Losowanie liczby naturalnej

Michał ADAMASZEK

Rozpatrzmy takie, całkiem naturalne i często pojawiające się pytanie: dla ustalonego k jakie jest prawdopodobieństwo tego, że losowo wybrana liczba naturalna dzieli się przez k? Zanim radośnie stwierdzimy, że odpowiedzią jest $\frac{1}{k}$ (to przecież jasne, co k-ta liczba ma tę własność...), przyjrzyjmy się sprawie dokładniej.

Zbiorem wszystkich zdarzeń elementarnych Ω w naszym zadaniu jest zbiór $\mathbb{N}$ (na potrzeby tego tekstu niech $\mathbb{N} = \{1, 2, \ldots\}$). W schemacie klasycznym każdemu zdarzeniu losowemu $A \subset \Omega$ przypisujemy prawdopodobieństwo

$$\frac{\#A}{\#\Omega},$$

gdzie przez $\#X$ oznaczamy liczbę elementów zbioru X.

Michał Adamaszek, student, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Tym razem jest to oczywiście niemożliwe! Musimy zastanowić się nad tym, jakie zbiory zdarzeń chcemy brać pod uwagę, i jak określić ich prawdopodobieństwo – a można to zrobić na wiele sposobów. Przyjmijmy na przykład

$$P(A) = \sum_{n \in A} \frac{1}{2^n}$$

dla $A \subset \mathbb{N}$. Jest to poprawna definicja, tymczasem

$$P(\{2, 4, 6, 8, 10, \ldots\}) = \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \ldots = \frac{1}{3}.$$

Dla innych definicji P wyniki mogą być inne. Jest to sytuacja typowa dla rozważań o losowości – od tego, jaką miarę prawdopodobieństwa wybierzemy, zależy, jakie wyniki otrzymamy. Musimy więc zacząć od znalezienia, wśród wielu możliwych definicji prawdopodobieństwa w naszej przestrzeni, takiego, które wydaje się najodpowiedniejsze dla rozważanego problemu.

Oto nasze minimalne wymagania: prawdopodobieństwo P powinno być określone dla każdego zbioru postaci

$$k\,\mathbb{N} = \{kn : n \in \mathbb{N}\},$$

opisującego własność bycia podzielnym przez k. Co więcej, aby uczynić zadość naszym początkowym intuicjom, chcemy, aby $P(k\,\mathbb{N}) = \frac{1}{k}$. Pozostałe warunki wynikają wprost z przeliczalnej addytywności prawdopodobieństwa. Skoro zbiory $k\,\mathbb{N}$ mają mieć określone prawdopodobieństwo (powiemy, że są *mierzalne*), to mierzalne muszą też być wszystkie zbiory powstałe z nich przez przeliczalne sumy i branie dopełnienia do $\mathbb{N}$ (czyli zbiory tworzące tzw. *σ-ciało* generowane przez zbiory $k\,\mathbb{N}$).

Jesteśmy gotowi, aby porządnie sformalizować nasz problem.

Pytanie. Czy istnieje funkcja P (prawdopodobieństwo) określona na σ-ciele $\mathcal{F}$ generowanym przez zbiory postaci $k\,\mathbb{N}$, o wartościach w $[0, 1]$, taka że

dla $A_1, A_2, \ldots \in \mathcal{F}$ parami rozłącznych

$$P\Big(\bigcup_{n=1}^{\infty} A_n\Big) = \sum_{n=1}^{\infty} P(A_n), \tag{1}$$

$$P(\mathbb{N}) = 1 \text{ i } P(\emptyset) = 0, \tag{2}$$

$$P(k\,\mathbb{N}) = \frac{1}{k} \text{ dla każdego } k \in \mathbb{N}. \tag{3}$$

Odpowiedź. Nie. Zainteresowanych dowodem odsyłam do podręczników rachunku prawdopodobieństwa, pod hasło „lemat Borela–Cantellego".

Skoro odpowiedź jest negatywna, to najwyraźniej nasze wymagania są zbyt wygórowane. Możemy więc zapytać o słabsze wersje problemu. Na przykład osłabienie warunku (3) daje następujące

Zadanie. Znaleźć prawdopodobieństwo określone na $2^{\mathbb{N}}$ (czyli dla wszystkich podzbiorów zbioru liczb naturalnych), które spełnia warunek (3) dla k będących liczbami pierwszymi.

