

**Р.А. ЗАТОРСЬКИЙ, П.І. ФЕДУРУК, Н.М. ДЯКІВ**

## **ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ У СИСТЕМІ ДИСТАНЦІЙНОГО КОНТРОЛЮ ЗНАНЬ**

---

**Abstract:** Article is dedicated to the problem of random numbers generator (RNG) that may be used in systems of distance education and knowledge control. Weak points of existing RNG applied for typical tasks in this area have been analyzed and a new type of generators based on described  $f_n$ -function has been offered. Conducted researches convincingly show that offered RNG can be effectively used not only in systems of distance education and knowledge control where its approbation has been carried out but also in other calculating and mathematical systems requiring RNG with the most uniform frequency distribution on given set.

**Key words:** random number generator, system of distance knowledge control.

**Анотація:** У статті розглянуто питання використання генератора випадкових чисел (ГВЧ) у системах дистанційного навчання та контролю знань. Проаналізовано недоліки застосування для даного типу задач існуючих ГВЧ та запропоновано принципово новий тип генератора на основі описаної у статті  $f_n$ -операції. Проведені дослідження показали, що запропонований нами ГВЧ може досить ефективно застосовуватись не тільки в системах дистанційного навчання і контролю знань, де і було проведено його апробацію, але й в інших областях застосування, які потребують ГВЧ з якомога більш рівномірним розподілом частот попадання виборки по всій заданій множині.

**Ключові слова:** генератор випадкових чисел, система дистанційного контролю знань.

**Аннотация:** В статье рассматриваются вопросы использования генератора случайных чисел (ГСЧ) в системе дистанционного образования и контроля знаний. Проанализировано недостатки применения для подобного типа задач существующих ГСЧ и предложено принципиально новый тип генератора на базе описанной в статье  $f_n$ -операции. Проведенные исследования показывают, что предложенный ГСЧ может достаточно эффективно использоваться не только в системах дистанционного образования и контроля знаний, где и была осуществлена его апробация, но и в других областях применения, которые нуждаются в ГСЧ с наиболее равномерным распределением частот попадания выборки по всему заданному множеству.

**Ключевые слова:** генератор случайных чисел, система дистанционного контроля знаний.

### **1. Вступ**

В наш час все ширшого розповсюдження в наш час набувають системи дистанційного навчання та контролю знань. Розвиток інформаційних та телекомунікаційних технологій постійно відкриває нові можливості для застосування в освіті систем, які використовують комп'ютерну техніку та інформаційні мережі. В таких системах на відміну від традиційного навчання використовуються інші засоби і методи передачі та контролю знань. Особливо велике значення має розробка і створення ефективних інструментів, які б забезпечили проведення процедури дистанційного контролю знань з достатньою мірою валідності. Валідність – це сукупність відомостей про те, відносно яких характеристик особистості можуть виноситись кваліфікаційні судження, а також про міру обґрунтованості останніх на підставі тестових оцінок або якихось інших засобів оцінювання [1].

В сучасних навчальних системах для контролю знань найчастіше використовуються тести. З'ясувати валідність тесту означає перевірити, чи дійсно тест вимірює потрібну нам характеристику і наскільки надійно він це робить. Зрозуміло, що метою розробника є максимально досяжна за даних умов валідність. Велике значення в забезпеченні валідності відіграє вибір з бази запитань у випадковому порядку для проведення тестування з рівномірним розподілом такої виборки по всій множині запитань, щоб випадково генеровані тестові комплекти були валідними з точки зору різноманітності й повноти охоплення матеріалу, рівень засвоєння якого потрібно визначити. Тому

використання в системі дистанційного контролю знань генератора випадкових чисел, за допомогою якого б організувалась рівномірно розподілена виборка, є важливою і актуальною задачею.

