

УДК 519.688

MSC 65K10, 65M06

NOVEL FREQUENTIST DEFINITION OF RANDOMNESS

DMITRY KLYUSHIN

Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine, E-mail: klyushin@unicyb.kiev.ua

НОВЕ ЧАСТОТНЕ ВИЗНАЧЕННЯ ВИПАДКОВОСТІ

Д. А. КЛЮШИН

Факультет комп'ютерних наук та кібернетики, Київський національний університет
імені Тараса Шевченка, Київ, Україна, E-mail: klyushin@unicyb.kiev.ua

ABSTRACT. The paper deals with a novel definition of random events that generalizes the well-known definition by von Mises and eliminates its deficiencies. It is shown that the admissible place selection rule introduced by von Mises may be eliminated from consideration using characteristic matrix of a random experiment. In the new model of random events, the field of events forms an atomic generated, complete, and completely distributive Boolean algebra. The probability distribution generated by random variables in this model is not a measure but only a finitely additive function of events in the case of continuous rational or real random variables. The results of computational experiments with quantum random numbers generators are given.

KEYWORDS: Randomness, Frequency, von Mises Model, Lattice, Boolean Algebra.

РЕЗЮМЕ. У статті розглядається нове визначення випадкових подій, яке узагальнює відоме визначення фон Мізеса і усуває його недоліки. Показано, що правило вибору, запропоноване фон Мізесом, може бути виключено з розгляду за допомогою характеристичної матриці випадкового експерименту. У новій моделі випадкових подій поле подій являє собою атомно породжену повну цілком аддитивну булеву алгебру, а розподіл ймовірностей, породжуваний неперервними раціональними або дійсними випадковими величинами, не є мірою, а лише є скінченно-аддитивною функцією подій. Наводяться результати обчислювальних експериментів з квантовими генераторами випадкових чисел.

КЛЮЧОВІ СЛОВА: випадковість, частота, модель фон Мізеса, гра-тка, булева алгебра.

ВСТУП

Поняття випадковості і ймовірності випадкових подій протягом всього життя належали до одних з основних об'єктів дослідження Ю. І. Петуніна. Великий досвід роботи з реальними випадковими даними та вивчення великої кількості теоретичних робіт, присвячених цій темі (див. наприклад [1]), переконали його, що ця тема вимагає нового, нетрадиційного підходу.

Історично першою спробою розв'язати цю проблему слід вважати роботу фон Мізеса [2], в якій було розроблено формальну теорію ймовірностей із урахуванням фізичної реальності. В основу своєї моделі фон Мізес поклав концепцію колективу — випадкової бінарної послідовності, яка має дві властивості:

- 1) існує границя послідовності її відносних частот;
- 2) відносні частоти є інваріантними щодо процедури так званого припустимого вибору, тобто вибору підпослідовності, в якій вибір n -го елемента не залежить від його значення.

Означення 1. (Р. фон Мізес). Нескінченна бінарна послідовність x_1, x_2, \dots є колективом, якщо виконуються дві умови.

1. *Глобальна регулярність.* Нехай h_n — відносна частота одиниць серед перших n членів послідовності. Тоді існує границя $\lim_{n \rightarrow \infty} h_n = p$, $0 < p < 1$.

2. *Локальна регулярність.* Кожна нескінченна підпослідовність x_{i_1}, x_{i_2}, \dots , отримана із послідовності x_1, x_2, \dots за допомогою припустимого вибору, має ту же саму границю p .

У статті [3] А. М. Колмогоров сформулював два основні недоліки теорії фон Мізеса:

1. Частотний підхід, який апелює до поняття граничної частоти, не може мати практичного застосування, оскільки в реальних застосуваннях дослідники мають справу із скінченними послідовностями.
2. Частотний підхід при великій кількості випробувань не можна розвинути суто математично.

Як альтернативу частотній моделі фон Мізеса А. М. Колмогоров запропонував теорію складності. Ця теорія набула широкої популярності і де факто стала домінуючим підходом до визначення випадковості. Втім, частотний підхід ще не вичерпав усіх можливостей. Зокрема, у роботі [4] Ю. І. Петуніним та автором було розвинено альтернативну частотну модель, яка знімає проблему формалізації правила припустимого вибору як таку.

