بسم الله الرحمن الرحیم

فرهنگ و اندیشهٔ ریاضی

ISSN 1022-6443

سال ۲۱، شمارهٔ ۱، بهار ۱۳۸۱
شمارهٔ پیاپی: ۲۸

نشانی:
تهران ــ صندوق پستی ۴۱۸ـ۱۳۱۴۵
iranmath@ims.ir
http://www.ims.ir

فرهنگ و اندیشهٔ ریاضی نشریهٔ علمی-ترویجیِ انجمن ریاضی ایران است که به چاپ و انتشارِ مطالبی می‌پردازد که هم جنبه‌های عام و فلسفیِ ریاضیات را ترویج دهند و هم بازگوکنندهٔ فرهنگ و روندِ ریاضیاتِ حاکم بر جامعهٔ ریاضی باشند. فرهنگ و اندیشهٔ ریاضی از مقالات در زمینه‌های ریاضیات محض، ریاضیات کاربردی، علومِ کامپیوتر، فیزیک نظری، وکاربردهای ریاضیات در علومِ دیگر که در چارچوب زیر نوشته شده باشند استقبال می‌کند:

• ارائهٔ موضوعیْ فعال و مطرح در ریاضیات در قالبی که علاقه‌مندان به زمینه‌های پژوهشی را برای پیگیریِ موضوعِ مورد بحث آماده سازد؛
• ترجمهٔ مقاله‌هایی از نوع یاد شده در بالا یا ترجمهٔ مقالاتِ کلاسیکِ ریاضی (ترجمهٔ آزاد پذیرفته نمی‌شود)؛
• ارائهٔ موضوعاتِ آموزشی حاوی نکات و قضایا و برهانهایی ساده‌تر از آنچه در متونِ کلاسیک موجود است.

علاقه‌مندان می‌توانند سه نسخه از مقالهٔ خود را با شرایطِ زیر به نشانی دفتر مجله ارسال دارند:

• متن مقاله روی یک طرف کاغذ، یک خط در میان، و با حاشیهٔ کافیْ تایپ شده یا ترجیحاً، در دیسکتِ کامپیوتری تحت ادیتورِ «TEX-پرشین» یا «فارسی‌تک» باشد.
• فرستادنِ اصلِ مقالهٔ ترجمه شده ــ با ذکر نشانیِ کاملِ آن ــ لازم است.
• اصطلاحاتِ ریاضیِ به‌کار رفته باید بر طبقِ واژه‌نامهٔ ریاضی و آمارِ انجمن ریاضی ایران باشد و اگر لغتی در این واژه‌نامه نیست، معادلِ انگلیسیِ آن داده شود. در صورتی که مؤلف یا مترجم معتقد است اصطلاحِ خاصی از واژه‌نامه مناسب نیست باید ترجیح دادنِ اصطلاحِ پیشنهادیِ خود را توجیه کند.
هیأت تحریریه در رد، قبول، حک، و اصلاحِ مقالاتْ آزاد است و ملزم به ارایه دلایل توجیهی نیست.
• مقالات ارسالی به فرهنگ و اندیشهٔ ریاضی نباید برای بررسی و چاپ به مجلات دیگر ارسال شده باشد.

فرهنگ و اندیشهٔ ریاضی

سال ۲۱، شمارهٔ ۱، بهار ۱۳۸۱
(تاریخ انتشار: پاییز ۱۳۸۲)
شمارهٔ پیاپی: ۲۸

فهرست مطالب

روی جلد: فلیکس کلین (Felix Klein)

فرهنگ و اندیشهٔ ریاضی هر سال در دو شماره (بهار و پاییز) منتشر و به اعضای حقیقی، حقوقی و مشترکین انجمن ریاضیِ ایران ارسال می‌شود.

علاقه‌مندان به عضویت حقیقی و دانشگاه‌ها، مؤسسات وکتابخانه‌هاکه تمایل به عضویت حقوقی یا اشتراک سالانه دارند می‌توانند با دبیرخانهٔ انجمن ریاضی ایران تماس حاصل نمایند.

شماره‌های قبلی این مجله با هماهنگی دبیرخانه قابل فروش می‌باشند.

فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۸ (بهار ۱۳۸۱)، صص. ۱ تا ۲۵

الگوریتمهایی برای محاسبه بزرگترین مقسوم‌علیه مشترک و کاربرد آنها در حل تک‌معادلات دیوفانتی خطی

حمید اسمعیلی و نظام‌الدین مهدوی امیری

چکیده

یکی از مراحل مهم در حل دستگاههای دیوفانتی (صحیح) خطی، محاسبه بزرگترین مقسوم علیه مشترک چند عدد صحیح است. الگوریتم اقلیدس اغلب به عنوان یکی از الگوریتمهای مؤثر برای محاسبهٔ بزرگترین مقسوم علیه مشترک دو عدد صحیح استفاده می‌شود. با ادغام الگوریتم اقلیدس با یک روند تکراری می‌توان آن را برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح نیز به کار برد. یکی از پدیده‌های نامطلوب کار با اعداد صحیح، رشد سریع اعداد است که در عمل می‌تواند حتی برای کامپیوترهای بزرگ نیز مشکل آفرین باشد. از این رو، تهیه و به کارگیری الگوریتمهایی که از رشد سریع نتایج میانی جلوگیری کنند، مهم است.

در این مقاله به بررسی چند الگوریتم برای محاسبهٔ بزرگترین مقسوم علیه مشترک شماری متناهی از اعداد صحیح همراه با چگونگی محاسبهٔ جواب عمومی تک معادله‌های دیوفانتی خطی می‌پردازیم. این الگوریتمها عبارتند از: الگوریتم بلانکین‌شیپ، الگوریتم برادلی، الگوریتم راسر، الگوریتم کرتزنر و الگوریتم موریتو-سالکین. نشان می‌دهیم که همهٔ این الگوریتمها را می‌توان بر حسب الگوریتم بلانکین‌شیپ، که خود پیرایشی از الگوریتم اقلیدس

است، بیان کرد. در این صورت خواهیم دید که این الگوریتمها تنها در چند مرحلهٔ جزئی از یکدیگر متمایز می‌شوند. سپس یک الگوریتم نیز برای محاسبهٔ بزرگترین مقسوم علیه مشترک اعداد صحیح ارائه می‌کنیم. سرانجام همهٔ این الگوریتمها را پیاده‌سازی و برنامه‌های تولید شده را با یک مسالهٔ نمونه آزمون می‌کنیم. به عنوان یک مقایسه، عملکرد برنامه‌ها را، از نقطه نظر بزرگی اعداد ایجاد شده در جواب عمومی و نیز زمان اجرا، مورد توجه قرار می‌دهیم.

۱ مقدمه

یکی از مراحل مهم در حل دستگاههای دیوفانتی (صحیح) خطی، محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح است. الگوریتم اقلیدس اغلب به عنوان یکی از الگوریتمهای مؤثر برای محاسبهٔ بزرگترین مقسوم علیه مشترک استفاده می‌شود. با استفاده از این الگوریتم می‌توان بزرگترین مقسوم علیه مشترک دو عدد صحیح a و b، (که در اینجا d نامیده می‌شود)، و اعداد صحیح x و y را چنان یافت که $ax + by = d$. اگر چه الگوریتم اقلیدس طبیعی و منطقی به نظر می‌رسد ولی لِهمر [۲۳] نشان داد که برای کاربردهای خاصی، مانند تهیهٔ جدولی از اعداد اول، می‌توان از روش‌های سریع‌تری استفاده کرد. به دنبال کار لِهمر، کنوث [۲۲] و پس از او شونهاگه [۳۳] الگوریتمهایی سریعتر، ولی از نظر منطقی پیچیده‌تر، برای یافتن بزرگترین مقسوم علیه مشترک دو عدد صحیح ارائه کردند. از الگوریتم اقلیدس می‌توان، علاوه بر تعیین بزرگترین مقسوم علیه مشترک چند عدد صحیح، برای به دست آوردن جواب عمومی تک معادله‌های دیوفانتی خطی نیز استفاده کرد.

الگوریتم اقلیدس را می‌توان به چند طریق به یک الگوریتم برای حل معادلهٔ دیوفانتی زیر تعمیم داد:

$$a_1 x_1 + \cdots + a_n x_n = d$$

این تعمیمها اساساً به ساختن یک ماتریس تک مدولی مانند M (یک ماتریس صحیح با قدرمطلق دترمینان برابر با یک) می‌پردازند به طوری که $a^T M = d\, e_1^T$، که در آن d بزرگترین مقسوم علیه مشترک مؤلفه‌های بردار $a = (a_1, \ldots, a_n)^T$ و e_1 ستون اول ماتریس همانی است. در این صورت، ستون اول ماتریس M یک جواب خاص برای معادلهٔ فوق است و بقیهٔ ستونهای M پایه‌ای برای فضای جوابهای صحیح معادلهٔ همگن متناظر تشکیل می‌دهند (بخش ۳ را ملاحظه کنید). از نقطه نظر محاسباتی خیلی مهم است که قدر مطلق عناصر ماتریس M کوچک باشند (به طور نظری ثابت شده است که ماتریسهای M با درایه‌های کوچک، از لحاظ قدر مطلق، وجود دارند). الگوریتمهایی وجود دارند که کوچک بودن مؤلفه‌های جواب خاص، ستون اول ماتریس M، را تضمین می‌کنند، بدین معنی که

$$\| Me_1 \|_\infty \leq \| a \|_\infty .$$

به هر حال، سایر عناصر ماتریس M می‌توانند به سرعت بزرگ شوند. تنها کران به دست آمده از الگوریتمها،

برای ساختن M، عبارت است از:

$$|M| \leq \| a \|_{\infty}^{3},$$

که در آن $|M|$ نشان دهنده بزرگترین درایهٔ ماتریس M از لحاظ قدر مطلق است. یکی از پدیده‌های نامطلوب کار با اعداد صحیح، رشد سریع اعداد است که در عمل می‌تواند حتی برای کامپیوترهای بزرگ نیز مشکل آفرین باشد [۹،۲۵]. از این رو تهیه و به کارگیری الگوریتمهایی که از رشد سریع نتایج میانی جلوگیری کنند، مهم است.

می‌دانیم که کامپیوتر امکان تحقیق درستی بعضی از قضایای نظریهٔ اعداد را فراهم ساخته است. در واقع کامپیوتر ابزار تجربی قدرتمندی برای نظریهٔ اعداد است. در این ارتباطِ بین کامپیوتر و نظریهٔ اعداد، چند مفهوم اساسی و بنیادی بروز می‌کنند. به طور دقیقتر، مسالهٔ پیچیدگی الگوریتمها باعث می‌شود تا مسایل کلاسیک نظریهٔ اعداد را از یک زاویهٔ جدید بنگریم که نتیجتاً مسایل تازه‌ای مطرح می‌شوند. مسالهٔ پیچیدگی الگوریتم چندان بر وجود الگوریتمهای حل برای مسایل معینی از نظریهٔ اعداد متمرکز نیست، بلکه بیشتر به کارایی الگوریتمها توجه دارد. در واقع، نارسایی اکثر الگوریتمها در نظریهٔ اعداد به خاطر یکی از دو دلیل زیر است: اولاً، با وجود اینکه بعضی از مسایل مشخص را می‌توان با استفاده از تعداد کمی از تکرارها حل کرد، ولی در دنبالهٔ تکرارها اعداد به قدری سریع رشد می‌کنند که تعداد ارقام به طور نمایی افزایش می‌یابد. این وضعیت در مواردی همچون تقلیل ماتریسهای صحیح به فرم نرمال هرمیت، یافتن مینیمم یک فرم درجهٔ دو با استفاده از اصل هرمیت و محاسبهٔ مقسوم علیه مشترک چند جمله‌ایها با تعداد زیادی از متغیرها، رخ می‌دهد. ثانیاً، در هندسهٔ اعداد یک سری از قضیه‌های «غیر سازنده»، مانند قضیه‌های وجودی، وجود دارند که، اگر چه تهیه الگوریتمها را ممکن می‌سازند، ولی الگوریتمهایی به دست می‌دهند که بررسی تمام نقاط صحیح در یک ناحیهٔ کراندار را ایجاب می‌کنند. از جملهٔ چنین قضیه‌هایی می‌توان به قضیهٔ لاگرانژ درباره متناوب بودن بسط به کسر مسلسل یک عدد اصم که در یک معادلهٔ درجه دو صدق می‌کند، اصل لانه کبوتری دیریکله، و قضیه مینکوفسکی برای یک ساختار محدب، اشاره کرد [۱۲].

اهمیت محاسبهٔ کارای بزرگترین مقسوم علیه مشترک و در نتیجه حل یک معادلهٔ دیوفانتی خطی به واسطهٔ کاربردهای فراوان آن است. یکی از مهمترین کاربردهای بزرگترین مقسوم علیه مشترک در حل دستگاههای دیوفانتی خطی است. تقریباً در هر الگوریتم برای حل یک دستگاه معادلات دیوفانتی محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح ظاهر می‌شود [۹،۱۳،۱۴،۱۵،۳۵].

در حل دستگاههای دیوفانتی و مسایل برنامه ریزی با اعداد صحیح فرمهای ویژه‌ای به نامهای فرم نرمال هرمیت و فرم نرمال اسمیت برای یک ماتریس صحیح کاربردهای فراوان یافته‌اند، مثلاً در تبدیل یک مسالهٔ برنامه‌ریزی خطی صحیح به یک مسالهٔ کوله‌پشتی گروهی [۱۸]، و در تعیین فرم کانونی ردهٔ مسایل برنامه‌ریزی صحیح [۵،۸]. درکلیهٔ الگوریتمهای محاسبه فرم نرمال هرمیت یا فرم نرمال اسمیت [۷،۹،۱۳،۱۶،۱۸،۲۰] محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح ظاهر می‌شود. کارایی این

الگوریتمها به چگونگی محاسبهٔ بزرگترین مقسوم علیه مشترک بستگی دارد. چند کاربرد دیگر بزرگترین مقسوم علیه مشترک را می‌توان در [۳۶،۱۹،۱۷،۱۶] یافت.

در این مقاله به بررسی چند الگوریتم برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح، و در نتیجه تعیین جواب عمومی برای تک معادله‌های دیوفانتی خطی، می‌پردازیم. این الگوریتمها عبارتند از: الگوریتم بلانکین‌شیپ، الگوریتم برادلی، الگوریتم راسر، الگوریتم کرتزنر و الگوریتم موریتو-سالکین. همهٔ این الگوریتمها را می‌توان بر حسب الگوریتم بلانکین‌شیپ، که خود پیرایشی از الگوریتم اقلیدس است، بیان کرد. در این صورت خواهیم دید که این الگوریتمها تنها در چند مرحلهٔ جزیی با هم اختلاف دارند. به علاوه، یک الگوریتم نیز برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح ارائه می‌کنیم. پیاده سازی همهٔ این الگوریتمها را با یک مسالهٔ نمونه آزمون می‌کنیم و به مقایسهٔ عددی این الگوریتمها، از نقطه نظر بزرگی اعداد در جواب عمومی محاسبه شده و زمان اجرا، می‌پردازیم.

بخش ۲ به شرح الگوریتم اقلیدس برای محاسبهٔ بزرگترین مقسوم علیه مشترک دو عدد صحیح می‌پردازد. در بخش ۳، ارتباط میان ماتریسهای تک مدولی و جواب عمومی یک تک معادلهٔ دیوفانتی خطی بیان می‌شود. در بخش ۴، به بیان الگوریتمهایی چند برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح می‌پردازیم. در بخش ۵، پیاده سازی این الگوریتمها را از نقطه نظر بزرگی اعداد در جواب عمومی محاسبه شده و زمان اجرا مقایسه می‌کنیم. نتیجه‌گیری در بخش ۶ آمده است.

۲ بزرگترین مقسوم‌علیه مشترک دو عدد صحیح و الگوریتم اقلیدس

فرض کنید u و v دو عدد صحیح باشند. اگر به ازای عددی صحیح مانند w داشته باشیم $u = wv$، آنگاه گوییم v عدد u را عاد می‌کند و می‌نویسیم $v|u$، در غیر این صورت گوییم v عدد u را عاد نمی‌کند و می‌نویسیم $v \not| u$. حال فرض کنید u و v اعداد صحیحی باشند که هر دو با هم صفر نیستند. بزرگترین مقسوم علیه مشترک u و v، که با $gcd(u,v)$ نشان می‌دهیم، بزرگترین عدد صحیح مثبتی است که هر دوی u و v را عاد می‌کند. این تعریف با معنی است چون اگر $u \neq 0$ آنگاه هیچ عدد صحیح بزرگتر از $|u|$ نمی‌تواند u را عاد کند، در حالی که ۱ هر دوی u و v را عاد می‌کند. بنابراین باید یک بزرگترین عدد صحیح مثبت وجود داشته باشد به طوری که هر دوی آنها را عاد کند. توجه داریم که اگر u و v هر دو صفر باشند آنگاه هر عدد صحیح آنها را عاد می‌کند و در این حالت تعریف بالا بی‌معنی است. پس قرار می‌دهیم:

$$gcd(0,0) = 0. \qquad (1)$$

تعریف بالا بلافاصله نتیجه می‌دهد:

$$gcd(u,v) = gcd(v,u), \tag{۲}$$

$$gcd(u,v) = gcd(-u,v), \tag{۳}$$

$$gcd(u,۰) = |u|. \tag{۴}$$

کوچکترین مضرب مشترک دو عدد صحیح u و v، $lcm(u,v)$، کوچکترین عدد صحیح مثبتی است که توسط u و v عاد می‌شود. در این تعریف نیز قرار می‌دهیم: $lcm(۰,۰) = ۰$.

بنا بر «قضیهٔ اساسی حساب» هر عدد صحیح مثبت مانند u را می‌توان به صورت

$$u = ۲^{u_۲}۳^{u_۳}۵^{u_۵}۷^{u_۷}۱۱^{u_{۱۱}}\dots \tag{۵}$$

به حاصلضرب عاملهای اول تجزیه کرد. در این تجزیه $u_۲$، $u_۳$، ... اعداد صحیح نامنفی هستند که به طور یکتا تعیین می‌شوند و همه غیر از تعدادی متناهی از آنها صفرند. از این تجزیه به سادگی می‌توان یک روش برای محاسبهٔ بزرگترین مقسوم علیه مشترک و کوچکترین مضرب مشترک اعداد صحیح u و v به دست آورد [۳۰،۲۲]. بنا بر (۲)، (۳) و (۴) می‌توان فرض کرد که u و v مثبت هستند. با تجزیهٔ u و v به صورت (۵) خواهیم داشت:

$$gcd(u,v) = ۲^{min(u_۲,v_۲)}۳^{min(u_۳,v_۳)}۵^{min(u_۵,v_۵)}\dots, \tag{۶}$$

$$lcm(u,v) = ۲^{max(u_۲,v_۲)}۳^{max(u_۳,v_۳)}۵^{max(u_۵,v_۵)}\dots. \tag{۷}$$

به عنوان مثال، بزرگترین مقسوم علیه مشترک $u = ۷۰۰۰ = ۲^۳۵^۳۷$ و $v = ۴۴۰۰ = ۲^۴۵^۲۱۱$ برابر است با $۲^{min(۳,۴)}۵^{min(۳,۲)}۷^{min(۱,۰)}۱۱^{min(۰,۱)} = ۲۰۰$. کوچکترین مضرب مشترک آنها برابر است با ۱۵۴۰۰۰.

روابط زیر را می‌توان از فرمولهای (۶) و (۷) نتیجه گرفت:

$$gcd(u,v)w = gcd(uw,vw), \qquad w \geq ۰, \tag{۸}$$

$$lcm(u,v)w = lcm(uw,vw), \qquad w \geq ۰, \tag{۹}$$

$$uv = gcd(u,v)lcm(u,v), \qquad u,v \geq ۰, \tag{۱۰}$$

$$gcd(lcm(u,v),lcm(u,w)) = lcm(u,gcd(v,w)), \tag{۱۱}$$

$$lcm(gcd(u,v),gcd(u,w)) = gcd(u,lcm(v,w)). \tag{۱۲}$$

دو قاعدهٔ آخر مشابه قواعد توزیع پذیری هستند. قاعدهٔ (۱۰) محاسبهٔ کوچکترین مضرب مشترک دو عدد صحیح را به محاسبهٔ بزرگترین مقسوم علیه مشترک آنها تبدیل می‌کند.

هر چند که (۶) از دیدگاه نظری سودمند است ولی برای محاسبهٔ بزرگترین مقسوم علیه مشترک هیچ استفادهٔ عملی ندارد، زیرا برای این منظور ابتدا باید تجزیهٔ اعداد صحیح u و v به عاملهای اول را به دست آورد. توجه داریم که هیچ روش شناخته شده‌ای برای تجزیهٔ «سریع» یک عدد صحیح به عاملهای اول وجود ندارد. خوشبختانه یک روش کارا برای محاسبهٔ بزرگترین مقسوم علیه مشترک دو عدد صحیح وجود دارد که نیازی به تجزیهٔ آنها ندارد. این روش که بیش از ۲۲۵۰ سال پیش ابداع شده است، همان «الگوریتم اقلیدس» است. شولارز [۲۲] معتقد است که این روش حتی ۲۰۰ سال پیشتر نیز شناخته شده بوده است. الگوریتم اقلیدس را باید پدر بزرگ تمام الگوریتمها دانست، زیرا قدیمیترین الگوریتم غیر بدیهی است که تا کنون شناخته شده است.

دو عدد صحیح a_1 و a_2 را در نظر بگیرید. توجه کنید:

$$gcd(a_1, a_2) = gcd(-a_1, a_2) = gcd(a_1, -a_2) = gcd(-a_1, -a_2).$$

بنابراین، بدون از دست دادن کلیت، فرض کنید $a_1 > 0$ و $a_1 \geq a_2$. ایدهٔ اساسی الگوریتم اقلیدس برای یافتن $gcd(a_1, a_2)$ این است که اگر q باقیماندهٔ تقسیم a_1 بر a_2 باشد، آنگاه $gcd(a_1, a_2) = gcd(a_2, q)$. بنابراین، الگوریتم اقلیدس را می‌توان به صورت زیر خلاصه کرد ($\lfloor \eta \rfloor$ نشان دهنده بزرگترین عدد صحیح کوچکتر از یا مساوی با η است) [۲۲]:

الگوریتم اقلیدس

(۱) قدمهای (۲) و (۳) را تا وقتی که یکی از a_1 یا a_2 به صفر تقلیل یابد تکرار کن.

(۲) a_1 را با $a_1 - \lfloor \frac{a_1}{a_2} \rfloor a_2$ جایگزین کن.

(۳) a_2 را با $a_2 - \lfloor \frac{a_2}{a_1} \rfloor a_1$ جایگزین کن.

پس از اجرای الگوریتم اقلیدس، عدد غیر صفر a_1 یا a_2 بزرگترین مقسوم علیه مشترک a_1 و a_2 اولیه است. به عنوان مثال $gcd(۴۰۹۰۲, ۲۴۱۴۰)$ به صورت زیر محاسبه می‌شود:

$$\begin{aligned} gcd(۴۰۹۰۲, ۲۴۱۴۰) &= gcd(۲۴۱۴۰, ۱۶۷۶۲) = gcd(۱۶۷۶۲, ۷۳۷۸) \\ &= gcd(۲۰۰۶, ۷۳۷۸) = gcd(۲۰۰۶, ۱۳۶۰) = gcd(۱۳۶۰, ۶۴۶) \\ &= gcd(۶۴۶, ۶۸) = gcd(۶۸, ۳۴) = gcd(۳۴, ۰) = ۳۴. \end{aligned}$$

هر چند که الگوریتم اقلیدس قرنهای متمادی مورد استفاده بوده است ولی این روش همواره بهترین روش برای یافتن بزرگترین مقسوم علیه مشترک نبوده است. یک الگوریتم تقریباً متفاوت برای یافتن بزرگترین مقسوم علیه مشترک، که بر پایه عملیات دودویی است، توسط اشتاین در سال ۱۹۶۱ ارائه شده است [۲۲]. در این الگوریتم به عمل تقسیم نیازی نیست و تنها از عملیاتی چون تفریق، بررسی زوج یا

فرد بودن یک عدد و انتقال نمایش دودویی یک عدد زوج به سمت راست (نصف کردن) استفاده می‌شود. هریس [۲۲] تلفیقی جالب از الگوریتم اقلیدس و الگوریتم دودویی اشتاین ارائه می‌کند.

با کمی تلاش می‌توان اعداد صحیح z_1 و z_2 را یافت به طوری که $a_1z_1 + a_2z_2 = d$ ، $d = gcd(a_1, a_2)$. برای این منظور ابتدا دنباله‌ای از ماتریسهای صحیح ۲×۳ مانند $\{C^{(k)}\}_{k\geq 0}$ به صورت زیر شکل داده می‌شود. ماتریس اولیهٔ $C^{(0)}$ با

$$C^{(0)} = \begin{bmatrix} a_1 & a_2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

مشخص می‌شود. حال فرض کنید $C^{(k)}$ تعیین شده است، مثلاً

$$C^{(k)} = \begin{bmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k \\ \epsilon_k & \eta_k \end{bmatrix}.$$

ماتریس $C^{(k+1)}$ به صورت زیر ساخته می‌شود:

الف) اگر k زوج است و $\beta_k > 0$، آنگاه $[\frac{\alpha_k}{\beta_k}]$ برابر ستون دوم $C^{(k)}$ را از ستون اول آن کم کن.

ب) اگر k فرد است و $\alpha_k > 0$، آنگاه $[\frac{\beta_k}{\alpha_k}]$ برابر ستون اول $C^{(k)}$ را از ستون دوم آن کم کن.

اعمال بالا برای $k = 0, 1, \ldots$ ادامه می‌یابند تا به ازای عدد صحیح $k = N$ داشته باشیم: $\alpha_N = 0$ یا $\beta_N = 0$. اگر $\beta_N = 0$ و $\alpha_N \neq 0$، آنگاه $d = \alpha_N$، زیرا در هر تکرار، بزرگترین مقسوم علیه مشترک درایه‌های سطر اول ماتریس $C^{(k)}$ تغییر نمی‌کند و می‌دانیم $gcd(\alpha_N, 0) = \alpha_N$. به طور مشابه اگر $\alpha_N = 0$ و $\beta_N \neq 0$، آنگاه $d = \beta_N$.