Якщо взяти до уваги генератори випадкових чисел, які найчастіше використовуються в різних операційних системах як одна з програм з стандартного набору, то в більшості випадків

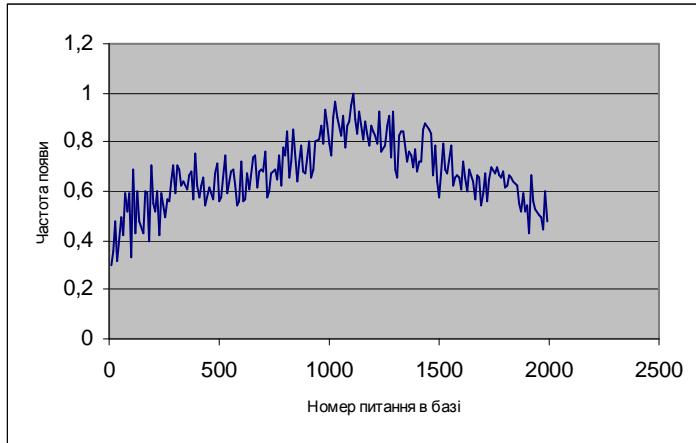


Рис. 1. Частота вибору з бази питань для тестування (від 1 до 2000)

використовується один і той же ж алгоритм. Тому на даний момент цей генератор вважається стандартним при використанні в різних програмах. Зокрема, в попередніх версіях розробленої нами системи дистанційного навчання і контролю знань використовувалась функція `rand` з операційної системи FreeBSD. Розподіл, отриманий за допомогою цієї функції, виглядає таким чином (рис. 1).

Як бачимо, забезпечити рівномірність вибору питань з бази за допомогою цієї функції не вдається. Тому нами пропонується застосувати генератор випадкових чисел на основі  $f_n$ -операції. Для цього опишемо  $f_n$ -операцію і її властивості.

## 2. $f_n$ -операція і її властивості

**Означення 1.** Нехай  $n$  – деяке натуральне  $L$  – цифрове число, а  $\Omega_n$  – множина пар, де  $x$  і  $y$  –

цілі невід’ємні числа, що належать відповідно відрізкам  $\left[0, \underbrace{9\dots9}_L\right]$  і  $[0, n-1]$ .  $f_n$ -операцією

назвемо операцію, яка парі  $(y, x) \in \Omega_n$  ставить у відповідність пару  $(v, u)$ , компоненти якої визначаються рівністю

$$n \cdot x + y = v \cdot 10^L + u, \quad (1)$$

де  $u < 10^L$ . Якщо  $f_n(y, x) = (v, u)$ , то вважатимемо, що

$$f_n \circ f_n(y, x) = f_n^2(y, x) = f_n(v, u).$$

**Зауваження.** Множина  $\Omega$ , очевидно, є множиною цілочисельних точок деякого прямокутника, тому пари  $(y, x)$  ми іноді називатимемо його точками.

**Властивість 1.** (Замкнутість)  $f_n$ -операція переводить множину  $\Omega_n$  в себе, тобто, якщо  $(y, x) \in \Omega_n$   $f_n(y, x) \rightarrow (v, u)$ , то і  $(v, u) \in \Omega_n$ .

*Доведення.* Те, що  $v \geq 0$  і  $u \in \left[0, \underbrace{9 \dots 9}_L\right]$  випливає з визначення  $f_n$ -операції. Доведемо, що  $v \leq n-1$ . Якщо  $x = \underbrace{9 \dots 9}_L$ , то  $n \cdot \underbrace{9 \dots 9}_L + y = (n-1) \cdot 10^L + 10^L - n + y$ , але оскільки  $y \leq n-1$ , то  $10^L - n + y \leq \underbrace{9 \dots 9}_L$ , і максимальне значення  $v$  дорівнює  $n-1$ .

