

Dr Ryszard ZIELIŃSKI

## GENERATORY LICZB LOSOWYCH

Już w poprzednich odcinkach poświęconych metodom Monte Carlo spotkaliśmy się z następującym zadaniem: „wylosować punkt z danego przedziału” lub „rzucić na chybił-trafił punkt na kwadrat jednostkowy”. Obecnie zajmiemy się bliżej sposobami realizacji takich poleceń. Mówiąc dokładniej, zajmiemy się nieco ogólniejszym zadaniem, a mianowicie: dana jest pewna zmienna losowa  $X$ ; należy zaprojektować taki eksperyment, aby w wyniku tego eksperymentu otrzymać wartość tej zmiennej losowej. Mówiąc, że „dana jest zmienna losowa  $X$ ” mamy na myśli to, że dany jest jej rozkład prawdopodobieństwa.

Zadanie jest bardzo łatwe, gdy zmienna losowa  $X$  ma następujący rozkład dwupunktowy:  $\{(x_1, 1/2), (x_2, 1/2)\}$ ; przy czym  $x_1 \neq x_2$  (gdy  $x_1 = x_2$ , zmienna losowa stale przyjmuje jedną i tę samą wartość). Odpowiedni eksperyment może przebiegać w następujący sposób. Rzucamy symetryczną monetą. Jeżeli wypadnie orzeł, rejestrujemy wartość  $x_1$ ; jeżeli reszka — wartość  $x_2$ .

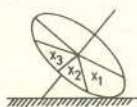
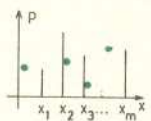
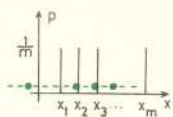
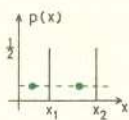
W ten sposób zarejestrowana wartość jest zmienną losową o zadanym rozkładzie. Zadanie nieco komplikuje się, gdy zmienna losowa może przyjmować  $m$  różnych wartości; ma ona wtedy rozkład  $\{(x_j, p_j), j = 1, 2, \dots, m\}$ . W specjalnych przypadkach, gdy  $m$  jest np. jedną z liczb 4, 6, 8, 12 lub 20 i gdy wszystkie  $p_j$  są równe, zamiast monety możemy użyć odpowiedniej kostki — wielościanu foremnego, na którego ścianach wypisano kolejno wartości  $x_1, x_2, \dots, x_m$ .

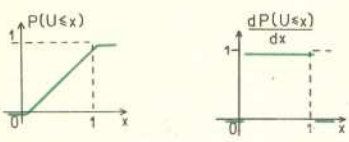
Obserwowane w wyniku rzutów wartości są realizacjami zmiennej losowej o danym rozkładzie. Gdy prawdopodobieństwa  $p_1, p_2, \dots, p_m$  są różne, najwygodniejszym mechanizmem jest tarcza koła, na którym zaznaczono segmenty o kątach proporcjonalnych do prawdopodobieństw  $p_j$  i każdemu segmentowi przyporządkowano odpowiednią liczbę  $x_j$ . Koło takie zamocowuje się na trzpieniu tak, żeby otrzymać zwykłego bąka. Gdy uruchomiony bąk zatrzyma się, punkt styczności krawędzi koła z podłożem wyznaczy wartość  $x_j$ .

Wszystkie takie urządzenia nazywa się zwykle generatorami liczb losowych. „Uniwersalnym” generatorem liczb losowych jest więc wirująca tarcza podzielona na sektory proporcjonalne do prawdopodobieństw, z jakimi powinny pojawiać się poszczególne liczby. Ponieważ zbudowanie odpowiedniej tarczy jest już sprawą czysto techniczną, zadanie „losowania” liczb o różnych rozkładach moglibyśmy uznać za rozwiązane. Ale ...