برای یافتن اعداد صحیح مانند z_1 و z_2 به طوری که $a_1z_1 + a_2z_2 = d$، توجه داریم که $(1, -a_1, -a_2)C^{(0)} = (0, 0)$ و بنابراین به ازای هر k داریم $(1, -a_1, -a_2)C^{(k)} = (0, 0)$، زیرا $C^{(k)}$ تنها با انجام تبدیلهای ستونی مقدماتی بر $C^{(k-1)}$، ساخته می‌شود. در نتیجه داریم:

$$a_1\gamma_k + a_2\epsilon_k = \alpha_k, \qquad a_1\delta_k + a_2\eta_k = \beta_k.$$

بنابراین، اگر $\beta_N = 0$ و $\alpha_N \neq 0$، آنگاه

$$a_1\gamma_N + a_2\epsilon_N = \alpha_N = d, \qquad a_1\delta_N + a_2\eta_N = 0.$$

حالت $\alpha_N = 0$ و $\beta_N \neq 0$ را می‌توان به طور مشابه بررسی کرد. به علاوه توجه کنید که به ازای هر k، داریم:

$$-\alpha_k\delta_k + \beta_k\gamma_k = a_2, \qquad \alpha_k\eta_k - \beta_k\epsilon_k = a_1, \qquad \gamma_k\eta_k - \delta_k\epsilon_k = 1,$$

زیرا زیردترمینانهای ۲ × ۲ ماتریسهای $C^{(k)}$ و $C^{(0)}$ برابرند (از آنجا که در تشکیل $C^{(k)}$ تنها از اعمال ستونی مقدماتی استفاده شده است).

توجه: با به کار بردن الگوریتم اقلیدس برای معادلهٔ $۲۰۲۴۳x + ۹۱۵۳y = ۶۹۰۸۴$، جواب $x = ۴۶۳۵۵۳۶۴$، $y = -۱۰۲۵۲۰۶۵۶$ به دست می‌آید. لویت [۲۴] روشی برای حل تک معادله دیوفانتی دو متغیره ارائه کرده است که برای معادلهٔ بالا جواب $x = ۴۵۷۲$، $y = -۱۰۱۰۴$ را به دست می‌دهد. او جواب مینیمال برای یک معادله را تعریف می‌کند و نشان می‌دهد که الگوریتم وی جواب مینیمال را بدست می‌دهد.

در مورد تعداد تکرارهای الگوریتم اقلیدس برای یافتن بزرگترین مقسوم‌علیه مشترک دو عدد صحیح و مثبت a_1 و a_2 که $a_1 \geq a_2$، لامه [۲۲،۶] نشان داد که تعداد تقسیمات لازم در الگوریتم اقلیدس از پنج برابر تعداد ارقام a_2 بیشتر نیست. دیکسون [۱۱] نشان داد که تعداد تکرارهای الگوریتم اقلیدس «همواره تقریباً در حدود» $۱۲\pi^{-2}\log ۲ \log a_1$است. کالینز [۱۰] حداقل و حداکثر زمان اجرای الگوریتم اقلیدس را به عنوان تابعی از طول (تعداد ارقام در نمایش دودویی) a_1، a_2 و d بدست می‌دهد. وی نشان داد که اگر طولهای a_1، a_2 و d، به ترتیب، برابر با m، n و k باشند آنگاه حداقل و حداکثر زمان اجرای الگوریتم اقلیدس، به ترتیب، برابر با $n(m-n+1)+k(n-k+1)$ و $n(m-k+1)$ هستند. می‌توان ثابت کرد که بزرگترین مقسوم علیه مشترک دو عدد صحیح و مثبت a_1 و a_2، $a_1 \geq a_2$، با $O((\log_2 a_1)^3)$ عملیات (دودویی) محاسبه می‌شود [۳۰].

پیچیدگی زمانی، یا به طور ساده پیچیدگی، یک الگوریتم برای حل برخی مسایل عبارت است از حداکثر تعداد اعمال محاسباتی لازم برای حل هر نمونه از آن مساله با یک اندازهٔ معلوم. اندازهٔ یک مساله معمولاً به صورت حداکثر تعداد ارقام دودویی لازم برای کد بندی تمام داده‌های مساله تعریف می‌شود. امروزه شمارش تعداد اعمال محاسباتی، برای اکثر الگوریتمهای شناخته شده، به تنهایی ایده‌آل نیست، بلکه پیچیدگی یک الگوریتم به عنوان تابعی از اندازهٔ آن مساله، وقتی که این اندازه به بینهایت میل می‌کند، مورد نظر است. یک الگوریتم با زمان اجرای چند جمله‌ای یا به طور ساده یک الگوریتم چند جمله‌ای زمانی عبارت است از الگوریتمی که پیچیدگی آن $O(p(s))$ است، که در آن $p(s)$ یک چند جمله‌ای از s، اندازهٔ مساله، است. یک الگوریتم با زمان اجرای نمایی الگوریتمی است که پیچیدگی آن تابعی از هیچ چند جمله‌ای از s نباشد. با توجه به این ملاحظات قضیهٔ زیر در دست است.

قضیهٔ ۱ [۳۴]. الگوریتم اقلیدس یک الگوریتم چند جمله‌ای زمانی است. □

در بخش بعدی، به بیان ارتباط میان ماتریسهای تک مدولی و جواب عمومی یک تک معادلهٔ دیوفانتی خطی می‌پردازیم.

۳ جواب عمومی یک معادله دیوفانتی خطی و ماتریسهای تک‌ـمدولی

در بخش قبلی الگوریتم اقلیدس را برای یافتن بزرگترین مقسوم علیه مشترک دو عدد صحیح بیان کردیم. همچنین دیدیم که برای دو عدد صحیح و مثبت a_1 وa_2 ، با بزرگترین مقسوم علیه مشترک d، می‌توان اعداد صحیح z_1، z_2، h_1 و h_2 را یافت به طوری که دترمینان ماتریس $\begin{bmatrix} z_1 & h_1 \\ z_2 & h_2 \end{bmatrix}$ برابر با $+1$ یا -1 باشد و به علاوه

$$a_1 z_1 + a_2 z_2 = d, \qquad a_1 h_1 + a_2 h_2 = 0 .$$

توجه کنید که به ازای هر عدد صحیح q، اعداد صحیح $x_1 = z_1 + q h_1$ و $x_2 = z_2 + q h_2$ در معادلهٔ دیوفانتی

$$a_1 x_1 + a_2 x_2 = d,$$

صدق می‌کنند. بنابراین، جواب عمومی این معادلهٔ دیوفانتی به صورت

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} + \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} q,$$

است، که در آن q یک عدد صحیح دلخواه است. پس، به بینهایت طریق می‌توان $gcd(a_1, a_2)$ را به صورت یک ترکیب خطی صحیح از a_1 و a_2 بیان نمود. این ملاحظه ما را به تعریف زیر برای جواب عمومی یک تک معادلهٔ دیوفانتی خطی هدایت می‌کند.

تعریف ۱. جواب عمومی، در صورت وجود، برای یک معادلهٔ دیوفانتی خطی $a^T x = b$ ، $x \in \mathbb{Z}^n$، که در آن $a^T = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ و $b \in \mathbb{Z}$، به صورت

$$x = z + U q, \qquad q \in \mathbb{Z}^{n-1}$$

است، که در آن $a^T z = b$، $z \in \mathbb{Z}^n$، و $U \in \mathbb{Z}^{n \times (n-1)}$ یک ماتریس با رتبه $n-1$ است و در $a^T U = 0$ صدق می‌کند. به علاوه، دترمینان ماتریس $(z, U) \in \mathbb{Z}^{n \times n}$ برابر با $+1$ یا -1 است.

اگر a_1،...، a_n اعداد صحیحی باشند که همگی با هم صفر نیستند، آنگاه بزرگترین مقسوم علیه مشترک آنها عبارت است از بزرگترین عدد صحیح مثبت d که تمام اعداد a_1،...، a_n را عاد می‌کند. در این حالت می‌نویسیم $d = gcd(a_1, \ldots, a_n)$. d را می‌توان به صورت یک ترکیب خطی صحیح از اعداد a_1،...، a_n نمایش داد. می‌توان نشان داد که مجموعهٔ ترکیبات خطی صحیح اعداد a_1،...، a_n (یعنی اعدادی به صورت $a_1 x_1 + \cdots + a_n x_n$ که $x_j \in \mathbb{Z}$ برای هر j) عبارت است از مجموعهٔ مضربهای صحیح d [۳۰]. لم زیر مبنایی را برای محاسبهٔ بزرگترین مقسوم علیه مشترک n عدد صحیح ارائه می‌دهد ($n \geq 3$).

لم ۱ [۳۰]. فرض کنید $a_1، \ldots، a_n$ اعداد صحیح باشند. در این صورت

$$gcd(a_1, \ldots, a_n) = gcd(gcd(a_1, a_2), a_3, \ldots, a_n).$$

بنا بر لم بالا، یافتن بزرگترین مقسوم علیه مشترک چند عدد صحیح به یافتن بزرگترین مقسوم علیه مشترک دو عدد صحیح کاهش می‌یابد. اکنون، $n \geq 3$، عدد صحیح a_j، $j = 1, \ldots, n$، و معادلهٔ دیوفانتی

$$a_1 x_1 + \cdots + a_n x_n = b, \qquad (13)$$

را، که در آن $b \in \mathbb{Z}$، در نظر بگیرید. می‌خواهیم معادلهٔ (۱۳) را با استفاده از الگوریتم اقلیدس حل کنیم. برای این منظور، با استفاده از الگوریتم اقلیدس، اعداد صحیح a'_2، z_1 و z_2 را بیابید به طوری که

$$a'_2 = gcd(a_1, a_2) = a_1 z_1 + a_2 z_2. \qquad (14)$$

حال معادلهٔ دیوفانتی خطی با $n-1$ متغیر به صورت

$$a'_2 x'_2 + a_3 x_3 + \cdots + a_n x_n = b, \qquad (15)$$

را در نظر بگیرید. اگر معادلهٔ (۱۵) دارای جواب صحیح نباشد، آنگاه معادلهٔ (۱۳) هم جواب صحیح ندارد. اگر $x'_2، x_3، \ldots، x_n$، یک جواب برای معادلهٔ (۱۵) باشد، آنگاه $x_1 := z_1 x'_2$، $x_2 := z_2 x'_2$، $x_3، \ldots، x_n$ یک جواب برای (۱۳) است. این الگوریتم، که در واقع استفادهٔ مکرر از الگوریتم اقلیدس برای دو عدد است، از یک روند بازگشتی، شامل دو مرحله، برای یافتن بزرگترین مقسوم علیه مشترک چند عدد صحیح و حل معادلهٔ دیوفانتی وابسته استفاده می‌کند. در مرحلهٔ اول، با تقسیمهای متوالی، ابتدا بزرگترین مقسوم علیه مشترک محاسبه می‌شود و در مرحلهٔ دوم، با جایگذاریهای پسرو، جواب معادله تعیین می‌شود. بنابراین، با توجه به قضیهٔ ۱ و مطالب بالا، قضیهٔ زیر نتیجه می‌شود.

قضیهٔ ۲ [۳۴]. یک معادلهٔ دیوفانتی خطی با ضرایب گویا را می‌توان در زمانی چند جمله‌ای حل کرد.

مثال ۱. با استفاده از روش بالا، جواب عمومی معادلهٔ دیوفانتی

$$۵۶۷۷x_1 + ۸۹۱۳x_2 + ۴۳۷۸x_3 = ۱$$

عبارت است از:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} ۷۹۶ \\ -۵۰۷ \\ ۰ \end{bmatrix} + \begin{bmatrix} -۸۹۱۳ & -۳۴۸۴۸۸۸ \\ ۵۶۷۷ & ۲۲۱۹۶۴۶ \\ ۰ & ۱ \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix}, \qquad q_1, q_2 \in \mathbb{Z}.$$

در روش بالا اعداد به همان ترتیب ظهور در معادله بررسی می‌شوند. در واقع، ترتیب اعداد هیچ نقشی در این الگوریتم ندارد. این عدم توجه به ترتیب اعداد می‌تواند باعث رشد سریع نتایج محاسبات شود. در بخش ۴ الگوریتمهایی را بیان می‌کنیم که مستقیماً جواب عمومی یک تک معادلهٔ دیوفانتی را بدست می‌دهند. در این الگوریتمها ترتیب اعداد مهم است. همه این الگوریتمها پیرایشی از الگوریتم اقلیدس هستند و بعضی از آنها برخی از نارساییهای الگوریتم اقلیدس را ندارند.

در ادامهٔ بحث از ماتریسهای تک مدولی مطابق با تعریف زیر استفاده می‌کنیم.

تعریف ۲. یک ماتریس $n \times n$، مانند M، را تک مدولی گوییم هرگاه M یک ماتریس صحیح باشد و $|det\ M| = ۱$.

توجه کنید که اگر M یک ماتریس تک مدولی باشد آنگاه معکوس آن نیز تک مدولی است. در واقع هر ماتریس تک مدولی یک تناظر یک به یک از $\mathbb{Z}^n$ به $\mathbb{Z}^n$ تعریف می‌کند.

قضیهٔ ۳. فرض کنید M یک ماتریس تک مدولی $n \times n$ است. به ازای هر $y \in \mathbb{Z}^n$ یک $x \in \mathbb{Z}^n$ یگانه وجود دارد به طوری که $y = Mx$.

اثبات: فرض کنید $y \in \mathbb{Z}^n$ دلخواه باشد. چون $M^{-۱}$ یکتاست پس، $x = M^{-۱}y$ نیز یکتاست. به علاوه، چون $M^{-۱}$ و y هر دو صحیح هستند، پس x نیز صحیح است. توجه داریم که $y = Mx$. □

قضیهٔ ۴. فرض کنید M یک ماتریس تک مدولی $n \times n$ باشد و $a \in \mathbb{Z}^n$. معادلهٔ دیوفانتی $a^T x = b$، $x \in \mathbb{Z}^n$، را که در آن $b \in \mathbb{Z}$، در نظر بگیرید. قرار دهید $\bar{a} = Ma$. در این صورت

$$\{x \in \mathbb{Z}^n \,|\, a^T x = b\} = \{y \in \mathbb{Z}^n \,|\, \bar{a}^T y = b\}.$$

اثبات: فرض کنید $\tilde{x} \in \mathbb{Z}^n$ در $a^T x = b$ صدق کند. قرار دهید $\tilde{y} = M^{-T}\tilde{x}$. توجه کنید که چون M یک ماتریس تک مدولی است، پس M^{-T} نیز تک مدولی است و بنابراین $\tilde{y}$ و $\tilde{x}$ در تناظر یک به یک هستند. به علاوه،

$$b = a^T\tilde{x} = a^T M^T M^{-T}\tilde{x} = \bar{a}^T\tilde{y},$$

که نشان می‌دهد $\tilde{y}$ یک جواب برای $\bar{a}^T y = b$، $y \in \mathbb{Z}^n$، است.

برعکس، فرض کنید $\tilde{y}$ یک جواب برای $\bar{a}^T y = b$، $y \in \mathbb{Z}^n$، باشد. قرار دهید $\tilde{x} = M^T\tilde{y}$. در این صورت $\tilde{x} \in \mathbb{Z}^n$ و

$$b = \bar{a}^T\tilde{y} = a^T M^T\tilde{y} = a^T\tilde{x}.$$

بنابراین $\tilde{x}$ یک جواب برای $a^T x = b$، $x \in \mathbb{Z}^n$، است. □

توجه: هر ماتریس تک مدولی را می‌توان با دنباله‌ای از اعمال ستونی مقدماتی صحیح به ماتریس همانی تبدیل کرد و برعکس. اعمال ستونی مقدماتی صحیح عبارتند از: (۱) ضرب یک ستون در ۱−، (۲) جا به جا کردن دو ستون، (۳) افزودن مضرب صحیحی از یک ستون به یک ستون دیگر.

قضیهٔ زیر ارتباط بین ماتریسهای تک مدولی و بزرگترین مقسوم علیه مشترک چند عدد صحیح را بیان می‌کند. فرض کنید e_1 بردار یکهٔ اول در $\mathbb{R}^n$ است.

قضیهٔ ۵. فرض کنید $a = (a_1, \ldots, a_n)^T \in \mathbb{Z}^n$ و M یک ماتریس تک مدولی است به طوری که $a^T M = de_1^T$. در این صورت $d = gcd(a)$.

اثبات: چون $a^T M e_1 = d$ پس هر مقسوم علیه مشترک عناصر a یک مقسوم علیه d است. از طرفی دیگر، چون $a^T M = de_1^T$، پس $a^T = de_1^T M^{-1}$، و در نتیجه به ازای هر j، $a_j = d(M^{-1})_{1j}$. بنابراین $d = gcd(a)$. □

توجه: در قضیهٔ بالا (و همچنین در قضیه‌های بعدی)، تنها برای سادگی از e_1 استفاده شده است. همهٔ قضیه‌ها را می‌توان، با تغییراتی جزیی، با حالت کلی e_k (به جای e_1) نوشت.

در قضیهٔ زیر از z برای نشان دادن اولین ستون M و از ماتریس $U \in \mathbb{Z}^{n\times(n-1)}$ برای نشان دادن ماتریس متشکل از بقیهٔ ستونهای M استفاده می‌کنیم ($M = (z, U)$). این قضیه نمایش عمومی تمام بردارهای $x \in \mathbb{Z}^n$ صادق در $a^T x = d$ را، که در آن $d = gcd(a)$، بدست می‌دهد.

قضیهٔ ۶. فرض کنید $a \in \mathbb{Z}^n$ و $d = gcd(a)$. به علاوه فرض کنید به ازای یک ماتریس تک مدولی مانند $M = (z, U)$ داریم: $a^T M = de_1^T$. در این صورت بردار x در معادلهٔ دیوفانتی $a^T x = d$، $x \in \mathbb{Z}^n$، صدق می‌کند اگر و تنها اگر

$$x = z + Uq, \qquad q \in \mathbb{Z}^{n-1}. \tag{۱۶}$$

اثبات: اگر x به صورت (۱۶) باشد، آنگاه به وضوح $x \in \mathbb{Z}^n$ و داریم:

$$a^T x = a^T z + a^T U q = d + 0 = d.$$

بر عکس، فرض کنید $x \in \mathbb{Z}^n$، به طوری که $a^T x = d$. X را ماتریس صحیح $n \times n$ای بگیرید که

ستون اول آن x و سایر ستونهایش صفر هستند. در این صورت

$$a^T(X-M) = a^TX - a^TM = de_1^T - de_1^T = 0.$$

بنابراین $n-1 \leq$ رتبهٔ$(X-M)$. از طرفی دیگر، با توجه به تعریف X، ستونهای دوم، سوم، ...، nام ماتریس $X-M$ مستقل خطی‌اند و در نتیجه $n-1 =$ رتبهٔ$(X-M)$. لذا، برای برخی اعداد حقیقی $r_2, r_3, \ldots, r_n$ داریم $(X-M)e_1 = \sum_{i=2}^{n} r_i(X-M)e_i$ و یا، بنا بر تعریف X، به ازای برخی اعداد حقیقی $q_2, q_3, \ldots, q_n$ داریم $x = z + \sum_{i=2}^{n} q_iMe_i = z + Uq$. با قراردادن $\bar{q} = (1, q_2, \ldots, q_n)^T$ خواهیم داشت $x = M\bar{q}$ و از آنجا $\bar{q} = M^{-1}x$. چون x و M^{-1} صحیح هستند پس $\bar{q}$ و در نتیجه q نیز بردارهای صحیح هستند. □

اکنون که نمایش عمومی تمام جوابهای صحیح معادلهٔ دیوفانتی $a^Tx = d$، $x \in \mathbb{Z}^n$، $d = gcd(a)$، در دست است، می‌توانیم شرایط لازم و کافی، و همچنین در صورت وجود، نمایش عمومی تمام جوابهای صحیح یک معادلهٔ دیوفانتی دلخواه $a^Tx = b$، $x \in \mathbb{Z}^n$، را که در آن $b \in \mathbb{Z}$، بیان کنیم.

قضیهٔ ۷. فرض کنید $a \in \mathbb{Z}^n$ و $d = gcd(a)$. به علاوه فرض کنید که به ازای یک ماتریس تک مدولی مانند $M = (z, U)$ داشته باشیم: $a^TM = de_1^T$. تک معادلهٔ دیوفانتی

$$a^Tx = b, \qquad x \in \mathbb{Z}^n \tag{۱۷}$$

را، که در آن $b \in \mathbb{Z}$، در نظر بگیرید. در این صورت (۱۷) دارای جواب صحیح نیست اگر و تنها اگر $d \nmid b$. اگر $d|b$، آنگاه بردار x در معادلهٔ دیوفانتی (۱۷) صدق می‌کند اگر و تنها اگر

$$x = \frac{b}{d}\, z + Uq, \tag{۱۸}$$

به ازای یک $q \in \mathbb{Z}^{n-1}$.

اثبات: قسمت اول بلافاصله از قضیهٔ ۶ نتیجه می‌شود. حال فرض کنید $d|b$. اگر x به صورت (۱۸) باشد، آنگاه به وضوح $x \in \mathbb{Z}^n$ و $a^Tx = b$، زیرا $a^Tz = d$ و $a^TU = 0$. از طرفی دیگر، فرض کنید $x \in \mathbb{Z}^n$ و $a^Tx = b$. مشابه با اثبات قضیهٔ ۶، X را ماتریسی بگیرید که ستون اول آن x و بقیه ستونها صفر هستند. توجه کنید:

$$a^T(X - \frac{b}{d}M) = a^TX - \frac{b}{d}a^TM = be_1^T - be_1^T = 0.$$

بنابراین، همانند اثبات قضیهٔ ۶، می‌توان نشان داد که x به صورت (۱۸) است. □

در بخش بعدی الگوریتمهایی را برای محاسبه ماتریس تک مدولی M، آمده در قضیهٔ ۷، بیان می‌کنیم.

۴ الگوریتمهایی برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح

الگوریتمهایی که در زیر شرح داده می‌شوند بر قضیه‌های بخش قبلی مبتنی هستند. این الگوریتمها برای محاسبه $gcd(a)$، یک ماتریس تک مدولی M می‌سازند که در قضیهٔ ۷ صدق می‌کند. ابتدا از ماتریس $(a \ , \ I)^T$ شروع می‌کنیم و با اعمالی شبیه الگوریتم اقلیدس، سطر اول این ماتریس را به de_1^T تبدیل می‌کنیم. در این مرحله ماتریس واقع در زیر de_1^T همان ماتریس تک مدولی مطلوب M خواهد بود. الگوریتمهای مورد نظر تنها در چند مرحلهٔ جزیی با هم اختلاف دارند و همهٔ آنها را می‌توان بر حسب الگوریتم بلانکین‌شیپ [۲۹،۲۸،۳،۲،۱] بیان نمود. بنابراین ابتدا الگوریتم بلانکین‌شیپ را بیان می‌کنیم.

برای این منظور تک معادلهٔ دیوفانتی زیر را در نظر بگیرید:

$$a^T x = a_1 x_1 + \cdots + a_n x_n = b.$$

بدون از دست دادن کلیت، فرض کنید $a_1 \geq a_2 \geq \ldots a_n \geq 0$ و $a_1 > 0$. (اگر $a_j < 0$ می‌توان x_j را با $-x_j$ جایگزین نمود. اگر برای برخی $j < i$، $a_j < a_i$، آنگاه می‌توان x_j و x_i را جا به جا کرد. اگر $a_1 = 0$ آنگاه معادله بدیهی است.) الگوریتم بلانکین‌شیپ با ماتریس زیر شروع می‌شود:

$$C = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 0 & \ldots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

فرض کنید c_{ij} نشان دهندهٔ درایهٔ واقع در سطر iام و ستون jام ماتریس C و C_j نشان دهنده ستون jام ماتریس C باشند. در ادامهٔ بحث، منظورمان از یک ستون قابل قبول ماتریس C، ستونی است که مؤلفهٔ اول آن غیر صفر (و بنابراین مثبت) است. در اینجا مراحل الگوریتم بیان می‌شوند.

الگوریتم بلانکین‌شیپ

(۱) قرار ده $C^{(0)} = C$ و $k = 0$.

(۲) ستون عملگر را یک ستون قابل قبول از $C^{(k)}$ با کوچکترین مؤلفه در سطر اول انتخاب کن.

(۳) هر ستون قابل قبول دیگر از $C^{(k)}$ را به عنوان ستون عملوند انتخاب کن. اگر هیچ ستون عملوندی وجود نداشته باشد آنگاه توقف کن.

(۴) یک مضرب صحیح از ستون عملگر را به ستون عملوند اضافه کن تا درایهٔ اول ستون عملوند نامنفی و اکیداً کوچکتر از درایهٔ اول ستون عملگر شود.

(۵) ستونهای $C^{(k)}$ را جا به جا کن به طوری که $c_{11}^{(k)} \geq \cdots \geq c_{1n}^{(k)}$.

(۶) قرار ده $k = k + 1$ و به قدم (۲) برو.

توجه: قدم (۵) در این الگوریتم، و همچنین در الگوریتمهای بعدی، تنها برای سادگی بیان نوشته شده است و البته با تمهیداتی ساختاری می‌توان از اجرای آن صرفنظر کرد. به علاوه، توجه کنید که در الگوریتم بالا ستون عملگر در واقع سمت راست‌ترین ستون قابل قبول در ماتریس $C^{(k)}$ است.

در الگوریتم بلانکین‌شیپ برای انتخاب یک ستون عملوند هیچ قاعده‌ای وجود ندارد. بلانکین‌شیپ انتخاب ستون با کوچکترین مؤلفهٔ غیر صفر بعدی در سطر اول (یعنی ستون ماقبل ستون عملگر) را، به عنوان ستون عملوند، پیشنهاد می‌کند. بنابراین، ستون عملوند فعلی، ستون عملگر بعدی است و ستون عملگر فعلی، ستون عملوند بعدی است. این قاعده برای انتخاب ستون عملوند، در الگوریتم بلانکین‌شیپ اصلاح شده رعایت می‌شود.

