شبه‌تصادفی بودن•

اودت گُلدرایش*

ترجمهٔ محمدقاسم وحیدی

این مقاله به شیئهایی متناهی می‌پردازد که به‌وسیلهٔ دنباله‌های دودویی متناهی به نام رشته کدگذاری می‌شوند. وقتی از توزیعها سخن به میان می‌آوریم، منظور ما توزیعهای احتمال گسسته‌اند یا تکیه‌گاهی متناهی که مجموعه‌ای از رشته‌هاست. توجه خاصی به توزیع یکنواخت داریم که به ازای پارامتر طولی مانند n (که در طول بحث به‌صراحت یا به‌طور ضمنی مطرح می‌شود)، به هر رشتهٔ nبیتی مانند $x \in \{0,1\}^n$ احتمالی برابر (یعنی، احتمال 2^{-n}) را تخصیص می‌دهد. وقتی به‌صورت محاوره‌ای صحبت از «رشته‌های کاملاً تصادفی» می‌کنیم، منظور ما رشته‌هایی هستند که مطابق با چنین توزیع یکنواختی برگزیده شده‌اند.

نیمهٔ دوم این سده شاهد پیدایش و بسط سه نظریه در بارهٔ تصادفی بودن بوده است، مفهومی که اندیشمندان را در طول اعصار سردرگم کرده است. نخستین نظریه (رک. [۳]) که آغازگر آن شانُن[1] بود، ریشه در نظریهٔ احتمال دارد و توجه آن معطوف به توزیعهایی است که کاملاً تصادفی نیستند. نظریهٔ اطلاع شانُن تصادفی بودن کامل را به عنوان حالتی کرانگینی[2] مشخص می‌کند که در آن گنجایش اطلاع ماکسیمم می‌شود (و هیچ زیادی[3]ای در بین نیست)[4]. بنابراین، تصادفی بودن کامل وابسته به توزیعی یکتاست ــ همان توزیع یکنواخت. به‌ویژه، بنابر تعریف، نمی‌توان چنان رشته‌های تصادفی کامل را از رشته‌های تصادفی کوتاهتر تولید کرد.

1. Shannon 2. extreme 3 redundancy

۴. در حالت کلی، میزان اطلاع در توزیعی مانند D به صورت $-\sum_x D(x)\log_2 D(x)$ تعریف می‌شود. بنابراین، توزیع یکنواخت بر رشته‌هایی به طول n دارای اندازهٔ اطلاع n است، و هر توزیع دیگر روی رشته‌های nبیتی اندازهٔ اطلاع کمتری دارد. همچنین، برای تابعی مانند

$$f : \{0,1\}^n \to \{0,1\}^m$$

با $m < n$، توزیع حاصل از عمال f بر رشته‌ای nبیتی با یک توزیع یکنواخت، اندازهٔ اطلاعی حداکثر n دارد که اکیداً کمتر از طول خروجی است.

نظریهٔ دوم (رک. [۱۱]، [۱۲])، منسوب به سولوموئوف[1]، کولموگوروف، و شایتین[2]، ریشه در نظریهٔ محاسبه‌پذیری و به‌ویژه در مفهوم یک زبان جهانی (معادل با ماشین یا ابزار محاسبهٔ جهانی) دارد. در این نظریه، پیچیدگی شیٔ برحسب کوتاهترین برنامه (برای ماشین جهانیِ ثابتی) اندازه گرفته می‌شود که این شیٔ را تولید می‌کند[3]. مانند نظریهٔ شانُن، پیچیدگی کولموگوروفی، کمّی است، و شیئهای تصادفی کامل به عنوان حالتهای کرانگینی مطرح می‌شوند. جالب توجه اینکه در این رهیافت، می‌توان گفت که یک شیٔ واحد، و نه یک توزیع بر روی شیئها، کاملاً تصادفی است. با این حال، رهیافت کولموگوروف ذاتاً اجرا نشدنی است (یعنی پیچیدگی کولموگوروفی محاسبه‌ناپذیر است)، و، بنابر تعریف، نمی‌توان رشته‌هایی با پیچیدگی کولموگوروفی بیشتر را از روی رشته‌های تصادفی کوتاه تولید کرد.

نظریهٔ سوم، که آغازگران آن بلوم، گولدواسر، میکالی[4]، و یائو [۸، ۲، ۱۳] بودند، ریشه در نظریهٔ پیچیدگی دارد و کانون توجه این مقاله است. این رهیافت صراحتاً به دنبال تدارکِ نظریه‌ای در بارهٔ تصادفی بودن کامل است که در عین حال امکانِ تولیدِ کارآیِ رشته‌های کاملاً تصادفی از رشته‌های تصادفی کوتاهتر را فراهم آورد. اُمّ این رهیافت، عبارت از این پیشنهاد است که شیئها را برابر تلقی کنیم در صورتی که نتوان آنها را با هیچ شیوهٔ کارآیی از هم تمیز داد. در نتیجه، توزیعی که نشود آن را به صورت کارآ از توزیع یکنواخت تمیز داد، تصادفی (یا بهتر است بگوییم «تصادفی برای کلیهٔ مقاصد عملی») که آن را «شبه‌تصادفی» می‌نامیم) تلقی می‌شود. بنابراین، تصادفی بودن، خاصیت «ذاتی» اشیا (یا توزیعها) نیست بلکه وابسته به

1. Solomonov 2. Chaitin

۳. مثلاً رشتهٔ 1^n دارای پیچیدگی کولموگوروفی $O(1)+\log_2 n$ است (بر مبنای برنامهٔ «n تا ۱ چاپ کن» که طولی نابیشتر از n (مثلاً در دستگاه دودویی)) دارد. در مقابل، استدلال شمارشی ساده‌ای نشان می‌دهد که اغلب رشته‌های nبیتی دارای پیچیدگی کولموگوروفی حداقل n اند.

4 Micali

مشاهده‌گر (و قابلیتهای محاسباتی وی) است. برای توضیح این رهیافت، تجربهٔ ذهنی زیر را در نظر می‌گیریم.

> آلیس و باب به یکی از چهار روش زیر مثلاً با خط بازی می‌کنند. در هر چهار روش، آلیس سکه‌ای را به هوا پرتاب می‌کند به‌طوری که تا ارتفاع زیادی بالا رود، و از باب خواسته می‌شود که برآمد آن را پیش از برخورد سکه با زمین حدس بزند. این روشها از لحاظ اطلاعی که باب پیش از حدس زدن در اختیار دارد، با هم متفاوت‌اند. در شق اول، باب باید حدس خود را پیش از پرتاب سکه اعلام کند. روشن است که در این حالت باب با احتمال ۱/۲ برنده می‌شود. در شق دوم، باب باید حدس خود را زمانی که سکه در هوا چرخ می‌خورد، اعلام کند. گرچه این برآمد در ۱۸۰ درجه با حرکت سکه تعیین می‌شود، باب اطلاع دقیقی در مورد حرکتِ آن ندارد و بنابراین معتقدیم که در این حالت نیز باب با احتمال ۱/۲ برنده می‌شود. شق سوم، مشابه دومی است، بجز اینکه باب ابزار پیچیده‌ای در اختیار دارد که قادر است اطلاع دقیقی در موردِ حرکتِ سکه و نیز شرایط محیط که بر برآمد تأثیر می‌گذارد، تهیه کند. با این حال، باب نمی‌تواند این اطلاع را به موقع پردازش کند که حدسِ خود را بهبود بخشد. در شق چهارم، دستگاه پرتاب باب مستقیماً به کامپیوتر قدرتمندی وصل است که برای حل معادلاتِ حرکت برنامه‌ریزی شده و خروجی آن یک پیشگویی است. قابل درک است که در چنین حالتی باب می‌تواند حدس خود از برآمد را به میزان قابل ملاحظه‌ای بهبود بخشد.

نتیجه می‌گیریم که تصادفی بودنِ یک پیشامد به اطلاع و منابع محاسباتی که در اختیار داریم، بستگی دارد. بدین ترتیب، یک مفهوم طبیعی شبه‌تصادفی بودن، مطرح می‌شود: توزیع را شبه‌تصادفی گوییم هرگاه هیچ شیوهٔ کارآیی نتواند آن را از توزیع یکنواخت تمیز دهد که در آن شیوه‌های کارآ به الگوریتمهای زمان‌چندجمله‌ای (احتمالاتی) وابسته‌اند.