Розглянемо випробування T , який має два наслідки: A та \bar{A} . Введемо індикатор події A у k -му випробуванні

$$x_k = \begin{cases} 1, & \text{якщо } A; \\ 0, & \text{якщо } \bar{A}. \end{cases}$$

Числову послідовність x_1, x_2, \dots , яка складається з нулів і одиниць, будемо називати бернулівською послідовністю порядку p , $0 \leq p \leq 1$, якщо

$$\lim_{n \rightarrow \infty} h_n(T, A) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n x_k = p,$$

де $h_n(T, A)$ — частота події A при n повтореннях випробування T . Основною особливістю запропонованої теорії є той факт, що для математичного визначення випадкового випробування недостатньо знати результати лише однієї серії випробувань $X = \{x_1, x_2, \dots\}$. Для цього необхідно знати послідовність результатів серій випробування X_1, X_2, \dots , які зручно розташувати у вигляді нескінченної матриці

$$\Theta(T) = \begin{pmatrix} x_{11} & \dots & x_{1n} & \dots \\ x_{21} & \dots & x_{2n} & \dots \\ \dots & \dots & \dots & \dots \\ x_{n1} & \dots & x_{nn} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix},$$

яку ми називатимемо характеристичною матрицею випробування T .

Нехай $X_i = (x_{i1}, x_{i2}, \dots, x_{in}, \dots)$ — це рядки, а $X_j^* = (x_{1j}, x_{2j}, \dots, x_{nj}, \dots)$ — стовпчики характеристичної матриці $\Theta(T)$. Легко бачити, що кожний рядок X_n і кожний стовпчик X_n^* матриці $\Theta(T)$ породжують деякі дійсні числа α_n і α_n^* з відрізка $[0, 1]$. Покладемо $\alpha_n = 0, x_{n1}x_{n2}\dots x_{nn}\dots$ і $\alpha_n^* = 0, x_{1n}x_{2n}\dots x_{nn}\dots$ і будемо розглядати ці вирази як бінарні дроби. Позначимо через M та M^* множини чисел α_n і α_n^* , відповідно.

Означення 2. Випробування T називається випадковим, якщо виконуються такі умови:

- 1) всі рядки X_n і стовпці X_n^* ($n = 1, 2, \dots$) характеристичної матриці $\Theta(T)$ є бернулівськими послідовностями одного і того ж порядку $p \in [0, 1]$;
- 2) множини чисел M та M^* , породжені рядками та стовпцями характеристичної матриці $\Theta(T)$, відповідно, є щільними на відрізку $[0, 1]$.

Означення 3. Випадковим експериментом E будемо називати нескінченну серію повторень випадкового випробування T .

Означення 4. Випадковою подією (E, R) будемо називати результат R випадкового випробування T , яке породжує випадковий експеримент E .

Означення 5. Ймовірністю $p(E, A)$ випадкової події (E, A) будемо називати порядок $p \in [0, 1]$ бернулівської послідовності, яка складається із результатів випадкового випробування T , яке породжує випадковий експеримент E .

Оскільки практичний аналіз випадковості здійснюється на скінченних матрицях, необхідно запропонувати означення випадковості для скінченного випадку.

Означення 6. Випробування T вважається випадковим, якщо всі рядки X_i і стовпці X_i^* ($i = 1, 2, \dots, n$) усіченої характеристичної матриці $\Theta_n(T)$ є відрізками бернулівських послідовностей одного і того ж порядку $p \in [0, 1]$ і якщо для довільного $\varepsilon > 0$ існує таке число n , що множини чисел M_n і M_n^* , породжені рядками і стовпцями усіченої характеристичної матриці

$$\Theta_n(T) = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{pmatrix},$$

утворюють ε -сітку на відрізьку $[0, 1]$.

Означення 7. Будемо називати експеримент псевдовипадковим, якщо принаймні одна з множин M та M^* , породжених рядками і стовпчиками відповідної характеристичної матриці, містить лише скінченну кількість різних елементів.

Зокрема, у роботі [4] доведено, що ймовірність того, що в схемі Бернуллі множини M і M^* , утворені рядками і стовпцями характеристичної матриці $\Theta(T)$, є щільними у відрізьку $[0, 1]$, дорівнює одиниці, отже, класична схема Бернуллі є випадковим експериментом у розумінні запропонованої теорії випадкових експериментів.

