مجله‌ی ریاضی شریف

دانشجویان دانشکده‌ی علوم ریاضی دانشگاه صنعتی شریف

دوره‌ی سوم، شماره‌ی اول، بهار ۱۴۰۲

مجله‌ی ریاضی شریف

دوره‌ی سوم، شماره‌ی اول، بهار ۱۴۰۲

مدیر مسئول:

دکتر امیر جعفری

سردبیر:

نوید دژبرد

هیئت تحریریه:

علی الماسی

متین انصاری‌پور

نیکی حسنی

هادی زمانی

نویسندگان و مترجمان:

دکتر امیر اصغری، امیرکسری جلال‌دوست، متین حاجیان، احمد رحیمی، محمد زارع، دکتر محمدصالح زارع‌پور، علیرضا شاولی، دکتر ساجد طیبی، علیرضا عظیمی‌نیا، دکتر مرتضی علیمی

طراح جلد:

پریسا ایزدی‌مند، پرناز بابِلیان

با سپاس از:

مریم ابراهیمی، نیما افشار، متین امینی، عرفان برزین، پارسا تربتی، علی توسلی، علی چراغی، سعید حقی، نیما خداویسی، دکتر حسام رجب‌زاده، ساینا سعدآبادی، الهه صادقی، زهرا عباسعلی‌نیا، دکتر کسری علیشاهی، دکتر حمیدرضا فنایی، ریحانه قاضی‌زاده، مینو معظمی، سید عرفان موسویان، امید نوری‌عابد، دیبا هاشمی

فهرست مطالب

یادداشت‌ها

سرمقاله ۱

آن‌ها که می‌نویسند. ۲

مقاله‌ها

جمع‌های گاوسی، از تقابل مربعی تا حدسیات ویل ٤

مرغ یا تخم‌مرغ؟ ۲۲

رویه‌های مینیمال و حدس دی‌جورجی ۲۸

احراز هویت خودکار بر اساس چهره ٤۱

مصاحبه‌ها و مکاتبه‌ها

گفت‌وگوی آبل ۲۰۲۱: لواس و ویگدرسون ٤۹

مکاتبات فرگه و راسل ٦۳

معرفی‌ها

کتاب‌هایی زیبا در نظریه‌ی محاسبه ٦٦

منطق، ریاضیات، و فلسفه‌های آن‌ها ۷۱

از نادر گمنام تا آدم‌ها و ریاضی ۷۳

مسئله‌ها

آزمون انتخاب تیم دانشکده‌ی علوم ریاضی ۷۵

طرح روی جلد

آدم‌ها و ریاضیات

طرح پشت جلد

به یاد طرحی سی‌ساله و ردشده

سرمقاله

نوید دژبرد*

«مدتی این مثنوی تاخیر شد.»

در اساطیر یونان، آتن پادشاهی افسانه‌ای دارد به نام تسئوس: فرزانه، دلیر و ماجراجو؛ یک پهلوان تمام‌عیار و مورد ستایش آتنی‌ها در طول اعصار. به روایت پلوتارک این ستایش در حدی بود که تدریجاً به یک مسئله‌ی فلسفی انجامید. تسئوس در یکی از ماجراجویی‌هایی که با جوانان آتنی ره‌سپار شده‌بود، با کشتی‌ای از جزیره‌ی کرت برمی‌گردد به آتن؛ کشتی‌ای با سی پارو. جهت بزرگ‌داشت یاد این اسطوره، اهالی آتن تصمیم به حفظ این کشتی می‌گیرند؛ بدین نحو که هر تخته‌ای را که از این کشتی می‌پوسید، با تخته‌ای جدید و مقاوم جای‌گزین می‌کردند. این تصمیم جمعی چندین قرن به درازا کشید؛ تا جایی که دیگر هیچ نشانی از کشتی اولیه باقی نماند؛ هر قطعه بارها و بارها تعویض شده‌بود. آتنی‌های نکته‌سنج‌تر از خود می‌پرسیدند آیا این همان کشتی‌ای‌ست که بود؟

دوره‌ی نخست هیئت تحریریه‌ی مجله اواخر دهه‌ی ۶۰ شمسی شروع به کار کرد، زیر نظارت و مشاوره‌ی دکتر یحیی تابش. وانگهی از آخرین شماره‌ای که دوره‌ی دوم هیئت تحریریه‌ی مجله‌ی ریاضی منتشر کرد ۵ سال می‌گذرد. در این ۵ سال توفان‌ها توفید، کشتی‌ها فروشکست، موج‌ها یکی‌یکی مشت بر ساحل کوبیدند و محو شدند. گاهی به رخوت زیستیم، که نکند دیگری سلامت‌مان را تهدید کند؛ گاهی به وحدت، که خدا کند از آشوب زمانه برهیم. چه در صحنه‌ی حیات تحصیلی و چه در عرصه‌ی اجتماعی.

دوره‌ی سوم با ازسرگذراندن چنین شرایطی تشکیل شد. دوباره جوان‌هایی پیدا شده‌اند که می‌خواهند میراث‌هایی را حفظ و احیا کنند، و من کم‌ترین آنان‌ام. جوانانی که می‌خواهند یادآوری کنند در دانش‌کده‌ی علوم ریاضی فعالیتی وجود داشت که، با محوریت یک مجله، ساختاری نو در بدنه‌ی دانش‌جویی القا می‌کرد و پیوندهایی انتزاعی و انضمامی با جامعه‌ی آکادمیک برقرار می‌ساخت. کشتی تسئوس بازسازی شده و آماده‌ی شکافتن دریا، ولو ــبه تعبیری ــ همان کشتی‌ای که بود نباشد، ولو ابرهایی تاریک افق را پوشانده‌باشد.

این شماره به دکتر یحیی تابش تقدیم می‌شود. ممکن است تعبیرتان از ایشان ناخدا باشد، یا ممکن است ترجیح دهید یک فانوس چشم‌گیر تصورش کنید. با هر استعاره‌ای در ذهن، همه متفق‌ایم که ایشان چه حقی بر گردن نشریات ریاضی کشور دارد، و مجله‌ی ریاضی شریف نیز مستثنا از این دسته نیست.

*سردبیر مجله‌ی ریاضی شریف، دانشجوی کارشناسی‌ارشد ریاضی، دانشگاه صنعتی شریف

آن‌ها که می‌نویسند.

امیر اصغری *

۱. آن‌ها که می‌نویسند.

می‌دانم! می‌دانم! بعد از این همه سال نوشتن و سر به دیوار کوفتن، باید عنوان آنچه را که می‌نویسم به گونه‌ای انتخاب کنم که از محتوای آن چیزی بگوید. مثلاً می‌دانم وقتی می‌خواهم چیزی بنویسم در مورد مجله‌های ریاضی ترویجی در ایران و نقش پررنگ یحیی تابش در تولید آن‌ها از صفر تا صد، احتمالاً خوب نیست که عنوان نوشته را بگذارم «آن‌ها که می نویسند». به هر حال امیدوارم در انتها قانع شوید که عنوان واقعاً ربطی به نوشته داشت که این نویسنده‌ی حقیر (تعارف الکی) آن را انتخاب کرد.

۲. کمی از تاریخ مجله‌های ریاضی

یعنی نمی‌دانید چه حس خوبی است که می‌توان با وجود تارنمایی که همه‌ی مجله‌های ریاضی ایران را به کمک بسیاری از آدم‌هایی مثل شما که در حال خواندن این متن هستید گرد هم آورده، به طور مستند در مورد تاریخ مجله‌های ریاضی ایران حرف زد؟

- از اولین آن‌ها، «حل المسائل ریاضی» که فقط در حدود یک سال و توسط سه تازه فارغ‌التحصیل دارالفنون که هر کدام بعداً آدم مهمی شدند منتشر می‌شد؛
- تا شاید معروف‌ترین آن‌ها، «نشر ریاضی» که به مدت نوزده سال و توسط آدم‌هایی که قبل و بعد از نشر ریاضی آدم‌های مهمی بودند، اداره می‌شد؛
- تا مجله‌های دانشجویی مثل «مجله‌ی ریاضی شریف» که هرازگاهی (به طور هرازگاهی‌ای هرازگاهی) توسط باقالی‌های دانشکده ریاضی دانشگاه شریف هرازگاهی می‌شد.

قبل از اینکه خون‌تان به جوش بیاید که ای وای به بچه‌های نازنین دانشکده ریاضی شریف بی‌احترامی شد و از این چیزها، لطفاً کمی دندان روی جگر بگذارید تا نوشته به انتها برسد. برگردم؛ از اولین مجله ریاضی که در ۱۳۰۶ منتشر شد تا الان که این متن نوشته می‌شود ۹۶ سال می‌گذرد. یحیی تابش در ۴۱ سال از این ۹۶ سال برای ایجاد و زنده‌نگه‌داشتن مجله‌های ریاضی حضور فعال داشته و هنوز دارد. فکرش را بکنید، چگونه یک نفر ممکن است ۴۱ سال ناامید نشود و مثلاً با خودش فکر نکند اصلاً این کارها در این اوضاع به چه درد می‌خورد (رکورد خود من به ۴۱ دقیقه هم نمی‌رسد).

۳. یحیی تابش

تابش در گفتگویی که در پروژه آدم‌ها و ریاضیات انجام داده‌است، تعریف می‌کند عشق او به مجله‌های ریاضی و آگاهی از اثرگذاری عمیق آن‌ها در نوجوانی و به کمک مجله ریاضی یکان شکل گرفته‌است. ولی خب آن شاعر شیرازی معروف راست می‌گفت که «عشق آسان نمود اول ولی افتاد مشکل‌ها». فکرش را بکنید می‌خواهید یک نشریه دربیاورید و اسم آن را بگذارید فرهنگ و اندیشه ریاضی و بعد در خیابان به دنبال آن باشید که یک خطاط پیدا کنید و اسم نشریه را بنویسد. بعدش هم که به هزار زور و زحمت و راضی کردن این و آن و حروف‌چینی ناموجود ریاضی و هزار اما و اگر دیگر، شماره‌ی اول مجله را درمی‌آورید، این که بنویسند زیر نظر فلانی‌ها بر دلتان سنگین می آید (در مورد فرهنگ و اندیشه ریاضی زیر نظر یحیی تابش و علی رجالی). فقط تابش باید باشید که ناامید نشوید و بروید یک جای دیگر (در این مورد، اصفهان) و با یکی دو نفر دیگر از دوستان، یک مجله‌ی دیگر منتشر کنید (در این مورد، پیک ریاضی). ولی خب این بار در شماره‌ی اول حتی نمی‌نویسید «زیر نظر» مبادا که

به کسی بربخورد. فکرش را بکنید، خدایش خود من اگر در همین نوشته چند جا اسم خودم را آن وسط نمی‌پراندم، راضی به نوشتن آن نبودم. پیک ریاضی با قوت ادامه می‌دهد تا اینکه تابش به تهران می آید و «نشر ریاضی» شروع می‌شود. می خواهید بپرسید پیک ریاضی چه می‌شود؟ خدایش آیا نمی‌توانید حدس بزنید؟ در همان وسط‌های نشر ریاضی، ناگهان خاطره و عشق یکان دوباره زنده می‌شود که ای داد بیداد پس بچه‌های مدرسه چی و نتیجه‌ی آن می‌شود ماه‌نامه‌ی ریاضیات که بعدها شد نشریه‌ی ریاضیات. اولین شماره‌ی نشر ریاضی در سال ۱۳۶۷ منتشر شد و اولین شماره‌ی ماه‌نامه‌ی ریاضیات دوازده سال بعد؛ در سال ۱۳۷۹. تابش پنج سال دنبال مجوز برای انتشار ماه‌نامه‌ی ریاضیات بوده‌است. این پنج سال را که از دوازده کم کنیم، هفت سال می‌ماند. یعنی در این هفت سال، تابش چه کار می کرده‌است؟ چون از همان اوایل نشر ریاضی آگاه بوده که نشر ریاضی برای دانشگاهی‌هاست و نه مدرسه‌ای‌ها. از طرفی به خاطر درگیری‌های چند ساله با مجله‌های ریاضی می‌دانسته‌است که چقدر راضی کردن آدم‌ها به همکاری با مجله‌ها سخت است و آن دوره‌ی یکان گذشته‌است که هی آدم‌های مختلف چیزمیز برای مجله می‌فرستادند چون قرار نبود جایی، تیکی بخورند که امتیازی بگیرند و برای دل خودشان چیزمیز می‌نوشتند. از طرفی با حساسیت آدم‌هایی مثل مهدی بهزاد و سیاوش شهشهانی به کیفیت نشر ریاضی، به نظر نمی رسید که نشر ریاضی محل مناسبی برای پیدا کردن آدم‌هایی باشد که به کار مجله‌ای برای ریاضیات مدرسه بیایند. در این اوضاع بود که تابش مهم‌ترین و تاثیرگذارترین حرکت خود را زد و در سال ۱۳۶۸ یعنی یک سال بعد از انتشار اولین شماره نشر ریاضی، مجله ریاضی شریف را پایه‌گذاری کرد (در اولین شماره اسم او به عنوان مشاور و راهنما آمده‌است).

۴. مجله‌ی ریاضی شریف

مجله‌ی ریاضی شریف یک عالمه مقاله‌ی بانمک دارد (باید اعتراف کنم وقتی دارم این تعریف‌ها را می‌نویسم، مجله‌ی ریاضی شریف در دور اول انتشار آن را در ذهن دارم)؛ مصاحبه با ریاضی‌دانانی که بعضی از آن‌ها هنوز هستند ولی در شریف نیستند و بعضی‌های دیگر کلاً نیستند و همچنین آمارها و داستان‌های هرازگاهی از وضعیت دانشکده در سال‌های مختلف (که کلی تاریخ در آن‌ها نهفته‌است و درس‌هایی که کسی نمی‌گیرد). ولی آن‌چه مجله‌ی ریاضی شریف را مجله‌ی ریاضی شریف می‌کند، آدم‌هایی هستند که با آن ساخته شدند و بعدها بعضی ریاضی‌دان شدند و بعضی ریاضی‌نویس و بعضی «ماه‌نامه‌ی ریاضیات»نویس و بعضی همه‌ی د این‌ها. در اینجا دیگر مهم نبود که اسم و رسم داشته باشی و فلانی بوده باشی. یک دانشجوی باقالی بودی که ریاضی را دوست داشتی و دوست داشتی این دوست‌داشتن را با دیگران به اشتراک بگذاری. این‌جا اولین جایی بود که امکان دیده‌شدن داشتی، اسم تو آن‌جا بود، بخشی از تاریخ دانشکده‌ی ریاضی شریف بود، بخشی که می‌توانست دیده شود؛ حالا اگر امروز نه، فردا یا پس‌فردا.

۵. مجله‌هایی برای نوشته‌شدن

پیک ریاضی دیگر نیست. نشر ریاضی دیگر نیست. ماه‌نامه‌ی ریاضیات دیگر نیست. مجله‌ی ریاضی شریف هست و نیست. بودن و نبودن آن بستگی به دل دانش‌جویان دوره‌های مختلف دارد. حتی وقتی هست شاید حتی توسط پنجاه نفر هم خوانده نشود. ولی باید باشد؛ باید باشد چون آن‌ها که می‌نویسند مهم‌اند. نمی‌نویسم نیاز دارند جایی برای نوشتن داشته باشند، درست‌تر است که بنویسم نیازمندیم جایی برای نوشتن داشته باشند. ریاضیات به این افراد نیاز خواهد داشت. حتی اگر مجله‌ی ریاضی شریف تنها میراث یحیی تابش بود، ریاضیات ایران را به او مدیون می‌دانم و تنها راه ادای این دین را زنده‌نگه‌داشتن مجله ریاضی شریف و همه‌ی آن مجله‌های دانشجویی می‌دانم که در دانشکده‌های ریاضی دیگری هی به طور هرازگاهی هرازگاهی منتشر می‌شوند.

* دانشگاه جان مورس لیورپول
رایانامه: a.h.asghari@ljmu.ac.uk

مجله‌ی ریاضی شریف
دوره‌ی سوم، شماره‌ی اول (بهار ۱۴۰۲)

جمع‌های گاوسی، از تقابل مربعی تا حدسیات ویل

علیرضا شاولی *

چکیده. در این مقاله درباره‌ی جمع‌های گاوسی و جمع‌های ژاکوبی و کاربردهای مختلف آن‌ها صحبت می‌شود. ابتدا با کمک این مجموع‌ها قانون تقابل مربعی را ثابت می‌کنیم و به قانون‌های تقابل درجات بالاتر نیز اشاره خواهیم کرد. سپس تعداد جواب‌های برخی معادلات چندجمله‌ای روی میدان‌های متناهی را تخمین می‌زنیم. پس از آن تابع زتای یک خم جبری تصویری روی یک میدان متناهی را معرفی کرده و حدس‌های آرتین در مورد این تابع را مطرح می‌کنیم. نهایتاً صورت حدسیات ویل را به عنوان تعمیم حدس‌های آرتین بیان خواهیم کرد.

۱. مقدمه

کارل فردریش گاوس[۱] ریاضی‌دان شهیر آلمانی، در طول عمر خود دست‌کم شش اثبات مختلف از قانون تقابل درجه‌ی دوم ارائه کرد. یکی از دلایل گاوس برای ارائه‌ی اثبات‌های مختلف، پیدا کردن اثباتی بود که بتواند برای یافتن تقابل‌هایی از درجات بالاتر نیز استفاده شود. گاوس در ۱۸۱۸ میلادی، ششمین اثبات خود را منتشر کرد و عقیده داشت این اثبات قابل تعمیم برای یافتن تقابل‌هایی از درجات بالاتر نیز هست. این اثبات مبتنی بر مطالعه‌ی مجموع‌هایی بود که اکنون جمع‌های گاوسی[۲] نامیده می‌شود. در اواسط قرن ۱۹، آیزنشتاین[۳] و ژاکوبی[۴] با استفاده از ایده‌های گاوس تقابل‌هایی از درجه‌ی سوم و چهارم را ثابت کردند. مجموع‌های گاوسی کاربردهای دیگری نیز در نظریه اعداد دارند که یکی از آن‌ها یافتن تعداد جواب‌های معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول (و یا به طور کلی‌تر روی یک میدان متناهی) است که با کارهای افراد مختلفی از جمله امیل آرتین[5] و آندره ویل[۶] در نیمه‌ی اول قرن بیستم، منجر به حدسیات مشهور ویل شد. این حدسیات سهم بسیار مهمی در جهت‌دهی به هندسه‌ی جبری مدرن در قرن بیستم داشتند.

۲. پیش‌نیازها

در این مقاله فرض شده است خواننده با نظریه اعداد و جبر مجرد در حد مقدماتی آشنایی دارد. برخی پیش‌نیازهایی که احتمال می‌رود برخی خوانندگان با آن آشنا نباشند، در حد بسیار مختصر در این بخش توضیح داده خواهند شد. خواننده برای مطالعه‌ی دقیق‌تر این مباحث می‌تواند به منابع معرفی‌شده در هر بخش مراجعه کند.

۱.۲. مانده و نامانده‌ی مربعی.

تعریف ۱.۲. فرض کنید p عددی اول و a عددی صحیح است و $p \nmid a$. گوییم a به پیمانه‌ی p یک مانده‌ی مربعی یا مانده‌ی درجه دوم است هرگاه عددی صحیح مانند x یافت شود که $x^{2} \equiv a \pmod{p}$.

---
[1] Carl Friedrich Gauss
[2] Gauss sums
[3] Gotthold Eisenstein
[4] Carl Gustav Jacob Jacobi
[5] Emil Artin
[6] André Weil

برای راحتی مانده یا نامانده بودن به پیمانه‌ی یک عدد اول را با نماد لژاندر[1] نشان می‌دهند که به صورت زیر تعریف می‌شود:

$$\left(\frac{a}{p}\right)=\begin{cases}+۱ & \text{مانده مربعی } a\\ -۱ & \text{نامانده مربعی } a\\ ۰ & p\mid a\end{cases}$$

فرض کنید عدد اول p فرد باشد. حال دقت کنید که به روشنی همه‌ی اعداد $۱^۲,۲^۲,\dots,(\frac{p-۱}{۲})^۲$ مانده‌ی مربعی هستند. از طرفی هر مانده‌ی مربعی به پیمانه p با یکی از این اعداد هم‌نهشت است. (چرا؟) به علاوه اعداد فوق دوبه‌دو باقی‌مانده‌های متفاوتی بر p دارند. لذا دقیقاً $\frac{p-۱}{۲}$ تا از باقی‌مانده‌های مختلف بر p مانده‌ی مربعی هستند.

قضیه ۲.۲. (محک اویلر) اگر p عددی اول و فرد و a عددی صحیح باشد آنگاه

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-۱}{۲}}\pmod p.$$

اثبات. به مرجع [۲] مراجعه کنید. □

نتیجه ۳.۲. اگر a و b اعداد صحیح و p عددی اول باشد آنگاه

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right).$$

نتیجه ۴.۲. برای هر p اول و فرد، تابع $\chi:\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times\to\{-۱,+۱\}$ با ضابطه‌ی $\chi(a)=\left(\frac{a}{p}\right)$ یک هم‌ریختی گروهی پوشا است.

از گزاره‌هایی که تا اینجا بیان کردیم نتیجه می‌شود اگر تجزیه‌ی عدد a به عوامل اول‌اش را به صورت $a=q_۱^{\alpha_۱}\dots q_k^{\alpha_k}$ داشته باشیم آنگاه $\left(\frac{a}{p}\right)=\left(\frac{q_۱}{p}\right)^{\alpha_۱}\dots\left(\frac{q_k}{p}\right)^{\alpha_k}$. لذا برای محاسبه $\left(\frac{a}{p}\right)$ کافی است برای p و q های اول، بتوانیم $\left(\frac{q}{p}\right)$ حساب کنیم. با کمک قانون تقابل مربعی ـکه در بخش‌های آینده درباره‌ی آن صحبت می‌کنیمـ می‌توان الگوریتم ساده‌ای برای این کار ارائه کرد.

۲.۲. حلقه‌ی اعداد صحیح جبری.

تعریف ۵.۲. به یک عدد مختلط $\alpha\in\mathbb{C}$ جبری گوییم هرگاه ریشه‌ی یک چندجمله‌ای با ضرایب صحیح باشد. مثلاً $۱+\sqrt{۲}$ و $\frac{\sqrt[۳]{۲}}{۳}$ اعداد جبری هستند. (چرا؟)

تعریف ۶.۲. به یک عدد مختلط $\alpha\in\mathbb{C}$ صحیح جبری گوییم هرگاه ریشه‌ی یک چندجمله‌ای تکین با ضرایب صحیح باشد. مثلاً $۱+\sqrt{۲}$ یک عدد صحیح جبری است اما $\frac{\sqrt[۳]{۲}}{۳}$ صحیح جبری نیست. (چرا؟) مجموعه اعداد صحیح جبری را با نماد Ω نشان می‌دهیم.

قضیه ۷.۲. مجموعه‌ی اعداد جبری (با ضرب و جمع معمولی مختلط) یک میدان و مجموعه اعداد صحیح جبری یک زیرحلقه‌ی آن است.

اثبات. به مرجع [۲] مراجعه کنید. □

تعریف ۸.۲. گوییم عدد صحیح جبری a عدد صحیح جبری b را عاد می‌کند و می‌نویسیم $a\underset{\Omega}{\mid}b$، هرگاه عدد صحیح جبری c یافت شود که $ac=b$. مثلاً در Ω، $\sqrt{۶}$ بر $\sqrt{۲}$ بخش‌پذیر است.

تعریف ۹.۲. گوییم عدد صحیح جبری a با عدد صحیح جبری b به پیمانه‌ی m هم‌نهشت است و می‌نویسیم $a\underset{\Omega}{\equiv}b\pmod m$ هرگاه $m\underset{\Omega}{\mid}a-b$.

[1] Legendre symbol

لم ۱۰.۲. فرض کنید $P(x) = a_n x^n + \dots + a_\circ$ یک چندجمله‌ای با ضرایب صحیح باشد و $\frac{p}{q}$، که p و q اعدادی صحیح و نسبت به هم اول هستند، ریشه‌ای گویا از آن باشد. آنگاه $q \mid a_n$.

اثبات لم فوق ساده است و آن را به عهده‌ی خواننده می‌گذاریم. نتیجه‌ی زیر فوراً از لم فوق حاصل می‌شود و در ادامه بسیار برای ما مفید خواهد بود.

نتیجه ۱۱.۲. اگر $a, b \in \mathbb{Z}$ و $a \underset{\Omega}{\mid} b$ آنگاه $a \underset{\mathbb{Z}}{\mid} b$.

لم ساده‌ی زیر که عیناً تعمیم لم مشابهی برای اعداد صحیح است، در آینده به کار خواهد آمد. برای اثبات آن کافی است از بسط دوجمله‌ای نیوتون استفاده کنید که آن را به خواننده واگذار می‌کنیم.

لم ۱۲.۲. برای عدد اول p و اعداد صحیح جبری a و b داریم

$$(a+b)^p \underset{\Omega}{\equiv} a^p + b^p \pmod p.$$

۳.۲. میدان‌های متناهی. ساده‌ترین مثال از یک میدان متناهی، میدان متناهی p عضوی برای یک p اول است که آن را با نماد $\mathbb{F}_p$ نشان می‌دهیم. البته میدان‌های متناهی دیگری نیز وجود دارند. در واقع برای هر p اول و k طبیعی، یک و تنها یک میدان p^k عضوی (در حد یک‌ریختی میدانی) وجود دارد. خواننده برای آشنایی مفصل با این میدان‌ها می‌تواند به هر کتاب مرجعی درباره نظریه‌ی میدان‌ها، مثلاً مرجع [۴]، رجوع کند.

۳. قانون تقابل مربعی

اولین بار اویلر[1] در قرن هجدهم میلادی صورت‌بندی دقیق قانون تقابل مربعی[2] را انجام داد. این قانون به طرز غیرمنتظره‌ای، برای p و q اول و فرد، داشتن یا نداشتن جواب برای معادله‌ی $x^۲ \equiv p \pmod q$ را به داشتن یا نداشتن جواب برای معادله‌ی $x^۲ \equiv q \pmod p$ مرتبط می‌سازد. این قضیه اولین بار توسط گاوس در سال ۱۷۹۶ میلادی به طور کامل ثابت شد. او این قضیه را یکی از زیباترین قضایای ریاضیات می‌دانست. همان طور که در مقدمه اشاره شد، گاوس اثبات‌های مختلفی برای این قضیه یافته‌بود. اثباتی که ما این جا می‌آوریم ساده‌شده‌ی آخرین اثبات گاوس از این قضیه است که در ۱۸۱۸ میلادی منتشر شد. قبل از این که صورت قانون تقابل مربعی را بیان و آن را ثابت کنیم، با استفاده از ایده‌ی آن اثبات، مقدار $\left(\frac{۲}{p}\right)$ را برای p های اول حساب می‌کنیم.

قضیه ۱.۳. برای هر p اول و فرد داریم:

$$\left(\frac{۲}{p}\right) = \begin{cases} +۱ & p \equiv \pm ۱ \pmod ۸ \\ -۱ & p \equiv \pm ۳ \pmod ۸ \end{cases}$$

اثبات. فرض کنید $\zeta = e^{\frac{۲\pi i}{۸}}$ یک ریشه هشتم واحد باشد. در این صورت به سادگی $\sqrt{۲} = \zeta + \zeta^{-۱}$. پس $۲^{\frac{p-۱}{۲}} = (\zeta + \zeta^{-۱})^{p-۱}$. حال به یاد بیاورید $\left(\frac{۲}{p}\right) \equiv ۲^{\frac{p-۱}{۲}} \pmod p$. از طرفی دقت کنید اعداد ζ و $\zeta^{-۱}$ اعداد صحیح جبری هستند. (چرا؟) پس

$$۲^{\frac{p-۱}{۲}} \times (\zeta + \zeta^{-۱}) = \left(\zeta + \zeta^{-۱}\right)^p \underset{\Omega}{\equiv} \zeta^p + \zeta^{-p} \pmod p$$

حال چون ζ ریشه هشتم واحد بود، اگر $p \equiv \pm ۱ \pmod ۸$ آن‌گاه $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-۱}$ و اگر $p \equiv \pm ۳ \pmod ۸$ آن‌گاه $\zeta^p + \zeta^{-p} = -\left(\zeta + \zeta^{-۱}\right)$ بنابراین اگر $p \equiv \pm ۱ \pmod ۸$ آن‌گاه

$$۲^{\frac{p-۱}{۲}} \times (\zeta + \zeta^{-۱}) \underset{\Omega}{\equiv} \zeta + \zeta^{-۱} \pmod p$$

و اگر $p \equiv \pm ۳ \pmod ۸$ آن‌گاه

$$۲^{\frac{p-۱}{۲}} \times (\zeta + \zeta^{-۱}) \underset{\Omega}{\equiv} -\left(\zeta + \zeta^{-۱}\right) \pmod p$$

[1] Leonhard Euler
[2] law of quadratic reciprocity

با یک استدلال ساده می‌توان نشان داد در حلقه‌ی Ω عدد p و $\zeta+\zeta^{-1}$ نسبت به هم اول اند و با ساده‌کردن $\zeta+\zeta^{-1}$ از دو طرف هم‌نهشتی‌ها و استفاده از نتیجه‌ی ۱۱.۲ و محک اویلر می‌توان حکم را ثابت کرد. ولی اینجا استدلال مقدماتی دیگری می‌آوریم.

با ضرب‌کردن هر یک از هم‌نهشتی‌های بالا در $(\zeta+\zeta^{-1})$ و توجه به این که $(\zeta+\zeta^{-1})^{۲}=۲$ داریم اگر $p\equiv \pm ۱ \pmod{۸}$ آن‌گاه

$$۲^{\frac{p-۱}{۲}}\times ۲ \underset{\Omega}{\equiv} ۲ \pmod{p}$$

و اگر $p\equiv \pm ۳ \pmod{۸}$ آنگاه

$$۲^{\frac{p-۱}{۲}}\times ۲ \underset{\Omega}{\equiv} -۲ \pmod{p}$$

حال چون دو طرف این هم‌نهشتی‌ها اعداد صحیح اند، طبق نتیجه‌ی ۱۱.۲ این هم‌نهشتی‌ها در $\mathbb{Z}$ هم برقرارند و لذا چون p فرد است با ساده کردن ۲ از دو طرف هم‌نهشتی‌ها حکم نتیجه می‌شود. $\square$

نکته‌ی کلیدی در اثبات بالا نمایش عدد $\sqrt{۲}$ به شکل مجموع $\zeta+\zeta^{-1}$ بود که به محاسبه‌ی $۲^{\frac{p-۱}{۲}}$ کمک کرد. اگر بتوانیم به جای عدد ۲، برای عدد اول دل‌خواه p چنین نمایشی برای $\sqrt{p}$ پیدا کنیم، می‌توان به محاسبه‌ی $\left(\frac{p}{q}\right)$ با روشی مشابه امیدوار بود. در ادامه با معرفی اولین نوع از مجموع‌های گاوسی یعنی مجموع‌های گاوسی مربعی[1] این کار را انجام خواهیم داد.

۱.۳. مجموع‌های گاوسی مربعی.

تعریف ۲.۳. فرض کنید p عددی اول و فرد و a عددی صحیح است. همچنین $\zeta=e^{\frac{۲\pi i}{p}}$ یک ریشه‌ی pام واحد باشد. در این صورت مجموع گاوسی مربعی متناظر a به صورت زیر تعریف می‌شود:

$$g_a=\sum_{i=۰}^{p-۱}\left(\frac{i}{p}\right)\zeta^{ia}$$

برای راحتی از این پس $g_۱$ را تنها با نماد g نشان می‌دهیم. لم بعدی نشان می‌دهد g_a و g ربط خیلی روشنی به هم دارند.

لم ۳.۳. برای هر a صحیح $g_a=\left(\frac{a}{p}\right).g$

اثبات. اولاً دقت کنید اگر a بر p بخش‌پذیر باشد، دو طرف صفرند و حکم واضح خواهد بود. لذا فرض کنید a بر p بخش‌پذیر نیست. چون $\left(\frac{a}{p}\right)=\pm ۱$ کافیست نشان دهیم $\left(\frac{a}{p}\right)g_a=g$. حال دقت کنید مقدار $\left(\frac{j}{p}\right)$ و ζ^j تنها به باقیمانده‌ی j بر p بستگی دارد و چون a نسبت به p اول است، $j=ai$ برای $i=۰,\cdots,p-۱$ تمام باقی‌مانده‌های مختلف به پیمانه‌ی p را می‌دهد. لذا:

$$\left(\frac{a}{p}\right)g_a=\left(\frac{a}{p}\right)\sum_{i=۰}^{p-۱}\left(\frac{i}{p}\right)\zeta^{ia}=\sum_{i=۰}^{p-۱}\left(\frac{a}{p}\right)\left(\frac{i}{p}\right)\zeta^{ia}$$
$$=\sum_{i=۰}^{p-۱}\left(\frac{ia}{p}\right)\zeta^{ia}=\sum_{j=۰}^{p-۱}\left(\frac{j}{p}\right)\zeta^{j}=g$$

$\square$

با توجه به نکته‌ای که در اثبات قضیه‌ی قبل بیان شد، مقدار $\left(\frac{i}{p}\right)$ و ζ^i تنها به باقی‌مانده‌ی i بر p بستگی دارد؛ بنابراین می‌توان تعریف مجموع گاوسی مربعی متناظر a را به صورت زیر در نظر گرفت:

$$g_a=\sum_{i\in\mathbb{F}_p}\left(\frac{i}{p}\right)\zeta^{ia}$$

همان طور که قبلاً اشاره شد به دنبال یافتن نمایشی برای $\sqrt{p}$ هستیم؛ مشابه نمایشی که برای $\sqrt{۲}$ به صورت $e^{\frac{۲\pi i}{۸}}+e^{-\frac{۲\pi i}{۸}}$ داشتیم. قضیه‌ی بعدی نشان می‌دهد مجموع‌های گاوسی مربعی در واقع چنین نمایشی را برای ما فراهم می‌کنند.

قضیه ۴.۳. برای عدد اول و فرد p داریم $g^{۲}=(-۱)^{\frac{p-۱}{۲}}\times p$.

[1] quadratic Gauss sums

اثبات. مجموع $\sum_{a=0}^{p-1} g_a g_{-a}$ را به دو روش مختلف حساب می‌کنیم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_a \left(\frac{a}{p}\right) g \left(\frac{-a}{p}\right) g = \sum_a \left(\frac{-a^2}{p}\right) g^2$$
$$= g^2 \times (p-1) \times \left(\frac{-1}{p}\right) = g^2 \times (p-1) \times (-1)^{\frac{p-1}{2}}$$

از طرف دیگر با محاسبه‌ی مستقیم داریم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_a \left(\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{ax}\right) \left(\sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^{-ay}\right)$$
$$= \sum_a \left(\sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}\right)$$
$$= \sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \sum_a \zeta^{a(x-y)}$$

حال دقت کنید اگر $x \neq y$ باشد $\sum_{a=0}^{p-1} \zeta^{a(x-y)} = 0$. (چرا؟) بنابراین کافی است مجموع فوق را روی $x = y$ حساب کنیم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{x=1}^{p-1} \left(\frac{x^2}{p}\right) \sum_{a=0}^{p-1} 1 = \sum_{x=1}^{p-1} \sum_{a=0}^{p-1} 1 = p(p-1)$$

با برابر قراردادن دو مقدار بالا که از محاسبه‌ی $\sum_a g_a g_{-a}$ حاصل شد، حکم نتیجه می‌شود. □

طبق قضیه‌ی قبل در حالتی که باقی‌مانده‌ی p بر ۴ برابر ۱ باشد $g^2 = p$ و در حالتی که باقی‌مانده‌ی p بر ۴ برابر ۳ باشد $g^2 = -p$ است. پس در حالت اول g یکی از دو مقدار $\sqrt{p}$ یا $-\sqrt{p}$ و در حالت دوم یکی از دو مقدار $i\sqrt{p}$ یا $-i\sqrt{p}$ را خواهد داشت. این که در هر حالت کدام مورد رخ خواهد داد مسئله‌ی مشکلی است. گاوس در ۱۸۰۱ حدس زده‌بود که در هر دو حالت مورد اول رخ می‌دهد؛ اما چهار سال طول کشید تا بتواند این ادعا را ثابت کند. در اینجا به این مسئله نخواهیم پرداخت.

۲.۳. اثبات قانون تقابل مربعی. در این بخش صورت قانون تقابل مربعی را بیان و با کمک نتایج بخش قبل آن را ثابت می‌کنیم. همانطور که گفته شد قانون تقابل مربعی ارتباطی بین وجود جواب برای دو معادله‌ی $x^2 \equiv p \pmod q$ و $x^2 \equiv q \pmod p$ برای دو عدد اول فرد p و q برقرار می‌کند. یعنی ارتباطی بین دو مقدار $\left(\frac{p}{q}\right)$ و $\left(\frac{q}{p}\right)$؛ که به طرز غیرمنتظره‌ای ساده است.

قضیه ۵.۳. (تقابل مربعی) برای هر دو عدد اول فرد $p \neq q$ داریم

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.$$

اثبات. طبق قضیه‌ی قبل $g^2 = (-1)^{\frac{p-1}{2}} \times p$ پس

$$g^{q-1} = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times p^{\frac{q-1}{2}}$$

در نتیجه

$$(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times \left(\frac{p}{q}\right) \times g \underset{\Omega}{\equiv} g^q \underset{\Omega}{\equiv} \left(\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^i\right)^q$$
$$\underset{\Omega}{\equiv} \sum_{i=0}^{p-1} \left(\frac{i}{p}\right)^q \zeta^{iq} = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^{iq} = g_q = \left(\frac{q}{p}\right) \times g$$

که همنهشتی‌های بالا همگی به پیمانه q هستند. پس

$$(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times \left(\frac{p}{q}\right) \times g \underset{\Omega}{\equiv} \left(\frac{q}{p}\right) \times g \pmod q$$

با ضرب کردن دو طرف در g داریم

$$(-۱)^{\frac{p-۱}{۲}\times\frac{q-۱}{۲}} \times \left(\frac{p}{q}\right) \times g^۲ \underset{\Omega}{\equiv} \left(\frac{q}{p}\right) \times g^۲$$

و چون دو طرف صحیح هستند، طبق نتیجه ۱۱.۲ این هم‌نهشتی در $\mathbb{Z}$ هم برقرار است و چون $g^۲ = (-۱)^{\frac{p-۱}{۲}} \times p$ نسبت به q اول است با ساده کردن $g^۲$ از دو طرف حکم ثابت می‌شود.

□

۴. قانون تقابل درجه سوم

در این بخش تنها می‌خواهیم صورت قانون تقابل درجه سوم را که توسط آیزنشتاین ثابت شده است، بیان کنیم. هیچ‌یک از گزاره‌های این بخش را ثابت نخواهیم کرد. مطالب این بخش در بخش‌های بعدی استفاده نخواهد شد. خواننده‌ی علاقه‌مند می‌تواند برای دیدن اثبات مطالب این بخش به مرجع [۲] مراجعه کند.

تقابل درجه سوم در حلقه‌ای بزرگ‌تر از حلقه‌ی اعداد صحیح مطرح است. این حلقه که به حلقه‌ی اعداد آیزنشتاین معروف است، از قرن نوزدهم و حتی شاید قبل از آن شناخته‌شده بود. فرض کنید ω یک ریشه سوم اولیه واحد، یا معادلاً ریشه‌ی چندجمله‌ای $x^۲ + x + ۱$ باشد. در این صورت حلقه مورد نظر به شکل زیر تعریف می‌شود:

$$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$$

می‌توان نشان داد که این حلقه یک دامنه‌ی تجزیه یکتا است.

تعریف ۱.۴. برای هر عنصر $z = a + b\omega$ در $\mathbb{Z}[\omega]$ نرم آن به صورت $N(z) = a^۲ - ab + b^۲$ تعریف می‌شود.

گزاره ۲.۴. عناصر یکه (وارون‌پذیر) حلقه $\mathbb{Z}[\omega]$ دقیقاً $\{۱, -۱, \omega, -\omega, \omega^۲, -\omega^۲\}$ هستند.

تعریف ۳.۴. دو عنصر در $\mathbb{Z}[\omega]$ را هم‌ارز گوییم هرگاه نسبت‌شان یکه باشد.

تعریف ۴.۴. عدد اول $\pi = a + b\omega$ در $\mathbb{Z}[\omega]$ را اولیه گوییم هرگاه $a \equiv ۲ \pmod ۳$ و $b \equiv ۰ \pmod ۳$. به سادگی می‌توان نشان داد هر عدد اول در $\mathbb{Z}[\omega]$ که با $۱ - \omega$ هم‌ارز نباشد، دقیقاً یک هم ارز اولیه دارد. دقت کنید تفاوت بین یک عدد اول اولیه با هم‌ارزهایش مانند تفاوت دو عدد اول p و $-p$ در اعداد صحیح است. لذا این تعریف اصلاً غیرطبیعی نیست.

از این پس در همه‌ی گزاره‌های بعدی فرض کنید عدد اول π با $۱ - \omega$ هم ارز نیست. این فرض دقیقاً مشابه فرض فردبودن اعداد اول است که در اکثر قضایای بخش ۳ وجود داشت.

گزاره ۵.۴. در حلقه‌ی $\mathbb{Z}[\omega]$ برای هر عدد اول π و هر a که بر آن بخش‌پذیر نباشد، $a^{\frac{N(\pi)-۱}{۳}}$ با یکی از سه عدد ۱ یا ω یا $\omega^۲$ به پیمانه‌ی π همنهشت است. مقدار $\left(\frac{a}{\pi}\right)_۳$ را در هر یک از این سه حالت به ترتیب ۱ یا ω یا $\omega^۲$ تعریف می‌کنیم.

گزاره ۶.۴. برای عدد اول π در $\mathbb{Z}[\omega]$ و هر a که بر آن بخش‌پذیر نباشد، $\left(\frac{a}{\pi}\right)_۳ = ۱$ است اگر و تنها اگر a به پیمانه‌ی π مانده‌ی مکعبی باشد، یعنی با یک مکعب کامل در $\mathbb{Z}[\omega]$ هم‌نهشت باشد.

گزاره ۷.۴. برای هر π اول، تابع $\chi : \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^\times \to \{۱, \omega, \omega^۲\}$ با ضابطه‌ی $\chi(a) = \left(\frac{a}{\pi}\right)_۳$ یک هم‌ریختی گروهی پوشا است.

قضیه ۸.۴. (تقابل درجه سوم) اگر π و ρ دو عدد اول متمایز و اولیه در حلقه‌ی $\mathbb{Z}[\omega]$ باشند و با $۱ - \omega$ هم‌ارز نباشند آنگاه $\left(\frac{\rho}{\pi}\right)_۳ = \left(\frac{\pi}{\rho}\right)_۳$.

۵. تعداد جواب‌های معادلات چندجمله‌ای

یکی کاربردهای جالب مجموع‌هایی از نوع مجموع‌های گاوسی، یافتن تعداد جواب‌های برخی معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول است. در ابتدای این بخش با کمک مفهوم مانده‌ی مربعی تعداد جواب‌های یک معادله‌ی ساده از درجه دو را محاسبه می‌کنیم و سپس جمع‌های گاوسی و ژاکوبی را در حالت کلی معرفی کرده و به کمک آن‌ها تعداد جواب‌های برخی معادلات از درجات بالاتر را هم حساب می‌کنیم. در این مقاله برای سادگی، ما تمرکز خود را بر روی معادلات دو متغیره (و در حالت تصویری، سه متغیره) که در واقع خم جبری هستند می‌گذاریم؛ ولی تمام این محاسبات را می‌توان به حالت nمتغیره تعمیم داد.

فرض کنید p عددی اول و فرد باشد. هدف ما در ابتدای این بخش یافتن تعداد جواب‌های معادله‌ی $x^۲ + y^۲ \equiv ۱ \pmod p$ است. به بیان دیگر می‌خواهیم در میدان $\mathbb{F}_p$ تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ را بیابیم. دو لم زیر تقریباً کار را تمام می‌کند.

لم ۱.۵. برای هر $۰ \neq a \in \mathbb{F}_p$ تعداد جواب‌های معادله $x^۲ = a$ در $\mathbb{F}_p$ برابر $۱ + \left(\frac{a}{p}\right)$ است.

اثبات. اگر a مانده‌ی مربعی باشد به روشنی معادله دو جواب (قرینه‌ی هم) دارد و اگر مانده نباشد، هیچ جوابی ندارد. لذا حکم واضح است. $\square$

لم ۲.۵. اگر p عددی اول و فرد باشد

$$\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\left(\frac{۱-a}{p}\right) = (-۱)^{\frac{p+۱}{۲}}.$$

اثبات. یک بررسی ساده نشان می‌دهد تابع

$$f:\mathbb{F}_p - \{۱\} \to \mathbb{F}_p - \{-۱\}$$

با ضابطه‌ی $f(a) = \frac{a}{۱-a}$ یک به یک و در نتیجه پوشاست. بنابراین

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\left(\frac{۱-a}{p}\right) &= \sum_{a\in\mathbb{F}_p\setminus\{۱\}} \left(\frac{a}{p}\right)\left(\frac{(۱-a)^{-۱}}{p}\right)\\ &= \sum_{a\in\mathbb{F}_p\setminus\{۱\}} \left(\frac{f(a)}{p}\right) = ۰ - \left(\frac{-۱}{p}\right) = (-۱)^{\frac{p+۱}{۲}}\end{aligned}$$

$\square$

حال می‌توانیم تعداد جواب‌های معادله‌ی $P: x^۲ + y^۲ = ۱$ را در میدان $\mathbb{F}_p$ بیابیم. برای راحتی تعداد جواب‌های معادله P را با نماد $N(P)$ نشان می‌دهیم.

قضیه ۳.۵. برای هر p اول و فرد داریم تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ در میدان $\mathbb{F}_p$ برابر $p + (-۱)^{\frac{p+۱}{۲}}$ است. به طور مختصر $N(x^۲ + y^۲ = ۱) = p + (-۱)^{\frac{p+۱}{۲}}$.

اثبات.

$$\begin{aligned}N(x^۲+y^۲=۱) &= \sum_{a+b=۱} N(x^۲=a)N(y^۲=b)\\ &= \sum_{a+b=۱}\left(۱+\left(\frac{a}{p}\right)\right)\left(۱+\left(\frac{b}{p}\right)\right)\\ &= p + \sum_{a+b=۱}\left(\frac{a}{p}\right) + \sum_{a+b=۱}\left(\frac{b}{p}\right) + \sum_{a+b=۱}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\\ &= p + (-۱)^{\frac{p+۱}{۲}}\end{aligned}$$

$\square$

۱.۵. فضای تصویری. همان طور که دیدیم تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ به پیمانه‌ی عدد اول و فرد p برابر $p + (-۱)^{\frac{p+۱}{۲}}$ است. بنابراین در حالتی که p به فرم $۴k + ۱$ باشد تعداد جواب ها $p - ۱$ و در حالت $۴k + ۳$ تعداد جواب‌ها $p + ۱$ است. این دوگانگی کمی ناخوشآیند است. در واقع این مسئله را گاوس هم بررسی کرده و تعداد جواب‌ها را در هر حالت $p + ۱$ به دست آورده است. دلیل این امر این است که گاوس برای حالت $۴k + ۱$ دو جواب در بی‌نهایت برای معادله در نظر گرفته است که در محاسبات ما از قلم افتاده‌اند. برای دقیق کردن این ایده لازم است فضای تصویری را معرفی کنیم. در اینجا تنها توضیحی مختصر در این‌باره می آید. خواننده می‌تواند جهت مطالعه‌ی مفصل‌تر به کتاب‌های هندسه‌ی جبری، مانند مرجع [۱]، مراجعه کند.

برای میدان دلخواه F مجموعه‌ی

$$A^n(F) = \{(x_۰, x_۱, ..., x_{n-۱}) | x_۰, x_۱, ..., x_{n-۱} \in F\}$$

را فضای آفین nـبعدی روی میدان F می‌نامند. حال روی مجموعه‌ی $A^{n+۱}(F) - ۰$ یک رابطه هم‌ارزی قرار می‌دهیم. دو نقطه x و x' در این مجموعه را هم‌ارز گوییم و می‌نویسیم $x \sim x'$ هرگاه $\lambda \in F^\times$ یافت شود که $x = \lambda x'$. بررسی اینکه این یک رابطه هم‌ارزی است را به عهده‌ی خواننده می‌گذاریم. فضای تصویری n بعدی روی میدان F به صورت کلاس‌های هم‌ارزی این رابطه تعریف می‌شود

$$P^n(F) = \frac{A^{n+۱}(F) - ۰}{\sim}$$

مثلاً اگر نقطه صوری ∞ را به $A^۱(F)$ بیفزایید، تناظر یک‌به‌یک طبیعی بین $P^۱(F)$ و $A^۱(F) \bigcup \{\infty\}$ وجود دارد. خواننده را تشویق می‌کنیم که این تناظر را دقیقاً بسازد.

