اثباتهای ریاضی: پیدایش شك موجّه•

جینا کولاتا
ترجمهٔ سعید ذاکری

از چهل سال پیش ریاضیدانها پی برده‌اند که تعداد بیشماری از گزاره‌ها در ریاضیات تصمیم‌ناپذیرند ــ یعنی صادق یا کاذب بودن آنها را نه می‌توان ثابت و نه می‌توان رد کرد. این نتیجهٔ نگران کننده عواقب فلسفی عمیقی برای ریاضیدانها در برداشت، چراکه در مقابل روشهای شکست‌ناپذیر پیشین اثبات، سدی در درون ریاضیات ایجاد می‌کرد. با این حال، ریاضیدانها به‌تدریج به‌اینجا رسیدندکه این‌نتیجه را بپذیرند واعتقاد داشته باشندکه نشان دادن تصمیم‌پذیری یك گزاره، به‌مثابهٔ نشان دادن امکان اثبات آن است. اما این‌روزها، گره دیگری در کار مسألهٔ تصمیم‌ناپذیری پدید آمده است. پژوهشگران دریافته‌اندکه حتی گزاره‌هایی‌که از لحاظ نظری تصمیم‌پذیرند ممکن است اثباتی چندان طولانی داشته باشند کــه نگاشتن‌آن، چه‌به‌دست‌آدمی‌وچه به‌یاری‌کامپیوتر، هرگز ممکن نباشد.

برای فائق‌آمدن برمسألهٔ اثباتهای طولانی، مایکل رابین، از دانشگاه عبری اورشلیم، پیشنهاد می‌کندکه ریاضیدانها تعریفشان‌از اثبات را تعدیل‌کنند. در بسیاری حالات، اگرکامپیوتر مجاز باشد که با احتمال ازپیش‌تعیین‌شدهٔ ناچیزی مرتکب خطا شود، شاید بشود گزاره‌ها را به‌کمك‌آن "اثبات" کرد. رابین‌کارایی این اندیشه را به‌یاری روش جدیدی نشان دادکه می‌تواند با احتمال خطای یك درمیلیارد، اول بودن یا نبودن یك‌عدد به‌دلخواه بزرگ را به‌سرعت تعیین‌کند.[1] روش اثبات رابین، از آنجا که در تقابل بــا مفاهیم عمیقاً پذیرفته‌شدهٔ صدق وزیبایی در ریاضیات‌قرارمی‌گیرد، موجب دامن‌زدن‌به‌بحث‌وجدلهای پرحرارتی میان پژوهشگران شده‌است.

رابین هنگامی درمورد سودمندی تعریف جدیدی برای‌اثبات متقاعد شد که تاریخچهٔ تلاشهایی راکه برای اثبات قضایا به‌کمك کامپیوترصورت گرفته بود، موردتوجه قرارداد. حدود۵ سال‌پیش، اشتیاق زیادی به‌این‌نوع اثبات قضایا نشان داده می‌شد. این‌علاقه در ارتباط با پژوهش در زمینهٔ هوش مصنوعی و به‌ویژه مسائلی‌از قبیل طــراحی شیوه‌هــای اتــوماتیك اشکال‌زدایــی برنــامه‌های کامپیوتری پدیدآمد. لکن، پژوهشگران به‌زودی دریافتندکه اثبات‌حتی ساده‌ترین‌گزاره‌هامستلزم‌صرف‌وقت‌غیرقابل‌قبولی‌توسط کامپیوتراست. رابین‌معتقداست‌که‌این‌عدم‌توفیق‌دراثبات‌اتوماتیك، قضایاممکن‌است ناشی‌ازدرازی‌اجتناب‌ناپذیراثبات بسیاری‌ازگزاره‌های تصمیم‌پذیر باشد ونه فقدان هوش‌وظرافت درطراحی‌الگوریتمهای‌کامپیوتری.

۱. رابین این نتیجــه را در همایش "گرایشهای جدید و نتایج تازه در باب الگوریتمها و پیچیدگی" کــه در دانشگاه کارنگی ـ ملون درپیتسبورگ از ۷ تا ۹ آوریل ۱۹۷۶ برگزارشد، عرضه‌کرد.

