ریاضیات و اینترنت•

پل دیویس*
ترجمهٔ میلاد نکویی

رابطهٔ میان ریاضیات و اینترنت مانند رابطهٔ میان زبان انگلیسی و آثار شکسپیر است. آثار شکسپیر بدون وجود زبان نمی‌توانست خلق شود، و در عین حال اشعار و نمایشنامه‌های وی زبان را در روند تکاملیش غنیتر کرده است.

کامپیوتر در زبان ریاضی متولد شد. اعداد دودویی به کامپیوتر امکان ارائهٔ کلمات، موسیقی، تصاویر و فراتر از آنها را دادند، و امروزه دستگاههای کامپیوتر در پهنهٔ اینترنت با الفبایی مرکب از صفر و یک با هم در ارتباط‌اند. قواعد بیطرفانهٔ منطق ریاضی بر عملیات کامپیوتری، آدرس‌دهی اینترنتی و حتی جستجوگرهای وب[1] حکمفرما هستند.

در اینترنت، ریاضیات مهمترین وسیله برای حفظ امنیت پیغامها و مبادلات مالی است. ریاضیات ابزار اصلی فشرده‌سازی اطلاعات، کدگذاری و تصحیح خطا در انتقال فایلهای بزرگ است. ریاضیات مبنای بانکها [پایگاهها]ی اطلاعاتی برای مدیریت آدرسهای پست الکترونیک و جستجو در وب، و وسیلهٔ مسیریابی پیغامها و مدیریت شبکه‌هاست.

از طرف دیگر، اینترنت نیز به پیشبرد تحقیقات و آموزش ریاضیات کمک می‌کند. گروههایی از مدرسان و پژوهشگران از طریق پست الکترونیک، گروههای خبری و جایگاهها [سایتها]ی خاصی از وب، با یکدیگر در ارتباط‌اند. همچنین اینترنت امکان محاسبات غیرمتمرکز را فراهم می‌کند؛ مانند تلاش جمعی اخیر که کامپیوترهای چند ده کشور به‌هم پیوستند تا رمزی را بگشایند که زمانی می‌پنداشتند تا ۲۰ هزار سال ایمن خواهد بود.

مدیریت اطلاعات در اینترنت

همان‌گونه که خیلیها می‌دانند، پیغامها در شبکهٔ اینترنت ــ پست الکترونیک، گرافیک، صدا و نتایج جستجو در بانکهای اطلاعاتی ــ به‌صورت رشته‌هایی از صفر و یک منتقل می‌شوند. ریاضیات در دو نمونه از این تبدیل و انتقال دیجیتال، اهمیت اساسی دارد.

• مثلاً انتقال دقیق یک پیام متنی که به ارقام دودویی تبدیل شده است، احتیاج به کدهایی برای یافتن و تصحیح خطا در انتقال دارد (تا کدهای محرمانه [رمزها]) اشتباه نشود).

• مثلاً برای کم کردن حجم داده‌ها در تصویری که باید به‌راحتی انتقال داده شود و با شباهت قابل قبولی با نسخهٔ اصلی بازسازی شود، از ابزارهای فشرده‌سازی داده‌ها استفاده می‌شود.

هنگامی که رشته‌های بسیار طویلی از صفر و یک در شبکه‌های رایانه‌ای منتقل می‌شوند، اشتباه در انتقال غیرقابل اجتناب است، در حالی‌که حتی از بین رفتن مقدار اندکی از داده‌ها هم ممکن است فاجعه‌آمیز باشد. کدهای مورد استفاده برای خطایابی، ابزارهایی ریاضی هستند که می‌توانند بسیاری از اطلاعات از بین رفته را مشخص کنند، روشی مانند شمردن تعداد صفحات یک نامهٔ طولانی برای تعیین اینکه آیا در مرسوله چیزی گم شده است یا نه.

