# 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 ـ 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 ـ 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 دوست‌ام، 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 $\mathcal{NP}$_کامل 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.

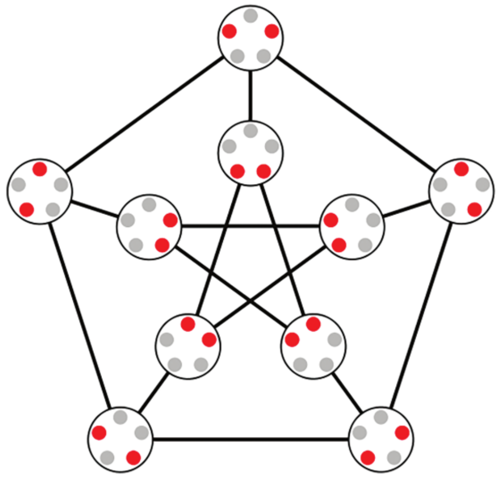
این را هم اضافه کنم، من روی سوالی از اردوش فکر می‌کردم که در نهایت به این لم رسیدم. آن زمان در یک مدرسه‌ی تابستانی در ایالت اوهایو همراه اردوش بودم؛ که ما مسأله را حل کردیم، و یک مقاله‌ی طولانی در مورد آن مسأله و مسائل مرتبط نوشتیم، از جمله این لم. اردوش متوجه شد که این لم بیش از یک لم برای این مورد خاص بود. با این حال او می‌خواست که لم با نام من شناخته شود. در حالی که به طور معمول باید لم موضعی اردوش–لواس 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 می‌کند، 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 [1] را به وسیله‌ی الگوریتمی که تقریبی از کوچک‌ترین بردار مشبکه [2] 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 [3] و الکساندر شریور [4] مشغول کار بر روی کاربردهای روش بیضی [5] 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 [6] مسائل معادل زمان چندجمله‌ای بودند. اما موردی وجود داشت که الگوریتم روی آن کار نمی کرد. و آن زمانی بود که جسم محدب [7] 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 [8] 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 [9] و اودلیزکو [10] این را یافتند که الگوریتم برای شکستن سیستم رمز کوله‌پشتی [11] 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 [12] با انجام محاسبات عددی زیادی توسط این الگوریتم، توانستند حدس مرتنز [13] درباره‌ی تابع زتای ریمان [14] 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، شروبر 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 شربور 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 می‌کنید، 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 نمی‌آورم، 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 شاخه‌های 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 غیره‌ـ 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 می‌کنندـ 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 $\epsilon$ مثبتی دلخواهی مساله را ثابت کند.

یک سال پیش دانیلا کوهن [7] و دانشجویان‌اش توانستند اثبات‌اش کنند؛ حداقل برای $n$های به اندازه کافی بزرگ. یکی از ویژگی‌های این حدس این بود که شما آن را براساس $n$های کوچک بیان کردید؛ ولی در نهایت برای $n$های 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 شگفت آور 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 می کنید 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