**Означення 2.** Операцію  $f_n^{-1}$  назвемо оберненою до операції  $f_n$ , якщо  $f_n^{-1}(f_n(y, x)) = (y, x)$ .

**Властивість 2.** (Єдиність) Операції  $f_n$  і  $f_n^{-1}$  кожному прообразу ставлять у відповідність єдиний образ.

*Доведення.* Доведемо справедливості цього твердження для  $f_n$ -операції. Припустимо, що виконуються дві рівності

$$n \cdot x + y = v \cdot 10^L + u;$$

$$n \cdot x + y = v_1 \cdot 10^L + u_1.$$

Причому  $v \neq v_1$  або  $u \neq u_1$ . Віднімемо від першої рівності другу, одержимо

$$(v - v_1) \cdot 10^L + (u - u_1) = 0.$$

Звідки, в силу нерівностей  $L \geq 1$ ,  $u \leq n-1$ ,  $u_1 \leq n-1$ , випливає рівність,  $u = u_1$ , що суперечить припущенню.

Доведення цього твердження для операції  $f_n^{-1}$  аналогічне.

**Властивість 3.** (Нерухомі точки) Якщо має місце рівність

$$x \cdot (n-1) = \underbrace{9 \dots 9}_L \cdot y, \quad (2)$$

то  $(y, x)$  – нерухома точка множини  $\Omega_n$ .

*Доведення.* Нехай виконується рівність (2), тоді  $nx + y = y \cdot 10^L + x$ , тобто за визначенням  $f(n)$ -операції маємо  $f(n) : (y, x) \rightarrow (y, x)$ .

**Зауваження 1.** З рівності (2) випливає, що всі нерухомі точки  $f(n)$ -операції знаходяться в цілочисельних точках діагоналі прямокутника  $\Omega_n$ , яка з'єднує точки  $(0,0)$  і  $(n-1, \underbrace{9 \dots 9}_L)$ .

**Приклад 1.** Знайдемо всі нерухомі точки  $f_{34}$ -операції. Точка  $(0,0)$  є нерухомою точкою будь-якої  $f_n$ -операції. Знайдемо всі пари  $(y, x) \in \Omega_{34}$ , що задовольняють рівності (2), тобто рівності  $x = 3 \cdot y$ .

Ними, очевидно, будуть пари  $(i, 3i)$ , де  $i = 0, 1, \dots, 33$ . Отже,  $f_{34}$ -операція має 34 нерухомі точки.

Оскільки множина  $\Omega$  складається з рухомих і нерухомих точок, то в результаті скінченності цієї множини можна стверджувати, що кожній рухомій точці  $(y, x)$  відповідає деяка орбіта

$$O_n(y, x) = \{(y, x) = f_n^0(y, x); f_n^1(y, x); \dots f_n^{k-1}(y, x)\},$$

де  $k$  – якнайменше натуральне число таке, що

$$f_n^k(y, x) = (y, x).$$

Точку  $(y, x)$  назвемо твірною цієї орбіти, а число  $k$  – її довжиною.

**Зауваження 1.** Нерухому точку можна вважати орбітою довжини 1.

**Зауваження 2.** Аналітичного методу знаходження довжини орбіти точки  $(y, x)$ , очевидно, не існує. Тому необхідно обчислювати її або вручну або за допомогою комп'ютера. Так, за допомогою комп'ютера було встановлено, що  $|O_{2000}(0, 2000)| = 9999999$ .

**Визначення 4.** Пари  $(y, x)$  і  $(n-1-y, \underbrace{9\dots 9}_L - x)$  назвемо взаємно спряженими парами. Дві орбіти, що складаються з взаємно спряжених пар, назвемо взаємно спряженими орбітами і позначимо  $O_n$  і  $\overline{O_n}$ .

Очевидно, що точки прямокутника  $\Omega$ , які відповідають взаємно спряженим парам, симетричні відносно точки перетину діагоналей цього прямокутника.