یک وسیلهٔ استاندارد برای یافتن اشتباه در انتقالات شبکهٔ اینترنت، کدهای دوری هستند؛ از میان آنها معمولاً CRC – ۱۶، یک کد فزونگی[1] دوری، انتخاب می‌شود که می‌تواند اشتباه را حتی تا ۱۶ بیت متوالی از یک پیام، پیدا کند. CRC – ۱۶ همچنین ۹۹٪ خطاهای با طول بزرگتر از ۱۶ بیت را پیدا می‌کند. وقتی خطایی کشف می‌شود، کامپیوتر مقصد تنها کاری که می‌کند این است که رسیدن مرسولهٔ شامل خطا را اعلام نمی‌کند و کامپیوتر فرستنده درمی‌یابد که باید دوباره مرسوله را بفرستد.

این کدها نوع خاصی از عمل تقسیم را روی نمایش عددی پیام انجام می‌دهند. فرستنده بدون اینکه طول پیام تغییر چندانی بکند، باقیماندهٔ تقسیم را به پیام ضمیمه می‌کند. این اطلاع اضافی به گیرنده امکان می‌دهد با تکرار عمل تقسیم، پیام را وارسی کند. به‌دست آوردن باقیماندهٔ نادرست به این مفهوم است که پیام مخدوش شده است.

ایده‌های مربوط به چنین کدگذاری برای نخستین بار در اوایل دههٔ ۱۹۵۰ مطرح شد؛ همینگ[2] و هافمن[3] در این زمینه پیشاهنگ بودند. ایده‌های ریاضی نظریهٔ جبری کدگذاری که در دههٔ ۱۹۶۰ مطرح شد و مبتنی بر مبحث قدیمتر میدانهای متناهی بود، باعث شد شیوهٔ یافتن و تصحیح خطا رشد کند و به‌صورت کارآمد امروزی خود درآید. برای مثال، کدهای تصحیح خطای ریدـسالومن، که در دههٔ ۱۹۶۰ ایروینگ رید[4] و گوستاو سالومن[5] آنها را با کاربرد مباحثی از [نظریهٔ] میدانهای متناهی به‌دست آوردند، روشی چنان کارآمد برای یافتن و تصحیح خطا به‌دست می‌دهند که در وسایلی از ماهواره‌ها گرفته تا دیسکهای فشرده مورد استفاده قرار می‌گیرد.

ایده‌های مربوط به فشرده‌سازی تصاویر نیز همانند کدهای تصحیح خطا، در پهنهٔ وسیعی از تکنولوژی، از جمله تلویزیونهای دیجیتال آینده، به‌کار می‌روند. (برای انتقال یک ثانیه تصویر ویدئویی با کیفیت بالا و فشرده نشده به‌وسیلهٔ مودم خانگی معمول، بیش از ۷ ساعت زمان لازم است) هدف نهایی فشرده‌سازی تصاویر، کاهش مرتبهٔ حجم داده‌ها و در نتیجه زمان انتقال آنها و در عین حال حفظ تمام بخشهایی از تصویر است که از نظر بصری مهم هستند.

شیوه‌های مناسب فشرده‌سازی داده‌ها کمک می‌کنند تا تصاویر گرافیکی وب به‌طور سریع و جذاب روی صفحهٔ رایانه نمایان شوند. چنین ابزارهایی فایلهای صوتیی را منتقل می‌کنند که هرچند بخشهایی از آنها پاک یا بازسازی

1. World Wide Web (www)

1. redundancy 2. R. W. Hamming 3. D. A. Huffman
4. Irving Reed 5. Gustave Solomon

شده است، برای گوش خوشایند هستند. بعضی از ایده‌های تازهٔ فشرده‌سازی تصاویر مبتنی است بر موجکها که گونه‌ای ابزار تحلیل چندمقیاسی هستند. موجکها ابزاری ریاضی هستند که در دههٔ گذشته به‌وسیلهٔ گراسمن[1]، مالت[2]، اینگرید دبشیس[3] و دیگران برای خلاصی از محدودیتهای آنالیز کلاسیک فوریه که محدود به تحلیل بسامدهای پایه‌ای است، ابداع شدند. در رویکرد فوریه با دردست داشتن دامنهٔ همسازهای اصلی یک طنین [تن] طولانی پیوسته، به‌راحتی می‌توان آن طنین را بازسازی کرد. اما سیگنالهای ناگهانی و کوتاه ــ آن‌گونه که در موسیقی واقعی شنیده می‌شوند یا در تصویر اثر انگشت دیده می‌شوند ــ به ابزاری نیاز دارند که بتواند با بسامدهایی از مقیاسهای مختلف و بازه‌های زمانی مختلف کار کند.