الگوریتمی را زمان‌چندجمله‌ای می‌نامند هرگاه یک چندجمله‌ای مانند p موجود باشد به‌طوری که برای هر ورودی x، الگوریتم در مدت زمانی با کران $p(|x|)$ اجرا شود که در آن $|x|$ طول رشتهٔ x را نشان می‌دهد. بنابراین، زمان اجرای چنان الگوریتمی میانه روانه به صورت تابعی از ورودی آن رشد می‌کند. الگوریتم احتمالاتی، الگوریتمی است که می‌تواند گامهایی تصادفی را اختیار کند که در آن، بی‌آنکه از کلیت کاسته شود، می‌توان گفت هرگام تصادفی عبارت است از اتخاذ تصمیم در بارهٔ اینکه کدام‌یک از دو گام از پیش تعیین شده باید در مرحلهٔ بعدی انتخاب شود به‌طوری که هرگام ممکن با احتمال ۱/۲ اختیار شود. این گزینه‌ها، «پرتابهای سکهٔ درونی» الگوریتم نامیده می‌شوند.

تعریف مولدهای شبه‌تصادفی

به بیانی نادقیق، هر مولد شبه‌تصادفی برنامه‌ای (یا الگوریتمی) کارآست که رشته‌های تصادفی کوتاه را کش می‌آورد و آنها را به دنباله‌های شبه‌تصادفی بلند تبدیل می‌کند. ما بر سه جنبهٔ بنیادین در مفهوم مولدِ شبه‌تصادفی تأکید می‌کنیم:

۱. **کارآیی.** مولد باید کارآ باشد. از آنجا که کارایی محاسبه را به زمان‌چندجمله‌ای بودن آن وابسته می‌دانیم، فرض می‌کنیم که این مولد به کمک یک الگوریتم زمان‌چندجمله‌ای تعیّنی قابل اجرا باشد.

این الگوریتم رشته‌ای به نام بذر را به عنوانِ ورودی دریافت می‌کند. این بذر، مقداری کراندار از تصادفی بودن را در اختیار خود می‌گیرد که به‌وسیلهٔ ابزاری که «دنباله‌های شبه‌تصادفی را تولید می‌کند» به کارگرفته می‌شود. این فرمولبندی، چنان ابزاری را شیوه‌ای تعیّنی تلقی می‌کند که بر بذری تصادفی اِعمال می‌شود.

۲. **کش‌آوری.** از مولد انتظار می‌رود که بذر ورودی را کش بیاورد و به دنبالهٔ خروجی طولانیتری تبدیل کند. به طور مشخص، مولدْ بذرهای به طول n بیت را به خروجیهای طولانیتر $l(n)$ بیتی کش می‌آورد که در آن $l(n) > n$. تابع l اندازهٔ کش‌آوری (یا تابع کش‌آوری) مولد نامیده می‌شود.

۳. **شبه‌تصادفی بودن.** خروجیِ مولد از دیدِ هر مشاهده‌گر کارآیی باید تصادفی به نظر آید. یعنی، هیچ شیوهٔ کارآیی نباید قادر به تمیز دادنِ خروجی یک مولد (روی بذری تصادفی) از یک دنبالهٔ واقعاً تصادفی با همان طول باشد. جملهٔ اخیر به مفهومی عام از «تمایزناپذیری [از نظر] محاسباتی» اشاره دارد که قلبِ کلِ این رهیافت است.

برای روشن شدن مطالب بالا، طرحِ زیر را برای یک مولدِ شبه‌تصادفی در نظر بگیرید. بذر آن متشکل از جفتی از اعداد صحیح ۳۲بیتی مانند x و N است، و خروجی ۱۰۰۰۰۰بیتی آن با مجذورکردن مکرر عدد جاری x به پیمانهٔ N و بیرون آوردن بیتِ با کمترین معنی در هر نتیجه در مراحل بینابینی به دست می‌آید. (یعنی، فرض کنید (به پیمانهٔ N) $x_i \leftarrow x_{i-1}^2$، برای $i = 1, \ldots, 10^5$، و خروجیها b_1، b_2، ...، b_{100000} هستند، که در آن b_i بند با کمترین معنای x_i است). این فرایند را می‌توان به بذرهایی به طول n (در اینجا ما از $n = 64$ استفاده کرده‌ایم) و خروجیهایی به طول $l(n)$ (در اینجا $l(n) = 10^5$) تعمیم داد. چنان فرایندی مطمئناً فقره‌های (۱) و (۲)ی بالا را برآورده می‌کند، در حالی که این پرسش که آیا فقرهٔ (۳) برقرار است یا خیر، قابل بحث است (پس از آنکه تعریفی دقیق برای آن ارائه شد). با اشارهٔ پیشاپیش به بخشی از بحثهای آتی، متذکر می‌شویم که، تحت این فرض که تجزیهٔ اعداد صحیح بزرگ، دشوار است، صورت اندک تغییریافته‌ای از فرایند بالا درواقع یک مولد شبه‌تصادفی است.

تمایزناپذیری [از نظر] محاسباتی

از لحاظ شهودی، دو شئ از نظر محاسباتی تمایزناپذیرند هرگاه هیچ شیوهٔ کارآیی نتواند آنها را از هم تمیز دهد. مطابق آنچه در نظریهٔ پیچیدگی معمول است، صورتبندی ظریف این موضوع مستلزم تحلیلی مجانبی است (یا بهتر است بگوییم بررسی زمان اجرای الگوریتمها به عنوان تابعی از طول ورودی آنها)[1]. بنابراین، شیئهای مورد بحث، دنباله‌هایی نامتناهی از توزیعها هستند که در آنها هر توزیع تکیه‌گاهی متناهی دارد. چنان دنباله‌ای یک جرگهٔ[2] توزیعی نامیده می‌شود. ما جرگه‌های توزیعی به شکل $\{D_n\}_{n\in\mathbb{N}}$ را در نظر می‌گیریم که در آن برای تابعی مانند $l : \mathbb{N} \to \mathbb{N}$، تکیه‌گاه هر D_n زیرمجموعه‌ای از $\{0,1\}^{l(n)}$ است. به علاوه نوعاً l یک چندجمله‌ای مثبت خواهد بود. برای

۱. بررسی مجانبی (یا تابعی) در این رهیافت جنبهٔ اساسی ندارد. می‌توان کل رهیافت را برحسب ورودیهای با طولهای ثابت و مفهومی مناسب از پیچیدگی الگوریتمها به پیش برد. ولی چنان شیوه‌ای پرزحمت‌تر است.

2. ensemble

چنان D_nای، فرایند انتخاب e مطابق توزیع D_n را با $e \sim D_n$ نشان می‌دهیم بنابراین، برای محمولی مانند P، احتمال آن را که $P(e)$ برقرار باشد وقتی که e مطابق با D_n توزیع (یا انتخاب) شده باشد با $\Pr_{e\sim D_n}[P(e)]$ نشان می‌دهیم

تعریف ۱. (تمایزناپذیری محاسباتی [۸، ۱۳]). دو چگونهٔ احتمال $\{X_n\}_{n\in\mathbb{N}}$ و $\{Y_n\}_{n\in\mathbb{N}}$ تمایز ناپذیر محاسباتی نامیده می‌شوند هرگاه برای هر الگوریتم زمان‌چندجمله‌ای احتمالاتی مانند A، هر چندجمله ی مثبت مانند p، و همهٔ nهای به قدر کافی بزرگ،

$$\left|\Pr_{x\sim X_n}[A(x)=1]-\Pr_{y\sim Y_n}[A(y)=1]\right|<\frac{1}{p(n)}$$

احتمال روی X_n (به‌ترتیب، Y_n) و نیز روی پرتابهای سکهٔ الگوریتم A اختیار می‌شود.