Нагадаємо основні положення запропонованої моделі [4]. Нехай T — випадкове випробування, а $S(T)$ — множина усіх випадкових подій, що можуть відбуватися внаслідок реалізації випробування T . Спираючись на традиційні означення класичної теорії ймовірностей, у множині $S(T)$ можна визначити операції складання та множення подій, а також операцію заперечення події, причому перші операції можна виконувати для довільної множини подій. Крім того, у множині $S(T)$ для кожної події A визначено її ймовірність $p(A)$, так що $S(T)$ перетворюється на поле, яке ми називатимемо полем подій $S(E)$. У полі подій $S(E)$, яке породжується випадковим експериментом E , можна ввести відношення напівупорядкованості: будемо говорити, що подія A тягне за собою подію B і позначати це символом $A \leq B$, якщо поява події A у результаті випадкового експерименту E неодмінно тягне за собою появу події B . Це відношення перетворює поле подій $S(E)$ у напівупорядковану множину [6]. Легко бачити, що для будь-яких двох подій $A, B \in S(E)$ мають місце співвідношення: $A + B = \sup(A, B) = A \vee B$ і $AB = \inf(A, B) = A \wedge B$, так що операції складання і множення можна здійснити на підставі відношення напівупорядкованості. Ці формули можна узагальнити для довільної множини подій

$$\sum_{i \in J} A_i = \sup_{i \in J} \{A_i\}$$

і

$$\prod_{i \in J} A_i = \inf_{i \in J} \{A_i\}.$$

Оскільки суми і добутки подій завжди існують і належать $S(E)$, то поле подій $S(E)$ є повною дистрибутивною ґраткою [5]. Згідно з означенням

під доповненням елемента A в ґратці з нулем розуміють такий елемент $A' \in S$, що $A \wedge A' = 0$ і $A \vee A' = I$, а ґратка $S(E)$ називається ґраткою з доповненням, якщо всі її елементи мають доповнення. Всі ці властивості виконуються для поля подій, де у ролі елемента O виступає неможлива подія, у ролі I — вірогідна, а доповнення — це заперечення події \bar{A} . Отже, поле подій $S(E)$ — булева алгебра з доповненням.

Теорема 1. [4] *Для довільного випадкового експерименту E поле подій $S(E)$ є цілком дистрибутивною повною булевою алгеброю.*

Теорема 2. [5] (Тарський). *Якщо повна булева алгебра S цілком дистрибутивна, то вона є ізоморфною алгебрі $2^{\mathbb{N}}$ всіх підмножин деякої множини M за структурами напівупорядкованих просторів (або булевих алгебр).*

За множину M можна взяти набір усіх атомів напівупорядкованого простору $S(E)$.

Означення 8. Називатимемо множину подій $B = \{B_i\}_{i \in J}$ із поля подій $S(E)$ базовою, якщо виконуються такі умови:

- 1) всі події B_i із B попарно несумісні, тобто $B_i B_j = 0$, якщо $i \neq j$;
- 2) довільну подію A із $S(E)$ можна подати у вигляді суми подій B_i із B : $A = \sum_{k \in K} B_{i_k}$.

Множина P усіх атомів із $S(E)$ є базовою множиною в $S(E)$. У зв'язку з цим алгебра подій $S(E)$ є атомарно породженою булевою алгеброю. У класичній теорії ймовірностей елементи базової множини в $S(E)$ називаються елементарними подіями. Розподіл ймовірностей $P(E, A)$ у полі подій $S(E)$ є функцією двох аргументів: випадкового експерименту E та випадкової події A .

У застосуваннях теорії ймовірностей зручно інтерпретувати випадкову величину x як деяку функцію, визначену на базовій множині поля подій $S(E)$, оскільки при цьому у деяких випадках кожній елементарній події $B_i \in B(E)$ ставиться у відповідність її числовий показник $x = x(B_i)$. Неважко помітити, що ці два означення є еквівалентними.

Перейдемо тепер до вивчення розподілу ймовірностей на полі подій, породжених значеннями випадкової величини. Розглянемо спочатку випадкові величини, що набувають значень із множини раціональних чисел Q , які, власне, і є результатами вимірювань в реальних застосуваннях.

Означення 9. Будемо називати випадкову величину x раціональною, якщо її можливі значення є раціональними числами. Позначимо через $B_E(x)$ множину всіх можливих значень раціональної випадкової величини x , значення якої спостерігаються при здійсненні випадкового експерименту E . Не обмежуючи загальності, можна вважати, що $B_E(x) = Q$. Тоді $S(E)$ складається з усіх можливих підмножин множини Q .

Означення 10. Раціональна випадкова величина x називається неперервною, якщо її функція розподілу $F_x(u)$ є неперервною на R^1 . Відповідний розподіл ймовірностей називається неперервним.