با اینکه آنالیز فوریه را می‌توان با کمی تغییر برای این امر به‌کار گرفت، موجکها برای این کار بسیار مناسبترند چراکه از بازسازی قطعهٔ مقیاس‌بندی شده خاصی از یک موالفهٔ اساسی سیگنال ساخته می‌شوند. آنها به‌طور طبیعی برای ذخیره‌سازی فشردهٔ تصاویری مثل تصویر اثر انگشت به‌کار می‌روند، هرچند طرح شیارها و برآمدگیهای اثر انگشت فقط در بخش محدودی از صفحه جا می‌گیرد.

امنیت در شبکهٔ اینترنت

امنیت در اینترنت به‌اندازهٔ امنیت در خزانهٔ بانک مهم است. مسائل امنیتی شامل خصوصی بودن پیغامها، «خوش حسابی» کامپیوترهای پیوسته به شبکهٔ اینترنت، قابل اعتماد بودن مبادلات مالی و بسیاری مباحث دیگرند. برای مثال بازار تجاری سریعاً رو به رشد در اینترنت اتکای زیاد به رمزهای محرمانه‌ای دارد که برای ابداع آنها دستاورد چند صدسالهٔ نظریهٔ اعداد با کشفیات دو دههٔ اخیر ترکیب شده است.

علاوه‌بر آن در کوششهایی که برای شکستن چنین رمزهایی می‌شود برای اینکه بار محاسباتی را بین چند کامپیوتر پخش کنند از شبکهٔ اینترنت استفاده می‌کنند. این‌گونه محاسبات غیرمتمرکز نیز اساساً مبتنی بر تعمیمهای نوین یک ایدهٔ قدیمی فرما در مورد جستجوی روشمند عوامل اول اعداد بزرگ، هستند.

امنیت شبکهٔ اینترنت دو مؤلفه دارد که مکمل یکدیگرند، یکی مسأله فرستادن پیغامی است که فقط گیرنده بتواند آن را بخواند و محرمانه بودن و درستی آن مورد اطمینان باشد. مسألهٔ دیگر، مطمئن شدن از هویت فرستندهٔ پیام است. حل مسألهٔ نخست مستلزم یافتن رمزی است که به آسانی قابل شکستن نباشد و در عین حال قابلیت انتقال و بازگشایی سریع داشته باشد. مسألهٔ دوم مسألهٔ امضاهای دیجیتال است: چگونه یک تاجر بینترنتی می‌تواند اطمینان یابد که امضای روی چک الکترونیکی معتبر است؟ حل هر دوی این مسائل مستقیماً برعهدهٔ نظریهٔ اعداد است، شاخه‌ای از ریاضیات که برخلاف ظاهرش بسیار عمیق است.

سیستمهای رمزنگاری سنتی مانند «سیستم معیار رمزنگاری داده‌ها» (DES) مانند یک صندوق پستی عمل می‌کنند که تنها دو کلید دارد و این دو کلید دردست گیرنده و فرستنده است. مشکلاتی که در این مورد وجود دارند عبارت‌اند از انتقال ایمن کلیدها به هر دو نفر جدید که با هم ارتباط برقرار می‌کنند و مدیریت مجموعهٔ بزرگی از کلیدها برای کسی که با اشخاص زیادی مرتبط است. سیستمهای کلید عمومی یا RSA (ترکیب حروف اول اسامی ریوست[1]، شامیر[2] و ایدلمن[3]. این اشخاص نخستین سیستم اجراشدنی را برپایهٔ ایده‌های دیفی[4] و هلمن[5] در ۱۹۷۸ مطرح کردند) به صندوقهای پستی بازی تشبیه شده‌اند که فرستنده‌ای که می‌خواهد یک پیام در آنها قرار دهد می‌تواند در آن را به سرعت ببندد و تنها صاحب صندوق پستی که همان گیرنده است می‌تواند در صندوق پستی را بازکند. یعنی، هر شخصی می‌تواند یک پیام را برای یک گیرندهٔ دلخواه به رمز درآورد ولی تنها خود گیرنده می‌تواند پیام را رمزگشایی کند.