در اینجا چند تذکر لازم است. نخست اینکه اجازه داده‌ایم الگوریتم A، که متمایزکننده نام دارد، احتمالاتی باشد. این کار، شرط را صرفاً قویتر می‌کند، و برای چندین جنبهٔ مهم رهیافت ما اساسی به نظر می‌رسد. دوم، ما پیشامدهایی را که کران بالای احتمال رخ‌دادن آنها عکس یک، چندجمله‌ای است، صرف‌نظرکردنی تلقی می‌کنیم. این امر با مفهوم کارآیی (یعنی محاسبات زمان‌چندجمله‌ای) به‌خوبی جفت‌وجور می‌شود: پیشامدی که با احتمالی صرف‌نظرکردنی (به‌عنوان تابعی از پارامتری مانند n) رخ می‌دهد در صورتی هم که آزمایش به دفعاتی برابر یک، چندجمله‌ای برحسب n تکرار شود، با احتمالی صرف‌نظرکردنی رخ خواهد داد. سوم، وقتی در تعریف بالا به A اجازه دهیم که تابعی داخواه (به جای الگوریتم زمان‌چندجمله‌ای احتمالاتی) باشد، یک مفهوم تمایزناپذیری آماری را به‌دست خواهیم آورد. مفهوم اخیر معادل با این شرط است که فاصلهٔ تغییرات بین X_n و Y_n (یعنی $\sum_z |X_n(z)-Y_n(z)|$) (نسبت به n) ناچیز است.

یادآور می‌شویم که تمایزناپذیری محاسباتی مفهومی بسیار آزادتر از تمایزناپذیری آماری است (رک. [۱۳]). حالتی مهم، آن است که توزیعها به توسط یک مولد شبه‌تصادفی (به صورتی که ذیلاً تعریف می‌شود) تولید شوند: چنان توزیعهایی از نظر محاسباتی از توزیع یکنواخت تمایزناپذیرند، اما از نظر آماری از توزیع یکنواخت غیرقابل تمایز نیستند.

تعریف ۲. (مولدهای شبه‌تصادفی [۲، ۱۳]). یک الگوریتم زمان‌چندجمله‌ای تعیینی مانند G مولد شبه‌تصادفی نامیده می‌شود هرگاه تابعی کش‌آورنده مانند $l:\mathbb{N}\to\mathbb{N}$ موجود باشد به‌طوری که دو جرگهٔ احتمال زیر، که با $\{G_n\}_{n\in\mathbb{N}}$ و $\{R_n\}_{n\in\mathbb{N}}$ نشان داده می‌شوند، تمایزناپذیر محاسباتی باشند:

۱. توزیع G_n به عنوان خروجی G روی بذری که به‌طور یکنواخت انتخاب شده، در $\{0,1\}^n$ تعریف می‌شود.

۲. توزیع R_n به‌عنوان توزیع یکنواخت بر $\{0,1\}^{l(n)}$ تعریف می‌شود.

یعنی، با نشان دادن توزیع یکنواخت روی $\{0,1\}^m$ با U_m، قید می‌کنیم که برای هر الگوریتم زمان‌چندجمله‌ای احتمالاتی مانند A، هر چندجمله‌ای مثبت مانند p، و همهٔ nهای به‌قدر کافی بزرگ،

$$\left|\Pr_{s\sim U_n}[A(G(s))=1]-\Pr_{r\sim U_{l(n)}}[A(r)=1]\right|<\frac{1}{p(n)}$$

بنابراین، مولدهای شبه‌تصادفی برنامه‌های تعیینی کارآ (یعنی زمان‌چندجمله‌ای) هستند که بذرهای کوتاه به تصادف انتخاب شده را منبسط کرده به صورت دنباله‌های بیتی شبه‌تصادفی بلندتر درمی‌آورند به‌طوری که دنباله‌های اخیر به صورت تمایزناپذیر محاسباتی از دنباله‌های واقعاً تصادفی، به وسیلهٔ الگوریتمهای کارآ (یعنی، زمان‌چندجمله‌ای) تعریف می‌شوند. نتیجه می‌گیریم که هر الگوریتم تصادفی‌شدهٔ کارآ نحوهٔ اجرای خود را، در صورتی که به‌جای پرتابهای سکهٔ درونی دنباله‌هایی قرار دهیم که به‌وسیلهٔ یک مولد شبه‌تصادفی تولید شده‌اند، حفظ می‌کند. یعنی

ساختمان ۳. (کاربرد نوعی مولدهای شبه تصادفی). فرض کنید که A یک الگوریتم زمان‌چندجمله‌ای احتمالاتی باشد، و فرض کنید که $\rho(n)$ معرف کرانی بالا برای پیچیدگی تصادفی بودن آن (یعنی تعداد سکه‌هایی که A روی ورودیهای n بیتی پرتاب می‌کند) باشد. همچنین تصورکنید که $A(x,r)$ معرف خروجی A روی ورودی x و دنبالهٔ پرتاب سکهٔ $r\in\{0,1\}^{\rho(|x|)}$ باشد. حال فرض کنید که G یک مولد شبه‌تصادفی با تابع کش‌آورندهٔ $l:\mathbb{N}\to\mathbb{N}$ باشد. در این صورت A_G یک الگوریتم تصادفی‌شده است که روی ورودی x به صورت زیر عمل می‌کند. عدد $k=k(|x|)$ را به‌عنوان کوچکترین عدد صحیح به‌طوری که $l(k)\geq\rho(|x|)$ قرار می‌دهد، به‌طور یکنواخت $s\in\{0,1\}^k$ را انتخاب می‌کند، و خروجی $A(x,r)$ را می‌دهد که در آن r پیشوندِ به طول $\rho(|x|)$ بیتِ $G(s)$ است.

می‌توان ثابت کرد که پیدا کردن xهای بلندی که روی آنها رفتار ورودی–خروجی A_G به‌طور محسوس متفاوت از آن A باشد، نشدنی است، گرچه A_G ممکن است از تعداد پرتابهای به مراتب کمتری در مقایسه با A استفاده کند. این موضوع در قضیهٔ زیر مدون شده است که در آن F معرف الگوریتمی است در پی یافتن x به گونه‌ای که $A(x)$ و $A_G(x)$ (به کمک الگوریتمی مانند D) قابل تمیز باشند.

قضیهٔ [فرعی] ۴. فرض کنید A و G به‌صورتی باشند که در بالا گفته شد. برای هر الگوریتم D، فرض کنید $\Delta_{A,D}(x)$ معرف اختلاف در رفتار A و A_G، به قضاوت D، روی ورودی x باشد یعنی $\Delta_{A,D}(x)$ به صورت زیر تعریف شود

$$\left|\Pr_{r\sim U_{\rho(n)}}[D(x,A(x,r))=1]-\Pr_{s\sim U_{k(n)}}[D(x,A_G(x,s))=1]\right|$$

که در آن احتمالها روی همهٔ U_mها و نیز روی کلیهٔ پرتابهای سکهٔ D گرفته شده‌اند. در این صورت برای هر جفت از الگوریتمهای زمان‌چندجمله‌ای احتمالاتی F و D، هر چندجمله‌ای مثبت p، و همهٔ nهای به قدر کافی بزرگ داریم

$$\Pr\left[\Delta_{A,D}(F(1^n))>\frac{1}{p(n)}\right]<\frac{1}{p(n)}$$

که در آن احتمال روی همهٔ پرتابهای سکه F گرفته می‌شود.

این قضیه با نشان دادن این موضوع ثابت می‌شود که یک سه‌تایی (A,F,D) را که حکم را نقض می‌کند می‌توان به الگوریتمی مانند D'

برگرداند که خروجی G را از توزیع یکنواخت متمایز می‌کند، و این برخلاف فرض است. با استدلالهای مشابهی می‌توان ثابت کرد که فرایند تصادفی‌شدهٔ کارآ (خواه مانند بالا الگوریتمی باشد و خواه محاسبه‌ای چندبخشی)، اگر شبه‌تصادفی بودن (با تعریف بالا) جانشین تصادفی بودن واقعی شود، رفتارش را حفظ می‌کند. بنابراین، با در دست داشتن مولدهای شبه‌تصادفی با تابع کش‌آوری بزرگ، می‌توان به‌طور قابل ملاحظه‌ای پیچیدگی تصادفی را در هر کاربرد کارآ کاهش داد.