حــدود ۴ سال پیش، آلبرت میر[1] از استیتو تکنولــوژی ماساچوست(MIT) نشان‌دادکه اثبات‌کامپیوتری برخی گزاره‌های دلخواه در یك دستگاه منطقی بسیار ساده، الزاماً به‌قدری طولانی است که‌امکان‌ناپذیراست. دستگاه موردنظرما، مرکب ازمجموعه‌هایی ازاعداد صحیح ویك عمل حسابی ــ جمع عدد ۱ با اعداد صحیح ــ است. از مدتها پیش ریاضیدانها می‌دانستندکه درستی یا نادرستی هرگزاره را در این دستگاه منطقی‌می‌توان در تعدادی متناهی‌مرحله ثابت‌کرد، اما میر نشان داد که تعداد این مراحل می‌تواند نمایی تکراری باشد، یعنی‌توانی ازیك توان از یك توان ... . گزاره‌ای به‌طول n می‌تواند به

$$2^{2^{\cdot^{\cdot^{2}}}}$$

مرحله نیازمند باشد، که در آن تعداد توانهای۲ متناسب با n است.

روش میر در نشان دادن اینکه حداکثر طول اثبات برخی‌از گزاره‌ها چقدر باید باشد، اکنون در دستگاههای منطقی دیگر نیز به‌کار رفته‌است. او ودیگران برای تقریباً همهٔ قضایای تصمیم‌پذیر معمول در منطق، احــکام مشابهی در باب امکان ناپذیری اثباتهــا به‌دست آورده‌اند.

حدود ۲ سال پیش، میر و لری‌استاکمیر[2]، که اکنون در یکی از مراکز تحقیقاتی آی بی‌ام‌کار می‌کنند، نتیجهٔ ملموستری دربارهٔ طول اثباتهای کامپیوتری به‌دست آوردند. اینان پژوهش خود را بر روی دستگاه منطقی اولیه‌ای کــه میر برای آن نتایجی درمورد امکان‌ناپذیری به‌دست آورده بود متمرکز، و این پرسش را مطرح کردندکه اثبات گزاره‌هایی با چه طول کاملاً ناممکن است. آنها "کاملاً ناممکن" را اثباتی تعریف کردندکه محتاج شبکهٔ کامپیوتری با $10^{10^{123}}$ مؤلفه باشد، که، بنا به‌نظرمیر، تخمینی از تعداد ذرات در مقیاس پروتونی است که می‌تواند به‌طور چگال جهان شناخته شده را پرکند. سپس، نشان دادندکه برای‌اثبات گزاره‌ای دلخواه‌مرکب از حدود ۶۱۷ نماد، کامپیوتر محتاج $10^{10^{123}}$ مؤلفه خواهد بود.

به‌زعم رابین، مسأله‌ای‌که درمورد اثبات وجود داردابن‌است که می‌خواهیم اثبات، بدون احتمال خطا درست باشد. ولی‌انسانها پیوسته در ریاضیات ودیگر موضوعات دچار خطا می‌شوند. شاید بدین‌دلیل‌است‌که افرادی‌که درگیرحل مسأله‌اند، مایل‌اندکار خود را به‌اتمام برسانند، حال آنکه کامپیوتر اغلب به‌خاطر کمی وقت

1. Albert Meyer 2. Larry Stockmeyer

کارخود را متوقف می‌کنند. بنابراین، رابین به‌جستجوی مواردی پرداخت که در آنها اگر به کامپیوتر اجازهٔ خطا کردن ندهیم نمی‌تواند کار خود را تمام کند، ولی اگر خطا کردن را مجاز بشماریم کارخود را به‌اتمام خواهد رساند. این موضوع او را به نتیجه‌ای در باب اعداد اول هدایت کرد.