در این مقاله ما تنها با مجموعه $P^۲(F)$ سروکار داریم. لذا کمی آن را دقیق‌تر مطالعه می‌کنیم. دقت کنید طبق تعریف برای $\lambda \in F^\times$، دو نقطه‌ی $(x_۰, x_۱, x_۲)$ و $(\lambda x_۰, \lambda x_۱, \lambda x_۲)$ در یک کلاس هم‌ارزی هستند. برای تاکید بر این نکته که تنها نسبت بین x_iها اهمیت دارد، کلاس هم‌ارزی شامل $(x_۰, x_۱, x_۲)$ را با نماد $(x_۰ : x_۱ : x_۲)$ نشان می‌دهیم. بنابراین $(\lambda x_۰ : \lambda x_۱ : \lambda x_۲) = (x_۰ : x_۱ : x_۲)$. حال نقاط $P^۲(F)$ را به دو دسته تقسیم می‌کنیم. اول نقاطی که $x_۲ \neq ۰$. به وضوح برای هر هم‌کلاس این نقطه هم مولفه سوم ناصفر است. لذا با ضرب‌کردن در λ مناسب می‌توان مولفه سوم را یک کرد. در این صورت $x_۰$ و $x_۱$ اعضای دلخواهی از F هستند. لذا این‌گونه نقاط در تناظر طبیعی با $A^۲(F)$ هستند. دسته‌ی دوم نقاطی هستند که $x_۲ = ۰$ و لذا مولفه سوم هر هم‌کلاس این نقطه هم صفر است. پس برای این نقاط، دو مولفه دیگر می‌توانند در هر $\lambda \in F^\times$ ضرب شوند. لذا این نقاط در تناظر یک‌به‌یک با $P^۱(F)$ هستند.

بنابراین $P^۲(F)$ اجتماع یک کپی از $A^۲(F)$ (نقاطی که به شکل $(x_۰ : x_۱ : ۱)$ هستند) و یک کپی از $P^۱(F)$ است (نقاطی که به شکل $(x_۰ : x_۱ : ۰)$ هستند) که آن‌ها را اصطلاحاً نقاط در بی‌نهایت گویند. خود این نقاط در بی‌نهایت هم دو دسته اند. یک کپی از $A^۱(F)$ (نقاطی که به شکل $(x_۰ : ۱ : ۰)$ هستند) و یک تک نقطه $(۱ : ۰ : ۰)$.

حال دقت کنید اگر یک چندجمله‌ای همگن سه‌متغیره مانند $f(x_۰, x_۱, x_۲)$ داشته باشیم، اگر $f(x_۰, x_۱, x_۲) = ۰$، برای هر λ ناصفر $f(\lambda x_۰, \lambda x_۱, \lambda x_۲) = ۰$. بنابراین مجموعه ریشه‌های چنین چندجمله‌ای روی $P^۲(F)$ خوش تعریف است. به عنوان مثال اگر $f(x_۰, x_۱, x_۲) = x_۰^۲ + x_۱^۲ - x_۲^۲$ و f روی یک نقطه صفر شود، روی تمام کلاس هم‌ارزی آن نقطه صفر می‌شود.

حال برای عدد اول p میدان F را میدان p عضوی $\mathbb{F}_p$ بگیرید و چندجمله‌ای $f(x_۰, x_۱, x_۲) = x_۰^۲ + x_۱^۲ - x_۲^۲$ را روی این میدان در نظر بگیرید، می‌خواهیم تعداد ریشه آن را در $P^۲(F)$ حساب کنیم. تعداد ریشه‌هایی که $x_۲$ مخالف صفر یا مساوی صفر باشد را جدا حساب می‌کنیم. اگر $x_۲$ ناصفر باشد میتوان آن را برابر یک فرض کرد و لذا باید جواب های $x_۰^۲ + x_۱^۲ - ۱ = ۰$ را در $A^۲(F)$ حساب کنیم که در بخش قبل حساب کردیم و در حالت $p = ۴k + ۱$ برابر $p - ۱$ و در حالت $p = ۴k + ۳$ برابر $p + ۱$ بود. حال جواب‌هایی که $x_۲ = ۰$ را می‌شماریم. پس باید جواب‌های $x_۰^۲ + x_۱^۲ = ۰$ در $P^۱(F)$ بشماریم. نقاط با $x_۲ = ۰$ هم دو دسته بودند. یک تک نقطه $(۱ : ۰ : ۰)$ که در معادله صدق نمی‌کند و مجموعه نقاط به شکل $(x_۰ : ۱ : ۰)$. اگر چنین نقطه‌ای در معادله صدق کند باید $x_۰^۲ + ۱ = ۰$ که در حالت $p = ۴k + ۱$ چون -۱ مانده‌ی مربعی است دو جواب دارد و اگر $p = ۴k + ۳$ چون -۱ نامانده‌ی مربعی است جوابی ندارد (دقت کنید $(۰ : ۰ : ۰)$ نقطه ای از $P^۲(F)$ نیست و

هر عضو $P^{۲}(F)$ دست کم یک مولفه ناصفر دارد). لذا در حالت $p = ۴k + ۱$ دو جواب در بی‌نهایت بجز جواب‌هایی که در $A^{۲}(F)$ داشتیم اضافه شدند و لذا در هر حالت تعداد جواب ها $p + ۱$ است.

۲.۵. کاراکترها. برای معرفی مجموع‌های گاوسی در حالت کلی لازم است ابتدا مفهوم کاراکتر را تعریف کنیم. همانطور که در قضیه ۴.۲ دیدیم $\left(\frac{a}{p}\right)$ یک همریختی گروهی از $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ به ± ۱ است. همین هم‌ریختی گروهی بودن ویژگی اساسی بود که خواص جمع‌های گاوسی مربعی را نتیجه می‌داد و همین طور کمک کرد تعداد جواب‌های معادله‌ی $x^{۲} + y^{۲} = ۱$ را در $\mathbb{F}_p$ بیابیم. لذا تعریف کلی‌تر زیر را انجام می‌دهیم.

تعریف ۴.۵. منظور از یک کاراکتر به پیمانه عدد اول p، یک هم‌ریختی گروهی به شکل زیر است

$$\chi : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} \to \mathbb{C}^{\times}$$

با توجه به اینکه هر عضو گروه $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ اگر به توان $p - ۱$ برسد برابر یک می‌شود، لذا تصویر آن عضو تحت χ یک ریشه $(p-۱)$ام واحد است و به علاوه $\chi(a^{-۱}) = \chi(a)^{-۱} = \overline{\chi(a)}$.

به عنوان مثال به وضوح $\left(\frac{a}{p}\right)$ یک کاراکتر است. به علاوه نگاشت ثابت ۱ روی $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ نیز یک کاراکتر است. این کاراکتر خاص را با نماد ε نشان می‌دهیم و آن را کاراکتر بدیهی می‌نامیم. لذا برای هر $a \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ داریم $\varepsilon(a) = ۱$. همان‌طور که نماد $\left(\frac{a}{p}\right)$ را برای حالتی که a بر p بخش‌پذیر باشد هم تعریف کردیم، مشابهاً برای هر کاراکتر غیر بدیهی اگر a بر p بخش‌پذیر باشد تعریف می‌کنیم $\chi(a) = ۰$. برای کاراکتر بدیهی تعریف می‌کنیم $\varepsilon(a) = ۱$.

پیش از تعریف جمع‌های گاوسی در حالت کلی لازم است برخی خواص مقدماتی کاراکترها را مطالعه کنیم. اولاً حاصل ضرب دو کاراکتر یک کاراکتر است. همچنین وارون یک کاراکتر هم خود کاراکتر است. پس مجموعه کاراکترها خود یک گروه است.

گزاره ۵.۵. مجموعه کاراکترها یک گروه دوری از مرتبه $p - ۱$ است و برای هر $a \in \mathbb{F}_p \neq ۱$ کاراکتر χ وجود دارد که $\chi(a) \neq ۱$.

اثبات. می‌دانیم گروه $\mathbb{F}_p^{\times}$ دوری است. فرض کنید g یک مولد آن باشد. لذا هر کاراکتر χ با تعیین $\chi(g)$ به طور یکتا تعیین می‌شود. از طرفی $\chi(g)$ باید یک ریشه $p-۱$ام واحد باشد و انتخاب هر یک از این $p - ۱$ تا ریشه‌ی $p-۱$ام واحد یک کاراکتر به ما می‌دهد. لذا تعداد کاراکترها $p - ۱$ است. از طرفی اگر مقدار $\chi(g)$ را برابر یک ریشه‌ی اولیه‌ی $p-۱$ام واحد انتخاب کنیم، این کاراکتر یک مولد برای گروه کاراکترها خواهد بود. (چرا؟) این مولد را λ بنامید. در این صورت چون $\lambda(g)$ یک ریشه‌ی $p-۱$ام اولیه‌ی واحد است، لذا برای هر $a \in \mathbb{F}_p \neq ۱$ داریم $\lambda(a) \neq ۱$. □

گزاره ۶.۵. برای هر کاراکتر غیربدیهی χ داریم $\sum_{a\in\mathbb{F}_p} \chi(a) = ۰$.

اثبات. چون $\chi \neq \varepsilon$ لذا $b \neq ۰$ وجود دارد که $\chi(b) \neq ۱$ حال

$$\chi(b)\sum_{a\in\mathbb{F}_p}\chi(a) = \sum_{a\in\mathbb{F}_p}\chi(ab) = \sum_{c\in\mathbb{F}_p}\chi(c) = \sum_{a\in\mathbb{F}_p}\chi(a)$$

پس $(\chi(b) - ۱)\sum \chi(a) = ۰$ و چون $\chi(b) \neq ۱$ حکم نتیجه می‌شود. □

گزاره ۷.۵. برای هر $a \neq ۱$ در $\mathbb{F}_p$ داریم $\sum_{\chi}\chi(a) = ۰$ که جمع روی همه‌ی کاراکترهاست.

اثبات. طبق گزاره ۵.۵ کاراکتر λ موجود است که $\lambda(a) \neq ۱$. پس

$$\lambda(a)\sum_{\chi}\chi(a) = \sum_{\chi}\lambda(a)\chi(a) = \sum_{\chi}(\lambda\chi)(a) = \sum_{\chi}\chi(a)$$

و چون $\lambda(a) \neq ۱$ حکم نتیجه می‌شود.

□

از نظریه اعداد مقدماتی می‌دانیم برای $a \in \mathbb{F}_p$ ناصفر، معادله‌ی $x^n = a$ در میدان $\mathbb{F}_p$ جواب دارد، اگر و تنها اگر $a^{\frac{p-1}{d}} = 1$ که $d = (p-1, n)$. لزوم این شرط به دلیل قضیه‌ی کوچک فرما و کفایت آن به دلیل وجود ریشه‌ی اولیه به پیمانه p است. به علاوه به آسانی می‌توان دریافت تعداد جواب‌ها دقیقاً برابر d است. از این به بعد فرض کنید $p-1$ بر n بخش‌پذیر است تا محاسبات راحت‌تر باشد. لذا معادله‌ی $x^n = a$ دقیقاً n جواب متمایز خواهد داشت اگر و تنها اگر $a^{\frac{p-1}{n}} = 1$. به کمک کاراکترها می‌توان فرمولی برای این تعداد جواب‌ها نوشت. قضیه‌ی بعد را به عنوان تعمیمی از لم ۱.۵ ببینید.

قضیه ۸.۵. اگر $n|p-1$ آنگاه

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$$

که مجموع فوق روی همه‌ی کاراکترهایی است که مرتبه‌ی آن‌ها در گروه کاراکترها، n را می‌شمارد.

اثبات. اولاً چون گروه کاراکترها دوری است، دقیقاً n کاراکتر وجود دارد که مرتبه آن‌ها n را بشمارد (این برای هر گروه دوری درست است). برای $a = 0$ حکم واضح است. برای $a \neq 0$ اگر $x^n = a$ جواب داشته باشد، برای هر یک کاراکترهایی که مرتبه آن‌ها n را بشمارد داریم:

$$\chi(a) = \chi(x^n) = \chi^n(x) = \varepsilon(x) = 1$$

و لذا $n = \sum_{\chi^n=\varepsilon} 1 = \sum_{\chi^n=\varepsilon} \chi(a)$ که همان تعداد جواب‌های معادله است. در حالتی که $x^n = a$ جواب نداشته باشد باید نشان دهیم مجموع مورد نظر صفر است که عیناً مشابه اثبات گزاره‌ی ۷.۵ است و به خواننده واگذار می‌شود. (دقت کنید مجموعه‌ی کاراکترهایی که مرتبه آن‌ها n را می‌شمارد یک گروه است.) □

۳.۵. جمع‌های گاوسی. حال می‌توانیم مجموع‌های گاوسی را در حالتی کلی‌تر معرفی کنیم. اثبات تمام قضایای این بخش عیناً مشابه اثبات‌هایی است که در حالت مجموع‌های گاوسی مربعی برای آن‌ها ارائه کردیم، لذا از تکرار اثبات‌ها می‌پرهیزیم. توصیه می‌کنیم خواننده شخصاً اثبات‌ها را کامل کند.

تعریف ۹.۵. برای هر p اول، $a \in \mathbb{F}_p$ و کاراکتر χ به پیمانه‌ی p، جمع گاوسی متناظر آن‌ها به شکل زیر تعریف می‌شود

$$g_a(\chi) = \sum_{i \in \mathbb{F}_p} \chi(i)\zeta^{ia}$$

که $\zeta = e^{\frac{2\pi i}{p}}$ ریشه‌ی pام واحد است.

برای راحتی از این پس g_1 را تنها با نماد g نشان می‌دهیم. لم زیر تعمیم لم ۳.۳ است. اثبات آن نیز کاملاً شبیه لم ۳.۳ است و به خواننده واگذار می‌شود.

لم ۱۰.۵. برای هر a و χ داریم $g_a(\chi) = \chi^{-1}(a)g(\chi) = \overline{\chi(a)}g(\chi)$

قضیه بعدی تعمیم قضیه ۴.۳ است که مهم‌ترین قضیه در بخش جمع‌های گاوسی مربعی بود.

قضیه ۱۱.۵. برای هر کاراکتر غیربدیهی χ داریم

$$g(\chi)g(\overline{\chi}) = \chi(-1)p$$

و از طرفی چون $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$ بنابراین $|g(\chi)| = \sqrt{p}$.

اثبات. با محاسبه دوگانه‌ی $\sum_a g_a(\chi)\overline{g_a(\chi)}$ کاملاً مشابه اثبات قضیه‌ی ۴.۳ حکم حاصل می‌شود. تکمیل اثبات را به عهده‌ی خواننده می‌گذاریم. □

۴.۵. جمع‌های ژاکوبی. در بخش‌های قبلی، برای اثبات قضیه ۳.۵ نیاز به محاسبه‌ی مجموع $\sum_{a+b=۱}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ داشتیم که این کار را در لم ۲.۵ انجام دادیم. این مجموع حالت خاصی از مجموع‌های کلی‌تری است که ژاکوبی در اواسط قرن ۱۹ آن‌ها را مطالعه می‌کرد. این مجموع‌ها برای محاسبه‌ی تعداد جواب‌های معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول بسیار مفید هستند. در این بخش مجموع‌های ژاکوبی را معرفی کرده و یک قضیه‌ی اساسی در مورد آن‌ها ثابت می‌کنیم که هم ارتباط آن‌ها با جمع‌های گاوسی را روشن خواهد کرد و هم در بخش‌های بعدی به کرات از آن استفاده خواهیم کرد.

تعریف ۱۲.۵. فرض کنید χ و λ دو کاراکتر به پیمانه‌ی عدد اول p باشند. مجموع ژاکوبی آن‌ها به صورت زیر تعریف می‌شود:

$$J(\chi,\lambda)=\sum_{a+b=۱}\chi(a)\lambda(b).$$

قضیه ۱۳.۵. اگر ε کاراکتر بدیهی و χ و λ دو کاراکتر غیربدیهی باشند و $\chi\lambda\neq\varepsilon$ آنگاه

الف) $J(\varepsilon,\varepsilon)=p$

ب) $J(\varepsilon,\chi)=۰$

ج) $J(\chi,\chi^{-۱})=-\chi(-۱)$

د) $J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$ و بنابراین $|J(\chi,\lambda)|=\sqrt{p}$

اثبات. قسمت الف طبق تعریف واضح است و قسمت ب همان گزاره ۶.۵ است. اثبات قسمت ج نیز عیناً همان اثبات لم ۲.۵ است. لذا تنها قسمت د را ثابت می‌کنیم. ابتدا $g(\chi)g(\lambda)$ را باز می‌کنیم:

$$g(\chi)g(\lambda)=\left(\sum_x\chi(x)\zeta^x\right)\left(\sum_y\lambda(y)\zeta^y\right)$$

$$=\sum_{x,y}\chi(x)\lambda(y)=\sum_t\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\zeta^t$$

پس کافی است مجموع را برای tهای مختلف حساب کنیم. برای $t=۰$ مجموع $\left(\sum_{x+y=۰}\chi(x)\lambda(y)\right)$ به سادگی برابر صفر است. (چرا؟) برای t ناصفر با تقسیم‌کردن x و y بر t می‌توان جمع را به یک مجموع ژاکوبی معمولی تبدیل کرد.

$$\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)=\sum_{\frac{x}{t}+\frac{y}{t}=۱}\chi(t)\lambda(t)\chi(\frac{x}{t})\lambda(\frac{y}{t})$$

$$=\chi(t)\lambda(t)\sum_{\frac{x}{t}+\frac{y}{t}=۱}\chi(\frac{x}{t})\lambda(\frac{y}{t})=(\chi\lambda)(t)J(\chi,\lambda)$$

در نتیجه

$$g(\chi)g(\lambda)=\sum_t(\chi\lambda(t))J(\chi,\lambda)\zeta^t=J(\chi,\lambda)g(\chi\lambda)$$

و لذا حکم ثابت می‌شود. حال با توجه به اینکه $|g(\chi)|=\sqrt{p}$ به روشنی داریم $|J(\chi,\lambda)|=\sqrt{p}$. □

۵.۵. محاسبه تعداد جواب‌ها با کمک مجموع ژاکوبی. با کمک مجموع‌های ژاکوبی که در قسمت قبل معرفی شد می‌توان تعداد جواب‌های بسیاری از معادلات چندجمله‌ای دومتغیره را در میدان $\mathbb{F}_p$ محاسبه کرد. در واقع مجموع ژاکوبی را می‌توان برای تعداد دل‌خواهی کاراکتر نیز تعریف کرد و به کمک آن تعداد جواب‌های معادلات با تعداد متغیر بیشتر را نیز محاسبه کرد ولی ما این جا برای سادگی تنها با معادلات دو متغیره کار می‌کنیم. در این بخش با کمک مجموع‌های ژاکوبی تعداد جواب‌های یک معادله‌ی درجه‌ی سوم خاص را به پیمانه‌ی عدد اول p حساب می‌کنیم. روشی که استفاده می‌کنیم قابل استفاده برای معادلات بسیار متنوعی است. آندره ویل در مقاله‌ی تاریخی خود (مرجع [۳]) این محاسبات را در حالت بسیار کلی انجام داده است که خواننده‌ی علاقه‌مند می‌تواند به آن مراجعه کند. ما اینجا به یک مثال خاص بسنده می‌کنیم.

فرض کنید p یک عدد اول $۳k+۱$ باشد. در این صورت سه کاراکتر وجود دارند که مرتبه آن‌ها ۳ را می‌شمارد. کاراکتر بدیهی و دو کاراکتر نابدیهی که آن‌ها را χ و λ می‌نامیم. این سه کاراکتر خود یک گروه (یک‌ریخت با $\frac{\mathbb{Z}}{۳\mathbb{Z}}$) می‌سازند. لذا $\lambda=\chi^۲$ و از طرف دیگر $\overline{\chi}=\chi^{-۱}=\chi^۲$. (چرا؟) در قضیه‌ی بعد به کمک این کاراکترها تعداد جواب‌های معادله‌ی $x^۳+y^۳=۱$ را به پیمانه p حساب می‌کنیم.

قضیه ۱۴.۵. اگر p عددی اول و $۳k+۱$ باشد و χ و λ کاراکترهای معرفی‌شده در بالا باشند آنگاه

$$N(x^۳+y^۳=۱)=p-۲+J(\chi,\chi)+J(\lambda,\lambda)$$

بنابراین از آنجا که $|J(\chi,\chi)|=|J(\lambda,\lambda)|=\sqrt{p}$ لذا

$$|N(x^۳+y^۳=۱)-p-۲|<۲\sqrt{p}.$$

اثبات. استدلال صرفاً استفاده‌ی مکرر از قضیه ۸.۵ و ۱۳.۵ است.

$$N(x^۳+y^۳=۱)=\sum_{a+b=۱}N(x^۳=a)N(y^۳=b)$$

$$=\sum_{a+b=۱}(۱+\chi(a)+\lambda(a))(۱+\chi(b)+\lambda(b))$$

$$=p+\sum_{a+b=۱}\chi(a)\chi(b)+\sum_{a+b=۱}\lambda(a)\lambda(b)+۲\sum_{a+b=۱}\chi(a)\lambda(b)$$

$$=p+J(\chi,\chi)+J(\lambda,\lambda)+۲J(\chi,\lambda)$$

$$=p+J(\chi,\chi)+J(\lambda,\lambda)+۲J(\chi,\chi^{-۱})$$

$$=p+J(\chi,\chi)+J(\lambda,\lambda)-۲\chi(-۱)$$

$$=p+J(\chi,\chi)+J(\lambda,\lambda)-۲$$

□

جواب‌های در بی‌نهایت معادله‌ی قبل را از قلم انداخته‌ایم که سعی می‌کنیم آن‌ها را اضافه کنیم. معادله‌ی همگن شده‌ی معادله‌ی قبل $x^۳+y^۳=z^۳$ است. باید جواب‌های آن را در $P^۲(\mathbb{F}_p)$ بیابیم. اگر z ناصفر باشد که می‌توان آن را یک کرد و همان جواب‌های قضیه قبل به دست می‌آیند. اگر $z=۰$ باشد (جواب‌های در بی‌نهایت) باید جواب‌های $x^۳+y^۳=۰$ را بیابیم. این نقاط خود دو دسته هستند. یک تک نقطه $(۰:۰:۱)$ که جواب نیست و یک دسته نقاطی که y آن‌ها ناصفر است، که اگر آن را یک کنیم باید جواب‌های $x^۳+۱=۰$ را بیابیم. طبق حرف‌هایی که در بخش کاراکترها زدیم این معادله ۳ جواب دارد. (دقت کنید $۳|p-۱$.) لذا با احتساب این ۳ جواب در بی‌نهایت تعداد جواب‌های معادله در فضای تصویری برابر $p+۱+J(\chi,\chi)+J(\lambda,\lambda)$ است.

۶.۵. جمع‌های گاوسی و ژاکوبی روی میدان متناهی. ما تا اینجا همواره روی میدان $\mathbb{F}_p$ که p عددی اول است کار کرده‌ایم ولی برای ادامه مسیر لازم است جواب‌های معادلات چندجمله‌ای روی سایر میدان‌های متناهی را هم در نظر بگیریم. لذا لازم است مفهوم کاراکتر، مجموع گاوسی و مجموع ژاکوبی را روی یک میدان متناهی دلخواه تعریف کنیم. تنها قسمت نابدیهی ماجرا این خواهد بود که ζ^a تنها به باقی‌مانده‌ی a بر p بستگی داشت و لذا برای $a\in\mathbb{F}_p$ معنادار بود؛ ولی روشن نیست که چطور این را به میدان متناهی دلخواه توسعه دهیم. برای این کار باید از مفهوم اثر[1] استفاده کرد.

می‌دانیم هر میدان متناهی از مشخصه‌ی p دارای $q=p^k$ عضو است، برای یک k مناسب. می‌خواهیم تابع خطی $tr:\mathbb{F}_q\to\mathbb{F}_p$ را تعریف کنیم. اگر با مفهوم اثر یک توسیع میدانی متناهی آشنایی دارید این اثر که ما اینجا تعریف خواهیم کرد در واقع اثر توسیع $\mathbb{F}_q/\mathbb{F}_p$ است. برای هر $a\in\mathbb{F}_q$ تعریف کنید

$$tr(a)=a+a^p+a^{p^۲}+\dots+a^{p^{k-۱}}.$$

می‌توان نشان داد $tr(a)\in\mathbb{F}_p$ است و به علاوه tr تابعی خطی و پوشاست. ما در اینجا این احکام را ثابت نمی‌کنیم. خواننده می‌تواند به مرجع [۲] مراجعه کند. حال می‌توانیم به کمک تابع tr مفاهیم قبلی را روی میدان متناهی دلخواه تعریف کنیم. در همه‌ی تعریف‌های زیر $q=p^k$ است.

[1] trace

تعریف ۱۵.۵. منظور از یک کاراکتر روی میدان $\mathbb{F}_q$، یک هم‌ریختی گروهی به شکل زیر است:

$$\chi : \mathbb{F}_q^{\times} \to \mathbb{C}^{\times}$$

تعریف ۱۶.۵. برای هر میدان متناهی $\mathbb{F}_q$، $a \in \mathbb{F}_q$ و کاراکتر χ روی آن، جمع گاوسی متناظر آن‌ها، به شکل زیر تعریف می‌شود:

$$g_a(\chi) = \sum_{i \in \mathbb{F}_q} \chi(i) \zeta^{tr(ia)}$$

که $\zeta = e^{\frac{2\pi i}{p}}$ ریشه‌ی pام واحد است.

تعریف ۱۷.۵. فرض کنید χ و λ دو کاراکتر روی میدان متناهی $\mathbb{F}_q$ باشند. مجموع ژاکوبی آن‌ها به صورت زیر تعریف می‌شود:

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

تمامی قضایایی که برای جمع‌های گاوسی و ژاکوبی ثابت کرده بودیم برای این جمع‌های جدید هم صادق است، فقط لازم است همه‌ی $\sqrt{p}$ ها به $\sqrt{q}$ تبدیل شود. عیناً همان اثبات‌های قبلی کار می‌کنند لذا از تکرار آن‌ها پرهیز می‌کنیم. به عنوان تمرین تکرار اثبات‌های قبلی توصیه می‌کنیم خواننده بررسی کند که تعداد جواب‌های معادله‌ی $x_2^2 = x_1^2 + x_0^2$ در $P^2(\mathbb{F}_q)$ برابر $q + 1 = p^k + 1$ است. همچنین اگر $p = 3k + 1$ باشد و χ' و λ' کاراکترهای مرتبه‌ی سه روی $\mathbb{F}_q$، آن‌گاه تعداد جواب‌های معادله‌ی $x^3 + y^3 = z^3$ در فضای تصویری برابر $q + 1 + J(\chi', \chi') + J(\lambda', \lambda')$ خواهد بود. به علاوه اگر χ و λ کاراکترهای مرتبه‌ی سه روی $\mathbb{F}_p$ باشند، می‌توان نشان داد $J(\chi', \chi') = -(-J(\chi, \chi))^k$ و $J(\lambda', \lambda') = -(-J(\lambda, \lambda))^k$؛ لذا اگر $\pi = J(\chi, \chi)$، تعداد جواب‌ها $p^k + 1 - (-\pi)^k - (-\overline{\pi})^k$ خواهد بود.

نتیجه ۱۸.۵. اگر p عددی اول باشد و $3|p-1$ و χ یکی از دو کاراکتر مرتبه سه به پیمانه‌ی p باشد و $\pi = J(\chi, \chi)$، آن‌گاه تعداد جواب‌های معادله‌ی $x^3 + y^3 = 1$ در میدان $\mathbb{F}_{p^k}$ (با احتساب نقاط در بی‌نهایت) برابر $p^k + 1 - (-\pi)^k - (-\overline{\pi})^k$ است.

۶. تابع زتای یک خم جبری

منظور ما از یک خم جبری آفین روی میدان F مجموعه جواب‌های یک معادله چندجمله‌ای به شکل $f(x, y) = 0$ است. مجموعه جواب‌های معادله همگن متناظر آن روی فضای تصویری را یک خم جبری تصویری گوییم. اولین بار امیل آرتین با الهام از تابع زتای ریمان و تابع زتای ددکیند، مفهوم تابع زتای یک خم جبری روی یک میدان متناهی را در تز دکترای خود مطرح کرد. پس از آرتین، آندره ویل تابع زتا را برای یک واریته‌ی جبری دل‌خواه تعریف کرد که بعداً به آن اشاره خواهیم کرد. تعریفی که آرتین از تابع زتای یک خم جبری ارائه داده، تعمیم طبیعی تابع زتای ریمان و ددکیند است و شباهت بین این توابع زتا را بیش‌تر نشان می‌دهد؛ اما نسبت به تعریف ویل جامعیت کمتری دارد. به علاوه تعریف ویل بسیار راحت‌تر قابل بیان است. به همین دلیل ما در این بخش تعریف ویل را در نظر خواهیم گرفت و در بخش هفتم، تعریف آرتین را خواهیم آورد.

تعریف ۱.۶. فرض کنید یک خم جبری (آفین یا تصویری) با معادله‌ی $f(x, y) = 0$ داده شده است که $f \in \mathbb{F}_p[x, y]$ چندجمله‌ای تحویل ناپذیر است. اگر تعداد جواب‌های معادله $f(x, y) = 0$ در میدان $\mathbb{F}_{p^k}$ را با N_k نشان دهیم آنگاه تابع زتای این خم جبری روی میدان $\mathbb{F}_p$ به شکل زیر تعریف می‌شود

$$\zeta(s) = exp\left(\sum_{k=1}^{\infty} \frac{N_k p^{-sk}}{k}\right)$$

که منظور از exp تابع نمایی است و s مختلط است.

با توجه به اینکه N_k در حالت خم آفین از p^{2k} و در حالت خم تصویری از $p^{2k} + p^k + 1$ بیشتر نیست (چرا؟)، لذا مجموع فوق برای $Re(s) > 2$ همگراست. در واقع با تقریب‌های بهتر برای N_k می‌توان نشان داد برای $Re(s) > 1$ همگراست.

نمایش متداول دیگری نیز برای تابع زتا وجود دارد که از تغییر متغیر $T = p^{-s}$ حاصل می‌شود. لذا تعریف می‌کنیم

$$Z(T) = exp\left(\sum_{k=1}^{\infty} \frac{N_k T^k}{k}\right)$$

بنابراین خواهیم داشت $Z(p^{-s}) = \zeta(s)$. این دو تابع تفاوت چندانی با هم ندارد و با یک تغییر متغیر ساده به هم تبدیل می‌شوند، دلیل تعریف Z صرفاً این است که گاهی کار کردن با تابع Z نسبت به ζ راحت‌تر است. در منابع مختلف هر دو این توابع را به عنوان تابع زتای خم جبری معرفی می‌کنند.

در ادامه تابع زتا را برای دو خم ساده که تعداد نقاط آن‌ها را در قسمت‌های قبل بدست آوردیم، محاسبه خواهیم کرد. ابتدا به عنوان یک مثال ساده چندجمله‌ای $f(x,y) = x^۲ + y^۲ - ۱$ را در نظر بگیرید. خم جبری تصویری متناظر آن را در نظر بگیرید. پیش‌تر نشان دادیم که تعداد نقاط این خم روی $\mathbb{F}_{p^k}$ برابر $p^k + ۱$ است. بنابراین $N_k = ۱ + p^k$ لذا داریم

$$Z(T) = exp\left(\sum_{k=۱}^{\infty} \frac{(p^k + ۱)T^k}{k}\right) = exp\left(\sum_{k=۱}^{\infty} \frac{p^kT^k + T^k}{k}\right)$$

$$= exp\left(\sum_{k=۱}^{\infty} \frac{T^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{(pT)^k}{k}\right)$$

$$= exp(-log(۱ - T))exp(-log(۱ - pT)) = \frac{۱}{۱ - T} \times \frac{۱}{۱ - pT}$$

$$= \frac{۱}{(۱ - T)(۱ - pT)}$$

بنابراین تابع $Z(T)$ یک تابع گویا بر حسب T است. می‌توان تابع $\zeta(s)$ را هم با جای‌گذاری $T = p^{-s}$ در رابطه‌ی فوق به دست آورد. دقت کنید تابع $\zeta(s)$ تنها برای $Re(s) > ۱$ همگرا بود؛ اما تابع فوق برای هر s همگراست. لذا این رابطه در واقع یک توسیع مرومورف از تابع زتا به کل صفحه‌ی مختلط بدست می‌دهد.

حال سراغ مثالی اساسی‌تر $f(x,y) = x^۳ + y^۳ - ۱$ می‌رویم. با همان نمادهای به‌کاررفته در نتیجه ۱۸.۵ کار خواهیم کرد. می‌خواهیم تابع زتای خم تصویری متناظر با f را حساب کنیم. طبق نتیجه ۱۸.۵ داریم $N_k = p^k + ۱ - (-\pi)^k - (-\overline{\pi})^k$. بنابراین

$$Z(T) = exp\left(\sum_{k=۱}^{\infty} \frac{\left(p^k + ۱ - (-\pi)^k - (-\overline{\pi})^k\right) T^k}{k}\right)$$

$$= exp\left(\sum_{k=۱}^{\infty} \frac{(pT)^k + T^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{-(-\pi T)^k - (-\overline{\pi} T)^k}{k}\right)$$

$$= \frac{exp\left(\sum_{k=۱}^{\infty} \frac{-(-\pi T)^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{-(-\overline{\pi} T)^k}{k}\right)}{(۱ - T)(۱ - pT)}$$

$$= \frac{(۱ + \pi T)(۱ + \overline{\pi} T)}{(۱ - T)(۱ - pT)}$$

همان طور که می‌بینید تابع Z برای این خم هم یک تابع گویا بر حسب T شد و این رابطه توسیع تحلیلی مرومورفی برای Z و ζ به کل صفحه می‌دهد. به اضافه تابع Z دارای دو ریشه $-\frac{۱}{\pi}$ و $-\frac{۱}{\overline{\pi}}$ هم می‌باشد. طبق قضایایی که برای جمع‌های ژاکوبی ثابت کرده بودیم می‌دانیم $\sqrt{p} = |\pi|$ لذا نرم این دو ریشه $p^{-\frac{۱}{۲}}$ است. پس اگر تغییر متغیر $T = p^{-s}$ را اعمال کنیم تابع $\zeta(s)$ دارای ریشه‌هایی با بخش حقیقی $\frac{۱}{۲}$ است (دقت کنید $|p^{-s}| = p^{-Re(s)}$). سعی کنید همه‌ی این ریشه‌ها را دقیقاً بیابید.

امیل آرتین در سال ۱۹۲۳ در تز دکترای خود تابع زتا را برای خم‌هایی به شکل $y^۲ = P(x)$ که به آن‌ها خم‌های ابربیضوی[1] می‌گویند، برای برخی چندجمله‌ای‌های خاص P محاسبه کرد. آرتین از روی این محاسبات حدس زد که برای هر خم جبری تصویری بدون تکینگی، تابع $Z(T)$ یک تابع گویا است و به علاوه تمام ریشه‌های آن دارای نرم $p^{-\frac{۱}{۲}}$ هستند یا به عبارت دیگر همه ریشه‌های تابع $\zeta(s)$ روی خط $Re(s) = \frac{۱}{۲}$ قرار دارند. تعریف تکینگی را در ادامه آورده‌ایم.

تعریف ۲.۶. گوییم خم $f(x,y) = ۰$ در نقطه‌ی $(x_۰, y_۰)$ دارای تکینگی است هرگاه $f(x_۰, y_۰) = ۰$ (یعنی آن نقطه روی خم باشد) و به علاوه $\frac{\partial f}{\partial x}(x_۰, y_۰) = ۰$ و $\frac{\partial f}{\partial y}(x_۰, y_۰) = ۰$.

(دقت کنید مشتق یک چندجمله‌ای روی هر میدان دلخواه به طور صوری قابل تعریف است.)

[1] hyperelliptic curve

حدس آرتین دوگان حدس ریمان برای تابع زتای ریمان است. در بخش بعدی بیش‌تر درباره‌ی شباهت این دو صحبت می‌کنیم. در سال ۱۹۳۴ هلموت هسه[1] موفق شد حدس‌های آرتین را برای حالتی که P درجه‌ی سه باشد (حالت خم بیضوی) ثابت کند. در سال ۱۹۴۸ آندره ویل حدس‌های آرتین را برای خم دل‌خواه ثابت کرد و تعمیمی از حدسیات آرتین برای واریته‌ی تصویری دل‌خواه ارائه کرد.

۷. توابع زتا

در این بخش تعریف تابع زتای ریمان و ددکیند را یادآوری می‌کنیم و نحوه‌ی تعریف تابع زتا توسط آرتین را بازگو می‌کنیم. هدف این بخش صرفاً دادن شهودی درباره شباهت این دو نوع تابع زتا است و چیز خاصی اثبات نخواهیم کرد. هم‌چنین در بخش‌هایی فرض می‌کنیم خواننده با مفاهیم اولیه‌ی نظریه جبری اعداد آشناست.

۱.۷. تابع زتای ریمان. همان‌طور که احتمالاً می‌دانید، در اواسط قرن نوزدهم، مطالعه‌ی حدس اعداد اول که توسط گاوس مطرح شده بود، ریمان را به سمت مطالعه‌ی تابع زتا که به صورت زیر تعریف می‌شود سوق داد.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

در واقع افراد مختلفی از جمله اویلر نیز این تابع را برای s های حقیقی مطالعه کرده‌بودند؛ ولی ریمان احتمالاً اولین شخصی است که این تابع را به عنوان تابعی مختلط مطالعه کرده است. به سادگی می‌توان دید این تابع برای $Re(s) > 1$ یک تابع هولومورف است. ریمان نشان داد این تابع گسترشی مرومورف به کل صفحه‌ی مختلط دارد که تنها یک قطب ساده در $s = 1$ خواهد داشت. اگر به یاد داشته باشید، تابع زتای یک خم جبری تصویری نیز برای $Re(s) > 1$ تابعی هولومورف بود و اگر حدس آرتین مبنی بر گویا بودن تابع $Z(T)$ را بپذیریم گسترشی مرومورف به کل صفحه خواهد داشت.

ریمان متوجه شد که می‌تواند حدس گاوس در مورد توزیع اعداد اول را به مکان صفرهای توسیع مرومورف تابع زتای ریمان مرتبط سازد. کلید ارتباط بین تابع زتا و اعداد اول، فرمول حاصل ضربی زیر است که اویلر نیز از آن مطلع بود و درستی آن صرفاً به دلیل وجود یکتایی تجزیه در اعداد طبیعی است.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in Primes} \left(\sum_{n=1}^{\infty} \frac{1}{p^{ns}} \right) = \prod_{p \in Primes} \left(\frac{1}{1 - p^{-s}} \right)$$

به دلایلی که ذکر شد ریمان به مطالعه‌ی صفرهای این تابع علاقه‌مند شد. می‌توان نشان داد تابع زتای ریمان در نقاط $s = -2k$ که k عددی طبیعی است ریشه دارد. اگر این ریشه‌ها را کنار بگذاریم، ریمان حدس زد که تمام ریشه‌های دیگر تابع زتا روی خط $Re(s) = \frac{1}{2}$ قرار دارند. این حدس که به فرضیه‌ی ریمان مشهور است، همچنان یکی از مهم‌ترین مسائل باز در نظریه‌ی اعداد و در تمام ریاضیات است.

۲.۷. میدان‌های عددی و تابع زتای ددکیند. ددکیند از بنیان‌گذاران نظریه جبری اعداد در قرن نوزدهم بود. او با الهام از کارهای ریمان، تابع زتا را برای یک توسیع متناهی دلخواه از اعداد گویا تعریف کرد که در این بخش آن را توضیح خواهیم داد. فرض کنید α یک عدد جبری روی $\mathbb{Q}$ و لذا $K = \mathbb{Q}(\alpha)$ یک توسیع متناهی $\mathbb{Q}$ باشد. به چنین میدان‌هایی میدان‌های عددی[2] گویند. حلقه‌ی اعداد صحیح میدان عددی K به صورت $O_K = K \cap \Omega$ تعریف می‌شود که Ω حلقه‌ی همه‌ی اعداد صحیح جبری است که در بخش ۲ آن را معرفی کردیم. حلقه‌ی O_K در نظریه اعداد کاربرد زیادی دارد. این حلقه‌ها در حالت کلی دامنه‌ی تجزیه‌ی یکتا[3] نیستند. کارهای کومر و ددکیند برای حل این مشکل، منجر به تعریف مفهوم ایده‌آل در حلقه‌ها شد. در واقع گرچه این حلقه‌ها دارای تجزیه یکتا نیستند؛ اما هر ایده‌آل در این حلقه‌ها را می‌توان به صورت یکتا به حاصل‌ضرب ایده‌آل‌های اول تجزیه کرد. یعنی یکتایی تجزیه در مورد ایده‌آل ها برقرار است. به چنین حلقه‌ای یک حوزه‌ی ددکیند می‌گویند. (حوزه‌ی ددکیند یک حوزه‌ی صحیح است که هر ایده‌آل آن را بتوان به طور یکتا به ضرب ایده‌آل‌های اول تجزیه کرد.)

[1] Helmut Hasse
[2] number fields
[3] unique factorization domain (UFD)

برای هر ایده‌آل I ناصفر در O_K، نرم I که آن را با نماد $N(I)$ نشان می‌دهیم، به صورت $|\frac{O_K}{I}|$ تعریف می‌شود. می‌توان نشان داد در حلقه‌هایی به صورت O_K (و نه در یک حوزه‌ی ددکیند دل‌خواه) نرم هر ایده‌آل ناصفر متناهی است. مثلا برای حالت $K = \mathbb{Q}$ حلقه‌ی O_K برابر $\mathbb{Z}$ خواهد بود و لذا ایده‌آل‌های ناصفر آن به صورت $n\mathbb{Z}$ هستند، که n عددی طبیعی است و نرم این ایده‌آل n است. لذا اعداد طبیعی دقیقاً نرم ایده‌آل‌های $\mathbb{Z}$ هستند.

ددکیند با الهام از کارهای ریمان، برای هر میدان عددی K تابع زتای ددکیند آن را به صورت زیر تعریف کرد:

$$\zeta_K(s) = \sum_{I \lhd O_K} \frac{۱}{N(I)^s}$$

با توجه به وجود یکتایی تجزیه برای ایده‌آل‌های حلقه‌ی O_K فرمول حاصل‌ضربی مشابهی برای این تابع زتا نیز به صورت زیر برقرار است

$$\sum_{I \lhd O_K} \frac{۱}{N(I)^s} = \prod_{\wp} \left(\frac{۱}{۱ - N(\wp)^{-s}} \right)$$

که حاصل‌ضرب روی همه‌ی ایده‌آل‌های اول ناصفر $\wp$ است.

ددکیند نشان داد این تابع گسترش مرومورفی به کل صفحه‌ی مختلط دارد و نیز حدس زد که همانند تابع زتای ریمان، تمام ریشه‌های نابدیهی (ریشه‌هایی که بخش حقیقی آن ها بین ۰ و ۱ است) این تابع نیز روی خط $Re(s) = \frac{۱}{۲}$ قرار دارند. به این حدس، حدس ریمان گسترش یافته[۱] می‌گویند.

۳.۷. میدان‌های تابعی و ایده‌ی آرتین. در نظریه‌ی اعداد تشابه جالبی که بین میدان‌های عددی و میدان‌های تابعی یک متغیره روی میدان‌های متناهی وجود دارد، الهام‌بخش بسیاری از تعاریف در هر یک از این دو زمینه بوده است. ابتدا کمی در مورد میدان‌های تابعی یک متغیره روی $\mathbb{F}_p$ صحبت می‌کنیم.

اگر میدان $\mathbb{F}_p(x)$ را به عنوان آنالوگی برای میدان $\mathbb{Q}$ در نظر بگیریم، حلقه‌ی $\mathbb{F}_p[x]$ نیز آنالوگ $\mathbb{Z}$ خواهد بود. در این تصویر، آنالوگی طبیعی برای میدان‌های عددی –که توسیع‌هایی به شکل $\mathbb{Q}(\alpha)$ از $\mathbb{Q}$ هستند که α روی $\mathbb{Q}$ جبری است– توسیع‌هایی به شکل $\mathbb{F}_p(x)(y)$ از $\mathbb{F}_p(x)$ هستند که y روی $\mathbb{F}_p(x)$ جبری است. لذا y در یک چندجمله‌ای با ضرایب در $\mathbb{F}_p(x)$ صدق می‌کند؛ یا به بیان دیگر x و y در یک چندجمله‌ای دو متغیره مانند $f(x, y)$ با ضرایب در $\mathbb{F}_p$ صدق می‌کنند. لذا یک آنالوگ برای حلقه‌ی O_K در یک میدان عددی K می‌تواند حلقه‌ی $O = \frac{\mathbb{F}_p[x,y]}{(f)}$ باشد. مشابه O_K این حلقه نیز یک حوزه‌ی ددکیند خواهد بود و می‌توان نشان داد (مثلاً با کمک لم زاریسکی) که هر ایده‌آل ماکسیمال آن دارای نرم متناهی است. از آن جا که در یک حوزه‌ی ددکیند ایده‌آل‌های ناصفر اول و ماکسیمال یکی هستند بنابراین می‌توان مشابه تابع زتای ددکیند، برای آن نیز تابع زتا را به صورت زیر تعریف کرد

$$\zeta(s) = \prod_{\wp \lhd O} \left(\frac{۱}{۱ - N(\wp)^{-s}} \right)$$

که حاصل ضرب روی همه‌ی ایده‌آل‌های اول ناصفر (ماکسیمال) است. این همان تابع زتای خم جبری f است که ما آن را در بخش‌های قبلی به شکلی دیگر تعریف کردیم. تعریفی که اینجا آوردیم همان تعریف آرتین است که وعده داده بودیم. آرتین حدس زد که همان طور که این تابع آنالوگ تابع زتای ریمان و ددکیند است، باید مشابهاً دارای گسترش مرومورف باشد و احتمالاً ریشه‌های نابدیهی آن روی خط $Re(s) = \frac{۱}{۲}$ باشند. محاسبات آرتین برای تعداد زیادی از خم‌های ابربیضوی، این حدس‌ها را تصدیق می‌کرد.

در واقع قبل از آرتین هم ریاضیدانی آلمانی به نام کُرنبلام[۲] تابع زتا را برای حالت خاص $O = \mathbb{F}_p[x]$ بررسی کرده بود؛ ولی آرتین اولین کسی بود که تابع زتا را برای توسیع‌های درجه دو این میدان‌ها (یا معادلاً خم‌های ابربیضوی) مطالعه کرد و حدس‌های آنالوگ فرضیه‌ی ریمان را در این حالات مطرح نمود. خواننده برای دیدن ایده‌های کرنبلام می‌تواند به منبع [۵] مراجعه کند.

[1] extended Riemann hypothesis
[2] Kornblum

۸. حدسیات ویل

همان طور که قبلاً گفتیم، هسه در سال ۱۹۳۴ موفق شد حدس‌های آرتین را برای خم‌های بیضوی بطور کامل ثابت کند و آندره ویل در ۱۹۴۸ آن‌ها را در حالت کلی ثابت کرد. در واقع ویل مسئله را در حالتی بسیار کلی‌تر از آنچه آرتین در نظر گرفته بود نیز مطالعه کرد و حدس‌های مهمی در این مورد زد که برخی از آن‌ها تعمیم طبیعی حدس‌های آرتین بودند. در این جا به طور مختصر حدسیات آندره ویل را مطرح می‌کنیم و کمی درباره‌ی تاریخچه‌ی آن‌ها توضیح می‌دهیم.

تا این جا تمام بحث‌هایی که ما مطرح کردیم درباره مجموعه‌ی صفرهای یک چندجمله‌ای دومتغیره $f(x,y)$ بوده است که در واقع همگی خم‌های جبری بوده‌اند. می‌توان هم تعداد متغیرها و هم تعداد معادلات را اضافه کرد. به بیان دقیق‌تر می‌توان مجموعه‌ی صفرهای مشترک m معادله‌ی چندجمله‌ای n متغیره را در نظر گرفت. به چنین مجموعه‌ای که در واقع زیرمجموعه‌ای از $A^n(F)$ است یک واریته‌ی جبری آفین گویند. اگر معادلات را چندجمله‌ای‌های همگن در نظر بگیرید، مجموعه صفرها روی فضای تصویری خوش‌تعریف خواهد بود که چنین مجموعه‌ای را یک واریته‌ی جبری تصویری می‌گوییم. اگر همه‌ی چندجمله‌ای ها را با ضرایب در میدان $\mathbb{F}_p$ در نظر بگیریم، می‌توان برای هر k تعداد جواب‌های دستگاه در میدان $\mathbb{F}_{p^k}$ را در نظر گرفت. این تعداد را N_kبنامید. می‌توان تابع زتای واریته را به طور مشابه به شکل زیر تعریف کرد.

$$\zeta(s) = exp\left(\sum_{k=1}^{\infty} \frac{N_k p^{-sk}}{k}\right)$$

یا مشابهاً

$$Z(T) = exp\left(\sum_{k=1}^{\infty} \frac{N_k T^k}{k}\right)$$

آندره ویل با مطالعه‌ی این تابع زتا برای واریته‌های تصویری دل‌خواهی که تکینگی ندارند و با الهام‌گرفتن از ایده‌های توپولوژی جبری به حدسیات معروف خود رسید. در واقع نکته‌ی درخشان در کارهای آندره ویل توجه به ارتباط این مسئله (با وجود ماهیت گسسته آن) با قضایایی از توپولوژی جبری بود.