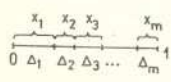
Właśnie! Istnieje jednak pewne „ale”, które nakazuje nam szukać innych rozwiązań. Tym „ale” jest mała praktyczna przydatność takich tarczowych generatorów. Po pierwsze, gdybyśmy mieli losować liczby według różnych rozkładów prawdopodobieństwa, musielibyśmy dla każdego rozkładu budować nową tarczę. Po drugie, wyobraźmy sobie, że mamy wylosować np. 100 000 liczb. Nawet, gdyby wszystkie liczby miały być losowane według tego samego rozkładu (tzn. za pomocą jednej tarczy), czasochłonność manipulacji z wirującą tarczą jest bardzo duża i praktycznie trudno pogodzić się z takim rozwiązaniem. W dodatku naturalne zużywanie się naszego narzędzia i zwykle zmęczenie może doprowadzić do tego, że tarcza nie będzie zatrzymywała się z jednakowym prawdopodobieństwem na każdym punkcie swojego obwodu, a więc realizowany rozkład prawdopodobieństwa będzie odbiegał od rozkładu postulowanego. Po trzecie, większość współczesnych rachunków wykonuje się na maszynach cyfrowych, a nie bardzo wiadomo, jak opisane wyżej urządzenie dopasować do takich maszyn.

Powyzsze zastrzeżenia stały się przyczyną opracowania specjalnych urządzeń, które mogą być wmontowane w maszynę cyfrową. Maszyna wyposażona w taki generator liczb losowych może na żądanie drukować potrzebną ilość takich liczb, otrzymywanych przy różnych rozkładach prawdopodobieństwa, lub wykorzystywać te liczby do zaprogramowanych obliczeń (np. do obliczania całek lub rozwiązywania równań metodami Monte Carlo). Jak zbudowane są takie urządzenia?





Rozkład jednostajny na przedziale (0,1)



$$\{U \in \Delta_j\} = \{X = x_j\}$$

Przed wszystkim pokażemy, że potrafimy generować liczby losowe według dowolnych rozkładów prawdopodobieństwa, jeżeli tylko potrafimy generować liczby według rozkładu jednostajnego na przedziale (0,1). Wyjaśnijmy, że zmienna losowa  $u$  ma rozkład jednostajny na przedziale (0,1), jeżeli dla dowolnych liczb  $a, b (a < b)$  z tego przedziału  $P\{a < u < b\} = b - a$  (patrz artykuł o prawdopodobieństwach geometrycznych, Delta 6/1975). Przypuśćmy, że umiemy generować takie liczby, a chcemy generować liczby losowe według rozkładu

$$(*) \quad \{(x_j, p_j), j = 1, 2, \dots, m\}.$$

Podzielmy odcinek jednostkowy na rozłączne podprzedziały  $\Delta_1, \Delta_2, \dots, \Delta_m$  o długościach odpowiednio równych  $p_1, p_2, \dots, p_m$  (można tak zrobić, gdyż jak wiadomo  $\sum p_j = 1$ ). Wygenerujemy teraz liczbę  $U$  według rozkładu jednostajnego na przedziale (0,1). Będziemy przypisywali zmiennej  $X$  wartości  $x_j$ , jeżeli wygenerowana liczba  $U$  należy do przedziału  $\Delta_j$ . Wtedy oczywiście

$$P\{X = x_j\} = P\{U \in \Delta_j\}$$

a ponieważ przedziały  $\Delta_j$  zostały tak dobrane, żeby prawdopodobieństwo po prawej stronie było równe  $p_j$ , to liczby  $X$  otrzymywane w wyniku naszego postępowania mają dany rozkład (\*). Pozostaje wyjaśnić, jak maszyna cyfrowa generuje liczby  $U$  według rozkładu jednostajnego na przedziale (0,1). Będzie nam tu potrzebna jeszcze jedna uwaga. Otóż każda liczba z przedziału (0,1) może być zapisana binarnie w postaci

$$0, c_1 c_2 c_3 \dots$$

gdzie  $c_1, c_2, c_3, \dots$  są równe zeru lub jedności. Niektóre liczby mają takie dwa zapisy: w jednym, poczynając od pewnego miejsca występują same jedynki, w drugim — same zera (patrz „Mała Delta” 8/1975). Dla jednoznaczności umówmy się, że liczby takie będziemy reprezentowali zapisem kończącym się samymi zerami (np. z dwóch postaci 0,01 (0) i 0,00 (1) liczby 1/4 wybieramy postać pierwszą). Istotną rolę w dalszych rozważaniach odgrywa następujące

**Twierdzenie.** Niech  $(c_i), i = 1, 2, \dots$  będzie nieskończonym ciągiem niezależnych zmiennych losowych takich, że dla każdego  $i$  mamy

$$P\{c_i = 0\} = P\{c_i = 1\} = \frac{1}{2}.$$

Jeżeli  $0, c_1 c_2 c_3 \dots$  jest zapisem binarnym liczby  $U$ , to dla każdych liczb  $a, b (a < b)$  z przedziału (0,1) mamy

$$P\{a < U < b\} = b - a$$

tzn.  $U$  ma rozkład jednostajny na przedziale (0,1).