تقویت تابع کش‌آوری

از مولدهای شبه‌تصادفی، به صورتی که در بالا تعریف شده‌اند، تنها انتظار می‌رود که ورودی خود را یک بیت کش بیاورند؛ مثلاً، کش‌آوردن ورودیهای به طول nبیت به خروجیهای به طول $(n+1)$بیت کفایت می‌کند. روشن است که مولدهایی با چنین تابعهای کش‌آوری میانه‌روی در عمل کمتر به درد می‌خورند. در مقابل، می‌خواهیم مولدهای شبه‌تصادفی با تابعهای کش‌آوریِ به دلخواه طویل داشته باشیم. بنابر شرط کارآیی، تابع کش‌آوری می‌تواند حداکثر چندجمله‌ای باشد. نتیجه آن می‌شود که مولدهای شبه‌تصادفی با کوچکترین تابعهای کش‌آوری ممکن را می‌توان برای ساختن مولدهای شبه‌تصادفی با هر تابع کش‌آوری چندجمله‌ای موردنظر به کار برد. (بنابراین، وقتی بحث از وجود مولدهای شبه‌تصادفی در میان است، می‌توانیم تابعهای کش‌آوری مشخص را نادیده بگیریم.)

قضیهٔ ۵. [۵، بخش ۲.۳.۳]. فرض کنید G یک مولد شبه‌تصادفی با تابع کش‌آوری $l(n)=n+1$ باشد و تصور کنید که l' هر تابع کش‌آوری دلخواه باشد به‌طوری که $l'(n)$ در زمان چندجمله‌ای برحسب n قابل محاسبه باشد. همچنین فرض کنید $G_1(x)$ معرف پیشوند به طول $|x|$ بیت $G(x)$ باشد و $G_2(x)$ معرف آخرین بیت $G(x)$ باشد (یعنی $G(x)=G_1(x)G_2(x)$). در این صورت

$$G'(S) \overset{\text{تعریف}}{=} \sigma_1\sigma_2\cdots\sigma_{l'(|s|)}$$

که در آن $x_0=s$، $\sigma_i=G_2(x_{i-1})$، و $x_i=G_1(x_{i-1})$ به ازای

$$i=1,\cdots,l'(|s|)$$

یک مولد شبه‌تصادفی با تابع کش‌آوری l' است.

چگونگی ساختن مولدهای شبه‌تصادفی

روشهای شناخته شده برای ساختن این مولدها، مشکل محاسباتی را در قالب تابعهای یکطرفه (که در زیر تعریف می‌شود) به مولدهای شبه‌تصادفی بودن تبدیل می‌کنند. به بیان غیردقیق، یک تابع محاسبه‌پذیر زمان‌چندجمله‌ای، یکطرفه نامیده می‌شود هرگاه هر الگوریتم کارآ بتواند آن را تنها با احتمال موفقیت صرف‌نظرکردنی وارون کند. برای سهولت، تنها تابعهای یکطرفهٔ طول نگهدار را در نظر می‌گیریم.

تعریف ۶. (تابع یکطرفه). هر تابع یکطرفه مانند f، یک تابع محاسبه‌پذیر زمان‌چندجمله‌ای است به‌طوری که برای هر الگوریتم زمان‌چندجمله‌ای احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدر کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x))\in f^{-1}(f(x))\right]<\frac{1}{p(n)}$$

که در آن U_n توزیع یکنواخت بر $\{0,1\}^n$ است.

در مورد تابعهای یکطرفه، کاندیداهای رایج بر مهارناپذیری[1] حدسی تجزیهٔ اعداد صحیح به عوامل اول، مسألهٔ لگاریتمی گسسته، و کدگشایی کدهای تصادفی خطی مبتنی هستند. ناشدنی بودن وارونسازی f، مفهومی ضعیف از پیشگویی‌ناپذیری را عاید می‌کند: فرض کنید $b_i(x)$ معرف بیت i ام x باشد. در این صورت، برای هر الگوریتم زمان‌چندجمله‌ای مانند

$$\Pr_{i,x}\left[A(i,f(x))\neq b_i(x)\right]>1/2n$$

که در آن احتمال به‌طور یکنواخت روی $i\in\{1,2,\cdots,n\}$ و $x\in\{0,1\}^n$ گرفته شده است. مفهومی قویتر (و در واقع، قویترین مفهوم ممکن) از پیشگویی‌ناپذیری همانا محمول «هسته‌ای» است. به بیان غیردقیق، یک محمول قابل محاسبهٔ زمان‌چندجمله‌ای چون b، هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه هر الگوریتم کارآ، با معلوم‌بودن $f(x)$، بتواند $b(x)$ را با احتمال موفقیتی که تنها به‌طور صرف‌نظرکردنی بیشتر از نیم باشد، حدس بزند.

تعریف ۷. (محمول هسته‌ای [۲]). یک محمول قابل محاسبهٔ زمان‌چندجمله‌ای مانند $b:\{0,1\}^*\to\{0,1\}$ هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه برای هر الگوریتم زمان‌چندجمله‌ای احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدر کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x))=b(x)\right]<\frac{1}{2}+\frac{1}{p(n)}$$

آشکار است که هرگاه b هستهٔ تابع یک‌به‌یک محاسبه‌پذیر زمان‌چندجمله‌ای f باشد، آنگاه f باید یکطرفه باشد[2]. نتیجه آنکه هر تابع یکطرفه را می‌توان اندکی بهبود بخشید به‌طوری که محمولی هسته‌ای داشته باشد.

قضیهٔ ۸. (یک هستهٔ عام [۷]). فرض کنید که f تابع یکطرفهٔ دلخواهی باشد، و تصور کنید g به صورت $g(x,r)\overset{\text{تعریف}}{=}(f(x),r)$ معرف شود که در آن $|r|=|x|$. حال فرض کنید $b(x,r)$ معرف ضرب داخلی بردارهای دودویی x و r به پیمانهٔ ۲ باشد. در این صورت محمول b یک هستهٔ تابع g است.

برهانی از این قضیه را می‌توان در [۵، پیوست C.۲] یافت. سرانجام به ساختمان مولدهای شبه‌تصادفی می‌رسیم.

قضیهٔ [فرعی] ۹. (شیوهٔ ساده‌ای برای ساخت مولدهای شبه‌تصادفی). احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدر کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x))\in f^{-1}(f(x))\right]<\frac{1}{p(n)}$$

که در آن U_n توزیع یکنواخت بر $\{0,1\}^n$ است.

در مورد تابعهای یکطرفه، کاندیداهای رایج بر مهارناپذیری[1] حدسی تجزیهٔ اعداد صحیح به عوامل اول، مسألهٔ لگاریتمی گسسته، و کدگشایی کدهای تصادفی خطی مبتنی هستند. ناشدنی بودن وارونسازی f، مفهومی ضعیف از پیشگویی‌ناپذیری را عاید می‌کند: فرض کنید $b_i(x)$ معرف بیت i ام x باشد. در این صورت، برای هر الگوریتم زمان‌چندجمله‌ای مانند

$$\Pr_{i,x}\left[A(i,f(x))\neq b_i(x)\right]>1/2n$$

که در آن احتمال به‌طور یکنواخت روی $i\in\{1,2,\cdots,n\}$ و $x\in\{0,1\}^n$ گرفته شده است. مفهومی قویتر (و در واقع، قویترین مفهوم ممکن) از پیشگویی‌ناپذیری همانا محمول «هسته‌ای» است. به بیان غیردقیق، یک محمول قابل محاسبهٔ زمان‌چندجمله‌ای چون b، هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه هر الگوریتم کارآ، با معلوم‌بودن $f(x)$، بتواند $b(x)$ را با احتمال موفقیتی که تنها به‌طور صرف‌نظرکردنی بیشتر از نیم باشد، حدس بزند.

تعریف ۷. (محمول هسته‌ای [۲]). یک محمول قابل محاسبهٔ زمان‌چندجمله‌ای مانند $b:\{0,1\}^*\to\{0,1\}$ هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه برای هر الگوریتم زمان‌چندجمله‌ای احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدر کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x))=b(x)\right]<\frac{1}{2}+\frac{1}{p(n)}$$

آشکار است که هرگاه b هستهٔ تابع یک‌به‌یک محاسبه‌پذیر زمان‌چندجمله‌ای f باشد، آنگاه f باید یکطرفه باشد[2]. نتیجه آنکه هر تابع یکطرفه را می‌توان اندکی بهبود بخشید به‌طوری که محمولی هسته‌ای داشته باشد.