**Властивість 4.** Довжини орбіт взаємно спряжених пар співпадають.

**Доведення.** Нехай  $f_n(y, x) = (v, u)$ , тобто  $n \cdot x + y = v \cdot 10^L + u$ . Доведемо, що

$$f_n(n-1-y, \underbrace{9\dots 9}_L - x) = (n-1-v, \underbrace{9\dots 9}_L - u).$$

Дійсно,

$$\begin{aligned} n \cdot (\underbrace{9\dots 9}_L - x) + n-1-y &= n \cdot 10^L - n \cdot x - y - 1 = n \cdot 10^L - v \cdot 10^L - u - 1 = \\ &= (n-1-v) \cdot 10^L + 10^L - 1 - u. \end{aligned}$$

Таким чином, якщо  $f_n^1(y, x), f_n^2(y, x), \dots, f_n^{T_n}(y, x)$  представляють різні пари, то і  $f_n^1(n-1-y, \underbrace{9\dots 9}_L - x), f_n^2(n-1-y, \underbrace{9\dots 9}_L - x), \dots, f_n^{T_n}(n-1-y, \underbrace{9\dots 9}_L - x)$  теж представляють різні пари, причому, оскільки  $f_n^{T_n}(y, x) = (y, x)$ , то і  $f_n^{T_n}(n-1-y, \underbrace{9\dots 9}_L - x) = (n-1-y, \underbrace{9\dots 9}_L - x)$ .

**Властивість 5.** Взаємно спряжені пари належать різним орбітам.

**Доведення.** Нехай  $(y, x), \overline{(y, x)}$  – дві спряжені пари, що належать одній орбіті  $O_n(y, x)$  довжини  $|O_n(y, x)| = k > 0$ . Тоді існує таке натуральне число  $l < k$ , що виконується рівність  $f_n^l(y, x) = \overline{(y, x)}$ , а одночасно і рівність

$$(y, x) = f_n^{-l}(\overline{(y, x)}). \quad (3)$$

Але оскільки орбіта  $O_n(y, x)$  має довжину  $k$ , то виконується рівність

$$f_n^{k-l}(\overline{(y, x)}) = (y, x). \quad (4)$$

Порівнюючи рівності (3), (4) і враховуючи властивість 2, приходимо до рівності  $k = 0$ , яка суперечить нерівності  $k > 0$ .

**Зауваження.** З властивостей (4) і (5) випливає, що  $f_n$ -операція розбиває кожну множину  $\Omega_n$  на парну кількість орбіт однакової довжини. Причому для кожної орбіти в цій множині існує спряжена орбіта.

**Приклад 2.**  $f_{11}$ -операція розбиває множину  $\Omega = X \times Y$ , де  $X = \{0; 1; \dots; 10\}$ ,  $Y = \{0; 1; \dots; 99\}$  на 28 орбіт, кожна з яких має довжину 39, дві орбіти довжиною 3 і дві нерухомі точки.

### 3. $f_n$ - операція як генератор випадкових чисел

Як вже згадувалось вище, відправляючись від пари  $(0, 2000)$ , при допомозі  $f_{2000}$  - операції можна одержати неперіодичну послідовність чисел, яка складається з 9999999 чотирицифрових чисел. Таким чином,  $f_n$ -операція при порівняно невеликих значеннях  $n$  генерує достатньо великі неперіодичні масиви  $L$ -цифрових чисел. Дослідимо гістограми частот деяких масивів чисел, що генеруються при допомозі  $f_n$ -операції.

Приведемо таблицю частот другої компоненти орбіти  $O_{90}(0, 90)$ , в якій у першому рядку записано другу компоненту, а в другому рядку – її кількість в масиві (табл. 1).