اینجا اشاره‌ای به صورت حدسیات ویل می‌کنیم. حدسایت ویل درمورد تابع زتای یک واریته‌ی جبری تصویری بدون نقطه‌ی تکینگی روی یک میدان متناهی، مثلاً میدان $\mathbb{F}_p$ است.

حدس اول ویل این است که تابع $Z(T)$ برای چنین واریته‌ای حتماً تابعی گویا بر حسب T است. در واقع حدس ویل دقیق‌تر است و حتی فرم این تابع گویا را پیش‌بینی می‌کند.

حدس دوم ویل این است که ریشه‌های $\zeta(s)$ برای چنین واریته‌هایی، همگی روی خط $Re(s) = \frac{1}{2}$ هستند. این حدس را فرضیه ریمان برای میدان‌های تابعی روی یک میدان متناهی گویند.

حدس سوم آندره ویل این است که تابع زتا در یک معادله تابعی (مشابه معادله تابعی که برای تابع زتای ریمان و ددکیند وجود دارد) که $\zeta(s)$ و $\zeta(n-s)$ را به هم مرتبط می‌کند صدق می‌کند. در واقع این معادله تابعی به شکل زیر است.

$$\zeta(n-s) = \pm p^{\frac{nE}{2} - Es}\zeta(s)$$

در این رابطه n بعد واریاته (مثلا برای خم‌ها $n = 1$ است) و E شاخص اویلر است که در این مقاله به آن‌ها اشاره‌ای نمی‌کنیم. خواننده می‌تواند به کتاب‌های استاندارد هندسه‌ی جبری مراجعه کند.

علاوه بر این سه حدس ویل حدس دیگری نیز دارد که درجه‌ی چندجمله‌ای‌هایی را که در تجزیه تابع گویای $Z(T)$ ظاهر می‌شوند، به عدد بتی[1] یک فضای توپولوژیک مناسب مرتبط می‌سازد. در مورد این حدس نیز صحبت بیشتری نمی‌کنیم.

آندره ویل علاوه بر مطرح‌کردن این حدس‌ها مسیری کلی به سمت اثبات آن‌ها نیز ترسیم کرد. در واقع ویل متوجه شده‌بود وجود یک نظریه‌ی کوهومولوژی استاندارد برای واریته‌های روی یک میدان متناهی، مشابه نظریه کوهومولوژی که برای واریته‌های مختلط شناخته شده بود، می‌تواند برخی حدس‌های او را نتیجه دهد. مشاهدات ویل انگیزه‌ی اصلی برای تعریف نظریه‌های کوهومولوژی مختلف برای واریته‌های مجرد در سال‌های آتی شد و مسیر هندسه‌ی جبری را در نیمه‌ی دوم قرن بیستم مشخص کرد. حدس اول ویل یعنی گویا بودن $Z(T)$ را برنارد دوورک[2] در ۱۹۶۰ با استفاده از روش‌های pـادیک ثابت کرد. با الهام از

[1]Betti number

[2]Bernard Dwork

ایده‌هایی که اولین بار توسط ژان پیر سِر[۱] مطرح شده بود، الکساندر گروتندیک[۲] با همکاری مایکل آرتین[۳] موفق شدند در ۱۹۶۵ یک نظریه کوهومولوژی مناسب ایجاد کنند که سه تا از حدسیات ویل (بجز فرضیه‌ی ریمان برای میدان‌های تابعی) را نتیجه می‌داد. گروتندیک برای این نتایج (و نتایجی دیگر) در سال ۱۹۶۶ برنده‌ی جایزه‌ی فیلدز شد. سرانجام سخت‌ترین قسمت حدسیات ویل یعنی فرضیه ریمان در حالت میدان‌های تابعی روی یک میدان متناهی در ۱۹۷۴ توسط پیر دلین[۴] ثابت شد. دلین برای این اثبات در ۱۹۷۸ جایزه‌ی فیلدز را برد.

مراجع

[1] Fulton, W. (2008). *Algebraic Curves: An Introduction to Algebraic Geometry.* W. A. Benjamin.

[2] Ireland, K., & Rosen, M. (1982). *A classical introduction to modern number theory*. Graduate texts in mathematics (Vol. 84). New York, NY: Springer New York.

[3] Weil, A. (1949). Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5), 497-508.

[4] Morandi, P. (1996). *Field and galois theory*. Graduate texts in mathematics (Vol. 167). New York, NY: Springer New York.

[5] Kato, K., Kurokawa, N., Saitō, T., Kurihara, M. (2000). Number Theory: introduction to class field theory. American Mathematical Soc.

* دانشجوی دکتری ریاضی، دانشگاه هایدلبرگ
رایانامه: alireza.shavali@iwr.uni-heidelberg.de

[1] Jean-Pierre Serre
[2] Alexander Grothendieck
[3] Michael Artin
[4] Pierre Deligne

مرغ یا تخم‌مرغ؟

امیرکسری جلال‌دوست*

۱. مقدمه

در این یادداشت کوتاه قصد دارم به معرفی موضوع مورد مطالعه‌ی خودم در سال اخیر بپردازم. علّیت[۱] از اساسی‌ترین موضوعات مورد توجه بشر حین مشاهده‌ی طبیعت بوده است. در طول تاریخ پدران ما شاهد وقایع و پدیده‌های بسیاری بوده‌اند که سؤال در مورد منشأ و علّت آن‌ها زمینه‌ساز پیشرفت دانش بشر و رد یا تأیید فرضیه‌ها بوده است. در بخش ۲ از اهمیت بررسی رابطه‌ی علّت و معلولی بین پدیده‌ها خواهیم گفت و با اشاره به مثال‌های واقعی نشان می‌دهیم که چگونه توجه نکردن به علّیت می‌تواند به تحلیل‌های اشتباه و بعضاً خنده‌داری منجر شود. در بخش ۳ کمی از تاریخ می‌گوییم و به کارهای انجام‌شده و نگرش‌های متنوعی که به این مسئله پرداخته‌اند اشاره‌ی کوتاهی خواهیم داشت. در بخش ۴ صحبت را با بررسی ظریف‌تر یک ابرچارچوب[۲] مدل‌سازی برای علّیت که توسط جودیا پرل[۳] بنیان‌گذاری شد، ادامه می‌دهیم. نهایتاً در بخش ۵ با معرفی یک مدل معروف و روش استنتاج تحت این مدل، صحبت را به پایان می‌بریم و در بخش ۶ برای جمع‌بندی به عناوین تعدادی از صورت‌بندی‌های رایج در مسائل استنتاج علّی می‌پردازیم. موضوع علّیت سابق بر این چارچوب در فلسفه، فیزیک و علوم اقتصادی مورد مطالعه بوده است و در هر یک از این علوم، ادبیات غنی خود را داشته است. تمرکز من در این نوشته روی کارهای مبتنی بر ابرچارچوب پرل خواهد بود، که اگر بخواهیم آن را در طبقه‌بندی سنتی علوم بیاوریم در جایی بین آمار و نظریه‌ی گراف قرار خواهد گرفت.

۲. مرز بین علم و خرافه

«افزایش مصرف بستنی در شهرهای ساحلی باعث افزایش حمله‌ی کوسه‌ها به انسان‌ها می‌شود.»

این شاید یک شروع هیجان‌انگیز برای مبحث علّیت در درس اقتصادسنجی باشد. احتمالاً تا الان متوجه لغزش این استدلال شده‌اید؛ همبستگی علّیت را نتیجه نمی‌دهد. اگر بشر به همین واقعیت ساده ایمان داشت، امروز پس از ۶۰۰۰ سال تمدن، موجودی به اسم «خرافه» زنده نمانده بود اما مشاهده می‌کنیم که بخش بسیار زیادی از زندگی ما انسان‌ها آمیخته با میل به ارائه‌ی تعابیر علّی است و مدام در لغزشگاه ساختن خرافه قرار می‌گیریم. اتفاقاً هنوز هم از ساختن تعابیر علّی مبتنی بر همبستگی لذت می‌بریم؛ برای مثال، فوتبالیست ولزی، آرون رمزی[۴] قاتل سلبریتی‌ها لقب گرفته است، چرا که گاه و بی‌گاه با گلزنی این هافبک تیم آرسنال می‌شنویم که باید منتظر مرگ یک سلبریتی باشیم و هر بار هم چنین رویدادی واقعاً اتفاق می‌افتد! طلسم آرون رمزی به نظر واقعی است. من معتقدم که هیچ انسان علم‌دوستی نباید از کنار این پدیده به سادگی بگذرد. به نقل از یک منبع معتبر[۵] فراوانی انسان‌های مشهور در جامعه بین $\frac{۱}{۲۰۰۰}$ و $\frac{۱}{۱۰۰۰۰}$ است. بیایید تصور کنیم این نسبت برای انسان‌های بسیار مشهور حداقل $\frac{۱}{۱۰۰۰۰۰}$ باشد؛ یعنی ده برابر کوچک‌تر از عددی که گزارش شده است. این یعنی حدود هشتاد هزار انسان مشهور وجود دارند، چیزی که در نگاه اول بعید به نظر می‌رسد. اگر فرض کنیم متوسط عمر سلبریتی‌ها هشتاد سال باشد، هر سلبریتی به طور متوسط سی هزار روز عمر می‌کند. حال اگر تولد و مرگ سلبریتی‌ها را یکنواخت در زمان در نظر بگیریم (به بیان دقیق‌تر، فرض کنیم این رویداد یک فرآیند پوآسون با پارامتر مناسب باشد)، نتیجه می‌شود که هر روز به طور متوسط بسیار بیش‌تر از

---
[1] Causality
[2] Meta-Framework
[3] Judea Pearl
[4] Aaron Ramsey
[5] wired.com/2013/01/the-fraction-of-famous-people-in-the-world/

یک سلبریتی خواهد مرد. با این حساب به نظر می‌رسد تمامی فوتبالیست‌ها باید قاتل سلبریتی‌ها باشند؛ اگر آرون رمزی قاتل ۲۳ چهره‌ی مشهور معرفی شود، با احتمال خیلی بالا علی دایی خودمان به تنهایی ۲۴۶ چهره‌ی مشهور را راهی گورستان کرده است. در قیاس با مثال مصرف بستنی و حمله‌ی کوسه، به نظر می‌رسد لغزش متفاوتی در تعبیر علّی رخ داده است. این لغزش‌ها به طور کامل دسته‌بندی شده‌اند و ما هم در حد حوصله‌ی بحث آن‌ها را شرح خواهیم داد. فعلاً به تعدادی مثال مشهور بسنده می‌کنیم و تحلیل لغزشی را که می‌تواند رخ بدهد به مخاطب واگذار خواهیم کرد.

- کشورهایی که مصرف سرانه‌ی شکلات بالاتری دارند، در به دست آوردن جایزه‌ی نوبل موفق‌ترند.
- مردان خوش‌قیافه‌تر، بداخلاق‌ترند (نمونه‌گیری صرفاً از مردان مجرد صورت گرفته است).
- مجموعه مثال‌های مربوط به پارادوک سیمپسون؛ به‌خصوص مثال سنگ کلیه.
- با افزایش تولید محصولات ارگانیک در آمریکا، نرخ ابتلا به اوتیسم در این کشور افزایش یافته است.
- با افزایش مصرف سرانه‌ی اینترنت، ابتلا به انواع سرطان در شهر تهران افزایش یافته است.

خوشبختانه برای جلوگیری از لغزش‌های این‌چنینی در مواردی که شناخت کافی از سازوکار طبیعت نداریم، روش‌هایی برای شناخت و فرمول‌بندی روابط علّی توسعه داده شده‌اند که در ادامه به معرفی دو کار اساسی در این حوزه خواهیم پرداخت.

۳. تاریخ ادبیات

ارسطو اولین بار یک طبقه‌بندی با عنوان علل اربعه برای علّیت بیان کرد.

- علّت مادی: چیزی که از آن گرفته شده یا چیز دیگر را تشکیل می‌دهد؛ مثلاً برنز به عنوان علّت مادی یک مجسمه‌ی برنزی.
- علّت صوری: شکل، فرم و نگرش مربوط به این که چه چیزی به نمایش گذشته شده است؛ مثلاً شکل مجسمه.
- علّت فاعلی: سبب و منبع اولیه‌ی تغییر یا رهایی یعنی صنعت‌گر و مجسمه‌ساز.
- علّت غایی: فرجام و پایان به این معنا که به چه منظوری است؛ مثلاً غایت پیاده‌روی، کم کردن وزن و غایت تطهیر و مصرف دارو، سلامتی است.

چنین تعبیری از علّت برای ما غریبه است، به طور مشخص غایت یک پدیده از دیدگاه ما نمی‌تواند علّت آن تلقی شود؛ چرا که در نظر ما گذر زمان مانعی برای وجود روابط علّی در جهت خلاف زمان خواهد بود. البته چنین نگاهی توسط رایخنباخ[۱] فیلسوف آلمانی به چالش کشیده می‌شود و اصالت زمان برای تعبیر علّی زیر سؤال می‌رود. او این دست اندیشه‌ها را در کتاب جهت زمان[۲] شرح داده است. بعدها دیوید هیوم[۳] فیلسوف اسکاتلندی طبقه‌بندی ارسطو را به واسطه‌ی مفهوم خلاف‌واقع[۴] رد کرد. خلاف‌واقع یعنی بیان گزاره‌ای در پی شرطی که واقعی نیست؛ مثلاً چنین اعایی یک ادعای خلاف‌واقع است:

«اگر مهدی طارمی در آخرین لحظات بازی ایران و پرتغال از فرصت استفاده می‌کرد، ایران قهرمان جام می‌شد.»

مفهوم خلاف‌واقع به معنی نادرست و غیرصحیح نیست؛ استفاده از این شکل استدلال صحبت درباره‌ی یک پدیده است که می‌توانست اتفاق افتاده باشد و چون هیچ وقت اتفاق نیفتاده، به آن خلاف‌واقع می‌گوییم. پس از تلاش‌های فلاسفه و در اواخر قرن نوزدهم که نظم در آمار در حال شکل‌گیری بود، رویکردهای احتمالاتی به پدیده‌ی علّیت خودشان را نشان دادند. تلاش آماردان‌ها برای درک علیّت، با معرفی مفهوم «بازگشت به سمت متوسط»[5] توسط فرانسیس گالتون آغاز شد. بعدها گالتون[۶] در این مسیر به مفهوم همبستگی[۷] رسید.

کارل پیرسون[۸]، ریاضی‌دان انگلیسی، علّیت را یک حالت خاص غیرقابل اثبات از همبستگی می‌دانست و برای اندازه‌گیری کمّی همبستگی، ضرایب همبستگی[۹] را معرفی کرد. از او نقل می‌شود که «تعبیر کردن نیرو به عنوان علّت حرکت، شبیه به تصور

[1] Reichenbach
[2] The Firection of Time
[3] David Hume
[4] Counter-Factual
[5] Regression to The Mean
[6] Francis Galton
[7] Correlation
[8] Karl Pearson
[9] Correlation Coefficients

وجود خدای درخت به عنوان علّت رشد است». او معتقد بود که علّیت صرفاً یک علاقه‌ی شدید[1] در داستان عصر مدرن علم است.

بعدها بیشتر در حوزه‌ی آمار زیستی به علّیت پرداخته شد و دانشمندانی به دنبال تعابیر علّی در پدیده‌ی وراثت بودند. در همین دوران بود که رایت[2]، آنالیز مسیر[3] را معرفی کرد و توانست مثال‌هایی از علّیت در وراثت را با کارهای خودش تفسیر کند. آماردان بزرگ انگلیسی، رونالد فیشر[4]، از منتقدان این دیدگاه بود و به دنبال او تقریباً تمامی آماردان‌ها متکی بر مفهوم همبستگی بودند و اصالتی برای علّیت قائل نمی‌شدند. در سال ۱۹۲۳، جرزی نیمن[5] لهستانی مفهوم نتایج بالقوه را معرفی کرد ولی کار او تا حدود ۵۰ سال بعد مورد توجه قرار نگرفت و حتی به انگلیسی ترجمه نشد، تا اینکه در سال ۱۹۷۴، دونالد روبین[6] مفهوم نتایج بالقوه را به عنوان زبانی برای پاسخ به سوالات علّی مطرح و اولین چارچوب کارا برای استنتاج علّی[7] را معرفی کرد. در این ۵۰ سال بی‌توجهی به کار نیمن، آماردان‌ها تحلیل رگرسیون را بیش از پیش توسعه داده بودند و مدل‌های ساختاری معادلات[8] را معرفی کردند که توسط اقتصاددان‌ها و دانشمندان دیگر علوم اجتماعی به طور جدی به کار گرفته شد و توسعه یافت، اما معمولاً از این مدل‌ها تعبیر علّی صورت نمی‌گرفت و تقدس فیشر باعث شد نگاه علّی هم شبیه به رویکرد بیزی برای مدت زیادی به تعویق بیفتد. فعالیت‌های جودیا پرل در حوزه‌ی شبکه‌های بیزی و استنتاج گرافی با طراحی یک ابرچارچوب برای مدل‌سازی روابط علّی همراه شد و او فصل جدیدی را در تحقیقات این حوزه آغاز کرد. در ادامه به دو کار اساسی روبین و پرل می‌پردازیم.

۴. مدل علّی روبین

از آن‌جایی که کار نیمن هم بسیار نزدیک به مدل روبین بود و اساس مدل الهام‌گرفته از مفهوم نتایج بالقوه بود، به این مدل عنوان نیمن-روبین را هم اتلاق می‌کنند. مفهوم نتایج بالقوه مبتنی بر شرط‌های خلاف‌واقع مطرح شد؛ باز هم صحبت از یک خروجی است که اتفاق نیفتاده است و می‌توانست اتفاق بیفتد؛ به عنوان مثال بررسی تأثیر خصوصی بودن یا دولتی بودن مدرسه بر میزان درآمد یک فرد در ۴۰ سالگی مثالی از تحلیل بر مبنای نتایج بالقوه است. هر شخصی می‌تواند یا در مدرسه‌ی خصوصی تحصیل کند یا در مدرسه‌ی دولتی و هنگامی که به ۴۰ سالگی می‌رسد مقداری درآمد خواهد داشت. برای بررسی اثر تحصیل در مدرسه‌ی خصوصی یا دولتی لازم است به سؤال شرطی خلاف‌واقع‌گونه‌ای پاسخ دهیم؛ مثلاً اگر می‌دانیم شخص در مدرسه‌ی دولتی تحصیل کرده است، لازم است به این سؤال شرطی پاسخ بگوییم که اگر همین شخص در مدرسه‌ی خصوصی تحصیل کرده بود، امروز چقدر درآمد داشت؟ تفاضل این دو مقدار درآمد، «اثر علّی» نوع مدرسه بر درآمد تلقی می‌شود.

چالش اصلی همین جا خود را نشان می‌دهد. به ازای هر شخص با ویژگی‌های خاص خودش، دقیقاً یکی از نتایج بالقوه را می‌بینیم و دقیقاً یکی را ممکن نیست ببینیم که آن را خروجی بالقوه نام‌گذاری می‌کنیم و برای محاسبه‌ی آن باید به سؤال خلاف‌واقع‌گونه‌ای که ذکر شد، پاسخ بدهیم. از این مشاهده با عنوان «مسئله‌ی اساسی استنتاج علّی» یاد می‌شود.

به این ترتیب می‌توان دید که در مورد یک مشاهده نمی‌توان استنتاج علّی ارائه کرد. ولی روبین روشی را ارائه کرد که با آن می‌توان در مورد کل جامعه مقدار «اثر علّی متوسط» را تخمین زد. اثر علّی متوسط، میانگین اثر علّی روی کل جامعه است و روشی که روبین برای تخمین این مقدار ارائه کرد، امروزه نیز در آزمایش‌ها استفاده می‌شود. این روش مبتنی بر آزمایش‌های تصادفیده[9] است.

پیش از شرح روش آزمایش‌های تصادفیده، لازم است به نکته‌ای توجه کنیم. در همان مثال مدرسه و درآمد، اگر صرفاً با مشاهده‌ی نتایجی که رخ داده است بخواهیم تعبیر علّی داشته باشیم، آنگاه لغزش‌گاه مهیبی پیش روی ما خواهد بود. با بررسی داده‌ی مشاهده‌شده (و نه حاصل آزمایش) از متغیرهای محذوف بسیاری صرف نظر خواهیم کرد؛ برای مثال بسیار معقول است که افراد از خانواده‌های ثروتمندتر تمایل بیشتری به مدارس خصوصی داشته باشند و اتفاقاً فرزندان به واسطه‌ی ثروت خانواده بتوانند کسب‌وکار پررونق‌تری ایجاد کنند و درآمد بیشتری داشته باشند. حال اگر ما عامل «واقعیت اقتصادی خانواده» را در

[1] Fetish
[2] Sewall Wright
[3] Path Analysis
[4] Ronald Fisher
[5] Jerzy Neyman
[6] Donald Rubin
[7] Causal Inference
[8] Structural Equation Models
[9] Randomized Controlled Trials

نظر نگیریم، دچار اشتباه می‌شویم و تمام اثر درآمدی را منسوب به نوع مدرسه خواهیم دانست. حتی با در نظر گرفتن عوامل این‌چنینی هنوز هم ممکن است عامل محذوفی از قلم بیفتد یا اصلاً در یکی از گروه‌ها نوع خاصی از نمونه را نداشته باشیم؛ مثلاً تصور کنید تمامی کارمندان دولتی باید فرزندان خود را در مدارس دولتی ثبت‌نام نمایند. به این ترتیب نمونه‌ی «فرزند با والدین کارمند دولت» را در یکی از دسته‌ها نخواهیم داشت و اگر این عامل تأثیر واقعی روی درآمد داشته باشد، دچار لغزش خواهیم شد.

لزوم اجرای آزمایش برای تعبیر علّی ضروری به نظر می‌رسد، لااقل مادامی که فرض خاصی در مورد داده نداشته باشیم. در روش آزمایش تصادفیده برای بررسی اثر علّی متوسط یک عامل، نمونه‌ای از جامعه گرفته می‌شود و به طور تصادفی و مستقل به دو گروه شاهد و تیمار تقسیم می‌شوند. برای گروه تیمار عامل مورد نظر فعال می‌شود و برای گروه شاهد این عامل غیرفعال می‌گردد. پس از مشاهده‌ی نتایج، میانگین متغیر هدف برای هر دو گروه محاسبه می‌شود و می‌توان به سادگی نشان داد که تفاضل میانگین آن‌ها تخمینی نااریب و سازگار برای اثر علّی متوسط خواهد بود؛ برای مثال در مورد تأثیر نوع مدرسه بر درآمد، یک آزمایش تصادفیده می‌تواند این‌چنین باشد که عده‌ای دانش‌آموز به طور تصادفی از جامعه نمونه گرفته شوند، سپس هر دانش‌آموز به احتمال برابر به گروه شاهد یا تیمار منسوب شود. برای مثال گروه شاهد را به مدارس دولتی می‌فرستیم و گروه تیمار را به مدارس خصوصی. حال تفاضل میانگین درآمد دو گروه وقتی به ۴۰ سالگی رسیدند، تخمین نااریبی از اثر علّی متوسط مدارس خصوصی (در قیاس با دولتی) روی میزان درآمد است. چنین آزمایشی در عمل ناکارآمد خواهد بود، لذا معمولاً در سازوکار تولید داده به دنبال تصادفیده شدن اتفاقی ورودی هستند؛ مثلاً تصور کنید که در یک شهر فقط مدرسه‌ی دولتی وجود داشته باشد و در شهر دیگر مدرسه‌ی خصوصی. حال با این فرض که دانش‌آموزان این دو شهر تفاوت خاصی ندارند و توزیع ویژگی‌های دانش‌آموزان این دو شهر نزدیک به هم است، می‌توان تصور کرد که یک آزمایش تصادفیده به طور اتفاقی صورت گرفته است و همگی دانش‌آموزان یک شهر باید به مدرسه‌ی دولتی می‌رفتند و همه‌ی دانش‌آموزان شهر دیگر به مدرسه‌ی خصوصی. اکنون با چارچوب روبین می‌توان استنتاج علّی انجام داد.

۵. مدل ساختاری علّی

با الهام از مدل‌های ساختاری معادلات، پرل یک چارچوب کلی‌تر و دقیق‌تر برای مدل‌سازی روابط علّی ایجاد کرد. قبل از معرفی این چارچوب لازم است با مدل‌های ساختاری علّی و برخی از مفاهیمی که او معرفی کرد، آشنا شوید.

مدل‌های ساختاری علّی یک پیاده‌سازی برای علّیت‌اند که مبتنی بر مدل‌های ساختاری معادلات طراحی شده‌اند. پس ابتدا لازم است مدل‌های ساختاری معادلات را بشناسیم. این مدل‌ها از تعدادی متغیر در مجموعه‌ی V و تعدادی معادله در مجموعه‌ی E تشکیل شده‌اند؛ که در سمت چپ هر معادله یک متغیر حاضر است و در سمت راست تابعی از باقی متغیرها. شرط لازم برای شکل‌گیری یک مدل ساختاری علّی این است که در این مجموعه معادلات دور وجود نداشته باشد؛ به تعبیر دقیق‌تر، اگر یک گراف جهت‌دار بسازیم و به ازای هر متغیر رأسی قرار دهیم و به ازای هر معادله، یال‌هایی از متغیرهای سمت راست معادله به متغیر سمت چپ وارد کنیم، این گراف بدون دور باشد.

یک مدل ساختاری علّی همان مدل ساختاری معادلات است با این تفاوت که مجموعه‌ای از متغیرها تحت عنوان متغیرهای مخدوش‌گر خارجی[1] در مجموعه‌ی N تعریف می‌شوند که از جنس متغیرهای تصادفی و به طور توأم مستقل هستند (به بیان دقیق توابعی هستند از فضای پیشامد به اعداد حقیقی). این متغیرهای مخدوش‌گر خارجی قابل مشاهده نیستند ولی با تأثیر بر دیگر متغیرها از طریق معادلات، تصادف را به باقی متغیرهای مدل منتقل می‌کنند و ما در استنتاج از طریق این مدل‌ها سعی داریم تصادف مشاهده‌شده در توزیع توأم متغیرهای مشاهده‌ای[2] را از طریق این متغیرهای مخدوش‌گر خارجی و روابط بین متغیرهای مدل توجیه کنیم.

پرل «نردبان علّیت[3]» را معرفی کرد. او در سه سطح انتزاعی ارتباط با علّیت را توصیف کرد.

- ائتلاف[4]

[1] Disturbance Exogenous Noises
[2] Observational
[3] Ladder of Causation
[4] Association

- مداخله[۱]
- خلاف‌واقع

دو موجود با هم در ائتلاف هستند اگر مشاهده‌ی یکی بر مشاهده‌ی دیگری تأثیرگذار باشد. این تأثیر لزوماً در جهت خاصی نیست و به همین دلیل باید به تفاوت همبستگی و ائتلاف توجه کرد. می‌توان ائتلاف را حالت کلی‌تری برای عدم‌استقلال در دیدگاه احتمالاتی دانست. در دیدگاه احتمالاتی، ائتلاف با ناصفر بودن ضریب همبستگی قابل تأیید کردن است، ولی با صفر بودن ضریب همبستگی، ائتلاف قابل رد کردن نیست. هیچ تعبیر علّی را نمی‌توان از ائتلاف دو متغیر تصادفی استخراج کرد؛ چرا که ممکن است هر یک علّت دیگری باشد یا علّت مشترک محذوفی در میان باشد.

مفهوم مداخله هم اولین بار توسط پرل به طور دقیق فرمول‌بندی شد. او عمل‌گر do را برای اندازه‌ی احتمال معرفی کرد و حسابان اختصاصی آن را ذیل مدل ساختاری علّی توسعه داد. اگر بخواهیم خیلی ساده‌انگارانه آن را شرح دهیم، می‌توان عمل‌گر do را پاسخی نظری به آزمایش‌های تصادفیده در حالتی که مسلط بر پارامترهای مدل هستیم، بدانیم. در مثال دانش‌آموزان و مدرسه، اگر مکانیزم حقیقی را به صورت یک مدل ساختاری علّی در نظر بگیریم، اجرای آزمایش تصادفیده در تخصیص دانش‌آموزان به مدارس را با یک عمل‌گر روی تابع اندازه‌ی احتمال تعبیر می‌کنیم که این عمل‌گر از طریق پارامترهای مدل ساختاری علّی قابل محاسبه است. اتفاقاً خود پرل سابق بر معرفی این چارچوب، چنین محاسباتی را روی شبکه‌های بیزی در زمان چندجمله‌ای محقق کرده بود که از نمونه‌های آن، الگوریتم نشر باور[۲] اوست. او با تکیه بر ایده‌های استفاده‌شده در توسعه‌ی استنتاج مبتنی بر شبکه‌های بیزی، حسابان مداخله[۳] را توسعه داد و جامعه‌ی علمی برای قدردانی نگاه راه‌گشایش در بیش از دو دهه، جایزه‌ی تورینگ سال ۲۰۱۱ را به او اعطا کرد.

در حقیقت اگر بتوانیم مدل خودمان را منطبق بر ابرچارچوب مورد نظر پرل پیاده‌سازی کنیم، حسابان مداخله این امکان را به ما خواهد داد که بدون اجرای آزمایش‌ها نتیجه را محاسبه کنیم؛ خواه این آزمایش تصادفیده باشد و خواه قطعی.

خلاف‌واقع‌ها هم در چارچوب پل قابل پیاده‌سازی‌اند و می‌توان آن‌ها را محاسبه کرد. اگر هر خلاف‌واقع، شرطی در مورد یک متغیر داخلی مطرح کند (که مثلاً معادل با یک تصمیم یا رویدادی تصادفی است)، پاسخ به سؤال این خلاف‌واقع (چه می‌شود اگر) با ثابت نگه داشتن مقادیر متغیرهای مخدوش‌گر خارجی و محاسبه‌ی دوباره‌ی متغیرهای مدل میسر خواهد بود. مدل‌های دیگری هم مبتنی بر حسابان مداخله توسعه یافته‌اند که مدل‌سازی‌های سری زمانی، دارای دور و بر پایه‌ی معادلات دیفرانسیل پاره‌ای از این دست‌اند. با توجه به اینکه شبکه‌های بیزی[۴] هم ساختارهای احتمالاتی مبتنی بر گراف‌های جهت‌دار بدون دور هستند، شباهت‌های ساختاری و بعضاً اشتراک در مفاهیم و رفتارهای آن‌ها با مدل‌های ساختاری علّی مشاهده می‌شود. بسیاری از الگوریتم‌های شبکه‌ی بیزی به توسعه‌ی مدل‌های ساختاری علّی کمک کرده‌اند.

۶. نتیجه‌گیری

مدل‌سازی محاسباتی علّیت و استنتاج علّی حدود ۱۰ سال است که مورد توجه جوامع علمی قرار گرفته است و دانشمندانی با پیش‌زمینه‌های گوناگون برای توسعه‌ی روش‌ها و ایجاد رویکردهای جدید در آن تلاش می‌کنند. مسائل بسیاری در این حوزه مطرح شده‌اند و شرایط متعددی برای استنتاج علّی صورت‌بندی شده است که برای نمونه، عناوین تعدادی از آن‌ها را در اینجا ذکر می‌کنیم.

- استنتاج در محیط‌های متعدد
- استنتاج در حضور متغیر پنهان[۵]
- استنتاج در سری‌های زمانی
- استنتاج در حالت مکانیزم‌های غیرپایا[۶]
- شرایط بُعد بالا
- پیاده‌سازی‌های موازی برای استنتاج سریع

[1] Intervention
[2] Belief Propagation
[3] Do-Calculus
[4] Bayesian Networks
[5] Hidden Variables/ Latent Variables/ Confounder
[6] Non-Stationary Causal Mechanism

- متغیرهای گسسته و حالت‌های ترکیبی
- یادگیری‌پذیری مسئله‌ی استنتاج
- یادگیری فعالانه یا منفعل ساختار علّی به کمک داده‌ی مداخله‌ای

* دانشجوی دکتری علوم‌کامپیوتر، دانشگاه کلمبیا

رایانامه: amirkasraj@gmail.com

مجله‌ی ریاضی شریف
دوره‌ی سوم، شماره‌ی اول (بهار ۱۴۰۲)

رویه‌های مینیمال و حدس دی‌جورجی

متین حاجیان *

چکیده. معادله ی آلن-کن یک معادله‌ی دیفرانسیل پاره‌ای نیم‌خطی است که هنگام بررسی مدل‌سازی ریاضی پدیده‌ی گذار فاز مطرح می‌شود. در این مقاله‌ی توصیفی قصد داریم حدس دی‌جورجی درمورد جواب‌های معادله‌ی آلن-کن را بیان کنیم و به ریشه‌های به‌وجودآمدن این حدس و تلاش‌هایی که برای حل آن انجام شده است بپردازیم. ابتدا انگیزه‌های فیزیکی مطرح‌شدن این معادله را بررسی می‌کنیم. برای این‌که انگیزه و شهود دی‌جورجی از این حدس را دریابیم نکاتی از نظریه‌ی رویه‌های مینیمال را بیان می‌کنیم و سپس به نتایجی که حول اثبات حدس دی‌جورجی به دست آمده است می‌پردازیم. هدف اصلی بیان چندی از اثبات‌ها و ایده‌های موجود حول موضوعاتی از نظریه‌ی رویه‌های مینیمال، نظریه‌ی معادلات دیفرانسیل با مشتقات جزئی و نظریه‌ی هندسی اندازه می‌باشد. از خواننده انتظار می‌رود آشنایی مقدماتی با نظریه‌ی معادلات دیفرانسیل با مشتقات جزئی و آنالیز حقیقی داشته باشد.

۱. انگیزه‌های فیزیکی

فرض کنید $\Omega \subset \mathbb{R}^n$ (زیرمجموعه‌ای کران‌دار از فضا) یک ظرف شامل نوعی سیال دوفازی باشد (به طور مثال مولکول‌های سازنده‌ی این سیال از دو نوع متفاوت باشند؛ مانند مخلوط آب و روغن). به هر حالت قرارگیری سیال در این ظرف یک تابع چگالی $u : \Omega \to [-۱, +۱]$ نسبت می‌دهیم (± ۱ نشان‌دهنده‌ی دو فاز ممکن از ذرات سیالمان هستند). در این صورت جرم کل سیال برابر است با $\int_\Omega u = m$. فرض کنید $W : \mathbb{R} \to [۰, +\infty)$ تابع چگالی انرژی این سیال باشد با این ویژگی که $W(\pm ۱) = ۰$ و $W(r) > ۰$ به ازای هر $r \neq \pm ۱$ (به چنین تابعی پتانسیل دوچاهه [۱] می‌گویند). در این صورت انرژی کل سیستم برابر است با $\mathcal{I}(u; \Omega) = \int_\Omega W(u)$. انتظار داریم سیستم در حالت تعادل کم‌ترین انرژی ممکن را داشته باشد. در این صورت مسأله‌ی یافتن حالت تعادل به مسأله‌ی زیر تبدیل می‌شود:

$$\min\{\int_\Omega W(u) : \int_\Omega u = m, u : \Omega \to [-۱, +۱]\}$$

اما این صورت‌بندی به میزان کافی دقیق نیست و انتظارات فیزیکی‌مان را از جواب‌هایی که به دست می‌دهد، برآورده نمی‌کند زیرا هزینه‌ای برای گذار فاز در آن در نظر گرفته نشده است و این باعث می‌شود که در بعضی موارد جواب مسأله یکتا نباشد و رفتارهای ناهمواری از خود نشان دهد. مثلاً قسمت‌هایی از سیال که در آن گذار فاز رخ می‌دهد می‌تواند رفتارهای به دلخواه پیچیده داشته باشد. به طور مثال فرض کنید $E \subset \Omega$ یک زیرمجموعه‌ی اندازه‌پذیر باشد به طوری که $\mu(E) = \frac{m+\mu(\Omega)}{۲}$. در این‌صورت تابع $u = \chi_E - \chi_{\Omega \setminus E}$ یک جواب این مسأله است. همان‌طور که مشاهده می‌کنید جواب مسأله در این حالت یکتا نیست و با توجه به رفتار مجموعه‌ی E می‌تواند پیچیده باشد.

فرم اصلاح‌شده‌ی تابعک نشان‌دهنده‌ی انرژی سیستم (که به انرژی گینزبرگ-لانداو [۲] معروف است و در نظریه وان در والس-کن-هیلارد [۳] [۹] برای گذار فاز معرفی می‌شود) به شکل زیر است:

$$\mathcal{I}_\epsilon(u; \Omega) = \int_\Omega \frac{\epsilon}{۲}|\nabla u|^۲ + \frac{۱}{\epsilon} W(u) \tag{۱.۱}$$

این تابعک انرژی را به ازای $\epsilon = ۱$ با $\mathcal{I}(u, \Omega)$ نشان می‌دهیم. می‌توان دید معادله‌ی اویلر-لاگرانژ این تابعک برابر است با $\epsilon \Delta u + \frac{۱}{\epsilon} W'(u) = ۰$، که به ازای $\epsilon = ۱$ و $W(x) = \frac{(۱-x^۲)^۲}{۴}$ معادله‌ی آلن-کن را به ما می‌دهد: $\Delta u = u^۳ - u$.

[1] Double well potential
[2] Ginzburg–Landau
[3] Van der Waals-Cahn-Hilliard

این معادله در حوزه‌هایی مانند بررسی ابررساناها و ابرسیالات [۱۱]، مطالعه‌ی گذار در گازها و جامدات [۱۲، ۱۳] و حتی در مطالعات کیهان‌شناسی [۱۴، ۱۵] نیز ظاهر می‌شود.

حدس دی‌جورجی درمورد ویژگی‌های تقارنی رده‌ی خاصی از جواب‌های معادله‌ی آلن-کن است. به طور دقیق‌تر این حدس بیان می‌کند که به ازای $n \leq ۸$ جواب‌هایی از معادله‌ی آلن-کن در $\mathbb{R}^n$ که کران‌دار و در یک جهت صعودی‌اند، توابعی یک‌بعدی‌اند یا معادلاً سطح ترازهایشان ابرصفحه‌هایی در فضا هستند. برای دریافت شهود پشت این حدس و اثبات‌های آن در بعضی از حالات ابتدا نیازمند مرور قضایا و تعاریفی از نظریه‌ی رویه‌های مینیمال به خصوص مسأله‌ی برنشتاین هستیم. به طور کلی ارتباط و شباهت‌های زیادی میان ادبیات نظریه‌ی رویه‌های مینیمال و تئوری مرتبط با حدس دی‌جورجی وجود دارد؛به طوری که بعضاً این حدس را نسخه‌ی اپسیلونی [۱] مسأله‌ی برنشتاین می‌نامند.

۲. نظریه‌ی رویه‌های مینیمال

مسأله‌ی پلاتو [۲] نقطه‌ی شروع نظریه‌ی رویه‌های مینیمال است. این مسأله عبارت است از یافتن رویه‌ای با کم‌ترین مساحت از میان رویه‌هایی که مرز مشخصی در فضا دارند. این مسأله به افتخار فیزیک‌دان بلژیکی جوزف پلاتو [۳] که با آزمایش با حباب‌های صابونی قصد داشت ویژگی‌های فیزیکی این رویه‌ها را به دست بیاورد نام‌گذاری شده است. تنش و انرژی حباب‌های صابونی با مساحتشان رابطه‌ی مستقیم دارد؛ برای همین حباب‌های صابونی تمایل به داشتن کم‌ترین مساحت ممکن را دارند و مدل فیزیکی خوبی برای شبیه‌سازی رویه‌های مینیمال هستند. البته این مسأله قبل‌تر از پلاتو توسط اویلر و لاگرانژ به عنوان حالت خاصی از مسائل حساب تغییرات [۴] بررسی شده بود. رادو [۵] و داگلاس [۶] این مسأله را با استفاده از ابزارهای هندسی حل کردند. اما روشی که آن‌ها به کار برده بودند مناسب برای تعمیم مسأله‌ی پلاتو به ابعاد بالاتر نبود. بعدها ریاضی‌دانانی مانند دی‌جورجی [۷]، فلمینگ [۸]، فدرر [۹]، آلمگرن [۱۰] و دیگران با استفاده از ابزارهای نظریه‌ی اندازه تعاریف و مفاهیم دیگری مرتبط با رویه‌های مینیمال ارائه کردند، به کمک آن‌ها به بررسی مسأله‌ی پلاتو در ابعاد بالاتر پرداختند و نظریه‌ی هندسی اندازه را پایه‌گذاری کردند. آن‌ها تعریف ضعیف‌تری از یک رویه‌ی مینیمال مطرح و با استفاده از آن اثبات ساده‌تری از وجود رویه‌های مینیمال را ارائه کردند اما از طرفی این جواب‌ها الزاماً یکتا و هموار نبود و بررسی هموار و یکتایی آن‌ها تلاش‌های بیشتری نیاز داشت.

یکی دیگر از مسائل تاثیرگذار در تاریخ نظریه‌ی رویه‌های مینیمال مسأله‌ی برنشتاین است:

«اگر نمودار تابع $u : \mathbb{R}^{n-۱} \to \mathbb{R}$ یک رویه‌ی مینیمال در $\mathbb{R}^n$ باشد آیا تابع مورد نظر حتما یک تابع خطی است؟»

برای حالت $n = ۳$ اثبات‌های متعددی یافت شده است. برنشتاین این مسأله را برای این حالت در ۱۹۱۵ با استفاده از قضیه‌ی دیگری به نام قضیه‌ی هندسی برنشتاین [۱۷] اثبات کرد. این قضیه بیان می‌کند که اگر نمودار تابع هموار $f(x,y)$ بر $\mathbb{R}^۲$ در هر نقطه دارای خمیدگی گاوسی نامثبت و حداقل در یک نقطه منفی باشد، آنگاه تابع f تابعی بی‌کران است. وی به کمک این قضیه اثبات کرد که جواب‌هایی با رشد خطی از معادله‌ی بیضوی $\Sigma a_{i,j}(x)\partial_{i,j}w(x) = ۰$ توابعی ثابتند و سپس نشان داد که اگر u یک جواب از معادله‌ی رویه‌ی مینیمال در صفحه باشد، تابع $w = \arctan(\partial_\nu u)$ به ازای هر بردار ν در یک معادله‌ی بیضوی به فرمی که بالاتر ذکر شد صدق می‌کند و به این وسیله نشان داد که جواب‌های معادله‌ی رویه‌ی مینیمال در بعد ۳، توابعی خطی‌اند. اثبات اولیه‌ی برنشتاین نقص‌هایی داشت که بعداً توسط هاپف [۲۰] و مایکل [۱۹] کامل شد. ایده‌ی برنشتاین با تمام هوشمندی‌اش قابل تعمیم به ابعاد بالاتر نبود. اولین اثبات از مسأله‌ی برنشتاین که قابلیت تعمیم به ابعاد بالاتر داشت را فلمینگ [۲۱] ارائه کرد. وی با اثبات عدم وجود مخروط مینیمال نابدیهی در $\mathbb{R}^۳$ و اینکه عدم برقراری حدس برنشتاین در بعد ۳ وجود مخروط مینیمال نابدیهی در این بعد را نتیجه می‌دهد، اثباتی دیگر برای مسأله‌ی برنشتاین در این بعد داد. دی‌جورجی [۱۸] نشان داد که عدم برقراری حدس برنشتاین در $\mathbb{R}^n$ وجود مخروط مینیمال نابدیهی در $\mathbb{R}^{n-۱}$ را نتیجه می‌دهد و در نتیجه‌ی اثبات

[1] ϵ-version
[2] The Plateau problem
[3] Joseph Plateau
[4] Variational Calculus
[5] Tibor Rado
[6] Jesse Doughlas
[7] Ennio De Giorgi
[8] Wendell Felming
[9] Herbert Federer
[10] Frederick Justin Almgren

پیشین فلمینگ اثباتی برای حدس برنشتاین در $\mathbb{R}^{۴}$ ارائه کرد. اثبات عدم وجود مخروط‌های مینیمال نابدیهی توسط آلمگرن [۲۲] در بعد ۴ و سایمونز[۱] [۲۳] تا بعد ۷ منجر به حل مسأله‌ی برنشتاین در این ابعاد شد. همچنین وجود مخروط مینیمال نابدیهی در بعد ۸ و یافتن مثال نقض در بعد ۹ توسط دی‌جورجی-جوستی[۲]-بومبیری[۳] [۲۴] مسأله‌ی برنشتاین را به طور کامل حل کرد. سایمون[۴] با استفاده از ابزارهای هندسه‌ی دیفرانسیل اثبات دیگری برای مسأله‌ی برنشتاین به ازای $n = ۳$ ارائه کرد که بعدها تعمیم آن توسط یائو و شوئن منجر به اثبات مسأله‌ی برنشتاین تا بعد ۶ شد. هدف نهاییمان از این بخش بیان ایده‌های مربوط به اثبات وجود رویه‌های مینیمال و همواری آن‌ها با استفاده از قضیه‌ی بهبودی صافی است که الهام‌بخش اثبات حدس دی‌جورجی توسط سوین بوده است.

۱.۲. تعاریف اولیه و قضیه‌ی وجود رویه‌های مینیمال. در این قسمت قصد داریم اثباتی از وجود رویه‌های مینیمال از نقص بعد[۵] ۱ با شرایط مرزی داده‌شده را بیان کنیم. برای این کار ابتدا در فضای بزرگتری از رویه‌های هموار به دنبال جواب مدنظرمان می‌گردیم و بدین‌ترتیب اثبات ساده‌تری از وجود چنین رویه‌ای خواهیم یافت. سپس همواری جوابی که به دست می‌آید را به کمک ابزارهای دیگری اثبات می‌کنیم. این کار مشابه تعریف جواب ضعیف برای معادلات دیفرانسیل با مشتقات جزئی و سپس تلاش برای اثبات همواری این جواب‌هاست. فضایی که در آن قصد داریم به جست‌وجوی رویه‌ی مدنظرمان بگردیم، فضای همه‌ی رویه‌هایی است که مرز مجموعه‌ی اندازه‌پذیری از فضا هستند. ابتدا نیازمند تعمیم تعریف مساحت برای چنین رویه‌هایی هستیم که الزاماً هموار نیستند.

برای مرز مجموعه‌ی هموار E، مساحت به صورت انتگرال نرم بردار نرمالش بر آن رویه تعریف می‌شود. می‌توانیم میدان برداری ناشی از بردار نرمال این رویه را با توابع برداری‌ای با تکیه‌گاه فشرده تقریب بزنیم. در این صورت تساوی زیر به دست می‌آید:

$$Area(\partial E) = \int_{\partial E} |\nu_E|^{۲} = \sup\{\int_{\partial E} X.\nu_E | X \in C_c^{۱}(\mathbb{R}^n;\mathbb{R}^n), |X| \leq ۱\} \tag{۱.۲}$$

با توجه به همواری ∂E و استفاده از قضیه‌ی دیورژانس داریم: $\int_{\partial E} X.\nu_E = \int_E \nabla \cdot X$. پس عبارت (۱.۲) را می‌توان به صورت زیر بازنویسی کرد:

$$Area(\partial E) = \sup\{\int_E \nabla \cdot X | X \in C_c^{۱}(\mathbb{R}^n;\mathbb{R}^n), |X| \leq ۱\}$$

توجه کنید که این عبارت جدید را می‌توان برای زیرمجموعه‌هایی از صفحه که مرز هموار ندارند نیز محاسبه کرد و این ابزاری را برای تعمیم تعریف مساحت به رویه‌هایی که هموار نیستند به ما می‌دهد.

تعریف ۱.۲. فرض کنید $\Omega \subset \mathbb{R}^n$ یک زیرمجموعه‌ی باز و $E \subset \mathbb{R}^n$ یک زیرمجموعه‌ی بورل باشد. در این صورت محیط[۶] E در Ω را به صورت زیر تعریف می‌کنیم:

$$Per(E;\Omega) = \sup\{\int_E \nabla \cdot X | X \in C_c^{۱}(\Omega;\mathbb{R}^n), |X| \leq ۱\}$$

مجموعه‌ی E را در Ω دارای محیط متناهی می‌نامیم اگر $Per(E;\Omega) < \infty$.