Z twierdzenia tego wynika, że potrafimy generować liczby losowe według rozkładu jednostajnego na przedziale (0,1) — a więc również według dowolnego rozkładu — jeżeli potrafimy generować ciągi zer i jedynek tak, by zera i jedynki pojawiały się z prawdopodobieństwem 1/2, a wyniki poszczególnych kroków były niezależne. Mamy tu więc do czynienia z dobrze znanym ciągiem prób Bernoulli’ego, w którym każda próba kończy się z prawdopodobieństwem 1/2 sukcesem („jedynka”) lub porażką („zero”). Wynika stąd, że dla generowania liczb o dowolnych rozkładach wystarczy nam symetryczna moneta. Pozostaje jeszcze tylko wyjaśnić, jak taką „monetą” posługuje się maszyna cyfrowa. Otóż maszyny cyfrowe korzystają zwykle z jednego z dwóch następujących rozwiązań.

1. Wiadomo, że w urządzeniach elektronicznych pojawiają się tzw. prądy szumowe. Prądy te mają w czasie przebieg bardzo nieregularny, a ich wartość w każdej chwili zależy od „czystego przypadku”. Typowy przebieg takiego prądu wygląda mniej więcej tak:



Prądy takie można wzmacniać i mierzyć. Można dobrać taką wartość tego prądu, aby prawdopodobieństwo, że wartość ta będzie w danej chwili  $t_i$  przekroczona było równe 1/2. Niezależność tego, co się dzieje w poszczególnych chwilach  $t_1, t_2, t_3, \dots$  można zagwarantować przez wybranie dostatecznie dużego odstępu czasu  $t_i - t_{i-1}$  pomiędzy kolejnymi odczytami („dostatecznie duży” odstęp czasu, to np. odstęp kilku tysięcznych sekundy). Wystarczy teraz wmontować do maszyny odpowiednie źródło szumów i rejestrować w jej pamięci 0, gdy w chwili pomiaru prąd szumowy ma wartość poniżej, lub wartość 1, gdy powyżej odpowiednio ustalonego poziomu. Z takich zer i jedynek maszyna składa liczbę i posyła ją do odpowiedniego rejestru, skąd może być czerpana do obliczeń. Ponieważ urządzenie szumiące pracuje bez przerwy, rejestr taki stale zmienia się i jeżeli z tego rejestru pobierzemy kolejno dwie liczby, to będą to liczby utworzone z różnych odcinków ciągu zer i jedynek.



2. Druga metoda stosowana w maszynach cyfrowych polega na wykorzystaniu źródeł promieniotwórczości. W odpowiednim bloku maszyny umieszcza się substancję promieniotwórczą i licznik wypromieniowanych cząstek. Stan tego licznika ulega zmianom w losowych chwilach czasu i po odpowiednim przeliczeniu może być traktowany jako źródło odpowiednich liczb losowych. Najczęściej wskazania licznika przelicza się odpowiednio na ciąg zer i jedynek (np. zero, gdy w danej chwili stan licznika jest parzysty i jedynka w przypadku przeciwnym), a następnie, zgodnie z podanym wyżej twierdzeniem te zera i jedynki składa się w liczby. Przedstawiony wyżej obraz generatorów liczb losowych w maszynach cyfrowych jest bardzo uproszczony i pozwala tylko na zorientowanie się w ogólnej idei tego typu rozwiązań. Naprawdę sytuacja jest znacznie bardziej skomplikowana. Wystarczy np. chwilę zastanowić się nad tym, jak wybierać poziom odniesienia szumów (który przecież decyduje o tym, czy w danej chwili zarejestrujemy zero, czy jedynkę), aby prawdopodobieństwo zera (lub jedynki) było dokładnie równe  $1/2$ . Albo, jak kontrolować rozpad substancji promieniotwórczej, aby zera i jedynki pojawiały się z jednakowym prawdopodobieństwem. Dla użytkownika maszyny nie są to jednak problemy istotne; wystarczy mu, że po napisaniu w programie odpowiedniej formuły otrzyma liczbę losową wygenerowaną według założonego rozkładu prawdopodobieństwa. Twierdzenie leżące u podstaw opisanych metod generowania liczb losowych w maszynach cyfrowych było już właściwie — chociaż w nieco innej wersji — przez nas wykorzystywane, gdy za pomocą kostki rzucaliśmy punkty na prostokąt obliczając pewną całkę (por. Delta 1/1976). Tam jednak poszczególne cyfry  $c_j$  pochodziły z dziesiętkowego systemu liczenia, a mechanizm losowy (dwudziestościan lub dziesięciograniasty bączek) gwarantowały nam pojawianie się każdej z dziesięciu cyfr z jednakowym prawdopodobieństwem. Sformułowanie tego twierdzenia dla przypadku  $k$ -arnego systemu zapisywania liczb i urządzenia, „produkującego” cyfry  $0, 1, \dots, k-1$ , każdą z prawdopodobieństwem  $\frac{1}{k}$ , pozostawiamy Czytelnikowi.