مثال ۲. الگوریتم بلانکین‌شیپ اصلاح شده جواب عمومی زیر را برای معادلهٔ دیوفانتی مثال ۱ بدست می‌دهد:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1429 \\ 0 \\ 1853 \end{bmatrix} + \begin{bmatrix} 4378 & 127366771 \\ 0 & 1 \\ -5677 & -165157891 \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix}, \quad q_1, q_2 \in \mathbb{Z}.$$

واینشتاک [۳۷] به روش ساختاری نشان داد که عدد صحیح d بزرگترین مقسوم علیه مشترک اعداد $a_1, \ldots, a_n$ است اگر و تنها اگر d کوچکترین عدد صحیح مثبتی باشد که تک معادلهٔ دیوفانتی $a_1x_1 + \cdots + a_nx_n = d$ دارای جواب (صحیح) باشد. با تکیه بر این اثبات ساختاری، وی یک الگوریتم برای حل تک معادلهٔ دیوفانتی $a_1x_1 + \cdots + a_nx_n = b$، $b \in \mathbb{Z}$، ارائه می‌کند که تنها قادر به یافتن یک جواب است. توجه داریم که اگر اعداد صحیح $x_1, \ldots, x_n$ به گونه‌ای باشند که $0 < a_1x_1 + \cdots + a_nx_n = s \neq d$، آنگاه اعداد صحیح $x'_1, \ldots, x'_n$ وجود دارند به طوری که $0 < a_1x'_1 + \cdots + a_nx'_n = r < s$. زیرا، چون $s \neq d$ و d باید s را عاد کند، پس حداقل یک a_j، مثلاً a_1، وجود دارد که $s \nmid a_1$. با تقسیم a_1 بر s داریم $a_1 = qs + r$، که در آن $0 < r < s$. بنابراین

$$a_1 = q(a_1x_1 + \cdots + a_nx_n) + r$$

یا

$$0 < a_1(1 - qx_1) + a_2(-qx_2) + \cdots + a_n(-qx_n) = r < s.$$

در نتیجه، با $x'_1 = 1 - qx_1$، $x'_j = -qx_j$، $j = 2, \ldots, n$، حکم به دست می‌آید. بنا بر ملاحظات بالا، واینشتاک الگوریتم زیر را برای محاسبهٔ $d = gcd(a_1, \ldots, a_n)$ ارائه می‌کند. فرض کنید $x_1^{(0)}, \ldots, x_n^{(0)}$ اعداد صحیح دلخواه باشند به طوری که $a_1x_1^{(0)} + \cdots + a_nx_n^{(0)} > 0$. اعداد صحیح $x_1^{(1)}, \ldots, x_n^{(1)}$ را به گونه‌ای تعیین می‌کنیم که

$$r_1 = a_1x_1^{(1)} + \cdots + a_nx_n^{(1)} < a_1x_1^{(0)} + \cdots + a_nx_n^{(0)} = r_0 \neq d,$$

و این عمل را تکرار می‌کنیم تا به ازای یک t، r_t تمام a_jها را عاد کند. در این صورت r_t همان d است. با توجه به بحث بالا، ملاحظه می‌کنیم که r_k، $k \geq 1$، در واقع کوچکترین باقیماندهٔ مثبت تقسیم یکی از a_jها بر r_{k-1} است و بنابراین در تلاش برای محاسبه d هیچ الزامی به محاسبهٔ صریح $x_j^{(k)}$ها نیست. به هر حال، قاعده برای محاسبه $x_j^{(k)}$ها به صورت زیر است:

$$x_j^{(k+1)} = -q_k x_j^{(k)} \qquad j \neq p,$$
$$x_p^{(k+1)} = 1 - q_k x_p^{(k)},$$

که در آن $a_p = q_k r_k + r_{k+1}$، $0 < r_{k+1} < r_k$ و a_p یکی از ضریبهاست که توسط r_k عاد نمی‌شود. به این ترتیب توجه داریم که تنها یک جواب برای معادلهٔ دیوفانتی $a_1x_1 + \cdots + a_nx_n = b$ به دست می‌آید. همان طور که واینشتاک ذکر می‌کند، انتخابهای متفاوت برای $x_j^{(0)}$ها منجر به جوابهایی متمایز می‌شود.

باند [۴]، الگوریتم واینشتاک را $n - 1$ بار برای یافتن جواب عمومی تک معادلهٔ دیوفانتی زیر به‌کار می‌برد:

$$a_1x_1 + \cdots + a_nx_n = b,$$

در روش باند، $n - 1$ معادلهٔ دیوفانتی زیر

$$a_{n-k}x_{n-k} + \cdots + a_nx_n = gcd(a_{n-k}, \ldots, a_n), \qquad k = 1, \ldots, n-1$$

با استفاده از الگوریتم واینشتاک حل می‌شوند.

در الگوریتم بلانکین‌شیپ اصلاح شده ابتدا معادلهٔ

$$a_{n-1}x_{n-1} + a_nx_n = gcd(a_{n-1}, a_n) = d_{n-1},$$

حل می‌شود. سپس، با استفاده از جواب عمومی بدست آمده، معادلهٔ

$$a_{n-2}x_{n-2} + a_{n-1}x_{n-1} + a_nx_n = gcd(a_{n-2}, d_{n-1}) = d_{n-2},$$

حل می‌شود و به همین ترتیب تا آخر.

توجه داریم که الگوریتم بلانکین‌شیپ اصلاح شده و الگوریتم باند یک معادلهٔ دیوفانتی را به طور مشابه حل می‌کنند با این تفاوت که روش باند معادلهٔ

$$a_{n-k}x_{n-k} + \cdots + a_n x_n = gcd(a_{n-k}, \ldots, a_n), \qquad k = ۱, \ldots, n-۱$$

را به عنوان یک معادلهٔ دیوفانتی مستقل تلقی می‌کند و یک جواب آن را با استفاده از روش واینشتاک، بدون در نظرگرفتن محاسبات انجام شده قبلی، بدست می‌آورد. بنابراین روش باند به کارایی روش بلانکین‌شیپ اصلاح شده نیست.

الگوریتم برادلی

تنها اختلاف الگوریتم برادلی [۷،۶]، با الگوریتم بلانکین‌شیپ اصلاح شده در تعیین ستون عملوند است. در الگوریتم برادلی ستون عملوند یک ستون قابل قبول از ماتریس $C^{(k)}$ انتخاب می‌شود که دارای بزرگترین مؤلفه در سطر اول است (یعنی ستون $C_۱^{(k)}$).

مثال ۳. برای معادلهٔ دیوفانتی مثال ۱، الگوریتم برادلی جواب عمومی زیر را به دست می‌دهد:

$$\begin{bmatrix} x_۱ \\ x_۲ \\ x_۳ \end{bmatrix} = \begin{bmatrix} ۹۱۰۰ \\ -۳۲۷۵۹۹ \\ ۶۵۵۱۴۶ \end{bmatrix} + \begin{bmatrix} -۲۲۷۴۹۹ & -۲۷۴۷۵ \\ ۸۱۸۹۹۳۹ & ۹۸۹۰۹۷ \\ -۱۶۳۷۸۵۷۸ & -۱۹۷۸۰۳۷ \end{bmatrix} \begin{bmatrix} q_۱ \\ q_۲ \end{bmatrix}, \qquad q_۱, q_۲ \in \mathbb{Z}.$$

در الگوریتم برادلی، چون با بزرگترین و کوچکترین اعداد (مثبت) در سطر اول ماتریس $C^{(k)}$ کار می‌شود، پس مضرب محاسبه شده در قدم (۴) معمولاً یک عدد بزرگ است. بنابراین، انتظار می‌رود که جواب عمومی حاصل از الگوریتم برادلی شامل اعداد بزرگ باشد.

با مقایسهٔ مثالهای ۲ و ۳ ملاحظه می‌شود که الگوریتم برادلی خیلی بیشتر از الگوریتم بلانکین‌شیپ باعث رشد اعداد محاسبه شدهٔ میانی می‌شود. این موضوع در حالت کلی نیز درست است.

برادلی، یک کران برای تعداد تکرارهای الگوریتم خود بدست می‌دهد. این کران در واقع تعمیمی از نتیجهٔ ارائه شده توسط لامه است، بدین ترتیب که تعداد تکرارهای الگوریتم اقلیدس برای n عدد صحیح هیچگاه بزرگتر از $n-۲$ به اضافه پنج برابر تعداد ارقام کوچکترین عدد نیست. برادلی همچنین یک کران برای تعداد عملیات این الگوریتم ارائه می‌کند. برای این منظور، قرار دهید $d_n = a_n$ و $d_{n-i} = gcd(a_{n-i}, d_{n-i+۱})$، $i = ۱, \ldots, n-۱$. فرض کنید K_i نشان دهنده تعداد تکرارهای الگوریتم اقلیدس برای محاسبه d_{n-i} باشد. قرار دهید $K = \sum_{i=۱}^{n-۱} K_i$. در این صورت الگوریتم مورد اشاره به $(n+۱)K$ عمل ضرب، همین تعداد عمل جمع و K عمل تقسیم نیاز دارد. به علاوه میزان حافظهٔ لازم برابر با $n(n+۱)$ است. برادلی پیرایشی از این الگوریتم را ارائه می‌کند که تنها به

$۲K + ۳(n-۱)$ عمل ضرب، $۲K + n - ۱$ عمل جمع و $K + n - ۱$ عمل تقسیم نیاز دارد. به علاوه میزان حافظهٔ لازم برابر با $۲n + ۴$ است. او همچنین نشان می‌دهد که با این پیرایش، الگوریتم قادر به محاسبهٔ «کوچکترین» ضرایب برای بیان بزرگترین مقسوم علیه مشترک چند عدد صحیح به صورت یک ترکیب خطی صحیح از آنهاست. این در واقع تعمیمی برای کار لویت [۲۴] است.

الگوریتم کرتزنر

در الگوریتم کرتزنر [۲۱]، ستون عملگر همانند الگوریتم بلانکین‌شیپ تعیین می‌شود. تمام ستونهای قابل قبول دیگر ماتریس $C^{(k)}$ به عنوان ستون عملوند انتخاب می‌شوند.

مثال ۴. الگوریتم کرتزنر جواب عمومی زیر را برای معادلهٔ دیوفانتی مثال ۱ بدست می‌دهد:

$$\begin{bmatrix} x_۱ \\ x_۲ \\ x_۳ \end{bmatrix} = \begin{bmatrix} -۴۲ \\ -۱۵ \\ ۸۵ \end{bmatrix} + \begin{bmatrix} ۶۱ & ۱۳۹ \\ ۵۳ & ۴۹ \\ -۱۸۷ & -۲۸۰ \end{bmatrix} \begin{bmatrix} q_۱ \\ q_۲ \end{bmatrix}, \qquad q_۱, q_۲ \in \mathbb{Z}.$$

با مقایسهٔ مثالهای ۲، ۳ و ۴ ملاحظه می‌کنیم که بزرگی اعداد در جواب عمومی حاصل از الگوریتم کرتزنر خیلی کوچکتر از مورد مشابه در الگوریتمهای بلانکین‌شیپ و برادلی است. آزمونهای عددی درستی این مطلب را در حالت کلی تأیید می‌کنند (بخش ۵ را ببینید).

الگوریتم راسر

در این الگوریتم [۳۲،۳۱،۹]، ستون عملوند ستون قابل قبول از ماتریس $C^{(k)}$ با بزرگترین درایه در سطر اول است (یعنی ستون $C_۱^{(k)}$). یک ستون قابل قبول دیگر $C^{(k)}$ با بزرگترین درایهٔ بعدی در سطر اول، ستون عملگر است (یعنی $C_۲^{(k)}$).

مثال ۵. الگوریتم راسر جواب عمومی زیر را برای معادلهٔ دیوفانتی مثال ۱ بدست می‌دهد:

$$\begin{bmatrix} x_۱ \\ x_۲ \\ x_۳ \end{bmatrix} = \begin{bmatrix} ۳۶ \\ -۱۹ \\ -۸ \end{bmatrix} + \begin{bmatrix} -۷۸ & ۶۱ \\ ۴ & ۵۳ \\ ۹۳ & -۱۸۷ \end{bmatrix} \begin{bmatrix} q_۱ \\ q_۲ \end{bmatrix}, \qquad q_۱, q_۲ \in \mathbb{Z}.$$

صفحه‌جدید **الگوریتم موریتو-سالکین**

در این الگوریتم [۲۶] نیز مشابه الگوریتم راسر $C_۱^{(k)}$ به عنوان ستون عملوند انتخاب می‌شود و در هر تکرار تمام ستونهای قابل قبول دیگر به عنوان ستون عملگر انتخاب می‌شوند.

مثال ۶. الگوریتم موریتو-سالکین جواب عمومی زیر را برای معادلهٔ دیوفانتی مثال ۱ بدست می‌دهد:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} ۳۶ \\ -۱۹ \\ -۸ \end{bmatrix} + \begin{bmatrix} ۱۷ & -۹۵ \\ -۵۷ & ۶۱ \\ ۹۴ & -۱ \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix}, \qquad q_1, q_2 \in \mathbb{Z}.$$

توجه: موریتو و سالکین [۲۷] یک روش دیگر نیز برای محاسبهٔ بزرگترین مقسوم علیه مشترک ارائه می‌کنند. این روش بسته به اینکه مضرب محاسبه شده در قدم (۴) غیر صفر باشد یا نه همان روش راسر یا روش بلانکین‌شیپ اصلاح شده است.

الگوریتم پیشنهادی

این الگوریتم شبیه به الگوریتم کرتزنر است. در این الگوریتم ستون عملگر یک ستون قابل قبول از میان ستونهای دوم تا nام ماتریس $C^{(k)}$ با کوچکترین نرم بینهایت انتخاب می‌شود. بقیه ستونهای قابل قبول دیگر ماتریس $C^{(k)}$ به عنوان ستون عملوند انتخاب می‌شوند.

مثال ۷. الگوریتم بالا جواب عمومی زیر را برای معادلهٔ دیوفانتی مثال ۱ بدست می‌دهد:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} ۳۶ \\ -۱۹ \\ -۸ \end{bmatrix} + \begin{bmatrix} -۷۸ & -۹۵ \\ ۴ & ۶۱ \\ ۹۳ & -۱ \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix}, \qquad q_1, q_2 \in \mathbb{Z}.$$

ملاحظات

- در الگوریتمهای بالا ماتریس $C^{(k+1)}$، به ازای هر $k \geq ۰$، از انجام عملیات ستونی مقدماتی صحیح روی ماتریس $C^{(k)}$ بدست می‌آید.
- اجرای همهٔ الگوریتمهای بالا منجر به ماتریس C به صورت $(de_1 \ , \ M^T)^T$ می‌شود، که در آن M یک ماتریس تک مدولی است.
- چون $(۱, -a^T)C = ۰$، پس به ازای هر k، $(۱, -a^T)C^{(k)} = ۰$. با فرض $M = (z, U)$ داریم: $a^T U = ۰$ و $a^T z = d$. بنابراین، M همان ماتریس مطلوب در قضیهٔ ۷ است.
- کارایی تمام الگوریتمها را می‌توان با در نظر گرفتن الگوریتم تقسیم با کوچکترین باقیماندهٔ مطلق در قدم (۴)، به جای تقسیم با کوچکترین باقیماندهٔ مثبت، افزایش داد.
- درکلیه الگوریتمهای بالا، هرگاه درایهٔ اول یک ستون از ماتریس $C^{(k)}$ صفر باشد، آنگاه می‌توان آن ستون را حذف کرد و بنابراین یک مساله با یک متغیر کمتر بدست آورد. در واقع، بردار حاصل از

حذف درایهٔ اول یک چنین ستونی از ماتریس $C^{(k)}$ جزء یکی از بردارهای پایه برای فضای جواب معادله است.

- چون در الگوریتم راسر و الگوریتم موریتو-سالکین با بزرگترین اعداد در سطر اول ماتریس $C^{(k)}$ سر و کار داریم، بنابراین مضربهای ایجاد شده در قدم (۴) معمولاً کوچک هستند. در نتیجه این دو الگوریتم معمولاً یک ماتریس تک مدولی M با درایه‌های تقریباً کوچک بدست می‌دهند.
- در الگوریتم پیشنهادی ما چون ستون عملگر یک ستون از ماتریس $C^{(k)}$ با کوچکترین نرم است، بنابراین انتظار داریم که نرم ستونهای ماتریس $C^{(k+1)}$ تغییر فاحشی نکنند.
- تمامی الگوریتمهای بالا و در نتیجه فرایند حل یک معادلهٔ دیوفانتی خطی در یک زمان چند جمله‌ای به توقف می‌رسند.

۵ مقایسهٔ عددی الگوریتمها

در این بخش به مقایسهٔ عددی الگوریتمهایی که در بخش قبلی، برای محاسبهٔ بزرگترین مقسوم علیه مشترک چند عدد صحیح بیان شد، می‌پردازیم. برای این منظور از زبان برنامه‌نویسی پاسکال و یک کامپیوتر مدل ۳۸۶ استفاده کرده‌ایم. این الگوریتمها را از نقطه نظر زمان اجرا و بزرگی اعداد در جواب عمومی محاسبه شده با یکدیگر مقایسه می‌کنیم. برای این منظور n عدد صحیح به طور تصادفی از بازه $[۱,۱۰^۷]$ انتخاب می‌کنیم. توجه داریم که اگر $M = (z, U)$ ماتریس تک مدولی نهایی حاصل از یک الگوریتم باشد، آنگاه بنا بر قضیهٔ ۷، بردار $\frac{b}{d}z$، $d = gcd(a)$، یک جواب خاص برای معادلهٔ دیوفانتی $a^T x = b$ است و ستونهای ماتریس U تشکیل یک پایه برای فضای جواب معادلهٔ دیوفانتی همگن متناظر می‌دهند. بنابراین جواب عمومی به صورت $x = \frac{b}{d}z + Uq$ است که در آن $q \in \mathbb{Z}^{n-۱}$ یک بردار دلخواه است. پس، بزرگی اعداد در جواب عمومی محاسبه شده به بزرگی درایه‌های ماتریس تک مدولی نهایی M بستگی دارند. بزرگی یک عدد را با تعداد بیتها در نمایش دودویی آن عدد اندازه می‌گیریم. وقتی که یک الگوریتم را برای یک مثال آزمون می‌کنیم بزرگترین عدد، از نظر قدر مطلق، در جواب عمومی محاسبه شده را با بزرگترین عدد در معادلهٔ دیوفانتی مقایسه می‌کنیم.

توجه داریم که در حالت $n = ۲$ تمام الگوریتمها یک جواب عمومی را بدست می‌دهند، چون در این حالت تنها یک پایه برای فضای جواب وجود دارد. بنابراین حالت $n = ۲$ را بررسی نمی‌کنیم. اما به ازای $n \geq ۳$، تعداد پایه‌ها برای فضای جواب نامتناهی است. مساله‌های مورد آزمون دارای $n = ۳, ۵, ۱۰, ۲۰, ۵۰, ۱۰۰$ متغیر هستند. به ازای هر n، چهل معادلهٔ دیوفانتی را حل می‌کنیم. بنابراین در مجموع ۲۴۰ معادلهٔ دیوفانتی حل شده است. برای هر یک از این معادله‌ها بزرگترین عدد از لحاظ قدر مطلق در جواب عمومی را محاسبه می‌کنیم و از میانگین آنها (برای چهل معادله) به عنوان یک معیار سنجش برای مقایسه الگوریتمها استفاده می‌کنیم.

با توجه به مطالب بخش قبلی، ملاحظه می‌کنیم که الگوریتمهای بلانکین‌شیپ، برادلی و راسر مشابه یکدیگر عمل می‌کنند، به این معنی که در هر تکرار فقط یک ستون عملگر و یک ستون عملوند وجود دارد. پس این الگوریتمها را می‌توان از نظر تعداد تکرارها و زمان اجرا نیز مقایسه کرد. شبیه به همین مقایسه را می‌توان در مورد الگوریتمهای کرتزنر، موریتو-سالکین و الگوریتم پیشنهادی انجام داد. بنابراین، به ازای هر n، زمان اجرای یک الگوریتم را برای هر یک از چهل معادلهٔ دیوفانتی محاسبه و از میانگین آنها برای مقایسهٔ زمان اجرای الگوریتمها استفاده می‌کنیم. معیاری مشابه برای تعداد تکرارهای یک الگوریتم در نظر می‌گیریم. نتایج آزمون را در جدول ۱ آورده‌ایم. در این جدول t، k و m، به ترتیب، نشان دهنده (میانگین) زمان اجرا، (میانگین) تعداد تکرارها و (میانگین) بزرگی اعداد در جواب عمومی می‌باشند. d نشان دهندهٔ (میانگین) بزرگی اعداد (تعداد بیتها در نمایش دودویی بزرگترین عدد موجود در یک معادله) در چهل معادلهٔ دیوفانتی، به ازای یک n خاص، است.

آزمونها مؤید آن هستند که تقریباً در تمام موارد الگوریتم راسر و پس از آن، الگوریتم موریتو-سالکین بهترین جواب عمومی را بدست می‌دهند، خصوصاً وقتی که n بزرگ است، در حالی که بیشترین زمان اجرا نیز از آنِ این الگوریتم‌هاست. تعداد تکرارهای این الگوریتمها نسبت به الگوریتم پیشنهادی و الگوریتم کرتزنر به طور قابل ملاحظه‌ای بیشتر است. الگوریتم برادلی و پس از آن الگوریتم بلانکین‌شیپ، در همهٔ موارد بدترین جواب عمومی را بدست می‌دهند. الگوریتم پیشنهادی ما در همه موارد یک جواب عمومی بهتر، نسبت به الگوریتم کرتزنر، بدست می‌دهد، در حالی که تعداد تکرارهای آن نیز بیشتر است.

۶ نتیجه‌گیری

الگوریتمهای عددی متعددی را برای پیداکردن بزرگترین مقسوم‌علیه مشترک چند عدد صحیح بررسی کرده‌ایم. کاربرد این الگوریتمها را همراه با یک الگوریتم پیشنهادی خود برای حل تک معادله‌های دیوفانتی متنوع تصادفی آزمون کرده‌ایم. اگر چه نتایج بدست آمده برخی الگوریتمها را نسبت به برخی دیگر در پاره‌ای از مساله‌های آزمون مناسب‌تر نشان می‌دهند، ولی در حالت کلی بزرگی اعداد صحیح بدست آمده همچنان در زمرهٔ مشکلات اساسی روشهای موجود در حل معادلات دیوفانتی باقی مانده است.

۷ قدردانی

نویسندگان از حمایتهای مالی شورای پژوهشی دانشگاه صنعتی شریف قدردانی می‌کنند.

جدول ۱. نتایج آزمون برای الگوریتم‌ها

		$n=۳$ $d=۱۶$	$n=۵$ $d=۱۶/۷$	$n=۱۰$ $d=۱۷/۶$	$n=۲۰$ $d=۱۷$	$n=۵۰$ $d=۱۷$	$n=۱۰۰$ $d=۱۷$
بلانکین‌شیپ	t	۰*	۰	۰	۰	۰/۰۰۳	۰/۰۰۹
	k	۸/۷	۱۰/۹	۱۴/۷	۲۳/۳	۵۲	۱۰۱/۶
	m	۲۰/۱	۲۲/۹	۲۲/۷	۲۱/۴	۲۰/۲	۱۹/۷
برادلی	t	۰	۰	۰	۰/۰۰۳	۰	۰/۰۰۳
	k	۹/۴	۹/۶	۱۵/۱	۲۲/۶	۵۱/۸	۱۰۶/۴
	m	۲۰/۳	۲۴/۳	۲۴/۵	۲۲/۵	۲۲/۲	۱۸/۶
راسر	t	۰	۰	۰/۰۰۳	۰/۰۰۳	۰/۰۲	۰/۱۲
	k	۱۳/۳	۲۵/۷	۵۰/۲	۸۷/۲	۱۷۵/۲	۳۰۳/۵
	m	۱۰	۸/۵	۴/۸	۳/۵	۲/۶	۲/۲۵
کرتزنر	t	۰	۰	۰	۰	۰	۰/۰۰۸
	k	۶/۱	۵	۳/۹	۲/۸۵	۲	۱/۸
	m	۱۱/۹	۱۲/۹	۱۲/۸	۱۴	۱۴/۶	۱۴/۲۵
مورتیو-سالکین	t	۰	۰	۰	۰	۰/۰۲	۰/۱۴
	k	۸/۵	۱۰/۹	۱۵	۲۴	۵۲/۲	۱۰۱/۸۵
	m	۱۰/۷	۸/۹	۷/۳	۵/۸	۵/۵	۴/۵
پیشنهادی	t	۰	۰	۰	۰/۰۰۳	۰	۰/۰۰۹
	k	۶/۹	۶/۳	۵/۴	۴/۲	۳/۷	۳
	m	۱۱/۲	۱۰/۷	۱۰	۱۱/۵	۱۲/۳	۱۳/۱

* اعداد ۰ آمده در جدول به جای اعداد بسیار کوچک بدست آمده به عنوان زمان اجرا درج شده‌اند.

مراجع

[1] W. A. Blankinship, "A new version of the Euclidean algorithm", Amer. Math. Monthly 70, (1963), 742-745.

[2] W. A. Blankinship, "Algorithm 287, Matrix triangulation with integer arithmetic", Comm. ACM 9, (1966), 513.

[3] W. A. Blankinship, "Algorithm 288, Solution of linear Diophantine equations", Comm. ACM 9, (1966), 514.

[4] J. Bond, "Calculating the general solution of a linear Diophantine equation", Amer. Math. Monthly 74, (1967), 955-957.

[5] V. J. Bowman, "The structure of integer programs under the Hermitian normal form", Operations Research 22, (1974), 1067-1080.