تعریف ۲.۲. فرض کنید $\Omega \subseteq \mathbb{R}^n$ باز و $E \subset \Omega$ یک زیرمجموعه‌ی بورل از Ω باشد. در این صورت می‌گوییم E یک مجموعه‌ی مینیمال در Ω است اگر به ازای هر زیرمجموعه‌ی فشرده مانند $K \subset \Omega$ و $F \subset \Omega$ که $F\backslash K = E\backslash K$، داشته باشیم: $Per(E;K) \leq Per(F;K)$. در این صورت ∂E را یک رویه‌ی مینیمال کمینه[۷] می‌نامیم.

در تعریف محیط یک مجموعه با ثابت نگه‌داشتن Ω، $Per(E;\Omega)$ را می‌توان به عنوان یک نگاشت از زیر مجموعه‌های Ω به $[۰,+\infty)$ در نظر گرفت. همچنین هر زیرمجموعه از Ω را می‌توان با تابع مشخصه‌اش یکی در نظر گرفت. بدین‌وسیله می‌توان همگرایی را برای زیرمجموعه‌های Ω و پیوستگی را برای تابعک $Per(E;\Omega)$ تعریف کرد.

---
[1] James Simons
[2] Enrico Giusti
[3] Enrico Bombieri
[4] Leon Simon
[5] co-dimension
[6] Perimeter
[7] Minimizing minimal surface

تعریف ۳.۲. فرض کنید E_k دنباله‌ای از زیرمجموعه‌های Ω و E نیز یک زیرمجموعه از Ω باشد. در این صورت می‌گوییم E_k در $L^1(\Omega)$ (مشابهاً در $L^1_{loc}(\Omega)$) به E میل می‌کند اگر χ_{E_k} در $L^1(\Omega)$ (مشابهاً در $L^1_{loc}(\Omega)$) به χ_E میل کند.

در نتیجه $Per(E;\Omega)$ را می‌توان به عنوان یک تابعک از زیرمجموعه‌ای روی فضای $L^1_{Loc}(\Omega)$ یا $L^1(\Omega)$ در نظر گرفت. مسأله‌ی یافتن رویه‌های مینیمال به نوعی مسأله‌ی یافتن کمینه‌های این تابعک است. برای این‌که نشان دهیم این تابعک کمینه دارد نیاز به ویژگی‌های آن مانند پیوستگی و از پایین کران‌دار بودن آن داریم. برای مشاهده‌ی اثبات قضایای پیش‌رو می‌توانید به مرجع [۱۰] مراجعه کنید.

قضیه ۴.۲. فرض کنید $\Omega \subset \mathbb{R}^n$ باز و E_k دنباله‌ای از زیرمجموعه‌های بورل Ω باشند که در $L^1_{loc}(\Omega)$ به E میل می‌کنند. در این صورت داریم: $Per(E;\Omega) \leq \liminf_{k\to+\infty} Per(E_k;\Omega)$

قضیه ۵.۲. فرض کنید $\Omega \subset \mathbb{R}^n$ باز و E_k دنباله‌ای از زیرمجموعه‌های بورل $\mathbb{R}^n$ باشد به طوری که $Per(E_k;\Omega) \leq C$، در این صورت زیردنباله‌ای همگرا در $L^1_{Loc}(\Omega)$ از E_k به مجموعه‌ي بورلی مانند E وجود خواهد داشت.

با استفاده از قضایای بالا وجود رویه‌های مینیمال را می‌توان نتیجه گرفت.

قضیه ۶.۲. فرض کنید F زیرمجموعه‌ای از B_2 با محیط متناهی باشد. در این صورت $E \subset B_2$ موجود است که $E\backslash B_1 = F\backslash B_1$ و به ازای هر $E' \subset B_2$ که $E'\backslash B_1 = F\backslash B_1$ داریم: $Per(E;B_1) \leq Per(E';B_1)$.

اثبات. ایده‌ی این اثبات مربوط به روش کلی‌تری در نظریه‌ی معادلات دیفرانسیل تحت عنوان روش‌های مستقیم حساب تغییرات[1] مربوط می‌شود. تعریف می‌کنیم: $p = \inf\{Per(E';B_2) : E'\backslash B_1 = F\backslash B_1\}$. داریم: $p \leq Per(F;B_2) \leq \infty$. بنابر تعریف دنباله‌ای از زیرمجموعه‌های B_2 مانند E_m موجودند که

$$E_m\backslash B_1 = F\backslash B_1, \lim_{m\to\infty} Per(E_m;B_2) = p.$$

در این صورت بنابر قضیه‌ی (۵.۲) زیردنباله‌ای از E_m مانند E_{m_k} موجود است به نحوی که: $\lim_{k\to\infty} E_{m_k} = E$ که همگرایی در $L^1_{loc}(B_2)$ رخ می‌دهد. بنابر قضیه‌ی (۴.۲) داریم: $Per(E;B_2) \leq p$. در نتیجه E یک مجموعه با مرز مینیمال و شرایط مرزی داده شده است. $\square$

۲.۲. رفتار موضعی رویه‌های مینیمال. اثباتی که در قسمت قبل برای وجود رویه‌های مینیمال ارائه کردیم تضمینی درمورد هموار‌بودن این رویه‌ها به ما نمی‌دهد. در این قسمت با بررسی رفتار موضعی این رویه‌ها همواری آن‌ها را اثبات می‌کنیم. روشی که اینجا پی می‌گیریم به نام اپسیلون-همواری[2] و روش انفجار[3] شناخته می‌شود و در اثبات همواری کمینه‌های تابعک‌های انرژی‌ای که در نظریه‌ی معادلات دیفرانسیل با مشتقات جزئی و نظریه‌ی هندسی اندازه ظاهر می‌شود نیز کاربرد دارد.
در حالت کلی همواری و مشتق‌پذیری یک تابع به نزول و سرعت نزول نرم خاصی از آن تابع مرتبط می‌گردد. به طور مثال اگر بتوانیم نرم مشتق ضعیف کمینه‌ای از تابعک انرژی دیریشله را به میزان کافی کوچک کنیم، می‌توانیم ثابت کنیم که آن تابع $C^{1,\alpha}$ است. این قضیه به اپسیلون-همواری معروف است [؟]. دی‌جورجی اولین‌بار مشابه این قضیه را برای رویه‌های مینیمال ثابت کرد. اثبات وی مبتنی بر تقریب‌زدن رویه‌های مینیمال با توابع هارمونیک بود [۲۵]. در اینجا ما به اثبات دیگری از این قضیه که سوین[4] آن را اثبات کرده است اشاره خواهیم کرد. این اثبات از نامساوی هارنک[5] برای جواب‌های چسبندگی استفاده و قضیه‌ی کلی‌تری به نام بهبودی صافی[6] را اثبات و از آن قضیه‌ی اپسیلون-همواری را برای رویه‌های مینیمال نتیجه‌گیری کرده است. سوین با استفاده از ایده‌های مشابه توانست حدس دی‌جورجی را تا بعد ۸ تحت شرط حد یکنواخت جواب‌ها اثبات کند.
به‌طور شهودی قضیه بهبودی صافی بیان می‌کند که اگر بتوانیم مجموعه‌ی مینیمال E را در درون استوانه‌ای با ارتفاع به میزان کافی کوچک محبوس کنیم، آن‌گاه در جهت دیگری می‌توانیم آن را در استوانه‌ای با ارتفاع کوچکتری محبوس کنیم به

[1] Direct method of calculus of variations
[2] ϵ-Regularity
[3] Blow up Method
[4] Ovidiu Savin
[5] Harnack's inequality
[6] Improvement of flatness

نحوی که میزان کوچک‌شدن آن ضریبی از ارتفاع استوانه اولیه است و این ضریب تنها به بعد فضا بستگی دارد. با استفاده‌ی مکرر از قضیه‌ی بهبودی صافی می‌توان دنباله‌ای همگرا از جهت‌ها را یافت به نحوی که حد آن‌ها بردار عمود بر رویه است و از این هموازی $C^{1,\alpha}$ رویه‌مان نتیجه می‌شود.

بنابراین برای اثبات همواری رویه‌ی مینیمال E کافیست ثابت کنیم که در همسایگی هر نقطه به میزان کافی صاف است. یک روش بررسی رفتار موضعی یک کمینه تابعک انرژی، انبساط آن حول نقطه‌ی مدنظر و دیدن رفتار حدی آن است. این حد در صورت وجود خود نیز یک کمینه‌ی موضعی سرتاسری برای تابعک انرژی مدنظر است(در اینجا منظور از کمینه موضعی، کمینه بودن نسبت به تغییرات در دامنه‌های فشرده است). در نتیجه اگر بتوانیم همگرایی یکنواخت این دنباله‌ی انبساطی را اثبات و کمینه‌های موضعی سرتاسری تابعک مدنظر را دسته بندی کنیم، آن‌گاه می‌توانیم صافی مورد نیاز برای همواری کمینه را استنتاج کنیم.

فرض کنید E یک مجموعه‌ی مینیمال و $x \in \partial E$ باشد. دنباله‌ی $E_{x,r}$ را تعریف می‌کنیم: $E_{x,r} = \frac{E-x}{r}$. همانطور که بیان شد هدف ما یافتن رفتار این دنباله هنگامی است که r به صفر میل می‌کند. ابتدا کران بالایی برای محیط این دنباله ارائه و سپس با استفاده از آن وجود زیردنباله همگرا را اثبات می‌کنیم. توجه کنید که به ازای هر $R > 0$ و $r \in (0, \frac{1}{R})$ داریم:

$$Per(E_{x,r}; B_R) = \frac{Per(E; B_{rR}(x))}{r^{n-1}} \leq R^{n-1} Per(E; B_1(x)) \tag{۲.۲}$$

از قضیه‌ی (۵.۲) نتیجه می‌شود که $E_{x,r}$ زیردنباله‌ای همگرا در B_R دارد. با افزایش R و استفاده از استدلال قطری می‌توان ادعا کرد $E_{x,r}$ زیردنباله‌ای همگرا در $\mathbb{R}^n$ به مجموعه‌ای مانند F دارد. هم‌چنین با توجه به از پایین پیوسته بودن تابعک محیط و مینیمال‌بودن $E_{x,r}$ها، F نیز یک مجموعه‌ی مینیمال است. هم‌چنین با توجه به روند حدی‌ای که برای به دست آوردن F داشتیم انتظار داریم که تحت انبساط ناوردا یا به طور معادل یک مخروط حول نقطه‌ی x باشد. برای اثبات این موضوع به فرمول یکنوایی برای رویه‌های مینیمال نیازمندیم که اولین‌بار توسط فلمینگ مطرح شد.

قضیه ۷.۲. فرض کنید E یک مجموعه‌ی مینیمال و $x \in \partial E$ باشد. در این صورت تابع

$$\Psi_E(r) = \frac{\mathcal{H}^{n-1}(\partial E \cap B_r(x))}{r^{n-1}}$$

یک تابع صعودی است. هم‌چنین این تابع ثابت است اگر و تنها اگر E یک مخروط باشد.

با توجه به تعریف حدی مجموعه‌ی F، با نوشتن فرمول یکنوایی برای این مجموعه متوجه می‌شویم که مقدارش همیشه ثابت و درنتیجه F یک مخروط مینیمال است. گام‌های نهایی برای استفاده از این نتیجه برای اثبات همواری رویه‌های مینیمال قوی‌تر کردن همگرایی دنباله‌ی انفجاریمان به مخروط حدی و رده‌بندی مخروط‌های مینیمال است. توجه کنید که همگرایی‌ای که از قضیه (۵.۲) نتیجه می‌شود یکنواخت نیست و حتی در صورتی که مخروط حدی یک صفحه در فضا باشد نمی‌تواند تخمین یکنواختی که برای استفاده در قضیه اپسیلون-همواری نیاز داریم را به ما بدهد.
برای اثبات همگرایی یکنواخت از این ویژگی استفاده می‌کنیم که مجموعه‌های مینیمال حول نقاط مرزیشان نمی‌توانند بسیار تنک یا بسیار چگال باشند و حجمی که در یک گوی حول یک نقطه‌ی مرزی اشغال می‌کنند، متناسب با شعاع آن گوی است. معادل این تخمین چگالی رویه‌های مینیمال و استفاده از آن برای همگرایی یکنواخت دنباله‌ی انفجاری، برای جواب‌های معادله‌ی آلن-کن نیز اثبات شده و در اثبات سوین برای آن حدس نیز کاربرد دارد.

قضیه ۸.۲. فرض کنید $E \subset \mathbb{R}^n$ یک مجموعه‌ی مینیمال و $x \in \partial E$ باشد. در این صورت ثابت $c(n)$ که تنها وابسته به بعد است وجود دارد به طوری که: $|B_r(x) \cap E| \geq c(n) r^n$.

نتیجه ۹.۲. فرض کنید E_k دنباله‌ای از رویه‌های مینیمال باشند که در L^1_{loc} به رویه‌ی مینیمال E میل می‌کنند. در این‌صورت E_k در L^∞_{loc} به E میل می‌کند.

اثبات. باید نشان دهیم به ازای هر زیرمجموعه‌ی فشرده مانند K و هر $\epsilon > 0$، $N \in \mathbb{N}$ موجود است که به ازای هر $k > N$ داریم :

$$\partial E \cap K \subset \{x \in K : dist(x, \partial E_k) < \epsilon\} \quad , \quad \partial E_k \cap K \subset \{x \in K : dist(x, \partial E) < \epsilon\}$$

فرض کنید دنباله‌ای از نقاط مانند $x_{k_j} \in \partial E_{k_j} \cap K$ موجودند که $dist(x_{k_j}, \partial E) \geq \epsilon$ (حالت دیگر مشابها ثابت می‌شود). فرض کنید x نقطه‌ی حدی دنباله‌ی x_{k_j} باشد. در این‌صورت داریم $dist(x, \partial E) \geq \epsilon$ و $B_{\epsilon/۲}(x) \subset E^o$ یا $B_{\epsilon/۲}(x) \subset \overline{E}^c$. فرض کنید $B_{\epsilon/۲}(x) \subset E^o$. حالت دیگر مشابهاً اثبات می‌شود. بنا بر فرض و قضیه‌ی بالا داریم:

$$c(n)(\frac{\epsilon}{۲})^n \leq \lim_{k_j \to +\infty} |B_{\epsilon/۲}(x_{k_j}) \cap E^c_{k_j}| = \lim_{k_j \to +\infty} \int_{B_{\frac{\epsilon}{۲}}(x_{k_j})} \chi_{E^c_{k_j}} = \int_{B_{\frac{\epsilon}{۲}}(x)} \chi_{E^c} = ۰$$

که تناقض است و در نتیجه همگرایی رویه‌ها بر روی مجموعه‌های فشرده، یکنواخت است. □

همان‌طور که در مقدمه‌ی این قسمت اشاره شد در بعد ۷ به پایین مخروط مینیمال نابدیهی وجود ندارد و درنتیجه هر مخروط مینیمال یک صفحه در فضا است. ترکیب این نتیجه و قضایای قبلی همواربودن رویه‌های مینیمال با نقص بعد ۱ در این فضاها را به ما می‌دهد (حتی می‌توان به صورت قوی‌تر نتیجه گرفت که هر مجموعه‌ی مینیمال یک نیم‌فضاست). اولین مثال از مجموعه‌ای مینیمال با تکینگی نیز مخروط سایمونز در بعد ۸ است:

$$C_s = \{x \in \mathbb{R}^۸ : x_۱^۲ + x_۲^۲ + x_۳^۲ + x_۴^۲ = x_۵^۲ + x_۶^۲ + x_۷^۲ + x_۸^۲\}$$

در حالت کلی‌تر فدرر اثبات کرده که مجموعه‌ی تکینگی‌های مجموعه‌های مینیمال در بعد $n \geq ۸$ یک مجموعه‌ی بسته و با بعد هاسدروف $n - ۸$ است.

۳. انگیزه‌های نظری حدس دی‌جورجی

در این قسمت حدس دی‌جورجی را بیان و انگیزه‌های مطرح‌شدن این حدس را بیان می‌کنیم.

حدس ۱.۳ (دی‌جورجی-۱۹۷۸). فرض کنید $u \in C^۲(\mathbb{R}^n, [-۱, ۱])$ که

$$\Delta u = u^۳ - u, \quad \partial_n u > ۰, \quad |u| < ۱ \tag{۱.۳}$$

در این صورت در $n \leq ۸$ سطح ترازهای u ابرصفحه‌هایی در فضا هستند یا به طور معادل u تابعی یک‌بعدی است؛ یعنی برداری مانند $\xi \in \mathbb{S}^{n-۱}$ موجود است که $u(x) = g(x \cdot \xi)$ که g جوابی از معادله‌ی (۱.۳) در بعد یک است.

برای دریافت شهود پشت حدس دی‌جورجی نیازمند بررسی کمینه‌های تابعک انرژی $\mathcal{I}_\epsilon(u; \mathbb{R}^n)$ هستیم. به همین جهت ابتدا تعریف دقیقی برای کمینه‌های این تابعک ارائه می‌دهیم.

تعریف ۲.۳. تابع u را موضعاً کمینه‌کننده‌ی تابعک انرژی $\mathcal{I}_\epsilon(u; \Omega)$ در Ω می‌نامیم هرگاه به ازای هر $A \subset \Omega$ که $\overline{A}$ در Ω فشرده است داشته باشیم:

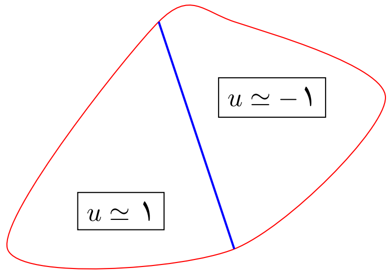
$$\mathcal{I}_\epsilon(u; A) \leq \mathcal{I}_\epsilon(u + \phi; A) \qquad \forall \phi \in C_c^\infty(A)$$

از این به بعد منظور از کمینه‌ی یک تابعک انرژی یک موضعاً کمینه‌کننده‌ی آن تابعک است.

فرض کنید u یک کمینه‌ی تابعک انرژی $\mathcal{I}_۱(u; B_{\epsilon^{-۱}})$ باشد که $B_{\epsilon^{-۱}}$ گوی به شعاع $\epsilon^{-۱}$ به مرکز مبدا است. در این صورت $u_\epsilon(x) = u(\frac{x}{\epsilon})$ یک کمینه‌ی تابعک انرژی $\mathcal{I}_\epsilon(u; B_۱)$ در $B_۱$ است. با توجه به تعاریف می‌توان دید که رفتار تابع u در کل فضا یا ناحیه‌هایی بزرگ از فضا مانند $B_{\epsilon^{-۱}}$، زمانی که ϵ به صفر میل می‌کند برابر رفتار u_ϵ در گوی واحد است. حال تابعک انرژی مربوط به معادله‌ی آلن-کن را در نظر بگیرید:

$$\mathcal{I}_\epsilon(u; B_۱) = \int_{B_۱} \frac{\epsilon}{۲}|\nabla u|^۲ + \frac{۱}{\epsilon}\frac{(۱ - u^۲)^۲}{۴} \tag{۲.۳}$$

$W(u) = \frac{(۱-u^۲)^۲}{۴}$ و $\frac{\epsilon}{۲}|\nabla u|^۲$ را به ترتیب انرژی پتانسیل و جنبشی این تابعک می‌نامیم. هنگامی که ϵ به صفر میل می‌کند ضریب انرژی پتانسیل در این تابعک به بی‌نهایت میل می‌کند. بنابراین از یک کمینه‌ی این تابعک انتظار داریم برای خنثی‌کردن اثر این ضریب مقدار $\frac{(۱-u^۲)^۲}{۴}$ را تا حد ممکن به صفر نزدیک کند و این یعنی تا حد ممکن مقادیر نزدیک به ± ۱ را اتخاذ کند. در همین حال قسمت انرژی جنبشی این تابعک نیز از جهش‌های ناگهانی و ناپیوسته میان ± ۱ جلوگیری می‌کند. پس انتظار داریم که به ازای ϵ به میزان کافی کوچک تابع کمینه‌کننده‌ی $\mathcal{I}_\epsilon(-; B_۱)$ شبیه شکل زیر رفتار کند:



از نامساوی یانگ [۱] نتیجه می‌شود:

$$\mathcal{I}_\epsilon(u;B_1) = \int_{B_1} \frac{\epsilon}{2}|\nabla u|^2 + \frac{1}{\epsilon}\frac{(1-u^2)^2}{4} \geq \int_{B_1} \frac{1}{\sqrt{2}}(1-u^2)|\nabla u|$$

با استفاده از رابطه‌ی نقص_مساحت [۲] سمت راست عبارت بالا را می‌توانیم به شکل زیر بازنویسی کنیم:

$$\int_{B_1} \frac{1}{\sqrt{2}}(1-u^2)|\nabla u| = \frac{1}{\sqrt{2}}\int_{-1}^{1}(\int_{u^{-1}(s)}(1-u^2)d\mathcal{H}^{n-1}(x))ds =$$
$$\frac{1}{\sqrt{2}}\int_{-1}^{1}(\int_{\{u=s\}}(1-s^2)d\mathcal{H}^{n-1}(x))ds = \frac{1}{\sqrt{2}}\int_{-1}^{1}(1-s^2)\mathcal{H}^{n-1}(u=s)ds$$

پس داریم:

$$\mathcal{I}_\epsilon(u;B_1) \geq \frac{1}{\sqrt{2}}\int_{-1}^{1}(1-s^2)\mathcal{H}^{n-1}(u=s)ds$$

از نامساوی بالا نتیجه می‌شود که اگر سطح ترازهای u رویه‌های مینیمال در گوی واحد به شعاع مبدا باشند و بنابر شرط برقراری تساوی در نامساوی یانگ که در ابتدای پاراگراف استفاده کردیم داشته باشیم $|\nabla u| = \frac{\epsilon}{\sqrt{2}}(1-u^2)$، آنگاه تابع مورد نظر یک کمینه برای تابعک انرژی $\mathcal{I}_\epsilon(u;B_1)$ است. اگر فرض کنیم $u(0)=0$، از تساوی آخر نتیجه می‌شود $u(x)=\tanh(\frac{d_\Gamma(x)}{\sqrt{2}\epsilon})$، که $\Gamma=\{u=0\}$ و $d_\Gamma(x)$ فاصله‌ی x از Γ است. اما در حالت کلی همه‌ی سطح ترازهای یک کمینه‌ی تابعک انرژی ذکر شده، رویه‌های مینیمال نیستند. اگر $\Gamma=\{u=0\}$ یک رویه‌ی مینیمال باشد، آن‌گاه $\{u=s\}$ به ازای s هایی که به ± 1 نزدیک نیستند و ϵ به میزان کافی کوچک، یک رویه‌ی مینیمال در گوی واحد است. از طرفی هنگامی که s به ± 1 نزدیک و Γ یک رویه‌ی مینیمال باشد، تابع u که به شکل بالا تعریف شده است تقریباً یک کمینه برای تابعک انرژی $\mathcal{I}_\epsilon(u;B_1)$ خواهد بود.
با توجه به نتایج بالا می‌توان حدس زد که سطح ترازهای کمینه‌های تابعک انرژی $\mathcal{I}_\epsilon(u;B_1)$ هنگامی که ϵ به صفر میل می‌کند، به یک رویه‌ی مینیمال نزدیک می‌شود. هم‌چنین توجه کنید که اگر تابعی که این کمینه‌ها به آن میل می‌کنند در یک جهت صعودی باشد آن‌گاه این رویه‌ی مینیمال، نمودار یک تابع است و بنابر قضیه‌ی برنشتاین در بعد کمتر از ۸ این رویه باید یک ابرصفحه در فضا باشد. بنابرین انتظار می‌رود سطح ترازهای جواب‌هایی از معادله‌ی آلن_کن که در کل فضا تعریف شده و در یک جهت صعودی‌اند ابرصفحه‌هایی در فضا باشند.
رفتار مجانبی کمینه‌های $\mathcal{I}_\epsilon(-;B_1)$ موضوع پژوهش‌های بسیاری بوده است. یکی از اولین نتایج دراین مورد متعلق به مودیکا است که با استفاده از مفهوم Γ_همگرایی قضیه‌ی زیر را اثبات کرد[۱۶].

قضیه ۳.۳ (مودیکا_۱۹۷۹). فرض کنید u_ϵ یک کمینه‌ی تابعک $\mathcal{I}_\epsilon(-;B_1)$ باشد. در این صورت زیردنباله‌ای همگرا در $L^1_{loc}(B_1)$ مانند u_{ϵ_k} و زیرمجموعه‌ی مینیمال E از B_1 موجود است که: $u_{\epsilon_k} \to \chi_E - \chi_{B_1\setminus E}$.

به وسیله‌ی قضیه‌ای درمورد تخمین چگالی یکنواخت سطح ترازهای کمینه‌های تابعک انرژی $\mathcal{I}_\epsilon(-;B_1)$ که توسط کافارلی [۳] و کوردوبا [۴] اثبات شده، می‌توان نشان داد که همگرایی سطح ترازها در قضیه‌ی مودیکا قوی‌تر از همگرایی در $L^1_{Loc}(B_1)$ است. در واقع می‌توان نشان داد که این سطح ترازها به طور یکنواخت روی زیرمجموعه‌های فشرده به ∂E میل می‌کنند.

[1] Young's Inequality
[2] Co-area formula
[3] Luis Caffarelli
[4] Antonio Cordoba

قضیه ۴.۳. فرض کنید u یک کمینه از تابعک انرژی $\mathcal{I}_\epsilon(-;B_1)$، $\alpha > -1$ و $\beta < 1$ به طوری که $u(0) \geq \alpha$. در این صورت برای $r \geq r(\alpha,\beta)$ داریم: $|\{u > \beta\} \cap B_r| \geq cr^n$ که $c = c(n,W)$ ثابتی وابسته به بعد و تابع پتانسیل است.

حال فرض کنید u یک کمینه از تابعک $\mathcal{I}_1(-,\mathbb{R}^n)$ در کل فضا باشد. در این صورت u_{ϵ_k} یک کمینه‌ی $\mathcal{I}_{\epsilon_k}(-,B_1)$ در B_1 است و بنابر قضیه‌ی مودیکا زیردنباله‌ی همگرایی مانند u_{ϵ_k} موجود است که:

$$u_{\epsilon_k} \to \chi_E - \chi_{B_1/E}$$

و $E \subset B_1$ یک مجموعه‌ی مینیمال باشد. حال با استفاده از فرمول چگالی کافارلی-کوردوبا همانند حالت رویه‌های مینیمال اثبات می‌شود که همگرایی سطح‌ترازهای u_{ϵ_k} بر مجموعه‌های فشرده یکنواخت است. به طور خاص همگرایی $\{u_{\epsilon_k} = 0\} = \epsilon_k\{u = 0\} \to \partial E$ به طور یکنواخت بر مجموعه‌های فشرده نتیجه می‌شود. می‌دانیم به ازای $n \leq 7$، ∂E یک ابرصفحه در فضا، مثلاً $\{x_n = 0\}$ است. در این صورت از همگرایی یکنواخت $\{u_{\epsilon_k} = 0\}$ در B_1 نتیجه می‌شود دنباله‌هایی مانند θ_k, l_k موجودند به طوری که $l_k \to +\infty$، $\frac{\theta_k}{l_k} \to 0$ و داریم:

$$\{u = 0\} \cap B_{l_k} \subset \{|x_n| \leq \theta_k\}.$$

این رابطه بیان می‌کند که سطح تراز $\{u = 0\}$ را می‌توانیم در استوانه‌هایی محصور کنیم که نسبت ارتفاع به شعاعی از سطح تراز که در بر میگیرند به صفر میل می‌کند. این نتیجه را صافی در بی‌نهایت[۱] نیز تعبیر می‌کنند.
شباهت‌های دیگری نیز میان کمینه‌های تابعک انرژی گینزبرگ-لانداو و رویه‌های مینیمال وجود دارد. به طور مثال مودیکا در ۱۹۸۹ اثبات کرد که اگر $F \geq F(1)$ و u یک جواب کران‌دار از معادله‌ی $\Delta u - F(u) = 0$ باشد آن‌گاه $\frac{E_R(u)}{R^{n-1}}$ بر حسب R مقداری صعودی است که در آن

$$E_R(u) = \int_{\mathbb{R}^n} \frac{1}{2}|\nabla u|^2 + F(u) - F(1).$$

۴. اثبات‌ها و نتایج حول حدس دی‌جورجی

یکی از اولین نتایج در مورد حدس دی‌جورجی را مودیکا[۲] و مورتولا[۳] با اثبات این حدس در بعد ۲ با این شرط اضافه که سطح ترازهای u نمودار خانواده‌ای هم-لیپشیتز از توابع هستند، به دست آوردند [۲]. ایده‌ی آن‌ها استفاده از قضایای لیوویل‌مانند[۴] برای معادلات بیضوی با فرم دیورژانسی برای نسبت $\sigma = \frac{u_{x_1}}{u_{x_2}}$ بود. حدس دی‌جورجی در حالت کلی در بعد ۲ توسط قصوب[۵] و گویی[۶] [۳] اثبات شد. آن‌ها نیز از نتایج لیوویل‌مانندی که توسط کافارلی-برستیکی[۷]-نایرنبرگ[۸] [۴] برای بررسی طیف عملگر شرودینگر توسعه داده شده بود، استفاده کردند. با استفاده از تکنیک‌های مشابه امبروزیو[۹] و کبره[۱۰] اثباتی برای حدس دی‌جورجی به ازای $n = 3$ ارائه کردند [۵].

حدس دی‌جورجی با این شرط اضافه که حد جواب‌ها در مثبت و منفی بی‌نهایت در جهت x_n به طور یکنواخت به ترتیب برابر مثبت و منفی یک است، به اسم حدس گیبونز[۱۱] شناخته می‌شود و ابتدا توسط قصوب و گویی در $n \leq 3$ و سپس برای همه‌ی ابعاد به طور مستقل توسط بارلو[۱۲]-بس[۱۳]-گویی [۶]، برستسکی-همل[۱۴]-مونئو[۱۵] [۷] و فرینا[۱۶] [۸] اثبات شد. سوین[۱۷]

[1] Flatness at infinity
[2] Luciano Modica
[3] Stefano Mortola
[4] liouville type inequalities
[5] Nassif Ghosoub
[6] Changfeng Gui
[7] Henri Berestycki
[8] Louis Nirenberg
[9] Luigi Ambrosio
[10] Xavier Cabre
[11] Gibbons conjecture
[12] Martin T. Barlow
[13] Richard F. Bass
[14] Francois Hamel
[15] Regis Monneau
[16] Alberto Farina
[17] Ovidiu Savin

تنها با فرضی ساده درمورد حد جواب‌های معادله‌ی آلن-کن توانست حدس دی‌جورجی را تا $n \leq 8$ اثبات نماید [۱]. در ادامه‌ی ایده‌هایی از اثبات حدس دی‌جورجی را بیان خواهیم کرد.

۱.۴. حدس دی‌جورجی در بعد ۲. قصوب و گویی در اصل حدس دی‌جورجی را برای رده‌ی وسیع‌تری از معادلات به شکل $\Delta u = F'(u)$ اثبات کردند که $F \in C^2(\mathbb{R})$. در ادامه فرض می‌کنیم که $u : \mathbb{R}^2 \to \mathbb{R}$ یک جواب کران‌دار از معادله‌ی بالاست با این ویژگی که $\partial_2 u > 0$. به ازای هر $x_0 \in \mathbb{R}^2$ تعریف می‌کنیم: $\phi = \phi_{x_0} = \nabla u \cdot \nu = \partial_\nu u$ که $\nu \in \mathbb{R}^2 \backslash \{0\}$ به نحوی انتخاب می‌شود که داشته باشیم: $\nabla u(x_0) \cdot \nu = 0$. در این صورت داریم:

$$\Delta\phi = \partial_{11}\phi + \partial_{22}\phi = \nu \cdot \nabla(\partial_{11}u) + \nu \cdot \nabla(\partial_{22}u) = \nu \cdot \nabla(\Delta u)$$

و در نتیجه ϕ در معادله‌ی روبه‌رو صدق می‌کند: $(\Delta - F''(u))\phi = \Delta\phi - F''(u)\phi = 0$. به عملگر بیضوی [1] به شکل $L = -\Delta - V$ عملگر شرودینگر می‌گویند. یکی از عوامل تاثیرگذار بر جواب‌های معادله‌ی $Lu = 0$ ویژگی‌های طیفی این عملگر می‌باشد.

اثبات قصوب و گویی از حدس دی‌جورجی بر پایه‌ی نتایجی از برستیکی-کافارلی-نایرنبرگ درمورد ویژگی‌های جواب‌های معادلات بیضوی در دامنه‌های بی‌کران بود. در واقع آن‌ها در پی یافتن مثال نقضی برای بعضی از مسائلی بودند که در [۴] درمورد طیف عملگر شرودینگر مطرح شده بود و در نتیجه‌ی آن اثباتی برای حدس دی‌جورجی در بعد ۲ پیدا کردند.

تابعک انرژی متناظر با عملگر شرودینگر $L = -\Delta - V$ عبارت است از:

$$\mathcal{L}(\phi) = \frac{\int_{\mathbb{R}^n} |\nabla\phi|^2 - V|\phi|^2}{\int_{\mathbb{R}^n} |\phi|^2}$$

اثبات می‌شود که مقدار ویژه‌ی اساسی عملگر L برابر کمینه‌ی این تابعک بر $C_c^\infty(\mathbb{R}^n)$ است.

قضیه ۱.۴. فرض کنید $L = -\Delta - V$ یک عملگر شرودینگر و $u \in C^2(\mathbb{R}^n)$ یک جواب از معادله‌ی $Lu = 0$ باشد. در این صورت داریم: $\lambda_1(V) \leq 0$ ($\lambda_1(V)$ مقدار ویژه‌ی اساسی عملگر L می‌باشد.).

اثبات این قضیه مبتنی بر استفاده از از توابع برشی [2] خاصی مانند ϕ_R و این نکته که u یک تابع ویژه برای این عملگر است، می‌باشد.

قضیه ۲.۴. فرض کنید $L = -\Delta - V$ عملگر شرودینگری بر $\mathbb{R}^n$ با پتانسیل هموار و کران‌دار V باشد. در این صورت $\lambda_1(V) < 0$ اگر و تنها اگر $Lu = 0$ هیچ جواب مثبتی نداشته باشد.

قضیه ۳.۴. فرض کنید $L = -\Delta - V$ عملگر شرودینگری با پتانسیل هموار و کران‌دار V باشد. همچنین فرض کنید $Lu = 0$ جوابی باشد که مقادیر مثبت و مقادیر منفی اتخاذ کند. در این صورت اگر $n = 1, 2$ داریم $\lambda_1(V) < 0$.

اثبات این قضیه نیز همانند قضیه (۱.۴) وابسته به وجود دسته‌ی خاصی از توابع برشی با تکیه‌گاه فشرده مانند ξ_R است به طوری که:

$$\xi_R \in H^1(\mathbb{R}^n),\ \xi_R\big|_{B_R} = 1,\ \lim_{R\to\infty}\int_{\mathbb{R}^n} u^2|\nabla\xi_R|^2 dx = 0$$

حال فرض کنید u جوابی از $Lu = 0$ باشد که علامتش در کل فضا یکسان نیست (برای مشاهده‌ی اثبات دقیق سه قضیه‌ی ذکرشده و لم اکلند که در ادامه به آن اشاره خواهیم کرد می‌توانید به مقاله‌ی [۳] مراجعه کنید.). با توجه به این می‌توانیم مقدار $\mathcal{L}(\xi_R u)$ را همانند زیر بازنویسی کنیم:

$$\mathcal{L}(\xi_R u) = \frac{\int_{\mathbb{R}^n} u^2|\nabla\xi_R|^2 dx}{\int_{\mathbb{R}^n} (\xi_R u)^2 dx} \tag{۱.۴}$$

فرض می‌کنیم که $\lambda_1(V) = 0$. در این صورت با توجه به خاصیت (۱.۴) توابع برشی دنباله‌ی $\xi_R|u|$ دنباله‌ای در H^1 است به طوری که $\lim_{R\to\infty}\mathcal{L}(\xi_R u) = 0$. سپس با استفاده از لم تغییراتی به نام لم اکلند [3] به هر جمله‌ی دنباله‌ی $\xi_R u$ که یک دنباله‌ی

[1] Elliptic Operator
[2] cutoff function
[3] Ekeland's theorem

کمینه‌کننده برای $\mathcal{L}$ است، تابع کمینه‌کننده‌ی دیگری نسبت می‌دهیم. این لم کران بالایی برای مشتق $\mathcal{L}$ در توابع کمینه‌کننده‌ی جدید به ما می‌دهد که با استفاده از آن می‌توانیم ثابت کنیم $|u|$ نیز جوابی برای معادله‌ی $Lu = ۰$ است و این‌گونه با این فرض که u بر فضا تنها مثبت یا منفی است به تناقض می‌رسیم.

اما آیا چنین توابع برشی در همه‌ی ابعاد موجودند؟ برای یافتن چنین توابع برشی نیازمند حل مسأله‌ی کمینه‌سازی زیر هستیم:

$$\inf\{\int_{B_{R'}\backslash B_R} |\nabla\xi|^۲ dx : \xi\big|_{B_R} = ۱, \xi\big|_{\partial B_{R'}} = ۰\}$$

برای این مسأله در بعد ۲ ابتدا تابع زیر را در نظر بگیرید:

$$\xi_{R,R'}(x) = \frac{\ln(|x|) - \ln(R)}{\ln(R') - \ln(R)}$$

در این صورت داریم:

$$\int_{B_{R'}\backslash B_R} |\nabla\xi|^۲ dx = \frac{۱}{\ln(R/R')}$$

در نتیجه تابع

$$\xi_R^۲(x) = \begin{cases} ۱ & x \in B_R \\ \xi_{R,R^۲}(x) & x \in B_{R^۲}\backslash B_R \\ ۰ & o.w. \end{cases}$$

یک تابع برش مناسب برای قضیه است. اما در بعد بزرگتر از ۳ جواب بنیادین این مسأله به صورت

$$\xi_{R,R'}(x) = \frac{|x|^{۲-n} - R^{۲-n}}{(R')^{۲-n} - R^{۲-n}}$$

است. با این حال نرم $H^۱$ این تابع هنگامی که $R \to \infty$ به صفر میل نمی‌کند و بنابراین برای استفاده در اثبات قضیه مناسب نیستند.

حال فرض کنید $u \in C^۲(\mathbb{R}^۲)$ تابعی کران‌دار باشد با این شرط که $\partial_۲ u > ۰$، در معادله‌ی (۱.۴) صدق کند و $\nu \in \mathbb{S}^۱$ به طوری که به ازای نقطه‌ای در دامنه مانند $x_۰$ داشته باشیم: $\nu \cdot \nabla u(x_۰) = ۰$. تعریف می‌کنیم : $\phi_{x_۰} = \phi = \nu \cdot \nabla u$. در این صورت دیدیم که این تابع و $\partial_۲ u$ در هسته‌ی عملگر شرودینگر $-\Delta - F''(u)$ قرار دارند. بنابر فرض $\partial_۲ > ۰$ و قضیه‌ی (۱.۴) و (۲.۴) می‌توانیم بگوییم $\lambda_۱(F''(u)) = ۰$. از طرفی بنابر قضیه‌ی (۳.۴) می‌توانیم بگوییم که ϕ تنها باید یک علامت داشته باشد. هم‌چنین داریم $\phi(x_۰) = ۰ = \min_{x\in\mathbb{R}^۲} \phi$. در نتیجه بنابر اصل ماکسیمم برای عملگرهای بیضوی ϕ برابر تابع ثابت صفر است و u در راستای ν ثابت است و حدس دی‌جورجی برای بعد ۲ اثبات می‌شود.

۲.۴. اثبات سوین از نسخه‌ی ضعیف‌تری از حدس دی‌جورجی. سوین با الهام از اثبات دی‌جورجی برای هموار‌ی رویه‌های مینیمال کمینه اثبات کرد سطح ترازهای جواب‌های معادله‌ی (۱.۳) که در شرط

$$\lim_{x_n\to\pm\infty} u(x', x_n) = \pm۱ \qquad (۲.۴)$$

صدق می‌کنند به ازای $n \leq ۸$ ابرصفحه‌هایی در فضا هستند. قضیه‌ی اصلی او که به بهبودی صافی [1] شهرت دارد ابرصفحه بودن سطح ترازهای کمینه‌های تابعک انرژی گینزبرگ‌ـلانداو را نشان می‌دهد. ابتدا اثبات می‌کنیم که نقاط بحرانی تابعک انرژی گینزبرگ‌ـلانداو (جواب‌هایی از معادله‌ی آلن‌ـکن) که در شرط حدی (۲.۴) صدق می‌کنند کمینه‌هایی برای این تابعک هستند. روشی که برای اثبات این حکم استفاده می‌شود به روش صفحات محرک [2] شهرت دارد و اولین توسط لویس نایرنبرگ توسعه داده شده است.

لم ۴.۴. فرض کنید $u \in C^۲(\mathbb{R}^n, [-۱, ۱])$ در شرایط حدس دی‌جورجی (۱.۳) و شرط حدی (۲.۴) صدق کند. در این صورت u یک کمینه‌ی موضعی تابعک $\mathcal{I}$ است.

[1] Improvement of flatness
[2] Moving Planes

اثبات. اثبات می‌کنیم که این تابع تنها جواب معادله‌ی آلن-کن در هر گوی باز به مرکز مبدا و شرایط مرزی $u|_{\partial B_R}$ است. فرض کنید v جواب دیگری از معادله‌ی

$$\begin{cases} \Delta v = v^{3} - v & x \in B_R \\ v = u & x \in \partial B_R \end{cases} \tag{۳.۴}$$

تعریف می‌کنیم

$$u_T(x) = u(x', x_n + T), \quad t_m = \inf\{t \geq 0 : v \leq u_t \in \overline{B_R}\}.$$

با توجه به این‌که v جواب متفاوتی نسبت به u است، $x_0 \in B_R$ موجود است که $u(x_0) \neq v(x_0)$. فرض کنید $u(x_0) > v(x_0)$ (اثبات حالت دیگر مشابه است). در این صورت داریم $t_m > 0$. بنابر تعریف داریم: $v \leq u_{t_m}$. هم‌چنین $x_1 \in \overline{B_R}$ موجود است به طوری که: $u_{t_m}(x_1) = v(x_1)$. بنابر خاصیت $\partial_n u > 0$ داریم:

$$u_{t_m}|_{\partial\Omega} > u|_{\partial\Omega} = v|_{\partial\Omega}$$

پس نقطه‌ی x_1 باید متعلق به B_R باشد. با توجه به اصل ماکسیمم از این موضوع نتیجه می‌شود که u_{t_m} و v باید در B_R با هم برابر باشند. □

قضیه‌ی صافی بهبودیافته بیان می‌کند که اگر سطح تراز یک کمینه‌ی تابعک انرژی $\mathcal{I}$ در یک استوانه با ارتفاع به میزان کافی کوچک قرار گرفت، آن‌گاه در دستگاه مختصات دیگری در یک استوانه‌ی کوچک‌تر قرار می‌گیرد.

قضیه ۵.۴. فرض کنید u یک کمینه‌ی تابعک انرژی $\mathcal{I}$ در استوانه‌ی $\{|x'| \leq l\} \times \{|x_n| \leq l\}$ باشد به طوری که $0 \in \{u = 0\} \subset \{|x_n| \leq \theta\}$. مقدار ثابت $\theta_0 > 0$ را در نظر بگیرید. در این صورت ثوابتی وابسته به بعد مانند $0 < \eta_1 < \eta_2 < 1$ و ثابتی وابسته به n، θ_0 و F مانند ϵ_0 موجود است به طوری که به ازای هر θ و l که $\frac{\theta}{l} \leq \epsilon \leq \epsilon_0$ و $\theta_0 \leq \theta$، داریم:

$$\{u = 0\} \cap (\{|x'| \leq \eta_2 l\} \times \{|x_n| \leq \eta_2 l\}) \subset \{|x \cdot \zeta| \leq \eta_1 \theta\},$$

به ازای یک $\zeta \in \mathbb{S}^{n-1}$.

حال فرض کنید u یک کمینه‌ی تابعک انرژی $\mathcal{I}$ در $\mathbb{R}^n$ باشد و $u(0) = 0$. فرض کنید دنباله‌های θ_k, l_k, ξ_k موجود باشند که

$$\xi_k \in \mathbb{S}^{n-1} \qquad l_k \to +\infty \qquad \frac{\theta_k}{l_k} \to 0 \tag{۴.۴}$$

به طوری که:

$$\{u = 0\} \cap \{|\pi_{\xi_k} x| \leq l_k\} \cap \{|x \cdot \xi_k| \leq l_k\} \subset \{|x \cdot \xi_k| \leq \theta_k\} \tag{۵.۴}$$

بنا بر فرض u یک کمینه در استوانه‌ی $\{|x'| \leq l_k\} \times \{|x_n| \leq l_k\}$ نیز هست. بنا بر شرط ۵.۴، $\{u = 0\}$ در یک دستگاه مختصات در درون استوانه‌ی کوتاه‌تری به ارتفاع θ_k قرار می‌گیرد. بنا بر شرط ۴.۴ برای هر $\epsilon > 0$ می‌توان k را به میزان کافی بزرگ انتخاب کرد به نحوی که $\frac{\theta_k}{l_k} \leq \epsilon$. θ_0 را ثابت در نظر بگیرید و فرض کنید $0 < \epsilon \leq \epsilon_0(\theta_0)$. در این صورت اگر داشته باشیم $\theta_0 \leq \theta$ می‌توان با استفاده از قضیه‌ی ۵.۴ دستگاه مختصات دیگری یافت که در آن $\{u = 0\}$ در استوانه‌ای با ارتفاع کمتر قرار گیرد. با تکرار اعمال این قضیه می‌توانیم فرض کنیم دستگاه مختصاتی وجود دارد که در آن $\{u = 0\}$ در استوانه‌ای به ارتفاع θ'_k قرار می‌گیرد؛ یعنی l'_k موجود است که:

$$\eta_1 \theta_0 \leq \theta'_k \leq \theta_0 \quad , \quad \frac{\theta'_k}{l'_k} \leq \frac{\theta_k}{l_k} \leq \epsilon \tag{۶.۴}$$

بنابراین داریم: $l'_k \geq \frac{\eta_1}{\epsilon}\theta_0$. با میل‌دادن ϵ به صفر نتیجه می‌شود که $\{u = 0\}$ در نواری با سطح مقطع $\mathbb{R}^{n-1}$ و ارتفاع θ_0 قرار می‌گیرد. با توجه به این‌که θ_0 مقداری دل‌بخواه بود نتیجه می‌شود که $\{u = 0\}$ یک صفحه است.

قضیه‌ی صافی بهبودیافته (۵.۴) از تعمیم نامساوی هارنک برای سطح ترازهای کمینه‌های موضعی تابعک $\mathcal{I}$ نتیجه می‌شود.

اثبات سوین از نامساوی هارنک برای سطح ترازهای جواب‌های معادله‌ی آلن-کن شامل تقریب‌های پیچیده‌ای از اندازه‌ی مجموعه‌هایی از سطح ترازها و تصویرشان بر زیرفضاهای خطی است که بررسی و بیان آن‌ها خارج از اهداف این نوشته است.

۵. تعمیم‌هایی از حدس دی‌جورجی

فیگالی [۱] و سرا [۲] ثابت کردند هر جواب پایدار از معادله‌ی $(-\Delta)^{۱/۲}u+f(u)=\circ$ در $\mathbb{R}^۳$ یک تابع یک‌بعدی است [۲۷]. جواب‌های پایدار این معادله در واقع کمینه‌های پایداری از تابعک انرژی زیر هستند:

$$\int_{\{x_{n+۱}\geq \circ\}}\frac{۱}{۲}|\nabla u|^۲\,dx\,dx_{n+۱}+\int_{\{x_{n+۱}=\circ\}}F(u)\,dx$$

چنین تابعک‌های انرژی‌ای ابتدا در نظریه‌ی بررسی تحول و پایداری کریستال‌ها مطرح شده‌اند [۲۶]. خواصی مشابه آنچه که برای تابعک انرژی گینزبرگ-لانداو اثبات کردیم قابل تعمیم به این تابعک نیز هستند. به طور مثال این تابعک نیز خاصیت Γ-همگرایی به تابعک محیط را دارد. یکی از گام‌های اساسی اثبات فیگالی و سرا این است که رویه‌های مینیمال پایدار در بعد سه تنها ابرصفحه‌ها هستند. حکمی که تا به حال نسخه مشابهش برای ابعاد بالاتر اثبات نشده است.

والدینوچی [۳]، شیونزی [۴] و سوین با ابزارهای مشابه احکام مرتبط با حدس دی‌جورجی را برای معادله‌ی آلن-کن و تابعک انرژی وابسته به p-لاپلاسین‌ها اثبات کرده‌اند [۲۸]. هم‌چنین سوین و داسیلوا [۵] توانسته‌اند تقارن یک‌بعدی جواب‌های چسبندگی کران‌دار و در یک جهت یکنوای معادله‌ی کاملاً غیرخطی $F(D^۲u)=f(u)$ را در بعد دو ثابت کنند [۲۹].