به رمز درآوردن یک پیام در سیستم کلید عمومی مستلزم دانستن دو عدد (بزرگ) است که آنها را کلید عمومی می‌نامند. برای رمزگشایی یک پیام نیاز به دانستن عدد دیگری است و این همان کلید خصوصی است که فقط گیرنده از آن آگاهی دارد. در مراحل رمزنگاری و رمزگشایی از حساب پیمانه‌ای ــ نوعی حساب که عملیات آن شبیه کارکرد عقربه‌های ساعت است ــ استفاده می‌شود (مثلاً تقسیم مجموع ساعاتی که یک مسافرت به طول انجامیده بر ۲۴ و به‌دست آوردن باقیمانده که همان ساعت ورود است).

وقتی اعضای جدید به یک سیستم رمزنگاری کلید عمومی می‌پیوندند، اولین گام برای تعیین کلیدهایشان انتخاب (تصادفی) دو عدد اول بزرگ توسط خود آنهاست. سپس کلیدها با استفاده از آن دو عدد اول در چندین گام پی‌درپی بر مبنای قضیه‌ای از اویلر که دو قرن قدمت دارد، محاسبه می‌شوند. سیستم کلید عمومی در حالتی امنیت خود را از دست می‌دهد که آن دو عدد اول با تجزیهٔ یکی از دو کلید عمومی به‌دست آیند؛ در سیستم RSA از اعداد ۱۲۹ رقمی استفاده می‌شود تا عوامل اول کلیدها به آسانی قابل دستیابی نباشند.

در واقع ریوست، شامیر و ایدلمن آنچنان از ایمنی روش خود مطمئن بودند که در سال ۱۹۷۷ جهان را به بازگشایی رمز پیغامی دعوت کردند که با یک عدد ۱۲۸ رقمی رمزنگاری شده بود. در آن زمان آنها تخمین زدند که تجزیهٔ آن عدد به عوامل اول ۲۳۰۰۰ سال طول خواهد کشید؛ اما در سال ۱۹۹۴، یک گروه غیررسمی متشکل از ۶۰۰ داوطلب از بیش از ۲۴ کشور که از طریق شبکهٔ اینترنت با یکدیگر در ارتباط بودند، CPU‌های بدون استفاده روی هر گونه کامپیوتر ــ حتی ماشینهای نمابر ــ را گرد هم آوردند تا «الگوریتم غربال درجه دو» (کارل پومرانس، ۱۹۸۱) را که زایده‌های ۳۵۰ سال پیش فرما نشأت گرفته، اجرا کنند. پس از ۸ ماه تلاش دسته‌جمعی، عوامل اول ۶۴ و ۶۵ رقمی عدد موردنظر یافته شدند.

مبارزه‌طلبی ۱۲۸ رقمی RSA، با استفاده از شبکهٔ اینترنت، هر چند نه چندان سریع، ولی بالاخره پاسخ دندان‌شکنی دریافت کرد. با محاسباتی غیرمتمرکز در سراسر اینترنت، در حصاری که حافظ محرمانه‌بودن ارتباطات سرتاسری است شکاف ایجاد شد؛ با به‌کار بردن کلیدهای عمومی با ارقام بیشتر، به راحتی می‌توان به امنیت بیشتر دست یافت.