Означення 11. Раціональна випадкова величина x називається сингулярною, якщо існує така підмножина $\Psi = \{a_1, a_2, \dots, a_n, \dots\} \subset \mathbb{Q}$, що $p(E, \{a_n\}) = p_n > 0 \forall n \in \mathbb{N}$ і $\sum_{n=1}^{\infty} p_n = 1$. Відповідний розподіл ймовірностей називається сингулярним.

Теорема 3. [4] Нехай $F(u)$ — довільна неперервна функція розподілу на прямій \mathbb{R}^1 , тоді існує випадковий експеримент E з базовою множиною (множиною елементарних наслідків) $B_E = \mathbb{Q}$ і розподілом ймовірностей $p(E, A)$, $A \subset \mathbb{Q}$, для якого при будь-яких $u \in \mathbb{R}^1$ $p(E, \mathbb{Q}_{(-\infty, u]}) = F(u)$, де $\mathbb{Q}_{(-\infty, u]} = \mathbb{Q} \cap (-\infty, u]$.

Теорема 4. [4] Нехай $F(u)$ — довільна функція розподілу, зосереджена на відрізьку $[a, b]$:

$$F(u) = \begin{cases} 0, & u \geq a, \\ 1, & u \leq b. \end{cases}$$

Тоді існує випадковий експеримент E з числовою базовою множиною $B_E = [a, b]$, що породжує розподіл ймовірностей $p(E, A)$ на всіх підмножинах $A \subset [a, b]$, для якого за умови, що $u \in (a, b)$, має місце співвідношення $p(E, (a, u]) = F(u)$.

ОБЧИСЛЮВАЛЬНІ ЕКСПЕРИМЕНТИ

Для перевірки практичної придатності запропонованого означення випадкової події було проведено ряд обчислювальних експериментів. Критерієм успіху цих експериментів вважалися стабілізація відносної частоти та виникнення ϵ -сітки у бінарних послідовностях, які утворюють характеристичну матрицю. Очевидно, що для стандартних генераторів псевдовипадкових чисел умови випадковості можуть спостерігатися лише до кінця періоду, після якого внаслідок повторів починають утворюватися атоми. Природно очікувати, що при використанні квантового генератора це явище спостерігатися не буде. Для експериментів використовувався квантові генератори Австралійського національного університету [6] та Гумбольдтського університету Берліна [7].

Алгоритм

- 1) Згенерувати випадкове натуральне число.
- 2) Якщо число є парним, присвоїти індикатору події 1, інакше 0.
- 3) Повторити кроки 1–2 N разів.
- 4) Повторити кроки 1–3 N разів.
- 5) Обчислити відносну частоту одиниць у кожному рядку і стовпці.
- 6) Обчислити десяткові числа, що утворюють множини M і M^* .
- 7) Упорядкувати за зростанням множини M і M^* .
- 8) Знайти максимальне відхилення між сусідніми числами у множинах M і M^* .
- 9) Знайти середні відстані між відносними частотами у суміжних рядках і стовпцях.

Результати

У табл. 1 і 2 використано наступні позначення: Δ_R — максимальна різниця між упорядкованими десятковими числами, що утворені рядками характеристичної матриці, Δ_C — максимальна різниця між упорядкованими десятковими числами, що утворені стовпцями характеристичної матриці, ΔF_R — максимальна різниця між відносними частотами в рядках, ΔF_C — максимальна різниця між відносними частотами у стовпцях, F_R — відносна частота одиниць у рядках, F_C — відносна частота одиниць у стовпцях.

ТАБЛИЦЯ 1. Результати обчислювальних експериментів з квантовим генератором ANU [6]

| N | Δ_R | Δ_C | ΔF_R | ΔF_C | F_R | F_R |
|-------|------------|------------|--------------|--------------|---------|---------|
| 1024 | 0.00714 | 0.00871 | 0.00488 | 0.00781 | 0.49843 | 0.49843 |
| 2048 | 0.00482 | 0.00401 | 0.00244 | 0.00293 | 0.49983 | 0.49983 |
| 3072 | 0.00241 | 0.00290 | 0.00423 | 0.00228 | 0.49992 | 0.49992 |
| 4096 | 0.00245 | 0.00185 | 0.00195 | 0.00537 | 0.49977 | 0.49977 |
| 5120 | 0.00198 | 0.00170 | 0.00137 | 0.00137 | 0.49994 | 0.49994 |
| 6144 | 0.00145 | 0.00137 | 0.00309 | 0.00244 | 0.49989 | 0.49989 |
| 7168 | 0.00129 | 0.00133 | 0.00614 | 0.00293 | 0.49985 | 0.49985 |
| 8192 | 0.00125 | 0.00106 | 0.00317 | 0.00439 | 0.49992 | 0.49992 |
| 9216 | 0.00103 | 0.00133 | 0.00119 | 0.00342 | 0.49992 | 0.49992 |
| 10240 | 0.00110 | 0.00087 | 0.00566 | 0.00293 | 0.49985 | 0.49990 |