تشکر و قدردانی

نویسنده این مقاله مراتب قدردانی صمیمانه‌ی خود را نسبت به آقای دکتر فتوحی ابراز می‌دارد که با مطالعه‌ی نسخه‌ی اولیه‌ی این نوشته و ارائه‌ی پیشنهادهای ارزنده‌شان او را راهنمایی کردند.

مراجع

[1] Savin, O. (2009) Regularity of flat level sets in phase transitions ,*Annals of Mathematics*, **169**, 41–78.

[2] Modica L., Mortola S. (1980) Some entire solutions in the plane of nonlinear Poisson equations ,*Boll. Un. Mat. Ital.*, **17**, no. 2, 614–622.

[3] Ghosuob N. , Gui C. (1998) On a conjecture of De Giorgi and some related problems ,*Math. Ann.*, **311**, 481-491.

[4] Berestycki H., Caffarelli L., Nirenberg L. (1997) Further qualitative properties for elliptic equations in unbounded domains ,*Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 25*, **25**, 69-94.

[5] Ambrosio L., Cabre X, (2000) Entire solutions of semilinear elliptic equations in $\mathbb{R}^3$ and a conjecture of De Giorgi. ,*J. American Math. Soc.*, **13**, 725-739.

[6] Barlow M., Bass R., Gui C., (2000) The Liouville property and a conjecture of De Giorgi. ,*Comm. Pure Appl. Math.*, **53**, 1007-1038.

[7] Berestycki H., Hamel F., Monneau, R., (2000) One-dimensional symmetry of bounded entire solutions of some elliptic equations. ,*Duke Math. J.*, **103**, no. 3, 375–396.

[8] Farina A., (1999) Symmetry for solutions of semilinear elliptic equations in $\mathbb{R}^n$ and related conjectures. ,*Ricerche Mat.*, **48**, 129–154.

[9] Cahn J., Hillard J., (1958) Free energy of a nonuniform system I. Interfacial free energy. ,*J. Chem. Phys.*

[10] Figalli A., Cozzi M., Regularity theory of minimal surfaces: an overview. ,https://people.math.ethz.ch/~afigalli/lecture-notes-pdf/Regularity-theory-for-local-and-nonlocal-minimal-surfaces-an-overview.pdf

[11] Ginzburg V.L., Pitaevski L. P., ROn the theory of superfluidity. ,*Soveit Physics JETP*, 1958

[12] Rowlinson J. S., (1979) Translation of J. D. van der Waals (The thermodynamic thoery of capillarity under the hypothesis of a continuous variation of density) ,*J. Statist. Phys.*

[13] Allen S., Cahn J., (1979) A microscopic theory for antiphase boundry mothion and its application to antiphase domain coarsening. ,*Acta Metallurgia*

[14] Gilles Carbou (1995)Unicité et minimalité des solutions d'une équation de Ginzburg-Landau ,*Annales de l'Institut Henri Poincaré C, Analyse non linéaire*

[15] Gibbons G. W. , Townsend P. K., (1999) Bogomol'nyi equation for intersecting domain walls. ,*Phys. Rev. Lett.*

[1] Alessio Figalli
[2] Joaquim Serra
[3] Enrico Valdinoci
[4] Berardino Sciunzi
[5] Daniela De Silva

[16] Modica L. (1979)Γ-convergence to minimal surfaces problem and global solutions of $\Delta u = u^3 - u$. ,*Proceedings of the International Meeting on Recent Methods in Nonlinear Analysis*

[17] Bernstein S., (1915) Sur un théorème de géométrie et son application aux équations aux dérivées partielles du type elliptique

[18] De Giorgi E, (1965) "Una extensione del teorema di Bernstein. ,*Ann. Scuola Norm. Sup. Pisa.*, **19**, 79-85.

[19] Mickle E., (1965) "A remarke on a theorem of Serge Bernstein.

[20] Hopf E., On S. Bernstein's theorem on surfaces z(x,y) of nonpositive curvature.

[21] Fleming W.H., (1962) On the oriented Plateau problem,*Rend. Circ. Mat. Palermo.*, **17**, no. (2) 11, 69-90.

[22] Almgren F.J., (1966) FSome interior regularity theorems for minimal surfaces and an extension of Bernstein's theorem. ,*Ann. of Math.*, **84**, 277-292.

[23] Simons J. (1968), Minimal varieties in riemannian manifolds. ,*Ann. of Math. (2)*, **88**, 62–105

[24] Bombieri E., De Giorgi E., Giusti E., (1969) Minimal cones and the bernstein theorem ,*Inventiones Math.*, **7**, 243-269.

[25] Giusti E. (1984) *Minimal surfaces and functions of bounded variation*. Birkh¨auser Verlag, Basel.

[26] Nabarro F.R.N.,. (1947) Dislocations in a simple cubic lattice. ,*Proc. Phys. Soc.*, **59**, 256–272.

[27] Figalli, A., Serra, J. , (2020) On stable solutions for boundary reactions: a De Giorgi-type result in dimension 4 + 1. , *Invent. math.*, **219**,153–177.

[28] Valdinoci E., Sciunzi B., Savin O. ,(2006) Flat Level Set Regularity of p-Laplace Phase Transitions, Mem. Amer. Math. Soc. 182 , no. 858.

[29] De Silva D., Savin O., (2009) Symmetry of global solutions to a class of fully nonlinear elliptic equations in 2D. ,*Indiana Univ. Math. J.*, **58**, no. 1, 301–315.

* دانشجوی کارشناسی ریاضی، دانشگاه صنعتی شریف

رایانامه: matin.hajian@sharif.edu

مجله‌ی ریاضی شریف
دوره‌ی سوم، شماره‌ی اول (بهار ۱۴۰۲)

احراز هویت خودکار بر اساس چهره

احمد رحیمی *

چکیده. امروزه در زندگی روزمره و بالاخص فعالیت‌های علمی، در سطوح مختلف، شاهد کاربردهای بسیار گسترده‌ی هوش مصنوعی هستیم. از ابزارهای مترجم متن گرفته تا جست‌وجو در تصاویر و ابزارهای تبدیل صوت به متن. یکی از این کاربردها که امروزه در بعضی لپ‌تاپ‌ها و گوشی‌های موبایل نیز مورد استفاده قرار می‌گیرد، قابلیت احراز هویت از طریق چهره است. این سیستم‌ها معمولاً به این شکل کار می‌کنند که در ابتدا تصویر یا فیلمی از چهره‌ی شما می‌گیرند و در دفعات بعدی که نیاز به احراز هویت باشد، با گرفتن عکس یا فیلمی جدید از چهره‌ی شما و تطبیق آن با تصویر یا فیلم اولیه، هویت شما را احراز می‌کنند. یکی از چالش‌های طراحی چنین سیستم‌هایی مطابقت‌دادن دو چهره با یکدیگر است. این مسأله که در حوزه‌ی بینایی کامپیوتر به طور مبسوط مورد مطالعه قرار گرفته، مسأله‌ی تأیید چهره نام دارد. در این نوشته ابتدا مدل Facenet را که از یادگیری متضاد استفاده می‌کند به عنوان راه‌حلی برای مسأله‌ی تأیید چهره معرفی می‌کنیم. سپس چالش زنده‌بودن را مطرح می‌کنیم و برای فائق‌آمدن بر آن، روشی برای تشخیص جهت صورت شخص در یک تصویر ارائه می‌دهیم. در نهایت اجزای مختلفی که ارائه شده را در کنار هم قرار داده و تصویری کلی از سیستم احراز هویت ارائه خواهیم داد.

۱. مقدمه

در قرن اخیر شاهد پیشرفت گسترده و پرشتابی در حوزه‌ی هوش مصنوعی بوده‌ایم؛ خصوصاً بعد از سال ۲۰۱۲ که ظهور شبکه‌های عصبی[۱] باعث انقلابی در این حوزه شدند. یکی از حوزه‌هایی که شبکه‌های عصبی در آن منجر به پیشرفت شگرفی شده‌اند بینایی کامپیوتر است. بینایی کامپیوتر شاخه‌ای از هوش مصنوعی است که به کامپیوترها این قدرت را می‌دهد که اطلاعات معناداری از تصاویر، فیلم‌ها و سایر ورودی‌های بصری به دست آورند. مسائل متنوعی در بینایی کامپیوتر وجود دارد که از معروف‌ترین آن‌ها می‌توان به دسته‌بندی تصاویر[۲]، تشخیص اشیا[۳] و قطعه‌بندی تصاویر[۴] اشاره کرد. مسأله‌ی ما که احراز هویت با استفاده از چهره می‌باشد نیز در حوزه‌ی بینایی کامپیوتر قرار می‌گیرد.

ما در این نوشته به دنبال طراحی سیستمی هستیم تا بتواند با دریافت یک ورودی بصری مانند تصویر یا فیلمی از چهره‌ی یک شخص و تطبیق آن با اطلاعاتی که پیشتر از آن شخص ذخیره کرده، مثلاً تصاویر و فیلم‌هایی که مطمئن است مربوط به این شخص هستند، هویت او را به صورت خودکار احراز کند. برای چنین سیستمی کاربردهای بسیاری می‌توان برشمرد؛ از استفاده در گوشی‌های هوشمند و لپ‌تاپ‌ها گرفته، تا انجام‌دادن کارهای اداری از راه دور. مورد اخیر خصوصاً در زمان همه‌گیری کرونا اهمیت پیدا می‌کند؛ چرا که افراد می‌توانند بدون نیاز به مراجعه‌ی حضوری و قرارگرفتن در معرض خطر ابتلا به بیماری کار اداری خود را انجام دهند.

مسأله‌ی مشابهی که در بینایی کامپیوتر وجود دارد، مسأله‌ی تأیید چهره[۵] نام دارد. در این مسأله، دو تصویر متفاوت در حالت کلی از صورت انسان‌هایی داده شده و هدف این است که بفهمیم آیا این دو تصویر متعلق به شخص یکسانی هستند یا خیر. توجه کنید که این دو تصویر می‌توانند مربوط به زمان‌های متفاوتی باشند؛ پس‌زمینه‌های تصاویر می‌توانند با هم متفاوت باشند؛ جهت صورت در عکس‌ها می‌تواند یکسان نباشد و حتی فرد ممکن است در یکی از تصاویر با عینک و در دیگری بدون عینک باشد، یا در یکی از عکس‌ها ریش داشته باشد و در دیگری ریشش را زده باشد. در کنار این چالش‌ها، مقایسه‌ی دو تصویر از

[1] neural networks
[2] image classification
[3] object detection
[4] image segmentation
[5] face verification

صورت و تأیید چهره‌های آن دو، به خودی خود مسأله‌ی بسیار دشواری است و حل این سوال را سخت و چالش‌برانگیز خواهد کرد.

مرجع [۲] با کمک شبکه‌های عصبی و با کمک‌گرفتن از روشی به نام یادگیری متضاد[1] تلاش کرده این مسأله را حل کند و به نتایج بسیار خوبی هم دست یافته است. در این مقاله یک شبکه‌ی عصبی در نظر گرفته شده که با ورودی گرفتن تصویری از صورت شخص یک بردار ویژگی ۵۱۲ بعدی خروجی می‌دهد. سپس این شبکه‌ی عصبی طوری آموزش داده می‌شود که بردارهای خروجی دو تصویر مربوط به یک شخص تا جای ممکن نزدیک به هم باشند و بردارهای خروجی دو تصویر از دو شخص متفاوت تا جای ممکن از هم دور باشند. به این ترتیب، اگر دو تصویر از صورت دو نفر داشته باشیم با دادن این دو تصویر به این شبکه‌ی عصبی و اندازه‌گیری فاصله‌ی بردارهای ویژگی خروجی آن از یک‌دیگر می‌توانیم در مورد یکی‌بودن شخص موجود در دو تصویر یادشده اظهارنظر کنیم. در بخش ۲ به جزئیات این روش خواهیم پرداخت.

نکته‌ی قابل توجه درباره‌ی روش Facenet این است که به مسأله به شکل کلی نگاه می‌کند؛ در حالی که در کاربردی که ما به دنبال آن هستیم می‌توانیم روی برخی شرایط تصویر محدودیت‌هایی قرار دهیم. برای مثال، یکی از چالش‌های بزرگ حل مسأله‌ی تأیید چهره در حالت کلی، همان‌طور که در بالا اشاره شد، تغییر زاویه‌ی صورت در تصاویر است؛ اما در احراز هویت با استفاده از چهره، می‌توانیم از کاربر بخواهیم از روبه‌رو از صورت خود عکس بگیرد و چهره‌اش حالت خاصی نداشته باشد (مثلاً خندان یا درهم نباشد). در نتیجه به مدلی نیاز داریم که بتواند در یک تصویر جهت صورت را تشخیص دهد تا اگر از روبه‌رو نبود از کاربر بخواهیم تصویر دیگری را که از روبه‌رو گرفته شده است برای ما ارسال کند.

چالش دیگری که در مسأله‌ی ما وجود دارد چالش زنده‌بودن تصویر یا فیلم ارسالی است؛ زیرا گاهی می‌خواهیم مطمئن شویم تصویر یا فیلمی که کاربر ارسال می‌کند در همان لحظه گرفته شده است. این مسأله چالشی حیاتی است چرا که در صورت حل‌نشدن این مشکل، شخصی ممکن است با داشتن یک تصویر یا فیلم از شخص دیگری بتواند به جای او احراز هویت شود و احتمالا خرابی‌هایی در حساب او ایجاد کند. با این‌حال، این چالش با داشتن مدل تشخیص جهت صورتی که در بالا ذکر شد به سادگی قابل حل است. کافی است دنباله‌ای از جهت‌های تصادفی تولید کنیم و به کاربر بدهیم و از او بخواهیم فیلمی برای ما ارسال کند که در آن صورت خود را طبق دنباله‌ی داده‌شده از جهات، حرکت دهد. سپس با استفاده از مدل تشخیص جهت صورت، صحت انجام این حرکات را بررسی کنیم.

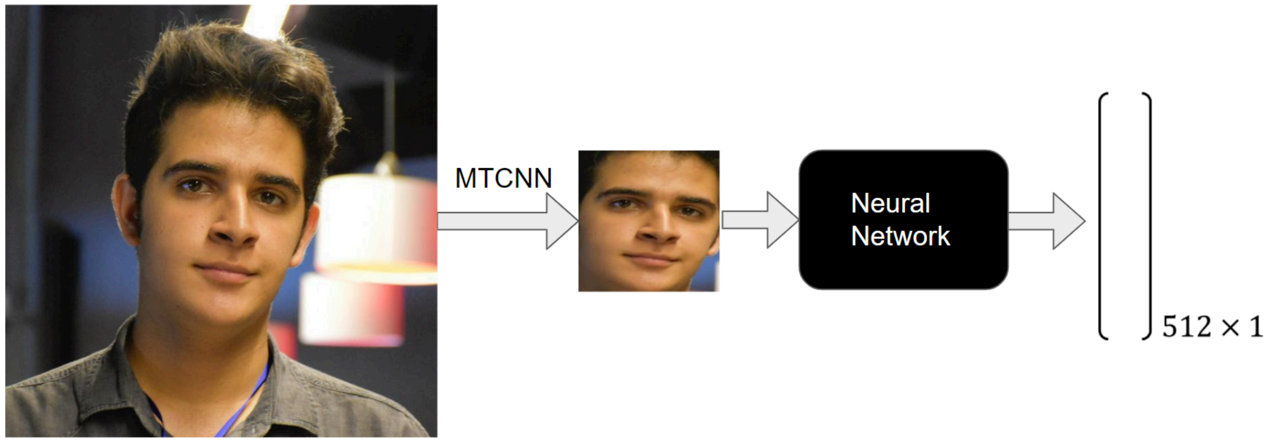
۲. روش Facenet

در این بخش روش Facenet را به اختصار توضیح می‌دهیم. هدف این است که خواننده در انتها اطلاعاتی کلی از نحوه‌ی کار کل سیستم به دست آورد. برای مطالعه‌ی بیشتر درباره‌ی این روش می‌توانید به [۲] مراجعه کنید.

در روش Facenet، تصویر ورودی ابتدا به الگوریتمی به نام MTCNN [۳] داده می‌شود تا مکان چهره در تصویر تشخیص داده شود. سپس تصویر ورودی را از آن قسمت برش[2] می‌دهیم و ابعاد آن را تغییر می‌دهیم تا قطعه عکسی مربعی به دست آوریم که تنها شامل صورت شخص و میزان پس‌زمینه‌ی آن تا جای ممکن کم است. سپس قطعه عکس حاصل را به شبکه‌ی عصبی می‌دهیم و بردار ویژگی ۵۱۲ بعدی عکس را از شبکه‌ی عصبی دریافت می‌کنیم (شکل ۱).

هدف این است که با انجام عمل فوق برای دو تصویر ورودی و مقایسه‌ی فاصله‌ی اقلیدسی بردارهای ویژگی نهایی آن‌ها، تشخیص دهیم دو تصویر از صورت یک شخص گرفته شده یا نه. برای آموزش شبکه‌ی عصبی در این روش، از یادگیری متضاد استفاده می‌شود. یادگیری متضاد به این شکل است که سه تصویر انتخاب می‌کنیم که دو تا از آن‌ها از یک شخص و سومی از شخص دیگری باشد. یکی از دو تصویری که از یک شخص گرفته شده را پایه[3] و دیگری را تصویر مثبت[4] می‌نامیم. تصویر سوم را نیز تصویر منفی[5] می‌نامیم. هدف این است که شبکه‌ی عصبی را طوری آموزش دهیم تا فاصله‌ی تصویر منفی از تصویر پایه بیشتر از فاصله تصویر مثبت از تصویر پایه شود (شکل ۲). به عبارت دیگر، اگر بردار ویژگی تصاویر پایه، مثبت و منفی را به ترتیب با v_a، v_p، v_n نشان دهیم، می‌خواهیم فاصله‌ی بردار ویژگی جفت تصویری که مربوط به یک شخص هستند، با یک

[1] contrastive learning
[2] crop
[3] anchor
[4] positive
[5] negative



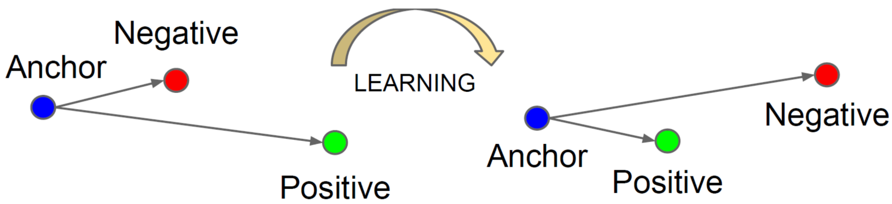
شکل ۱: روند روش Facenet که در آن ابتدا تصویر ورودی به مدل MTCNN داده می‌شود تا قطعه‌ای مربعی از صورت شخص در تصویر به دست آید. سپس آن را به شبکه‌ی عصبی می‌دهیم و بردار ویژگی را خروجی می‌گیریم.

حاشیه‌ی امن، کمتر از فاصله‌ی بردار ویژگی جفت تصویری که مربوط به دو شخص مختلف هستند شود:

$$\|v_a - v_p\|_2^2 + \alpha < \|v_a - v_n\|_2^2$$

که در آن α حاشیه‌ی امن بین جفت‌های مثبت و جفت‌های منفی است. در نتیجه شبکه‌ی عصبی را به گونه‌ای آموزش می‌دهیم که تابع هزینه‌ی زیر را کمینه کند:

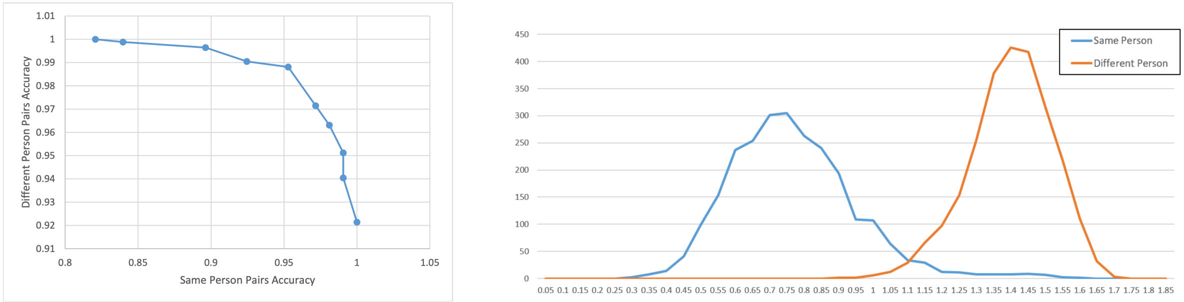
$$\max\left(\|v_a - v_p\|_2^2 - \|v_a - v_n\|_2^2 + \alpha, 0\right)$$



شکل ۲: یادگیری متضاد که در آن تلاش می‌شود بعد از یادگیری فاصله‌ی میان جفت پایه و مثبت کمتر از فاصله‌ی میان جفت پایه و منفی شود.

در نتیجه با آموزش شبکه‌ی عصبی به شیوه‌ی فوق، به ازای دو تصویر ورودی، از آن‌ها طبق روند شکل ۱ دو بردار ویژگی به دست می‌آوریم. با داشتن یک مقدار آستانه و مقایسه‌ی فاصله‌ی دو بردار ویژگی با این مقدار آستانه، می‌توان راجع به یکی‌بودن افراد موجود در تصویر اظهارنظر کرد؛ به این شکل که اگر فاصله‌ی دو بردار ویژگی کمتر از این مقدار آستانه باشد، این دو تصویر از صورت یک شخص گرفته شده‌اند و در غیر این صورت اشخاص موجود در دو تصویر متفاوت هستند.
برای بررسی بهتر نتیجه‌ی این روش، ۵۰۰۰ جفت تصویر در نظر گرفته‌ایم که ۲۵۰۰ تا از آن‌ها از یک شخص گرفته شده و ۲۵۰۰ تای دیگر تصاویر مربوط به اشخاص متفاوتی هستند. سپس این عکس‌ها را به الگوریتم Facenet داده و دو بردار ویژگی ۵۱۲ بعدی خروجی گرفته‌ایم. شکل ۳(آ) هیستوگرام فاصله‌ی این بردارها است.همان‌طور که در هیستوگرام می‌توان دید، جفت تصاویر با افراد مختلف به خوبی با استفاده از فاصله‌ی بردارهای ویژگی از جفت تصاویر مربوط به یک فرد جدا شده‌اند. در واقع، اگر مقدار آستانه را برابر با ۱/۱ قرار دهیم و طبق روشی که در پاراگراف قبل ذکر شد عمل کنیم، وضعیت ۹۹ درصد از جفت تصاویر را می‌توانیم به درستی تشخیص دهیم که دقت بالایی به شمار می‌رود. هم‌چنین در شکل ۳(ب) دقت برای جفت تصویرهای مربوط به اشخاص مختلف و مربوط به جفت تصویرهای مربوط به یک شخص را به ازای مقادیر مختلف آستانه نشان داده‌ایم.

به این ترتیب هر کاربری با توجه به نیاز و میزان حساسیتش روی اشتباه‌کردن در هر یک از این دو دسته می‌تواند مقدار آستانه‌ی مناسبی برای خود انتخاب کند. به بیان دیگر این روش در میزان حساسیت مدل نیز انعطاف خواهد داشت.



(ب) (آ)

شکل ۳: نتایج مدل Facenet. (آ) هیستوگرام فواصل میان بردارهای خروجی از روش Facenet برای جفت عکس‌هایی از یک‌نفر (رنگ آبی) و جفت عکس‌هایی از افراد مختلف (رنگ نارنجی). (ب) دقت در جفت تصویرهای مربوط به اشخاص مختلف و در جفت تصویرهایی از یک شخص به ازای مقادیر آستانه‌ی مختلف.

۳. مدل تشخیص جهت صورت

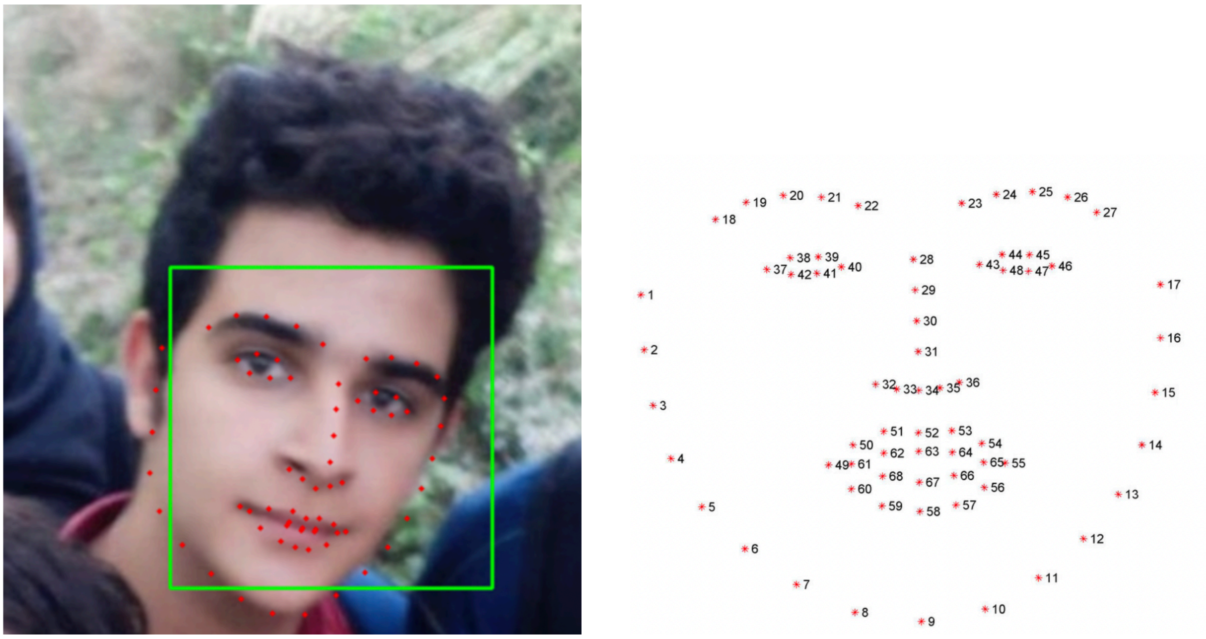
در این بخش مدل تشخیص جهت صورت را توضیح می‌دهیم. این مدل با ورودی‌گرفتن یک تصویر از چهره‌ی یک فرد، جهت صورت او در عکس را خروجی می‌دهد. هدف این است که یکی از پنج حالت روبه‌رو، بالا، پایین، چپ و راست را خروجی دهد. برای سادگی در این بخش فقط روش تشخیص از روبه‌رو بودن را توضیح می‌دهیم. برای چهار حالت دیگر نیز به طور مشابه می‌توان عمل کرد. برای تشخیص جهت صورت، از نقاط خاص صورت[1] استفاده می‌کنیم. نخست استخراج نقاط خاص صورت با استفاده از کتابخانه‌ی Dlib [۱] را معرفی می‌کنیم. سپس دو روش متفاوت را ارائه می‌کنیم که برای تشخیص از روبه‌رو بودن تصویر، از نقاط خاص صورت استفاده می‌کنند. در نهایت راهی ارائه می‌دهیم که دو روش ذکرشده را با هم ترکیب کرده و یک مدل نهایی قدرتمند به ما می‌دهد.

۱.۳ نقاط خاص صورت. با استفاده از کتابخانه‌ی Dlib [۱] می‌توان نقاط خاص صورت موجود در یک تصویر را به دست آورد. در واقع می‌توان یک تصویر شامل صورت یک انسان را به این کتابخانه داد و مختصات ۶۸ نقطه‌ی خاص از صورت در تصویر را خروجی گرفت. این ۶۸ نقطه در یک شمایل صورت در شکل ۴(آ) نشان داده شده‌اند. هم‌چنین یک تصویر واقعی شامل صورت انسان به این کتابخانه ورودی داده شده و در مختصات خروجی آن نقاط قرمز کشیده شده که نتیجه را می‌توانید در شکل ۴(ب) مشاهده کنید.

۲.۳ روش اول. در اولین روش، به نحوی به دنبال سنجش میزان تقارن در صورت هستیم. هرچه صورت موجود در عکس متقارن‌تر باشد، زاویه‌ی صورت شخص به روبه‌رو نزدیک‌تر است. به این منظور، ابتدا از نقاط روی بینی، وسط لب و وسط چانه بهترین خط ممکن را عبور می‌دهیم. سپس هر نقطه از سمت چپ این خط را نسبت به این خط قرینه کرده و فاصله‌ی قرینه‌شده‌ی آن نقطه با نقطه‌ی متناظرش در سمت راست خط را محاسبه می‌کنیم. مجموع تمام این فواصل، به ما معیاری از میزان متقارن‌بودن و در نتیجه از روبه‌رو بودن صورت می‌دهد. در واقع هرچه این حاصل‌جمع عدد کمتری باشد، صورت متقارن‌تر است. برای فهم بهتر این روش می‌توانید به شکل ۵ مراجعه کنید.

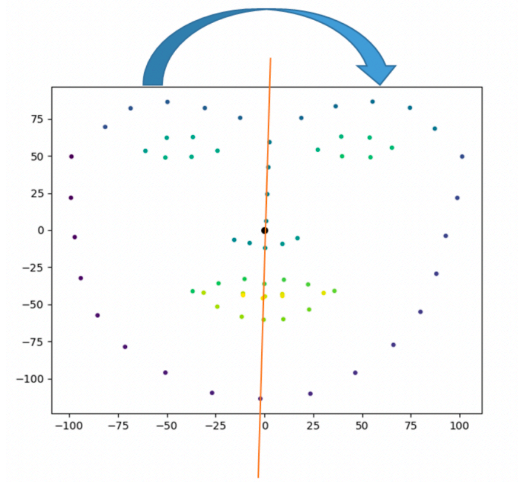
۳.۳ روش دوم. در این روش هدف تطبیق نقاط خاص به‌دست‌آمده از تصویر هدف با نقاط خاص به‌دست‌آمده از یک تصویر ذخیره‌شده است که می‌دانیم از روبه‌رو است. این تصویر را تصویر نمونه می‌نامیم. ابتدا یک تابع پردازش اولیه‌ی[2] ساده روی نقاط خاص صورت معرفی می‌کنیم که شامل یک انتقال، یک دوران و یک تجانس است. ابتدا نقاط خاص را به گونه‌ای

[1] facial landmarks
[2] pre processing function



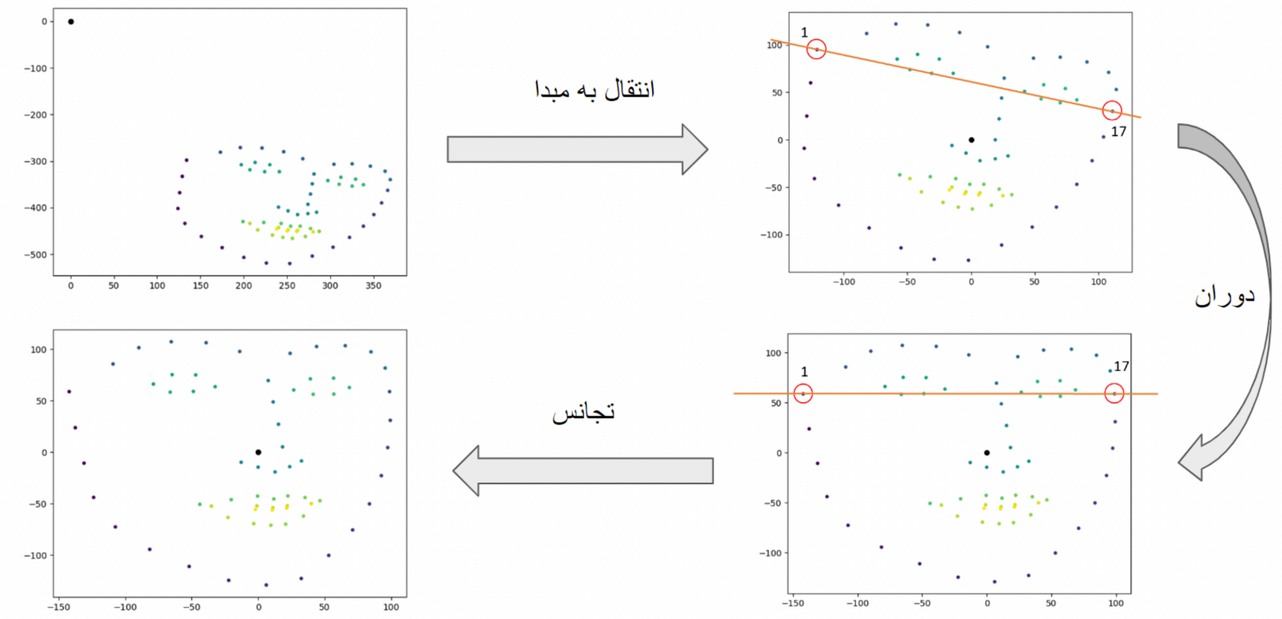
(آ) (ب)

شکل ۴: ۶۸ نقطه‌ی خاص صورت (آ) در یک شمایل و (ب) در یک صورت واقعی.



شکل ۵: ابتدا بهترین خط ممکن از نقاط روی بینی، وسط لب و وسط چانه را به دست آورده، نقاط سمت چپ خط را نسبت به خط قرینه کرده و فاصله‌ی نقاط حاصل از نقاط متناظرشان در سمت راست خط را محاسبه می‌کنیم و با هم جمع می‌زنیم.

انتقال می‌دهیم که میانگین آن‌ها در مبدأ قرار گیرد. سپس نقاط را به گونه‌ای دوران می‌دهیم که خط واصل نقاط ۱ و ۱۷ (به شکل ۴(آ) مراجعه کنید.) خطی افقی شود. به این ترتیب، صورت موجود در تصویر صاف می‌شود. در نهایت روی نقاط خاص به دست آمده یک تجانس را به گونه‌ای اعمال می‌کنیم که یک مربع به ضلع ۲۵۰ به آن‌ها محیط شود. مراحل این تابع پردازش اولیه را در شکل ۶ می‌توانید مشاهده کنید. حال نقاط خاص تصویر نمونه (که از روبه‌رو می‌باشد) و تصویر هدف (تصویر ورودی) را استخراج کرده و به تابع پردازش اولیه‌ای می‌دهیم که در بالا تعریف کردیم. فرض کنید نقاط خاص تصویر هدف بعد از اعمال تابع پردازش اولیه در ماتریس M و نقاط خاص تصویر نمونه نیز بعد از اعمال تابع پردازش اولیه در ماتریس N آمده باشد که



شکل ۶: مراحل سه‌گانه‌ی تابع پردازش اولیه.

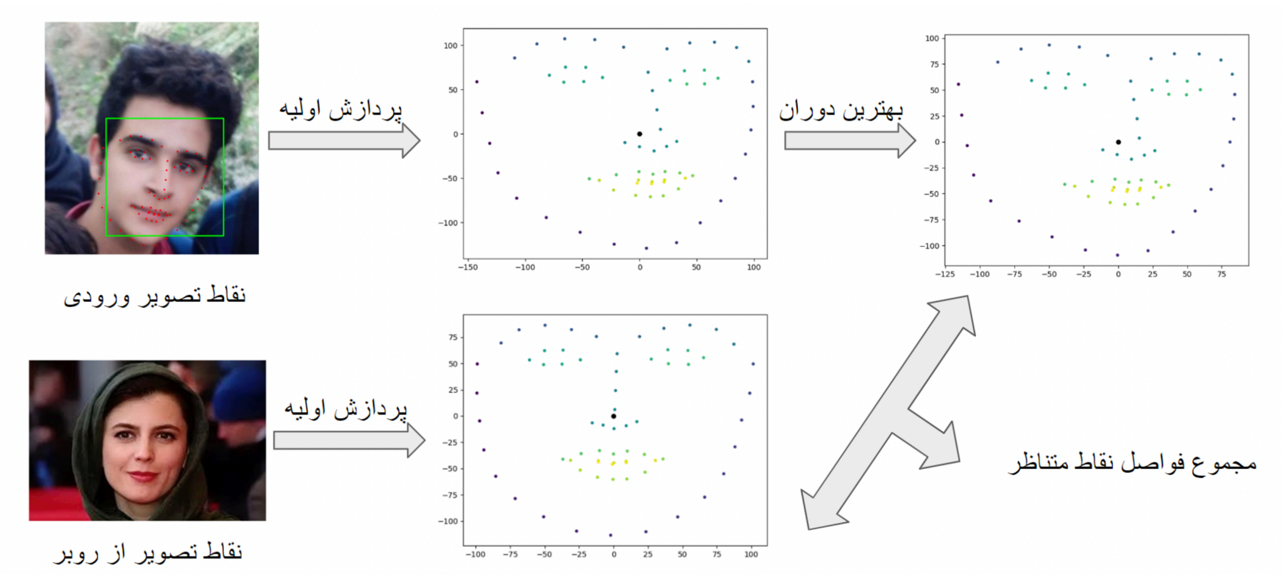
M, N به شکل زیر هستند:

$$M = \begin{bmatrix} x_۱ & x_۲ & \dots & x_{۶۸} \\ y_۱ & y_۲ & \dots & y_{۶۸} \end{bmatrix}, \quad N = \begin{bmatrix} x^t_۱ & x^t_۲ & \dots & x^t_{۶۸} \\ y^t_۱ & y^t_۲ & \dots & y^t_{۶۸} \end{bmatrix}$$

می‌خواهیم بهترین دورانی را پیدا کنیم که با اعمال آن روی نقاط M، آن‌ها را تا جای ممکن به نقاط N شبیه کند. اگر قرار دهیم $H = MN^T$ و $H = USV^T$ تجزیه‌ی طیفی H باشد، می‌توان دید بهترین دوران مذکور از رابطه‌ی $R = VU^T$ به دست می‌آید. این دوران را بر نقاط M اعمال می‌کنیم، سپس فاصله‌ی نقاط به‌دست‌آمده را از نقاط متناظرشان در N محاسبه می‌کنیم. حاصل‌جمع تمامی این فواصل، خروجی این روش است. تصویری کلی از این روش را می‌توانید در شکل ۷ ببینید.

در حقیقت این روش شباهت نقاط تصویر ورودی را با نقاط تصویری که می‌دانیم از روبه‌رو است می‌سنجد. هرچه خروجی این روش عددی بزرگ‌تر باشد یعنی این دو دسته از نقاط با هم متفاوت‌تر هستند و هرچه عدد کوچکتری باشد یعنی این دو دسته از نقاط به هم شبیه‌تر بوده و در نتیجه تصویر ورودی از روبه‌رو است.

۴.۳. ترکیب روش‌های اول و دوم و به‌دست‌آوردن مدل نهایی. هر یک از دو روشی که در بالا توضیح داده شدند ممکن است ضعف‌هایی داشته و در شرایطی کارکرد مطلوبی نداشته باشند. به همین دلیل در این بخش می‌خواهیم دو روش فوق را به گونه‌ای ترکیب کنیم تا مدلی نهایی به دست آوریم که از هر کدام از دو روش فوق قوی‌تر باشد. درواقع می‌خواهیم مقادیر مجهول a, b, c را به گونه‌ای بیابیم که اگر x خروجی روش اول و y خروجی روش دوم برای یک تصویر باشد، با محاسبه‌ی $ax + by$ و مقایسه‌ی آن با c بفهمیم آن تصویر از روبه‌رو گرفته شده یا خیر. به این منظور، ابتدا ۴۵ تصویر مختلف را انتخاب کرده و آن‌ها را بر حسب از روبه‌رو بودن مرتب کرده‌ایم. ۲۵ تصویر اول به عنوان تصویر از روبه‌رو و باقی تصاویرْ غیر روبه‌رو در نظر گرفته شده‌اند. سپس به آن‌ها وزن‌هایی مطابق شکل ۸(آ) داده شده که وزن هر تصویر اهمیت پیش‌بینی درست آن برای مدل ما را نشان می‌دهد. حال روش‌های اول و دوم را روی این ۴۵ تصویر اعمال کرده و عدد خروجی آن‌ها را ثبت می‌کنیم. در نتیجه می‌توان به هر تصویر به عنوان یک نقطه در فضای دوبعدی نگاه کرد که مؤلفه‌ی اول آن خروجی روش اول و مؤلفه‌ی دوم آن خروجی روش دوم می‌باشد. همچنین اگر نقاط مربوط به ۲۵ تصویر اول را سبز به نشانه‌ی روبه‌رو بودن و باقی نقاط را قرمز به نشانه‌ی غیر روبه‌رو بودن در نظر بگیریم، پیدا کردن a, b, c که به آن اشاره شد معادل پیدا کردن بهترین خط $ax + by = c$ است که نقاط سبز را از قرمز جدا کند (شکل ۸(ب)). حل چنین سوالی یک مسأله در یادگیری ماشین کلاسیک می‌باشد که SVM



شکل ۷: تصویری کلی از روش دوم.

وزن‌دار با هسته‌ی خطی[1] نام دارد و به تفصیل مطالعه شده است. با حل این سوال، مقادیر $a = ۰/۰۰۲, b = ۰/۰۹۱, c = ۷/۳۳۶$ به دست می‌آید. در نتیجه مدل نهایی به این شکل حاصل می‌شود که نقاط خاص تصویر ورودی را به دست آورده و آن‌ها را به روش‌های اول و دوم می‌دهیم. خروجی روش اول را در a و خروجی روش دوم را در b ضرب کرده و حاصل را با هم جمع می‌کنیم. در صورتی که مقدار حاصل از c کم‌تر بود می‌گوییم تصویر حاصل از روبه‌رو بوده و در غیر این صورت از روبه‌رو بودن آن را رد می‌کنیم.

۵.۳. جمع‌بندی. در این بخش قطعه‌های مختلف سیستم که در قسمت قبل توضیح داده شدند را در کنار هم قرار می‌دهیم تا یک تصویر کلی از سیستم احراز هویت داشته باشیم.

سیستم کلی احراز هویت بر اساس چهره را می‌توان با الگوریتم زیر توضیح داد:

(۱) یک دنباله‌ی تصادفی از جهت‌های بالا، پایین، چپ، راست و روبه‌رو بساز که شامل حداقل یک جهت روبه‌رو باشد.
(۲) از کاربر بخواه از خود فیلمی بفرستد که در آن با صورتش دنباله‌ی فوق از جهت‌ها را انجام دهد.
(۳) با استفاده از مدل تشخیص جهت صورت، جهت صورت او را در طول فیلم محاسبه کن. در صورتی که با دنباله‌ی تولیدشده در مرحله‌ی ۱ مطابق نبود، اعلام خطا کن و به ۱ برو. در غیر این صورت به مرحله‌ی بعد برو.
(۴) فریمی از فیلم ارسالی کاربر که خروجی مدل تشخیص روبه‌رو بودن برای آن کم‌ترین مقدار ممکن است را جدا کن. این مقدار باید حتماً از مقدار c کم‌تر باشد و در نتیجه این عکس به عنوان عکسی که از روبه‌رو گرفته شده است شناسایی شود؛ چرا که در دنباله‌ی تصادفی حتماً یک جهت روبه‌رو قرار داشته و چون فیلم ارسالی با آن دنباله تطابق داشته حتماً فریمی با مقدار کمتر از c پیدا می‌شود و در نتیجه فریم با کمترین مقدار ممکن نیز از c کمتر است.
(۵) این فریم را با تصویری که از او داریم به روش Facenet بده. اگر طبق این روش، تصاویر با هم تطابق داشتند و مربوط به یک شخص بودند، او را احراز هویت کن. در غیر این صورت خطا نشان بده.

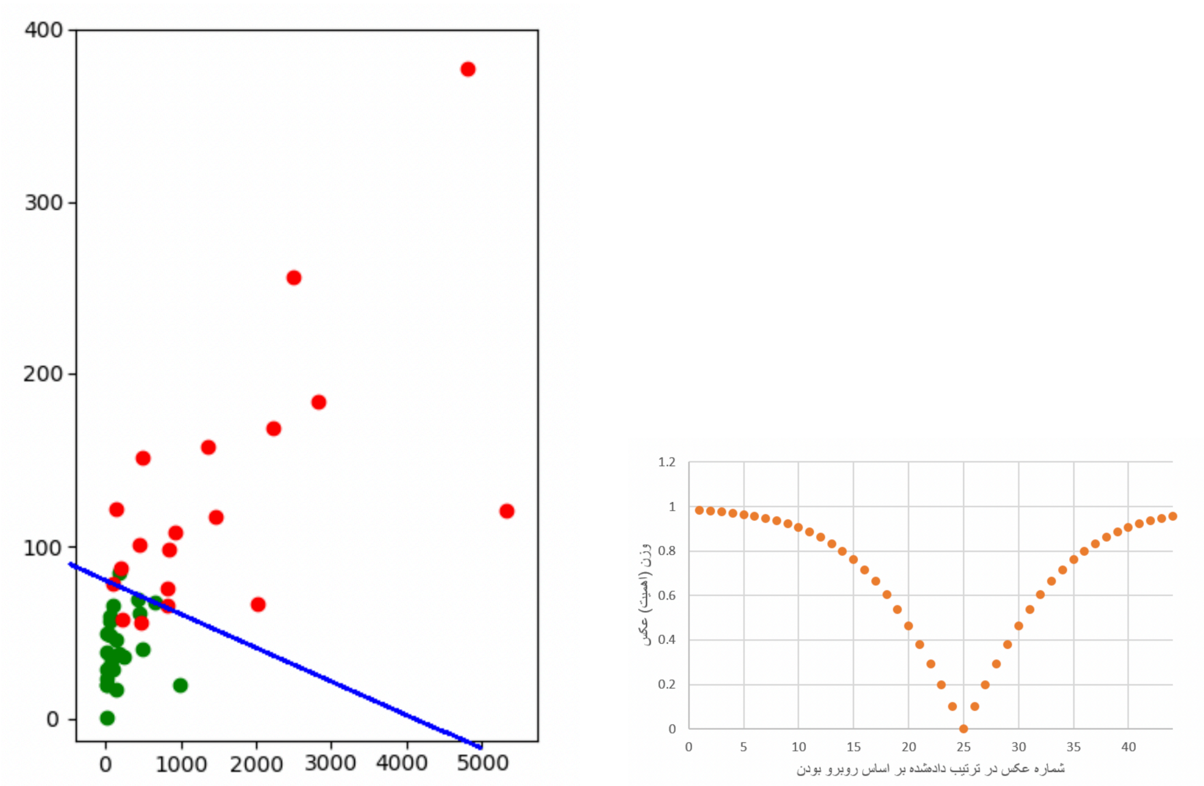
مراجع

[1] King, D. E. (2009). Dlib-ml: A machine learning toolkit. The Journal of Machine Learning Research, 10, 1755-1758.

[2] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).

[3] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE signal processing letters, 23(10), 1499-1503.

[1] weighted SVM with linear kernel



(ب) (آ)

شکل ۸: ادغام روش‌های اول و دوم تشخیص روبه‌روبودن یک تصویر. (آ) وزن‌دهی به تصاویر مرتب‌شده بر اساس میزان روبه‌روبودنشان را نشان می‌دهد. (ب) به هر یک از ۴۵ عکس به چشم یک نقطه در فضا نگاه شده که مؤلفه‌ی اول آن خروجی روش اول برای آن عکس و مؤلفه‌ی دوم خروجی روش دوم است. هم‌چنین یک نقطه سبز است در صورتی که عکس متناظر با آن از روبه‌رو باشد و در غیر این صورت قرمز است. خط آبی بهترین خطی است که نقاط قرمز و سبز را از هم جدا می‌کند و با استفاده از روش SVM به دست آمده است.

* دانشجوی دکتری علوم‌کامپیوتر، اکول پلی‌تکنیک فدرال لوزان (EPFL)
رایانامه: ahmadrahimiuni@gmail.com

گفت‌وگوی آبل ۲۰۲۱: لواس و ویگدرسون*

بیورن ایان دونداس و کریستین اف اسکائو

چکیده. جایزه‌ی آبل، شاید مهم‌ترین جایزه‌ی ریاضیات است. سال ۲۰۲۱ این جایزه به لاسولو لواس و آوی ویگدرسون تعلق گرفت، که اغلب با عنوان دانشمند علوم کامپیوتر شناخته می‌شوند. این نوشتار ترجمه‌ای است از مصاحبه‌ی آبل ۲۰۲۱.