My jednak skierujemy się w inną stronę. Będziemy walczyć o ostatnią własność, rezygnując w zamian z przeliczalnej addytywności. Innymi słowy, pytamy o istnienie prawdopodobieństwa takiego, jakie rozważa się w „szkolnym" rachunku prawdopodobieństwa, to znaczy skończenie addytywnego. Zmieniamy więc definicję $\mathcal{F}$ – teraz będzie to *ciało* zbiorów, czyli rodzina zamknięta na branie *skończonych* sum i dopełnienia do $\mathbb{N}$ generowana przez zbiory postaci $k\,\mathbb{N}$ – i zastępujemy warunek (1) żądaniem, aby

$$P(A \cup B) = P(A) + P(B) \tag{4}$$

dla rozłącznych $A, B \in \mathcal{F}$.

Zanim zaczniemy zgłębiać strukturę ciała $\mathcal{F}$ i w gąszczu należących do niego zbiorów sprawdzać, czy szukana funkcja daje się określić bez żadnych konfliktów (co jest nietrudne i wykonalne, ale trochę pracochłonne), spróbujmy spojrzeć na całe zagadnienie z szerszej perspektywy. Dlaczego w zasadzie nasze intuicyjne wyobrażenia podpowiadają, że prawdopodobieństwo podzielności przez k powinno być równe $\frac{1}{k}$? Zapewne dlatego, że skłonni jesteśmy mierzyć prawdopodobieństwo zbioru $A \subset \mathbb{N}$ jego *gęstością*, która jest zdefiniowana tak:

$$d(A) = \lim_{n \to \infty} \frac{\#(A \cap \{1, 2, \ldots, n\})}{n}$$

(o ile ta granica istnieje). Faktycznie $d(k\,\mathbb{N}) = \frac{1}{k}$.

To podejście wydaje się dobre, bo gęstość wyraża naszą intuicję: patrzymy, jaką część początkowego odcinka liczb naturalnych wypełnia badany zbiór, i przechodzimy do granicy z długością tego odcinka.

Zauważamy szybko, że gęstość zachowuje się jak prawdopodobieństwo także pod innymi względami: $d(\emptyset)=0$, $d(\mathbb{N})=1$, $0\leqslant d(A)\leqslant 1$. Ponadto, jeśli $A\cap B=\emptyset$ i zbiory A,B mają gęstość (odpowiednie granice istnieją), to także zbiór $C=A\cup B$ ma gęstość, i $d(C)=d(A)+d(B)$. Ta równość zachodzi, bo

$$\#((A\cup B)\cap\{1,2,\ldots,n\})=$$
$$=\#(A\cap\{1,2,\ldots,n\})+\#(B\cap\{1,2,\ldots,n\})$$

dla $A\cap B=\emptyset$. Teraz wystarczy podzielić przez n i skorzystać z rozdzielności granicy względem dodawania.

Czyżby więc o to chodziło? Nie, jest bowiem pewien problem, który był już delikatnie zasugerowany: ze względu na operację brania granicy nie dla wszystkich zbiorów gęstość jest dobrze określona. Przykładem zbioru, dla którego definicja gęstości nie działa, jest zbiór:

$$\bigcup_{n=1}^{\infty}\{2^{2n},2^{2n}+1,\ldots,2^{2n+1}-1\}.$$

Dla tego zbioru ciąg z definicji gęstości ma granice dolną i górną równe odpowiednio $\frac{1}{3}$ i $\frac{2}{3}$, więc nie jest zbieżny. Nie jest to zatem dobra miara każdego zbioru.

Co więcej, nawet jeśli ograniczymy się do zbiorów, które mają dobrze określoną gęstość, to ich rodzina nie jest zamknięta ze względu na sumę zbiorów.

Zadanie. Podać dwa zbiory mające gęstość, których suma nie ma gęstości (w świetle jednej z ostatnich uwag takie zbiory nie mogą być rozłączne).

Wyklucza to sensowne określenie prawdopodobieństwa jako gęstości na tych zbiorach, dla których jest ona określona, bo nie tworzą one ciała zbiorów.

Cóż, próby uogólnienia wydają się prowadzić donikąd. Może uda się chociaż sprawdzić, jak gęstość zachowuje się w naszym pierwotnym problemie i czy przynajmniej na ciele zbiorów generowanym przez zbiory postaci $k\,\mathbb{N}$ jest ona dobrą funkcją skończenie addytywną. Chyba że coś jeszcze wymyślimy...

