدهای درهمتنیدگی کوانتومی است و به همین دلیل ساخت این شاهدها از موضوعات مهم مبحث اطلاعات کوانتومی به شمار می‌آید. در سال‌های اخیر، روش بهینه سازی محدب کاربرد فراوانی در اکثر زمینه‌های اطلاعات کوانتومی، از جمله در ساخت شاهدهای کوانتومی، پیدا کرده است.

این رساله در سه فصل تدوین شده است. فصل اول به پیشینهٔ پژوهش و بررسی منابع مربوط به موضوع رساله اختصاص یافته است. در فصل دوم، تعریف‌ها و مفاهیم مورد نیاز و نیز ابزارهای ریاضی و راهکارهای لازم برای دستیابی به نتایج اصلی رساله آمده است. فصل سوم نتایج اصلی رساله را در بر می‌گیرد و از چهار بخش تشکیل شده است. بخش اول به ساخت کدهای پایدارساز غیر دوتایی از ماتریس‌های دیراک می‌پردازد. در بخش دوم، ساخت شاهدهای درهمتنیدگی پایدارساز با عملگرهای گروه پایدارساز برخی کدهای پایدارساز دوتایی به روش برنامه ریزی خطی مورد بررسی قرار می‌گیرد. موضوع بحث بخش سوم، ساخت شاهدهای درهمتنیدگی به روش بهینه سازی محدب است. سر انجام، موضوع بحث بخش چهارم ساخت شاهدهای درهمتنیدگی با ماتریس‌های گِل ـ مان است.

فصل ۱

پیشینهٔ پژوهش و بررسی منابع

پیشینهٔ تاریخی نظریهٔ کدگذاری کلاسیکی به مسئلهٔ اطلاع‌رسانی مطمئن از طریق کانال‌های نوفه‌دار که از مسائل نظریهٔ اطلاعات کلاسیکی است، می‌رسد. این دو نظریه، یعنی نظریهٔ کدگذاری و نظریهٔ اطلاعات کلاسیکی، از مقالهٔ مشهور ۱۹۴۸ شانون[۱] [۱] سرچشمه گرفتند. در این مقاله، شانون قضیهٔ معروف «کدگذاری کانال» خود را ارائه داد که وجود کدهای طویل خوب را تضمین می‌کرد. در سال ۱۹۵۰، همینگ[۲] نخستین کدهای تصحیحگر خطای کلاسیکی را معرفی کرد [۲].

زمانی که شور[۳] در سال ۱۹۹۴ الگوریتم زمان ـ چندجمله‌ای خود برای تجزیهٔ عددهای صحیح بزرگ روی رایانه‌های کوانتومی را ارائه داد [۳]، محاسبات و اطلاعات کوانتومی نیز به گونه‌ای چشمگیر مورد توجه قرار گرفت. اطلاعات کوانتومی در «حالت‌های درهمتنیدهٔ»[۴] سیستم‌های کوانتومی ذخیره می‌شوند. امامشکل اینجاست که این حالت‌ها در برابر «واهمدوسی»[۵] ناشی از برهم‌کنش سیستم کوانتومی با محیط و «عدم دقت»[۶] ناشی ازپیوسته بودن عمل‌های کوانتومی، بسیار آسیب‌پذیرند. هرچند نظریهٔ کدگذاری کلاسیکی در آن زمان بسیار پیشرفته بود، اما چهار مشکل اساسی مانع از آن می‌شد که راهکارهای نظریهٔ کدگذاری کلاسیکی بتوانند در حوزهٔ اطلاعات کوانتومی نیز کارایی داشته باشند:

۱) **اندازه‌گیری**— در راهکارهای کلاسیکی، فرض بر این است که برای تشخیص و تصحیح خطاها می‌توان روی تمام «بیت»[۷]ها (کوچکترین واحدهای اطلاعات کلاسیکی) اندازه‌گیری انجام داد. اماانجام هرگونه اندازه‌گیری روی «کیوبیت»[۸]ها (کوچکترین واحدهای اطلاعات کوانتومی)، اطلاعات کوانتومی کدگذاری شده در آنها را تباه می‌کند.

۲) **خطاهای فاز**— کدهای کلاسیکی فقط برای تشخیص و تصحیح خطای «وارونی بیت» طراحی شده‌اند. اما در اطلاعات کوانتومی، خطای «وارونی فاز» نیز روی می‌دهد.