مسألهٔ امضای دیجیتال ــ مثلاً امضا کردن چکهای الکترونیک ــ با معکوس کردن فرایند کلید عمومی حل می‌شود. فرستنده هم پیام را می‌فرستد

1. A. Grossman 2. Stephen Mallet 3. Ingrid Daubechies

1. R. L. Rivest 2. A. Shamir 3. L. Adleman
4. W. Diffie 5. M. Hellman

و هم نسخهٔ «رمزگشایی‌شدهٔ» آن را. اگر گیرنده پس از دوباره به رمز درآوردن نسخهٔ رمزگشایی‌شده به نسخهٔ اصلی پیام رسید، آنگاه پیام معتبر است. در اینجا نیز مانعی به نام تجزیهٔ اعداد بزرگ امنیت لازم را تأمین می‌کند.

ریاضیات همچنین در سایر راههای رخنه در سیستمهای مختلف امنیتی نقش عمده‌ای ایفا می‌کند. این نقش مبتنی است بر یک رهیافت سیستمی برای کشف کلید ریاضیِ رمز مورد استفاده.

اطلاعات بیشتر در گزارش جدیدی از آکادمی ملی علوم [آمریکا] با عنوان «نقش رمزنگاری در ایجاد امنیت برای جامعهٔ اطلاعاتی» آمده است.

بانکهای اطلاعاتی و جستجو

جستجوگرهای قدرتمند وِب مانند «آلتاویستا[1]» و «یاهو![2]» به استفاده‌کنندگان شبکهٔ اینترنت این امکان را می‌دهند که اطلاعات ارزشمند تخصصی را که در اقصا نقاط «فضای اطلاعات» پنهان است، بیابند. هستهٔ بیشتر ابزارهای جستجو، فهرستی از واژه‌های کلیدی است؛ هر درایهٔ فهرست دربرگیرندهٔ لیستی از تمام جایگاههای وب جهانی است که حاوی آن کلمهٔ کلیدی هستند. (درایهٔ مربوط به واژهٔ «ریاضیات» در یکی از فهرستهای جستجو شامل لیستی از ۳۳۲۹۶۶ جایگاه است!) در حالت ایده‌آل، جستجوگر علاوه بر لیست کردن اشتراکات تمام درایه‌های فهرست برای واژه‌های کلیدی داده شده، درجهٔ تقدم هر جایگاه را نیز که نشانگر ارتباط بالقوهٔ هر جایگاه لیست شده با احتیاجات جوینده است، نشان می‌دهد.

برخی از آخرین تحقیقات در زمینهٔ ایجاد تعادل میان گستردگی جستجو و ذیربط بودن نتایج جستجو، باعث ایجاد یک مدل فضای برداری از اطلاعات موجود در فهرست شده است. مختصات فضا اصطلاحات موجود در فهرست هستند، یعنی مجموعهٔ واژه‌های کلیدی که جستجو در میان آنها انجام می‌گیرد. هر جایگاه وب یک نقطه در آن فضاست که مختصاتش به‌وسیلهٔ «میزان وابستگی» آن جایگاه به هر واژهٔ کلیدی مشخص می‌شود و قاعدتاً بیشترین مقادیر مختصات به آن واژه‌های کلیدی داده می‌شود که بیشترین ارتباط را با آن جایگاه دارند. جایگاههایی که اطلاعاتی مشابه ارائه می‌کنند در این فضا با نقاطی نمایش داده می‌شوند که به تعبیری نزدیک یکدیگرند.

در این صورت جستجو تبدیل به مسألهٔ زیر می‌شود. یافتن نزدیکترین همسایگان در فضایی با بعد بسیار بالا و، در حالت ایده‌آل، با میزانی از محاسبات که سریعتر از بعد فضا افزایش نیابد. در نظر گرفتن مدلهایی احتمالاتی برای چگونگی توزیع اطلاعات در این فضاها، به هندسه‌های نااستاندارد می‌انجامد. برای مثال، نابرابری آشنای مثلثی ــ اینکه مجموع طول دو ضلع مثلث همواره از ضلع سوم بزرگتر است ــ ممکن است برقرار نباشد و این خود، مسألهٔ یافتن الگوریتمهای مناسب جستجو را پیچیده‌تر می‌کند.