پروفسور لواس و پروفسور ویگدرسون! نخست قصد داریم به شما به خاطر دریافت جایزه‌ی آبل در سال ۲۰۲۱ تبریک بگوییم. جا دارد که به آن‌چه کمیته‌ی آبل درباره‌ی علت اعطای این جایزه به شما گفته است، اشاره کنیم:
«برای کمک‌های اساسی آن‌ها به علوم کامپیوتر نظری و ریاضیات گسسته، و نقش راهبرانه‌ی آن‌ها در بدل‌کردن این حوزه‌ها به حوزه‌های اصلی ریاضیات نوین.»
مایل هستیم که در ابتدا از شما خواهش کنیم درباره‌ی تغییر قابل توجهی که در چند دهه‌ی اخیر در رویکرد جریان اصلی ریاضیات نسبت به ریاضیات گسسته و علوم کامپیوتر نظری رخ داده است، نظر دهید. همان‌طور که می‌دانید در سال‌هایی نه چندان دور، در میان بسیاری از ریاضیدانان تراز اول داشتن نظری بدبینانه، اگر نگوییم تحقیرآمیز، نسبت به این نوع ریاضیات کاملا رایج بود. پروفسور لواس، آیا ممکن است که شما اول شروع کنید؟

لواس: به باور من این حرف درست است. زمان زیادی طول کشید تا دو چیز در مورد علوم کامپیوتر نظری که برای ریاضیات محلی از اعراب دارد، فهمیده شود.
یکی اجمالاً این است که علوم کامپیوتر نظری منبع مسائل هیجان‌انگیز است. وقتی که من دانشگاه را تمام کردم، همراه با چند پژوهشگر جوان دیگر گروهی را برای مطالعه‌ی محاسبه و علوم کامپیوتر راه‌اندازی کردیم؛ زیرا متوجه شدیم که این حوزه -با مسائلی در مورد اینکه چه چیزهایی را می‌توان محاسبه کرد، چقدر سریع و چقدر خوب می‌توان این کار را انجام داد و امثال این‌ها- حوزه‌ی ناشناخته‌ی بزرگی است.
مطلب دوم این است که وقتی پاسخ‌دادن به سوالات فوق آغاز شد، به ویژه وقتی مفاهیم $\mathcal{P}$ و $\mathcal{NP}$، یعنی محاسبات قطعی و غیرقطعی با زمان چندجمله‌ای، به مفاهیمی محوری بدل گشتند، متوجه شدیم که به کل ریاضیات می‌توان به نحوی کاملاً متفاوت، از منظر این مفاهیم نگریست؛ از منظر محاسبات مؤثر و از منظر اثبات‌های کوتاه وجود.
برای ما جوانان این دو چیز آن قدر الهام‌بخش بود که شروع به برقراری ارتباطاتی با بقیه‌ی ریاضیات کردیم. به باور من زمان برد تا سایر حوزه‌های ریاضی نیز به اهمیت این موضوع پی ببرند، اما به تدریج این امر محقق شد. این مفاهیم در نظریه‌ی اعداد بسیار مهم بودند و در نظریه‌ی گروه‌ها نیز اهمیت یافتند، و سپس به آرامی در بسیاری از شاخه‌های دیگر ریاضیات نیز مهم شدند.

ویگدرسون: بله، کاملاً موافقم. در حقیقت، این حرف درستی است که رویکرد تحقیرآمیزی نسبت به ریاضیات گسسته در میان برخی ریاضی‌دانان وجود داشت. در مورد علوم کامپیوتر نظری چنین رویکردی شاید کم‌تر بود؛ زیرا از آن‌جا که علوم کامپیوتر نظری در آن زمان در ابتدای مسیر توسعه بود، در همان قلمرو علوم کامپیوتر مانده بود و شاید افراد آگاهی مستقیم کم‌تری از آن داشتند. من فکر می‌کنم که لواس درست می‌گوید که ایده‌ی الگوریتم‌های موثر و مفاهیم پیچیدگی محاسباتی که در علوم کامپیوتر نظری معرفی شدند، برای ریاضیات اساسی هستند و زمان برد تا این مسأله فهمیده شود.
با این حال، حقیقت آن است که ریاضی‌دانان همه‌ی اعصار از الگوریتم‌ها استفاده می‌کردند. آن‌ها به محاسبه‌کردن چیزها نیازمند بودند. چالش مشهور گاوس برای جامعه‌ی ریاضی، که

*این نوشته، ترجمه‌ای از مقاله‌ی زیر است:

Abel Interview 2021: László Lovász and Avi Wigderson, NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY, VOLUME 69, NUMBER 5

یافتن روشی سریع برای تست اول‌بودن و یافتن تجزیه‌ی یک عدد دل‌خواه است، با در نظر گرفتن زمانه‌ای که در آن نوشته شده، بسیار فصیح و گویاست. این چالش، واقعاً فراخوانی برای توسعه‌ی الگوریتم‌های سریع است.

قسمت‌هایی از ریاضیات گسسته از آن‌جا که تنها تعداد محدودی حالت هست که باید بررسی شوند، برای برخی بدیهی به نظر می‌رسید. و قاعدتاً قابل انجام است، پس مسأله چیست؟

فکر کنم مفهوم الگوریتم کارا ماهیت مسأله را روشن می‌کند. ممکن است تعداد نمایی از چیزها برای بررسی موجود باشد که شما هیچ‌وقت انجام‌شان نمی‌دهید، درست؟ اما اگر الگوریتمی سریع برای انجام آن داشته باشید، وضعیت را به‌کل تغییر می‌دهد. و به این ترتیب این سوأل که آیا چنین الگوریتمی وجود دارد مهم می‌شود.

این درکی تکامل یافته است. اولین بار پیش‌گامانی در دهه‌ی ۷۰ در شاخه ترکیبیات و ریاضیات گسسته با آن روبه‌رو شدند، زیرا که پرسش این مسأله در این شاخه‌ها بسیار طبیعی است؛ حداقل فرمول‌بندی مسائل آسان است، طوری که می‌توانید مفهوم پیچیدگی را به آن‌ها اضافه کنید. این نگاه به تدریج به سایر بخش‌های ریاضی هم گسترش یافت. نظریه‌ی اعداد یک مثال عالی است، زیرا در آن جا نیز مسائل و روش های گسسته‌ای پشت بسیاری از نتایج نظریه اعدادی معروف پنهان است. و از آن جا به تدریج به سایر شاخه‌ها گسترده شد. فکر می‌کنم اکنون اهمیت ریاضیات گسسته و علوم کامپیوتر نظری به‌طور فراگیری درک شده‌است.

تورینگ و هیلبرت

مسلماً این یک سؤال ساده لوحانه است، اما به عنوان افراد غیرمتخصص، بازداری‌های کمی داریم، و آن را مطرح می‌کنیم: چرا ایده‌ی تورینگ از آن‌چه امروز ماشین تورینگ نامیده می‌شود دربرگیرنده‌ی ایده‌ی شهودی یک رویه‌ی مؤثر است، و به اصطلاح، استانداردی را برای آن‌چه می‌توان محاسبه کرد به ما می‌دهد؟ و این چه ربطی به مسأله تصمیم هیلبرت دارد؟

ویگدرسون: فکر کنم اولین توصیه‌ام خواندن مقاله‌ی تورینگ باشد، در اصل خواندن تمام مقالات او. چرا آن‌ها را بسیار شیوا نوشته است. اگر مقاله‌ی او در مورد رویه های محاسباتی و مساله تصمیم بخوانید، همه چیز را می‌فهمید.

چندین دلیل برای چرایی بسیار پایه‌ای و اساسی بودن ماشین تورینگ وجود دارد. اولین آن این است که ساده‌است، به‌شدت ساده است، و این برای تورینگ و بسیاری دیگر در آن زمان مشهود بود. آن‌چنان ساده است که به طور مستقیم قابل پیاده‌سازی است. چنان‌چه او آغازگر انقلاب کامپیوتر بود. اگر به‌مدل های دیگر محاسبه‌پذیری که مردم مطالعه‌کردند نگاه کنیم، گودل و دیگران ـمسلماً هلیبرتـ با توابع بازگشتی و غیره. آن‌ها به این سمت که بتوانند ماشینی از رویشان بسازند کشیده نشدند. پس این اساسی بود.

و دوم آن که چند سال بعد ثابت شد تمام بیان‌های دیگر محاسبه‌پذیری کارا معادل‌اند. بنابراین ماشین تورینگ می‌توانست تمام آن‌ها را شبیه‌سازی کند. تمام آن‌ها را در خود گنجانده‌بود، اما توصیف‌اش بسیار ساده‌تر بود.

سوماً، یکی از الهام‌های تورینگ در ساخت مدل‌اش مشاهده‌ی نحوه‌ی محاسبه‌ی مسائل توسط انسان‌ها بود، مثلا ضرب دو عدد بزرگ. مشاهده‌ی این که ما روی کاغذ چه کار می‌کنیم، ما اول انتزاع می‌کنیم و سپس فرمول‌بندی می‌کنیم. و وقتی این کار را می‌کنیم، به طور خودکار به مدلی شبیه ماشین تورینگ می‌رسیم.

دلیل چهارم فراگیری آن است، در واقع مدل او یک مدل فراگیر است. در یک ماشین تنها بخشی از داده می‌تواند برنامه ای باشد که می‌خواهیم اجرا کنیم، و آن‌گاه این ماشین تنها آن را اجرا می‌کند. و به همین علت ما لپ‌تاپ، کامپیوتر و... داریم. همه‌ی آن‌ها تنها یک ماشین اند. شما به ماشین متفاوتی برای ضرب‌کردن ماشین متفاوتی برای تفریق و ماشین متفاوتی برای تشخیص اول‌بودن یک عدد نیاز ندارید. شما تنها یک ماشین دارید که می‌توان روی آن برنامه نوشت. این یک انقلاب

شگفت‌انگیز بود که همه می‌توانستند آن را بفهمند و از آن استفاده کنید، بنابراین این قدرت آن است.
شما در مورد رابطه‌ی آن با مسأله‌ی تصمیم پرسیدید. می‌دانید که هیلبرت رویایی داشت و آن رویا از دو بخش تشکیل شده بود: هر چیزی که در ریاضیات درست است قابل اثبات است، و هر چیزی که قابل اثبات است به صورت خودکار قابل محاسبه است. خب، گودل قسمت اول آن را در هم شکست، چیزهای درستی مثلاً راجع به اعداد هست که قابل اثبات نیست. چرچ و تورینگ قسمت دوم آن را در هم شکستند. آن‌ها نشان دادند چیزهای اثبات‌پذیری هستند که قابل محاسبه نیستند. اثبات تورینگ نه تنها از اثبات گودل بسیار ساده‌تر است، با استفاده از استدلال قطری هوشمندانه تورینگ، بلکه حتماً حکم گودل هم با کمی فکر از آن نتیجه می‌شود. این راه معمول که اغلب مردم برای تدریس قضیه‌ی ناتمامیت گودل در پیش می‌گیرند. مطمئن نیستم که آن‌ها با این موافق باشند؛ اما از ایده‌های تورینگ استفاده می‌کنند. این هم ارتباط بین این دو بود. البته که تورینگ از کار گودل الهام گرفته بود. در واقع تمام آن‌چه او را به سمت کار روی محاسبه‌پذیری کشاند کار گودل بود.

لواس: تنها یه چیز است که مایلم اضافه کنم. ماشین تورینگ واقعا از دو قسمت تشکیل شده است. اتوماتا و حافظه. اگر در این‌باره فکر کنید، حافظه نیاز است. هر محاسبه‌ای که انجام می‌دهید نیاز است قسمتی از نتیجه‌ی آن را به یاد داشته باشید. حافظه در ساده‌ترین حالت ممکن می‌تواند روی نواری به صورت رشته‌ای نوشته شود. یک اتوماتا ساده‌ترین چیزی است که می‌توانید تعریف کنید که قابل انجام بعضی، و در واقع هر نوعی، از محاسبات است. اگر این دو را با هم ترکیب کنیم یک ماشین تورینگ به‌دست می‌آید. که از این نظر نیز فرمی طبیعی است.

$\mathcal{P}$ **دربرابر** $\mathcal{NP}$

اکنون به موضوعی واقعاً مهم می‌رسیم، یعنی مسأله $\mathcal{P}$ در برابر $\mathcal{NP}$، یکی از مسائل جایزه هزاره. مسأله $\mathcal{P}$ در برابر $\mathcal{NP}$ چیست؟ چرا مهم ترین مسأله‌ی علوم کامپیوتر نظری است؟ اگر $\mathcal{P} = \mathcal{NP}$ باشد، چه عواقبی خواهد داشت؟ برای اثبات $\mathcal{P} \neq \mathcal{NP}$ چه ابزارهایی لازم است؟

لواس: خب، اجازه دهید دوباره به زمانی که دانشجو بودم برگردم. من با تیبور گالای [1]، که یک نظریه‌پرداز برجسته گراف و استاد من بود، صحبت کردم. او گفت: در این‌جا دو مسأله‌ی گراف‑نظری بسیار ساده وجود دارد. آیا گراف تطابق کامل دارد؛ یعنی آیا می‌توان رئوس را طوری جفت کرد که هر جفت با یک یال به هم متصل شوند؟ مورد دیگر این است که آیا گراف دور همیلتونی دارد، یعنی آیا دوری دارد که شامل تمام رأس‌هایش باشد؟
مسأله‌ی اول اساساً حل شده است. ادبیات زیادی در مورد آن وجود دارد. در مورد دیگر، ما فقط نتایج سطحی داریم، شاید نتایج غیر پیش‌پاافتاده؛ اما هنوز هم بسیار سطحی.
گالای گفت، باید در مورد آن فکر کنید، تا شاید بتوانید توضیحی ارائه دهید. متأسفانه، من نتوانستم توضیحی برای آن ارائه کنم، اما با دوستم، پیتر گاکس [2]، سعی کردیم آن را توضیح دهیم. سپس هر دوی ما برای مدتی از آن‌جا رفتیم. بورسیه های تحصیلی متفاوتی گرفتیم: گاچ برای یک سال به مسکو رفت و من برای یک سال به نشویل، تنسی. بعد که برگشتیم هر دو می‌خواستیم اول صحبت کنیم، چون هر دو در مورد نظریه $\mathcal{P}$ در برابر $\mathcal{NP}$ یاد گرفته بودیم، که این را کاملاً توضیح می‌دهد. پیتر گاچ آن را از لئونید لوین در مسکو آموخته بود و من هم آن را از گوش‌دادن به بحث‌هایی که در حاشیه‌ی کنفرانس‌ها شکل می‌گرفت.
مسأله تطابق کامل در $\mathcal{P}$ و مسأله دور همیلتونی $\mathcal{NP}$‑کامل است. این توضیح می‌داد که چه سؤال واقعا سختی بود. واضح بود که این یک موضوع محوری خواهد بود، و این با کار کارپ در اثبات کامل‌بودن بسیاری از مسائل روزمره تقویت شد. بنابراین، به طور خلاصه، مفاهیم $\mathcal{P}$ و $\mathcal{NP}$ در جایی که قبلاً هرج و مرج وجود داشت نظم ایجاد کرد. واقعا همینطور بود، خردکننده.

ویگدرسون: این واقعیت که در دنیایی که به نظر بسیار آشفته به نظر می‌رسد، نظم ایجاد می‌کند، دلیل اصلی اهمیت این مسأله است. در واقع، تقریباً یک دوگانگی است، تقریباً تمام مسائل طبیعی که می‌خواهیم حل کنیم، تا آنجا که می‌دانیم یا در $\mathcal{P}$ هستند، یا $\mathcal{NP}$‑کامل هستند. در دو مثالی که لواس آورد، اول تطابق کامل، که در $\mathcal{P}$ است، می‌توانیم آن را سریع حل کنیم، می‌توانیم آن را مشخص کنیم و خیلی کارها را انجام دهیم، واقعاً آن را خوب درک می‌کنیم. مثال دوم، مسأله دور همیلتونی نماینده یک مسأله $\mathcal{NP}$‑کامل است.

نکته اصلی در مورد $\mathcal{NP}$‑کامل بودن این است که هر مسأله‌ای در این کلاس معادل هر مسأله دیگری است. اگر یکی را حل کنید، همه آنها را حل کرده‌اید. در حال حاضر ما هزاران مسأله را که می‌خواهیم حل کنیم می‌دانیم، در منطق، در نظریه اعداد، در ترکیبات، در بهینه سازی و غیره که همگی معادل

[1]Tibor Gallai
[2]Péter Gács

هستند.

بنابراین، ما این دو کلاس را داریم که به نظر جدا از هم هستند، اینکه آیا این دو با هم برابر هستند یا نه، سوال $\mathcal{P}$ در مقابل $\mathcal{NP}$ است. و تنها چیزی که باید بدانیم پاسخ یکی از مسائل $\mathcal{NP}$ـکامل است.

اما من می‌خواهم به اهمیت این مسأله از دیدگاه بالاتری نگاه کنم. مرتبط با آن‌چه که در مورد مسائل طبیعی که می‌خواهیم محاسبه کنیم گفتم، من اغلب در سخن‌رانی های رایج استدلال می‌کنم که مسائل در $\mathcal{NP}$ مسائلی هستند که ما مردم، به ویژه ریاضی‌دانان می‌توانیم امید حل کردن آن‌ها را داشته‌باشیم، چرا که تنها مسائلی هستند که اگر آن‌ها را حل کنیم قادر به فهمیدن این‌موضوع هستیم. درست است؟ و این تنها برای ریاضی‌دانان صادق نیست. برای مثال، فیزیک‌دانان سعی نمی‌کنند مدلی برای چیزی بسازند که وقتی آن را پیدا کردند، متوجه نشوند که آن را پیدا کرده‌اند یا خیر. همین امر در مورد مهندسان با طراحی یا کارآگاهانی که راه‌حل‌هایی برای معماهای خود دارند نیز صادق است. در هر کاری که به طور جدی انجام می‌دهیم، فرض می‌کنیم که وقتی چیزی را که به دنبال‌اش بودیم پیدا می‌کنیم، می‌دانیم که آن را پیدا کرده‌ایم. که این دقیقا تعریف $\mathcal{NP}$ است: یک مسأله در $\mathcal{NP}$ است اگر قادر به چک‌کردن این باشیم که حل ارائه شده برای آن درست است.

خب، الان ما می‌دانیم $\mathcal{NP}$ چیست. اگر $\mathcal{P} = \mathcal{NP}$ ، این یعنی تمام این مسائل الگوریتمی کارا دارند، به طوری که خیلی سرعت به وسیله‌ی کامپیوتر قابل حل هستند. به عبارتی اگر $\mathcal{P} = \mathcal{NP}$ باشد تمام‌آنچه در تلاش برای انجامشان هستیم قابل انجام است. شاید یافتن درمانی برای سرطان یا حل کردن مسائل مهم دیگری، تمام این‌ها توسط یک‌الگوریتم می‌توانند سریعاً پیدا شوند. این دلیل اهمیت $\mathcal{P} = \mathcal{NP}$ است و عواقب زیادی در پی دارد. هرچند که فکر می‌کنم اغلب مردم بر این باورند که $\mathcal{P} \neq \mathcal{NP}$.

لواس: به من اجازه دهید این فکر را که چگونه ممکن است $\mathcal{P} \neq \mathcal{NP}$ را ثابت کرد اضافه کنم. این‌جا یک تناسب خوب با ساختارهایی که با خط‌کش و قطب‌نما به دست می‌آید وجود دارد. که یکی از قدیمی ترین الگوریتم‌ها است، چه چیزهایی را می‌توانید با خط‌کش و پرگار بسازید؟ یونانی‌ها مسائل مربوط به تثلیث زاویه و تضعیف مکعب توسط خط کش و پرگار را فرمول‌بندی کردند و احتمالاً معتقد بودند یا حدس می‌زدند که اینها با خط‌کش و پرگار قابل حل نیستند. اما اثبات این امر حتی امروز نیز آسان نیست. یعنی در مقطع لیسانس می‌توان آن را تدریس کرد، در یک کلاس پیشرفته مقطع کارشناسی. باید با تئوری اعداد جبری و کمی تئوری گالوا سروکار داشته باشید تا بتوانید این را ثابت کنید. بنابراین اثبات این که این مسائل با الگوریتم خاصی قابل حل نیستند، نیاز به پیشرفت عظیمی در شاخه‌ی کاملاً متفاوتی از ریاضیات داشت.

من انتظار دارم که $\mathcal{P} \neq \mathcal{NP}$ هم مشابه باشد. البته، احتمالا لازم نیست ۲۰۰۰ سال برای راه حل آن صبرکنیم. اما این نیازمند توسعه‌ي قابل توجهی در شاخه‌هایی است که ما امروز احتمالا حتی نسبت به آن‌ها آگاه هم نیستیم.

اما ما این را فرض گرفتیم که هر دوی شما معتقدید که $\mathcal{P}$ با $\mathcal{NP}$ متفاوت است.

ویگدرسون: بله، اما باید بگویم دلایلی که داریم زیاد قوی نیستند. دلیل اصلی این است که برای ریاضیدانان آشکارا خواندن اثبات قضایای کشف‌شده بسیار آسان‌تر از کشف این اثبات‌ها است. این نشان می‌دهد که$\mathcal{P}$ با $\mathcal{NP}$ متفاوت است. بسیاری از افراد با دلایل عملی تلاش کردند تا برای بسیاری از مسائل $\mathcal{NP}$ الگوریتم پیدا کنند، برای مثال انواع مسائل زمان‌بندی و مسائل بهینه‌سازی و مسائل نظریه‌ی گراف و غیره. آن‌ها شکست خوردند، این شکست‌ها احتمالاً پیشنهاد می‌دهند که چنین الگوریتم‌هایی وجود ندارد. با این حال، این یک استدلال ضعیف است.

به عبارتی، به طور شهودی حس می‌کنم $\mathcal{P} \neq \mathcal{NP}$، ولی فکر نمی‌کنم این یک استدلال قوی باشد. تنها به‌عنوان فرضی کارا به آن باور دارم.

مسائل در برابر نظریه

ما اغلب ریاضیدانان را به عنوان نظریه‌پرداز و یا به عنوان مسأله‌حل‌کن توصیف می‌کنیم. در بازه‌ی بین نظریه‌پرداز تا مسأله‌حل‌کن خود را کجا قرار می‌دهید؟

ویگدرسون: اول از همه، من عاشق حل مسأله هستم. اما بعد از خودم می‌پرسم: اوه، این روش حل‌اش کرد، اما شاید این تکنیکی باشد که بتوان در جاهای دیگر نیز به کار برد؟ سپس سعی می‌کنم آن را در جاهای دیگر اعمال کنم و سپس آن را به کلی‌ترین شکل‌اش می‌نویسم و اینگونه ارائه می‌کنم. به این ترتیب ممکن است من را یک نظریه‌پرداز نیز بخوانند. من نمی‌دانم. من نمی‌خواهم خودم را در قالب نظریه‌ساز یا مسأله‌حل‌کن توصیف کنم.

من از انجام هر دو کار، یافتن راه حل برای مسأله و تلاش برای درک این که چگونه آن‌ها در جاهای دیگر کاربرد دارند، لذت می‌برم. من عاشق درک ارتباط بین مسائل مختلف و

حتی بیش‌تر بین شاخه‌های مختلف هستم. من فکر می‌کنم ما در علوم کامپیوتر نظری خوش‌شانس هستیم که بسیاری از شاخه‌های به ظاهر پراکنده بسیار نزدیک به هم مرتبط هستند، اما دیدن این ارتباط همیشه واضح نیست، مانند ارتباط بین سختی و تصادفی‌بودن . نظریه از چنین پیوندهایی ساخته شده است.

لواس: من احساسات مشابهی دارم. من دوست دارم مسأله حل کنم. من با الهام از پال اردوش شروع کردم که واقعاً همیشه سؤالات را به سوال‌های کوچک‌تری تقسیم می‌کرد. فکر می‌کنم که این نقطه قوت خاصی از ریاضیات او بود، اینکه او می‌توانست مسائل ساده‌ای را فرموله کند که در واقع یک نظریه‌ی زیربنایی را آشکار کرد. یادم نیست چه کسی این را در مورد او گفته است: خوب است نظریات کلی را بدانیم که در ذهن او وجود دارد، آن‌ها را به این مشکلات تقسیم می‌کند که تا بتوانیم آنها را حل کنیم. و در واقع، بر اساس مسئله‌های او، شاخه‌های کاملاً جدیدی پدید آمد، نظریه‌ی گراف بحرانی، نظریه‌ی گراف تصادفی، ترکیبات احتمالی به طور کلی، و شاخه‌های مختلف نظریه اعداد. بنابراین من به عنوان یک مسأله‌حل‌کن شروع کردم، اما همیشه دوست داشتم ارتباط برقرار کنم، و سعی کردم از یک مسأله خاص که حل کرده بودم، چیزی کلی‌تر بسازم.

لم موضعی لواس (Lovasz Local Lemma)

پروفسور لواس، شما چند مقاله ـ فکر کنیم در مجموع شش مقاله ـ با استادتان، پال اردوش منتشر کرده‌اید. حدس می‌زنیم که پاسخ این سوال را که کدام یک از بین‌شان محبوب‌ترین شماست را می‌دانیم، اگر اشتباه می‌کنیم ما را اصلاح کنید. نسخه‌ی ضعیفی از قضیه‌ای مهم که به‌اصطلاح لم موضعی لواس نامیده می‌شود، در مقاله‌ی مشترکی با اردوش در سال ۱۹۷۵، مقاله‌ی موردنظر ماست. سال ۲۰۲۰ رابین موزر [1] و گابور تاردوس [2] جایزه‌ی گودل را برای ارائه نسخه الگوریتمی لم موضعی لواس دریافت کردند، که شاهدی بر اهمیت بالای آن است. ممکن است به ما بگویید که لم موضعی لواس درباره‌ی چیست؟

لواس : بله، سعی‌ام را می‌کنم. تقریباً همه چیز در ریاضیات، یا حداقل در ریاضیات گسسته به این صورت قابل فرمول‌بندی است: تعدادی اتفاق بد وجود دارند، و شما می‌خواهید از رخ‌دادن هر یک از آن‌ها اجتناب کنید. ابتدایی‌ترین‌شان این است که مجموع احتمال وقوع تمامی آن‌ها کمتر از یک باشد، در این صورت می‌توان با احتمال مثبتی از وقوع تمامی‌شان اجتناب کرد. این یکی از پایه‌ای‌ترین ترفندها در استفاده‌ی احتمال در ریاضیات گسسته است. حال فرض کنید که که تعدادشان بسیار بزرگ باشد، به طوری که مجموع احتمال وقوع آن‌ها عددی بزرگ شود. چگونه از پس این شرایط بر می‌آیید؟ یک مثال خاص دیگر حالتی است که این اتفاقات مستقل از هم باشند. در این صورت اگر به طور جداگانه بتوانید از رخ‌دادن هر یک از آن‌ها با احتمال مثبتی اجتناب کنید، با احتمال مثبتی می‌توانید از رخ‌دادن تمامی‌شان نیز اجتناب کنید، به راحتی ضرب احتمال‌های اجتناب از تک‌تک آن‌ها را بگیرید. لم موضعی به نحوی ترکیب این دو ایده است. اگر پیش‌آمدها مستقل نباشند، ولی هر یک از آن‌ها تنها به تعداد کمی از بقیه وابسته باشد و اگر جمع احتمالات این تعداد کم، کم‌تر از یک باشد ـنه جمع تمامی آن‌ها، تنها آن‌هایی که به آن وابسته است‌ـ آن‌گاه شما هنوز هم می‌توانید با احتمال مثبتی از رخ‌دادن تمامی پیش‌آمدهای بد جلوگیری کنید.

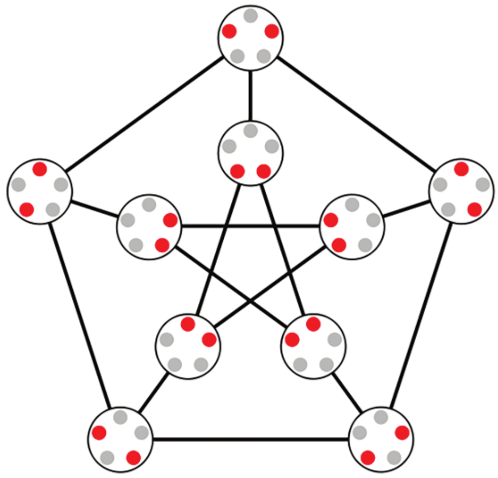
این را هم اضافه کنم، من روی سوالی از اردوش فکر می‌کردم که در نهایت به این لم رسیدم. آن زمان در یک مدرسه‌ی تابستانی در ایالت اوهایو همراه اردوش بودم؛ که ما مسأله را حل کردیم، و یک مقاله‌ی طولانی در مورد آن مسأله و مسائل مرتبط نوشتیم، از جمله این لم. اردوش متوجه شد که این لم بیش از یک لم برای این مورد خاص بود. با این حال او می‌خواست که لم با نام من شناخته شود. در حالی که به طور معمول باید لم موضعی اردوش‌ـلواس نام می‌گرفت. چرا که در یک مقاله مشترک ظاهر شد. اما او همیشه جوانان را تبلیغ می‌کرد و همیشه می‌خواست مطمئن شود که چنان‌چه آن‌ها مسأله مهمی را ثابت کردند، این موضوع معلوم باشد. و من از سخاوت‌اش بهره بردم.

حدس نسر

سال ۱۹۵۵ نسر حدسی را در مورد تعداد رنگ‌های لازم برای رنگ‌آمیزی رده‌ی طبیعی از گراف‌ها، که اکنون با نام گراف‌های نسر شناخته می‌شوند، مطرح کرد. سال ۱۹۷۸ شما، پروفسور لواس، این حدس را با کدگذاری مسأله به‌عنوان یک مسأله روی فضاهای با بعد بالا، ثابت کردید. که در آن از ابزارهای استاندارد در نظریه‌ی هوموتوپی استفاده کردید و به این ترتیب موجب ترقی شاخه‌ی توپولوژی ترکیبیاتی شدید. چگونه چنین رویکردی به ذهن‌تان رسید؟ آیا ممکن است کمی

[1] Robin Moser
[2] Gábor Tardos

در مورد مسأله و راه‌حل‌تان بگویید؟



لواس : این پرسش به‌یکی از مسائل سخت بر می‌گردد، مسأله عدد رنگی: به چند رنگ نیاز دارید تا یک گراف را به درستی رنگ‌آمیزی کنید؟ در این جا درستی به این معنی است که رئوس همسایه باید رنگ‌های متفاوتی داشته باشند، که در حالت کلی یک مسأله سخت است، یک مسأله کامل- است. اولین رویکرد نگاه به ساختار موضعی است. اگر یک گراف رئوس زیادی داشته باشد که به یک‌دیگر وصل باشند، واضحاً به رنگ‌های زیادی نیز نیاز دارید. سوال این است: آیا همیشه چنین استدلالی بر اساس خاصیت‌های موضعی وجود دارد؟ این نکته‌ای دانسته شده بود، که گراف‌هایی وجود دارند که ساختار موضعی‌ای ندارند، پس هیچ دور کوتاهی نیز ندارند. اما برای رنگ‌آمیزی آن‌ها به تعداد رنگ‌های زیادی نیاز است. ساختن چنین گراف‌هایی یک مسأله‌ی جذاب بود. برای مثال، گراف‌هایی که مثلث یا به طور کلی‌تر، دورهای به طول فرد ندارند. یک ساخت شناخته‌شده برای چنین گرافی با مشاهده‌ی کره است و وصل هر دو نقطه‌ای که تقریباً متضاد قطبی‌اند. قضیه‌ی بورساک-اولام [1] می‌گوید، برای آن که نقاط تقریباً متضاد قطبی رنگ‌های متفاوتی داشته باشند، تعداد رنگ‌های مورد نیاز شما بیشتر از بعد فضاست. این یک طریقه‌ی ساخت آن‌ها بود، یک راه دیگر این است که راس‌های ما زیر مجموعه‌های k عضوی از مجموعه‌ای n عضوی باشد به طوری که $2k < n$

و دو رأس را به هم متصل می‌کنیم اگر از یک‌دیگر مجزا باشند. حدس نسر راجع به عدد رنگی چنین گرافی است. این مسأله‌ای جذاب بود که در بوداپست از آن صحبت می‌شد. سیمونویتز [2] دوست و همکارم بود که من را متوجه ساخت که این دو مسأله واقعاً شبیه یک‌دیگرند، یا این‌که این دو ساختار می‌توانند شبیه هم باشند. در نهایت من تقلیلی از یکی از این دو مسأله به دیگری پیدا کردم؛ اما معلوم شد که این تقلیل در واقع جامع‌تر از این مسأله است و حد پایینی برای هر گرافی بر اساس ساختارهای توپولوژیک ارائه می‌دهد. این‌گونه بود که توپولوژی وارد شد، و واقعا زمان زیادی کشید تا بتوانم آن را عملی کنم. تا جایی که به یاد دارم تقریباً دو سال برای عملی‌کردن این ایده صرف کردم تا در نهایت کار کرد.

اثبات‌های دانش‌صفر

پروفسور ویگدرسون، در اوایل زندگی حرفه‌ای خود، کمک‌هایی اساسی به مفهوم جدیدی در رمزنگاری، یعنی اثبات دانش صفر داشتید، که بیش از ۳۰ سال بعد اکنون به عنوان مثال در فناوری زنجیره‌ی‌بلوکی [3] استفاده می‌شود. لطفاً به ما بگویید که اثبات دانش صفر چیست و چرا این مفهوم در رمزنگاری بسیار سودمند است؟

ویگدرسون: به عنوان یک ریاضی‌دان، فرض کنید که اثبات چیزی مهم مانند حدس ریمان را پیدا کردید و می‌خواهید همکاران خود را متقاعد کنید که این اثبات را پیدا کردید؛ اما نمی‌خواهید قبل از شما آن را منتشر کنند. شما فقط می‌خواهید آنها را متقاعد کنید. با این واقعیت که شما دلیلی برای این قضیه دارید و نه چیز دیگری. مضحک به نظر می‌رسد، کاملاً مضحک به نظر می‌رسد، و این برخلاف تمام شهود ما است که راهی برای متقاعدکردن کسی وجود دارد، در مورد چیزی که باور ندارد و بدون دادن اطلاعات جدیدی به او.

الگوریتم LLL

پروفسور لواس، ما می‌خواهیم در مورد الگوریم LLL صحبت کنیم، الگوریتمی که کاربردهای چشم‌گیری دارد. به عنوان مثال، ادعا شده‌است که تنها سیستم‌های رمزی که می‌توانند در برابر حمله‌ی یک کامپیوتر کوانتومی مقاومت کنند از LLL استفاده می‌کنند. این الگوریتم در مقاله‌ی مشترک شما با برادران لنسترا [4] در مورد تجزیه‌ی چندجمله‌ای‌ها ظاهر می‌شود، که کمویش مسیر مورد انتظاری را طی می کند، کاهش به پیمانه‌ی اعداد اول و سپس استفاده از لم هنسل [5] . ولی با

[1] Borsuk–Ulam
[2] Miklós Simonovits
[3] blockchain
[4] Lenstra
[5] Hensel

آن‌چه که ما می‌فهمیم، نقطه‌ی عطف کار شما و برادران لنسترا این بود که توانستید ترفیع [۱] را به وسیله‌ی الگوریتمی که تقریبی از کوچک‌ترین بردار مشبکه [۲] را می‌داد، در زمان چندجمله‌ای انجام دهید. به ما بگویید همکاری با این برادران لنسترا چگونه بود؟

لواس : این یک داستان جالب در مورد ریاضیات و نقش زیبایی، یا حداقل ظرافت، در ریاضیات است. همراه مارتین گروتشل [۳] و الکساندر شریور [۴] مشغول کار بر روی کاربردهای روش بیضی [۵] در بهینه‌سازی ترکیبیاتی بودیم. ما به یک قضیه کلی رسیدیم که هم‌ارزی‌ای را بین جداسازی و بهینه‌سازی بیان می‌کرد. در واقع، این‌ها تحت قیود اضافی ملایمی [۶] مسائل معادل زمان چندجمله‌ای بودند. اما موردی وجود داشت که الگوریتم روی آن کار نمی کرد. و آن زمانی بود که جسم محدب [۷] روی یک زیر فضای خطی با ابعاد پایین‌تر بود. همیشه راهی برای دورزدن این موارد بود؛ گاهی اوقات با متدهای ریاضیاتی، برای مثال ترفیع به ابعاد بالاتر. اما همیشه بعضی از ترفندها دخیل می‌شدند که ما می‌خواستیم از آن‌ها اجتناب کنیم.

یک جا من متوجه شدم که اگر موفق به حل الگوریتمی بعضی سوالات واقعا قدیمی ریاضی شویم، ما می‌توانیم این مشکل را حل کنیم .

و آن کاری از دیریکله [۸] بود، که بیان می‌کرد چند عدد حقیقی می‌توانند به صورت همزمان با با اعداد گویای با مخرج یکسان تخمین زده شوند. سوال این بود که آیا می‌توان این سوال را به صورت الگوریتمی حل کرد. می‌توانید به سراغ راه حل آن بروید و متوجه شوید دقیقا خلاف یک راه حل الگوریتمی است؛ چرا که براساس اصل لانه کبوتری است، و تنها وجود چنین تقریبی را نشان می‌دهد. در نهایت بعد از چند بار آزمون و خطا، به الگوریتمی که واقعا تقریب با اعداد گویای با مخرج مشترک را در زمانی چندجمله‌ای انجام داد دست یافتم.

کمی پیش از این، سخن‌رانی‌ای از هنری لنسترا می‌شنیدم که در مورد مسأله‌هایی مشابه بود، اما بر اساس مشبکه‌ها، و کاهش پایه در مشبکه‌ها. الان دیگر آسان بود که مسأله دیریکله را به مسأله کوچک‌ترین بردار مشبکه تقلیل داد. این را به آن‌ها نوشتم، و سرانجام معلوم شد که اگر من بتوانم سوال دیریکله را حل کنم، آن‌ها می‌توانند تجزیه‌ی چندجمله‌ای‌ها را در زمان چندجمله‌ای حل کنند.

این واقعاً حیرت‌انگیز بود. چنان‌چه این فکر در نظر درست می‌آمد که تجزیه‌ی یک عدد آسان‌تر از تجزیه‌ی یک چندجمله‌ای است. اما دقیقا برعکس، چندجمله‌ای‌ها را می‌توان در زمان چندجمله‌ای تجزیه کرد. به این ترتیب بود که مقاله مشترک ما منتشر شد. چند سال بعد لاگاریس [۹] و اودلیزکو [۱۰] این را یافتند که الگوریتم برای شکستن سیستم رمز کوله‌پشتی [۱۱] قابل استفاده است. از آن به بعد، از آن برای ارزیابی سیستم‌های مختلف رمزنگاری بسیاری استفاده شد.

خب، این طور که ما متوجه شدیم کاربردهای آن فراتر از چیزی بود که انتظار داشتید.

بله، البته. برای مثال کمی بعد از چاپ آن، اندرو اودلیزکو و هرمان ته رایلی [۱۲] با انجام محاسبات عددی زیادی توسط این الگوریتم، توانستند حدس مرتنز [۱۳] درباره‌ی تابع زتای ریمان [۱۴] در نظریه‌ی اعداد را رد کنند. اما نکته‌ای که من می‌خواستم روی آن تاکید کنم این بود که گاهی وقت‌ها همه چیز از چیزی شروع می‌شود که ظاهراً اهمیتی ندارد. گروتشل، شروِیر و من تنها می‌خواستیم به زیباترین قضیه‌ی ممکن در مورد معادل بودن بهینه‌سازی و جداسازی برسیم. هرچند که این انگیزه‌ای شد برای اثبات چیزی که بعدها اهمیت فراوانی یافت.

روش بیضی

البته. سال ۱۹۸۱ شما و هم‌کاران‌تان گروشتل و شریور مقاله‌ای با عنوان «روش بیضی و تاثیر آن بر بهینه‌سازی ترکیبیاتی» چاپ کردید. مقاله‌ای که بسیار ارجاع داده شده است و در پاسخ قبلی هم به آن اشاره کردید. تاریخچه‌ای برای این مقاله وجود دارد، و آن هم مقاله‌ی یک روسی به نام

[1] lift
[2] Lattice
[3] Martin Grötschel
[4] Alexander Schrijver
[5] ellipsoid method
[6] mild additional conditions
[7] convex body
[8] Dirichlet
[9] Lagarias
[10] Odlyzko
[11] knapsack crypto system
[12] Herman te Riele
[13] Mertens
[14] Riemann zeta function
[1] Khachiyan

خاچیان [1] است، که حاوی نتایجی تاثیرگذار است. اگر ممکن است در این مورد نظرتان را به ما بگویید. و این‌که چگونه مقاله‌ی شما به این‌مقاله ربط پیدا می کند؟

لواس: خاچیان اولین الگوریتم با زمان چندجمله‌ای را برای برنامه‌ریزی خطی ارائه کرد که امروز به آن روش بیضی می‌گویند. این را هم ذکر کنم که آن زمان چند نفر دیگر هم در جماهیر شوروی بر روی این مسأله کار می‌کردند؛ اما او بود که جزئیات لازم را ثابت کرد. به این ترتیب خاچیان کسی بود که ثابت کرد برنامه‌ریزی خطی در زمان چندجمله‌ای قابل‌حل است.

مسلماً، این موضوع همه را علاقه‌مند کرد. قبل از آن در نظریه‌ی الگوریتم‌ها، مسائل اسرارآمیزی وجود داشتند که در عمل به‌صورت کارا حل می‌شدند. با این‌وجود هیچ الگوریتمی با زمان چندجمله‌ای برای آن‌ها شناخته نشده بود. بنابراین ما هم به آن علاقه‌مند شدیم و متوجه شدیم در روش خاچیان نیاز به توصیف صریحی از مسأله برنامه‌ریزی خطی نیست. تنها کافی است مسأله برنامه‌ریزی خطی به این صورت داده شود که بتوان در مورد هر نقطه‌ای به شدنی‌بودن [2] آن نقطه جواب داد، و هم‌چنین اگر جواب منفی بود بتوان فهمید که کدام قیود نقض شده‌اند. این مشاهده توسط چند نفر دیگر، شامل کارپ [3] و پاپادیمیتریو [4] و فکر می‌کنم پادبرگ [5] و رائو [6] انجام شد. ما متوجه شدیم در بهینه‌سازی ترکیبیاتی موقعیت‌های بسیار دیگری مانند این وجود دارد.

بعدتر با مارتین گروتشل دیدار کردم. او راهی پیدا کرده‌بود که بتوان این روش‌ها را بر روی مسأله‌ی قدیمی دیگری پیاده کرد. به این ترتیب که او الگوریتمی ارائه داد که در زمان چندجمله‌ای قادر به یافتن عدد رنگی گراف تام [7] در زمان چندجمله‌ای بود، که یکی دیگر از مسائل حل‌نشده آن روزها بود و این را آشکار ساخت که لازم است روش بیضی را نه تنها در بهینه‌سازی خطی، بلکه در رده‌ی وسیع‌تر بهینه‌سازی محدب پیاده کرد. ما همراه لکس شریور، که به مدت یک سال در دانشگاه سگد [8] بود و دفتر مشترکی داشتیم، بر روی این موضوع کار کردیم و شروع کردیم به دیدن آن‌چه در بهینه‌سازی محدب جریان داشت و چگونگی به کاربردن این روش در آن حوزه. این راهی بود که ما برای رسیدن به آن‌چه قبل‌تر اشاره کردم طی کردیم؛ یعنی معادل بودن جداسازی و بهینه‌سازی. این به نوعی اصلی‌ترین خروجی مطالعه‌ی ما بود. در نهایت هم کتابی را در مورد این موضوع نوشتیم.

ضرب زیگ-زاگی

گراف‌های بالنده یک موضوع پرتکرار برای جایزه آبل بوده است. سال گذشته ما مارگولیس [9] را داشتیم که اولین گراف‌های بالنده صریح را پس از اثبات وجود آن‌ها توسط پینسکر [10] ساخت. گروموف، که در سال ۲۰۰۹ برنده‌ی جایزه‌ی آبل شد، از بالنده‌ها بر روی گراف‌های کیلی بر روی گروه های بنیادی استفاده کرد که با مطالعه‌ی حدس باوم-کُن [11] مرتبط بودند. همچنین زمردی که در سال ۲۰۱۲ برنده‌ی جایزه آبل شد، از گراف‌های بالنده استفاده کرد. در سال ۲۰۰۰، شما، پروفسور ویگدرسون، همراه با رینگلد و وادان، حاصل ضرب زیگ-زاگ گراف‌های منتظم را ارائه کردید، که تا آن‌جایی که ما متوجه شدیم، مشابه ضرب نیم‌مستقیم [12] در نظریه‌ی گروه است و توسط آن ساختارهای صریحی از گراف‌های بالنده‌های خیلی بزرگ و ساده ارائه کردید. آیا می‌توانیم با این سؤال شروع کنیم: زیگ چیست و زاگ چیست؟

ویگدرسون: خب، شاید باید با این شروع کنم که گراف بالنده چیست؟ باید به شبکه‌ها فکر کنید، یکی از ویژگی های مطلوب شبکه‌ها این است که نوعی تحمل خطا در آن‌ها وجود دارد. اگر برخی از ارتباطات قطع شود، شما هم‌چنان هم می‌توانید ارتباط برقرار کنید. این می‌تواند شبکه های کامپیوتری باشد، یا می‌تواند شبکه‌هایی از جاده‌ها باشد که دوست دارید به شدت به هم متصل باشند. البته که نمی خواهید هزینه زیادی بپردازید، بنابراین دوست دارید این شبکه‌ها تُنک باشند؛ یعنی نمی‌خواهید اتصالات زیادی داشته باشید. شما یک گراف بزرگ می‌خواهید که در آن درجه هر رأس - یعنی تعداد اتصالات به هر راس- کوچک باشد، یا بگوییم ثابت باشد، مثلاً ده.
یک گراف تصادفی این ویژگی را خواهد داشت، و کل سوال

[2] feasible
[3] Karp
[4] Papadimitriou
[5] Padberg
[6] Rao
[7] perfect
[8] Szeged
[9] Margulis
[10] Pinsker
[11] Baum–Connes
[12] semidirect

تبدیل به این می‌شود–این همان چیزی است که پینسکر متوجه شد–: آیا می‌توانید چنین گراف‌هایی را توصیف کنید و آن‌ها را به طور موثر پیدا کنید؟ مارگولیس اولین ساخت را با استفاده از این مفهوم عمیق جبری، یعنی ویژگی کژدان [1] (T) ارائه کرد. با استفاده از نتایج سلبرگ و دیگران نیز می‌توانند ساخته شوند. سپس مردم شروع به ساده‌سازی برهان کردند. تا آن زمان که من داشتم این مطالب را آموزش می‌دادم، شواهد نسبتاً ساده‌ای وجود داشت، مانند آن‌چه توسط جیمبو [2] و ماروکا [3] ارائه شد، و شما می‌توانید آن را در یک یا دو ساعت در کلاس تدریس کنید. این فقط اساساً تبدیل فوریه در گروه‌های متناهی است. بنابراین شما هر چیزی را که می‌خواهید دارید، ساختار صریح بسیار زیبایی دارید، حتی می‌توانید آن را در کلاس به دانشجویان ثابت کنید؛ اما برای من، مانند بسیاری از اثبات‌های مبتنی بر جبر، بسیار مرموز بود. یعنی چه خبر بود؟ واقعاً چه چیزی پشت این واقعیت است که این‌ها گراف‌های بسیار متصل هستند؟ سال‌ها این نوعی وسواس برای من بود و نمی‌دانستم با آن چه کنم.

سال ۲۰۰۰، درست پس از این که به آی‌ای‌اس نقل مکان کردم، دو دانشجوی پسادکترا در آن‌جا داشتم، سالیل وادان و عمر رینگلد. ما روی یک پروژه‌ی کاملاً متفاوت در مورد اشیای شبه‌تصادفی کار می‌کردیم، که با یک مفهوم مهم، مفهوم استخراج‌کننده، ارتباط دارد. استخراج‌کننده نوعاً تصادفی‌بودن را برای ما خالص می‌کند. من اکنون در مورد آن صحبت نمی‌کنم؛ اما ما در تلاش بودیم تا استخراج‌کننده‌های بهتری بسازیم. همان طور که ما این کار را انجام می‌دادیم، متوجه شدیم که یکی از ساختارهای ما ممکن است برای ساختن بالنده‌ها مفید باشد. ساختارها در استخراج‌کننده اغلب تکراری بودند و ماهیت‌هایی با ساختار جبری داشتند. هنگامی که متوجه این موضوع شدیم، فهمیدیم که ساختار ترکیبی کاملاً متفاوتی از بالنده‌ها داریم، و حتی بیش‌تر از آن، ساختاری که در آن –برای من– علت بالندگی مشخص بود.

این نتیجه زیگ–زاگ است. نام زیگ–زاگ در واقع توسط پیتر وینکلر پیشنهاد شد. ساخت‌وساز با یک گراف کوچک شروع می‌شود که در حال بسط است، و یکی از آن برای تقویت یک گراف دیگر استفاده می‌کند تا یک بالنده باشد. بنابراین شما این گراف کوچک را به نحوی وصل می‌کنید، و یک بالنده بزرگ‌تر می‌گیرید، سپس این کار را تکرار می‌کنید تا بالنده بزرگ‌تر به دست آورید، و به همین ترتیب. بنابراین می‌توانید بالنده‌های بزرگ دل‌خواه تولید کنید. اگر به این ساخت‌وساز موضعی نگاه کنید، تصویری زیگ–زاگ را در خود دارد، اما این نکته مهمی نیست.