قضیهٔ ۸. (یک هستهٔ عام [۷]). فرض کنید که f تابع یکطرفهٔ دلخواهی باشد، و تصور کنید g به صورت $g(x,r)\overset{\text{تعریف}}{=}(f(x),r)$ معرف شود که در آن $|r|=|x|$. حال فرض کنید $b(x,r)$ معرف ضرب داخلی بردارهای دودویی x و r به پیمانهٔ ۲ باشد. در این صورت محمول b یک هستهٔ تابع g است.

برهانی از این قضیه را می‌توان در [۵، پیوست C.۲] یافت. سرانجام به ساختمان مولدهای شبه‌تصادفی می‌رسیم.

قضیهٔ [فرعی] ۹. (شیوهٔ ساده‌ای برای ساخت مولدهای شبه‌تصادفی).

---

1 intractability

۲. تابعهایی که یک‌به‌یک نیستند، ممکن است محمولهای هسته‌ای با ماهیت نظریهٔ اطلاعی داشته باشند، اما این تابعها در اینجا به درد ما نمی‌خورند. مثلاً، تابعهایی به شکل

$$f(\sigma,x)=0f'(x)$$

(برای $\sigma\in\{0,1\}$) دارای یک محمول هسته‌ای «نظریهٔ اطلاعی» مانند $b(\sigma,x)=\sigma$ هستند.

فرض کنید b یک محمول هسته‌ای تابع محاسبه‌پذیر زمان‌چندجمله‌ای f باشد، در این صورت

$$G(s) \stackrel{\text{تعریف}}{=} f(s)b(s)$$

(یعنی $f(s)$ و پس از آن $b(s)$) یک مولد شبه‌تصادفی است.

به یک معنی، نکتهٔ اصلی در برهان قضیهٔ بالا عبارت از اثبات آن است که پیشگویی‌ناپذیری خروجی G (که بنا به تعریف واضح است) مستلزم شبه‌تصادفی بودن آن است. این حقیقت که پیشگویی‌ناپذیری (بیت بعدی) و شبه‌تصادفی بودن در حالت کلی معادل‌اند، در توصیف دیگری از موضوع که در زیر می‌آید، به صراحت ثابت می‌شود.

توصیف دیگر

شیوه‌ای که برای ساخت مولدهای شبه‌تصادفی، از طریق قضیه‌های ۵ و ۹، عرضه کردیم، متفاوت اما مشابه با طرز ساخت مولدهای شبه‌تصادفی است که **به‌وسیلهٔ** بلوم و میکالی [۲] مطرح شده است: با مفروض بودن تابع‌کش‌آوری دلخواه $l : \mathbb{N} \to \mathbb{N}$ و یک تابع یکطرفهٔ یک‌به‌یک با هستهٔ b، تعریف می‌کنیم

$$G(s) \stackrel{\text{تعریف}}{=} b(x_0)b(x_1)\cdots b(x_{l(|s|)-1})$$

که در آن $x_0 = s$ و $x_i = f(x_{i-1})$ به ازای $i = 1, \cdots, l(|s|) - 1$. یک مصداق ملموس، بر مبنای این فرض که تجزیهٔ اعداد صحیح بزرگ کاری دشوار است، در شکل ۱ شرح داده شده است. شبه‌تصادفی بودن G در دو گام با استفاده از مفهوم پیشگویی‌ناپذیری (بیت بعدی) برقرار شده است. جرگه‌ای چون $\{Z_n\}_{n\in\mathbb{N}}$ پیشگویی‌ناپذیر نامیده می‌شود هرگاه هیچ ماشین زمان‌چندجمله‌ای احتمالاتی که پیشوندی از Z_n را به‌دست می‌آورد، قادر به پیشگویی بیت بعدی آن با احتمالی که به طور صرف‌نظرناکردنی بزرگتر از ۱/۲ است، نباشد.

گام ۱. ابتدا ثابت می‌کنیم که جرگهٔ $\{G(U_n)\}_{n\in\mathbb{N}}$، که در آن U_n توزیع یکنواخت روی $\{0,1\}^n$ است، پیشگویی‌ناپذیر (از لحاظ بیت بعدی) است (از راست به چپ [۲]). به بیانی غیردقیق، اگر بتوان $b(x_i)$ را از روی $b(x_{i+1})\ldots b(x_{l(|s|)-1})$ پیشگویی کرد آنگاه می‌توان $b(x_i)$ را با مفروض‌بودن $f(x_i)$ پیشگویی کرد (یعنی، با محاسبهٔ x_{i+1}، x_{i+2}، ...، $x_{l(|s|)-1}$ و به این ترتیب، به‌دست آوردن $b(x_{i+1})\cdots b(x_{l(|s|)-1})$). اما این نتیجه با فرض هسته در تناقض است.

گام ۲. سپس از نتیجه‌گیری بالا استفاده می‌کنیم که بنابر آن یک جرگهٔ شبه‌تصادفی است اگر و تنها اگر پیشگویی‌ناپذیر (از لحاظ بیت بعدی) باشد (رک. ۴، بخش ۳.۳.۴).

روشن است که اگر بتوان بیت بعدی را در یک جرگه پیشگویی کرد، آنگاه می‌توان این جرگه را از جرگهٔ یکنواخت تمیز داد (که صرف‌نظر از توان محاسبه، پیشگویی‌ناپذیر است). ولی ما طرف دیگر را که کمتر بدیهی است لازم داریم. می‌توان نشان داد که پیشگویی‌ناپذیری (بیت بعدی) مستلزم تمایزناپذیری از جرگهٔ یکنواخت است. به طور مشخص، توزیعهای «دورگه»‌ای را در نظر بگیرید که در آن دورگهٔ iام، i بیت نخست را از جرگهٔ مورد بحث و بقیه

فرض می‌کنیم که تجزیهٔ اعداد صحیحی که حاصلضرب دو عدد اول بزرگ‌اند (هر یک همنهشت با ۳ به پیمانهٔ ۴) ناشدنی باشد. تحت این فرض، مجذورکردن به پیمانهٔ چنان اعداد صحیحی یک تابع یکطرفه خواهد بود. به علاوه، مجذورکردن به پیمانهٔ چنان Nای روی مانده‌های مربعی به پیمانهٔ N یک‌به‌یک است، و کم‌معناترین بیت شناسه، یک هستهٔ متناظر است [۱].

مولد شبه‌تصادفی زیر از یک الگوریتم زمان‌چندجمله‌ای استفاده می‌کند که وقتی $4m$ بیت به آن خورانده شود، عددی mبیتی تولید می‌کند به‌طوری که وقتی ورودیهای $4m$بیتی به صورت یکنواخت توزیع شده باشند، خروجی اساساً یک عدد اول تصادفی mبیتی (همنهشت با ۳ به پیمانهٔ ۴) است.

ورودی: یک بذر nبیتی $s = abc$، که در آن $|a| = |b| = 4n/10$.

گامهای آغازی:

۱. با استفاده از a، عدد اول $n/10$ بیتی (به پیمانهٔ ۴) $p \equiv 3$ را تولید کنید.

۲. به همین نحو، از b استفاده کرده، (به پیمانهٔ ۴) $q \equiv 3$ را تولید کنید.

۳. p را در q ضرب کنید و N را به‌دست آورید.

۴. فرض کنید (به پیمانهٔ N) $x_0 \leftarrow c^2$.

تکرارها: برای $i = 0, \cdots, l(n) - 1$

۵. فرض کنید b_i کم‌معناترین بیت x_i باشد.

۶. فرض کنید (به پیمانهٔ N) $x_{i+1} \leftarrow x_i^2$.

خروجی: $b_0, b_1, \cdots, b_{l(n)-1}$.

شکل ۱ یک مولد شبه‌تصادفی بر مبنای اجرا ناشدنی بودن تجزیه به عاملها.

را از توزیع یکنواخت اختیار می‌کند. بنابراین، تمیزدادن دورگه‌های کرانگینی مستلزم تمیزدادن برخی دورگه‌های همسایه است که به نوبهٔ خود مستلزم پیشگویی‌ناپذیری بیت بعدی (در جرگهٔ مورد بحث) است.