آزمون رابین برای اعداد اول بر مبنای نتیجه‌ای است که گری‌میلر از دانشگاه واترلوی کانادا اخیراً به‌دست آورده است. میلر دریافت که اگر n عددی اول باشد، هرعدد صحیح بین ۱ و n به‌آزمون ریاضی خاصی پاسخ مثبت می‌دهد. بنابراین اگرهرچنین عدد صحیحی به‌آزمون پاسخ مثبت ندهد، n عددی اول نخواهد بود. علاوه براین، میلر نشان داد که لازم نیست این آزمون را برای همهٔ اعداد صحیح بین ۱ و n انجام دهیم. کافی است آن را برای اعداد صحیح بین ۱ و عددی مانند m که به n بستگی دارد به کار بندیم. چنانچه n اول نباشد، یکی از اعداد صحیح بین ۱ و m به‌آزمون پاسخ منفی خواهد داد. مزیت آزمون میلر این است که نسبتاً سریع عمل می‌کند، لکن این عیب را هم دارد که با افزایش n، تعداد اعداد صحیحی که باید آنها را آزمود افزایش می‌یابد.

رابین دریافت که اگر n عددی اول نباشد، دست‌کم نیمی از اعداد صحیح بین ۱ و n به‌آزمون میلر پاسخ منفی خواهند داد. بنابراین، مادامی که n اول نباشد، اگرعددی رابین ۱ و n به‌تصادف انتخاب و آن را آزمایش کنیم، احتمال به‌دست‌آوردن پاسخ منفی دست‌کم ۱/۲ خواهد بود. اگر در همین وضعیت، یعنی وقتی که n اول نیست، دو عدد بین ۱ و n را به تصادف انتخاب و آنها را آزمایش کنیم، احتمال به‌دست آوردن پاسخ منفی درمورد یکی از آن دو دست‌کم ۳/۴ است، و اگر ۳۰ عدد را به‌تصادف انتخاب کنیم، احتمال به‌دست‌آوردن پاسخ منفی برای یکی از آنها دست‌کم $1-(1/2)^{30}$ خواهد بود. در این‌صورت احتمال اینکه همهٔ این ۳۰ عدد بین ۱ و n که تصادفاً انتخاب شده‌اند، به‌آزمون پاسخ مثبت دهند، تنها $(1/2)^{30}$ یا ۱ در میلیارد است. در این روش احتمالاتی، با آزمودن تعداد نسبتاً اندکی عدد صحیح سروکاردایم. تعداد اعداد صحیحی که باید آنها را بیازماییم به n وابسته نیست، بلکه به‌احتمال خطای موردنظرما بستگی دارد.

آزمون احتمالاتی رابین بسیار سریعتر از آزمونهای دقیق است. آزمونهای دقیق چندان طولانی‌اند که فقط اعداد بزرگتراز 10^{60}ی که تا به‌حال آزموده شده‌اند، ازشکل خاصی برخوردارند. چنین اعدادی را رابین می‌تواند ظرف حدوداً ۱ ثانیه به‌کمك کامپیوتر آزمایش کند. به‌عنوان نمونه‌ای از توان بالقوهٔ این‌روش، رابین و وان‌پراپ[1] از انستیتوتکنولوژی ماساچوست نشان دادند که عدد $2^{593}-2^{400}$ به‌این‌آزمون پاسخ مثبت می‌دهد وبنابراین "برای همهٔ مقاصد عملی" عددی اول‌است.

پیتر واینبرگرکه اکنون در آزمایشگاههای بل‌کارمی‌کند، این پرسش را مطرح می‌کند که اول بودن "برای همهٔ مقاصد عملی" یعنی چه؟ تولید اعداد تصادفی، و محاسبهٔ تبدیلهای سریع فوریه (FFT)، از جمله موارد استفاده از اعداد اول بزرگ است. واینبرگرمدعی‌است که وجود روشهای دقیق برای یافتن اعداد اول بزرگ برای چنین کاربردهایی کافی است. او در پاسخ به‌ادعای رابین مبنی براینکه روشهای احتمالاتی برای اثبات ضروری‌اند، می‌گوید: "اگرتنها یك مثال واقعی به‌من نشان بدهید، من متقاعد خواهم شد."