[6] G. H. Bradley, "Algorithm and bound for the greatest common divisor of n integers", Comm. ACM 13, (1970), 433-436.

[7] G. H. Bradley, "Algorithms for Hermite and Smith normal matrices and linear Diophantine equations", Math. Comp. 25, (1971), 897-907.

[8] G. H. Bradley, "Equivalent integer programs and canonical problems", Manag. Sci. 17, (1971), 354-366.

[9] T. J. Chou and G. E. Collins, "Algorithms for the solution of systems of linear Diophantine equations", SIAM J. Comp. 11, (1982), 687-708.

[10] G. E. Collins, "The computing time of the Euclidean algorithm", SIAM J. Computing 3, (1974), 1-10.

[11] J. D. Dixon, "The number of steps in the Euclidean algorithm", J. Number Theory 2, (1970), 414-422.

[12] J. Donaldson, "Minkowskyi reduction of integer matrices", Math. Comp. 33, (1979), 201-216.

[13] H. Esmaeili, N. Mahdavi-Amiri and E. Spedicato, "A class of ABS algorithms for Diophantine linear systems", Numer. Math. 90, (2001), 101-115.

[14] H. Esmaeili, N. Mahdavi-Amiri and E. Spedicato, "ABS methods and solving Diophantine linear systems", Report TR/4, Department of Mathematical Sciences, Sharif University of Technology, Tehran, 1999.

[15] H. Esmaeili, N. Mahdavi-Amiri and E. Spedicato, "Generating the integer null space and conditions for determination of an integer basis using the ABS algorithms", Bull. Iran. Math. Soc. 27, (2001), 1-18.

[16] H. Esmaeili, N. Mahdavi-Amiri and E. Spedicato, "ABS solution of a class of linear integer inequalities and integer LP problems", Optimization Methods and Software 16, (2001), 179-192.

[17] J. Ch. Fiorot, "Generation of all integer points for given sets of linear inequalities", Math. Prog. 3, (1972), 276-295.

[18] R. S. Garfinkel and G. L. Nemhauser, *Integer Programming*, John Wiley and Sons, 1972.

[19] M. F. Hurt and C. Waid, "A generalized inverse which gives all the integral solutions to a system of linear equations", SIAM J. Appl. Math. 19, (1977), 547-550.

[20] R. Kannan and A. Bachem, "Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix", SIAM J. Comput. 8, (1979), 499-507.

[21] S. Kertzner, "The linear Diophantine equation", Amer. Math. Monthly 88, (1981), 200-203.

[22] D. E. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1969.

[23] D. H. Lehmer, "Euclid's algorithm for large numbers", Amer. Math. Monthly 45, (1938), 227-233.

[24] R. J. Levit, "A minimum solution of a Diophantine equation", Amer. Math. Monthly 63, (1956), 647-651.

[25] M. T. McClellan," The exact solution of systems of linear equations with polynomial coefficients", J. Assoc. Comput. Mach., 20, (1973), 563-588.

[26] S. Morito and H. M. Salkin, "Finding the general solution of a linear Diophantine equation", The Fibonacci Quarterly 17, (1979), 361-368.

[27] S. Morito and H. M. Salkin, "Using the Blankinship algorithm to find the general solution of a linear Diophantine equation", Acta Inf. 13, (1980), 379-382.

[28] J. E. L. Peck, "Algorithm 139, Solutions of the Diophantine equation", Comm. ACM 5, (1962), 556.

[29] J. E. L. Peck, "Algorithm 237, Greatest common divisor", Comm. ACM 7, (1964), 481.

[30] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, 1986.

[31] J. B. Rosser, "A note on the linear Diophantine equation", Amer. Math. Monthly 48, (1941), 662-666.

[32] J. B. Rosser, "A method of computing exact inverses of matrices with integer coefficients", J. Res. Nat. Bur. Standards 49, (1952), 349-358.

[33] A. Schönhage, "Schnelle berechnung von kettenbruchentwicklungen", Acta inf. 1, (1971), 133-144.

[34] A. Schrijver, *Theory of Linear and Integer Programming*, John Wiley and Sons, 1986.

[35] E. Spedicato, H. Esmaeili and Z. Xia, "A review of ABS algorithms for linear real and Diophantine equations and optimization", Proceedings XVI CEYDA and VI CMA Conferences, Las Palmas de Gran Canaria, September 1999 (editors: R. Montenegro, G. Montero and G. Winter), 11-23.

[36] R. P. Stanley, "Linear Diophantine equations and local cohomology", Invent. Math. 68,(1982), 175-193.

[37] R. Weinstock, "Greatest common divisor of several integers and an associated linear Diophantine equation", Amer. Math. Monthly 67, (1960), 664-667.

حمید اسمعیلی
دانشگاه صنعتی شریف، دانشکده علوم ریاضی
پست الکترونیک:esmaeili47@yahoo.com
نظام‌الدین مهدوی امیری
دانشگاه صنعتی شریف، دانشکده علوم ریاضی
پست الکترونیک: nezam@math.sharif.ac.ir

فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۸ (بهار ۱۳۸۱)، صص. ۲۷ تا ۳۹

فضاهای کوانتمی و توپولوژی ناجابجایی آنها

ج. کونتز

هندسهٔ ناجابجایی هندسهٔ «فضاهای کوانتمی» را مطالعه می‌کند، به عبارت ساده‌تر، این کار به معنی مطالعهٔ «خواص هندسی» جبرهای ناجابجایی (به عنوان مثال روی میدان اعداد مختلط $\mathbb{C}$) است. چنین جبرهایی به عنوان مثال شامل جبرهای زیر هستند:

- جبرهای عملگرهای شبه دیفرانسیل، جبرهای عملگرهای برگ‌وار دیفرانسیل بر خمینه‌های برگ‌بندی شده، جبرهای فرم‌های دیفرانسیل، گروه جبرها یا جبرهای پیچشی برای گروهوارها.
- صورت‌های ناجابجایی یا «کوانتیدهٔ» جبرهای مشهور مانند جبرهای نگاشت‌ها بر کره‌ها، یا بر چنبره‌ها، بر مجتمع‌های سادکی یا بر فضاهای رده‌بندی؛
- جبرهای واقعاً ناجابجایی جدید مانند جبرهای ناشی شده از مکانیک کوانتمی.

اساس کار بر توجه به این نکته است که رسته‌های مختلفی از فضاها را می‌توان به وسیلهٔ جبرهای (جابجایی) نگاشت‌ها بر آنها کاملاً توصیف کرد (یک فضای موضعاً فشرده به‌وسیله جبر نگاشت‌های پیوسته، یک خمینه هموار به وسیلهٔ جبر نگاشت‌های هموار، یک واریتهٔ جبری آفین به وسیله حلقهٔ مختصاتی‌اش). در این صورت، به یک جبر جابجایی می‌توان به عنوان جبر نگاشت‌ها بر یک «فضای ناجابجایی» نگریست. این رویکرد بسیار انعطاف‌پذیر است، مثلاً این دیدگاه جبر نگاشت‌ها بر یک خمینه، جبر عملگرهای شبه دیفرانسیل و جبر فرمهای دیفرانسیل را به‌طور یکسان پوشش می‌دهد.

حال سؤال این است: خاصیت «هندسی» یک جبر ناجابجایی چیست؟ چگونه می‌توان کلاسهای مشخصه یا ساختارهای اضافی مانند متریک ریمانی را برای یک جبر ناجابجایی توصیف کرد؟ این‌گونه سؤال‌ها مطالبی است که هندسه ناجابجایی دربارهٔ آنها بحث می‌کند. کتاب بسیار جذاب آلَن کنز [۵] را ببینید.

دو «ابزار» بنیادی هندسهٔ ناجابجایی عبارت‌اند از مانستگی دوری و Kـتئوری توپولوژیک دو متغیره.

نظریهٔ دوری را می‌توان به عنوان تعمیمی از همانستگی دُرام[1] کلاسیک، با نتایج پر دامنه، درنظر گرفت. درحالی‌که Kـتئوری، Kـتئوری توپولوژیک دو متغیرهٔ اَتیاـهرزبروخ را به عنوان یک حالت خیلی خاص شامل می‌شود. Kـتئوری دو متغیره ابتدا به وسیله کاسپاروف بر روی رستهٔ C^*ـجبرها تعریف شد و توسعه یافت، از این طریق کارهای قبلی اَتیاـهرزبروخ، براونـ دوگلاس ـفیلمُر و دیگران وحدت یافت و به صورت بنیادین گسترش داده شد. کاسپاروف همچنین نظریهٔ دو متغیرهٔ خود را به‌کار برد و نتایج مثبت حیرت‌آوری دربارهٔ حدس نوویکف به‌دست آورد. همین اواخر کشف شد که Kـتئوری‌های توپولوژیک دومتغیره می‌تواند بر طیف گسترده‌ای از جبرهای توپولوژیک شامل جبرهای گسسته و جبرهای موضعاً محدب و جبرهای باناخ یا C^*ـجبرها تعریف شود.

نظریهٔ دوری یک نظریهٔ مانستگی است که مستقلاً توسط کنز و تسیگان توسعه یافت، که هر یک متأثر از جنبه‌های مختلف ساختارهای Kـتئوری بودند. پس از آن فوراً مشخص شد که مانستگی دوری ارتباط‌های نزدیکی با نظریه درام، مانستگی جبر لی، همانستگی گروه و قضایای اندیس دارد.

قابل توجه است که نظریه‌های جدید به هیچ وجه تعمیم سادهٔ ساختارهای کلاسیک نیستند. درواقع، در حالت جابجایی، دیدگاهی جدید و تعبیری کاملاً بدیع از نظریه‌های مشهور کلاسیک ارائه می‌دهند. خاصیت‌های اساسی این دو نظریه فقط در رستهٔ ناجابجایی قابل مشاهده است. مثلاً هر دو نظریه در این زمینه تعدادی خاصیت شمول دارند.

در اینجا نگاهی داریم به نوع اطلاعات هندسی که این دو نظریه برای تعدادی از «فضاهای کوانتمی» ساده ارائه می‌دهند. تعریف رسمی کلاس‌های دوری و Kـتئوری که در این مثال‌ها ذکر شده است در بخش بعدی توضیح داده می‌شود. در اینجا برای ایجاد یک درک شهودی نیازی به تعریف دقیق نیست.

۱. **فضاهای با n نقطه و پیوندهای ناجابجایی.** این فضا دارای n نقطه و پیکان‌هایی بین هر دو نقطه است. به عنوان یک جبر، این فضا به وسیلهٔ جبر $M_n(\mathbb{C})$ متشکل از ماتریس‌های $n \times n$ توصیف می‌شود. (تابع‌های روی n نقطه متناظر با ماتریس‌های قطری‌اند).

نظریهٔ دوری و Kـتئوری، هر دو به یک ردهٔ زوج مانستگی نظر می‌کنند، و رده‌های فرد را در نظر

1) de Rham

نمی‌گیرند. در هر دو نظریه، ردهٔ زوج نابدیهی صفربُعدی است و هیچ ردهٔ همانستگی نابدیهی با بُعد بالاتر وجود ندارد. از آنجا که یک رده وجود دارد که نمایانگر ردهٔ هم‌ارزی n نقطه است و هیچ رده‌ای از بعد بالاتر وجود ندارد، $M_n(\mathbb{C})$ شبیه یک فضای صفربعدی همبند است.

این ساده‌ترین حالتِ یک جبر پیچشی برای یک گروهوار است. در حالت کلی، یک گروهوار (توپولوژیک) عبارت است از یک فضای اشیاء و خانواده‌ای از پیکان‌های (برگشت‌پذیر) که می‌تواند مانند مثال بالا به عنوان مسیرهایی ناجابجایی بین اشیاء در نظرگرفته شود. از دیدگاه نظریه‌های مانستگی ناجابجایی، نقاط مختلفی که توسط یک پیکان به هم وصل شده‌اند از یک ردهٔ مانستگی هستند. رده‌های مانستگی بالاتر نیز می‌تواند از پیکربندیهایی از پیکان‌ها (مانند طوقه‌ای از پیکان‌ها)، از پیکربندیهای متشکل از پیکان‌ها و اشیاء، یا حتی از ترکیب‌های خطی چنین چیزهایی ناشی شود. به عنوان مثال، جبر تعیین شده توسط ترکیب‌های خطی همه مسیرهای ممکن درگراف زیر را در نظر گیرید. این جبر، علاوه بر ردهٔ 0ـبعدی داده شده توسط ردهٔ هم‌ارزی نقاط، یک ردهٔ یک‌بعدی ناشی از مسیر روی دایره را نیز در بر دارد (برعکس حالت $M_n(\mathbb{C})$، در اینجا فرض می‌کنیم این مسیر مخالف مسیر بدیهی است).

۲. فضای فاز در مکانیک کوانتمی. این فضا توسط جبر یکه‌دار $A(p,q)$ توصیف می‌شود. $A(p,q)$ با دو مولد p,q که در رابطهٔ هایزنبرگ $pq-qp=1$ صدق می‌کنند، تولید می‌شود. (گاهی این جبر،جبر ویل[1] نامیده می‌شود). در حال حاضر هیچ محاسبه‌ای از Kـتئوری برای این جبر (یا تکمیل شدهٔ هموار آن) وجود ندارد. از دیدگاه نظریهٔ دوری یک رده همانستگی ۲ـبعدی وجود دارد و هیچ ردهٔ (نابدیهی) در بعدهای مخالف دو وجود ندارد. در این صورت ما یک فضای ناجابجایی ۲ـبعدی داریم (فرضاً شبیه یک صفحهٔ ۲ـبعدی). باوجوداین، نه تنها این فضا هیچ نقطه‌ای ندارد، بلکه حتی هیچ ردهٔ

1) Weyl algebra

هم‌ارزی یک نقطه را نیز ندارد.

۳. چنبرهٔ ۲ـبعدی ناجابجایی. این فضا عبارت است از جبر یکه‌دار A_θ داده شده توسط سریهای توانی با ضرایب سریعاً نزولی در دو مولد u و v که در رابطه‌های $uu^* = u^*u = vv^* = v^*v = 1$ و $vu = e^{2\pi i\theta}$ برای یک $\theta \in [0, 1]$ صدق می‌کنند. هر زوج مولدهای $\{u, u^*\}$ و $\{v, u^*\}$ یک زیرجبر جابجایی یکریخت با جبر نگاشت‌های هموار بر دایره، تولید می‌کند. اگر $\theta = 0$، آنگاه این زیرجبرها جابجا می‌شوند و A_θ با جبر نگاشت‌های هموار بر چنبرهٔ ۲ـبعدی $S^1 \times S^1$ یکریخت است. Kـتئوری برای جبر A_θ دو ردهٔ زوج‌ـبُعدی و دو ردهٔ فرد‌ـبُعدی را در بر دارد.

نظریهٔ دوری با دقت بیشتری نشان می‌دهد که یکی از رده‌های زوج 0ـبعدی و دیگری ۲ـبعدی است. دو رده فرد هر دو یک‌ـبعدی‌اند (و توسط ۱ـفرم‌های $u^{-1}du$ و $v^{-1}dv$ نمایش داده می‌شوند). بنابراین، از این دیدگاه، چنبرهٔ ناجابجایی دقیقاً شبیه چنبرهٔ معمولی ۲ـبعدی است.

۴. مجتمع‌های سادکی ناجابجایی. فرض کنید Σ یک مجتمع سادکی متناهی باشد که توسط

مجموعهٔ رأسهایش V و مجموعه سادکهایش که عبارت است از زیرمجموعه‌های متناهی $F \subset V$، داده شده است. می‌توانیم به Σ یک جبر ناجابجایی C_Σ به صورت زیر متناظر کنیم. فرض کنید C_Σ جبر یکدار داده شده توسط سریهای توانی با ضرایب سریعاً نزولی در مولدهای $h_s (S \in V)$ باشد که در روابط زیر صدق می‌کنند:

- $\Sigma_{S \in V} h_s = 1$ ؛
- اگر $\{S_0, S_1, \ldots, S_n\}$ در Σ نباشد، آنگاه حاصلضرب $h_{s_0} h_{s_1} \ldots h_{s_n}$ صفر است.

(توجه کنید که هنگامی‌که ما شرط اضافی جابجایی مولدها را معرفی می‌کنیم یک جبر یکریخت با جبر نگاشت‌های هموار بر تعبیر هندسی Σ را به دست می‌آوریم). Kـتئوری و مانستگی دوری متناوب برای C_Σ به ترتیب یکریخت با Kـتئوری و همانستگی تکین $\mathbb{Z}_2$ـمدرج تعبیر هندسی Σ است. با این حال، بُعد یک رده همانستگی دوری برای C_Σ، خیلی بزرگتر از بعد (d) ردهٔ مانستگی جابجایی نظیر آن (که از مرتبهٔ 3^d است) می‌باشد. همچنین یک پالایش درجه‌ای روی Kـمانستگی جبرهای موضعاً محدب وجود دارد. درجهٔ Kـمانستگی یک ردهٔ Kـمانستگی برای C_Σ با بعد ردهٔ مانستگی جابجایی نظیرش برابر است.

در این مثال‌ها رده‌های دوری و Kـتئوری برای توصیف «شکل» یک فضای ناجابجایی به کار رفته است. اما کارکردِ این ناورداهابه اینجا ختم نمی‌شود. آنها همچنین ابزار اصلی هستند که برای توصیف اطلاعات توپولوژیکی دیگر مانند داده‌های چسبان در توسیع‌ها و اندیس عملگرها به کار می‌روند.

در این مقاله ما دیدگاهی یکنواخت از نظریهٔ دوری و نظریهٔ ناوردای دو طرفهٔ Kـتئوری را ارائه می‌کنیم که در حقیقت می‌تواند در رسته‌های مختلف جبرها قابل اعمال باشد. این دیدگاه بر شباهت بین نظریهٔ دوری با نظریهٔ دُرام و رابطهٔ بین Kـتئوری و توسیع‌ها تأکید می‌کند. این دیدگاه به طور طبیعی به خواص بنیادی در دو نظریه منتج می‌شود. ما همچنین ساختار شاخص دو متغیرهٔ چرن‌ـکُنز[1] را که از Kـتئوری دومتغیره به نظریهٔ دومتغیره دوری گذر می‌کند، توضیح می‌دهیم. وجود این تبدیل ضربی با این کلیت

1) Chern-Connes

فقط در همین سالهای اخیر در نتیجهٔ پیشرفت در نظریه‌های K و مانستگی دوری به دست آمده است، [۹],[۶](حالت‌های مهم خاص توسط کنز و دیگران بررسی شده بود، [۱۲],[۴]). این تعمیمی وسیع از شاخص کلاسیک چرن در هندسه دیفرانسیل است و اجازه می‌دهد که کلاس‌های مشخصه را بتوان با اشیاء Kـتئوری متناظر کرد.

من برای تصاویر مثال‌های بالا به پسرانم نیکلاس و میکائیل مدیونم. زیرا این تصویرها هیچ معنی تکنیکی ندارند، و هدف آنها فقط نوعی تجسّم فضاهای کوانتمی وابسته است.

همبافت درام ناجابجایی‌ـ یا چگونه از یک فضای کوانتمی اطلاعات جابجایی استخراج کنیم

هر جبر ناجابجایی A با عمل خارج قسمت گرفتن نسبت به ایده‌آل تولیدشده توسط همه جابجاگرها می‌تواند تعویض‌پذیر شود. با این حال این روش، اطلاعات مربوط را تقریباً در همه حالت‌های جالب از بین می‌برد. در حقیقت، خارج قسمت آبلی نوعاً صفر است (مثلاً در مثال‌های ۱ و ۲ و ۳ قبلی وضع چنین است).

یک رویکرد نویدبخش عبارت است از تقسیم جبر فقط بر فضای خطی جابجاگرها، یا به طور دوگان، بررسی اثرها بر A. یک اثر[1] به موجب تعریف عبارت است از یک تابعک خطی f بر A چنانکه $f(xy) = f(yx)$ برای هر $x, y \in A$.

در این صورت، استراتژی ما برای توصیف اطلاعات توپولوژیکی عبارت است از بررسی رده‌های هموتوپی اثرها. هموتوپی برای اثرها چیست و چگونه می‌تواند به صورت جبری فرموله شود؟

یک جواب به وسیله Xـهمبافتی که توسط کویلن [۱۴]، در ارتباط با جبرهای دیفرانسیل مدرج معرفی شد، به دست می‌آید، پس از آن این Xـهمبافت به طور سیستماتیک در [۷] و [۸] و [۹] به کار رفت.

فرض کنید A یک جبر باشد. فضای $\Omega^1 A$ متشکل از همه ۱ـفرمهای مجرد روی A به عنوان دوـمدول[2] تشکیل شده از ترکیب‌های خطی عبارت‌های به صورت $xd(y)$، تعریف می‌شود که $x \in \tilde{A}$ و $y \in A$، که $\tilde{A}$ عبارت است از یکان شدهٔ[3] A. ساختار دوـمدول به وسیلهٔ قانون‌های زیر داده می‌شود:

$$a(xdy) = axdy, (xdy)a = xd(ya) - xyda, a \in A$$

(یعنی رابطهٔ $d(xy) = xdy + d(x)y$ معرفی می‌شود).

یک اثر بر $\Omega^1 A$ عبارت است از یک تابعک خطی f چنانکه $f(aw) = f(wa)$ برای $a \in A$ و $w \in \Omega^1 A$. Xـهمبافت (دوگان) $X'(A)$ عبارت است از همبافت $\mathbb{Z}_2$ـ مدرج زیر

$$\{\text{اثرها بر } \Omega^1 A\} \underset{\delta}{\overset{\beta}{\longleftarrow}} \{\text{نگاشتها بر } A\}$$

عملگرهای مرزی به‌وسیله فرمول‌های $(\beta f)(xdy) = f([x,y]), (\delta f)(x) = f(dx)$ تعریف می‌شوند. تحقیق این‌که $\beta\delta = \delta\beta = 0$ سرراست است.

این همبافت فقط دو گروه مانستگی دارد که عبارت‌اند از مانستگی‌های زوج و فرد. مانستگی زوج HX^{ev} عبارت است از فضای اثرهاــ تابعک‌های خطی بر A که روی جابجاگرها صفر می‌شوندــ خارج

1) trace 2) bimodule 3) unitization

قسمت‌گیری شده توسط فضای «مشتق‌های» اثرها- تابعک‌های خطی به‌صورت $f\circ d$ که f یک اثر بر $\Omega^1 A$ است. این خارج قسمت به درستی می‌تواند به عنوان فضای رده‌های مانستگی اثرها بر A درنظر گرفته شود. با بحث مشابهی برای مانستگی فرد، به دست می‌آوریم:

$$HX^{ev}(A) = \{\text{رده‌های هموتوپی اثرها بر } A\}$$
$$HX^{od}(A) = \{\text{رده‌های اثرهای بسته بر } \Omega^1 A\}$$

که اثر f بسته است اگر $f\circ d = 0$.

یک همبافت طبیعی $X(A)$ وجود دارد که $X'(A)$ دوگان آن می‌باشد: یعنی،

$$A \underset{\beta}{\overset{\delta}{\rightleftarrows}} \Omega^1 A_\natural$$

که $\Omega^1 A_\natural$ عبارت است از خارج قسمت $[A,\Omega^1 A]$ از $\Omega^1 A$ توسط جابجاگرها و $\natural : \Omega^1 A \to \Omega^1 A_\natural$ نگاشت خارج قسمت است و عملگرهای مرزی توسط رابطه‌های زیر تعریف می‌شوند:

$$\delta(x) = \natural(dx) \quad \text{و} \quad \beta(\natural(x\,dy)) = [x,y].$$

مسلماً تا اندازه‌ای تعجب‌آور است که همبافت فوق‌العاده سادهٔ $X(A)$ باید نقش همبافت درام را در هندسهٔ ناجابجایی ایفا کند. در حالت جابجایی به‌وضوح این همبافت به همبافت درام تقلیل نمی‌یابد. مشابهت این همبافت درام اکنون توضیح داده می‌شود. این توضیح همچنین منتج به یک تعبیر جدید از نظریهٔ درام کلاسیک می‌شود.

نقطهٔ شروع این است که اگرچه کارکردن با اثرها یک شیوهٔ معتدل‌تر نسبت به روش آبلی‌کردن است، هنوز برای خیلی از جبرهای ناجابجایی به نتایج بدیهی منتج می‌شود. درواقع مثال‌هایی طبیعی از جبرهای A وجود دارد که برای آنها هیچ (نگاشت) اثر نابدیهی وجود ندارد.

به همین دلیل محقق به بررسی اثرها بر جبرهایی که با A از طریق توسیع مرتبط‌اند، رهنمون می‌شود. یک توسیع A عبارت است از یک جبر E که A را به عنوان یک خارج قسمت (به‌وسیله یک ایده‌آل I) در بر دارد یا، به‌طور خلاصه، یک دنبالهٔ دقیق $0 \to I \to E \to A \to 0$ که فلش‌ها همریختی‌های جبرها هستند. توسیع‌ها نقشی اساسی در هندسهٔ ناجابجایی ایفا می‌کنند.

جبر A شبه-آزاد نامیده می‌شود اگر در هر توسیع A که ایده‌آل I پوچ‌توان است (یعنی $I^K = 0$ برای یک K)، همریختی $E \to A$ وجود داشته باشد که یک وارون چپ‌نگاشت خارج‌قسمت $E \to A$ باشد. این شرط به‌لحاظ صوری تقریباً با شرط هموار بودن که توسط گروتندیک برای جبرهای جابجایی و واریته‌های جبری معرفی شده، یکی است. هر جبر آزاد شبه-آزاد است.

همانستگی دوری تناوبی جبر A، $HP^*(A)$ که $* = ev/od$، از نمایش A به عنوان خارج‌قسمت یک جبر شبه-آزاد T به‌وسیلهٔ یک ایده‌آل I، به‌دست می‌آید و در این صورت می‌نویسیم

$$H(P)^*(A) = \varinjlim_n HX^*(T/I^n).$$

حقیقت مهم این است که این تعریف بستگی به انتخاب جبر شبه‌آزاد T ندارد. مانستگی $HX^*(T/I^n)$ به طور اصولی عبارت است از همانستگی دوری معمولی (ناتناوبی) $HC^{۲n+*}(A)$.