شرطی عام برای وجود مولدهای شبه‌تصادفی

به خاطر آورید که با مفروض بودن هر تابع یک‌به‌یک یکطرفه، می‌توان به‌آسانی یک مولد شبه‌تصادفی ساخت. درواقع، می‌توان شرط یک‌به‌یک بودن را کنار گذاشت، اما شیوهٔ فعلاً معلوم برای ساخت ــ در حالت کلی ــ کاملاً پیچیده است. با این‌حال، داریم:

قضیهٔ ۱۰. (دربارهٔ وجود مولدهای شبه‌تصادفی [۹]). مولدهای شبه‌تصادفی موجودند اگر و تنها اگر تابعهای یکطرفه موجود باشند.

برای نشان دادن اینکه وجود مولدهای شبه‌تصادفی مستلزم وجود تابعهای یکطرفه است، مولدی شبه‌تصادفی مانند G را با تابع کش‌آوری $l(n) = 2n$ در نظر بگیرید. برای هر $x, y \in \{0,1\}^n$، تعریف کنید $f(x,y) \stackrel{\text{تعریف}}{=} G(x)$

به طوری که f محاسبه‌پذیر زمان‌چندجمله‌ای (و طول نگهدار) باشد. باید f یکطرفه باشد چه در غیر این‌صورت می‌توان $G(U_n)$ را از U_{2n}، با تلاش برای وارون کردن و امتحان کردن نتیجه، تمیز داد: وارون کردن f روی توزیع دامنهٔ آن به توزیع $G(U_n)$ باز می‌گردد، درحالی که احتمال اینکه U_{2n} تحت f دارای وارون باشد، صرف‌نظرکردنی است.

مسیر جالب توجه، ساختن مولدهای شبه‌تصادفی براساس هر تابع یکطرفه دلخواه است. در حالت کلی (وقتی که f ممکن است یک به یک نباشد)، جرگهٔ $f(U_n)$ ممکن است شبه‌تصادفی نباشد، و بنابراین ساختمان ۹، (یعنی $G(s) = f(s)b(s)$، که در آن b یک هستهٔ f است) نمی‌تواند مستقیماً مورد استفاده قرار گیرد. در عوض این ساختمان همراه با چند ایدهٔ دیگر به‌کار می‌رود (رک. [۹]). متأسفانه، این ایده‌ها و بیشتر از آن، جزئیات به اجرا درآوردن آنها به‌مراتب پیچیده‌تر از آن هستند که بتوان در اینجا توصیفشان کرد. درواقع شیوهٔ دیگری برای ساخت مولدهای شبه‌تصادفی بر مبنای هر تابع یکطرفهٔ دلخواه ارزش بیشتری دارد.

تابعهای شبه‌تصادفی

مولدهای شبه‌تصادفی امکان تولید کارآی دنباله‌های شبه‌تصادفی بلند را از بذرهای تصادفی کوتاه فراهم می‌آورند. تابعهای شبه‌تصادفی (که در زیر تعریف می‌شوند) از این هم نیرومندترند: آنها امکان دسترسی کارآی مستقیم به دنبالهٔ شبه‌تصادفی عظیمی را (که بررسی بیت به بیت آن ناشدنی است) فراهم می‌آورند. به عبارت دیگر، تابعهای شبه‌تصادفی را می‌توان در هرکاربرد کارآ (مثلاً، قابل ذکرتر از همه در رمزنگاری) به جای تابعهای واقعاً تصادفی قرار داد. یعنی، تابعهای شبه‌تصادفی از تابعهای تصادفی به‌وسیلهٔ ماشینهای کارآیی که مقادیر تابعها را در شناسه‌هایی به انتخاب خود به‌دست می‌آورند، قابل تمایز نیستند. چنان ماشینهایی ماشینهای مکاشفه[1] نامیده می‌شوند؛ و اگر M چنان ماشینی باشد و f یک تابع باشد، آنگاه $M^f(x)$ معرف محاسبهٔ M روی ورودی x است وقتی پرسشهای M به‌وسیلهٔ تابع f پاسخ داده می‌شوند.

تعریف ۱۱. (تابعهای شبه‌تصادفی [۶]). یک تابع شبه‌تصادفی (جرگه)، با پارامترهای طول $l_D, l_R : \mathbb{N} \to \mathbb{N}$، مجموعه‌ای از تابعهای

$$F \stackrel{\text{تعریف}}{=} \{f_s : \{0,1\}^{l_D(|s|)} \to \{0,1\}^{l_R(|s|)}\}_{s\in\{0,1\}^*}$$

است که در شرطهای زیر صدق می‌کند:

- (محاسبهٔ کارآ). یک الگوریتم کارآی (تعیینی) موجود است به‌طوری که وقتی یک بذر، s و یک شناسهٔ $l_D(|s|)$ بیتی، x، داده شده باشد، مقدار $f_s(x)$ به طول $l_R(|s|)$ را باز می‌گرداند.

  (بنابراین، بذر s «توصیف کارآیی» از تابع f_s است.)

- (شبه‌تصادفی بودن). برای هر ماشین مکاشفهٔ زمان‌چندجمله‌ای احتمالاتی مانند M، هر چندجمله‌ای مثبت مانند p، و همهٔ nهای به قدر کافی بزرگ،

$$\left|\Pr_{f\sim F_n}[M^f(1^n) = 1] - \Pr_{\rho\sim R_n}[M^\rho(1^n) = 1]\right| < \frac{1}{p(n)}$$

که در آن F_n معرف توزیع روی $f_s \in F$ است که با انتخاب s به‌طور یکنواخت در $\{0,1\}^n$ به‌دست آمده است و R_n معرف توزیع یکنواخت روی کلیهٔ تابعهایی است که $\{0,1\}^{l_D(n)}$ را به $\{0,1\}^{l_R(n)}$ می‌نگارند.

برای سهولت فرض کنید که $l_D(n) = n$ و $l_R(n) = 1$. در این صورت تابعی که به‌طور یکنواخت از بین 2^n تابع (از یک جرگهٔ شبه‌تصادفی) انتخاب شده است، در زمان چندجمله‌ای برحسب n، یک رفتار ورودی-خروجی تمایزناپذیر از رفتار تابعی که به تصادف از بین کلیهٔ 2^{2^n} تابع بولی انتخاب شده است، نشان می‌دهد. این را با توزیعی روی 2^n دنباله، که با یک مولد شبه‌تصادفی به‌کار رفته در مورد یک بذر تصادفی nبیتی تولید شده است، مقایسه کنید. بذر اخیر غیرقابل تمایز از دنباله‌ای است که به‌طور یکنواخت از بین همهٔ چندجمله‌ای برحسب 2^n دنباله انتخاب شده است. در عین حال، تابعهای شبه‌تصادفی را می‌توان از روی هر مولد شبه‌تصادفی ساخت.

قضیهٔ ۱۲. (چگونگی ساختن تابعهای شبه‌تصادفی [۶]). فرض کنید که G یک مولد شبه‌تصادفی با تابع کش‌آوری $l(n) = 2n$ باشد. همچنین فرض کنید $G_0(s)$ (به ترتیب، $G_1(s)$) معرف نخستین (به ترتیب، آخرین) $|s|$ بیت در $G(s)$ باشد، و

$$G_{\sigma_{|s|}\cdots\sigma_2\sigma_1}(s) \stackrel{\text{تعریف}}{=} G_{\sigma_{|s|}}(\cdots G_{\sigma_2}(G_{\sigma_1}(s))\cdots)$$

در این صورت جرگهٔ تابعی $\{f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}\}_{s\in\{0,1\}^*}$، که در آن $f_s(x) \stackrel{\text{تعریف}}{=} G_x(s)$، شبه‌تصادفی با پارامترهای طول $l_D(n) = l_R(n) = n$ است.

شیوهٔ ساخت بالا را می‌توان به آسانی در مورد هر نوع پارامترهای طول (که کرانی به صورت چندجمله‌ای داشته باشند):

$$l_D, l_R : \mathbb{N} \to \mathbb{N}$$

به کار برد.