۳) «**تکثیر ـ ممنوع**»[۹]— در کدگذاری کلاسیکی، اطلاعات را از طریق تکثیر آنها حفظ

---

[۱] Claude Shannon

[۲] Hamming

[۳] Shor

[۴] entangled states

[۵] decoherence

[۶] inaccuracy

[۷] bit

[۸] qubit

[۹] no-cloning

می‌کنند. اما بنا بر قضیهٔ «تکثیر ـ ممنوع» [۴]، اطلاعات کوانتومی دلخواه تکثیرناپذیرند.

۴) **خطاهای کوچک**— کدهای کلاسیکی برای تصحیح خطاهای بزرگ طراحی شده‌اند. اما به سبب پیوسته بودن اطلاعات کوانتومی، پیوستاری از خطاها می‌تواند در یک حالت کوانتومی رخ دهد. مثلاً نوفه ممکن است حالت کوانتومی را اندکی بچرخاند. این خطاهای کوچک، در صورت عدم مقابله، به مرور زمان روی هم انباشته شده اطلاعات کوانتومی را تباه می‌کنند.

علیرغم این موانع، شور [۵] و استین[۱۰] [٦] در سال ۱۹۹٦ نشان دادند که کدهای تصحیحگر خطای کوانتومی وجود دارند. شور نخستین کد تصحیحگر خطای کوانتومی را ارائه کرد و نشان داد که چگونه می‌توان یک کیوبیت را با کدگذاری آن در زیرفضایی از یک فضای هیلبرت، در برابر واهمدوسی حفظ کرد. کد شور بر تمام موانع فوق فائق آمد و اصول اساسی نظریهٔ عمومی «تصحیح خطای کوانتومی» را پایه‌ریزی کرد. در ساختن کد شور، بسیاری از اصول برجستهٔ مکانیک کوانتومی همچون برهم‌نهی، درهمتنیدگی، تحول یکانی و اندازه‌گیری، به کار رفته است. در همان زمان، کالدربنک[۱۱]، شور و استین هر یک جداگانه ساخت کدهای تصحیحگر خطای کوانتومی را از طریق برخی کدهای تصحیحگر خطای کلاسیکی پیشنهاد کردند [٦، ۷]. اکنون این قبیل کدها را کدهای CSS می‌نامند. کدهای کلاسیکی که در ساخت کدهای کوانتومی CSS به کار می‌روند باید دوگان[۱۲] خود را در بر داشته و یا دارای خاصیت خود ـ تعامدی باشند. پس از آن، نشان داده شد که ساخت کدهای کوانتومی از روی کدهای کلاسیکی را می‌توان بر شالودهٔ عمومی‌تری به نام «صورت‌بندی پایدارساز» [۱۳] استوار ساخت [۸، ۹]. در این صورت‌بندی، کد تصحیحگر خطای کوانتومی، بنا به تعریف، زیرفضایی است که توسط یک «گروه پایدارساز» تثبیت می‌شود. کدهای CSS، کدهای توپولوژیکی [۱۰] و کدهای رنگ [۱۱] مثال‌هایی از کدهای پایدارسازاند. نظریهٔ پایدارساز این امکان را فراهم می‌سازد که کدهای دوتایی[۱۴] یاچهارتایی[۱۵] کلاسیکی که در بر دارندهٔ دوگان خوداند یا خود ـ متعامداند، در ساخت کدهای کوانتومی مورد استفاده قرار بگیرند [۱۲].

---
[۱۰] Steane
[۱۱] Calderbank
[۱۲] dual
[۱۳] Stabilizer formalism
[۱۴] binary
[۱۵] quaternary

این محدودیت، یعنی در بر داشتن دوگان یا خود ـ تعامدی، سد محکمی است که مانع از آن می‌شود که از کدهای کلاسیکی نوینی همچون کدهای توربو[۱۶] و کدهای $LDPC$[۱۷] که کارایی بالایی دارند، در ساخت کدهای کوانتومی استفاده شود. در راستای برطرف کردن این محدودیت، نظریهٔ کدهای تصحیحگر خطای کوانتومی «درهمتنیدگی ـ یاور»[۱۸] توسعه یافته‌اند [۱۳، ۱۴، ۱۵]. این نظریه تعمیمی از نظریهٔ کدهای پایدارساز است و امکان ساخت کدهای کوانتومی را از طریق هر نوع کد کلاسیکی فراهم می‌سازد [۱۶].