خیلی مشکل نیست که ببینیم HP^* را می‌توان به طریق دیگر به‌وسیله فرمول زیر که در آن $od = ev + ۱$ می‌باشد به‌دست آورد:

$$HP^*(A) = \varinjlim_n HX^{*+۱}(I^n)$$

در این تصویر یک هم‌دور دوری(از بعد $۲n - ۱$) توسط یک نگاشت اثر بر توان nـام ایده‌آل در یک توسیع A توصیف می‌شود.

این تعریف مانستگی دوری آشکارا با تعریف اولیهٔ ارائه‌شده توسط کُنز یا تسیگَن کاملاً متفاوت است. اثبات اینکه هر دو تعریف یک نتیجه را به‌دست می‌دهند نابدیهی است. توجه کنید که هر جبر A دارای یک تجزیهٔ[1] ذاتی شبه‌آزاد (حتی آزاد)، که به‌وسیله جبر تانسوری TA روی A داده می‌شود، می‌باشد.

یک شباهت چشمگیر بین مانستگی دوری تناوبی و مفهوم گروتندیک از مانستگی بینهایت کوچک، که توپولوژی واریته‌های ناهموار را در هندسهٔ جبری توصیف می‌کند، وجود دارد. در این مقایسه، جبرهای شبه‌آزاد نقشی را ایفا می‌کنند که واریته‌های هموار در کاتگوری ناجابجایی به عهده دارند و Xـهمبافت متناظر با همبافت درام است.

درحقیقت، در هندسهٔ جبری همانستگی بینهایت کوچک به این صورت تعریف می‌شود که حلقهٔ مختصاتی واریته، A را به عنوان خارج‌قسمت S/I حلقهٔ مختصاتی واریته هموار S بنویسیم و آنگاه همانستگی درام کامل‌شدهٔ S یعنی $\hat{S} = \varinjlim S/I^n$، را محاسبه کنیم. می‌توان نشان داد که این تعریف به انتخاب نشاندن در یک واریتهٔ هموار بستگی ندارد. این روش دقیقاً مشابه تعریف همانستگی دوری تناوبی است که در بالا ارائه شد. در آن تعریف، ما A را به عنوان خارج‌قسمتی از یک جبر شبه‌آزاد T می‌نویسیم و سپس مانستگی $HX^*(\hat{T})$ را محاسبه می‌کنیم.

فرض کنید دو جبر $A_۲, A_۱$ داده شده‌اند، ما همچنین می‌توانیم نظریهٔ دو متغیرهٔ دوری تناوبی $HP_*(A_۱, A_۲)$، که $* = ۰, ۱$ را به عنوان مانستگیِ همبافت همریختی بین Xـهمبافت‌های وابسته به توسیع‌های شبه‌آزاد $A_۱$ و $A_۲$ تعریف کنیم. یک ضرب (ترکیب) طبیعی به‌صورت زیر وجود دارد:

$$HP_i(A_۱, A_۲) \times HP_j(A_۲, A_۳) \longrightarrow HP_{i+j}(A_۱, A_۳)$$

هر همریختی جبرها $\alpha : A \longrightarrow B$ یک عضو $HP_۰(A, B)$ در $HP(\alpha)$ را مشخص می‌کند.

نظریهٔ دوری تناوبی $HP_i(A_۱, A_۲)$ خاصیت‌های خیلی خوبی دارد. می‌توان نشان داد که این نظریه تحت اثر هموتوپی مشتق‌پذیر (هموار) و با ناوردای مُرتیا[2] در هر دو متغیر، ناوردا است. همچنین به موجب مرجع [۹] این نظریه در اصل کَندن[3]، به معنی زیر، صدق می‌کند.

1) resolution 2) Mortia 3) excision

فرض کنید D یک جبر باشد. هر توسیع $0 \to I \xrightarrow{i} A \xrightarrow{q} B \to 0$ دنباله‌هایی دقیق در $HP_*(0,D), HP_*(D,0)$ به صورت زیر القا می‌کند:

$$\begin{array}{ccccc} HP_*(D,I) & \xrightarrow{HP(i)} & HP_*(D,A) & \xrightarrow{HP(q)} & HP_*(D,B) \\ \uparrow & & & & \downarrow \\ HP_1(D,B) & \xleftarrow{HP(q)} & HP_1(D,A) & \xleftarrow{HP(i)} & HP_1(D,I) \end{array}$$

و

$$\begin{array}{ccccc} HP_*(I,D) & \xleftarrow{HP(q)} & HP_*(A,D) & \xleftarrow{HP(i)} & HP_*(B,D) \\ \downarrow & & & & \uparrow \\ HP_1(B,D) & \xrightarrow{HP(i)} & HP_1(A,D) & \xrightarrow{HP(q)} & HP_1(I,D) \end{array}$$

حالت‌هایی خاص از این دنباله‌های دقیق قبلاً در مرجع‌های [۱۰] و [۱۶] به دست آمده‌بود. اینها یکی از ابزارهای اصلی در محاسبهٔ ناورداهای مانستگی دوری هستند.

نشاندن فضاهای کوانتمی در فضاهای هموار-توسیع‌ها و K-تئوری

در خلال سال‌ها (مثلاً [۳] و [۱۱] ، [۴] و [۶] را ببینید) محرز شده است که مهمترین مفهوم در توپولوژی ناجابجایی عبارت است از مفهوم توسیع. همچنانکه در بالا گفته شد، توسیع یک جبر، یک دنبالهٔ دقیق $0 \to I \to E \to A \to 0$ است که پیکان‌ها هم‌ریختی‌های جبرها هستند. به‌طور دوگان و شهودی چنین توسیعی متناظر با نشاندن فضای کوانتمی وابسته به A در فضای کوانتمی وابسته به E است.

برای توضیح نوع اطلاعات توپولوژیکی که در یک توسیع نهفته است، متذکر می‌شویم که محتوای قضیهٔ اندیس اَتیا-سینگر [۱] ممکن است به عنوان تعیین کلاس توسیع تعریف شده توسط عملگرهای شبه دیفرانسیل روی یک خمینه فشرده، تعبیر شود. دیگر قضیه‌های اندیس با توسیع‌های پیچیده‌تر مرتبط هستند.

اکنون می‌خواهیم به ترسیم یک ساختار کلی از K-تئوری توپولوژیک دومتغیره مبنی بر توسیع‌ها اقدام کنیم. این ساختار برای رسته‌های بسیاری از جبرهای ناجابجایی کار می‌کند و به‌خوبی در تعریف نظریهٔ دوری که طرحی از آن در بالا به دست داده شد، جا می‌گیرد. در نتیجه یک تبدیل طبیعی، مشخصهٔ چرن-کُنز دو متغیره، از K-تئوری توپولوژیک به نظریهٔ دوری وجود دارد.

به‌طور مشخص‌تر، از این به بعد فرض می‌کنیم، که همهٔ جبرهایمان جبرهای توپولوژیک با ساختاری تمام موضعاً محدب هستند که توسط یک خانواده از نیم‌نرمال‌ها (p_α) که در رابطه $p_\alpha(xy) \le p_\alpha(x)p_\alpha(y)$ برای هر x, y در جبر صدق می‌کند، داده می‌شوند.

برای هر چنین جبر موضعاً محدب A، جبر تانسوری $A \oplus A^{\otimes 2} \oplus A^{\otimes 3} + \ldots$ یک تکمیل‌شدهٔ طبیعی TA دارد که یک جبر موضعاً محدب است. یک همریختی ذاتی جبرها $TA \to A$ وجود دارد که $x_1 \otimes \ldots \otimes x_n$ را به حاصلضرب $x_1 x_2 \ldots x_n$ تصویر می‌کند. هستهٔ این همریختی را با JA نمایش

می‌دهیم، به‌این‌ترتیب یک تجزیهٔ آزاد برای A به‌صورت $0 \to JA \to TA \to A \to 0$ به‌دست می‌آید که می‌تواند به عنوان یک نشاننده از فضای کوانتمی وابسته به A به فضای کوانتمی هموار وابسته به TA تعبیر شود. این ایده‌آل با مکمل تصویر فضای کوانتمی برای A متناظر است. چون JA نیز یک جبر موضعاً محدب است، می‌توانیم با تکرار این روش $J^{۲}A = J(JA)$ و به‌طور استقرایی $J^{n}A = J(J^{n-۱}A)$ را بسازیم.

با یک جبر موضعاً محدب B، می‌توانیم جبر $M_{\infty}(B)$ متشکل از ماتریس‌های بینهایت $(b_{ij})_{i,j\in\mathbb{N}}$ را مرتبط کنیم که درایه‌های آنها در B سریعاً نزولی است. فضای کوانتمی متناظر شبیه مثال (۱) از مقدمه است. آن فضا دارای بینهایت نقطه است که به‌وسیله $\mathbb{N}$ نشاندار شده‌اند و نیز فلش‌های بین نقاط اندیس‌دار، که به‌وسیلهٔ همه اعضای ممکن B نشاندار شده‌اند. یک توسیع بنیادی، با به‌کاربردن عملگرهای شبه‌ـدیفرانسیل روی دایره، نشان می‌دهد که برای هر جبر A همریختی ذاتی $J^{۲}A \to M_{\infty}(B)$ وجود دارد. این نگاشت را می‌توان برای تشکیل حد استقرایی در تعریف زیر به‌کار برد.

فرض کنید A و B جبرهای موضعاً محدب باشند و $* = ۰, ۱$. تعریف می‌کنیم

$$KK_{*}(A,B) = \varinjlim_{K}[J^{۲k+*}A, M_{\infty}(B)]$$

که $[J^{۲k+*}A, M_{\infty}(B)]$عبارت است از مجموعهٔ کلاس‌های هموتوپی (مشتق‌پذیر) همریختی‌های $J^{۲k+*}A \to M_{infty}(B)$. $KK_{*}(A,B)$، با عمل جمع مستقیم عادی نگاشت‌ها در ماتریس‌ها، یک گروه آبلی است.

چون محاسبهٔ مانستگی Xـهمبافت یک صورت جبری از محاسبهٔ کلاس‌های هموتوپی است، این تعریف به‌طور قابل توجهی شبیه تعریف نظریهٔ دوری تناوبی در معادلهٔ (۱) از بخش قبلی است.

این دوـ تابعگر KK_{*} همان خواص مجرد HP^{*} را دارد (بخش قبل را ببینید). بالاخص:

- هر همریختی $\alpha : A \to B$ یک عضو $KK_{۰}(\alpha)$ را القا می‌کند.
- یک ضرب شرکت‌پذیر $KK_{i}(A,B) \times KK_{j}(B,C) \to KK_{i+j}(A,C)$ (که $i,j \in \mathbb{Z}_{۲}$، و A و B و C جبرهای موضعاً محدب هستند) وجود دارد که در هر دو متغیر جمعی است و در رابطهٔ $KK(\alpha)KK(\beta) = KK(\alpha,\beta)$ برای هر دو همریختی α و β صدق می‌کند.
- KK_{*} ناوردای هموتوپی است (تحت هموتوپی ناوردا است) و اصل کُندن را در هر دو متغیر ارضاء می‌کند (همچنانکه در بخش قبل توصیف شد). نگاشت ذاتی $B \to M_{\infty}(B)$ یک یکریختی در هر دو متغیر KK_{*} القا می‌کند.

در حقیقت می‌توان نشان داد که $KK_{۰}$ عبارت است از تابعگر جهانی از رستهٔ جبرهای موضعاً محدب مانند بالا به یک رستهٔ جمعی که در خاصیت سوم صدق می‌کند.

اگرچه این روش ساخت Kـتئوری واقعاً متفاوت از رویکرد معمولی است که افکنش‌ها یا مدول‌های افکنشی را به کار می‌برد، مشاهده می‌شود هنگامی‌که در حالت خاص متغیر اول را به یک نقطه تبدیل کنیم،

یعنی به جبر $\mathbb{C}$ از اعداد مختلط، $KK_*(\mathbb{C},B)$ چیزی جز Kـگروه معمولی در حالتیکه B یک جبر باناخ [۲] یا یک جبر فرشه[1] [۱۳] باشد، نیست (حالت‌هایی که در آنها Kـتئوری معمولی تعریف شده است).

یک خاصیت مهم دیگر این است که هر توسیع، یا به‌طورکلی‌تر هر توسیع $n-$"مرحله‌ای" به صورت $0 \to B \to E_1 \to \cdots \to E_n \to A \to 0$ عضوی از $KK_n(A,B)$ را به‌دست می‌دهد که n به پیمانهٔ ۲ شمرده می‌شود. در جبر همولوژی می‌توان یک ضرب مشهور روی این توسیع‌ها به‌نام ضرب یُنِدا را به‌کار برد که به‌طور ساده عبارت است از به هم بستن[2] دو توسیع از این نوع. این ضرب با ضرب $KK_n(A,B) \times KK_m(B,C) \to KK_{n+m}(A,C)$ سازگار است.

عملگرهای شبه دیفرانسیل روی یک خمینه هموار فشرده به یک توسیع $0 \to \Psi_{-1} \to \Psi_0 \to C^\infty(S^*M) \to 0$ منجر می‌شود که Ψ_0, Ψ_{-1} ترتیب جبرهای عملگرهای شبه دیفرانسیل از مرتبه‌های -1 و 0 هستند و $C^\infty(S^*M)$ عبارت است از جبر نگاشت‌های هموار روی کلاف هم‌کروی M. مسأله‌ای که به‌وسیله قضیهٔ اندیس اتیا‌ـسینگر حل شد دقیقاً عبارت است از تعیین کلاسی در $KK_1(C^\infty(S^*M),\Psi_{-1})$ که توسط این توسیع تعریف می‌شود.

مشخصهٔ دو متغیرهٔ چرن‌ـکُنز

مهمترین بخش در ساختن یک تبدیل دو متغیرهٔ ضربی از KK_* به نظریهٔ دو متغیرهٔ HP_* بر رسته جبرهای موضعاً محدب عبارت است از خاصیت جهانی بودن KK_0 که در پایان بخش قبلی بیان شد.

چون HP_0 خواصی را که KK_0 برای آنها جهانی است، داراست، فوراً تبدیل زیر را $Ch : KK_0(A,B) \to HP_0(A,B)$ که با حاصلضرب قابل مقایسه است، به‌دست می‌آوریم.

در کوشش برای گسترش این تبدیل به یک تبدیل ضربی از نظریهٔ $\mathbb{Z}_2$ـمدرج KK_* به HP_*، با این مسأله مواجه می‌شویم که حاصل‌ضرب دورهٔ فرد در KK_* و HP_* به صورت‌های مختلف تعریف می‌شوند. برای رفع این مشکل باید ضریب (تا اندازه‌ای به دلخواه) $\sqrt{2\pi i}$ را معرفی کرد. با این شرط تبدیل زیر که با عمومیت تمام ضربی است به‌دست می‌آید:

$$Ch : KK_*(A,B) \to HP_*(A,B)$$

هر دو نظریهٔ همانستگی دوری $HP^*(A)$ و Kـمانستگی $KK_*(A,\mathbb{C})$، چون به عنوان حدهای القایی تعریف می‌شوند، دارای یک پالایش (بُعدی) طبیعی هستند. به این پالایش بعدی در مقدمه به‌طور ضمنی اشاره شد.

رفتار این پالایش‌ها تحت شاخص چرن‌ـکُنز به‌خاطر بررسی خیلی ظریف نگاشت مرزی دنبالهٔ دقیق در مانستگی دوری توسط م. پوشینگ و ر. مِیِر به‌خوبی بررسی شده است. به‌ازای عضو α در $KK_*(A,\mathbb{C})$ ، بُعد $Ch(\alpha)$ دارای کران 3^d است که d بعد α در Kـتئوری است. این تخمین بهینه است. در پایان این مقاله، می‌خواهیم تأکید کنیم که علیرغم تعریف به‌ظاهر مجرد، ناورداهای نظریهٔ دوری و

1) Fréchet 2) splicing

Kـتئوری می‌توانند برای گسترهٔ بزرگی از جبرهای ناجابجایی به صورتی بسیار صریح محاسبه شوند. چند مثال نمادین در مقدمه توصیف شد.

مراجع

[1] M. F. ATIYAH and I. M. SINGER, the index of elliptic operators I,*Ann. of Math.* (2) **87** (1968), 484-530.

[2] B. BLACKADAR, *K-theory for Operator Algebras,* Springer-Verlag, Heidelberg-Berlin-New York-Tokyo, 1986.

[3] L. G. BROWN, R. G. DOGLAS, and P.FILLMORE, Extensions of C^*-algebras and K-homology, *Ann. of math.* 105 (1977), 265-324.

[4] A. CONNES, Non-commutative differential geometry, *Inst. Hautes Études Sci. Publ. Math.* **62** (1985), 257-360.

[5] ——, *Non-commutative Geometry*, Academic Press, London-Sydney-Tokyo-Toronto, 1994.

[6] J. CUNTZ, Bivariante K-theorie für lokalkonvexe Algebren und der bivariante Chern-Connes-Charakter, *Doc. Math.* J. DMV **2** (1997), 139-182; http://www.mathematik.uni-bielefeld.de/documenta/.

[7] J.CUNTZ and D. QUILLEN, Algebra extensions and nonsingularity, *J.Amer. Math. Soc.* **8** (1995), 251-289.

[8] ——, Cyclic homology and nonsingularity, *J.Amer. Math. Soc.* **8** (1995), 373-442.

[9] ——, Excision in bivariant periodic cyclic cohomology, *Invent. Math.***127** (1997), 67-98.

[10] T. G. GOODWILLIE, Cyclic homology and the free loopspace, *Topology* **24** (1985), 187-215.

[11] G. G. Kasparov, The operator K-functor and extentions of C^*-algebras (in Russian), *Izv. Akad. Nauk.* SSSR Ser. Mat. **44** (1980),571-636; Math. USSR Izv. **16** (1981), 513-572.

[12] V. NISTOR, A bivariant Chern-Connes character, *Ann. of Math.* **138** (1993), 555-590.

[13] C. PHILLIPS, K-theory for Fréchet algebras, Internat. J. Math. **2** (1991), 77-129.

[14] D. QUILLEN, Chern-Simons forms and cyclic cohomology, *the interface of Mathematics and Particle physics*, Claredon Press, 1990, pp. 117-134.

[15] B. TSYGAN, The homology of matrix Lie algebras over rings and the Hochschild homology (in Russian), *Uspekhi. Mat. Nauk* **38** (1983), 217-218; *Russian Math. Surveys* **38** (1983), 198-199.

[16] M. WODZICKI, Excision in cyclic homology and in rational algebraic K-theory, *Ann. of Math.* **129** (1989), 591-639.

سید محمدباقر کاشانی
دانشگاه تربیت مدرس، بخش ریاضی
پست الکترونیک: kashanim@net1c.modares.ac.ir

فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۸ (بهار ۱۳۸۱)، صص. ۴۱ تا ۵۲

روشهای احتمالاتی در حل مسائل دترمینیستیک

بیژن ظهوری زنگنه

چکیده

اثبات قضیه‌های احتمال بر اساس تکنیکهای آنالیز ریاضی را در اغلب قضیه‌های نظریهٔ احتمال دیده‌ایم. در این مقاله قصد داریم که جریان معکوس این پدیده را یعنی کاربرد روشهای تصادفی در حمله به مسائل آنالیز کلاسیک را بررسی کنیم. یکی از ابتدایی‌ترین مثالهای این روشها اثبات قضیهٔ تقریب وایراشتراس به‌وسیله احتمالات است. این روشها در حل مسائل نظریهٔ پتانسیل، مسألهٔ دیریشله و مسألهٔ شرایط مرزی مارتین نیز کاربرد دارد.

در این مقاله سعی خواهیم کرد با زبان شهودی و غیررسمی به بعضی از این کاربردها بپردازیم.

احتمال به روایت تاریخ

نظریهٔ احتمال در ابتدا و نیز پس از آن برای مدتی طولانی، عبارت بود از صورت آرمانی و تحلیل برخی از پدیده‌های زندگی واقعی در خارج از حیطهٔ ریاضیات، اما اندک اندک در نیمهٔ نخست این قرن احتمال ریاضی، بخشی معمولی از ریاضیات شد. تا قرن پانزدهم هیچگونه بررسی علمی در مورد پیشامدهای تصادفی انجام نشد. دانش پژوهان ایتالیایی لوکا با چولی (۱۴۴۵ـ۱۵۱۴)، نیکولا تارتاگلیا (۱۴۹۹ـ۱۵۵۷)، چرولاموکاردانو (۱۵۰۰ـ۱۵۷۱)، از جمله پیشکسوتان دانش ریاضی هستند که احتمالهای مربوط به بسیاری از بازیهای تصادفی را محاسبه کرده‌اند. به‌قول دیود مامفرد در مقالهٔ طلوع عصر روشهای تصادفی «اگر

جلوتر بیاییم، می‌بینیم که در عصر رنسانس، کاردانو شخصیت بی‌نظیری است. او به خاطر کتاب فن کبیرش (۱۵۴۵) غالباً مبدع i خوانده می‌شود. ظاهراً وی یکی از خبره‌ترین افراد در زمینهٔ عملیات صوری جبر بود به‌طوری که تبعات قواعد منطقی جبر را یک گام فراتر از اسلاف خویش برد. ولی او در عین حال، معتاد به قمار هم بود و در کتاب «بازیهای شانسی» خود نخستین تحلیل را از قوانین شانس ارائه کرد، اما خجالت می‌کشید آن را انتشار دهد و این کتاب تا ۱۶۶۳ به چاپ نرسید، یعنی تقریباً مقارن با زمانی که یاکوب برنولی کار خود را آغاز کرد.» (مامفرد [۱۵]). به هر حال پیشرفت واقعی در فرانسه از سال ۱۶۵۴ آغاز شد، از وقتی بلز پاسکال (۱۶۲۳ـ۱۶۶۲) و پیردو فرما (۱۶۰۱ـ۱۶۶۵) دو ریاضیدان نامی نامه‌هایی به یکدیگر رد و بدل کردند که در این نامه‌ها در مورد روشهای کلی محاسبهٔ احتمالها بحث کرده‌اند. در سال ۱۶۵۵ دانشمند معروف آلمانی کریستین هویگنس (۱۶۲۹ـ۱۶۹۵) به آنها پیوست، و این همکاری بسیار پر ثمر بود. در سال ۱۶۵۷ هویگنس اولین کتاب دربارهٔ احتمال را تحت عنوان «دربارهٔ محاسبات بازیهای شانسی» نوشت. این کتاب به منزلهٔ تولد واقعی احتمال محسوب می‌شود.

بعد از این تمام غول‌های ریاضی مانند برنولی، لاپلاس، پواسن و گاوس که استادان وقت در رشته‌های دیگر ریاضی بودند، قضیه‌های غلط و یا کم دقتی را در احتمال ثابت کردند تا اینکه در سال ۱۹۰۰ در کنگرهٔ بین‌المللی ریاضیدانها در پاریس، دیوید هیلبرت (۱۸۶۳ـ۱۹۴۳) ۲۳ مساله را که به عقیدهٔ او حل آنها در پیشرفت ریاضیات مؤثر بود پیشنهاد کرد. یکی از این مسایل، بحث اصول موضوعی نظریهٔ احتمال بود. در راستای رسیدن به این هدف کارهایی به وسیله امیل بورل (۱۸۷۱ـ۱۹۵۶)، و برنشتاین (۱۸۸۰ـ۱۹۶۸) انجام شد، تا اینکه در سال ۱۹۳۳ اندری کولموگورف (۱۹۰۳ـ۱۹۸۷) به صورتی موفقیت‌آمیز نظریهٔ احتمال را اصل موضوعی کرد.

نظریهٔ احتمال کلموگرف بر اساس نظریهٔ اندازه لبگ (۱۹۰۲) بنیان گذاشته شد. کلموگرف در نخستین صفحات تک‌نگاشت مشهور خود دربارهٔ نظریهٔ احتمال صراحتاً می‌گوید که متغیرهای تصادفی حقیقی مقدار، همان توابع اندازه‌پذیرند و امیدهای ریاضی انتگرالهای آنها معهذا، اندازه‌پذیری یک تابع حقیقی مقدار را تعریف می‌کند و وقتی که می‌خواهد امید ریاضی یک متغیر تصادفی را تعریف کند صاف و ساده نمی‌گوید که این مقدار برابر است با انتگرال متغیر تصادفی نسبت به اندازهٔ احتمال مفروض، بلکه انتگرال را نیز تعریف می‌کند (دوب [۱۲]) این سنت در اغلب کتب نظریهٔ احتمال باقی مانده است (به‌عنوان مثال رجوع شود به [۵]).

کلموگورف در تک‌نگاشت خود مطالب بسیار مهمی را مطرح کرد. او فضای احتمال، ساختن فرآیند تصادفی روی فضای بینهایت بعدی احتمال و امید شرطی نسبت به یک میدان سیگمایی را معرفی کرد. فهم قضیهٔ توسیع کلموگرف روی فضای بینهایت بعدی مدتها برای بسیاری از ریاضیدانها مشکل بود. جوزف دوب از بنیان‌گذاران احتمال در آمریکا می‌گوید:

«نویسنده به یاد می‌آورد که منظور کولموگروف از اندازه روی فضای تابعی را تا زمانی دراز پس از آنکه تک‌نگاشت وی را خوانده بود، در نمی‌یافته است» [۱۲].