متذکر می‌شویم که تابعهای شبه‌تصادفی برای استخراج نتایج منفی در نظریهٔ یادگیری محاسباتی و نظریهٔ پیچیدگی به‌کار رفته‌اند.

کاربردپذیری مولدهای شبه‌تصادفی

شبه‌تصادفی بودن نقشی با اهمیت روزافزون در محاسبات ایفا می‌کند: اغلب در طرح الگوریتمهای دنباله‌ای، موازی، و توزیع شده به‌کارگرفته می‌شود و البته نقشی مرکزی در رمزنگاری دارد. هر چند طرح چنین الگوریتمهایی با استفادهٔ آزادانه از تصادفی بودن، آسان است اما در عین حال مطلوب آن است که استفاده از تصادفی بودن در اجراهای واقعی به حداقل برسد زیرا تولید کردن بیتهای کاملاً تصادفی از طریق سخت‌افزار ویژه بسیار گران است. بنابراین، مولدهای شبه‌تصادفی (به‌صورتی که در بالا تعریف شدند) جزء اصلی در یک «جعبه ابزار الگوریتمی» است: این مولدها برنامه‌های مترجم خودکاری برای برگرداندن برنامه‌هایی که آزادانه از تصادفی بودن استفاده می‌کنند به برنامه‌هایی که استفادهٔ صرفه‌جویانه‌ای از تصادفی بودن به‌عمل می‌آورند، در اختیار می‌گذارند.

درواقع، «مولدهای اعداد شبه‌تصادفی» با نخستین کامپیوترها به عرصه درآمدند. با این‌حال، در اجراهای نوعی از مولدهایی استفاده می‌کنند که

1. oracle machines

بنابر تعریف بالا شبه‌تصادفی نیستند. در عوض، نشان داده می‌شود که این مولدها، در بهترین حالت، برخی آزمونهای آماری خاص را با موفقیت از سر می‌گذرانند. (رک. [۱۰]). با این‌حال، این حقیقت که یک «مولد اعداد شبه‌تصادفی» برخی آزمونهای آماری را با موفقیت می‌گذراند، به این معنی نیست که آزمون جدیدی را خواهد گذراند یا برای کاربردی (آزمون نشده) در آینده مناسب خواهد بود. به‌علاوه، رهیافتِ قراردادنِ مولد در معرض برخی آزمونهای خاص، قادر به تأمین نتایج کلی از نوعی که در بالا بیان شد، نیست (یعنی، به شکل «برای کلهٔ مقاصد عملی، استفاده از خروجی مولد، همان حسن را دارد که استفاده از پرتابهای سکهٔ نااریب واقعی»). در مقابل، رهیافتی که در تعریف ۲ مندرج است، چنان کلیتی را هدف خود قرار می‌دهد و درواقع برای به‌دست آوردن آن طرح‌ریزی شده است: مفهوم تمایزناپذیری محاسباتی، که زمینهٔ تعریف ۲ ـ ست، کلیهٔ کاربردهای ممکن کارآ را دربرمی‌گیرد و مبتنی بر این فرض است که برای همهٔ آنها، دنباله‌های شبه‌تصادفی به‌خوبی دنباله‌های واقعاً تصادفی‌اند.

مولدها و تابعهای شبه‌تصادفی در رمزنگاری اهمیت اساسی دارند. آنها نوعاً برای ایجاد طرحهای رمزگذاری کلیدْ شخصی[1] و تعیین صحت به‌کار می‌روند (رک. [۵، بخشهای ۲.۵.۱ و ۲.۶.۱]). به عنوان مثال، فرض کنید که دو گروه در یک رشتهٔ تصادفی nبیتی مانند s، که یک تابع شبه‌تصادفی را (مطابق تعریف ۱۱ با $l_D(n) = l_R(n) = n$) مشخص می‌کنند، شریک‌اند، و s برای رقیب آنها نامعلوم است. در این صورت دو گروه مزبور می‌توانند پیامهایی رمزی را با XOR[2] کردن پیام با مقدار f_s در نقطه‌ای تصادفی به یکدیگر ارسال کنند، یعنی برای رمزگذاری $m \in \{0,1\}^n$، فرستنده به‌طور یکنواخت $r \in \{0,1\}^n$ را انتخاب و $(r, m \oplus f_s(r))$ را به گیرنده می‌فرستد. امنیت این طرح رمزگذاری بر این حقیقت متکی است که برای هر رقیبِ از نظر محاسباتی ممکن (نه تنها برای استراتژیهای رقیب که به تصور درآمده و مورد امتحان قرارگرفته‌اند)، مقادیر تابع f_s روی چنان rهایی تصادفی به نظر می‌رسد.

درونمایه‌های نظری مولدهای شبه‌تصادفی

اینک به اختصار برخی جنبه‌های نظری مولدهای شبه‌تصادفی را، به صورتی که در بالا تعریف شدند، مورد بحث قرار می‌دهیم.

رفتارشناخت در برابر هستی‌شناخت

تعریف ما از مولدهای شبه‌تصادفی مبتنی بر مفهوم تمایزناپذیری محاسباتی است. ماهیت رفتارشناختی مفهوم اخیر به بهترین نحو از مقایسهٔ آن با رهیافت کولموگوروف شایتین به تصادفی بودن، مدلل می‌شود. به بیان غیردقیق، یک رشتهٔ تصادفی ـ کولموگوروفی است هرگاه طول آن برابر با طول کوتاهترین برنامه‌ای باشد که آن را تولید می‌کند. این کوتاهترین برنامه را می‌توان «توضیح واقعی» پدیده‌ای که به‌وسیلهٔ آن رشته توصیف می‌شود، تلقی کرد. بنابراین یک رشتهٔ تصادفی ـ کولموگوروفی رشته‌ای است که توضیح اساساً ساده‌تری (یعنی کوتاهتری) در مقایسه با خودش نداشته باشد. در نظرگرفتن ساده‌ترین توضیح یک پدیده را می‌توان رهیافتی هستی‌شناختی تلقی کرد. در مقابل، در نظرگرفتن تأثیر پدیده (بر یک مشاهده‌گر) به‌عنوان زمینهٔ تعریفِ شبه‌تصادفی بودن، یک رهیافت رفتارشناختی است. به علاوه، توزیعهای احتمالی موجودند که یکنواخت نیستند (و حتی از نظر آماری به یک توزیع یکنواخت نزدیک نیستند) اما به وسیلهٔ هیچ شیوهٔ کارآیی از یک توزیع یکنواخت قابل تمایز نیستند. بنابراین، توزیعهایی که از نظر هستی‌شناختی بسیار متفاوت باشند، بنابر دیدگاه رفتارشناختی که در تعریف بالا اتخاذ شد، معادل تلقی می‌شوند.

دیدگاه نسبی‌گرایانه‌ای در بارهٔ تصادفی بودن

شبه‌تصادفی بودن در بالا نسبت به مشاهده‌گر آن تعریف شد. منظور از آن، توزیعی است که نمی‌توان آن را به‌وسیلهٔ هیچ مشاهده‌گر کارآ (یعنی، زمانْ‌چندجمله‌ای) از یک توزیع یکنواخت تمیز داد. با این‌حال، دنباله‌های شبه‌تصادفی را می‌توان از دنباله‌های تصادفی به‌وسیلهٔ کامپیوترهای بینهایت قدرتمند (که در اختیار ما نیستند!) تمیز داد. به‌طور مشخص، یک ماشین زمانْ‌نمایی می‌تواند به آسانی، خروجی یک مولد شبه‌تصادفی را از رشته‌ای با همان طول که به‌طور یکنواخت انتخاب شده است، تمیز دهد (مثلاً، فقط با امتحان کردن کلیهٔ بذرهای ممکن). بنابراین، شبه‌تصادفی بودن، امری ذهنی، و وابسته به تواناییهای مشاهده‌گر است.