ТАБЛИЦЯ 2. Результати обчислювальних експериментів з квантовим генератором QRNG [7]

| N | Δ_R | Δ_C | ΔF_R | ΔF_C | F_R | F_R |
|------|------------|------------|--------------|--------------|---------|---------|
| 323 | 0.02347 | 0.02081 | 0.00929 | 0.00929 | 0.49682 | 0.49682 |
| 647 | 0.01056 | 0.01060 | 0.00927 | 0.01236 | 0.49934 | 0.49934 |
| 971 | 0.00890 | 0.00809 | 0.00412 | 0.00927 | 0.49970 | 0.49970 |
| 1295 | 0.00591 | 0.00908 | 0.00232 | 0.00541 | 0.49983 | 0.49983 |
| 1619 | 0.00745 | 0.00469 | 0.00432 | 0.00371 | 0.49986 | 0.49986 |
| 1942 | 0.00417 | 0.00350 | 0.00309 | 0.00515 | 0.49968 | 0.49968 |
| 2266 | 0.00590 | 0.00415 | 0.00309 | 0.00265 | 0.49970 | 0.49970 |
| 2590 | 0.00413 | 0.00365 | 0.00541 | 0.01004 | 0.49972 | 0.49972 |
| 2914 | 0.00282 | 0.00276 | 0.00240 | 0.00377 | 0.49974 | 0.49974 |
| 3238 | 0.00238 | 0.00244 | 0.00401 | 0.00185 | 0.49985 | 0.49985 |

Як показують результати обчислень, ϵ -сітка одиничного відрізка для $\epsilon = 0.001$ виникає досить швидко. Для цього у першому експерименті достатньо було трохи більше 10 тисяч випробувань, а в другому — 4000. До того ж спадання максимальної відстані між сусідніми числами у множинах M і M^* має практично монотонний характер. Крім того, в обох експериментах спостерігалось досить швидко спадання коливань відносної частоти, хоча воно мало немонотонний характер. Обидва ці фактори свідчать про випадковість чисел, згенерованих за допомогою квантових генераторів, відповідно до запропонованого у роботі означення.

Автор висловлює подяку бакалавру факультету кібернетики Київського національного університету імені Тараса Шевченка Олексію Морозову за допомогу в проведенні обчислень.

ВИСНОВКИ

Запропонований у роботі [4] частотний підхід, який базується на понятті характеристичної матриці випадкового експерименту, дозволив зняти проблему формалізації правила припустимого вибору колективу за фон Мізесом. У новій моделі колективи породжуються рядками і стовпцями характеристичної матриці. Застосування топологічних властивостей множин чисел, породжених рядками і стовпцями характеристичної матриці, робить запропонований критерій випадковості легко реалізованим у практичних застосуваннях. Показано, що частотний підхід при великій кількості випробувань можна розвинути математично за допомогою математичного апарату теорії ґраток. Обчислювальні експерименти підтверджують практичність частотного підходу.

ЛІТЕРАТУРА

1. Vitanyi P. M. B. Randomness // In A. Schrijver, N. Temme, and K. R. Apt, Eds., *From Universal morphisms to megabytes: a Baayen space Odyssey*, CWI, Amsterdam, 1994. — p. 627–642.
2. von Mises R. Grundlagen der Wahrscheinlichkeitsrechnung // *Math. Zeitschrift*. — 5. — 1919. — P. 52–99.
3. Колмогоров А. Н. О таблицах случайных чисел // *Семиотика и информатика*. — М.: ВИНТИ, 1981. — Вып. 18. — С. 3–13.
4. Петунін Ю. І., Ключин Д. А. Структурний підхід до розв'язання постійної проблеми Гільберта // *Теор. ймовір. і матем. статист.* — 2004. — № 71. — С. 145–159.
5. Бирхгоф Г. Теория решеток. — М.: Наука, 1984. — 568 с.
6. ANU (2016). ANU Quantum Random Numbers Server, Australian National University. Available at: <https://qrng.anu.edu.au>
7. QRNG Service (2016). Nano-Optics groups at the Department of Physics of Humboldt University. Available at: <https://qrng.physik.hu-berlin.de>

Надійшла 07.04.2017