در ادامهٔ پیشرفت مبحث نظریهٔ کدگذاری، اخیراً نظریهٔ «کدهای تصحیحگر خطای کوانتومی عملگری» ارائه شده است [۱۷—۲۴] که آمیزه‌ای از طرح‌های «اجتناب ـ خطا»[۱۹] همچون «زیرفضاهای بی‌واهمدوسی»[۲۰] و «زیرسیستم‌های بی‌نوفه» و نظریهٔ معمول تصحیح خطای کوانتومی است. هرچند نظریهٔ کدهای کوانتومی عملگری به ساخت کدهای کوانتومی جدیدی نمی‌انجامد، اما در عوض روش کدگشایی تازه‌ای را فراهم می‌آورد که «آستانهٔ خطا»[۲۱]ی محاسبات کوانتومی را بهبود می‌بخشد [۱۸].

علاوه بر کدهای کوانتومی پایدارساز دوتایی، کدهای پایدارساز غیر دوتایی نیز مطالعه شده است و برای سیستم‌های کوانتومی که بُعد آنها توانی از یک عدد اول است، کدهای کوانتومی خوب بسیاری ساخته شده است [۲۵—۳۱]. با این حال، این زمینه هنوز نوپا بوده و مسائل حل نشدهٔ زیادی را پیش روی خود دارد.

درهمتنیدگی از شگفت انگیزترین پدیده‌های کوانتومی است که در بسیاری از فرایندهای محاسبات و اطلاعات کوانتومی نقش اساسی دارد [۳۲، ۳۳، ۳۴]. از اینرو، تشخیص حالت‌های کوانتومی درهمتنیده از حالت‌های کوانتومی جداپذیر از مسائل مهم حوزهٔ اطلاعات کوانتومی است. یکی از رهیافت‌های این مسئله به کارگیری شاهدهای درهمتنیدگی کوانتومی است [۳۵]-[۴۰]. برای ساختن شاهدهای درهمتنیدگی کوانتومی، روش بهینه سازی محدب و روش برنامه ریزی خطی از روش‌هایی هستند که اخیراً مورد توجه قرار گرفته‌اند [۴۱—۴۶].

---

[۱۶] Turbo
[۱۷] Low-Density Parity Check
[۱۸] Entanglement-assisted
[۱۹] error-avoiding
[۲۰] decoherence-free
[۲۱] error threshold

فصل ۲

مبانی و روش ها

۱.۲ جبر نیم ـ ساده

پیش از پرداختن به تعریف جبر نیم ـ ساده، مفاهیم گروه، میدان، فضای برداری و جبر را که در این تعریف دخیل اند معرفی می‌کنیم.

- گروه G عبارت است از یک مجموعهٔ G همراه با یک قانون ترکیب که آن را عمل ضرب می‌نامیم به گونه‌ای که

  ۱– به ازای هر دو عضو g و h از G، حاصلضرب gh عضوی از G است،

  ۲– G دارای عضو همانی مانند e است به طوری که به ازای هر g از G داریم

$$eg = ge = g$$

  ۳– به ازای هر g از G، عضو وارون $g^{-۱}$ از G وجود دارد به طوری که

$$gg^{-۱} = g^{-۱}g = e$$

  ۴– عمل ضرب شرکت‌پذیر است، یعنی به ازای هر g، h و k از G داریم

$$(gh)k = g(hk).$$

  هرگاه به ازای هر دو عضو g و h از گروه G، تساوی $gh = hg$ برقرار باشد گروه G را «آبلی» می‌نامند. اگر تعداد اعضای گروه G متناهی باشد، G را «گروه متناهی» و تعداد اعضای آن $|G|$ را مرتبهٔ G می‌نامند.

- میدان $\mathbb{F}$ عبارت است از یک مجموعهٔ $\mathbb{F}$ همراه با دو قانون ترکیب که آنها را عمل‌های جمع و ضرب می‌نامیم به گونه‌ای که

  ۱– مجموعهٔ $\mathbb{F}$ همراه با عمل جمع، یک گروه آبلی است.

  ۲– اعضای غیر صفر $\mathbb{F}$ همراه با عمل ضرب، یک گروه آبلی است.

  ۳– عمل ضرب در عمل جمع توزیع‌پذیر است.