Таблиця 1. Частота повторів другої компоненти

Компонента	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Кількість повторів	56	49	54	44	48	52	44	48	55	39	48	47	50	49	41	45	43	53	42	37

Компонента	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
Кількість повторів	47	46	46	47	44	52	51	45	49	38	38	45	47	43	52	44	43	44	44	45

Компонента	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
Кількість повторів	50	49	52	35	47	44	42	44	41	41	49	49	46	48	46	43	55	38	41	40

Компонента	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
Кількість повторів	45	46	46	47	46	38	47	43	45	52	52	41	45	39	38	46	43	44	44	43

Компонента	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99
Кількість повторів	53	48	37	47	45	49	41	40	43	42	51	35	42	46	38	42	46	36	41	33

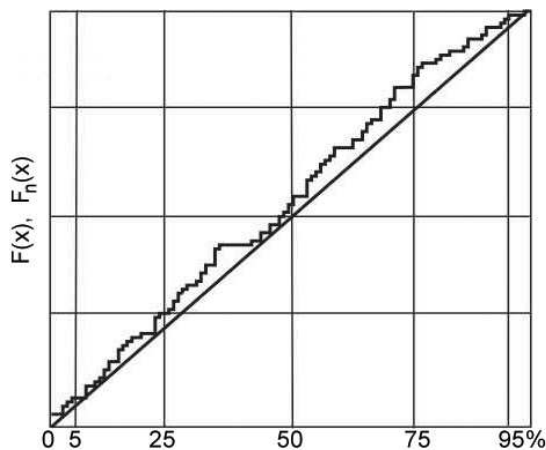
За допомогою ЕОМ знайдено, що довжина орбіти  $O_{90}(0,90)$  рівна 4499. Отже, кожне із ста різних значень в середньому повинне повторюватися 44,99 раз. Як видно з цієї таблиці, частота появи чисел досить стійко коливається біля числа 45.

#### 4. Оцінка генератора випадкових чисел

Для того, щоб все ж таки визначити, чи буде наш генератор генератором випадкових чисел в загальноприйнятому розумінні, проведемо дослідження відповідності його певним відомим критеріям [2]. Розглянемо декілька специфічних критеріїв, які традиційно застосовуються для перевірки, чи буде послідовність випадковою.

**Критерій рівномірності (критерій частот).** Найперша вимога, яка висувається до послідовності випадкових чисел від  $a$  до  $b$ , полягає в тому, щоб її члени були рівномірно розподілені на відрізку  $[a;b]$ . Застосуємо критерій Колмогорова-Смірнова з  $F(x) = x$  для  $a \leq x \leq b$ . Було виконано  $n = 1000$  випадкових досліджень і отримано випадкові значення  $X_1, X_2, \dots, X_n$ ; *емпіричну функцію розподілу*  $F_n(x)$  було побудовано за формулою

$$F_n(x) = \frac{\text{кількість } X_1, X_2, \dots, X_n \text{ таких, що вони } \leq x}{n}.$$



На (рис. 2) зображено графік знайденої емпіричної функції розподілу (зигзагоподібна лінія) та накладений на неї графік функції розподілу  $F(x) = x$ . При зростанні  $n$   $F_n(x)$  більш точно наближає функцію розподілу.

Критерій Колмогорова-Смірнова базується на різниці між  $F(x)$  та  $F_n(x)$ . Очевидно, що велика різниця між ними є неймовірною, і тільки КС-критерій може показати, наскільки саме.

Рис. 2. Приклад емпіричного розподілу

Щоб побудувати КС-критерій, утворимо такі статистики:

$$K_n^+ = \sqrt{n} \max_{-\infty < x < \infty} (F_n(x) - F(x));$$

$$K_n^- = \sqrt{n} \max_{-\infty < x < \infty} (F(x) - F_n(x)).$$

Тут  $K_n^+$  визначає найбільше з відхилень, коли  $F_n(x)$  більша, ніж  $F(x)$ , а  $K_n^- - F_n(x)$  менша, ніж  $F(x)$ . Для розглядуваного прикладу ці статистики набувають значень:  $K_{1000}^+ = 0.8136$

