الگوریتم‌ها در جیب شما چه می‌کنند؟

چگونه از الگوریتم‌ها در حل مسائل زندگی امروز استفاده می‌شود؟

نازنین حسن‌نیا
عکاس: شادی رضائی

برای حل یک مسئله، دچار مشکل شده بودم. یکی از دوستانم که متوجه مشکل من شده بود، گفت: چرا از رایانه استفاده نمی‌کنی نرم‌افزاری هست که این مسئله را به راحتی حل می‌کند.

مشکل من به راحتی حل شد، اما سؤالی در مغزم جوانه زد. چه مسیری طی شد تا به این نرم‌افزارها و ماشین‌حساب‌های پیشرفته برسیم. ممکن است این سؤال برای شما هم مطرح باشد. برای پاسخ به سؤالم با دکتر امیر دانشگر، دکتر سلمان ابوالفتح‌بیگی، دکتر امید اعتصامی، دکتر شهرام خزایی و دکتر زینب مالکی گفت‌وگویی کردم، در این گفت‌وگو به این سؤال‌ها جواب داده شده است.

الگوریتم چیست؟

«الگوریتم»، روش گام‌به‌گام برای پاسخ‌گویی به یک سؤال است که در هر گام آن، یکی از چند عملِ مشخص و از پیش تعیین شده اجرا می‌شود. برای مثال روشی که برای ضرب دو عدد چندرقمی می‌شناسیم، «الگوریتم ضرب» است. اگر دو عددی که در هم ضرب می‌شوند تغییر دهیم، حاصل‌ضرب عوض می‌شود، اما در نوعِ عملیاتی که انجام می‌دهیم یا در ترتیب انجام آن‌ها، تغییری به‌وجود نمی‌آید.

۱۴۵
× ۲۷
۱۰۱۵
+۲۹۰۰
۳۹۱۵

دانشگر: در طول تاریخ، بشر، همیشه به‌دنبال ابزارهایی بوده تا انجام محاسبات را برایش راحت‌تر کند؛ مثل چرتکه یا ماشین‌حساب. محاسبات ماشینی یا «اتوماتیک (خودکار)» بسیار جذاب بود و ماشین‌حساب‌ها دائم پیشرفت کردند و عملیات جدید به آن‌ها اضافه شد. اوایل قرن بیستم، ریاضی‌دانِ بزرگی به‌نام «دیوید هیلبرت» این سؤال را مطرح کرد که آیا می‌توان حل مسئله‌های ریاضیات را خودکار کرد؟ یعنی آیا می‌توان ماشینی ساخت که بتواند درستی یا نادرستی هر جملهٔ ریاضی را که به آن می‌دهیم مشخص کند؟ او می‌دانست برای اینکه ماشین بتواند یک مسئله ریاضی را حل کند، باید بتوان برای حل آن مسئله، یک الگوریتم نوشت.

ریاضی‌دان نامی «کورت گودِل» نشان داد که با تعداد متناهی عمل و قانون استنتاج، گزاره‌های درستی وجود دارند که درستی آن‌ها را نمی‌توان به‌صورت الگوریتمیک بررسی و تأیید کرد. همچنین «آلن تورینگ» نشان داد که سؤال‌هایی وجود دارند، که برای پاسخ‌گویی به آن‌ها هیچ الگوریتمی وجود ندارد. پس، در حل مسائل ریاضی، استفاده از فکر خودمان الزامیست! از این رو بود که دانشمندان زیادی برای تعیین مفهوم دقیق الگوریتم به تعیین

تعریف دقیقی از مفهوم «محاسبه» روی آوردند که تاریخچهٔ جذابی دارد. در این سیر تاریخی، نکتهٔ جالب توجه این است که تلاش‌های این‌چنینی در زمانی رخ داد که هیچ دستگاه یا مفهومی شبیهِ آنچه امروزه «کامپیوتر» می‌نامیم اصلاً وجود نداشت!

● **ابوالفتح‌بیگی:** هشتاد سال پیش در دههٔ ۴۰ میلادی، اولین کامپیوتر ساخته شد. پس از آن ساخت این نوع ماشین‌های حسابگر بزرگ (کامپیوترها یا رایانه‌ها) سرعت گرفت. هر رایانه تواناتر از رایانه‌های قبل از خودش بود، یعنی می‌توانست مسئله‌های قبلی را در زمان کوتاه‌تر حل کند. همچنین می‌توانست مسائل جدیدی را حل کند که رایانه‌های قبلی نمی‌توانستند. هم‌زمان با پیشرفت رایانه‌ها، الگوریتم‌های محاسبه نیز پیشرفت می‌کردند. یعنی الگوریتم‌های جدیدی طراحی می‌شد که با کمک ابزارهای ریاضی، «کاراتر» (یا کارآمدتر) از الگوریتم‌های قبلی بود.