- فضای برداری V روی میدان $\mathbb{F}$ عبارت است از یک مجموعهٔ V همراه با دو قانون ترکیب به نام‌های عمل جمع و عمل ضرب در اسکالر به گونه‌ای که

  ۱– مجموعهٔ V همراه با عمل جمع، یک گروه آبلی است،

۲– به ازای هر u و v از V و هر λ و μ از $\mathbb{F}$ داریم

$$\lambda(u+v)=\lambda u+\lambda v, \quad (\lambda+\mu)u=\lambda u+\mu u, \quad (\lambda\mu)u=\lambda(\mu u), \quad 1u=u.$$

فضای برداری V را «تقلیل‌ناپذیر» می‌گویند اگر خود V و فضای برداری صفر تنها زیرفضاهای برداری آن باشند. در غیر این صورت، آن را «تقلیل‌پذیر» می‌گویند. فضای برداری V را «کاملاً تقلیل‌پذیر» یا «نیم ـ ساده» می‌گویند اگر جمع مستقیم زیرفضاهای ناوردا باشد.

- جبر A عبارت است از یک فضای برداری A روی میدان $\mathbb{F}$ که مجهز به قانون ترکیبی به نام عمل ضرب است به گونه‌ای که به ازای هر a، b و c از A و هر λ از $\mathbb{F}$ داریم

$$a(bc)=(ab)c, \quad a(b+c)=ab+ac, \quad (a+b)c=ac+bc, \quad \lambda(ab)=(\lambda a)b=a(\lambda b).$$

اینک آماده‌ایم تا جبر نیم ـ ساده را تعریف کنیم. جبر نیم ـ ساده به جبری گفته می شود که به عنوان فضای برداری کاملاً تقلیل‌پذیر باشد. گروه‌جبر[1] یک گروه متناهی G نمونه‌ای از جبرهای نیم ـ ساده است [۴۷]. فرض کنید $\mathbb{F}$ یک میدان و g_1، ...، g_n اعضای گروه متناهی G باشند. گروه‌جبر G که آن را با نماد $\mathbb{F}G$ نشان می‌دهند، فضایی برداری روی میدان $\mathbb{F}$ است که پایهٔ آن مجموعهٔ اعضای گروه G و عمل ضرب تعریف شده در آن مبتنی بر ضرب اعضای گروه G است. اعضای $\mathbb{F}G$ به شکل زیر اند

$$\sum_{i=1}^{n}\lambda_i g_i, \quad \forall\lambda_i\in\mathbb{F}.$$

به ازای هر دو عضو $u=\sum_{i=1}^{n}\lambda_i g_i$ و $v=\sum_{j=1}^{n}\mu_j g_j$ از $\mathbb{F}G$ و هر $\lambda\in\mathbb{F}$، تعریف عمل‌های جمع، ضرب در اسکالر و ضرب به شکل زیر است

$$u+v=\sum_{k=1}^{n}(\lambda_k+\mu_k)g_k, \quad \lambda u=\sum_{i=1}^{n}(\lambda\lambda_i)g_i, \quad uv=\sum_{i,j=1}^{n}(\lambda_i\mu_j)g_ig_j.$$

از جبرهای نیم ـ سادهٔ دیگر می توان به جبر جابه‌جایی بوز ـ مزنر[2] و جبر ناجابه‌جایی ترویلیجر[3] وابسته به یک شمای همبسته [4] اشاره کرد که موضوع بحث بخش بعدی است.

[1] group algebra
[2] Bose-Mesner
[3] Terwilliger
[4] association-scheme

۲.۲ شمای همبسته و جبرهای نیم ـ سادهٔ وابسته به آن

یک شِمای همبستهٔ متقارن از ردهٔ d عبارت است از جفت $(X, \{R_i\}_{i=0}^{d})$ متشکل از مجموعهٔ متناهی X و رابطه‌های ناتهی R_i روی آن به گونه‌ای که :

۱ـ مجموعهٔ این رابطه‌ها افرازی از $X \times X$ است،

۲ـ $R_0 = \{(\alpha, \alpha) : \alpha \in X\}$،

۳ـ به ازای $i = 0, 1, ..., d$، $R_i = R_i^t$ که بنا به تعریف $R_i^t = \{(\beta, \alpha) : (\alpha, \beta) \in R_i\}$،

۴ـ به ازای هر $(\alpha, \beta) \in R_k$، تعداد γ های واقع در X به نحوی که جفت (α, γ) در R_i و جفت (γ, β) در R_j واقع باشد مستقل از (α, β) بوده و فقط به k، i و j وابسته است. این تعداد را با p_{ij}^k نشان می دهند.

اعداد p_{ij}^k را عددهای تقاطعی[5] و d را قطر شِمای همبسته می نامند [۴۸، ۴۹، ۵۰].