та  $K_{1000}^- = 0.3828$ . Для порівняння було взято аналогічні результати для а) методу Мак-Лорена-Марсалья, б) генератора Фібоначчі, в) для стандартного UNIX-генератора. Отримано такі результати (табл. 2):

Таблиця 2. Порівняння значень характеристик в КС-критерії

Генератор \ Статистика	а)	б)	в)
$K_{1000}^+$	0,577	2,819	0,949
$K_{1000}^-$	0,867	0,258	0,141

Як і для  $\chi^2$ -критерію, отримані значення  $K_n^+$  і  $K_n^-$  можна порівняти з процентною таблицею і визначити, чи є вони суттєво більшими, чи меншими. При цьому відмінність від  $\chi^2$ -критерію полягає в тому, що процентна таблиця містить не просто наближені значення, справедливі при великих значеннях  $n$ , а точні значення (з урахуванням похибки обчислень). Значення деяких процентних точок для розподілу  $K_{1000}^+$ ,  $K_{1000}^-$  (табл. 3):

Таблиця 3. Деякі процентні точки розподілів  $K_n^+$  і  $K_n^-$

Точка \ Степінь свободи	p=1%	p=5%	p=25%	p=50%	p=75%	p=95%	p=99%
$n = 1000$	0,0656	0,1548	0,3740	0,5834	0,8273	1,2186	1,5121

Отримані значення  $K_{1000}^+ = 0,8136$  та  $K_{1000}^- = 0,3828$  знаходяться між 25- та 50-процентною точками, тому розглядувати ці значення як значно більші або значно менші не можна. Таким чином, проведені спостереження є задовільно випадковими по відношенню до розглянутого критерію.

**Метод інтервалів.** Використовується для перевірки довжини "інтервалів" між появою  $U_j$  ( $a \leq U_j \leq b$ ) на деякому відрізку. Якщо  $\alpha$  і  $\beta$  – два цілі числа, то розглядається довжина підпослідовності  $U_j, U_{j+1}, \dots, U_{j+r}$ , в яких  $U_{j+r}$  лежить між  $\alpha$  і  $\beta$ , а інші члени не лежать між цими числами (цю підпослідовність, яка складається з  $r+1$  числа, і називатимемо інтервалом довжиною  $r$ ).

Для дослідження було використано такий алгоритм підрахунку кількості інтервалів довжиною  $(0, 1, \dots, t-1)$  та кількості інтервалів довжиною понад  $t$  (щоб у підсумку було рівно  $n$  інтервалів) для довільних чисел  $\alpha$  і  $\beta$ :

**Крок 1.** [Ініціалізація] Присвоїти  $j \leftarrow -1$ ,  $s \leftarrow 0$  і присвоїти  $\text{COUNT}[r] \leftarrow 0$  для кожного  $0 \leq r \leq t$ .

**Крок 2.** [Присвоєння  $r$  значення 0]. Присвоїти  $r \leftarrow 0$ .

**Крок 3.** Збільшити  $j$  на 1. Якщо  $U_j \geq \alpha$  і  $U_j < \beta$ , то перейти до кроку 5.

**Крок 4.** Збільшити  $r$  на 1 і повернутись до кроку 3.

**Крок 5.** (Щойно знайдено інтервал завдовжки  $r$ ). Якщо  $r \geq t$ , то збільшити COUNT[t] на 1, в іншому випадку – збільшити COUNT[r] на 1.