از دیدگاه جبری، بردارهای مختصات واژه‌های کلیدی را می‌توان به مثابهٔ ستونهایی در یک «ماتریس وقوع» کلمه‌ـجایگاه در نظر گرفت. در سطر مربوط به هر واژهٔ کلیدی جلوی هر جایگاهی که شامل آن واژهٔ کلیدی است یک درایهٔ غیرصفر قرار دارد. هدف این است که با یافتن روابطی میان واژه‌های کلیدی، مثلاً میان «ریاضیات» و «عدد»، که احتمالاً برای جوینده مشخص نبوده است، جایگاههایی با اطلاعات مشابه بیابیم.

از روی این ماتریس وقوع می‌توان جهتهای مرجعی را معین کرد که به بردارهای ویژه در فضای برداری واژه‌های کلیدی موسوم‌اند. به هر بردار ویژه، شاخصی از اهمیت آن بردار متناظر است که آن را مقدار تکین آن بردار می‌نامند. جایگاههایی که در جهت مشخص شده به‌وسیلهٔ یک بردار ویژه قرار دارند، همگی دارای اطلاعات مشترکی هستند که آن بردار ویژه نمایندهٔ آن است. مقادیر تکین بزرگتر مشخص‌کنندهٔ اشتراکات معنایی مهمترند. محاسبهٔ بردارهای ویژه و مقادیر تکین برای چنین ماتریسهای بزرگی خودش مسألهٔ مشکلی است اما این روش، نویدبخش جستجوهایی با نتایج کامل و مرتبط با موضوع است.

در عمل جستجوگرها صریحاً با ماتریسهای چند صد سطری و چند صد ستونی سروکار ندارند. بلکه بر مبنای دستورالعملهای محاسباتی هوشمندانه روی بانکهای اطلاعاتی کار می‌کنند.

بسیاری از بانکهای اطلاعاتی به‌صورت شیئی ریاضی به نام درخت ساخته شده‌اند. این درختها شبیه شجره‌نامهٔ خانوادگی هستند که نسبتهای بین والدین و فرزندان و اجداد و نوادگان آنها را نشان می‌دهند. برای مثال ممکن است فهرستی شامل ۲۶ درخت، هر یک برای یک حرف الفبای انگلیسی، باشد، اولین سطح از فرزندان [بالاترین سطح] حاوی تمام ترکیبات دو حرفی مجاز خواهد بود و به همین ترتیب سطوح بعدی پر خواهند شد؛ مثلاً aardvark [مورچه‌خوار] یکی از نوادگانِ دور aa است.

«بانکهای اطلاعاتی رابطه‌ای»، علاوه بر روابط والد-فرزند روابطی اضافی میان عناصرشان تعریف می‌کنند. قدرت یک بانک اطلاعاتی رابطه‌ای از توانایی آن در کارکردن با این روابط سرچشمه می‌گیرد، مانند اجرای یک عمل اشتراک‌گیری که رشتهٔ مشترکی از حروف را در دو واژهٔ متفاوت می‌یابد. قوانین حاکم بر این عملیات به‌صورت ریاضی و بر اساس نوعی جبر رابطه‌ای یا حساب رابطه‌ایِ مختص به ساختار هر بانک اطلاعاتی مشخص شده‌اند. ریاضیات، چارچوبی برای توصیف ساختار بانکهای اطلاعاتی فراهم می‌کند و ابزارهای ریاضی مبنایی برای افزایش کارایی و قابلیت اعتبار این بانکها هستند.

مسیریابی و پیکربندی شبکه

یک شبکهٔ محلی با اندازهٔ معمولی، تقریباً حاوی ۱۰۰۰۰ جفت گره مرتبط با یکدیگر است. پیغامها روی این شبکه از گرهها مانند قطارهایی هستند که با سرعت نور روی خطوط مختلف شبکه حرکت می‌کنند. هر واگن قطار یک قطعه از پیام را حمل می‌کند، درست مانند اینکه یک نامهٔ طولانی روی چندین کارت پستال نوشته شده باشد و هر کارت در یک واگن قرار داشته باشد. معمولاً کارتهایی از پیغامهایی مختلف در یک قطار با هم مخلوط می‌شوند.