روش دیگری برای توصیف بالنده‌ها وجود دارد که من فکر می‌کنم شهودی‌تر است. بالنده گرافی است که، فارغ از آن که چه توزیعی روی رئوس دارید، اگر یک راس از این توزیع بگیرید و از این راس به یک همسایه تصادفی بروید، آنتروپی توزیع افزایش می‌یابد. این روش دیگری برای توصیف بالنده‌ها است و این را تقریباً با چشمان خود در ساختار زیگ–زاگ می‌بینید. شما می‌بینید که چگونه آنتروپی رشد می‌کند و این چیزی است که من در این نوع نگاه به آن دوست دارم.

برای اینکه تصویری از آنچه در حال وقوع است به دست آورید: تا آن جا که ما می‌دانیم شما گرافی دارید و گرافی دیگر را جای تمام رئوس قرار می‌دهید. سپس باید تصمیم بگیرید که چگونه یال‌ها را در آن قرار دهید. اساساً کاری که انجام می‌دهید، کمی در یکی از رئوس حرکت می‌کنید و سپس به رأس بعدی می‌پرید؛ درست مانند وضعیت حاصل‌ضرب نیم‌مستقیم که در آن قانون ضرب دارید. بعد پرش مشابهی را در آنجا انجام می‌دهید. آیا این درست است؟

کاملاً درست است، و علاوه بر این، ارتباط با ضرب نیم‌مستقیم چیزی بود که دو یا سه سال بعد همراه الکساندر لوبوتسکی و نوگا الون متوجه‌اش شدیم. این یک جور چالشی بود که من در اوایل احساس کردم؛ یعنی گراف‌هایی که به دست آوردیم بالنده بودند. آن‌ها به صورت ترکیبی تولید می‌شدند. ما آنها را درک می‌کردیم و در این فکر بودم که آیا ساخت ما می‌تواند برای ساختن گراف‌های کیلی مفید باشد یا نه. سپس با نوگا الون و الکساندر لوبوتسکی متوجه شدیم که فقط مشابه نیست، بلکه ضرب زیگ–زاگ یک تعمیم ترکیبی از ضرب نیم‌مستقیم گروه‌ها است که در گراف‌های کیلی اعمال می‌شود. این کلی‌تر است که در مورد گراف‌های کیلی می‌شود همان ضرب نیم‌مستقیم. به عنوان مثال، به همین دلیل شما می‌توانید ثابت کنید که گراف‌های کیلی، از گروه‌هایی که ساده نیستند، می‌توانند با تعداد ثابتی از مولدها بسط یابند. هیچ روش جبری‌ای برای ارائه این نتیجه شناخته‌شده نیست.

این به طور گسترده در بسیاری از موقعیت‌ها استفاده شده است، و یکی از مواردی که باید به آن اشاره کرد این است: همان طور که رینگولد سال ۲۰۰۴ نشان داد، فضای لگاریتمی متقارن و فضای لگاریتمی یکسان هستند. به نظر می‌رسد این

[1] Kazhdan

[2] Jimbo

[3] Maruoka

ایده‌ای است که واقعاً مورد توجه قرار گرفته است. آیا هنوز خودتان از آن استفاده می کنید، یا اجازه داده‌اید «کودک» شما بزرگ شود و وارد جامعه ریاضی شود؟

ویگدرسون: فکر می‌کنم خیلی خوب است که ما یک جامعه‌ی ریاضی داریم. بسیاری از ایده‌های ما به مکان‌هایی فراتر از تصور من رفته‌اند. چیزی اساسی در مورد این ساختار وجود دارد، و همانطور که گفتید، این ابزار در نتیجه رینگولد استفاده شد که می‌توان آن را ساده‌تر به عنوان الگوریتم فضای لگاریتمی برای هم‌بندی در گراف‌ها توصیف کرد. در واقع، این به یک نتیجه از لواس و همکارانش برمی‌گردد و می‌تواند به عنوان نتیجه‌ای در شاخه‌ی تصادفی‌بودن در نظر گرفته شود.
لواز با کارپ و دیگران در سال ۱۹۸۰ نشان داد که اگر می‌خواهید بررسی کنید که آیا یک گراف بزرگ هم‌بند است، ولی حافظه‌ای ندارید، کافی است این را به یاد داشته باشید که کجا هستید، سپس با پرتاب سکه می‌توانید کل گراف را کاوش کنید. این الگوریتم حافظه‌ی لگاریتمی تصادفی برای بررسی هم‌بندی گراف است. غیرتصادفی کردن این الگوریتم یکی دیگر از پروژه‌های من بود که هرگز نتوانستم آن را انجام دهم، اما رینگلد مشاهده کرد که اگر ضرب زیگ-زاگ را بگیرید و آن را بسیار هوشمندانه در الگوریتم تصادفی آنها اعمال کنید، الگوریتم با حافظه‌ی لگاریتمی قطعی برای همان مسأله را دریافت خواهید کرد. بنابراین این یک مولد شبه‌تصادفی خاص است که برای این طراحی شده است. همچنین در قضیه جدید PCP ایریت دینور [1] استفاده شد. بنابراین، بله، یک چیز کلی در این ضرب زیگ-زاگ وجود دارد که دیگران آن را سودمند می‌دانند.

تاثیر مشترک

خب، این ما را به جای جالبی در این مصاحبه می‌برد، زیرا ما شاهد ارتباط بین کارهای شما دو نفر هستیم.

ویگدرسون: بگذارید یکی از تاثیرگذارترین اتفاقاتی را که در سال‌های پسادکتری برای من رخ داده است تعریف کنم. سال ۱۹۸۵ بود که من در برکلی دانشجوی پسادکترا بودم و کارگاهی در اورگان در جریان بود که در آن لواس ارائه داد. اسم‌اش را دقیقاً به خاطر نمی آورم، اما سخن‌رانی‌هایی درباره بهینه‌سازی، هندسه‌ی اعداد و غیره وجود داشت. یک هفته کامل سخن‌رانی بود و همه می‌خواستند صحبت‌های لواس را بشنوند. همه هم از واضح‌بودن ارائه‌اش استقبال کردند.
اما مهم‌ترین چیزی که من از این ارائه‌ها گرفتم چگونگی توصیف خود او بود وقتی سؤالی درباره الگوریتم و رابطه‌ی آن با کار روی بیضی و غیره پرسیدید. او بر این تاکید کرد که چگونه یک دید سطح بالا، به جای تمرکز بر یک مسأله خاص، می‌تواند بسیاری از ساخه‌های بسیار مهم ریاضیات را به هم مرتبط کند. لواس برای ما توضیح داد که چگونه یک سوال کمی عجیب -یعنی در مورد داشتن یک راه حل ظریف‌تر برای یک مسأله در بهینه‌سازی- منجر به حل مسأله‌ی کاهش پایه‌ی مشبکه شد، و چگونه به تقریب دیوفانتین مرتبط شد، و همین طور چگونه به رمزنگاری ربط پیدا کرد: هم برای شکستن سیستم‌های رمز و هم برای ساختن آن‌ها. می‌دانید، شما این نمای پانوراما را دریافت می‌کردید که در آن همه‌چیز با همه‌چیز هماهنگ است. من به شدت تحت تأثیر این موضوع قرار گرفتم، این یک رویداد شگفت‌انگیز و به‌یادماندنی در اوایل کار من بود.
لواس: فکر کنم من هم خاطرات مشابهی داشته باشم. اثبات دانش صفر موضوعی شوکه‌کننده و هیجان‌انگیز بود که من در موردش آموختم و به نوعی، عظمت قدرت ایده‌های جدید در رمزنگاری و -کلی‌تر- علوم کامپیوتر را نشان‌ام داد. من همیشه به کارهای ویگدرسون روی تصادفی‌بودن علاقه‌مند بودم، و حتی بعضی وقت‌ها تلاش می‌کردم که جهت مخالف آن را طی کنم و مثال‌هایی را پیدا کنم که تصادفی‌بودن واقعاً کمک کند.
کسی ممکن است این را بیان کند که بعضی وقت‌ها تنها مسأله نوع مدل است، مدل محاسباتی ما. من به نتایجی در مورد بهینه‌سازی محدب، هندسه محدب، و نتایج الگوریتمی روی تحدب بعدهای بالا اشاره کردم. این یک مسأله‌ی پایه‌ای است که اگر جسم محدبی داشته باشیم، چگونه حجم آن را محاسبه کنیم. یکی از دانشجویان دکترای من در آن زمان، جورج الکس [2] ، به راه حل زیبایی رسید که نشان می‌داد که شما به زمانی نمایی نیاز دارید که این حجم را تخمین بزنید، حتی اگر ضریب کارایی [3] ثابت باشد. این در مدل ما بود، معادل بودن مسأله بهینه‌سازی و جداسازی جسم‌های محدب با یک اوراکل جداسازنده. چند سال بعد -و این در واقع چیزی بود که ویگدرسون گفت- دایر [4] ، فریز [5] و کنون [6] الگوریتمی تصادفی ارائه دادند که در زمان چندجمله‌ای حجم را با خطای نسبی کمی محاسبه می‌کرد.

[1] Irit Dinur
[2] György Elekes
[3] factor
[4] Dyer
[5] Frieze
[6] Kannan

نکته‌ی جالب وابستگی آن به بعد بود، اگر بعد n بود آن‌گاه الگوریتم $n^{۲۹}$ گام داشت. به‌وضوح این عدد برای داشتن کاربرد بسیار بزرگ بود. اما این جریان تحقیقات آن‌ها را شروع کرد. من هم بخشی از آن بودم و واقعاً این نتیجه را دوست داشتم. بسیار علاقه‌مند بودم که آن را بهینه‌تر کنم و بفهمم که چرا توان آن تا این اندازه بزرگ است. به این ترتیب توان آن به زیبایی از ۲۹ به ۱۷ و بعد به ۱۰ و به ۷ به ۵ و به ۴ کاهش یافت و تا مدت زیادی روی ۴ باقی ماند؛ اما سال پیش به ۳ رسید. بنابراین الان به داشتن کاربرد نزدیک است. هرچند که هنوز کاربردی نیست، چرا که مکعب n همچنان عدد بزرگی است، اما قطعا دیگر به صورت خنده‌داری دور از مسیر کاربرد نیست. دو نکته در مورد این مثال. اولاً، به خاطر این که مدل محاسباتی متفاوتی است، قابل اثبات است که تصادفی‌بودن کمک می‌کند. قابل اثبات است که بدون تصادفی‌بودن، زمان نمایی مورد نیاز است؛ اما با وجود تصادفی‌بودن به زمان چندجمله‌ای کاهش پیدا می‌کند و با تصادفی‌بودن حتی به زمان چندجمله‌ای مطلوبی نیز می‌رسد. دوم این که زمان چندجمله‌ای نشان‌گر آن است که مسأله ساختار عمیقی دارد. شما این ساختار عمیق را کاوش می‌کنید و سرانجام این زمان‌چندجمله‌ای را به آن‌چه مطلوب باشد بهبود می‌دهید.

گرافون‌ها

این جا سوالی برای شما هست، پروفسور لواس. درباره‌ی موضوعی که شما بزرگ‌ترین سهم را در آن ایفا کرده‌اید: نظریه‌ی حد گراف‌ها چیست و چه فایده‌ای دارد؟ همچنین توضیح بدهید که گرافون چیست.

لواس: سعی‌ام را می‌کنم که بیش از حد تخصصی نباشد. یک گراف اغلب به وسیله ماتریس مجاورت آن داده می‌شود، که می‌توان به صورت ماتریس ۰ و ۱ تصورش کرد. حال تصور کنید که گراف بزرگ و بزرگ‌تر شود، به این ترتیب دنباله‌ای از ماتریس‌ها داریم که همیشه می‌توان به آن‌ها به چشم تابع‌هایی روی مربع واحد فکر کرد که به مربع‌های کوچکتری‌تقسیم شدند و هر کدام حاوی صفر یا یک هستند. به این ترتیب این تابع‌ها با تعریفی می‌توانند به تابعی روی مربع واحد میل کنند، که ممکن است پیوسته باشد، یا حداقل دیگر گسسته نباشد: این همان گرافون است. چنان‌چه، برای مثال، گراف تصادفی باشد، به این ترتیب هر یک از این مربع‌ها به تصادف صفر یا یک‌اند. به این ترتیب به مربعی طوسی‌رنگ میل می‌کند که با گرافون یک‌دوم معادل است. بنابراین یک گرافون تابعی است روی مربع واحد، که اندازه‌پذیر و متقارن است و شما می‌توانید دقیقا همگرایی یک دنباله از گراف‌ها را به یک گرافون تعریف کنید. اکنون ما بسیاری از خواص گراف‌ها را حفظ کردیم، اگر تمام گراف‌های دنباله ویژگی مشخصی را داشته باشند، آن‌گاه حد آن‌ها نیز این ویژگی را دارد. برای مثال، اگر تمام گراف‌ها فاصله‌ی طیفی خوبی داشته باشند ـویژگی‌ای که گراف‌های بالنده دارندـ آن‌گاه حد آن‌ها نیز فاصله طیفی خوبی دارد. این جا ما گراف‌های چگال را در نظر می‌گیریم. اکنون فضای متشکل از گرافون‌ها را نگاه کنید. باید ثابت کنید ـجزییات فنی زیادی در آن استـ که فضای گرافون‌ها، با یک متر مناسب، یک فضای فشرده است که کار کردن با آن بسیار راحت است؛ چرا که، برای مثال، از این به بعد می‌توانید یک پارامتر گراف را بگیرید، مثلاً چگالی مثلث‌ها. معنای چگالی مثلث‌ها در گرافون حدی قابل تعریف است. آن‌گاه در این گرافون‌های حدی، گرافونی هست که این پارامتر را با وجود قیود دیگری کمینه می‌کند.

به این ترتیب بازی‌های معمولی که در آنالیز قابل انجام بود، مانند مطالعه‌ی کمینه و کمینه‌ساز و تشخیص این که کمینه موضعی است یا سراسری، این جا نیز وجود دارد. به این ترتیب کارهایی که در آنالیز قابل انجام بود، اینجا نیز می‌توانید انجام‌شان دهید و هم‌چنین آن‌ها را به زبان نظریه‌ی گراف‌ها ترجمه کنید.

قابل اشاره است که لم منظمی [1] از زمردی [2] عمیقا به توپولوژی گرافون‌ها مرتبط است. برای مثال، فشردگی فضای گرافون‌ها نوع قوی‌ای از لم منظمی را القا می‌کند.

ظرفیت شنون

پروفسور لواس، سال ۱۹۷۹ شما مقاله‌ای با عنوان «درمورد ظرفیت شنون یک گراف» منتشر کردید که به طور گسترده‌ای ارجاع داده شده است. در این مقاله شما ظرفیت شنون پنج‌گون را با معرفی ابزارهای عمیق ریاضیاتی تعیین کردید و ثابت کردید عددی، که اکنون با نام عدد لواس شناخته می‌شود، وجود دارد که در زمان چندجمله‌ای قابل محاسبه است. و حد بالایی برای ظرفیت شنون مربوط به یک گراف است. می‌توانید دراین‌باره بیش‌تر به ما بگویید و شرح دهید که ظرفیت شنون چیست؟

لواس: تعریف صوری از این که ظرفیت شنون چیست ارائه نمی‌دهم، با این‌حال شما الفبایی دارید و می‌خواهید پیام‌هایی بفرستید که متشکل از حروف این الفبا باشد. بعضی از این

[1] Regularity Lemma

[2] Szemerédi

حروف وقتی به گیرنده می‌رسند ممکن است با حروف دیگری اشتباه گرفته شوند. شما می‌خواهید بزرگترین مجموعه از کلماتی را پیدا کنید که بعد از ارسال، خطر به‌اشتباه گرفته‌شدن با کلمات دیگر را نداشته باشند. پس برای هر دو کلمه‌ای باید جایگاهی وجود داشته باشد که حرف نظری‌شان قابل اشتباه گرفته‌شدن با یک‌دیگر نباشند. الفبا را با رئوس گرافی نشان دهیم و بین هر دو حرفی که قابل اشتباه‌گرفتن با یک‌دیگر هستند یالی در نظر می‌گیریم. شنون این مدل را ارائه داد و مفهوم ظرفیت را تعریف کرد. اگر شما بخواهید کلماتی طولانی را با طول مشخصی بفرستید، حداکثر قادر به ارسال چه تعداد کلماتی هستید که در نهایت با یک‌دیگر اشتباه گرفته نشوند؟ این عدد به صورت نمایی رشد می‌کند و مبنای آن ظرفیت شنون است.

گراف پنج‌گون اولین مثالی بود که ظرفیت شنون آن معلوم نبود. من تکنیکی را که نمایش عمودی [1] نامیده شد معرفی کردم که قادرم می‌ساخت به این سوال پاسخ دهم.

این مثالی بود از چیزهایی که به طور معمول وقتی به سوالی پاسخ می‌دهید به وجود می‌آیند و سرانجام زندگی مستقل خودشان را شروع می‌کنند. برای مثال، از آن برای تعیین عدد رنگی گراف‌های تام استفاده شد. حتی در جهتی بسیار متفاوت، به تازگی عده‌ای فیزیک‌دان کاربردهای جذابی از آن را در فیزیک کوانتومی یافتند. این‌که می‌شنوی کاری که انجام دادی الهام‌بخش کارهای واقعاً جذابی توسط دیگران شده، بسیار خوش‌آیند است.

لم اردوش–فابر–لواس

آخرین سوال ریاضیاتی ما از شما، پروفسور لواس، در مورد حدسی اردوش–فابر–لواس است، حدسی که سال ۱۹۷۲ ارائه شد. چه‌گونه این حدس را زدید، و تصور اولیه‌ی شما از میزان سختی اثبات آن چه طور بود؟ همین اواخر این حدس توسط کانگ، کلی، کون، متوکو و اوستوس ثابت شد. این را هم اضافه کنیم که ظاهراً اردوش این مسأله را به عنوان سه مسأله ترکیبیاتی موردعلاقه‌اش در نظر می‌گرفت.

لواس: پس‌زمینه این مسأله این چنین بود که سال ۱۹۷۲ ما در دانشگاه ایالتی اهایو با یک‌دیگر دیدار کردیم و در مورد نظریه‌ی ابرگراف‌ها بحث کردیم که آغاز ظهور یک شاخه‌ی جدید بود. ایده چنین بود که به جای داشتن یک گراف استاندارد، که هر یال آن دو سر داشت، می‌توان ساختاری را در نظر گرفت که هر یال‌اش سه رأس، یا پنج راس، و یا به همین ترتیب رأس‌های بیشتری داشته‌باشد، به آن‌ها ابرگراف می‌گفتند، و پرسش این بود: سوال‌هایی را که در نظریه گراف وجود داشت ـمانند عدد رنگی، هم‌بندی و غیره- چگونه می‌توان به ابرگراف‌ها تعمیم داد؟

یکی از این سوأل‌ها چیزی بود که در نظریه‌ی گراف، عدد رنگی یالی نامیده می‌شود. نوعی معروف از سوال عدد رنگی است، که در آن به جای رنگ‌آمیزی رئوس، یال‌ها را رنگ می‌کنید و می‌خواهیم دو یالی که رأس مشترک دارند هم‌رنگ نباشند. و خب همین سوال را می‌توان در مورد ابرگراف‌ها پرسید و حد بالایی برای تعداد رنگ‌های مورد نیاز داد. ما این مشاهده را در تمامی مثال‌هایی که بررسی کردیم داشتیم، که تعداد رئوس همیشه کران‌بالایی برای تعداد رنگ‌های مورد نیاز برای رنگ‌آمیزی یالی ابرگراف‌ها بود.

چند هفته بعد از این دیدار در ایالت اهایو، من همراه اردوش مشغول بازدید از دانشگاه کولاردو [2] در بولدر [3] بودم. که فابر [4] مهمانی‌ای برپا کرد و ما آن‌جا شروع به صحبت از ریاضیات کردیم ـکاری که معمولا ریاضی‌دان‌ها در یک مهمانی می‌کنند- و در نهایت به این مسأله رسیدیم.

اردوش خیلی باور نداشت که این درست باشد. من خوش‌بین‌تر بودم و فکر می‌کردم احتمالاً درست است. واقعاً حدس زیبایی بود که بیان کرد تعداد رئوس کران‌بالایی برای تعداد رنگ‌های لازم است. ما بعداً فهمیدم که این‌حدس موردهای غیربدیهی هم دارد، مانند آنچه نامساوی فیشر [5] در نظریه‌ی طرح‌های بلوکی نامیده می‌شود. این همان جایی بود که ما را در اثبات مسأله گیر انداخت. حدس معروف و معروف‌تر شد. سوالی که بسیار مقدماتی بود و به راحتی بیان می‌شد؛ اما هیچ‌کسی نتوانسته بود به چنگ‌اش آورد. در نهایت جف کاهن [6] حدود ده سال و اندی پیش توانست با اضافه کردن فاکتور $1 + \epsilon$ برای هر ϵ مثبتی دلخواهی مساله را ثابت کند.

یک سال پیش دانیلا کوهن [7] و دانشجویان‌اش توانستند اثبات‌اش کنند؛ حداقل برای nهای به اندازه کافی بزرگ. یکی از ویژگی‌های این حدس این بود که شما آن را براساس nهای کوچک بیان کردید؛ ولی در نهایت برای nهای خیلی بزرگ قادر به اثبات‌اش شدید و بازه‌ی میان این دو علامت سوال باقی ماند. چند ماه پیش او از اثبات‌اش در کنگره‌ی اروپا ارائه‌ای

[1] Orthogonal representation
[2] University of Colorado
[3] Boulder
[4] Faber
[5] Fisher
[6] Jeff Kahn
[7] Daniela Kühn

داد، که بسیار قانع‌کننده بود. پس دیگر آن را اثبات‌شده می‌دانم.

اثبات‌های تعاملی کوانتومی

در ژانویه ۲۰۲۰، پنج نفر به نام‌های جی، ناتاراجان، ویدیک، رایت و یوئن اعلام کردند که نتیجه‌ای را در نظریه پیچیدگی کوانتومی به اثبات رسانده‌اند که حاکی از پاسخ منفی به مسأله نشاندن کُن [1] در نظریه‌ی جبر عمل‌گرهاست. این برای بسیاری از مردم شگفت‌انگیز بود -از جمله ما دو نفر- زیرا تا حدودی با مسأله کُن آشنا هستیم. مسأله‌ای که اثبات آن در طول بیش از چهل سال گذشته در برابر تمام تلاش‌ها مقاومت کرده بود. این که مسأله‌ای که به نظر می‌رسد هیچ ارتباطی با نظریه پیچیدگی کوانتومی ندارد، باید راه حل‌اش را در این شاخه پیدا کند، برای ما شگفت‌آور است. پروفسور ویگدرسون، آیا نظری دارید؟

ویگدرسون: از زمانی که این نتیجه منتشر شد، سعی کردم سخن‌رانی‌های رایجی در مورد تکامل شاخه‌ی خاصی که به این نتیجه مرتبط است، یعنی اثبات‌های تعاملی، به‌ویژه مطالعه اثبات‌های تعاملی کوانتومی ارائه کنم. همچنین چگونگی ارتباط‌اش به نتیجه‌ی $MIP^* = RE$ و هم‌چنین به سؤالات خاصی مانند مسأله نشاندن کُن و مسأله تسیرلسون [2] در نظریه‌ی اطلاعات کوانتومی. البته، هر نتیجه‌ی خاصی ممکن است تعجب‌آور باشد؛ اما من اصلاً از این ارتباط تعجب نمی‌کنم. در حال حاضر ما جاهای زیادی در سراسر ریاضیات داریم که در آن ایده‌هایی از علوم کامپیوتر نظری، الگوریتم‌ها و البته ریاضیات گسسته وجود دارند و قدرت خود را آشکار می‌کنند. از نظر ارتباط به جبر عمل‌گرها -خاصه جبر فون نویمن- به دلیل اندازه‌گیری‌های کوانتومی که شامل کاربرد عمل‌گرها می‌شود، آنقدر که به نظر می‌رسد مرموز نیست. این سوال که آیا این عمل‌گرها جابه‌جا می‌شوند، هم از نظر تئوری اطلاعات کوانتومی و هم از نظر درک قدرت اثبات‌های تعاملی کوانتومی اساسی است. من بیش‌تر بر این دلیل متمرکز بودم که احتمالاً می‌توان یک اثبات در حیطه‌ی اثبات های تعاملی کوانتومی به دست آورد و نه در نظریه‌ی کلاسیک اطلاعات کوانتومی.
اگر به فرمول‌بندی اثبات‌های تعاملی کوانتومی -به ویژه اثبات‌های MIP^* یکی از چندین اثبات‌کننده- نگاه کنید و آنها را با مقاله ، آزمایش معروف اینشتین-پودولسکی-روزن گدانکن که مکانیک کوانتومی را آزمایش می‌کند، مقایسه کنید، تصویر یکسانی را می‌بینید. شما در آن جا یک اثبات تعاملی با دو اثبات‌کننده را می‌بینید که در برهان‌های تعاملی کوانتومی نظری مشاهده می‌کنید. اگر به تاریخچه‌ی مطالعه‌ی چنین آزمایش‌ها یا اثبات‌هایی نگاه کنید، در دنیای فیزیک تمرکز بر روی انواع خاصی از مسائل بود. چندین مورد معروف مانند نابرابری‌های بل وجود دارد. در حالی که برای افرادی که اثبات‌های تعاملی کوانتومی را مطالعه می‌کنند بسیار طبیعی است که آن‌ها را به عنوان یک مجموعه مطالعه کنند. مجموعه‌ای از بازی‌ها وجود دارد، که برخی از بازی‌ها قابل تقلیل به یکدیگرند، و اثبات این که $MIP^* = RE$ مجموعه‌ای بی‌نظیر از نتایج تقلیل‌ها و توسعه‌هاست که از ترفندهای نظریه کدینگ کوانتومی و غیره مختلفی استفاده می‌کند، حتی از تکنیک‌های . این روش نظریه‌ی پیچیدگی برای نگاه‌کردن به چیزها درک بهتری از نحوه رفتار آنها به عنوان یک کل ایجاد می‌کند، و من فکر می‌کنم که منبع قدرت این رویکرد است و کاربردها فقط از نتیجه‌ی نهایی ناشی می‌شوند؛ زیرا اشیاء مورد مطالعه عمل‌گرهایی در فضای هیلبرت هستند.

ابرقهرمانان ل.ل و آ.و

موجب خرسندی ماست که برخی از کره‌ای‌های جوان نیز دریافتند که شما قهرمانان ریاضی هستید. دو پسر شما استادراهنمای دکتری مشترکی -یعقوب فاکس [3] - در استنفورد دارند، و این توسط یک مجله علمی محبوب کره جنوبی که مخاطبان جوان‌تری را هدف گرفته، مورد توجه قرار گرفت، جایی که شما و پسران‌تان به عنوان شخصیت‌های مختلف جنگ ستارگان به تصویر کشیده شدید. به عنوان دانشمندان برجسته، آیا احساس راحتی می‌کنید که قهرمان‌های واقعی با شمشیرهای نوری باشید؟

[1] Connes' embedding
[2] Tsirelson
[3] Jacob Fox

لواس: من همیشه یک جوک خوب را دوست دارم، فکر می‌کنم این کارتون عالی بود.
ویگدرسون: من هم آن را دوست داشتم، و فکر می‌کنم این نشان می‌دهد که همیشه می‌توان انتظار خلاقیت بیش‌تری در جذب مخاطبان جوان‌تر به ریاضیات داشت، با روش‌هایی که قبلاً انتظارش را نداشتید.

آیا علم تحت فشار است؟

سوالی که مایل‌ایم بپرسیم ربطی به ریاضیات ندارد: آیا شما علم را تحت فشار می‌بینید؟ و آیا این چیزی است که ریاضی‌دانان می‌توانند و باید درگیر آن شوند؟

لواس: فکر کنم درست است، علم تحت فشار است. این گونه که من می‌بینم، یک علت ساده‌ی آن این است که علم به‌سرعت درحال رشد است، و مردم کم‌تر و کم‌تر آنچه در هر شاخه‌ی خاصی می‌گذرد را می‌فهمند، و این ترسناک است؛ چرا که آن را یک بیگانه می‌کند. حتی تشخیص بین آن‌چه باید باور کرد و نکرد سخت‌تر می‌شود، و همین‌طور تمییز بین علم و شبه‌علم. این یک معضل واقعی است. فکر کنم باید در مورد این که در دبیرستان‌ها به دانش‌آموزان چه بیاموزیم باید کاملاً از نو بیندیشیم. الان، ریاضیات شاخه‌ای است که آموزش‌اش آن جایی نیست که می‌توانست باشد. حدس می‌زنم ۹۰ درصد مردمی که ملاقات می‌کنم این را می‌گویند: من همیشه از ریاضیات متنفر بودم.
فکر می‌کنم ما کارمان را در آموزش ریاضی خوب انجام ندادیم. من این را با وجود این می‌گویم که بهترین دوستان‌ام مشغول کار روی بهبود آموزش ریاضی‌اند. خیلی از آدم‌ها تشخیص دادند که مشکلی آن جا هست؛ اما حرکت روبه‌جلو در آن بسیار سخت است. من تخصص کمتری راجع به رشته‌های دیگر دارم، اما از بیرون که نگاه کنم این را می‌بینم که بیولوژی امروز با بیولوژی‌ای که من در مدرسه خواندم چقدر متفاوت است. این واضح است که این وظیفه عظیم در برابر جامعه‌ی علمی قرار دارد.
ریاضیات باید نقشی مرکزی را بازی کند؛ چرا که طی زمان علوم از ریاضیات بیش‌تر و بیش‌تری استفاده می‌کنند، و نه تنها آمار، که به‌گونه‌ای ابزار استاندارد شمرده می‌شود. برای مثال تئوری شبکه، و یا البته آنالیز و معادلات دیفرانسیل، و فیزیک کوانتوم، که واقعا ریاضیات هم هست، چنان‌چه می‌توان گفت این علم شاخه‌ی پیچیده‌ی جبر چندخطی است. فکر کنم مسأله برقرار است و ما باید در این‌باره کاری کنیم.
از طرف انجمن ریاضی نروژ و انجمن ریاضی اروپا و ما دو نفر از شما به خاطر این مصاحبه‌ی بسیار جالب تشکر می کنیم و باز هم به خاطر دریافت جایزه آبل تبریک می گوییم!
ویگدرسون: خیلی‌ممنون!
لواس: خیلی‌ممنون!

مترجم: محمد زارع[†]

[†]دانشجوی کارشناسی ارشد علوم کامپیوتر، دانشگاه صنعتی شریف

مکاتبات فرگه و راسل*

ترجمه‌ی ساجد طیبی
sadjad.tayebi@gmail.com

چکیده. در این مقاله ۲ نامه‌ی ابتدایی از ۲۰ نامه‌ی فرگه و راسل ترجمه شده است. ابتدائاً مقدمه‌ی ویراستار کتاب، Brian McGuinness، بر بخش راسل-فرگه را می‌خوانیم. در شماره‌های بعدی مجله به باقی نامه‌ها خواهیم پرداخت.

۱. مقدمه‌ی ویراستار

برتراند راسل (۱۸۷۲-۱۹۷۰) از ۱۹۰۲ تا ۱۹۱۲ با فرگه مکاتبه داشت، گرچه بیشتر مکاتبات مربوط‌اند به سال‌های ۴-۱۹۰۲. مکاتبات با اعلام آن چه امروزه به‌عنوان پارادوکس راسل شناخته می‌شود توسط راسل آغاز می‌شوند، و بیشتر آنها ناظر اند بر راه‌حل‌های مختلفی که راسل برای پارادوکس پیش می‌نهد و فرگه آن‌ها را رد می‌کند. اما در آن‌ها به اغلب مفاهیم محوری فلسفه‌ی زبان فرگه نیز پرداخته می‌شود: مفاد و مرجع، شیء و مفهوم، صدق و کذب، جمله و رده. راسل زمانی پارادوکس را کشف کرد که مهم‌ترین اثر فرگه در شرف اتمام بود: در آستانه‌ی انتشار جلد II قوانین پایه‌ای‌اش. آثار اصلی راسل هنوز منتشر نشده بود: او در زمان این کشف به آماده‌سازی اصول ریاضیات برای انتشار مشغول بود. تمام نامه‌های راسل به فرگه به زبان آلمانی نوشته شده‌اند. دست‌کم یک نامه که در سال ۱۹۱۲ نوشته شده است امروز مفقود شده. نامه‌ی اول راسل (نامه ۱ در ادامه) و جواب مشهور فرگه به آن (نامه ۲) پیش از این به انگلیسی منتشر شده‌اند. ر.ک. به

Jean van Heijnoort (ed.) (1967) *From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931*. Cambridge. Mass. 1967.

از میان تمام نامه‌های فرگه به راسل، تنها اصلِ نامه‌ی آخر (نامه بیستم) باقی مانده است. راسل، بر این اساس که آن را کاملاً شخصی می‌دانسته، آن را پیش خودش نگاه داشته بوده است. باقی نامه‌ها برای شولز[1] فرستاده شده بودند و اکنون تنها فتوکپی آن‌ها در اختیار است.

۲. نامه‌ی اول: راسل به فرگه

فرایدز هیل
هسلمر
۱۹۰۲/۰۶/۱۶

همکار عزیز،
یک سال و نیم است که با قوانین پایه‌ای حساب شما آشنا هستم؛ اما اکنون بالاخره توانستم فرصتی را که قصد داشتم صرف مطالعه کامل آثارتان کنم به دست آورم. در تمام نکات اصلی با شما کاملاً موافقم، علی‌الخصوص در مورد ردیّه شما بر هر گونه عنصر روان‌شناختی در منطق، و اهمیتی که قائل‌اید برای نمادگذاری مفهومی در مبانی حساب و مبانی منطق، که البته به دشواری قابل تمییزند. در امور متعددی درباره جزئیات، در آثار شما به مباحث، تمایزها، و تعریف‌هایی برمی‌خورم که جست‌وجوی

*این نوشته ترجمه‌ی بخشی از کتاب زیر است:

Frege, G. (1980) *Philosophical and Mathemtical Correspondence of Gottlob Frege*. University of Chicago Press.

[1] H. Scholz

آن‌ها در آثار دیگر منطق‌دانان بی‌فایده است. مشخصاً راجع به توابع (بخش ۹ از مفهوم‌نگاشت شما) مستقلاً به نظرات مشابهی حتی در جزئیات رسیده‌ام. تنها در یک مورد به مشکل برخوردم. شما می‌گویید (ص. ۱۷) که تابع نیز می‌تواند چونان عنصری نامتعین عمل کند. این چیزی است که در گذشته به آن باور داشتم، اما در حال حاضر به دلیل این تناقض برایم محل تردید است: فرض کنید w محمولِ محمولی غیرقابل حمل بر خود بودن باشد. آیا w می‌تواند بر خودش حمل شود؟ از هر پاسخی نقیض آن نتیجه می‌شود. بنابراین، باید نتیجه بگیریم که w محمول نیست. به همین ترتیب، هیچ رده‌ای (به‌مثابه یک کل) وجود ندارد که شامل رده‌هایی باشد که، به مثابه یک کل، عضوی از خودشان نیستند. از این نتیجه می‌گیرم که در شرایطی خاص مجموعه‌ای تعریف‌پذیر تشکیل یک کل نمی‌دهد.

من در حال تکمیل کتابی درباره اصول ریاضیات‌ام و مایل‌ام در آن مفصلاً راجع به آثار شما بحث کنم. کتاب‌هایتان را یا دارم یا به زودی تهیه خواهم کرد؛ اما بسیار سپاس‌گزار می‌شوم اگر رونوشت مقالات‌تان در نشریات مختلف را برایم ارسال کنید. با این حال، اگر این کار مقدور نباشد، آن‌ها را از کتاب‌خانه‌ای به دست خواهم آورد.

هنوز تا بررسی دقیق منطق در حوزه پرسش‌های اساسی‌ای که نمادها برایشان بسنده نیست راه درازی باقی مانده است. در دوره حاضر آثار شما بهترین موردی است که می‌شناسم، و به این دلیل است که به خود اجازه دادم احترام عمیق‌ام را به شما اظهار کنم. بسیار مایه‌ی تأسف است که مجال انتشار جلد دوم قوانین پایه‌ای خود را نیافته‌اید؛ با این حال، امیدوارم این اتفاق روزی رخ دهد.

با احترام،
برتراند راسل

تناقض فوق را با نمادهای پئانو چنین می‌توان بیان کرد:

$$w = cls \cap x \ni (x \sim \varepsilon x) \cdot \supset : w \varepsilon w \cdot = \cdot w \sim \varepsilon w.$$[۱]

۳. نامه‌ی دوم: راسل به فرگه

ینا
۱۹۰۲/۰۶/۲۲

همکار عزیز،
بابتِ نامه‌ی جالب توجه مورخ ۱۶ ژوئن ۱۹۰۲ سپاس‌گزارم. از این که درباره‌ی بسیاری نکات با من موافق اید و از این که قصد دارید مفصلاً راجع به کار من بحث کنید خوشحال‌ام. به درخواست شما رونوشت‌های این مقالات را ارسال می‌کنم:

(۱) «توضیحات انتقادی ...»[۲]
(۲) «در باب نمادگذاری پئانو ...»[۳]
(۳) «در باب مفهوم و شیء»[۴]
(۴) «در باب مفاد و مرجع»[۵]
(۵) «در باب نظریه‌های صوری حساب»[۶]

پاکتی خالی دریافت کرده‌ام که به نظر آدرس آن به خط شماست. گمان می‌کنم قصد داشته‌اید چیزی را برایم بفرستید، اما تصادفاً مفقود شده است. اگر چنین است، از لطف‌تان ممنونم. رویه‌ی پاکت را برایتان ارسال می‌کنم.

[۱] این فرمول می‌گوید که اگر w رده‌ی xهایی باشد که $x \notin x$، آن‌گاه $w \in w \leftrightarrow w \notin w$.
[2] (1895) A Critical Elucidation of some Points in E. Schroeder's *Algebra der Logik'*, in *Translations from the philosophical writings of G. Frege*, 2nd ed. (Oxford I960), pp. 86-106.
[3] (1897) On Herr Peano's Begriffsschrift and My Own, in *Australian Journal of Philosophy* XLVII (1969), pp. 1-14.
[4] (1892) On Concept and Object, as for 1, pp. 42-55.
[5] (1892) On Sense and Reference, as for 1, pp. 56-78.
[6] (1886) On Formal Theories of Arithmetic, in *On the Foundations of Geometry and Formal Theories of Arithmetic* (London and New Haven 1971), pp.141-153.

اکنون که مفهوم‌نگاشت را دوباره می‌خوانم، می‌بینم که راجع به برخی نکات تغییر عقیده داده‌ام، کمااین‌که اگر خودتان آن را با قوانین پایه‌ای حساب مقایسه کنید متوجه خواهید شد. لطفاً در ص. ۷ مفهوم‌نگاشت پاراگرافی را که با «ما به همین سادگی» شروع می‌شود حذف کنید، چرا که نادرست است. مع‌ذلک، این خطا هیچ تالی فاسدی برای بقیه محتوای کتاب من ندارد.[۱]

تناقضی که کشف کرده‌اید چنان مرا شگفت‌زده کرده است که قابل بیان نیست، و مایل‌ام بگویم که بهت‌زده‌ام کرده است، چرا که بنیادی را که در پی بنای حساب بر آن بودم به لرزه درآورده است. فلذا به نظر می‌رسد که تبدیل عمومیتِ یک این‌همانی به این‌همانیِ گستره‌های مقادیر (بخش ۹ قوانین پایه‌ای من) همواره مجاز نیست، و این که قانون V من (بخش ۲۰، ص. ۳۶) نادرست است، و این که توضیح من در بخش ۳۱ برای به دست دادن مرجعی برای ترکیب نشانه‌ها، در همه موارد کفایت نمی‌کند. باید تأمل بیشتری در این باره بکنم. موضوع حتی جدی‌تر است، چرا که به نظر می‌رسد فروپاشی اصل V من نه تنها مبانی من برای حساب، بلکه تنها مبانی ممکن برای حساب را ویران می‌کند. و مع‌ذلک فکر می‌کنم باید بتوان قیودی بر تبدیل عمومیتِ یک این‌همانی به این‌همانیِ گستره‌های مقادیر وضع کرد بی آن که بخش‌های اساسی برهان‌های من متأثر شوند. با این حال، کشف شما، گرچه در نگاه اول ممکن است ناخوش‌آیند به نظر برسد، کشفی چشم‌گیر است که چه بسا به پیش‌رفتی عظیم در منطق بیانجامد.

در ضمن به نظرم عبارت «محمولی بر خودش حمل می‌شود» دقیق نیست. یک محمول علی‌القاعده تابعی مرتبه اول است و این تابع نیازمند یک شیء به عنوان آرگومان است و لذا آرگومان (موضوع)اش نمی‌تواند خودش باشد. بنابراین من ترجیح می‌دهم بگویم: «یک مفهوم بر مصداق خودش حمل می‌شود»؛ اگر تابع $\Phi(\xi)$ یک مفهوم باشد، من با «$\acute{\varepsilon}\Phi(\varepsilon)$» به مصداق (یا رده‌ی متناظر) آن اشاره می‌کنم (گرچه البته اکنون راجع به توجیه این موضوع تردید دارم). بنابراین «$\Phi(\acute{\varepsilon}\Phi(\varepsilon))$» یا «$\acute{\varepsilon}\Phi(\varepsilon) \cap \acute{\varepsilon}\Phi(\varepsilon)$» حمل مفهوم $\Phi(\xi)$ است بر مصداق خودش.

جلد دوم قوانین پایه‌ای به زودی منتشر خواهد شد. لازم است ضمیمه‌ای به آن اضافه کنم که در آن به کشف شما چنان که در خور آن است بپردازم. خود اگر دریابم نحوه درست پرداختن به آن چیست!

با احترام،
گ. فرگه

[۱] این اشتباه در نخستین جمله این پاراگراف است، جایی که فرگه توضیح می‌دهد که فرمول «موردی را که در آن B تصدیق شده است، ولی A و Γ انکار شده‌اند انکار می‌کند» (مفهوم‌نگاشت، بخش. ۵، ص. ۷). ارنست شرودر (Ernst Schröder) نیز پیش از آن در ص. ۸۸ از نقدش بر مفهوم‌نگاشت در Zeitschrift für Mathematik und Physik 25(1880), pp. 81-94. این اشتباه را متذکر شده بود. شرودر این حدس معقول را مطرح می‌کند که فرگه در تبدیل یک عبارت به نمادگذاری مفهومی‌اش که باید به

$$non(non(B\,et\,non A))\,et\,non\Gamma$$

ختم می‌شد، سهواً نشانه نقیض دوم را از قلم انداخته است. توضیح هوسرل درباره این قطعه، آن طور که در گزارش آی. آنجلی (I. Angelelli) آمده، کمتر روشن است: ر.ک. به ضمیمه‌ی II [با عنوان]

Husserls Anmerkungen zur ‘Behriffsschrift’

در

G. Frege, Begreffsschrift und andere Aufsätze, 2nd ed. (Hildescheim 1964).

کتاب‌هایی زیبا در نظریه محاسبه

مرتضی علیمی *

چکیده. شور و علاقه یک نویسنده و عطش او برای انتقال مطالب به مخاطب می‌تواند تأثیری شگرف در اثرش بگذارد. در این مقاله دو کتاب جالب علوم کامپیوتر نظری که علاقه نویسندگانشان در آن‌ها مشهود است را معرفی می‌کنیم.

۱. مقدمه

سال‌ها پیش، هنگام وبگردی به کتاب جالبی در زمینه علوم کامپیوتر نظری تحت عنوان «طبیعت محاسبه» برخوردم که تازه چاپ شده بود. به‌طور خاص عنوان یکی دو فصل آن توجه مرا جلب کرد؛ موضوع‌هایی بودند که دوست داشتم یاد بگیرم، و حداقل از روی فهرست به نظر می‌رسد توسط کتاب خوب پوشش داده شده‌اند. با جستجو معلوم شد که نسخه پیش‌نویس همه فصل‌ها روی وب‌سایت نویسنده‌ها بوده است، اما بعد از چاپ کتاب فایل‌ها را از روی سایت برداشته بودند.

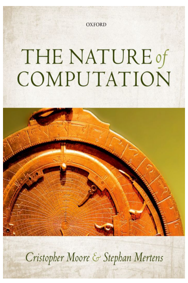
به نویسنده اول ایمیل زدم و گفتم کتابش به نظرم جالب می‌رسد، توضیح دادم خریدن کتاب از ایران سخت است، و درخواست کردم نسخه پیش‌نویس یکی دو تا از فصل‌ها را برایم بفرستد. جواب داد: مرتضی، کیندل داری؟ یا آدرس فیزیکی‌ات چیست؟ گفتم کیندل ندارم، و آدرس را برایش ایمیل کردم. دو سه ماه بعد دی‌اچ‌ال کتاب را درب منزل تحویل داد. از انتشارات دانشگاه آکسفورد پست شده بود.

جذاب بودن رفتار نویسنده کتاب، نحوه ارائه مطالب، کیفیت چاپ و خود محتوای کتاب یکی از انگیزه‌های نوشتن این مقاله شد.

۲. کتاب‌ها

۱.۲. طبیعت محاسبه [۱]. کتابی با گستره وسیع در مورد علوم کامپیوتر نظری. نویسندگان کتاب (کریستوفر مور و استفان مرتنز[1]) اصالتاً فیزیکدان بوده‌اند که به علوم‌کامپیوتر علاقه‌مند شده‌اند و سال‌ها در این زمینه کار کرده‌اند. بر این اساس کتابی هم که نوشته‌اند پیش‌نیاز علوم‌کامپیوتری در نظر نمی‌گیرد و برای دانشمندان حوزه‌های غیرعلوم‌کامپیوتر قابل استفاده است.

[1] Cristopher Moore and Stephan Mertens



شکل ۱: طبیعت محاسبه.

کتاب با استفاده از دانش و شهود مقدماتی برنامه‌نویسی (که فرض می‌کند مخاطب دارد) بحثش را در مورد الگوریتم‌ها، حل کارآی مسائل محاسباتی، و سختی مسائل آغاز می‌کند. معرفی مدل‌های فرمال محاسبه (ماشین‌های تورینگ، حساب لاندا، توابع بازگشتی) تا فصل ۷ به تعویق می‌افتد.

در ادامه، کتاب راجع به بهینه‌سازی و الگوریتم‌های تقریبی و تصادفی صحبت می‌کند. سپس به مباحث جالبی چون تعامل و تصادف، قدم‌زدن تصادفی و نمونه‌گیری و غیره می‌پردازد و در پایان، فصل مفصلی نیز در مورد محاسبات کوانتومی دارد.

کتاب جذاب نوشته شده است و باحال[۱] بودن نویسندگان در آن مشهود است. صفحه‌بندی و شکل‌های زیبایی دارد و یادداشت‌های آخر فصل‌ها نیز خواندنی هستند. همچنین تمرین‌های خیلی خوبی نیز دارد که شامل بسیاری از سؤال‌های کلاسیک حیطه‌های مختلف علوم کامپیوتر نظری می‌شود.

باحال بودن کتاب و اینکه در بسیاری از بحث‌هایش از فرمت معمول قضیه‌ـاثبات اجتناب می‌کند، ممکن است این ذهنیت را ایجاد کند که کتاب سطحی یا غیردقیق است. اما در واقع کتاب مور و مرتنز کتاب عمیقی است و در مورد بسیاری از مسائل با دقت خوبی صحبت می‌کند.[۲] شاید بتوان گفت بهترین استفاده از این کتاب این است که به عنوان منبع کمکی در کنار سایر منابع کلاسیک نظریه محاسبه، پیچیدگی محاسبه، و الگوریتم‌ها استفاده شود.

اگر قرار بود یک دوره ارشد علوم کامپیوتر طراحی کنم و ۳ درس اجباری در آن قرار دهم، به‌طور جدی به این فکر می‌کردم که دو درس را بر مبنای این کتاب بگذارم.

چند نمونه از مطالب کتاب [۳]

- **بحثی در مورد مستقل بودن مسئله** $P \stackrel{?}{=} NP$. یکی از امکان‌هایی که در مورد مسئله $P \stackrel{?}{=} NP$ وجود دارد این است که این مسئله مستقل از اصول موضوعه استاندارد ریاضیات باشد. در صورتی که اینگونه باشد و $P = NP$، وضعیت عجیبی به وجود می‌آید. یک برنامه Q، به هر زبان برنامه‌نویسی‌ای که بخواهیم وجود دارد که مسئله ۳SAT را روی همه نمونه‌های ممکن در زمان چندجمله‌ای حل می‌کند. اما Q این خاصیت عجیب را دارد که نمی‌توان ثابت کرد که کار می‌کند، حتی اگر سورسش را داشته باشیم.