این رویکرد مورد توجه و توافق اغلب احتمال‌دانها قرارگرفت. تا جایی که خیلی از احتمال‌دانها احتمال را جزیی از آنالیز می‌دانند. دوب می‌گوید «برخی ریاضیدانان بر آنند که هرگاه با خواص تحلیلی احتمال و امید ریاضی سر و کار داشته باشیم، موضوع بخشی از آنالیز است، ولی اگر با دنباله‌های نمونه‌ای و توابع نمونه‌ای سر و کار داشته باشیم، موضوع عبارت است از احتمال، نه آنالیز. این مؤلفان در موقعیت جالب توجهی هستند از این رو که در نظرکردن به تابع دو متغیرهٔ $(t,\omega) \to x(t,\omega)$ مثلاً در فرآیندهای تصادفی اگر خانوادهٔ توابع $x(t,.)$ هنگامی که t تغییر می‌کند مورد مطالعه باشد آن را آنالیز می‌خوانند، ولی اگر خانوادهٔ توابع $x(.,\omega)$ هنگامی که ω تغییر می‌کند مورد بررسی باشد آن را احتمال می‌نامند و قطعاً آنالیز به حساب نمی‌آورند. دقیقتر بگوییم، ایشان بحث پیرامون توزیعها و پرسشهای مربوطه را آنالیز می‌دانند، اما بحثهای به زبان توابع نمونه‌ای را آنالیز نمی‌دانند. این دیدگاه در قول ذیل بیان شده است.

پروتر: ایتو[1] در سال ۱۹۴۴، با ارائهٔ انتگرالش که در آن فرآیندهای تصادفی انتگرال بودند، توانست بخش چند بعدی را با تکنیکهای احتمالاتی محض مورد بررسی قرار دهد، که نسبت به روشهای آنالیز فلر بهتر است» [۱۲].

در هر حال دوب این ایده را که احتمال مستقل از آنالیز باشد قبول ندارد و در آخر این مقاله با آوردن استدلالی درباره توابع رادماچر[2]، و قضیهٔ پل لوی می‌نویسد:

«دیگر بر عهدهٔ خواننده است که داوری کند کدامیک از این نتایج نظریهٔ اندازه‌ای است و کدام یک احتمالاتی، و آیا اصلاً بیرون راندن احتمال ریاضی از قلمرو آنالیز فایده‌ای دارد، و اگر دارد، آیا نظریهٔ اندازه را هم نباید بیرون راند؟» [۱۲].

در مقابل رهیافت دوب، رهیافت دیگری است که به‌وسیله دیوید مامفرد مطرح می‌گردد که معتقد است که «رهیافت دیگر آن است که مفهوم «متغیر تصادفی» در مرکز توجه قرار بگیرد و همه کارها با انواع و اقسام دستکاری در متغیرهای تصادفی انجام شود.» مامفرد [۱۵].

دیوید مامفورد در مقالهٔ «طلوع عصر روشهای تصادفی» می‌خواهد ریاضی جدیدی به‌وجود آورد. او می‌نویسد «در رهیافت تقلیل‌گرا، متغیر تصادفی برحسب اندازه تعریف می‌شود که خود برحسب نظریهٔ اعداد حقیقی تعریف می‌شود، و این را هم نظریهٔ مجموعه‌ها تعریف می‌کند که خودش بر اساس حساب محمولات تعریف می‌شود. در عوض من می‌خواهم بگویم که باید علی‌الاصول بتوان متغیرهای تصادفی را در مبانی منطق و ریاضیات ادغام کرد و به صورتبندی شفافتر و کاملتری از دیدگاه تصادفی رسید. من خودم هنوز صورتبندی کامل و قطعی از این قضیه ندارم».

در هر حال چه ما مانند «دوب» نظریهٔ احتمال را جزئی از آنالیز بدانیم چه مانند «دیوید مامفرد» قصد داشته باشیم ریاضی جدیدی با تغییر در مبانی آن به‌وجود آوریم و یا مانند پروتر بخشی را آنالیز و بخشی را احتمال بنامیم، این مسأله مسلم است که نظریهٔ احتمال کاملاً آغشته به آنالیز است و بر اساس آن توسعه یافته است حال چه بخواهد در درون آنالیز باقی بماند و چه از آن خارج شود. روشهای تصادفی دارای شهود ویژه خود است که در بقیهٔ قسمتهای آنالیز وجود ندارد. این شهود باعث مطرح شدن مسائل زیادی

1) Ito 2) Rademacher

در احتمال گشته و منبع گسترش آن است. در اغلب مسائل برای اثبات قضیه‌های احتمال از آنالیز کمک می‌گیریم. در این مقاله قصد داریم برای اثبات مسائل کلاسیک آنالیز از روشهای تصادفی کمک بگیریم و آنها را اثبات کنیم. بنابراین با نگاه یک احتمال دان به اشیاء آنالیز ریاضی می‌پردازیم.

نگاه احتمالاتی به آنالیز کلاسیک

بازهٔ بستهٔ $[۰,۱]$ را در نظر بگیریم. می‌خواهیم به این بازهٔ دترمینیستیک با تعبیر احتمالی جان تازه‌ای بدمیم.

امیل بورل در سال ۱۹۰۹ هر $x \in [۰,۱]$ را به‌صورت بسط دودوئی

$$x = ۰.x_۱, x_۲, \ldots$$

نوشت که رقم x_j یا صفر است یا یک: این رقمها توابعی از x هستند. «اگر بازهٔ $[۰,۱]$ را با اندازهٔ لبگ در نظر بگیریم که یک اندازهٔ احتمال بر این بازه است، این تابعها به شکل معجزه آسایی متغیرهایی تصادفی می‌شوند که دقیقاً همان توزیعهایی را دارند که در محاسبهٔ احتمالات پرتاب سکه به‌کار می‌روند. یعنی ۲^{-n} برابر است با احتمال منسوب به این رویداد که در یک آزمایش پرتاب سکه نخستین n پرتاب دنبالهٔ معینی از شیر و خط به دست بدهد، و ۲^{-n} همچنین طول کل (مساوی اندازهٔ لبگ) تعدادی متناهی بازه است که نقاط متعلق به آنها بسطهایی دودویی با دنباله‌ای مشخص از صفرها و یکها در n جایگاه خاص دارند.» (دوب [۱۲]). با این دید بازهٔ $[۰,۱]$ فضای نمونه‌ای آزمایش برنولی است (رجوع شود به [۱]).

از بسط دودویی بالا و آزمایش برنولی یعنی پرتاب مستقل بینهایت بار سکه، می‌توان نشان داد که $\frac{x_۱+x_۲+\cdots+x_n}{n}$ به $\frac{۱}{۲}$ میل می‌کند. «ولی بیان قویتری از قانون اعداد بزرگ حکمی بود که بورل به‌دست آورد ـ طی یک برهان اشتباه و غیرقابل تصحیح ـ که این دنباله از میانگینها به ازای تقریباً هر x به $\frac{۱}{۲}$ میل می‌کند (با احتمال ۱). یک سال بعد فیبر[1] برهان درستی برای این حکم ارائه کرد و از آن هنگام برهانهای بسیار ساده‌تری هم به دست آمده‌اند، [۱۳, ۵, ۴, ۳]. فرشه، حرمت بورل را نگه داشت: «برهان بورل بیش از حد کوتاه است. در آن چندین استدلال میانی حذف شده است و نیز احکامی بدون برهان فرض شده‌اند» [۱۲].

با استفاده از قضیهٔ قانون قوی اعداد بزرگ برای دنباله‌های برنولی می‌توان به اثبات سادهٔ برنشتین از قضیهٔ وایراشتراس برای تقریب توابع پیوسته با چند جمله‌ای‌ها دست یافت.

فرض کنیم $f = f(x)$ یک تابع پیوسته روی بازهٔ $[۰,۱]$ باشد. ثابت می‌کنیم f حد یکنواخت چندجمله‌ایهای برنیشتین به‌صورت زیر است:

$$B_n(x) = \sum_{k=۰}^{n} f(k/n) C_n^k x^k (۱-x)^{n-k}$$

1) Faber

برهان. فرض کنیم $X_1, X_2, \ldots, X_n$، دنباله‌ای از متغیرهای تصادفی (i.i.d.) برنولی با

$$P\{X_i = 1\} = x, \ P\{X_i = 0\} = 1 - x$$

باشد و $S_n = X_1 + X_2 + \cdots + X_n$، آنگاه

$$\begin{aligned} E(f(\tfrac{S_n}{n})) &= \sum_{k=0}^{n} f(\tfrac{S_n}{n}) P\{S_n = k\} \\ &= \sum_{k=0}^{n} f(k/n) C_n^k x^k (1-x)^{n-k} \\ &= B_n(x). \end{aligned}$$

چون تابع f روی $[0, 1]$ پیوسته است، پیوستهٔ یکنواخت است و بنابراین برای هر $t > 0$، $\delta > 0$ وجود دارد طوری که

$$|x - y| \leq \delta \Rightarrow |f(x) - f(y)| \leq t$$

اما تابع f پیوسته و درنتیجه کراندار است، در نتیجه یک M چنان وجود دارد که برای هر x

$$|f(x)| \leq M < \infty$$

با به‌کار بردن این نامساوی داریم

$$\begin{aligned} |f(x) - B_n(x)| &= |\sum_{k=0}^{n} f(x) C_n^k (1-x)^{n-k} \\ &\quad - \sum_{k=0}^{n} f(k/n) C_n^k x^k (1-x)^{n-k}| \\ &= |\sum_{k=0}^{n} (f(x) - f(k/n)) C_n^k x^k (1-x)^{n-k}| \\ &\leq \sum_{k=0}^{n} |f(x) - f(k/n)| C_n^k x^k (1-x)^{n-k} \\ &= \sum_{\{k : |k/n - x| \leq \delta\}} |f(x) - f(k/n)| C_n^k x^k (1-x)^{n-k} \\ &\quad + \sum_{\{k : |k/n - x| > \delta\}} |f(x) - f(k/n)| C_n^k x^k (1-x)^{n-k} \\ &\leq \epsilon \sum_{k=0}^{n} C_n^k x^k (1-x)^{n-k} \\ &\quad + 2M \sum_{\{k : |k/n - x| > \delta\}} C_n^k x^k (1-x)^{n-k} \end{aligned}$$

حال چون برای $n \geq 1$، $0 \leq k \leq n$، جرم احتمال در نقطهٔ k احتمال دوجمله‌ای زیر است:

$$P_n(k) = C_n^k x^k (1-x)^{n-k}$$

بنابراین

$$\sum_{\{k : |k/n - x| > \delta\}} P_n(k) = P\{|\frac{S_n}{n} - x| > \delta\}$$

در نتیجه

$$|f(x) - B_n(x)| \le \epsilon + ۲MP\{|\frac{S_n}{n} - x| > \delta\} \qquad (*)$$

اما چون برای هر متغیر تصادفی ξ داریم

$$P\{|\xi - E(\xi)| \ge \epsilon\} \le \frac{V(\xi)}{\epsilon^۲}$$

و در حالت $\xi = \frac{S_n}{n}$، $E(\xi) = x$ و

$$Var(\frac{S_n}{n}) = \frac{Var(S_n)}{n^۲} = \frac{nx(۱-x)}{n^۲} = \frac{x(۱-x)}{n}$$

بنابراین

$$P\{|\frac{S_n}{n} - x| > \delta\} \le \frac{Var(\frac{S_n}{n})}{\delta^۲} = \frac{x(۱-x)}{n\delta^۲} \le \frac{۱}{۴n\delta^۲}$$

در نتیجه داریم

$$\begin{aligned} |f(x) - B - n(x)| &\le \epsilon + ۲MP\{\tfrac{S_n}{n} - x| > \delta\} \\ &\le \epsilon + ۲M\tfrac{۱}{۴n\delta^۲} \\ &= \epsilon + \tfrac{M}{۲n\delta^۲} \end{aligned}$$

و بنابراین

$$\lim_{n\to\infty} \max_{۰\le x\le ۱} |f(x) - B_n(x)| = ۰$$

که نتیجهٔ قضیهٔ وایرشتراس است.

یکی از کاربردهای جالب احتمالات در آنالیز قضیهٔ (Szegö) است برای اثبات آن می‌توان به ([۱] صفحه ۱۶۷) رجوع کرد.

یکی از کاربردهای مهم احتمالات در آنالیز کلاسیک اثبات قضیهٔ رادن-نیکودیم به‌وسیله مارتینگل‌ها است. چون ما معمولاً احتمال و امید شرطی را به‌وسیله قضیهٔ رادن-نیکودیم تعریف می‌کنیم این نظریهٔ مارتینگل‌ها است که بر اساس این قضیه استوار می‌گردد. اما اثبات قضیهٔ رادن-نیکودیم به‌وسیله مارتینگل‌ها چندان هم غیرمنتظره نیست، برای دیدن این قضیه رجوع کنید به [۱۳].

آخرین مسألهٔ دترمینیستیک که ما می‌خواهیم در این مقاله به آن بپردازیم مسألهٔ دیریشله است. این مسأله یکی از مسأله‌های مهم نظریهٔ معادلات دیفرانسیل پاره‌ای بیضوی است و نظریهٔ پتانسیل دیریشله به‌حساب می‌آید.

مسألهٔ دیریشله

فرض کنیم D یک میدان در $\mathbb{R}^n$ باشد. فرض کنیم تابع f روی مرز D تعریف شده باشد می‌خواهیم ثابت کنیم یک تابع هارمونیک u روی میدان D چنان موجود است که $u|_{\partial D} = f$.

اثبات وجود این مسأله با روش‌های دترمینیستیک پیچیده است و تنها وجود جواب را می‌توان ثابت کرد. در صورتی که در راه‌حل احتمالاتی که ارائه می‌دهیم نه تنها وجود جواب را ثابت می‌کنیم بلکه فرمولی برای جواب نیز ارائه می‌دهیم. اثبات با روشهای احتمالاتی این قضیه بر اساس آنالیز تصادفی و خواص حرکت برونی است. در بند بعد ما به‌طور شهودی و توصیفی درباره حرکت برونی و خواص آن صحبت می‌کنیم و سپس مسألهٔ دیریشله را ثابت می‌کنیم. برای مطالعه عمیق حرکت برونی و خواص آن رجوع کنید به [۷, ۱۰].

حرکت برونی و مسألهٔ دیریشله

حرکت برونی نامی است که به حرکت نامنظم گردهٔ گیاهان که در آب معلق هستند داده شده است. رابرت براون گیاه‌شناس معروف انگلیسی برای اولین بار در ۱۸۲۸ با مشاهدهٔ این حرکت، متوجه اهمیت آن در مطالعهٔ ذرات معلق میکروسکوپی شد. پس از آن دامنهٔ کاربرد حرکت برونی از مطالعهٔ ذرات معلق میکروسکوپی بسیار فراتر رفته است و شامل مدل‌سازی قیمتهای سهام، نوفهٔ حرارتی در مدارهای الکتریکی، برخی حالتهای حدی در سیستمهای صف و موجودی و اختلالات تصادفی در انواع دیگر از سیستمهای فیزیکی، زیستی، اقتصادی و مدیریت شده است.

آنچه براون در ابتدا مشاهده نمود این بود که گرده‌های گیاهان درون مایع دارای حرکت‌اند و علاقه‌مند شد تا قانون و علت این حرکت را بیابد، اما از عهده این کار برنیامد و مسأله بدون پاسخ باقی ماند. سپس در سال ۱۹۰۶ میلادی، اینشتین موفق به حل مسأله شد و علت حرکت را بمباران دانه‌های گرده توسط ملکولهای مایع معرفی نمود. با این حال اولین مدل ریاضی حرکت برونی در تز دکتری ریاضی بشلیه[1] در سال ۱۹۰۰ میلادی در دانشگاه پاریس و برای مدل اقتصادی مطرح شد.

بشلیه توزیع‌های مهم متعددی استخراج کرده بود که همگی به فرآیند حرکت براونی در $\mathbb{R}$ مربوط بودند، «از جمله توزیع مربوط به تغییر بیشینه در طول یک بازهٔ زمانی. بدین منظور وی توزیعهای متناظر با یک قدم زدن تصادفی گسسته را پیدا می‌کرد و سپس حد را هنگامی که طول قدمها به سمت صفر میل می‌کرد به‌دست می‌آورد. دقیقتر بگویم، آنچه بشلیه استخراج نمود توزیعهایی بودند که برای فرآیند حرکت برونی کارایی داشتند، به فرض آنکه اصلاً چیزی تحت عنوان حرکت برونی وجود داشته باشد، و به فرض اینکه بشود آن را با آن قدم زدنهای تصادفی تقریب زد.» [۱۲]

پس از آن نوربرت وینر ریاضیدان برجسته و نابغهٔ قرن بیستم در سال ۱۹۱۸ مدل ریاضی این حرکت را به‌طور کامل بررسی کرد. «توجه کنید که شکی در وجود حرکت برونی نیست: حرکت برونی را می‌شود زیر میکروسکوپ نظاره کرد. ولی هنوز برهانی برای وجود یک فرآیند تصادفی، یک حساب ریاضی، با خواص مطلوب در دست نبود. وینر (۱۹۲۳) فرآیند مطلوب حرکت برونی را که امروزه گاه فرآیند وینر نامیده می‌شود ساخت. بدین منظور وی از رهیافت دانیل به نظریهٔ اندازه استفاده کرد تا اندازه‌ای با خواص ذیل

1) Bachelier

برفضای S از توابع پیوسته به دست آورد: اگر $X(t,.)$ متغیری تصادفی باشد که با مقدار یک تابع در S در زمان t تعریف شده باشد، فرآیند تصادفی این متغیرهای تصادفی فرآیندی تصادفی است با اعضای S به‌عنوان توابع نمونه‌ای، و با توزیعهای توأمی که برای فرآیند حرکت برونی داشتیم به‌عنوان توزیعهای توأم متغیر تصادفی» [۱۲]

ریاضیدانان زحمت برای تولید یک نظریهٔ عمیق ریاضی می‌کشند اما متأسفانه آنچه باقی می‌ماند نتیجهٔ این نظریه به صورت یک مقاله است، همانطور که ۷۵ ریاضیدان در سال ۱۹۶۲ در بیانیه‌ای در مورد تدریس ریاضی اعلام کردند: «تفکر ریاضی تنها استدلال استنتاجی نیست، همچنین اثبات صورت صرف هم نمی‌باشد. فرآیندهای ذهنی و فکری که اثبات و چگونگی اثبات را ارائه می‌کنند همانند خود اثبات که نتیجهٔ تفکر ریاضی است بخشی از تفکر ریاضی محسوب می‌شود. استخراج مفاهیم درست از وضعیت‌های محسوس و ملموس، تعمیم از حالات شهود، استدلال استقرایی، استدلال از طریق تمثیل، زمینه‌های شهودی که برای آشکارکردن یک حدسیه به‌کار می‌روند همگی سبک و طریقه ریاضی گونهٔ تفکر است.» [۱۲] خوشبختانه نوربرت وینر با نوشتن کتابهای توصیفی مانند «من یک ریاضیدان هستم» پشت پردهٔ تفکر و فرآیند به‌وجود آوردن یک نظریه را تا اندازه‌ای بررسی کرده است، بنابراین داستان حرکت برونی را از زبان نوربرت وینر می‌شنویم. وینر در M.I.T. استخدام شده بود: «ساختمان M.I.T. در ساحل رودخانهٔ چارلز ساخته شده بود و طوری قرار داشت که می‌شد مستقیماً از پنجره‌های آن، از چشم‌انداز گستردهٔ سرزمین زیبای دور و بر آن لذت برد، به‌خصوص وجود رودخانه، موجب شادی بود. به‌نظر می‌رسید که می‌توان از بام تا شام به تماشای ناز و کرشمه‌های عجیب و غریب آب نشست. ولی آن چه در میان این همه زیبایی مرا به طرف خود می‌کشید، ریاضیات و فیزیک بود. آن قانون‌مندی‌های ریاضی، که همه این تودهٔ بی‌نظم و ناآرام آب را هدایت می‌کند، کدام است؟ مگر اهمیت اصلی ریاضیات در این نیست که می‌تواند نظم و ترتیبی را که زیر این هرج و مرج و نابسامانی ظاهر دور و بر ما پنهان شده است، پیدا کند؟ رودخانهٔ چارلز، گاهی ناگهان از موج‌های بلند، با شانه‌های بلندکف، پوشیده می‌شود و گاه چنان چین خوردگی ملایمی دارد که به زحمت می‌توان موج‌های کوتاه آن را دید. طول موج‌های آن، گاه از دو یا سه بند انگشت تجاوز نمی‌کند و گاه به چند متر می‌رسد. چگونه می‌توان بیان ریاضی همهٔ این پدیده‌ها را داد؟ از چه دستگاهی باید استفاده کنیم تا در تنوع بی‌پایان جزئیات این منظره غرق شویم؟ برایم روشن بود که این مسئله، با مسألهٔ میانگین آماری بستگی دارد که با انتگرال لبگ خویشاوند است.» ([۱۶] صفحهٔ ۴۱).

وینر در کتاب خود به آشنایی با آثار ویلارد گیبس، اشاره می‌کند: «یکی از بزرگ‌ترین دانشمندان آمریکایی است که در واقع رشتهٔ تازه‌ای از دانش را پایه گذاشت، رشته‌ای که در حد فاصل فیزیک و ریاضیات قرار دارد» ([۱۶] صفحه ۴۲). «گیبس آثار بسیار جالبی هم در فیزیک و هم در ریاضیات دارد، ولی کارهای اساسی او در زمینهٔ مکانیک آماری، بیش از هر چیز دیگری برایم جالب بود، همین کارهای او بود که، تا حد زیادی، مسیر خاص زندگی مرا مشخص کرد.»

دیدگاه سنتی در فیزیک، که از نیوتون بزرگ سرچشمه می‌گیرد، بستگی خلل‌ناپذیری با تصورهای

دترمینیستیکی دارد و، بر طبق آن، معرفت دقیق چگونگی جهان و یا هر قسمت بسته‌ای از آن در یک لحظهٔ معین، شامل معرفت دقیق آن در زمان‌های بعدی هم می‌باشد. بنابر تصور اصلی نیوتون، اگر موقعیت و سرعت ذره‌ها را در موج‌های سطح رودخانهٔ چارلز بدانیم، می‌توان حرکت این موج‌ها را در همهٔ سده‌های آینده محاسبه کرد. متأسفانه با وسیله‌های اندازه‌گیری که در اختیار داریم، و همهٔ آن با دستهای آدمی ساخته شده‌اند، نمی‌توانیم مقادیر مطلقاً دقیق و سرعت همهٔ ذرّه‌ها را، در لحظهٔ اولین زمان، به‌دست آوریم. به این ترتیب، فیزیک، که باید عملاً به درد پدیده‌های طبیعت بخورد، ناگزیر مواجه با مشکلی می‌شود: چگونه می‌توان با تکیه بر این داده‌های تقریبی مربوط به وضع اولیه، که به کمک وسیله‌های موجود به دست می‌آیند، دربارهٔ واقع امر قضاوت کرد؟» ([۱۶] صفحه ۴۳).

با این ایده وینر فضای نمونه‌ای را فضای توابع پیوسته یا در واقع فضایی که هر عضو آن یک موج باشد در نظر گرفت. متغیر تصادفی از فضای توابع پیوسته $\Omega = C[۰, T]$ به اعداد حقیقی تعریف شده بود. دراینجا وینر مفهوم مهمی را کشف کرده بود، توابعی که روی فضایی تعریف می‌شوند که دامنهٔ آن نقطه (در فضای چندبعدی) نیست بلکه دامنهٔ آن یک فضای بینهایت بعدی است. خود می‌گوید «به تعمیم مفهوم احتمال، در مواردی مربوط می‌شود که «حالت‌های ممکن» را نمی‌توان به‌صورت نقطه‌های یک صفحه یا حوزه‌ای از فضا در نظر گفت، ولی خصلت منحنی‌هایی را دارند که معرف اشیای متحرکی هستند.» ([۱۶] صفحه ۴۴).

به این ترتیب، حرکت برونی موقعیتی را در برابر ما قرار می‌دهد که در آن، ذره‌ها به رسم منحنی‌هایی مشغول‌اند، و این منحنی‌ها، به مجموعه‌ای آماری از منحنی‌ها تعلق دارند. «این حرکت، بهترین زمینه برای اندیشه‌های من در مورد به‌کار بردن انتگرال‌گیری لبگ در فضای منحنی‌ها بود. و ضمناً دارای این خصوصیت بود که موضوع آن، از لحاظ فیزیکی، به دنیای واقع مربوط می‌شد و دقیقاً به اندیشه‌های گیبس بستگی داشت. در واقع، در این جا بود که توانستم با به‌کار بردن نظرات خود در تعمیم نظریهٔ انتگرال‌گیری، به موفقیت بزرگی برسم. خود حرکت برونی، موضوعی نبود که در فیزیک، بدون بررسی باقی مانده باشد. ولی در کارهای اساسی و عمیقی که اینشتین و سمولوخوفسکی در این زمینه کرده‌اند، یا به رفتار یک ذره در یک لحظهٔ زمانی ثابت پرداخته‌اند و یا به خصلت‌های آماری مجموعهٔ بزرگی از ذره‌ها در جریان زمان: ولی خاصیت‌های ریاضی خط سیر ذره‌های جداگانه، هیچگاه مورد مطالعه قرار نگرفته بود.» در مورد موضوع اخیر، تقریباً هیچ چیز روشن نبود، البته اگر اظهار نظر عمیق یه رن فیزیک دان فرانسوی، را که در کتاب خود به‌نام «اتم‌ها» آورده است، به‌حساب نیاوریم. او می‌گوید: «خط سیر به‌کلی بی‌نظم ذره‌ها، که در اثر حرکت برونی به وجود می‌آید، آدمی را به یاد منحنی‌های پیوستهٔ ریاضی دانان می‌اندازد که در هیچ نقطهٔ خود مشتق نداشته باشند» ([۲۶]، صفحه ۴۸ و ۴۹).

«با کمال تعجب، و در عین حال لذت، دریافتم که با چنین درکی از حرکت برونی، می‌توان نظریهٔ صوری آن را در حد بالایی از کمال و ظرافت تنظیم کرد. در چارچوب این نظریه توانستم ملاحظهٔ یه‌رن را ثابت کنم که، به استثنای چند موردی که احتمال آن در مجموع برابر صفر است، مسیرهای حرکت برونی،

منحنی‌های پیوسته‌ای هستند که در هیچ جا مشتق ندارند» ([۱۶] صفحه ۴۹).