تصادفی بودن و دشواری محاسباتی

شبه‌تصادفی بودن و دشواری محاسباتی نقشهایی دوگان یکدیگر دارند: تعریف شبه‌تصادفی بودن بر این حقیقت متکی است که قراردادن محدودیتهای محاسباتی بر مشاهده‌گر به توزیعهایی منجر می‌شود که یکنواخت نیستند ولی با این‌حال نمی‌توان آنها را از توزیع یکنواخت تمیز داد. به‌علاوه، ساختمان مولدهای شبه‌تصادفی متکی بر حدسهایی در بارهٔ دشواری محاسباتی (یعنی، وجود تابعهای یکطرفه) است، و این امر اجتناب‌ناپذیر است: با مفروض بودن یک مولد شبه‌تصادفی، می‌توانیم تابعهای یکطرفه بسازیم. بنابراین، شبه‌تصادفی بودنِ نابدیهی و دشواری محاسباتی را می‌توان با هم جابه‌جا کرد.

تعمیم

شبه‌تصادفی بودن را به‌صورتی که در بالا مرور شد، می‌توان حالت خاص مهمی از یک پارادیم [الگوی] کلی تلقی کرد. یک صورتبندی عام مولدهای شبه‌تصادفی عبارت است از مشخص کردن سه جنبهٔ بنیادی ــ اندازهٔ کش‌آوری مولدها، ردهٔ متمایزکنندگانی که انتظار می‌رود مولدها فریبشان بدهند (یعنی الگوریتمهایی که نسبت به آنها تمایزناپذیری محاسباتی باید برقرار باشد)، و منابعی که مولدها مجاز به استفاده از آنها هستند (یعنی، پیچیدگی محاسباتی خود آنها). در توصیف بالا، ما بر مولدهای زمانْ‌چندجمله‌ای عطف توجه کردیم (بنابراین اندازهٔ کش‌آوری چندجمله‌ای را داشتیم) که هر مشاهده‌گر زمانْ‌چندجمله‌ای احتمالاتی را فریب می‌دهد. حالتهای گوناگون دیگری نیز مورد توجه‌اند، و به اختصار بعضی از آنها را مورد بحث قرار می‌دهیم. برای تفصیل بیشتر، رک. [۵].

مفاهیم ضعیفتر تمایزناپذیری محاسباتی

هر گاه منظور ما این باشد که به جای دنباله‌های تصادفی، که به‌وسیلهٔ الگوریتمی به‌کارگرفته شده‌اند، دنباله‌های شبه‌تصادفی را قرار دهیم، می‌توان

1. private-key 2. exclusive or

تلاش کرد که از اطلاعات مربوط به الگوریتم هدف سود برده شود. در بالا صرفاً از این حقیقت استفاده کرده‌ایم که الگوریتم هدف در زمان چندجمله‌ای اجرا می‌شود. ولی اگر مثلاً بدانیم که الگوریتم از فضای کاری بسیار کمی استفاده می‌کند، آنگاه ممکن است قادر باشیم بهتر عمل کنیم. همین‌طور ممکن است بتوانیم بهتر عمل کنیم هر گاه بدانیم که تحلیل الگوریتم تنها به برخی خاصیتهای دنبالهٔ تصادفی که به‌کار می‌برد، و وابسته است (مثلاً، استقلال دوبه‌دوی عناصر آن). در حالت کلی، مفاهیم ضعیفتر تمایزناپذیری محاسباتی نظیر فریب‌دادن الگوریتمهای فضاکراندار، مدارهای ژرفا ثابت، و حتی آزمونهای مشخص (مثلاً، آزمون کردن استقلال دوبه‌دوی دنباله) به‌طور طبیعی پیش می‌آیند. مولدهایی که دنباله‌هایی را تولید می‌کنند که چنان آزمونهایی را فریب می‌دهند، در کاربردهای گوناگونی مفیدند؛ اگر در کاربرد مورد نظر، تصادفی بودن به‌طریقی محدود به کاربرده شود، در این صورت دادن **دنباله‌هایی** با کیفیت تصادفی پایین به خورد آن، ممکن است کافی باشد. نیازی به گفتن نیست که نویسنده از صورتبندی دقیق مشخصه‌هایی با چنان کاربردها و ساخت دقیق مولدهایی هواداری می‌کند که آن نوع از آزمونها را که پیش می‌آیند، فریب دهد.

سایر مفاهیم کارآیی مولدها

پاراگراف پیشین بر یک جنبه از مسألهٔ شبه‌تصادفی بودن تمرکز داشت: منابع یا نوع مشاهده‌گر (یا متمایزکنندهٔ بالقوه). پرسش مهم دیگر این است که آیا چنان دنباله‌های شبه‌تصادفی را می‌توان از دنباله‌های بسیار کوتاهتر تولید کرد و به چه بهایی (یعنی با چه میزان پیچیدگی). در سرتاسر این مقاله شرط کرده‌ایم که فرایند تولید دست‌کم به قدر متمایزکننده، کارآ باشد[۱]. این شرط درواقع، «منصفانه» و طبیعی است. مجاز داشتن مولد به اینکه پیچیده‌تر از متمایزکننده باشد (یعنی، از زمان یا فضای بیشتر استفاده کند)، غیرمنصفانه به نظر می‌رسد اما باز هم پیامدهای جالب توجهی در چارچوب تلاش برای «پادتصادفی‌سازی[۲]» رده‌های پیچیدگی تصادفی دارد. به عنوان مثال، می‌توان مولدهایی را در نظر گرفت که نسبت به طول بذر در زمان نمایی کار می‌کنند. در برخی حالتها، چنین آسانگیریهایی (یعنی مجازداشتن مولدهای زمان‌نمایی) چیزی از دست نمی‌دهیم. برای ملاحظهٔ دلیل آن، یک استدلال نوعی مبتنی بر پادتصادفی‌سازی را در نظر می‌گیریم که مرکب از دو گام است: ابتدا به جای دنباله‌های واقعاً تصادفی الگوریتم، دنباله‌های تصادفی تولید شده از بذرهای بسیار کوتاهتر را قرار می‌دهیم، و سپس به‌طور تعینی به تمام بذرهای ممکن رجوع می‌کنیم و در پی یافتن رفتار با بیشترین فراوانیِ الگوریتم اصلاح‌شده برمی‌آییم. در چنین حالتی، پیچیدگی تعینی در هر حال نسبت به طول بذر، نمایی است. نفع این کار آن است که ساختن مولدهای زمان‌نمایی ممکن است آسانتر از ساختن مولدهای زمان‌چندجمله‌ای باشد.

۱. درواقع شرط کرده‌ایم که مولد کارآتر از متمایزکننده باشد: یعنی شرط کرده‌ایم که مولد یک الگوریتم زمان‌چندجمله‌ای ثابت باشد، در حالی که متمایزکننده مجاز است که هر الگوریتمی با زمان اجرای چندجمله‌ای باشد.

2. derandomization

مراجع

1. W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA/Rabin functions: Certain parts are as hard as the whole, *SIAM J. Comput.* **17** (1988), 194-209.

2. M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo-random bits, *SIAM J. Comput.* **13** (1984), 850-864.

3. T. M. Cover and G. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

4. O. Goldreich, *Foundation of Cryptography-Fragments of a Book*, February 1995, available from
http://theory.lcs.mit.edu/~oded/frag.html.

5. ———, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, Algorithms and Combinatorics, vol. 17, Springer-Verlag, New York, 1998.

6. O. Goldreich, S. Goldwasser, and S. Micali, How to construct random functions, *J. ACM* **33** (1986), 792-807.

7. O. Goldreich and L. A. Levin, Hard-core predicates for any one-way function, *21st ACM Symposium on the Theory of Computing*, 1989, pp. 25-32.

8. S. Goldwasser and S. Micali, Probabilistic encryption, *J. Comput. System Sci.* **28** (1984), 270-299.

9. J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby, A pseudorandom generator from any one-way function, *SIAM J. Comput.* **28** (1999), 1364-1396.

10. D. E. Knuth, *Seminumerical Algorithms*, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, MA, 1969; second edition. 1981.

11. L. A. Levin, Randomness conservation inequalities: Information and independence in mathematical theories, *Inform. and Control* **61** (1984), 15-37.

12. M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, 1993.

13. A. C. Yao, Theory and application of trapdoor functions, *23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 80-91.

******

• Oded Goldreich, "Pseudorandomness", *Notices Amer. Math. Soc.*, (10) **46** (1999) 1209-1216.

* اودت گُلدرایش، مؤسسهٔ علوم وایزمن، اسرائیل

oded@wisdom.weizmann.ac.il