  دلایل خوبی دارد که فکر کنیم این سناریو نامحتمل است. قضیه آخر فرما را در نظر بگیرید: اعداد صحیح $x, y, z > ۰,\ n > ۲$ وجود ندارند که $x^n + y^n = z^n$ (فرض کنید این قضیه هنوز اثبات نشده بود). اگر این قضیه غلط می‌بود، حتماً قابل اثبات بود: کافی بود یک مثال نقض ارائه کنیم. بنابراین اگر قضیه مستقل از یک سیستم منطقی باشد که قدرت بررسی کردن مثال‌های نقض را دارد، باید درست باشد.

  حال گزاره زیر را، که آن را «۳SAT **دشوار است**» می‌نامیم در نظر بگیرید.

  > برای هر $n \geq ۱۰۰۰$، هیچ مدار بولی با حداکثر $n^{\log n}$ گیت وجود ندارد که همه نمونه‌های ۳SAT با اندازه n را حل کند.

  در صورتی که $P = NP$، این گزاره غلط است، چون اگر ۳$SAT \in P$، برای n به اندازه کافی بزرگ چنین مدارهایی وجود دارند. از طرف دیگر، اگر $P \neq NP$، معقول است تصور کنیم «۳SAT **دشوار است**» درست است است. چون صرفاً در صورتی می‌تواند نادرست باشد که $NP \subseteq DTIME(n^{\log n})$ یا $NP \subseteq SIZE(n^{\log n})$ یا اینکه پیچیدگی ۳SAT به‌طور عجیبی نوسان کند؛ یعنی برای بعضی nها آسان و برای برخی سخت باشد. در صورتی که این احتمال‌ها را کنار بگذاریم، می‌توان درستی «۳SAT **دشوار است**» را معادل درستی $P \neq NP$ در نظر گرفت.[۴]

  اما گزاره «۳SAT **دشوار است**» همان ساختار منطقی قضیه آخر فرما را دارد. اگر نادرست باشد، یک اثبات متناهی برای این واقعیت وجود دارد: مثلاً مداری با یک میلیارد گیت که ۳SAT را روی همه نمونه‌های با سایز هزار حل می‌کند.

  بنابراین اگر «۳SAT **دشوار است**» مستقل از اصول موضوعه منطق باشد، باید درست باشد، و در نتیجه $P \neq NP$.

---

[1] cool

[۲] همچنین ذهنیت «آسان» بودن کتاب هم اشتباه است؛ فهمیدن بسیاری از مطالب نیاز به صرف وقت و تمرکز زیاد دارد.

[۳] نحوه بیان عیناً منطبق با کتاب نیست.

[۴] طبق این شهود که اگر مسئله ۳SAT در زمان چندجمله‌ای قابل حل نباشد، احتمالاً به زمان نمایی نیاز دارد و مثلاً در زمان $O(n^{\log n})$ یا توسط مدارهایی با این اندازه نیز قابل حل نیست.

- **اثبات قضیه ناتمامیت گودل با استفاده از تصمیم‌ناپذیری مسئله توقف.** خلاصه اثبات: سیستم منطقی‌ای مثل Φ را در نظر بگیرید که به اندازه‌ای قوی باشد که گزاره‌های معمول در مورد محاسبه توسط آن قابل بیان باشند. به‌طور خاص بتوان توقف کردن یا نکردن یک ماشین تورینگ روی یک ورودی را در آن بیان کرد. همچنین هر وضعیت ماشین تورینگ را بتوان از وضعیت قبلی و توصیف ماشین تورینگ استنتاج کرد. در این صورت اگر ماشین M روی x متوقف شود، حتماً اثباتی برای آن در Φ وجود دارد (دنباله تمام وضعیت‌های محاسبه M روی x). در این صورت حتماً باید ماشین M و ورودی xی وجود داشته باشند که M روی x متوقف نشود و این موضوع در Φ قابل اثبات نباشد. در غیر این صورت می‌توان برای هر ماشین M و ورودی x، شروع به تولید همه اثبات‌ها (به ترتیب طول) کنیم و بررسی کنیم هر اثبات آیا متناظر با توقف یا عدم توقف M روی x است یا نه. به این ترتیب مسئله توقف محاسبه‌پذیر می‌شود که تناقض است. بنابراین گزاره درستی وجود دارد که در Φ قابل اثبات نیست.
- **یک یادداشت آخر فصل ۸.** خوانندگانی که نگران تعداد حالت‌های زیاد بازی Go هستند، خیالشان راحت خواهد شد اگر بفهمند که صرفاً یک درصد موقعیت‌های یک صفحه ۱۹×۱۹ می‌تواند به‌طور قانونی اتفاق بیفتد. به این ترتیب تعداد حالت‌ها از حدود $۱۰^{۱۷۲}$ به $۱۰^{۱۷۰}$ کاهش پیدا می‌کند.
- **تمرینی از فصل ۱۰ کتاب.** لم زیر را در نظر بگیرید.

لم ۱.۲ (لم ایزوله‌سازی). مجموعه m عضوی $S = \{e_۱, \dots, e_m\}$ و خانواده $\{T_۱, \dots, T_N\}$ از زیرمجموعه‌های S، به همراه عدد صحیح مثبت α را در نظر بگیرید. اگر تابع وزن $w : S \to \mathbb{Z}_+$ را به‌گونه‌ای در نظر بگیریم که $w(e_i)$ برای هر i به طور تصادفی مستقل و یکنواخت از $\{۱, \dots, \alpha m\}$ انتخاب شده باشد، به احتمال حداقل $۱ - \frac{۱}{\alpha}$ مجموعه T_j با وزن کمینه یکتاست.

با استفاده از لم ایزوله‌سازی، یک تحویل تصادفی چندجمله‌ای از مسئله CLIQUE به مسئله UNIQUE-CLIQUE ارائه دهید. به‌طور دقیق‌تر، یک الگوریتم تصادفی چندجمله‌ای بیان کنید که با ورودی گراف G و عدد k، گراف G' و عدد k' را خروجی دهد، به‌طوری که

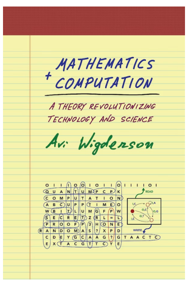
(۱) اگر G خوشه‌ای با اندازه k ندارد، G' هم خوشه‌ای با سایز k' ندارد.

(۲) اگر G خوشه با اندازه k دارد، به احتمال $\Omega(۱/n)$ G' خوشه‌ای با سایز k' دارد، و خوشه بیشینه آن نیز یکتاست.

- **عنوان برخی یادداشت‌های آخر فصل ۱۲ (قدم‌زدن تصادفی و مخلوط شدن سریع).**

Boltzmann. Free Energy. Metropolis. Rapid vs. polynomial. Card shuffling. Glauber dynamics. As rapid as possible. Graph colorings. Spanning trees and time reversal. Topological defects. Coupling from the Past. Arctic circles. Mixing times for tilings. Height functions for magnets and ice. Fourier Analysis. High conductance, large gap. Conductance and flows. Expanders. The zig-zag product. Spatial mixing and coloring the square lattice. Torpid mixing. Walks with momentum. The cutoff phenomenon.

۲.۲. ریاضیات و محاسبه [۲]. اوی ویگدرسون[۱] یکی از بزرگترین علوم‌کامپیوتردانان جهان است که جوایز معتبر



شکل ۲: ریاضیات و محاسبه.

متعددی به خاطر پژوهش‌هایش دریافت کرده است؛ از جمله جایزه گودل، جایزه کنوث، و جایزه آبل. وی در کتابش تلاش می‌کند

[۱] Avi Wigderson

دیدی از بالا به حیطه‌های مختلف علوم‌کامپیوتر نظری داشته باشد. در این راستا، او در ابتدا تمرکز را روی پیچیدگی محاسباتی می‌گذارد و بعد از مرور برخی مفاهیم محوری این حیطه، به مفهوم مهم تصادف[1] و نقش محوری آن در محاسبه می‌پردازد، و از شبه‌تصادف[2] و اثبات‌های تعاملی تصادفی نیز سخن می‌گوید. بعد از پرداختن به برخی پارادایم‌های دیگر پیچیدگی محاسباتی، از جمله پیچیدگی ارتباطی، پیچیدگی حسابی، و پیچیدگی حافظه، به برخی حیطه‌هایی که ارتباط عمیقی با پیچیدگی محاسباتی دارند می‌پردازد و همچنین از برخی پارادایم‌های متفاوت محاسباتی صحبت می‌کند. به‌طور خاص ویگدرسون فصل‌هایی را به نظریه یادگیری محاسباتی، رمزنگاری، محاسبات برخط و محاسبات توزیع‌شده، و همچنین محاسبات کوانتومی اختصاص می‌دهد.

دید عمیق و تجربه پژوهشی وسیع ویگدرسون به او این توانایی را می‌دهد که بتواند ارتباط عمیق شاخه‌های مختلف علوم‌کامپیوتر نظری (به‌طور کلی)، و پیچیدگی محاسباتی (به‌طور خاص) را بررسی کند و ظهور برخی ایده‌های مرکزی در شاخه‌های مختلف را نشان دهد.

وی از ارتباط پیچیدگی محاسباتی با بخش‌های مختلف ریاضیات نیز صحبت می‌کند، و در فصل آخر کتاب راجع به برخی مسائل کلی مرتبط با نظریه محاسبه و پیچیدگی محاسبه صحبت می‌کند. او سعی می‌کند تا نشان دهد که محاسبه یک مفهوم بسیار گسترده در جهان است. به‌علاوه، ابزارهای پیچیدگی محاسباتی در چند دهه اخیر را منشأ یک زاویه دید جدید به بسیاری از مسائل و حیطه‌های علمی معرفی می‌کند که باعث غنای درک ما از جهان می‌شود.

کتاب ویگدرسون در صدد منتقل کردن ایده‌های محوری و ارتباط آنها با یکدیگر است و عموماً وارد جزئیات نمی‌شود؛ به‌طور خاص در کتاب تقریباً هیچ قضیه‌ای [به‌طور دقیق] اثبات نمی‌شود. در همین راستا کتاب تمرین هم [رسماً] ندارد؛ هر چند متن کتاب ذهن را به فکر کردن روی موضوعات و مسائل مختلف وا می‌دارد.

بر این اساس کتاب ویگدرسون می‌تواند منبع کمکی بسیار خوبی برای تعمیق و تحکیم دانش علوم کامپیوتر نظری برای علاقمندان باشد.

منتخبی از کتاب

در فصل ۲۰، ویگدرسون متدلوژی مورد استفاده در علوم کامپیوتر نظری را در ده مورد خلاصه می‌کند.

- **مدل‌سازی محاسباتی.**[3] عملیات بنیادین، جریان اطلاعات، و منابع مورد استفاده هر فرایند را کشف و به صورت فرمال بیان کنید.
- **کارآیی الگوریتمی.**[4] تلاش کنید منابع استفاده شده توسط فرایندهای محاسباتی را کمینه کنید و مصالحه بین آنها را مطالعه کنید.
- **تفکر مجانبی.**[5] سعی کنید مسائل را روی نمونه‌های بزرگ و بزرگ‌تر مطالعه کنید؛ ساختارها معمولاً در حد خودشان را نشان می‌دهند.
- **تفکر دشمنانه.**[6] خودتان را برای بدترین حالت آماده کنید. محدودیت‌های خاص و ساختاری را با محدودیت‌های دشمنانه و بدترین حالت جایگزین کنید. انتظارات بالاتر در بسیاری از موارد درک چیزها را ساده‌تر می‌کند!
- **طبقه‌بندی.**[7] مسائل محاسباتی را بر حسب منابع مختلفی که در مدل‌های محاسباتی مختلف مصرف می‌کنند به کلاس‌های پیچیدگی طبقه‌بندی کنید.
- **تحویل.**[8] نادانی خود را نادیده بگیرید. حتی اگر نمی‌توانید مسئله‌ای را به‌طور کارآ حل کنید، فرض کنید می‌توانید، و بررسی کنید با این فرض چه مسائل دیگری را نیز می‌توانید به‌طور کارآ حل کنید.
- **تمامیت.**[9] سخت‌ترین مسائل هر کلاس پیچیدگی را بیابید.
- **سختی.**[10] سعی کنید نتایج مربوط به سختی مسائل اثبات کنید؛ این‌گونه نتایج مفیدند!

---
[1] Randomness
[2] Pseudo-randomness
[3] Computational modeling
[4] Algorithmic efficiency
[5] Asymptotic thinking
[6] Adversarial thinking
[7] Classification
[8] Reductions
[9] Completeness
[10] Hardness

- **موانع.**[۱] اگر مدت زیادی است که برای حل یک مسئله به بن‌بست خورده‌اید، همه تکنیک‌های امتحان شده برای حل مسئله را انتزاع کنید، و سعی کنید با استدلالی فرمال نشان دهید این تکنیک‌ها برای حل مسئله کافی نیستند.
- **بازی.**[۲] واقعیت را فراموش کنید. به دنبال غیرممکن‌ها بروید.

۳. برای خوش‌اشتهاها

در این بخش، چند منبع جالب و تقریباً تصادفی را برای علاقمندان نظریه محاسبه معرفی می‌کنم.

[۳]: لذیذ است، اما مطمئن شوید کارد و چنگال مناسب در اختیار دارید.

[۴]: می‌توان در کنار خانواده خورد.

[۵]: برای عضله‌سازی مفید است.[۳]

[۶]: خوراک تحویل‌کارها.

مراجع

[1] Cristopher Moore, Stephan Mertens, “The Nature of Computation”, Oxford University Press, 2011.

[2] Avi Wigderson, “Mathematics and Computation”, Princeton University Press, 2019.

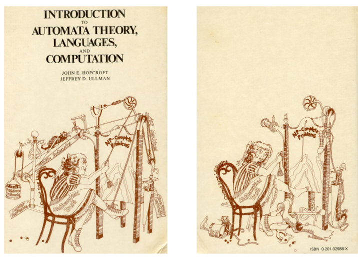
[3] Sebastian Oberhoff, “Incompleteness Ex Machina”, 2019.

[4] Scott Aaronson, “$P \stackrel{?}{=} NP$”.

[5] John Hopcroft, Jeffrey Ullman, “Introduction to Automata Theory, Languages, and Computation”, 1st Edition[4], Addison-Wesley, 1979.

[6] Erik Demaine,“Algorithmic Lower Bounds: Fun with Hardness Proofs”, MIT course, Spring 2019.

پیوست آ. جلد هاپکرافت-اولمن



شکل ۳: جلد کتاب هاپکرافت-اولمن

متن زیر را در جوانی در مورد جلد کتاب [۵] نوشته بودم.

Mathematical truth governs Turing machines, operating beyond the limits of practical tractibility, with time and space complexity nevertheless always lurking in the background.

The more fragile, yet always practical world of finite machines - which can come alive through its intimate interaction with the living world - is under the threat of being toppled by Mathematical Truth, getting a helping hand from the pull of Turing machines’ non-finite yet more limited counterpart, the push-down automaton.

One should be wary of underestimating the role of regular yet not trivial expressions, which can lend a meaning to parts of the computation machinery, strengthened from more general languages which can come about handy in more specific contexts.

* فارغ‌التحصیل دکترای علوم کامپیوتر، دانشگاه صنعتی شریف
رایانامه: morteza.alimi+academic@gmail.com

[1] Barriers
[2] Play

[۳] جلد و پشت جلد جالبی هم دارد! پیوست آ را ببینید.
[4] ویرایش اول!

معرفی کتاب:

منطق، ریاضیات، و فلسفه‌های آن‌ها:

جستارهایی به افتخار محمد اردشیر

محمدصالح زارع‌پور*

از من خواسته شده است که درباره‌ی کتاب ریاضیات، منطق، و فلسفه‌های آن‌ها بنویسم. با این‌که خودم از پدیدآورندگان این کتاب بوده‌ام، نوشتنْ برای معرفی و تبلیغ آن را دور از تواضع نمی‌دانم. شاید به این دلیل که این کار را در جهت هدف اصلی کتاب می‌بینم. چنان‌که از عنوان فرعی کتاب (یعنی: جستارهایی به افتخار محمد اردشیر) برمی‌آید، این کتاب دربردارنده‌ی مجموعه‌ای از مقالات است که به افتخار محمد اردشیر و برای گرامی‌داشت میراث علمی او نوشته شده‌اند. دکتر محمد اردشیر استاد دانشکده‌ی علوم ریاضی دانشگاه صنعتی شریف است و به‌واسطه‌ی آثار علمی مهم و متعددْ شهرت و اعتبار جهانی دارد. اردشیر در درجه‌ی اول متخصص ریاضیات ساختی و منطق ریاضی است. اما صاحب آثار مهمی در فلسفه‌ی منطق و ریاضیات هم هست. بعضی از این آثار با تکیه بر شهودگرایی معاصر و بعضی دیگر با تکیه بر دیدگاه‌های فلاسفه‌ی نامدار سنت اسلامی (مثلاً ابن سینا و سهروردی) نوشته شده‌اند. عنوان کتاب مورد بحث هم بازتاب‌دهنده‌ی مؤلفه‌های اصلی علایق علمی و فلسفی اردشیر است: ریاضیات، منطق، و فلسفه‌های آنها.

این کتاب در مجموعه‌ی منطق، معرفت‌شناسی، و وحدت علم (Logic, Epistemology, and the Unity of Science) از انتشارات اشپرینگر (Springer) منتشر شده است. این انتشارات یکی از معتبرترین ناشران دانشگاهی جهان است. سرویراستار مجموعه‌ی منطق، معرفت‌شناسی، و وحدت علم شاهد رحمان، استاد برجسته‌ی دانشگاه لیل فرانسه، است. رحمان سرویراستار یک مجموعه‌ی دیگر از کتاب‌های انتشارات اشپرینگر نیز هست: مجموعه‌ی منطق، احتجاج، و استدلال (Logic, Argumentation & Reasoning). پیشنهاد اولیه‌ی تهیه‌ی کتابی به افتخار محمد اردشیر را هم خود شاهد رحمان مطرح کرد. گمان می‌کنم همین که این کتاب را ناشری چنین معتبر منتشر کرده و بانی اصلی تهیه‌ی آن منطق‌دان و فیلسوف برجسته‌ای چون شاهد رحمان بوده است نشان از اعتبار و بلندی جایگاه علمی اردشیر در سطح جهانی دارد. زمستان ۱۳۹۷ شاهد رحمان از من و مجتبی مجتهدی برای همکاری در تهیه‌ی این کتاب دعوت کرد. مجتبی مجتهدی، استادیار دانشکده ریاضیات، آمار و علوم کامپیوتر دانشگاه تهران، است. او از دانشجویان دکتری اردشیر در دانشگاه صنعتی شریف بوده و چند مقاله‌ی مشترک با اردشیر منتشر کرده است. من و مجتبی در دوران کارشناسی و به‌طور خاص در چند درس اردشیر (مثل مبانی ریاضیات، منطق ریاضی، و مقولات ویژه در منطق) هم‌کلاسی بوده‌ایم. برای من، تجربه‌ی همکاری با مجتبی و شاهد رحمان تجربه‌ای بسیار مطبوع و آموزنده بود. حوزه‌ی کاری و پژوهشی هر کدام از ما سه نفر به بخشی از کارهای اردشیر مربوط می‌شد. اما هیچ کدام از ما به همه‌ی زمینه‌هایی که اردشیر درباره‌ی آن‌ها پژوهش کرده و نوشته است اشراف نداشتیم. این هم نشانی است از وسعت دامنه‌ی پژوهش‌های اردشیر؛ به‌خصوص برای کسانی که از دانش وسیع شاهد رحمان و مجتبی مجتهدی باخبرند.

کتابْ با مقدمه‌ای درباره‌ی زندگی علمی اردشیر آغاز می‌شود. در این مقدمه زمینه‌های مختلفی که اردشیر در آن‌ها پژوهش کرده و مهم‌ترین دست‌آوردهای او در هر یک از این زمینه‌ها به اختصار معرفی شده است. پیش از مقاله‌های اصلی کتاب، فهرستی کامل از آثار اردشیر آمده است. این فهرست دربرگیرنده‌ی سه کتاب و چهل‌ویک مقاله (به فارسی یا انگلیسی) است که اردشیر تا پایان سال ۲۰۲۰ میلادی منتشر کرده است. شناخته‌شده‌ترین اثر اردشیر در جامعه‌ی دانشگاهی ایران احتمالاً کتاب منطق ریاضی است که چاپ اول آن در سال ۱۳۸۴ توسط انتشارات هرمس منتشر شده است. این کتاب که برنده‌ی جایزه‌ی کتاب سال ایران شده تا کنون پنج بار چاپ شده و به کتاب استانداردِ درس منطق ریاضی در دانشگاه‌های ایران تبدیل شده است.

در کتاب ریاضیات، منطق، و فلسفه‌های آنها هجده مقاله منتشر شده است که برخی از آن‌ها بیش از یک نویسنده دارند. همه‌ی این مقالات به زبان انگلیسی نوشته شده‌اند و در مجموع سی پژوهشگر در نوشتن آن‌ها دخیل بوده‌اند؛ دوازده پژوهشگر ایرانی و هجده پژوهشگر غیرایرانی. اکثر این پژوهشگران از همکاران، شاگردان و دوستان اردشیر هستند و زمینه‌ی کاری هر کدام از ایشان به برخی از کارهای پژوهشی اردشیر مرتبط است. دوازده مقاله از مقالات این کتاب به زمینه‌ی اصلی کارهای اردشیر یعنی ریاضیات ساختی و منطق ریاضی مربوط است. سه مقاله در حوزه‌ی فلسفه‌ی منطق و ریاضی معاصر قرار می‌گیرند و سه مقاله به مقولاتی در منطق و معرفت‌شناسی ابن سینا می‌پردازند. ویم ولدمن، دیک دِ یانگ، آلبرت فیسر و هانس فان دیتمارش از برجسته‌ترین منطق‌دانان غیرایرانی هستند که در میان نویسندگان مقالات این کتاب قرار دارند. از افتخارات ویراستاران کتاب این است که سیاوش میرشمس شهشهانی، استاد ممتاز دانشگاه صنعتی شریف، دعوت ویراستاران را پذیرفت و برای این مجموعه مقاله‌ای درباره‌ی بی‌توجهی به هندسه در فلسفه‌ی ریاضی معاصر نوشت. اطلاع از دیدگاه فلسفی شهشهانی درباره‌ی این موضوع به‌طور خاص از این جهت مغتنم است که هم هندسه‌دانی تراز اول است و هم چندین دوره فلسفه‌ی ریاضی درس داده است. در کنار متن فنی مقالاتْ یادداشت‌های کوتاهی که برخی نویسندگان درباره‌ی اردشیر و کارهای علمی او نوشته‌اند نیز بسیار خواندنی است؛ مثلاً نگاه کنید به یادداشت مجتبی مجتهدی در بخش ۱.۹ کتاب و پانوشت اول از مقاله‌ی کاوه لاجوردی.

مطمئناً این مجموعه نواقصی هم دارد. اما بسیار امیدوارم که نشانی کوچک باشد از این‌که ما قدردان حضور محمد اردشیر هم به عنوان پژوهشگری برجسته در جامعه‌ی علمی و هم به عنوان معلم، دوست، و همکاری دوست‌داشتنی هستیم. امیدوارم محمد اردشیر عمری بسیار طولانی داشته باشد و ما هم‌چنان، سال‌های سال، از دقت‌نظر علمی، وسعت دانش، انضباط سرسختانه، شوخ‌طبعی‌های لطیف، و مهربانی درون‌گرایانه‌ی او بهره‌مند شویم.

(این نوشته با اجازه‌ی نگارنده از صفحه‌ی اینترنتی http://old.bookcity.org/detail/25310 برگرفته شده است.)

* دانشگاه منچستر
رایانامه: mohammadsaleh.zarepour@manchester.ac.uk

معرفی پادکست:
از نادر گمنام تا آدم‌ها و ریاضی

علی الماسی*

یادم است یک بار در قفسه‌ای خاک‌گرفته در کتابخانه‌ی مدرسه‌ی راهنمایی‌مان کشف جدیدی کردم. مجله‌هایی که اسم‌شان برهان بود و مطالب‌شان درباره‌ی ریاضیاتی که آن روزها، تازه در حال تجربه‌کردن و چشیدن طعم‌اش بودم، و خودمان‌ایم، مزه‌اش هم به دل‌ام نشسته بود. با اشتیاقی حاصل از کشف جدید، آن چند شماره را به خانه آوردم و شروع به خواندن‌شان کردم. راستش آن موقع، در کل، چندان چنگی به دلم نزد. با این وجود، دو صفحه در همه‌ی شماره‌ها بود که برایم بسیار جذاب بود. داستان‌های مصوری به قلم «نادر گمنام»، که از گیلان و اصفهان و مسجدسلیمان تا یونان و آمریکا سفر می‌کرد و هم‌صحبت ریاضی‌دانانی می‌شد که نام خیلی‌هایشان را اولین بار بود که می‌شنیدم. شخصیت‌هایی که آن موقع نمی‌دانستم بعضی‌هایشان چند سال بعد، از داستان‌های نادر گمنام به داستان زندگی خودم هم می‌آیند.

چند سال بعد، در دبیرستان، دوباره پای قصه‌ای به رابطه‌ی من و ریاضی آشنا شد. این بار اما قصه، مثل داستان‌های نادر گمنام پایان خوشی نداشت که آدم بعد از خواندن‌اش، دل‌اش غنج برود برای ریاضی‌دان‌شدن. برای من، که با خواندن چند صفحه‌ی اول کتاب، طوری میخ‌کوب داستان شدم که تمام کتاب را در پنج‌ـشش ساعت خواندم، قصه به قدری مهیب بود که تا چند روز نمی‌توانستم دست از فکرکردن درباره‌اش بردارم. کتاب درباره‌ی «سفری حماسی برای یافتن حقیقت» بود. سفری که آدم را هم‌چون کمدی الهی دانته، از میان دوزخ و برزخ می‌گذراند تا (شاید) به بهشت حقیقت برساند، و من گمان می‌کنم که در همان برزخ با قهرمان‌های کمدی منطق جا ماندم.

وقتی داشتم وارد شریف می‌شدم که ریاضی بخوانم، تازه فهمیدم که نادر گمنام سال‌های راهنمایی، همان مترجم کمدی منطق دوران دبیرستان، همان سلبریتی آموزش ریاضی شریف و بهشتی و همان امیر اصغری است. راست‌اش، برای من خیلی سخت است که امیر اصغری را معرفی کنم. با این حال، فکر می‌کنم هر کدام‌مان یک جوری با او آشنا هستیم. بعضی، از آن ریاضی دوی افسانه‌ای و به قول خودش غیر استانداردش در شریف می‌شناسندش؛ عده‌ای با مجله‌ی شفاهی و شماره‌هایی از مجله که درباره‌ی آموزش ریاضی هستند و او پای ثابت‌شان است؛ بعضی با math4maryams و کلکسیون بی‌نظیری که از مجله‌های ریاضی فارسی درست کرده است و ما همبندی‌ها علاوه بر همه‌ی این‌ها با این اخلاق‌اش که هیچ‌وقت نه نمی‌آورد و (شاید) تنها استادی است که خیلی وقت‌ها ما را جدی گرفته است.

نادر گمنام ما، این روزها روایت مجموعه داستان جدیدی را آغاز کرده است. آدم‌ها و ریاضی نام پروژه‌ی تازه‌ی اوست. راویان داستان‌ها، خودشان ریاضی‌دان‌اند و روایت‌گر ماجراهایشان با ریاضیات. امیر از آن‌ها می‌خواهد که برایمان تعریف کنند که چه مسیری در زندگی آن‌ها طی شده است تا به جایگاه فعلی‌شان در ریاضیات برسند، و گاهی خودش هم سوالاتی می‌پرسد تا جنبه‌های مجهول داستان را روشن‌تر کند. هر داستان، گرچه از دیگری مستقل است، اما بی‌ارتباط به آن نیست. شهشهانی، مصاحب و شریف، از جمله شخصیت‌هایی هستند که در بیشتر داستان‌ها حضور دارند و در هر گفت‌وگو ابعادی متفاوت از آن‌ها روشن می‌شود. این را نیز باید در نظر گرفت که بستر تاریخی و اجتماعی روایت‌ها با یکدیگر اشتراکات زیادی دارد و به این ترتیب، از خلال گفت‌وگوها می‌توان نکات تاریخی و اجتماعی ارزشمندی را درباره‌ی ایران دهه‌های گذشته دریافت.

برای من، مجموعه داستان جدید امیر اصغری با دو داستان قبلی که بالاتر به آن‌ها اشاره کردم متفاوت است؛ و البته من به عنوان شنونده‌ی داستان نیز با آن آدم قبلی فرق دارم. آدم‌ها و ریاضی مجموعه‌ای از داستان‌های واقعی است؛ داستان‌هایی که راوی بعضی‌هایشان با نسل ما فقط یک دهه تفاوت سنی دارند و بعضی حرف‌هایشان را می‌توانید با گوشت و پوست‌تان احساس کنید؛ با قصه‌ی مونا آزادکیا از ته دل شاد شوید، با شنیدن داستان سیامک یاسمی بغض گلویتان را فشار دهد و به چشمان‌تان

اشک بنشیند، با روایت اسماعیل بابلیان پشت پرده‌ی تالیف کتب درسی که با آن‌ها ریاضی آموخته‌اید را ببینید و با صحبت‌های سیاوش شهشهانی، حسرت این به دل‌تان بنشیند که کاش چند سال زودتر به شریف آمده بودید و با او درس می‌گرفتید. آدم‌ها و ریاضی برای آن‌ها که ریاضی خوانده و می‌خوانند، روشن‌گر و الهام‌بخش است؛ و بالاخص برای کسانی که در ایران ریاضی خوانده‌اند، متضمن نکات تاریخی ارزشمند و مهمی درباره‌ی فرهنگ ریاضی ایران است که احتمالاً می‌توان جای دیگری به آن‌ها دست‌رسی پیدا کرد.

از آن‌جا که فرض کرده‌ام مخاطبان این نوشته در وهله‌ی اول هم‌دانشکده‌ای‌های خودم در شریف و اعضای انجمن علمی همبند هستند، بیان نکته‌ای را خالی از لطف نمی‌بینم. بهار ۹۹، در آستانه‌ی تولد دکتر سیاوش شهشهانی، اعضای همبند آن دوره در تکاپو بودند که برنامه‌ی بزرگ‌داشتی به مناسبت تولد ایشان برگزار کنند. یکی از ایده‌هایی که در آن زمان توسط دکتر علی کمالی‌نژاد طرح شد، تهیه‌ی یک مصاحبه‌ی مفصل با خود دکتر شهشهانی درباره‌ی جنبه‌های مختلف زندگی و فعالیت‌های علمی، آموزشی، تالیفی و اجتماعی‌شان به سبک پروژه‌ی تاریخ شفاهی ایران در دانشگاه هاروارد بود. برای ما که آن روزها، با وجود تلاش فراوان موفق به انجام این کار نشدیم، آغاز شدن پروژه‌ی آدم‌ها و ریاضی، به عنوان طرحی که با ایده‌های اولیه‌ی ما قرابت زیادی دارد، بسیار خرسندکننده است. از طرفی، در دوره‌های مختلف، همبند برنامه‌هایی را به سبک گفت‌وگو درباره‌ی مسیر زندگی و فعالیت‌های آکادمیک با اساتید ریاضی و علوم‌کامپیوتر برنامه‌ریزی و اجرا کرده است (جدیدترین چنین برنامه‌هایی را که از سال ۹۷ آغاز شده و ـ‌کمابیش‌ـ تاکنون ادامه داشته است، احتمالاً با نام ریسمان می‌شناسید.). به باور من، این تجربه‌های همبند، و ایده‌ها و طرح‌هایی که اعضای آن در طول سال‌ها به حافظه‌ی آن افزوده‌اند، می‌تواند به یاری آدم‌ها و ریاضی بیاید و چه بسا برخی کاستی‌ها و نقص‌های فعلی را نیز برطرف کند. ارتباط نزدیک امیر اصغری با همبند در سال‌های اخیر، برای من نویدبخش تحقق چنین هم‌فکری و هم‌کاری‌هایی است و امیدوارم که هر چه زودتر اتفاق بیفتد.

به هر ترتیب، اگر دوست دارید با شخصیت‌های مهم ریاضیات معاصر ایران آشنا شوید، فراز و نشیب‌ها و پیچ و خم‌های مسیر زندگیشان برای رسیدن به جایگاه فعلی‌شان در ریاضیات را بدانید و در یک کلام، از پنجره‌ی زندگی «آدم‌ها» نیم‌نگاهی به «ریاضی» بیندازید، آدم‌ها و ریاضی فرصتی برای آن است. فرصتی که به دست کسی فراهم شده که خودش هم ید طولایی در روایت‌گری ریاضیات و آدم‌های آن را دارد.

* فارغ‌التحصیل کارشناسی ریاضی، دانشگاه صنعتی شریف
رایانامه: ali.almasi@sharif.edu

مجله‌ی ریاضی شریف
دوره‌ی سوم، شماره‌ی اول (بهار ۱۴۰۲)

آزمون انتخاب تیم دانشکده‌ی علوم ریاضی

علیرضا عظیمی‌نیا*

چکیده. آزمون انتخاب تیم دانشکده‌ی علوم ریاضی شریف برای مسابقات دانش‌جویی سال ۱۴۰۲ در سوم خردادماه امسال برگزار شد. در این بخش مسائل این آزمون و پاسخ آن‌ها را از نظر خواهیم گذراند.

۱. مسئله‌ها

(۱) دنباله‌ی $a_n > 0$ به صفر همگراست. نشان دهید هر بازه‌ی باز ناتهی (a,b) یک زیربازه‌ی باز ناتهی (c,d) دارد که هیچ عضوی در آن به صورت حاصل‌جمع ۱۴۰۲ عضو متمایز از دنباله‌ی a_n نیست.

(۲) فرض کنید $f:\mathbb{R}\to\mathbb{R}$ تابعی سه‌بار مشتق‌پذیر با مشتقات پیوسته باشد. نشان دهید عدد حقیقی a وجود دارد که

$$f(a)f'(a)f''(a)f'''(a) \geq 0$$

(۳) فرض کنید S یک مجموعه‌ی متناهی از اعداد صحیح بزرگ‌تر از یک باشد که برای هر عدد طبیعی داده‌شده، یا عددی در S وجود دارد که آن را عاد کند و یا عددی در S وجود دارد که نسبت به آن اول باشد. ثابت کنید S یا شامل یک عدد اول است یا شامل دو عدد است که ب.م.م آن‌ها یک عدد اول باشد.

(۴) فرض کنید G یک گروه متناهی از ماتریس‌های $n\times n$ (با درایه‌های حقیقی) با عمل ضرب ماتریسی باشد. نشان دهید اگر جمع اثر (trace) همه‌ی عناصر این گروه صفر باشد، آنگاه جمع همه‌ی عناصر گروه هم صفر خواهد بود.

(۵) از سه کشور ایران، آلمان و فرانسه تعداد مساوی دانشمند قصد تشکیل گروه‌های تحقیقاتی سه نفره دارند. شرط این گروه‌ها این است که هر دانشمند در حداکثر یک گروه می‌تواند شرکت کند و هر گروه از هر سه کشور دانشمند داشته باشد. در ضمن هر سه دانشمند با هم سازگار باشند. سازگاری یک رابطه‌ی دوطرفه است. اگر الف با ب سازگار باشد، ب هم با الف سازگار است.

ابتدا نشان دهید برای هر تعداد زوجی از دانشمندان، اگر هر دانشمند با نصف دانشمندان هر کشور دیگر سازگار باشد، مثالی وجود دارد که حتی نتوان یک گروه تحقیقاتی هم ایجاد کرد. سپس نشان دهید اگر هر دانشمند با حداقل سه‌چهارم دانشمندان هر کشور دیگر سازگار باشد، می‌توان همه‌ی دانشمندان را به گروه‌های مجاز سه نفری افراز کرد.

(۶) فرض کنید R یک حلقه‌ی جابه‌جایی، یک‌دار و حوزه صحیح (یعنی ضرب عناصر ناصفر، ناصفر است) باشد. عنصر وارون‌ناپذیر p اول نامیده می‌شود اگر در شرط اقلیدس صدق کند، یعنی اگر $p|ab$ آنگاه $p|a$ یا $p|b$. نشان دهید اگر ایده‌آل I متشکل از همه‌ی عناصری که بر همه‌ی توان‌های مثبت عنصر اول p بخش‌پذیرند متناهی مولد باشد، آنگاه صفر است. با فرض $I = 0$ نشان دهید ایده‌آل تولید شده توسط p در بین تمام ایده‌آل‌های اول ناصفر مینیمال است.

۲. پاسخ مسائل

۱.۲. پاسخ مسئله‌ی اول. مجموعه S_k را مجموعه‌ی همه‌ی اعداد حقیقی که بصورت حاصل‌جمع k عضو متمایز دنباله a_n نوشته می‌شوند در نظر بگیرید. حکم را با استقرا روی k ثابت می‌کنیم.

فرض کنید $k = 1$ و بازه (a,b) داده شده است. اگر $b \leq 0$، چیزی برای اثبات وجود ندارد؛ پس فرض کنید $b > 0$. برای $0 < c < b$ و n بزرگ داریم $a_n < c$، پس $a_n \notin (c,b)$. یعنی فقط تعداد متناهی از اعضای دنباله در (c,b) قرار دارند. پس می‌توان $c < d < b$ را طوری انتخاب کرد که (c,d) شامل هیچ عضو دنباله نباشد.

حال با فرض درستی حکم برای k، آن را برای $k+1$ ثابت می‌کنیم. برای بازه (a,b) داده شده، زیربازه (c',d) را طوری انتخاب کنید تا با S_k اشتراک نداشته باشد. $h>0$ را نصف طول بازه (c',d) فرض کنید. پس $c=c'+h$ وسط (c',d) است. عدد N را می‌توان یافت به طوری که $a_i<h$ برای $i>N$. حال عضو دلخواه $s\in S_{k+1}$ که جمع $k+1$ جمله متمایز از دنباله است را در نظر بگیرید. اگر $s\in(c,d)$ آنگاه جمله‌ی آخر حتماً یکی از $a_1,\ldots,a_N$ است؛ در غیر این صورت جمله‌ی آخر از h کمتر است، و جمع k جمله‌ی اول در (c',d) می‌افتد، که متناقض است با نحوه تعریف (c',d). اکنون با استقرا روی N، می‌توان زیربازه‌ای از (c,d) یافت که مجموع‌های با جمله آخر $a_1,\ldots,a_N$ در آن نیستند. بازه $(c-a_1,d-a_1)$ را در نظر بگیرید. زیربازه (e,f) را می‌توان یافت به طوری که با S_k اشتراک ندارد. اکنون (c_1,d_1) که $c_1=e+a_1$ و $d_1=f+a_1$ زیربازه‌ای از (c,d) است که شامل هیچ عضو S_{k+1} با جمله‌ی آخر a_1 (یا هر a_i که $i>N$) نیست. به همین ترتیب، می‌توان زیربازه (c_2,d_2) از (c_1,d_1) را یافت که شامل هیچ عضو S_{k+1} با جمله‌ی آخر a_2 (یا a_1 یا هر a_i که $i>N$) نیست. و الی آخر.

۲.۲. پاسخ مسئله‌ی دوم. اگر هر کدام از f، f'، f''، f''' تغییر علامت دهند، نقطه تغییر علامت جواب است. نشان می‌دهیم اگر f، f'، f'' تغییر علامت ندهند آنگاه f و f'' هم‌علامت‌اند. فرض کنید f'' مثبت باشد. آنگاه $f(x)=f(0)+f'(0)x+f''(c)x^2/2$ برای c مناسب. پس $f(x)>f(0)+f'(0)x$ برای هر x، که نتیجه می‌دهد حتماً $f(x)$ برای x بزرگ و هم‌علامت با $f'(0)$ مثبت است؛ و چون f تغییر علامت نمی‌دهد پس همه‌جا مثبت است. به طور مشابه، اگر f'' منفی باشد، f نیز اینگونه است. بنابراین $f(x)f''(x)\geq 0$ برای هر x. به طور مشابه، $f'(x)f'''(x)\geq 0$ برای هر x.

۳.۲. پاسخ مسئله‌ی سوم. عدد طبیعی n را کوچکترین عددی در نظر بگیرید که نسبت به هیچ‌کدام از عناصر S اول نباشد. توجه شود که مثلا ضرب تمام عناصر S نسبت به هیچ‌کدام از عناصر S اول نیست؛ پس چنین n وجود دارد. طبق فرض، $m\in S$ وجود دارد که n را عاد کند. اگر m اول باشد، کار تمام است. در غیر اینصورت عدد اول p که m (و در نتیجه n) را عاد می‌کند انتخاب کنید و قرار دهید $n'=n/p$. دقت کنید $n'<n$، پس $m'\in S$ یافت می‌شود که نسبت به n' اول باشد. از آنجایی که $n=n'p$ نسبت به m' اول نیست، p حتماً m' را عاد می‌کند. به علاوه، p لزوماً ب.م.م m و m' است؛ زیرا اگر pd هر دو m و m' را عاد کند، حتماً n و m' را نیز عاد می‌کند، پس d دو عدد m' و n' را (که نسبت به هم اول بودند) عاد می‌کند، پس $d=1$. در نتیجه، m و m' دو عضو S هستند که ب.م.م آنها، p، عددی اول است.

۴.۲. پاسخ مسئله‌ی چهارم. اعضای G را بصورت $A_1,\ldots,A_m$ در نظر بگیرید و قرار دهید $A=\sum A_i$. چون G یک گروه ضربی است با تغییر ترتیب عناصر سیگما می‌توان دید $A_iA=A$ که نتیجه می‌دهد

$$A^2=mA \tag{۱.۲}$$

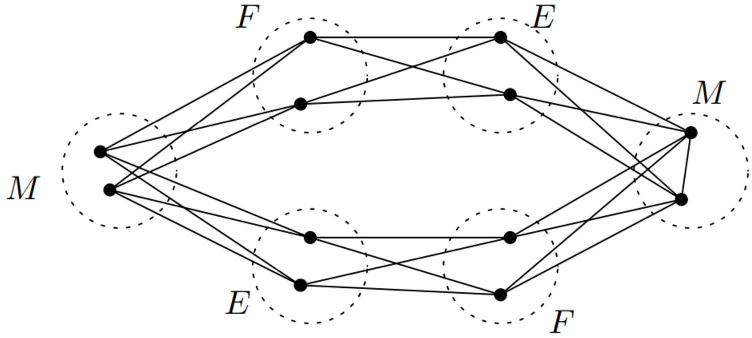
حال اگر مقادیر و بردارهای مختلط را مجاز در نظر بگیریم، A دارای m مقدار ویژه (با احتساب تکرر) است. اگر $Av=\lambda v$ آنگاه ۱.۲ نتیجه می‌دهد $\lambda^2=m\lambda$. پس یا $\lambda=0$ یا $\lambda=m$. از آنجایی که $\mathrm{trace}(A)$ برابر جمع مقادیر ویژه A است، پس m نمی‌تواند مقدار ویژه A باشد، یعنی $A-mI$ وارون‌پذیر است. رابطه ۱.۲ را می‌توان بصورت $A(A-mI)=0$ نوشت. پس

$$A=A(A-mI)(A-mI)^{-1}=0$$

۵.۲. پاسخ مسئله‌ی پنجم. مجموعه‌ی دانشمندان این سه کشور را به ترتیب با E، M و F نشان دهید. گراف سه‌بخشی H با رئوس $E\cup M\cup F$ را در نظر بگیرید که یال‌ها همان روابط سازگاری باشند. یک دور به طول ۳ می‌تواند نشان‌دهنده یک گروه تحقیقاتی باشد. H را «گراف سازگاری» می‌نامیم. n را تعداد دانشمندان هر کشور در نظر بگیرید.

برای قسمت اول، n زوج است و باید یک گراف سازگاری بدون دور به طول ۳ بسازیم. ایده این است که هر کدام از E، M و F را به دو قسمت مساوی تقسیم می‌کنیم و رئوس هر دو قسمت که مطابق شکل زیر به هم وصل هستند را دو به دو به هم وصل می‌کنیم.

برای قسمت دوم، ابتدا به دلخواه تمامی دانشمندان را به گروه‌های تحقیقاتی سه‌نفره تقسیم کنید به طوری که هر گروه از هر سه کشور دانشمند داشته باشد. کمیت «نارضایتی» را برای چنین تقسیمی به صورت تعداد زوج دانشمند تعریف کنید که در یک گروه هستند ولی با یکدیگر سازگار نیستند. چنین زوجی را «ناراضی» می‌نامیم. در ادامه نشان می‌دهیم اگر نارضایتی عددی



مثبت باشد، با عملیاتی ساده می‌توان آن را کاهش داد. این نتیجه می‌دهد که پس از تعداد متناهی گام به تقسیمی با نارضایتی صفر می‌رسیم.

فرض کنید یک ایرانی با حداقل یکی از هم‌گروهی‌هایش سازگار نباشد (استدلال برای آلمانی یا فرانسوی مشابه است). این ایرانی را با یک ایرانی «مناسب» دیگر جابجا کنید به طوری که این دو نفر با هم‌گروهی‌های جدیدشان سازگار باشند. از آنجایی که تغییری در زوج‌های ناراضی دیگر رخ نداده، نارضایتی در تقسیم‌بندی جدید اکیداً کمتر است.

می‌ماند اثبات وجود یک ایرانی مناسب. گروه‌ها را با $۱, \ldots, n$ شماره‌گذاری کنید، و اعضای گروه iـام را بر اساس ملیتشان به صورت E_i، M_i و F_i نشان دهید. بدون کاستن از کلیت می‌توان فرض کرد که $E_۱$ با حداقل یکی از $M_۱$ یا $F_۱$ سازگار نیست. به دنبال اندیس مناسب $i > ۱$ هستیم به طوری که $E_۱$ با M_i و F_i سازگار باشد و E_i با $M_۱$ و $F_۱$. آن وقت $E_۱$ را با E_i جابجا می‌کنیم.

حداکثر $n/۴$ اندیس i وجود دارد به طوری که $E_۱$ با M_i سازگار نباشد. همینطور حداکثر $n/۴$ اندیس i وجود دارد به طوری که $E_۱$ با F_i سازگار نباشد. پس حداکثر $n/۲$ اندیس i وجود دارد که E_i با یکی از M_i یا F_i سازگار نباشد. توجه شود که ۱ نیز یکی از این اندیس‌هاست. به طور مشابه حداکثر $n/۲$ اندیس i وجود دارد که $M_۱$ یا $F_۱$ با E_i سازگار نباشد. این دو مجموعه اندیس اخیر هرکدام شامل ۱ هستند و حداکثر $n/۲$ عضو دارند. پس اجتماعشان شامل تمام اندیس‌ها نیست. پس حداقل یک اندیس مطلوب وجود دارد.

۶.۲. پاسخ مسئله‌ی ششم. ابتدا توجه کنید که $I = p \cdot I$؛ اگر $x \in I$ آنگاه x بر p بخش‌پذیر است، پس می‌توان نوشت $x = py$. اما y باید بر همه‌ی توان‌های p بخش‌پذیر باشد، پس $y \in I$.

مولدهای I را بصورت $x_۱, \ldots, x_m$ در نظر بگیرید. پس $x_i = py_i$، و $y_i \in I$ به فرم $y_i = a_{i۱}x۱ + \ldots + a_{im}x_m$ است. ماتریس $[a_{ij}]$ را با A نشان دهید. x را بردار ستونی $(x_۱, \ldots, x_m)$ در نظر بگیرید. داریم $(I - pA)x = ۰$ که با ضرب در ماتریس الحاقی $I - pA$ بدست می‌آوریم $\det(I - pA)x = ۰$. اگر I ناصفر باشد آنگاه x نیز ناصفر است، و از آنجایی که R حوزه صحیح بود بدست می‌آید $\det(I - pA) = ۰$. اما این دترمینان به فرم $۱ + pz$، $z \in R$ است و از صفربودنش نتیجه می‌شود که p وارون‌پذیر است. تناقض.

برای قسمت دوم، اگر Q یک ایده‌آل اول سره داخل (p) باشد، آنگاه هر $x \in Q$ به فرم $px_۱$ است. چون $p \notin Q$ لزوماً $x_۱ \in Q$ و در نتیجه به فرم $px_۲$ است. دوباره $x_۲ \in Q$ و به فرم $px_۳$ است و الی آخر. بنابراین هر $x \in Q$ بر همه‌ی توان‌های p بخش‌پذیر است، در نتیجه عضوی از $I = ۰$ است؛ یعنی $Q = ۰$.

* دانشجوی کارشناسی‌ارشد ریاضی، دانشگاه صنعتی شریف