ارتباط رایانه‌ها با هم

● **برهان:** به تدریج لازم شد که رایانه‌ها بتوانند از اطلاعات یکدیگر استفاده کنند. مدتی این ارتباط تنها از طریق سیم و کابل و یا انواع دیسک‌ها انجام می‌شد. تا اینکه با پیشرفتِ فناوری، ارتباط بی‌سیم بین رایانه‌ها برقرار شد و کم‌کم شبکهٔ جهانی اینترنت، همهٔ نقاط دنیا را به هم مرتبط کرد. در این زمان، مسئلهٔ رمزنگاری و ارتباط ایمن میان رایانه‌های مختلف، جدی‌تر از قبل شد. برای مثال امروزه در جیب هر کدام از ما یک کارت عابر بانک وجود دارد. هر بار که با کارت عابر بانک خود کار می‌کنیم، اتفاق بسیار جالبی می‌افتد. ما رمز کارتمان را به دستگاه عابر بانک وارد می‌کنیم؛ اما در همان لحظه، این عدد تبدیل به یک رمز می‌شود. هیچ‌کس، حتی رایانه‌های بانک یا کارمندان بانک، رمز ما را نمی‌دانند و نباید بدانند. رایانه‌های بانک، بدون اینکه بدانند رمز ما چیست، بررسی می‌کنند که آیا رمز را درست وارد کرده‌ایم یا نه!

اما چطور چنین کاری ممکن است؟

● **دانشگر:** فرض کنید تعدادی مداد روی میز است. شکل آن‌ها هم شبیه به هم است؛ اما بعضی قرمز و بعضی آبی می‌نویسند. یک شخص نابینا از ما می‌خواهد که یک مداد آبی در دست راست و یک مداد قرمز در دست چپ او بگذاریم. او مدادها را نمی‌بیند، اما می‌خواهد مطمئن شود که ما رنگ‌ها را درست به او داده‌ایم. او دست‌هایش را زیر میز می‌برد و با احتمال یک دوم، مدادها را در دست خود جابه‌جا می‌کند. سپس آن‌ها را روی میز می‌آورد و می‌پرسد «مداد آبی در کدام دست من است؟». و این آزمون را چندین بار تکرار می‌کند. نکته اینجاست که اگر ما مدادهای هم‌رنگ به او داده باشیم، نمی‌توانیم جواب همهٔ سوالات را به درستی بدهیم، اما اگر از اول صادقانه عمل کرده باشیم، همهٔ پاسخ‌هایمان درست خواهد بود. پس فرد نابینا، بدون اینکه مدادها را ببیند، می‌تواند مطمئن شود که سرش کلاه نرفته است! رایانهٔ بانک، با روش‌هایی مشابه روش فرد نابینا، بدون اینکه رمز کارت ما را بداند، می‌تواند از درست بودن آن مطمئن شود.

● **برهان:** کمی دربارهٔ کارهای خودتان بگویید. در ایران چه کارهایی در حال انجام است؟

● **ابوالفتح‌بیگی:** حوزهٔ تحقیقاتی من «محاسباتِ کوانتومی» است. همان‌طور که پیشتر گفته شد، رایانه‌ها روزبه‌روز پیشرفت می‌کنند. اگر روزی رایانه‌هایی ساخته شوند که قطعات و مدارهایشان به‌جای فیزیکِ کلاسیک، براساس فیزیک کوانتومی کار کنند، تحول بزرگی اتفاق می‌افتد. این رایانه‌ها آن‌قدر قوی خواهند بود که بعضی از محاسبات پیچیدهٔ امروزی را به سرعت و در زمان‌های کوتاه انجام می‌دهند. کارِ من این است که الگوریتم‌هایی طراحی کنم که روی رایانه‌های کوانتومی قابل اجرا باشد و کاراتر از الگوریتم‌های امروزی باشد. از سوی دیگر مسائلی که «الگوریتم کارا» برای حل‌شان وجود ندارد، کمک بزرگی به علوم رایانه