یکی از شِماهای همبستهٔ معروف، شِمای همینگ[6] است که در مبحث کدها اهمیت ویژه‌ای دارد. شِمای همینگ را در بخش ۷.۲ معرفی می‌کنیم. گروه‌ها از جمله منابع شِماهای همبسته می‌باشند. چنانچه گروه G روی مجموعهٔ X به صورت ترایا اثر کند، اثر آن روی مجموعهٔ $X \times X$ به طور طبیعی تعریف می‌شود. در این صورت، مجموعهٔ مدارهای حاصل از اثر گروه روی $X \times X$ رابطه‌های یک شِمای همبسته را تعریف می‌کنند.

۱.۲.۲ جبر بوز ـ مزنر

از جمله راه‌های مطالعهٔ ساختار یک شِمای همبسته استفاده از جبر ماتریسی است. در این روش، هر رابطهٔ R_i از شِمای همبستهٔ متقارن $Y = (X, \{R_i\}_{i=0}^{d})$ را با یک ماتریس متقارن A_i نمایش می‌دهند. A_i را ماتریس همسایگی i ام Y نامیده به صورت زیر تعریف می‌کنند

$$(A_i)_{\alpha,\beta} = \begin{cases} 1 & if\ (\alpha,\beta)\in R_i \\ 0 & otherwise \end{cases} \tag{۱.۲}$$

برحسب ماتریس‌های A_i، چهارمین ویژگی شِمای همبسته را می‌توان چنین نوشت

$$A_i A_j = \sum_{i=0}^{d} p_{ij}^k A_k.$$

[5] intersection numbers
[6] Hamming-scheme

می‌توان دید که ماتریس‌های متقارن $A_0, A_1, ..., A_d$ پایه‌ای برای یک جبر جابه‌جایی مختلط M، معروف به جبر بوز ـ مزنر، می‌سازند. جبر M پایه دیگری متشکل از ماتریس‌های خودتوان $E_0, E_1, ..., E_d$ دارد به‌گونه‌ای که $E_0 = \frac{1}{|X|}J$ ، $E_iE_j = \delta_{ij}E_i$ و $\sum_{i=0}^{d} E_i = I$. در اینجا، J یک ماتریس مربعی است که تمام درایه‌های آن ۱ است. این دو پایه با ماتریس‌های حقیقی P و Q، معروف به ویژه‌ماتریس اول و ویژه‌ماتریس دوم شِمای همبسته، به یکدیگر تبدیلپذیرند

$$A_i = \sum_{i=0}^{d} P_{ji}E_j, \quad E_i = \frac{1}{|X|}\sum_{i=0}^{d} Q_{ji}A_j, \quad i = 0, 1, ..., d. \tag{۲.۲}$$

این دو معادلهٔ تبدیل نشان می‌دهد که

$$PQ = QP = |X|I, \quad A_jE_i = P_{ij}E_i.$$

از این رو P_{ij} ویژه‌مقدار i ام A_j است.

۲.۲.۲ جبر بوز ـ مزنر دوگان و جبر ترویلیجر

به هر شِمای همبستهٔ Y یک جبر جابه‌جایی به نام دوگان بوز ـ مزنر نیز وابسته است. جبر دوگان نسبت به یک عضو مرجع از X تعریف می‌شود. برای یک عضو معین α از X و به ازای $i = 0, 1, ..., d$، ماتریس‌های قطری E_i^* را به صورت زیر تعریف می‌کنند

$$(E_i^*)_{\beta,\beta} = \begin{cases} 1 & if\ (\alpha,\beta)\in R_i \\ 0 & otherwise \end{cases} \tag{۳.۲}$$

از این تعریف پیدا است که

$$\sum_{i=0}^{d} E_i^* = I, \quad E_i^*E_j^* = \delta_{ij}E_i^*, \quad i,j = 0, 1, ..., d.$$

دیده می‌شود که ماتریس‌های قطری $E_0^*, E_1^*, ..., E_d^*$ پایه‌ای برای یک جبر جابه‌جایی مختلط M^*، معروف به جبر بوز ـ مزنر دوگان، می‌سازند.

برای یک عضو معین α از X، جبر بوز ـ مزنر و دوگان آن یک جبر نیم ـ سادهٔ ناجابه‌جایی تولید می‌کنند که جبر ترویلیجر شِمای همبستهٔ Y نسبت به عضو α نامیده می‌شود.