کارایی شبکه وابسته به طول قطارها ــ طول بسته‌های پیغامها ــ و فضای بین قطارهاست. مثلاً یک پیام طولانی که در زمان نادرست وارد شبکه می‌شود تا زمانی که از خطوط شبکه بگذرد باعث تأخیر پیغامهای دیگر می‌شود در حالی‌که پیغامهای کوتاه را که با فاصلهٔ مناسبی وارد شبکه شده‌اند می‌توان در میان یکدیگر جای داد.

1. Alta Vista 2. Yahoo!

با استفاده از ایده‌های ریاضی نظریهٔ صف، بر پایهٔ اطلاعاتی راجع به اندازه و الگوی ورود پیغامها به شبکه، می‌توان به پیش‌بینی کارکرد «قرارداد[1]»های پیام‌رسانی پرداخت. (کاربرد کلاسیک نظریهٔ صف، تخمین زدن زمان انتظار در بانک، با در دست داشتن الگوی ورود مشتریها و مدت زمان سرویس‌دهی تحویلدار بانک است.)

امّا بررسی قراردادهای پیام‌رسانی مختلف بر اساس مدلهای ریاضی ترافیک پیغامها صورت می‌گیرد. مدلهای خوب این اطمینان را به ما می‌بخشند که یک قرارداد جدید در عمل همانگونه است که نظریهٔ صف پیش‌بینی می‌کند؛ و مدلهای بد ممکن است باعث شوند که طراح پروتکل وعده‌هایی در مورد کارکرد قرارداد [پیشنهادیش] بدهد که قابل تحقق نباشند.

اخیراً دانشمندان در بلکُر[2]، آزمایشگاههای AT & T و دانشگاه بوستون کشف کرده‌اند که ترافیک، شبکه در طول زمان دارای خاصیت فرکتالی خودمشابهی[3] است. این کشف، مبنای فیزیکی موجهی فراهم می‌کند تا مدلهای ساده‌تر و دقیقتری برای ترافیک اینترنت طراحی شود که بتوان قراردادهای پیشنهادی را با آنها محک زد. مفاهیم خودمشابهی مربوط به بخشی از ریاضیات هستند که از تحلیل پیشین بازارکالا توسط بنوا مندل بروت، سرچشمه گرفته است. مفهوم فیزیکی اصلی این است که تعامل یک کامپیوتر و شبکه، همانند تعامل یک انسان با کامپیوتر، در مقیاسهای زمانی گوناگونی صورت می‌گیرد.

طراح قراردادهای مدیریت ترافیک شبکه، با در دست داشتن یک مدل خوب از ترافیک داده‌ها در شبکه، باید بکوشد میان ارسال داده‌ها از طریق کوتاهترین مسیر و کم کردن بار ترافیکی تعادل ظریفی ایجاد کند، مانند کسی که می‌خواهد در ساعت اوج ترافیک در شهر سفر کند و باید تصمیم بگیرد که آیا از بزرگراهی که مستقیماً به مقصد می‌رود و احتمالاً بسیار شلوغ است استفاده کند یا یک مسیر پرپیچ و خم و طولانی اما خلوت را در پیش گیرد.