نظر دانلدکنوت از دانشگاه استنفرد در این باره این است که مثال رابین نقداً کاربردهای جدیدی ندارد؛ با این‌حال، وقتی که راهی برای محاسبهٔ چیزی پیدا شد، همیشه یکی هم یافت می‌شود که‌کاربردی برای آن پیدا کند. او مسائل دشوار دیگری را مانند ردهٔ مسائلی که در علوم کامپیوتر مسائل NP تمام نامیده می‌شوند، نامزدهای مناسبی برای روشهای احتمالاتی می‌داند. با وجود این، او معتقداست که آثاراولیهٔ نتیجهٔ رابین، بیشترجنبهٔ زیباشناسی‌دارد تا عملی؛ و در زمینهٔ زیباشناسی‌است که بگومگو آغازمی‌شود.

یك نمونه از واکنش بسیاری از ریاضیدانها را می‌توان در سخنان کسی یافت که می‌گفت نمی‌تواند روش احتمالاتی اثبات را بپذیرد، چراکه "شکوه ریاضیات در این‌است که روشهای موجود اثبات ریاضی، اساساً بری از خطا هستند". دانلد گراهام از آزمایشگاههای بل و دیگران، درپاسخ می‌گویندکه آنها به‌نتایجی که از روشهای احتمالاتی نظیر آزمون اعداد اول رابین به‌دست می‌آیند بیشتر اطمینان دارند تا به‌اغلب اثباتهای ریاضی ۴۰۰ صفحه‌ای. بررسی صحت چنین اثباتهایی غالباً نزدیك به ناممکن است، ومناظره‌ای پیرامون یك نتیجهٔ خاص درنظریهٔ هموتوپی، که مبحثی‌است در توپولوژی، گواهی براین مدعاست. دراین مناظره، یکی از پژوهشگران با اثبات یك گزاره، و دیگری با اثباتی از نقیض آن شرکت کرده بود. هردواثبات طولانی‌وفوق‌العاده پیچیده بودند؛ از این رو، آن دو اثباتهای خود را به یکدیگر دادند تا هر یك کار دیگری را بررسی کند. هیچ یك از آن دو نتوانست اشتباهی در اثبات دیگری بیابد. دراین میان نفرسومی پیدا شد و اثبات طولانی دیگری بر له یکی از دو اثبات اصلی ارائه داد. بنابراین، نتیجه ۲ بر ۱ به‌نفع یکی‌از اثباتها شد، اما مسألهٔ اصلی هنوز حل‌نشده باقی‌مانده‌است.

گراهام نگران این‌موضوع است که در ریاضیات، یادست‌کم در برخی زمینه‌ها مثل نظریهٔ گروهها، اثباتهای طولانی بجای استثنا دارند به‌صورت قاعده درمی‌آیند. به‌نظراواین وضعیت‌ممکن است نتیجهٔ این باشدکه در مقایسه با تعدادکل گزاره‌های ریاضی جالب ممکن، تعداد نسبتاً اندکی گزارهٔ جالب با اثبات کوتاه‌وجود دارد؛ و روز به‌روز تعدادکمتر و کمتری گزارهٔ با اثبات کوتاه‌برای بررسی باقی می‌ماند. او و پال اردیش معتقدند که امروزه حجم برخی از اثباتهای طولانی منتشره، درحد مقدارکل اطلاعاتی‌است که مغز آدمی می‌تواند بپذیرد. بنابراین، گراهام و دیگران براین عقیده پا می‌فشارندکه تحقیق صحت قضایا به‌کمك کامپیوتر ممکن است بخشی از ریاضیات فردا باشد، و ریاضیدانها ممکن است مجبور شوند در تصور خود از آنچه‌که دلیل‌کافی و محکم برای صحت یك گزاره به‌شمار می‌آید، تجدیدنظرکنند.

1. Vaughn Perapp

• Gina Bari Kolata, "Mathematical proofs: the genesis of reasonable doubt," *Science*, (4243) **192** (1976) 989-990.