می‌کنند. متخصصین، از این مسائل برای رمزنگاری استفاده می‌کنند، چون می‌دانند که اگر کسی بخواهد این رمز را بشکند یا پیدا کند، زمان بسیار زیادی لازم است. کارِ دیگرِ من این است که مسائلی پیدا کنم که حتی با رایانه‌های کوانتومی هم الگوریتم‌های کارا برای حل‌شان وجود نداشته باشد. اگر ثابت کنیم الگوریتم‌هایی که روی رایانهٔ کوانتومی قابل اجرا هستند، نمی‌توانند به‌طور کارا این مسئله‌ها را حل کند، آنگاه می‌توانیم از این مسئله‌ها برای رمزگذاری استفاده کنیم. من در تحقیقاتم از شاخه‌های مختلف ریاضی مثل «آنالیزِ ریاضی»، «جبرِ خطی»

و شـــاخه‌هایی از علـــوم کامپیوتر مثل «پیچیدگـــیِ محاســـبات»، «طراحی الگوریتم» و... استفاده می‌کنم.

● **اعتصامـــی:** من در گذشـــته، هم کارهای نظری می‌کردم و هم کارهایی کاربردی که شرکت‌های کامپیوتری و مخابراتی، برای رفع مشکلات خود به آن نیاز داشتند. از وقتی به ایران آمدم، بیشتر به حل مسائل نظری می‌پردازم. به‌تازگی دیدم کـــه در ایران، بعضی شـــرکت‌ها نیازهای خود را به الگوریتم‌های جدید مطرح می‌کنند و از متخصص‌ها کمک می‌خواهند.

● **ابوالفتح‌بیگی:** بـــرای مثال یک فروشـــگاه اینترنتی، نیاز به الگوریتمی دارد که تشخیص دهد هر خریدار، چه کالاهایـــی را نیاز دارد و این کالاها را به او معرفی کند. مســـئلهٔ شگفت‌انگیزی اســـت! رایانه آن شـــرکت می‌خواهد با کمک یک الگوریتم، تشخیص دهد که من چه کالایی نیـــاز دارم و همان کالا را برای من تبلیغ کنـــد! این الگوریتم چه اطلاعاتی از مـــن دارد؟ می‌داند که من یک ماه پیش یک لپ‌تاپ با مارک خاص خریده‌ام و مثلاً امروز یک شلوار قهوه‌ای. پس خوب است که لوازم جانبی آن لپ‌تاپ مثل کابل‌ها یا مثلاً ســـاعت یا گوشی هوشمندی که به آن لپ‌تاپ وصل می‌شـــود، حافظهٔ مناســـب آن و ... را به مـــن معرفی کند. همچنین در بین لباس‌های ایـــن فروشگاه، یک پیراهن کرم رنگ یا یک کت هماهنگ با شلواری که خریده‌ام وجود دارد. تبلیغ این لباس‌ها هم ممکن است مرا وسوسه کند تا خرید بیشتری از فروشگاه انجام دهم. این‌ها تبلیغاتِ هوشمند و هدفمند برای این فروشـــگاه اســـت. حالا اگر الگوریتم این شرکت، مناسب نباشد، و مثلاً امـــروز و روزهای بعـــد، تبلیـــغ همان لپ‌تاپ یـــا همـــان شلواری که خریـــده‌ام را برایـــم بفرستد، در من احساس مزاحمـــت ایجاد می‌کند و شاید دفعهٔ بعد، فروشگاه اینترنتی دیگری را برای خرید انتخاب کنـــم. پس میزانِ ســـود این شـــرکت، به الگوریتم تبلیغ این شرکت مربوط می‌شود.