**Крок 6.** Збільшити  $s$  на 1. Якщо  $s < n$ , то повернутись до кроку 2.

Критерій інтервалів часто використовується для значень для того, щоб на кроці 3 уникнути порівняння. Особливі випадки  $(\alpha, \beta) = (a, \frac{b}{2})$  та  $(\alpha, \beta) = (\frac{b}{2}, b)$  іноді називають „відхиленням вище середнього” та „відхиленням нижче середнього” відповідно. Тестування здійснювалось для випадків  $\alpha = 0, \beta = 50; \alpha = 50, \beta = 100; \alpha = 20, \beta = 80$ . Після реалізації даного алгоритму  $\chi^2$  – критерій застосовувався до значень COUNT[0], COUNT[1], ... , COUNT[t] з такими ймовірностями:

$$p_r = p(1-p)^r \quad \text{для } 0 \leq r \leq t-1; \quad p_t = (1-p)^t.$$

Тут  $p = \beta - \alpha$  – ймовірність того, що  $\alpha \leq U \leq \beta$ . Значення  $n$  і  $t$  вибирались так, щоб очікуване значення COUNT[r] було не меншим 5. В результаті тестування було отримано такі значення  $\chi^2$  – статистики: для відхилення вище середнього  $\chi^2 = 6,462328$ ; для відхилення нижче середнього  $\chi^2 = 9,18699$ ; для випадку  $\alpha = 20, \beta = 80$  значення  $\chi^2 = 12,90351$  при ступені свободи 11. Отримані значення знаходять відповідно між 10- і 25-, 25- і 50- та між 50- і 70- процентними точками, а тому всі результати вважаються задовільно випадковими відносно критерію інтервалів.

**Покер-критерій (критерій розбиттів).** „Класичний” покер-критерій розглядає  $n$  груп по п'ять послідовних цілих чисел  $\{Y_{5j}, Y_{5j+1}, Y_{5j+2}, Y_{5j+3}, Y_{5j+4}\}$  для  $0 \leq j \leq n$  і перевіряє, які з наступних семи комбінацій відповідають таким п'ятіркам чисел (порядок не має значення) (табл. 4):

Таблиця 4. Типи категорій для класичного покер-критерію

Тип п'ятірки чисел	Схематичне позначення
Всі числа різні:	abcde
Одна пара:	aabcd
Дві пари:	aabb
Три числа одного виду:	aaabc
Повний набір:	aaabb
Чотири числа одного виду:	aaaab
П'ять чисел одного виду:	aaaaa

$\chi^2$  – критерій базується на підрахунку кількості п'ятірок у кожній категорії.

Проте для використання покер-критерію при роботі з комп'ютером використовують дещо спрощену його версію, яка здійснює простіший підрахунок *різних* значень у множині п'ятірок. У цьому випадку виділяють п'ять категорій (табл. 5):

Таблиця 5. Типи категорій для модифікованого покер-критерію

Категорія	Умова належності п'ятірки чисел до категорії
5 =	всі різні
4 =	одна пара
3 =	дві пари або три числа одного виду
2 =	повний набір або 4 числа одного виду
1 =	п'ять чисел одного виду

При такій схемі спрощуються підрахунки і критерій залишається практично таким же ефективним.

При цьому ймовірність того, що в групі з  $k$  елементів є  $r$  різних елементів, становить

$$p_r = \frac{d(d-1)\dots(d-r+1)}{d^k} \begin{Bmatrix} k \\ r \end{Bmatrix},$$

де  $d = 100$  (для розглядуваного випадку);  $\begin{Bmatrix} k \\ r \end{Bmatrix}$  – числа Стірлінга.

При аналізі отриманих послідовностей випадкових чисел було отримано такі результати (табл. 6):

Таблиця 6. Результати застосування модифікованого покер-критерію

Категорія	Кількість	Ймовірність
5	825	0,90345
4	83	0,09558
3	2	0,00097

Отримане значення  $\chi^2$  – статистики 1,605333 при цьому знаходиться між 50- і 75-процентними точками, тобто згенеровані числа є досить випадковими.