بدین ترتیب وینر در سال (۱۹۲۳) از خاصیت گاوسی بودن حرکت برونی استفاده می‌کند و حرکت برونی را به‌صورت یک سری (فوریه) با پایهٔ دنباله‌های توابع شاودر، و ضرایب متغیرهای تصادفی گوسی می‌سازد. حرکت برونی بعدها با اصلاحاتی به‌وسیله پل‌لوی در سال (۱۹۴۸) و چیشلسکی (۱۹۶۱) به‌صورت ساده تری ساخته می‌شود (برای این روش رجوع کنید به لامپرتی [۸]). حرکت برونی یک فرآیند تصادفی است که دارای خاصیت مارکفی، گوسی، مارتینگلی، با نموهای ایستا و مستقل است. دارای مسیرهای پیوسته‌ای است که در هیچ نقطه‌ای مشتق ندارد.

حال به حل مسألهٔ دیریشله می‌پردازیم. با توجه به این واقعیت که حرکت برونی دارای خاصیت قوی مارکف نیز می‌باشد، یعنی اگر B_t یک حرکت برونی و T یک زمان توقف باشد آنگاه فرآیند جدید $B_{T+t} - B_T$ یک حرکت برونی جدید است. حرکت برونی یک مارتینگل موضعی است یعنی اگر T یک زمان توقف باشد آنگاه $B_{T\wedge t}$ (که در اینجا $T \wedge t$ می‌نیمم t و T است) یک مارتینگل است.

فرض کنیم D یک مجموعهٔ فشردهٔ نسبی باشد، یعنی $\bar{D}$ فشرده باشد. قرار می‌دهیم

$$\tau_D = \inf\{t : B_t \in D^c\}$$

یعنی زمان برخورد حرکت برونی با مرز مجموعهٔ D یا اولین زمانی که حرکت برونی می‌خواهد از مجموعهٔ D خارج شود. می‌توان ثابت کرد که τ_D یک زمان توقف است، توجه شود که τ_D متناهی است. یعنی حرکت برونی با احتمال ۱ از مجموعهٔ D خارج می‌شود. اگر f تابعی باشد که روی D تعریف شده است آنگاه $f(B_t)$ فقط برای $t < \tau_D$ تعریف شده است.

قضیه: فرض کنیم f یک تابع هارمونیک در D باشد (یعنی $\triangle f = ۰$ در D) و فرض کنیم $B_۰ = x \in D$ (یعنی حرکت برونی در لحظه صفر در نقطه x باشد). آنگاه $f(B_t)$ یک مارتینگل موضعی است.

برهان: با استفاده از آنالیز تصادفی و فرمول ایتو [۷, ۹, ۱۰, ۱۴] داریم

$$\begin{aligned} f(B_t) = f(x) &+ \int_۰^t \bigtriangledown f(B_s) dB_s \\ &+ \tfrac{۱}{۲} \int_۰^t \triangle f(B_s) ds \end{aligned}$$

چون f هارمونیک است، $\triangle f = ۰$ و از آنجا

$$f(B_t) = f(x) + \int_۰^t \bigtriangledown f(B_s) dB_s$$

چون انتگرال تصادفی یک مارتینگل است، نتیجه برقرار است .

قضیه (مسألهٔ دیریشله)

فرض کنیم D یک میدان باشد که در آن برای تمام xها

$$P^x(\tau_D < +\infty) = ۱$$

و گیریم f یک تابع مثبت برل اندازه‌پذیر باشد. تابع $h(x) := E^x(f(B_{\tau_D}))$ را در نظر می‌گیریم، اگر x موجود باشد که $h(x) < +\infty$ آنگاه h روی D هارمونیک است.

تبصرهٔ ۱. توجه کنید P^x و E^x، احتمال و امید شرطی به شرط $\{B_۰ = x\}$ (یعنی حرکت برونی در لحظهٔ صفر در نقطه x) باشد.

تبصرهٔ ۲. در اینجا فرمول صریح $h(x) := E^x(f(B_{\tau_D}))$ حل مسألهٔ دیریشله را به ما می‌دهد.

برهان. گیریم $x \in D$ و گیریم V گویی به مرکز x باشد که $\bar{V} \subset D$ قرار می‌دهیم

$$\tau_v = \inf\{t : B_t \in \partial V\}$$

اگر $x = B_۰$، آنگاه $\tau_v < \tau_D$. لذا

$$\begin{aligned} E^x(f(B_{\tau_D})) &= E^x(E(f(B_{\tau_D})|\mathcal{F}_{\tau_v})) \\ &= E^x(E(f(B_{\tau_D})|B_{\tau_v})). \\ &= h(B_{\tau_v}) \end{aligned}$$

بنابراین $h(x) = E^x(h(B_{\tau_v}))$. اما حرکت برونی نسبت به دوران ناوردا است، لذا B_{τ_v} روی ∂V یکنواخت است. حال

$$h(x) = \frac{۱}{|\partial V|}\int_{\partial V} h(y)dy$$

در نتیجه برای هر گوی به مرکز x که در D واقع شود، اگر h متناهی یا نامتناهی باشد

$$h(x) = \frac{۱}{|V|}\int_{V} h(y)dy$$

پس $h(x)$ متناهی است اگر و فقط اگر h در یک همسایگی x متناهی باشد، که نشان می‌دهد مجموعهٔ $\{x : h(x) < +\infty\}$ باز است. از همبند بودن D نتیجه می‌شود که اگر یک x در D موجود باشد که $h(x) < +\infty$، آنگاه برای هر x، $h(x) < +\infty$، لذا h هارمونیک است.

مراجع

[1] Adams, M., Guiliemin, V., *Measure Theory and Probability.*

[2] Bass, R.F. ,*Probabilistic Techniques in Analysis*, Springer-Verlag 1995.

[3] Billingsley, P., *Probability and Measure*, New York: Wiley.

[4] Brelman,*Probability*, Siam 1992.

[5] Chung, K.L., *A Course in Probability Theory*, Acadamic Press, 1977.

[6] Kac, M., "Statistical Independence in Probability", Analysis and Number Theory. Mathematical Association of America (Carus Mathematical Monograph, no 12) 1959.

[7] Karatzas, Shreve E., *Brownian Motion and Stochastic Calculus* Springer-Verlag New York 1988.

[8] Lamperli, J., *probability* W.A. Benjamin Inc 1966.

[9] Ksendal, B., *Stochastic Differential Equations*, Springer-Verlag, Berlin.

[10] Revuz, D., Yor, M., *Continuous Martingales and Brownlan Motion*, Springer Berlin 1992.

[۱۱] در باب برنامه‌ریزی درسی دبیرستان، ترجمه جواد حاجی‌بابایی، رشد آموزش ریاضی شماره ۴۶، ۱۳۷۴.

[۱۲] دوب، جوزف (ترجمه عطاءالله تقاء) «سیر پیدایش دقت در احتمال ریاضی» (۱۹۰۰ـ۱۹۵۰)، نشر ریاضی، سال ۱۲، شماره ۱ و ۲.

[۱۳] ظهوری زنگنه، بیژن، نظریهٔ فرآیندهای تصادفی، جزوات درسی، دانشگاه صنعتی شریف.

[۱۴] ظهوری زنگنه، بیژن، آنالیز تصادفی، جزوات درسی، دانشگاه صنعتی شریف.

[۱۵] مامفرد، دیوید، ترجمه شاپور اعتماد، طلوع عصر روشهای تصادفی، نشر ریاضی سال ۱۳، شماره ۱.

[۱۶] وینر، نوربرت، ترجمهٔ پرویز شهریاری،من یک ریاضیدانم، انتشارات فاطمی، خرداد ۱۳۶۸.

بیژن ظهوری زنگنه

دانشگاه صنعتی شریف، دانشکده علوم ریاضی

پست الکترونیک: zangeneh@sina.sharif.edu

فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۸(بهار ۱۳۸۱)، صص. ۵۳ تا ۶۶

کاربرد برچسب‌گذاری دلپذیر

کورش عشقی

چکیده

برچسب‌گذاری یک گراف یکی از شاخه‌های تحقیقاتی فعال در نظریهٔ گراف است. اولین بار ایدهٔ برچسب‌گذاری گراف‌ها با برچسب‌گذاری دلپذیر مطرح شد اما به‌سرعت توسط محققین انواع متنوعی از برچسب‌گذاری‌های مختلف برای یک گراف تعریف گردید. علیرغم گستردگی در انواع برچسب‌گذاری گراف‌ها همچنان برچسب‌گذاری دلپذیر یکی از جذاب‌ترین شاخه‌های این رشتهٔ تحقیقاتی محسوب می‌شود. در این مقاله سعی شده است به بررسی کاربردهایی که گراف‌های دلپذیر در دنباله‌های متشکل از اعداد صحیح دارند پرداخته شود و زمینه‌های پژوهشی موجود بررسی گردد.

۱. تعاریف مقدماتی

در این مقاله منظور از گراف $G = (V, E)$ یک گراف غیرجهت‌دار و همبند و ساده با m رأس و n یال است که فاقد هرگونه یال چندگانه و طوقه می‌باشد.

تعریف ۱.۱: منظور از برچسب‌گذاری گراف $G = (V, E)$ یک نگاشت یک به یک مانند Ψ از مجموعهٔ رئوس $V(G)$ به مجموعهٔ اعداد صحیح غیرمنفی است به‌نحوی که به هر یال مانند $\{u, v\} \in E(G)$ یک برچسب یالی که به برچسب‌های رئوس آن یعنی $\Psi(u)$ و $\Psi(v)$وابسته باشد اختصاص یابد.

تعریف ۲.۱: برچسب‌گذاری دلپذیر گراف $G = (V, E)$ عبارت است از یک نگاشت یک به یک مانند Ψ از مجموعهٔ رئوس $V(G)$ به مجموعهٔ اعداد صحیح $\{۰, ۱, ۲, \ldots, n\}$ به‌نحوی که اگر برای هر یال

$e = \{u, v\} \in E(G)$ یک برچسب یالی به صورت $\Psi^\bullet(e) = |\Psi(u) - \Psi(v)|$ تعریف شود آنگاه $\Psi^\bullet$ یک نگاشت یک به یک از مجموعهٔ یالهای $E(G)$ به مجموعه اعداد صحیح $\{۱, ۲, \ldots, n\}$ باشد.

یک گراف دلپذیر نامیده می‌شود اگر دارای برچسب‌گذاری دلپذیر باشد. مفهوم برچسب‌گذاری دلپذیر نخستین بار توسط رزا[1] در سال ۱۹۶۶ معرفی شد [۷]. در شکل زیر برچسب‌گذاری دلپذیر برای برخی از انواع گرافها نشان داده شده است:

گراف پترسن

شکل ۱: گراف‌های دلپذیر

بسیاری از گرافها دلپذیر نیستند. برای مثال می‌توان از $C_۵$ و K_n به ازای $n > ۴$ نام برد. همچنین یک گراف دلپذیر می‌تواند چندین برچسب‌گذاری دلپذیر داشته باشد، مانند شکل زیر:

شکل ۲: برچسب‌گذاری‌های دلپذیر متمایز برای یک گراف

معروفترین مسألهٔ حل نشده در مبحث برچسب‌گذاری دلپذیر حدس زیر است که توسط رزا بیان شده است:

حدس ۱: تمام درختها دلپذیر هستند [۷].

قضیهٔ زیر یکی از کاربردهای این حدس را در تجزیهٔ گرافهای کامل نشان می‌دهد:

1) Rosa

قضیه ۱.۱: اگر درخت T با n یال دلپذیر باشد آنگاه گراف کامل K_{2n+1} قابل تجزیه به $2n+1$ کپی از T است [۷, ۱۱].

اثبات: رئوس K_{2n+1} را به‌صورت کلاسهای هم‌نهشتی به سنج $2n+1$ درنظر بگیرید که به‌صورت دایره‌وار مرتب شده‌اند. تفاضل دو کلاس هم‌نهشتی برابر ۱ است اگر متوالی باشند و ۲ است اگر یک کلاس در بین آنها باشد و به همین ترتیب می‌توان تا تفاضل n پیش رفت. یالهای K_{2n+1} را با توجه به قدر مطلق تفاضل دو رأس انتهایی هر یال دسته‌بندی می‌کنیم، دراین صورت به‌ازای $1 \leq j \leq n$ دارای $2n+1$ یال با اختلاف j هستیم. با توجه به برچسب‌گذاری دلپذیر، کپی‌های T در K_{2n+1} را به‌صورت $T_0, T_1, \ldots, T_n$ تعریف می‌کنیم. همچنین رئوس کپی T_k به‌صورت $k, k+1, k+n$ به سنج $2n+1$ می‌باشند که در آن رأس $k+i$ همسایهٔ رأس $k+j$ است اگر و فقط اگر در برچسب‌گذاری دلپذیر T رأس i همسایهٔ رأس j باشد. کپی T_0 همانند برچسب‌گذاری دلپذیر T است و دارای یک یال به ازای هر تفاضل است. درکپی بعدی با افزودن ۱ به مقدار رئوس انتهای تشکیل‌دهندهٔ هر یال در حقیقت هر یال به یال دیگری که دارای همان تفاضل است تبدیل می‌شود. چون به ازای هر قدرمطلق تفاضل ممکن از یالها دارای یک یال با آن مقدار در هر T_k هستیم بنابراین در حقیقت $T_0, T_1, \ldots, T_n$ گراف K_{2n+1} را تجزیه می‌کنند. در شکل ۳ برچسب‌گذاری درخت T و کپی‌های T_0, T_1 آن در K_9 نشان داده شده‌اند:

شکل ۳: برچسب‌گذاری درخت T و کپی‌های T_0, T_1 آن در K_9

همچنین حدس زیر نیز یکی دیگر از حدسهای حل‌نشدهٔ معروف در این شاخه است:

حدس ۲: تمام گراف‌هایی که در آن فقط یک دور منحصربه‌فرد وجود داشته باشد دلپذیر است به جز دور C_n که در آن (پیمانه ۴) $n \equiv 1$ یا 2.

اردیش[1] نشان داد که بیشتر گراف‌ها دلپذیر نیستند. همچنین نیازی نیست که زیرگراف یک گراف دلپذیر خود دلپذیر باشد. برای مثال اگرچه C_5 دلپذیر نیست اما زیرگراف پترسن است که دلپذیر است.
یکی از انواع برچسب‌گذاری دلپذیر برچسب‌گذاری نوع α است که به صورت زیر تعریف می‌شود:

1) Erdös

تعریف ۳.۱: برچسب‌گذاری نوع α در یک گراف $G=(V,E)$ عبارت است از برچسب‌گذاری دلپذیر گراف G که در آن شرط اضافهٔ زیر نیز موجود باشد:

یک عدد مانند γ که $0 \leq \gamma \leq |E(G)|$ وجود داشته باشد به‌نحوی که به ازای هر یال $e=\{u,v\} \in E(G)$ داشته باشیم: $\min[\Psi(u),\Psi(v)] \leq \gamma < \max[\Psi(u),\Psi(v)]$

برای مثال در شکل ۱ گراف C_4 دارای برچسب‌گذاری نوع α است زیرا $\gamma = 2$ و در شکل ۲ درختهای T_3, T_2, T_1 زیرا $\gamma_1 = 1, \gamma_2 = 3, \gamma_3 = 3$. اما درخت چهارم دارای برچسب‌گذاری نوع α نیست زیرا نمی‌توان γ را برای آن یافت.
همانگونه که قبلاً نیز توضیح داده شد انواع گوناگونی از برچسب‌گذاری دلپذیر وجود دارد که در اینجا تنها به ذکر یک نمونه دیگر که مورد استفاده این مقاله قرار می‌گیرد می‌پردازیم:

تعریف ۴.۱: یک برچسب‌گذاری kـدلپذیر از گراف $G=(V,E)$ یک نگاشت یک به یک نظیر Ψ از مجموعهٔ رئوس $V(G)$ به مجموعهٔ اعداد صحیح $\{0,1,2,\ldots,n+k-1\}$ است به‌نحوی که اگر برای هر یال نظیر $e=\{u,v\} \in E(G)$ یک برچسب یالی به صورت $\Psi^\bullet(e) = |\Psi(u) - \Psi(v)|$ تعریف شود آنگاه $\Psi^\bullet$ یک نگاشت یک به یک از مجموعهٔ یالهای $E(G)$ به مجموعهٔ اعداد صحیح $\{k, k+1, k+2, \ldots, n+k-1\}$ باشد.

مفهوم برچسب‌گذاری kـدلپذیر به‌وسیله اسلاتر[1] معرفی شد [۱۰]. به سادگی می‌توان دریافت که گراف ۱ـدلپذیر همان گراف دلپذیر است. در شکل زیر برچسب‌گذاری ۳ـدلپذیر برای یک گراف نشان داده شده است:

شکل ۴: برچسب‌گذاری‌های ۳ـدلپذیر برای یک گراف

برای اطلاع از انواع مختلف برچسب‌گذاری دلپذیر و آخرین تحقیقات انجام شده در این موضوع می‌توانید به مرجع [۵] مراجعه نمایید.

1) Slater

۲. دنبالهٔ اعداد صحیح و گراف‌های دلپذیر

برچسب‌گذاری دلپذیر یک گراف را می‌توان بر حسب یک دنباله از اعداد صحیح بیان کرد. شپارد[1] نخستین کسی بود که ارتباط بین توالی اعداد صحیح و برچسب‌گذاری دلپذیر گرافها را نشان داد [۸].

تعریف ۱.۲: برای یک عدد صحیح n دنبالهٔ اعداد صحیح $(j_1, j_2, j_3, \ldots, j_n)$ یک دنبالهٔ برچسب‌گذاری[2] نامیده می‌شود و با (j_i) نشان داده می‌شود هرگاه به ازای هر $1 \leq i \leq n$ داشته باشیم:

$$0 \leq j_i \leq n - i$$

برای مثال برای $n = 5$ دنباله‌های $(0, 2, 1, 1, 0)$, $(4, 3, 2, 1, 0)$ و $(1, 3, 0, 1, 0)$ دنباله‌های برچسب‌گذاری هستند.

قضیهٔ ۱.۲: تناظر یک به یک بین گرافهای دلپذیر با n یال و دنباله برچسب‌گذاری j_i با n جمله وجود دارد [۸].

اثبات: اگر G یک گراف دلپذیر با n یال و برچسب‌گذاری دلپذیر Ψ باشد آنگاه فرض کنید j_i کوچکترین برچسب رأسی باشد که برچسب یالی i را تولید می‌نماید. به عبارت دیگر اگر $|\Psi(u) - \Psi(v)| = i$ آنگاه تعریف می‌کنیم: $j_i = \min(\Psi(u), \Psi(v))$. برعکس فرض کنید که یک دنبالهٔ برچسب‌گذاری به‌صورت (j_i) با n جمله داده شده باشد در این صورت برچسب‌گذاری دلپذیر گراف وابسته به آن را می‌توان به‌صورت زیر به‌دست آورد: تعداد $n + 1$ برچسب را از بین $[0, n]$ به دلخواه به $n + 1$ رأس مجزا نسبت دهید. به ازای هر j_i رئوس با برچسب‌های j_i و $j_i + i$ را به هم متصل کنید. چنین برچسب‌های رئوسی با توجه به تعریف دنبالهٔ برچسب‌گذاری وجود دارند، بنابراین یال حاصل دارای برچسب i می‌باشد بنابراین کلیهٔ مقادیر از ۱ الی n به‌عنوان برچسب‌های یال‌ها استفاده می‌شوند و بنابراین برچسب‌گذاری دلپذیر گراف بدست می‌آید.

در شکل زیر تمام برچسب‌گذاری‌های دلپذیر یک گراف با ۳ یال و دنبالهٔ برچسب‌گذاری متناظر با آن

1) Sheppard 2) labeling sequence

نشان داده شده است:

شکل ۵: برچسب‌گذاریهای دلپذیر یک گراف با ۳ یال و دنبالهٔ برچسب‌گذاری متناظر با آن

از آنجا که دارای $n!$دنباله برچسب‌گذاری با n جمله هستیم پس دارای $n!$ گراف دلپذیر با n یال می‌باشیم. بعضی از این گرافهای دلپذیر دارای برچسب‌گذاری نوع α نیز می‌باشند. اگر گراف G دارای برچسب‌گذاری نوع α باشد آنگاه دنبالهٔ برچسب‌گذاری متناظر با آن به‌نام یک دنباله متوازن[1] نامیده می‌شود و دارای خاصیت زیر می‌باشد:

تعریف ۲.۲: یک دنبالهٔ برچسب‌گذاری (j_i) متوازن است اگر به ازای هر $1 \leq i \leq n$ داشته باشیم:
$j_i \leq j_1 < j_i + i$

قضیه ۲.۲: دنبالهٔ برچسب‌گذاری (j_i) با n جمله یک دنبالهٔ متوازن است اگر و فقط اگر دنباله $(j_i{}^*)$ برای هر $1 \leq i \leq n$ که به صورت $j_i{}^* = j_1 - j_{n-i+1}$ تعریف می‌شود یک دنبالهٔ برچسب‌گذاری باشد [۸].

اثبات: به‌سادگی از روی تعریف دنبالهٔ متوازن به‌دست می‌آید.

برای مثال در شکل ۴ دنبالهٔ برچسب‌گذاری G_2 عبارت است از $(j_{G2}) = (2,0,0)$. از آنجا که $(j^*_{G2}) = (2,0,0)$ یک دنبالهٔ برچسب‌گذاری نیست (j_{G2}) نیز یک دنبالهٔ متوازن نمی‌باشد و G_2 دارای برچسب‌گذاری نوع α نیست. با استفاده از تعریف دنبالهٔ متوازن شپارد موفق شد که تعداد گرافهای دارای برچسب‌گذاری نوع α را به صورت زیر محاسبه کند:

1) balanced sequence

قضیهٔ ۳.۲: تعداد دنباله‌های متوازن با n جمله به صورت زیر به‌دست می‌آیند [۸]:

اگر $n^{۲} \equiv ۰$

$$(۱) \quad ۲ \sum_{i=۱}^{(۱/۲)n} (j!)^{۲} j^{n-۲j}$$

اگر $n^{۲} \equiv ۱$

$$(۲) \quad ۲ \sum_{i=۱}^{(۱/۲)(n-۱)} [(j!)^{۲} j^{n-۲j}] + [((۱/۲)(n+۱))!((۱/۲)(n-۱))!]$$

تعداد گرافهای دارای برچسب‌گذاریهای دلپذیر و نوع α برای گرافهای با n یال و نسبت آنها به یکدیگر در جدول زیر آمده است:

n	تعداد گراف‌های دارای برچسب‌گذاری دلپذیر (۱)	تعداد گراف‌های دارای برچسب‌گذاری نوع α (۲)	نسبت به مقدار ستون (۲) به ستون (۱)
۱	۱	۱	۱
۲	۲	۲	۱
۳	۶	۴	۰٫۶۷
۴	۲۴	۱۰	۰٫۴۲
۵	۱۲۰	۳۰	۰٫۲۵
۱۰	۳۶۲۸۸۰۰	۵۳۵۷۸	۰٫۰۱۵
۱۵	$۱٫۳ \times ۱۰^{۱۲}$	$۸٫۹ \times ۱۰^{۸}$	$۶٫۸ \times ۱۰^{-۴}$
۲۰	$۲٫۴ \times ۱۰^{۱۸}$	$۶٫۹ \times ۱۰^{۱۳}$	$۲٫۸ \times ۱۰^{-۵}$
۳۰	$۲٫۶ \times ۱۰^{۳۲}$	$۱٫۱ \times ۱۰^{۲۵}$	$۴٫۲ \times ۱۰^{-۸}$

جدول ۱: تعداد گرافهای دارای برچسب‌گذاری‌های دلپذیر و نوع α برای گراف‌های با n یال

با مشاهدهٔ این جدول مشخص می‌شود که با افزایش تعداد یال‌ها نسبت گرافهای دارای برچسب‌گذاری نوع α به گراف‌های دلپذیر به سمت صفر میل می‌کنند.

۳. سیستم کامل از مجموعه‌های تفاضلی و برچسب‌گذاری دلپذیر

تعریف ۱.۳: فرض کنید $c, m, p_m, \ldots, p_۲, p_۱$ اعداد مثبت صحیح باشند و نیز $S_i = \{X_{۰i} < X_{۱i} < \ldots < X_{pi}\}; i = ۱, ۲, \ldots, m$ یک دنباله از اعداد صحیح و $D_i = \{X_{ji} - X_{ki}, ۰ \leq k \leq j \leq p_i\}, i = ۱, ۲, \ldots, m$ مجموعه‌های تفاضلی[1] و یا به اختصار PSDS گفته می‌شود که با c شروع می‌شود اگر

$$\bigcup_{i=۱}^{m} D_i = \{c, c+۱, c+۲, \ldots, c-۱+\sum_{i=۱}^{m}(۱/۲)(p_i(p_i+۱)\}$$

1) perfect system of difference sets

برای مثال $S_1 = \{0, 2, 8\}, S_2 = \{1, 5, 10\}, S_3 = \{0, 3, 10\}$ تشکیل مجموعه‌های تفاضلی $D_1 = \{2, 6, 8\}, D_2 = \{4, 5, 9\}, D_3 = \{3, 7, 10\}$ را می‌دهند که درنتیجه $\{D_1, D_2, D_3\}$ یک PSDS است زیرا

$$\bigcup_{i=1}^{m} D_i = \{2, 3, 4, \ldots, 10\}$$

به هر مجموعهٔ D_i یک مؤلفهٔ $\{D_1, D_2, \ldots, D_m\}$ PSDS گفته می‌شود. یک PSDS را معمولی[1] نامند اگر تمام مؤلفه‌های آن دارای اندازهٔ یکسان باشند یعنی $p_1 = p_2 = \cdots = p_m = n - 1$. یک PSDS معمولی با m مؤلفه با اندازهٔ $n - 1$ که از c شروع می‌شود را با (m, n, c) نشان می‌دهیم.

اگر فرض کنیم که

$$X_{j+k-1,i} - X_{j-1,i} = d_{ji}(k), j = 1, 2, \ldots, p_i + 1 - k, k = 1, 2, \ldots, p_i, i = 1, 2, \ldots, m$$

آنگاه عناصر D_i می‌توانند به‌صورت زیر نوشته شوند:

$$d_{1i}(p_i)$$

.....

.....