● **مالکی:** من روی مسئله‌ای کار می‌کنم که مربـــوط به دانش زیست‌شناســـی اســـت. در بدنِ ما پروتئین‌های زیادی وجود دارند. آن‌ها هر کدام کاری انجام می‌دهند و بر کارِ پروتئین‌های دیگر اثر می‌گذارند. اگر این پروتئین‌ها کارِ خود را به‌درستی انجام ندهند و ارتباط آن‌ها با پروتئین‌های دیگر از حالتِ عادی خارج شود، ممکن است غدهٔ سرطانی تشکیل شود. ما الگویی می‌سازیم که در آن هر پروتئین را با یک نقطه و ارتباط میان هر دو پروتئین را با یک پاره‌خط بین آن دو نقطه نشان می‌دهیم. با این کار شبکه‌ای به‌دســـت می‌آید که می‌توانیم آن را با کمک ابزارهای ریاضی بررســـی کنیم تا بفهمیم در چه قســـمت‌هایی، امکان دارد غده‌های ســـرطانی تشکیل شوند و رشـــد کنند. تعداد نقاط و پاره‌خط‌ها در این شبکه بسیار بســـیار زیاد است و بررســـی آن، تنها با کمک برنامه‌های رایانه‌ای امـــکان دارد. گاهی وقت‌ها هم لازم می‌شود که شبکهٔ پروتئین‌های یک قسمت از بدن را با شبکهٔ پروتئین‌های قســـمت دیگری از بدن مقایسه کنیم. چون این شبکه‌ها خیلی بزرگ هستند، مقایســـهٔ آن‌ها با هم از مسائلِ سختِ علوم رایانه است. بخش دیگری از کارِ ما این است که الگوریتم‌هایی بنویسیم که بتوانند این مقایسه را انجام دهند.

● **خزایی:** من در حـــوزهٔ رمزگذاری کار می‌کنم. رمز نگاری برای هدف‌های مختلف امنیتی استفاده می‌شود. همهٔ کســـانی‌که در این حوزه کار می‌کنند، به‌دنبال روش‌هایی می‌گردند که بتوان از کانال‌های مختلـــف، مانند اینترنت، اطلاعات را به‌صورت محرمانه رد و بدل کرد. فرض کنید می‌خواهید با دوستی که در شـــهری دیگـــر زندگی می‌کند، نامه‌نگاری کنیـــد؛ و نمی‌خواهید هیچ فردِ دیگری از مطالبِ نامهٔ شـــما باخبر شود. به پستچی هم اعتماد کافی ندارید. یک راه‌حل که مال قبل از میلاد مسیح است، این است که یک‌بار که دوست‌تان را می‌بینید، باهم روی یک کلید (کلمه عبور) توافق کنید و پـــس از آن، همهٔ نامه‌هایتان را با آن کلید توافق شده رمز کنید. این کار توسط یک الگوریتم، که الگوریتم رمزنگاری نامیده می‌شود، انجام می‌شود. دوست شما می‌تواند با استفاده از همان کلید، متن رمزشـــدهٔ شـــما را رمزگشـــایی کند و بـــه محتوای اصلی پیام دست یابد. اگر الگوریتم رمزنگاری به خوبی طراحی شـــده باشد، هیچ فرد دیگری که کلیـــد را نداند، نمی‌تواند از نوشته‌های رمزی شما سر درآورد؛ یعنی از روی متن‌های رمزشده، نمی‌تواند در مورد متن‌های اصلی اطلاعات کســـب کند. حدود چهل ســـال قبل ســـؤالی در مجامـــع علمی مطرح شـــد که علم

رمزنگاری را متحول کرد: آیا ممکن است که شما و دوستتان، بدون اینکه یکدیگر را دیده باشید، بتوانید نامه‌های رمزی برای یکدیگر ارسال کنید به طوری که هرکدام بتواند نامهٔ دیگری را رمزگشایی کند ولی مطمئن باشید که هیچ فرد دیگری نمی‌تواند نوشته‌های رمزی شما را بخواند؟ پاسخ این سؤال مثبت است. الگوریتم‌های رمزنگاری که این امکان را فراهم می‌کنند، تحت عنوان سیستم رمز نامتقارن (یا کلید عمومی)، شناخته می‌شوند. در مقابل، به الگوریتم‌های رمزنگاری سنتی، سیستم رمز متقارن (یا کلید خصوصی) اطلاق می‌شود. امروزه، تعدادی مؤسسهٔ بین‌المللی هستند که برای طراحی الگوریتم‌های رمزنگاری مسابقه‌هایی برگزار می‌کنند. افراد از سراسر دنیا برای آن‌ها الگوریتم می‌فرستند.

کارایی
(یا کارآمدی) محاسبه
یعنی چه؟ می‌خواهیم ۲۴ را در ۵۸ ضرب کنیم. دانش‌آموز دوم ابتدایی، عدد ۵۸ را ۲۴ بار پشت سر هم می‌نویسد و بعد آن‌ها را با هم جمع می‌کند؛ ولی دانش‌آموز چهارم ابتدایی این دو عدد را زیر هم می‌نویسد و با الگوریتم ضرب آن‌ها را در هم ضرب می‌کند. روش دوم «کارایی» بیشتری دارد، چون خیلی سریع‌تر ما را به جواب می‌رساند. «کارایی» یعنی اینکه با انجام عملیات کمتر و در زمان کوتاه‌تر به جواب مسئله برسیم.