Ostateczne rozwiązanie nadchodzi z zupełnie innej strony. Jedyne, co jest potrzebne, to... jeszcze większe uogólnienie! Paradoks? Skorzystamy z pewnego pięknego i zaskakującego twierdzenia, które w pierwszej chwili wydaje się całkowicie nieprawdopodobne.

Twierdzenie (granica Banacha). Każdemu ciągowi ograniczonemu $(a_n)_{n\in\mathbb{N}}$ można przypisać liczbę rzeczywistą, którą oznaczymy (nie bez powodu) $Lim(a_n)$ w taki sposób, że:

$$Lim(\alpha a_n+\beta b_n)=\alpha Lim(a_n)+\beta Lim(b_n),$$
$$\liminf_{n\to\infty}a_n\leqslant Lim(a_n)\leqslant\limsup_{n\to\infty}a_n,$$
$$Lim(a_n)=Lim(a_{n+1}).$$

W szczególności z drugiego warunku wynika, że jeśli ciąg jest zbieżny, to $Lim(a_n)=\lim_{n\to\infty}a_n$. Pierwszy warunek oznacza, że Lim jest (jak zwykła granica) rozdzielne z dodawaniem ciągów i mnożeniem ich przez liczbę. Zatem (uwaga!) Lim jest rozszerzeniem pojęcia granicy na wszystkie ciągi ograniczone (niekoniecznie zbieżne) i to w sensowny sposób – uogólniona granica mieści się tam, gdzie się jej spodziewamy: pomiędzy granicą dolną i górną ciągu. Na dodatek granica uogólniona nie zmienia się przy przesuwaniu ciągu (warunek ostatni).

Pytanie kontrolne. Względem jakiego działania na ciągach nie została zachowana rozdzielność granicy?

Dowód twierdzenia o granicy Banacha wymaga metod analizy funkcjonalnej – korzysta się z twierdzenia o przedłużaniu funkcjonału, które z kolei opiera się na lemacie Kuratowskiego–Zorna, co niejako „gwarantuje” niekonstruktywność całego dowodu.

Zadanie. Mimo owej niekonstruktywności granice uogólnione pewnych ciągów dają się obliczyć. Ile jest równe $Lim(1,-1,1,-1,1,-1,\ldots)$?

Choć ciągle w szoku nad niezwykłością tego faktu, możemy już łatwo zastosować go do naszego zadania. Zdefiniujemy mianowicie uogólnioną gęstość wzorem

$$\varrho(A)=Lim\frac{\#(A\cap\{1,2,\ldots,n\})}{n}.$$

Jest ona określona tym razem już dla wszystkich podzbiorów $\mathbb{N}$ i zachowuje wszystkie wcześniejsze własności gęstości. Z własności Lim wynika, że $\varrho(A)=d(A)$ dla zbiorów mających gęstość d i $0\leqslant\varrho(A)\leqslant 1$ dla dowolnego $A\subset\mathbb{N}$ (to z drugiej własności Lim). Addytywności ϱ dla zbiorów rozłącznych dowodzi się identycznie jak dla d, bo Lim jest addytywne.

Uzyskaliśmy zatem dużo więcej niż trzeba! Sformułujmy ten wynik w postaci twierdzenia

Twierdzenie. Istnieje skończenie addytywne prawdopodobieństwo P, określone na *wszystkich* podzbiorach $\mathbb{N}$ (czyli funkcja spełniająca warunki $P(A\cup B)=P(A)+P(B)$ dla dowolnych $A,B\subset\mathbb{N}$ rozłącznych, $0=P(\emptyset)\leqslant P(A)\leqslant P(\mathbb{N})=1$) które jest rozszerzeniem gęstości, tzn. $P(A)=d(A)$ dla zbiorów A mających gęstość. Jest ono określone wzorem $P(A)=\varrho(A)$.

Jak widać, całe zagadnienie okazało się, dzięki odpowiedniemu uogólnieniu, dużo prostsze. Można teraz zdradzić, że wcześniej postulowana konstrukcja dla szczególnego przypadku – zdefiniowanie miary tylko na mniejszym ciele zbiorów (generowanym przez zbiory postaci $k\,\mathbb{N}$, a nawet $k\,\mathbb{N}+r$) jako ich gęstości – udaje się, choć po cięższej pracy. Całe to zagadnienie to kolejny przykład na to, jak odpowiednie uogólnienie czy też spojrzenie na problem w świetle innych dziedzin matematyki niż te, w których języku został sformułowany, może przyspieszyć jego rozwiązanie.