هنگامی که ترافیک سبک باشد، طول مسیرْ عاملِ تعیین‌کننده خواهد بود و بسته‌های پیام به بهترین نحو از طریق کوتاهترین مسیر منتقل می‌شوند. یافتن کوتاهترین مسیر در یک شبکه مسأله‌ای است که در شاخه‌ای از ریاضیات به نام نظریهٔ گراف در حد مطلوبی بررسی شده است. (بلمن[4]، فُرد[5] و دایکسترا[6] از جمله ریاضیدانانی هستند که نخستین بار الگوریتمهای کوتاهترین مسیر را در اواخر دههٔ ۱۹۵۰ طراحی کردند.) وقتی ترافیک شبکه سنگینتر می‌شود، مسیریاب شبکه باید تمام مسیرهای بین فرستنده و گیرنده را بیابد که این کار با کمک تکنیکهای نوین جستجوی گراف انجام می‌شود که در دههٔ ۱۹۷۰ تاریان[7] و هپکرافت[8] و دیگران آنها را ارائه کردند. با اطلاع از اینکه هم کوتاهترین مسیر و هم تمامی مسیرهای قابل دسترس را می‌توان یافت، بسیاری از قراردادهای مسیریابی شبکه معطوف به تعیین ملاکهای گوناگون برای انتخاب مسیر از بین مسیر کوتاهتر ولی احیاناً شلوغ و مسیر طولانیتر ولی خلوت‌تر، جلب می‌کنند.

1. protocol 2. Bellcore 3. self-similarity 4. R. E. Bellman
5. L. R. Ford 6. E. W. Dijkstra 7. R. E. Tarjan
8. J. E. Hopcroft

ریاضیات در وب

ریاضیدانان از امکانات شبکهٔ اینترنت و وب به خوبی استفاده می‌کنند. این ابزارها به آنها امکان می‌دهند تا ایده‌ها، روشها و منابع خود را فارغ از مرزهای جغرافیایی و رشته‌ای با یکدیگر در میان بگذارند تا هم آموزش و هم تحقیق پیشرفت کند.

مراکز اصلی برای حوزهٔ وسیعی از فعالیتهای ریاضی، از جملهٔ بررسی نقش ریاضیات در جامعه، عبارت‌اند از Math Forum؛ منزلگاههای[1]ی سه جامعهٔ پشتیبان «هفتهٔ هشیاری ریاضیات»: انجمن ریاضی آمریکا (AMS)؛ جامعهٔ ریاضی آمریکا (MAA)؛ انجمن ریاضیات صنعتی و کاربردی (SIAM).

نمونه‌هایی از جایگاههای تخصصی‌تر عبارت‌اند از Math Archive (آرشیو ریاضی)، که به‌طور تخصصی به مباحث آموزشی می‌پردازد و Geometry Center (مرکز هندسه) که تأکید آن بر محاسبه و به تصویر درآوردن ساختارهای هندسی است. متخصصین نظریهٔ اعداد که علاقه‌مند به جستجوی اعداد اول مرسن هستند منابع خود را در اختیار Great Internet Mersenne Prime Search (جستجوی بزرگ اعداد اول مرسن به وسیلهٔ اینترنت) قرار می‌دهند. سالهاست که متخصصان محاسبات عددی، مسائل، راه‌حلها و روشهای خود را از طریق NA-Net با یکدیگر در میان می‌گذارند. در NA-Net بهترین نرم‌افزار آنالیز عددی برای استفادهٔ عموم قرار دارد.

ریاضیات و اینترنت

ریاضیاتْ زبان عملیاتی شبکهٔ اینترنت است، از اعداد دودویی که بیانگر متون و تصاویر هستند گرفته تا ساختار داده‌ای پیچیدهٔ جستجوگرهای وب جهانی. تلفیق هوشمندانه ایده‌های نو و قدیمی از رشته‌هایی مانند نظریهٔ اعداد دستیابی به امکانات اساسی اینترنت مانند به رمز درآوردن داده‌ها برای ایمنی مبادلات مالی را میسر کرده است. در عین حال، اینترنت سرآغازی برای همکاریهای جهانی میان معلمان و پژوهشگران علوم ریاضی ایجاد کرده است. این همکاریها هم به پیشبرد امر آموزش از کودکستان تا سطوح دانشگاهی و هم به پیشبرد پژوهش در زمینهٔ برخی از دشوارترین مسائل ریاضیات محض و کاربردی کمک می‌کنند.

******

• این مقاله در Math Forum، ۱۸ مارس ۱۹۹۷، آمده است.

* پال دیویس، بخش علوم ریاضی، مؤسسهٔ پلی‌تکنیک ووستر، آمریکا
pwadiv@wpi.edu

1. home pages