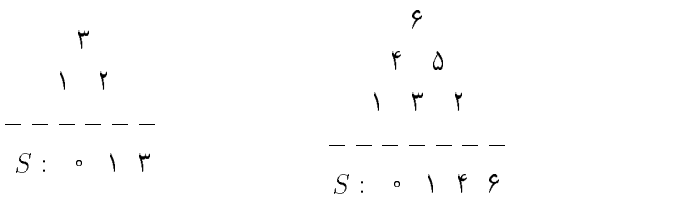
$$d_{1i}(2)\ d_{2i}(2) \ldots\ldots d_{pi-2,i}(2)\ d_{pi-1,i}(2)$$

$$d_{1i}(1)\ d_{2i}(1)\ d_{3i}(1) \ldots\ldots d_{pi-2,i}(1)\ d_{pi-1,i}(1)\ d_{pi,i}(1)$$

$$X_{0i}\quad X_{1i}\quad X_{2i} \ldots\ldots X_{pi-1,i}\quad X_{pi,i}$$

بیراد[2] و بلوم[3] و ریبس[4] نخستین کسانی بودند که ارتباط مابین برچسب‌گذاری دلپذیر و PSDS بیان کردند [۲, ۳].

$(1, n, 1)$ یک PSDS معمولی با یک مؤلفه است که از یک شروع می‌شود. فقط دو $\mathrm{PSDS}(1, n, 1)$ معمولی وجود دارند:



$\mathrm{PSDS}(1, n, 1)$ با برچسب‌گذاری دلپذیر K_n در ارتباط است. برای مثال $(1, 3, 1)$ و $(1, 4, 1)$ به

1) regular 2) Biraud 3) Blum 4) Ribes

برچسب‌گذاری دلپذیر K_3 و K_4 مربوط هستند:

شکل ۶: برچسب‌گذاریهای دلپذیر گراف‌های K_3 و K_4

در حالت کلی وجود یک PSDS $(m, n, 1)$ وابسته به برچسب‌گذاری دلپذیر گرافی متشکل از mK_n است که دارای یک رأس مشترک باشند. به چنین گرافی آسیاب بادی[1] گفته می‌شود. در حالتی که $n = 3$ باشد گراف آسیاب بادی متشکل از m کپی از K_3 است که دارای یک رأس مشترک هستند. به چنین گرافی آسیاب بادی هلندی با m پره[2] گفته می‌شود. برموند[3] قضیهٔ زیر را اثبات کرد:

قضیهٔ ۱.۳: گرافهای آسیاب بادی هلندی با m پره دلپذیر هستند اگر و فقط اگر داشته باشیم [۳]:

$$m \equiv 0 \quad \text{or} \quad 1 \pmod 4$$

در حالتی که $n = 4$ باشد گراف آسیاب بادی متشکل از m کپی از K_4 است که دارای یک رأس مشترک هستند. به چنین گرافی آسیاب بادی فرانسوی با m پره[4] گفته می‌شود. حدس زیر همچنان یکی از مسائل حل نشده در برچسب‌گذاری گرافها است اگرچه صحت آن برای $4 \leq m \leq 32$ نشان داده شده است:

حدس ۳: گرافهای آسیاب بادی فرانسوی با m پره دلپذیر هستند اگر $m \geq 4$ باشد [۳].

در شکل زیر یک آسیاب بادی هلندی با ۵ پره و یک آسیاب بادی فرانسوی با ۴ پره نشان داده شده

1) Windmill graphs 2) Dutch m-windmill 3) Bermond 4) French m-windmill

است که دلپذیر هستند:

آسیاب بادی هلندی با ۵ پره آسیاب بادی فرانسوی با ۴ پره

شکل ۷: برچسب‌گذاری‌های دلپذیر گرافهای آسیاب بادی

با توجه به آنچه گفته شد مسألهٔ وجود $\mathrm{PSDS}(m,۳,۱)$ و $\mathrm{PSDS}(m,۴,۱)$ به مسألهٔ برچسب‌گذاری گراف‌های آسیاب بادی هلندی با m پره و آسیاب بادی فرانسوی با m پره برمی‌گردد. بنابراین بر طبق قضیهٔ ۱.۳ یک $\mathrm{PSDA}(m,۳,۱)$ وجود دارد اگر و فقط اگر $m \equiv ۰$ یا $۱ \pmod ۴$.

یک PSDSکه از c شروع می‌شود بیانگر یک برچسب‌گذاری cـدلپذیر گرافی است که می‌تواند به زیرگراف‌های کامل تجزیه شود چون ثابت می‌شود که هیچ $(۱,n,c)$ با $c > ۱$ موجود نیست [۲]. پس هیچ گراف کاملی نیز به ازای $c > ۱$ دارای برچسب‌گذاری cـدلپذیر نیست. سیستم کامل $(۳,۳,۲)$ زیر

۸	۹	۱۰
۲ ۶	۴ ۵	۳ ۷
$S_۱$: ۰ ۲ ۸	$S_۲$: ۰ ۴ ۹	$S_۳$: ۰ ۳ ۱۰

نشان‌دهندهٔ آن است که آسیاب بادی هلندی با ۳ پرهٔ زیر ۲ـدلپذیر است:

شکل ۸: برچسب‌گذاری ۲ـدلپذیر گراف آسیاب بادی هلندی با ۳ پره

توجه کنید که یک PSDS می‌تواند برچسب‌گذاری cـدلپذیر را برای انواع متفاوتی از گراف‌ها تولید کند. برای مثال اگر PSDS بالا را با $S_۲$ دیگری در نظر بگیریم داریم:

۸	۹	۱۰
۲ ۶	۴ ۵	۳ ۷
– – – – – –	– – – – – – –	– – – – – – –
$S_۱$: ۰ ۲ ۸	$S_۲$: ۱ ۵ ۱۰	$S_۳$: ۰ ۳ ۱۰

و در این صورت برچسب‌گذاری ۲ـدلپذیر زیر را برای گراف داده شده در بر خواهد داشت:

شکل ۹: برچسب‌گذاری ۲ـدلپذیر

دنباله اسکلم و برچسب‌گذاری دلپذیر

تعریف ۱.۴: یک دنباله اسکلم با رتبهٔ nعبارت است از یک دنباله مانند $S = \{S_۱, S_۲, \ldots, S_{۲n}\}$ از اعداد صحیح مثبت که دارای خصوصیات زیر باشند:

۱. به ازای هر $k \in \{۱, ۲, \ldots, n\}$ دقیقاً دو اندیس $i(k), j(k)$ وجود داشته باشند به نحوی که $S_{i(k)} = S_{j(k)} = k$

۲. دو اندیس شرط $|i(k) - j(k)| = k, k = ۱, ۲, \ldots, m$ را ارضا کنند.

برای مثال مجموعهٔ $S = \{۱, ۱, ۳, ۴, ۵, ۳, ۲, ۴, ۲, ۵\}$ یک دنبالهٔ اسکلم با رتبهٔ ۵ است زیرا
$S_۱ = S_۲ = ۱, S_۷ = S_۹ = ۲, S_۳ = S_۶ = ۳, S_۴ = S_۸ = ۴, S_۵ = S_{۱۰} = ۵$
شکل دیگر نمایش یک دنبالهٔ اسکلم را می‌توان به صورت $S(G) = \{a_۱, b_۱, a_۲, b_۲, \ldots, a_n, b_n\}$ نشان داد با این فرض که در آن $b_r - a_r = r, r = ۱, ۲, \ldots, n$ باشد. برای مثال دنبالهٔ اسکلم فوق را می‌توان به صورت $S = \{۱, ۲, ۷, ۹, ۳, ۶, ۴, ۸, ۵, ۱۰\}$نیز نشان داد.

قضیهٔ زیر توسط اسکلم ثابت شده است:

قضیهٔ ۱.۴: یک دنبالهٔ اسکلم با رتبهٔ n وجود دارد اگر و فقط اگر $n \equiv ۰$ یا $۱ \pmod ۴$ [۷].

اثبات: برای اثبات شرط لازم این قضیه ابتدا فرض کنید که $S(G) = \{a_۱, b_۱, a_۲, b_۲, \ldots, a_n, b_n\}$ یک دنبالهٔ اسکلم باشد که در آن $b_r - a_r = r$ به ازای $r = ۱, ۲, \ldots, n$. در این صورت با توجه به تعریف دنبالهٔ اسکلم داریم: $\sum b_r - \sum a_r = (\frac{۱}{۲})n(n+۱)$ از طرف دیگر

$$\sum b_r + \sum a_r = ۲n(۲n+۱)/۲ = n(۲n+۱)$$

که درنتیجه خواهیم داشت:

$$\sum b_r = \frac{1}{4}n(5n+3)$$

رابطهٔ فوق در صورتی مقدار صحیح به خود می‌گیرد که $n \equiv 0$ یا $1 (mod 4)$. اثبات شرط کافی از طریق بررسی حالات مختلف موجود انجام می‌شود که برای آگاهی از آن می‌توانید به مرجع [۹] مراجعه نمایید.

حال فرض کنید که G یک گراف ۲ـمنتظم دلپذیر به روی n رأس باشد. می‌خواهیم بدانیم که آیا می‌توان یک دنبالهٔ اسکلم از اعداد صحیح نظیر $S(G) = \{a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n\}$ را به برچسب‌های این گراف نسبت داد یا خیر؟

ابتدا با کمک الگوریتم زیر به برچسب‌گذاری دلپذیر G یک دنباله از اعداد صحیح نسبت می‌دهیم که این دنباله ضرورتاً اسکلم نیست اما در حالات خاصی که بعداً ذکر می‌شود می‌تواند به دنبالهٔ اسکلم تبدیل شود [۱, ۳]:

الگوریتم ساختن $S(G)$:

فرض کنیم: G یک گراف ۲ـمنتظم دلپذیر به روی n رأس است و یال‌های G به صورت $e_1, e_2, \ldots, e_n$ شماره شده‌اند به نحوی که برچسب e_k در برچسب‌گذاری دلپذیر k است. در طی فرآیند ساخت عبارات موجود در $S(G)$ می‌گوییم که یک عبارت مانند a_i یا b_i آزاد است اگر به آن مقداری تخصیص داده نشده باشد.

- گام اول: یک دور دلخواه نظیر C را در G انتخاب کرده و در جهتی دلخواه به روی آن حرکت کنید.
- گام دوم: یک یال دلخواه e_k را از C انتخاب کنید. فرض کنید که برچسب رئوس انتهایی این یال i و $i+k$ باشند.
- گام سوم: یکی از عبارات $(a_i, a_{i+k}), (b_i, b_{i+k}), (a_i, b_{i+k}), (a_{i+k}, b_i)$ را انتخاب کنید و به آن مقدار k را تخصیص دهید.
- گام چهارم: به یال مجاور یال e_k که در جهت انتخاب شده است حرکت کرده و نام یال جدید را e_r بنامید.
- گام پنجم: فرض کنید که برچسب رئوس انتهایی e_r، p و $p+r$ باشند. در این صورت یکی از جفت‌های $(a_p, a_{p+r}), (b_p, b_{p+r}), (a_{p+r}, b_p), (a_p, b_{p+r})$ را که دارای دو عبارت آزاد باشد انتخاب کنید و توجه داشته باشید که امکان چنین کاری همواره وجود دارد و مقدار r را به هر دو عبارت موجود در این جفت اختصاص دهید.
- گام ششم: تا زمانی که تمام یال‌های موجود در دور C استفاده شوند ادامه دهید.
- گام هفتم: اگر G فقط دارای یک دور باشد در انتهای اجرای گام‌های قبلی یک جفت (a_x, b_x) باقی خواهد ماند که فقط دارای دو عبارت آزاد است. در این صورت $a_x = b_x = n+1$.

اگر G دارای بیش از یک دور باشد در این صورت دور دیگری از G را اختیار کرده و گام‌های بالا را مجدداً تکرار می‌نماییم، تا زمانی که یک جفت آزاد (a_x, b_x) باقی بماند و در این صورت $a_x = b_x = n + ۱$.

برای مثال گراف G و برچسب‌گذاری دلپذیر آن در شکل زیر نشان داده شده است. میخواهیم $S(G)$ را بسازیم با این فرض که جهت انتخاب شده در جهت عقربه‌های ساعت باشد.

شکل ۱۰: برچسب‌گذاری دلپذیر گراف $C_۸$

با به‌کارگیری گام به گام الگوریتم فوق در این مثال جدول زیر را خواهیم داشت:

مرحله	برچسب یال انتخاب شده	زوجهای مرتب ممکن با دو جمله آزاد	جملات انتخاب‌شده
۰	۴	$(a_۳, a_۷), (a_۳, b_۷), (b_۳, a_۷), (b_۳, b_۷)$	$b_۳ = b_۷ = ۴$
۱	۶	$(a_۱, a_۷), (a_۷, b_۱)$	$a_۱ = a_۷ = ۶$
۲	۷	$(b_۱, b_۸), (a_۸, b_۱)$	$b_۱ = b_۸ = ۷$
۳	۸	$(a_۰, a_۸), (a_۸, b_۰)$	$a_۰ = a_۸ = ۸$
۴	۵	$(b_۰, b_۵), (a_۵, b_۰)$	$b_۰ = b_۵ = ۵$
۵	۱	$(a_۴, a_۵), (a_۵, b_۴)$	$a_۴ = a_۵ = ۱$
۶	۲	$(b_۴, b_۶), (a_۶, b_۴)$	$b_۴ = b_۶ = ۲$
۷	۳	$(a_۳, a_۶), (a_۶, b_۳)$	$a_۳ = a_۶ = ۳$

جدول ۲: طرز ساخت $S(G)$ برای مثال

در نهایت زوج $(a_۲, b_۲)$ باقی می‌ماند که دراین‌صورت $a_۲ = b_۲ = n + ۱ = ۹$ و خواهیم داشت:

$$S(G) = (a_۰, a_۱, \ldots, a_۸, b_۰, b_۱, \ldots, b_۸) = (۸, ۶, ۹, ۳, ۱, ۱, ۳, ۶, ۸, ۵, ۷, ۹, ۴, ۲, ۵, ۲, ۴, ۷)$$

دنبالهٔ $S(G)$ که در بالا ساخته می‌شود ضرورتاً یک دنبالهٔ اسکلم نیست اما در دو حالت زیر تبدیل به یک دنبالهٔ اسکلم با رتبه $n + ۱$ می‌شود:

۱. اگر G یک گراف ۲ منتظم با n رأس باشد که فقط شامل دورهایی با طول زوج باشد یعنی $n \equiv ۰ \pmod ۴$،

۲. اگر G یک گراف ۲ منتظم با $n \equiv ۳ \pmod ۴$ رأس باشد که دارای یک مؤلفه با طول فرد باشد.

برعکس گاهی اوقات یک دنبالهٔ اسکلم می‌تواند یک برچسب‌گذاری دلپذیر یا برچسب‌گذاری نوع α را تولید کند اگر دارای شرایط خاصی باشد که در مرجع [۱] در مورد آن بحث شده است.

مراجع

[1] J. Abrham, "Graceful 2-regular graphs and Skolem sequences", *Discrete Math.* 93(1991) 115-121.

[2] J. Abrham, "Perfect systems of difference sets: A survey", *Ars Comb.* 17 A(1984) 5-36.

[3] J.C. Bermond, "Graceful graphs, radio antennae and French windmills", *Graph Theory and Combinatorics,* Pitman (1979), 18-37.

[4] K. Eshghi, Existence and construction of a-labeling of 2-regular graphs with three components, Ph.D. Thesis, University of Toronto (1997).

[5] J. A. Gallian, "A dynamic survey of graph labeling", *Elec. J. of Combin.,* (2000)1-79.

[6] S. W. Golomb, *How to number a graph, Graph Theory and Computing, Academic press, New York* (1972) 23-37.

[7] A. Rosa, *On certain valuations of the vertices of a graph, Theory of Graphs* (International Symposium, Rome, July 1966), Gordon and Breach, New York and Dunod Paris (1967) 349-355.

[8] D. A. Sheppard, "The factorial representation of balanced labelled graphs", *Discrete Math.* 15 (1976) 379-388.

[9] T. Skolem, "On certain distribution of integers into pairs with given differences", Math. Scand. 5 (1957) 57-68.

[10] P. J. Slater, "On k-sequential and other numbered graphs", *Discrete Math.* 34 (1981) 185-193.

[11] D. B. West, *Introduction to graph theory*, prentice Hall (2001), 88-9.

کورش عشقی

دانشگاه صنعتی شریف، دانشکده صنایع

پست الکترونیک: eshghi@sharif.edu

فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۸(بهار ۱۳۸۱)، صص. ۶۷ تا ۶۹

مسأله

این قسمت از فرهنگ و اندیشهٔ ریاضی به طرح و سپس حلِ مسائلی در حدِ دروسِ دوره‌های کارشناسی و کارشناسی ارشدِ ریاضیات اختصاص دارد. از کسانی که مایل به ارسال مسائل یا حل مسائلِ مطرح شده می‌باشند، تقاضا می‌شود مسائل خود را به نشانی تهران، مرکز تحقیقات فیزیک نظری و ریاضی، پژوهشکدهٔ ریاضیات، صندوق پستی ۵۷۴۶ـ۱۹۳۹۵، محمدرضا پورنکی ارسال فرمایند. مسائلِ ارسال‌شده باید همراه با حل کامل مسأله باشد و در مجله به نامِ شخصِ فرستنده درج خواهد شد.

توضیح: با عرض پوزش از خوانندگان، حل مسائل ۳۱ـ۳۴ که مدتی به تعویق افتاده بود، در این شماره آورده می‌شود. شایان ذکر است که این موارد مربوط به دورهٔ تحت مسؤولیت آقای دکتر محمدرضا درفشه بوده است که اخیراً توسط خود ایشان برای چاپ ارسال شده است. از شمارهٔ آینده مسائل و حل مسائل تحت مسؤولیت آقای دکتر محمدرضا پورنکی ادامه خواهد یافت.

حل مسائل فرهنگ و اندیشهٔ شمارهٔ ۲۳:

حل مسألهٔ ۳۱: فرض کنید G گروه متناهی از مرتبه فرد n و φ اتومورفیسمی از G باشد به طوریکه $\varphi^2 = id$. همچنین قرار می‌دهیم: $A = \{x \in G | \varphi(x) = x\}$ و $B = \{x \in G | x \neq 1 \varphi(x) = x^{-1}\}$ و $n_1 = |A|$ و $n_2 = |B|$. آنگاه ثابت کنید $n = n_1(n_2 + 1)$ و از آن نتیجه بگیرید اگر $n_2 \geq n/3$ آنگاه G آبلی است.

حل: واضح است که A زیرگروه G می‌باشد. قرار می‌دهیم $B' = B \cup \{1\}$ و ثابت می‌کنیم $G = A.B'$ و $|B'| = [G : A]$. چون n فرد است لذا اعداد صحیحی مانند γ و S موجودند به طوریکه $2r + ns = 1$. حال تابع $f : G \to G$ با ضابطه $f(x) = x^2$ یک به یک است زیرا اگر

$f(x)=f(y)$ آنگاه $x=x^{۲r+nS}=(x^۲)^r=(y^۲)^r=y^{۲r+nS}=y$ و چون G متناهی است لذا f پوشا نیز هست. حال فرض کنیم $g\in G$ دلخواه باشد، چون f پوشا است لذا عضو منحصربه‌فردی مانند $x\in G$ موجود است به‌طوریکه $g^{-۱}\varphi(g)=x^۲$. ادعا می‌کنیم که $x^{-۱}\in B'$ و $gx\in A$ و بنابراین $g=(gx).x^{-۱}$. از رابطهٔ سطر قبل داریم:

$\varphi(g^{-۱}\varphi(g))=\varphi(x^۲)=(\varphi(x))^۲\Rightarrow\varphi(g)^{-۱}g=(\varphi(x))^۲\Rightarrow(x^۲)^{-۱}=(\varphi(x))^۲$ چون f یک به یک است لذا $\varphi(x)=x^{-۱}$ و بنابراین $x^{-۱}\in B'$. دوباره از رابطهٔ فوق داریم: $gx=\varphi(g)x^{-۱}$ و بنابراین خواهیم داشت: $\varphi(gx)=\varphi(\varphi(g)x^{-۱})=g.\varphi(x^{-۱})=gx\Rightarrow gx\in A$.

پس نشان دادیم $G=A.B'$. حال تابع $h:B'\to\{Ag|g\in G\}$ را چنین تعریف می‌کنیم: $h(x)=Ax$. واضح است که h خوش‌تعریف است. نشان می‌دهیم h یک به یک و پوشا است. فرض کنیم $g\in G$ دلخواه باشد. پس وجود دارند $a\in A$ و $b\in B'$ به طوریکه $g=ab$ لذا $h(b)=Ab=Aab=Ag$، پس h پوشا است. حال فرض کنیم $x,y\in B'$ به طوریکه $h(x)=h(y)$ در نتیجه $Ax=Ay$ و بنابراین $xy^{-۱}\in A$ پس $\varphi(xy^{-۱})=xy^{-۱}$ و نتیجتاً $\varphi(x)\varphi(y^{-۱})=xy^{-۱}$. چون $x,y\in B'$ پس $x^{-۱}y=xy^{-۱}$ و بنابراین $x^۲=y^۲$ و چون f یک به یک است داریم $x=y$ و h یک به یک است پس: $n=|G|=|A||G:A|=n_۱(n_۲+۱)$. حال اگر $n_۲\geq n/۳$ خواهیم داشت: $n_۱\leq\frac{n}{n/۳+۱}<۳\Rightarrow n\geq n_۱(n/۳+۱)\Rightarrow n_۱(n_۲+۱)$ چون n فرد است و $A\leq G$ پس $n_۱|n$ و لذا $n_۱=۱$ و بنابراین $G=B'$ آبلی است.

حل مسألهٔ ۳۲: فرض کنید $I\neq R$ و M ایدآل ماکسیمالی از R شامل I باشد. در این صورت R/M یک میدان است که مرتبه‌اش حداکثر ۴ می‌باشد. اکنون می‌توان تحقیق کرد که در میدان‌های ۲، ۳ و ۴ عضوی رابطهٔ $x^۳=x+۱$ برقرار نمی‌باشد.

حل مسألهٔ ۳۳: با توجه به نامساوی داده شده نتیجه می‌گیریم

$$\frac{d}{dx}(\arctan(f(x))+x)=\frac{f'(x)}{۱+f^۲(x)}+۱\geq۰\quad,\ \forall x\in(a,b)$$

پس تابع $\arctan(f(x))+x$ در فاصلهٔ (a,b) غیرنزولی است و با توجه به حدود داده شده نتیجه می‌شود $b+\frac{\pi}{۲}\leq a-\frac{\pi}{۲}$ و لذا $b-a\geq\pi$. اگر $f(x)=cotgx$، $a=۰$ و $b=\pi$ آنگاه تساوی برقرار است.

حل مسألهٔ ۳۴: قرار می‌دهیم $||g||_۱=\int_۰^b|g(x)|dx$ و $w(f,t)=\sup\{|f(x)-f(y)|:x,y\in[۰,b],|x-y|\leq t\}$ چون f به طور یکنواخت پیوسته است وقتیکه $t\to۰$ داریم $w(f,t)\to۰$. با استفاده از متناوب بودن g به دست می‌آوریم:

$$\int_{۰}^{b} f(x)g(nx)dx = \sum_{k=۱}^{n} \int_{b(k-۱)/n}^{bk/n} f(x)g(nx)dx$$
$$= \sum_{k=۱}^{n} f(bk/n) \int_{b(k-۱)/n}^{bk/n} g(nx)dx + \sum_{k=۱}^{n} \int_{b(k-۱)/n}^{bk/n} (f(x) - f(bk/n)g(nx))$$
$$= ۱/n \sum_{k=۱}^{n} f(bk/n) \int_{۰}^{b} g(x)dx + o(w(f, b/n)||g||_۱)$$
$$= \frac{۱}{b} \sum_{k=۱}^{n} \int_{b(k-۱)/n}^{bk/n} f(x)dx \int_{۰}^{b} g(x)dx +$$
$$\frac{۱}{b} \sum_{k=۱}^{n} (\frac{b}{n} f(bk/n) - \int_{b(k-۱)/n}^{bk/n} f(x)dx (\int_{a}^{b} g(x)dx + o(w(f, b/n)||g||_۱)$$
$$= \frac{۱}{b} \int_{۰}^{b} f(x)dx \int_{۰}^{b} g(x)dx + o(w(f, b/n)||g||_۱)$$

(۱)

و به این ترتیب (الف) ثابت می‌شود، برای (ب) قرار می‌دهیم $b = \pi$، $f(x) = \sin x$، $g(x) = (۱ + ۳\cos^۲ x)^{-۱}$ که با استفاده از (الف) و اینکه $\int_{۰}^{\pi} \sin x dx = ۲$ و $\int_{۰}^{\pi} (۱ + ۳\cos^۲ x)^{-۱} dx = \pi/۲$ حاصل می‌شود

$$\lim_{n\to\infty} \int_{۰}^{\pi} \frac{sinx}{۱ + ۳\cos^۲ nx} dx = ۱$$

حل مسألهٔ ۳۵. (الف) قرار می‌دهیم $S = \frac{۱}{۲}(T + I)$. در این صورت به‌راحتی تحقیق می‌شود که $S^۲ = S$ و لذا S یک تصویر است. چون هر تصویر قطری شدنی است پس $T = ۲S - I$ نیز قطری شدنی است.

(ب) فرض کنید $\{A_i | i \in I\}$ مجموعه‌ای از برگردان‌های دو به دو جابه‌جا شونده باشد. بنا به (الف) هر کدام از A_iها قطری شدنی هستند و در نتیجه عناصر مجموعهٔ فوق به طور همزمان قطری شدنی هستند. از آنجا که در این حالت عناصر روی قطر اصلی ± ۱ هستند باید داشته باشیم $|I| \leq ۲^n$.

تشکر: از آقایان محمد حسین جعفری و کمال عزیزی هریس از دانشگاه تهران که مسائل شمارهٔ ۳۱ تا ۳۵ را ارسال کرده‌اند متشکریم.