این مؤسسه‌ها، الگوریتم‌ها را ارزیابی می‌کنند و الگوریتم‌های خوب را معرفی می‌کنند و در اختیار همه در همه‌جای دنیا قرار می‌دهند. به این ترتیب این الگوریتم‌ها ممکن است در جایی برای حل یک مسئله تحقیقاتی و یا در صنعت استفاده شود. با گذشت زمان، افراد جدید این الگوریتم‌های برتر را بازبینی و بازسازی می‌کنند و الگوریتم‌ها بهتر و بهتر می‌شوند. در دوره دکترا، بخشی از کار پژوهشی من، ارزیابی الگوریتم‌هایی بود که باید امنیت آن‌ها برای استفادهٔ بین‌المللی مورد ارزیابی قرار گیرد. بعضی از نتایج ما حاکی از مقاومت بالای برخی از این الگوریتم‌ها بودند که هم اکنون به عنوان استاندارد در برخی از شبکه‌های مخابراتی استفاده می‌شوند. البته همهٔ کارهای من این‌قدر کاربردی نیست و تحقیقات نظری هم انجام می‌دهم.

دکتر امیر دانشگر:
متولد ۱۳۴۶ / کارشناسی: مهندسی برق دانشکده مهندسی برق دانشگاه صنعتی شریف/ کارشناسی ارشد: ریاضی محض دانشکده ریاضی دانشگاه علم و صنعت ایران/ دکتری ریاضی دانشکده علوم ریاضی دانشگاه صنعتی شریف/ عضو هیئت علمی دانشگاه صنعتی شریف / علائق تحقیقاتی: نظریه رسته‌ها، نظریه سیستم‌ها، ترکیبیات و نظریه گراف، علوم کامپیوتر، رمزنگاری.

دکتر شهرام خزایی:
متولد ۱۳۵۹ / مدرک کارشناسی و کارشناسی ارشد رشتهٔ مهندسی برق در سال‌های ۱۳۷۷-۱۳۸۳ از دانشگاه صنعتی شریف / دریافت مدرک دکترای علوم کامپیوتر در سال ۱۳۸۹ از دانشگاه EPFL سوئیس و گذراندن یک دوره تحقیقاتی یک ساله در دانشگاه KTH سوئد / عضو هیئت علمی دانشکده علوم ریاضی دانشگاه صنعتی شریف / زمینه‌های علمی-پژوهشی مورد علاقه: علوم کامپیوتر نظری، بالاخص رمزنگاری.

دکتر سلمان ابوالفتح‌بیگی:
متولد ۱۳۶۰ / کارشناسی ریاضی در سال ۱۳۸۳ از دانشکده علوم ریاضی دانشگاه صنعتی شریف / مدرک دکتری از دانشگاه MIT در سال ۲۰۰۹/ عضو هیئت علمی پژوهشکده ریاضیات پژوهشگاه دانش‌های بنیادی / زمینهٔ کاری: محاسبات کوانتمی و نظریه اطلاعات کوانتمی.

دکتر امید اعتصامی:
متولد ۱۳۶۱ / مدرک کارشناسی مهندسی کامپیوتر از دانشگاه صنعتی شریف و دکتری علوم کامپیوتر از دانشگاه برکلی، کالیفرنیا / علایق تحقیقاتی: محاسبات، به ویژه ارتباط آن با تصادف و احتمال.

دکتر زینب مالکی:
متولد ۱۳۶۲ / لیسانس ریاضی محض دانشگاه صنعتی اصفهان/ فوق لیسانس ریاضی دانشگاه صنعتی اصفهان/ دکتری ریاضی دانشگاه صنعتی اصفهان/ دوره پسادکتری یک ساله در پژوهشگاه دانش‌های بنیادی تهران (IPM)/ محل اشتغال فعلی دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی اصفهان،گروه نرم‌افزار/ زمینه‌های تحقیقاتی: علوم کامپیوتر، شبکه‌های پیچیده، الگوریتم، بیوانفورماتیک و زیست محاسباتی، نظریه گراف و ترکیبیات.