**Критерій „максимум- $t$ ”.** Позначимо  $V_j = \max(U_{tj}, U_{tj+1}, \dots, U_{tj+t-1})$  для  $0 \leq j \leq n$ . Після цього застосуємо критерій Колмогорова-Смірнова до послідовності  $V_0, V_1, \dots, V_{n-1}$ , таким чином перевіряючи гіпотезу про те, що функція розподілу  $V_j$  дорівнює  $F(x) = x^t$ ,  $0 \leq x \leq 1$ . Оскільки даний критерій застосовний до чисел, що належать відрізку  $0 \leq x \leq 1$ , то, щоб використати даний критерій до випадкової послідовності чисел  $V = \{V_1, V_2, \dots, V_n\}$ ,  $0 \leq V_i \leq 99$ , було здійснено перехід до послідовності  $A = \{A_1, A_2, \dots, A_n\}$ , де  $0 \leq A_i \leq 1$  за формулою  $A_i = \frac{V_i}{99}$ ,  $i = 0, 1, \dots, n$ .

Значення  $t$  було вибрано рівним 10. На (рис. 3) зображено емпіричну функцію розподілу та графік функції  $F(x) = x^{10}$ .

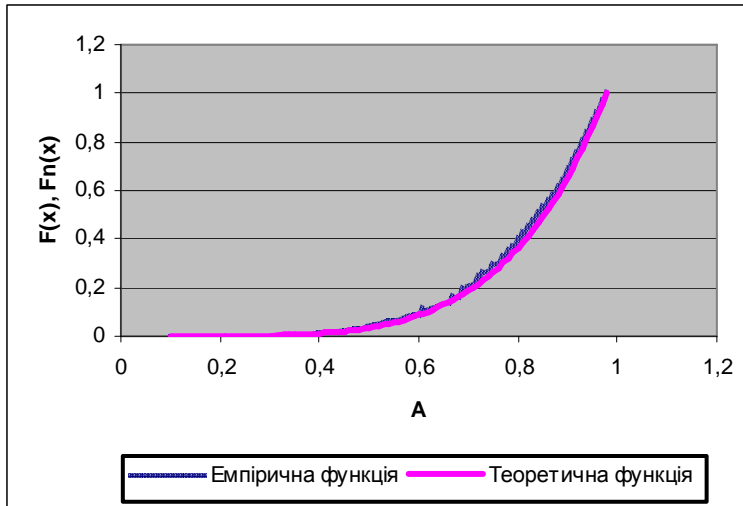


Рис. 3. Графік емпіричної та теоретичної функцій розподілу

Отримані значення статистик  $K_n^+$  і  $K_n^-$  становлять відповідно 0,177947 та 0,761599, тим самим знаходячись між 5- та 75-процентними точками. Результати не заперечують задовільної випадковості отриманої послідовності.

## 5. Висновки

З результатів проведених досліджень можна зробити висновок про відповідність запропонованого у статті генератора випадкових чисел критеріям рівномірності, інтервалів, „максимуму- $t$ ” і покер-критерію [2]. Більше того, порівняння з результатами, отриманими для стандартних генераторів випадкових чисел, які застосовуються на даний момент, дозволяє сказати, що результати тестування побудованого генератора свідчать про задовільну, а часто навіть кращу, випадковість отриманих послідовностей порівняно з існуючими.

Отже, запропонований нами генератор випадкових чисел на базі  $f_n$ -операції може досить ефективно застосовуватись не тільки в системах дистанційного навчання і контролю знань, де і було проведено його апробацію, але й в інших областях застосування обчислювальних, які потребують генератора випадкових чисел з якомога більш рівномірним розподілом частот попадання виборки по всій заданій множині.

## СПИСОК ЛІТЕРАТУРИ

1. Федорук П.І. Система дистанційного навчання та контролю знань на базі Internet-технологій (на прикладі медичних вузів). – Івано-Франківськ: Плай, 2003. –138 с.
2. Кнут Д. Искусство программирования: Учебное пособие: Пер. с англ. – 3-е изд. – М.: Издательский дом «Вильямс», 2000. – Т. 2: Получисленные алгоритмы. – 832 с.