## Zadania

Redaguje mgr Andrzej MAKOWSKI

**M 79.** Udowodnić, że jeżeli  $n$  jest liczbą naturalną większą od 3 i różną od 5, to dowolny trójkąt można podzielić na  $n$  trójkątów podobnych do niego.

Rozwiązanie na str. 12

W. Mnich

**M 80.** Czy istnieje liczba naturalna  $n$ , którą można przedstawić w postaci  $n = x! + y!$  ( $x < y$ ) dwoma sposobami?

Rozwiązanie na str. 2

**M 81.** Udowodnić, że równania

$$\begin{aligned} ax^2 + bx + c &= 0 \\ cx^2 + bx + a &= 0 \end{aligned}$$

gdzie  $a \neq c$ , mają wspólny pierwiastek wtedy i tylko wtedy, gdy  $|a+c| = |b|$ .  
Rozwiązanie na str. 3.

Redaguje dr Andrzej ZIEMIŃSKI

**F 27.** W artykule zamieszczonym na stronie 4 niniejszego numeru «Deltę» został omówiony tzw. efekt Dopplera. Zainteresowanym proponujemy obecnie rozwiązanie dwóch przykładów praktycznego wykorzystania tego zjawiska.

**Przykład 1.**

Na rakiemie umieszczono nadajnik radiowy emitujący regularne sygnały o częstotliwości 10 MHz. Następnie rakieta została wysłana w górne, zjonizowane warstwy atmosfery, gdzie współczynnik załamania dla fal radiowych jest różny od jedności. Stacja naziemna odbierała sygnały od rakiety nakładając je na inne, wzorcowe oscylacje, również o częstotliwości 10 MHz. Kiedy szybkość oddalania się rakiety wzdłuż kierunku obserwacji wynosiła  $600 \frac{\text{m}}{\text{s}}$ , w aparaturze odbiorczej zaobserwowano występowanie wzmocnień z częstotnością 10 Hz.

Jaki jest współczynnik załamania środowiska, w którym poruszała się rakieta? Rozwiązanie na str. 2

**Przykład 2.** (zaczepnięty ze zbioru zadań A. B. Pipparda).

Sztuczny satelita Ziemi, emitujący sygnały radiowe o stałej częstotliwości, przelatuje nad punktem obserwacyjnym, gdzie notuje się co  $T = 20$  s częstotliwości odbieranych sygnałów. Zanotowano następujące wartości: 40,00215 MHz, 40,00208 MHz, 40,00196 MHz, 40,00175 MHz, 40,00141 MHz, 40,00106 MHz, 40,00077 MHz, 40,00059 MHz, 40,00049 MHz, 40,00043 MHz. Czy powyższe obserwacje mogą posłużyć do wyznaczenia prędkości satelity oraz jego najmniejszej odległości od punktu obserwacyjnego? Trajektorię satelity można przyjąć za linię prostą. Rozwiązanie na str. 14.



W rozwiązaniu zadania M 52 (Delta 6/1975, str. 7) napisaliśmy, że nie wiadomo nam, czy przestrzeń trójwymiarowa pozbawiona jednego punktu jest sumą prostych rozłącznych.

Profesor Jan Mycielski z University of Colorado w Boulder (USA) podał w liście z dnia 20 października ub. r. dowód twierdzenia orzekającego, że odpowiedź na to pytanie jest twierdząca. W dowodzie tym korzysta on z pewnika wyboru (dokładniej: z twierdzenia o dobrym uporządkowaniu).