

М. В. СЕМАНЬКІВ

кандидат технічних наук,

доцент кафедри комп'ютерних наук та інформаційних систем

Карпатський національний університет імені Василя Стефаника

ORCID: 0000-0002-1314-8923

ВДОСКОНАЛЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА РЕГІСТРАХ ЗСУВУ ЗВОРОТНОГО ЗВ'ЯЗКУ ТА ДОСЛІДЖЕННЯ ЙОГО ХАРАКТЕРИСТИК

В даній роботі розглянуто застосування генераторів псевдовипадкових чисел для методу Монте-Карло, комп'ютерних симуляцій, 2D і 3D рендерингу. Проаналізовано їх характеристик та відзначено одну з важливіших характеристик генераторів – якість рівномірності розподілу, тобто наскільки рівномірно будуть розподілені згенеровані точки чи напрямки у просторі. Відзначено, що якісний генератор випадкових чисел у 3D-моделюванні та рендерингу є фундаментом того, щоб результати обчислень і зображення були точними, швидко збіжними та візуально чистими. Проведено огляд останніх публікацій на тему покращення характеристик генераторів псевдовипадкових чисел. У результаті аналізу визначено, що низка існуючих рішень полягає в комбінуванні класичних швидких генераторів або додаванні операції для забезпечення рівномірного заповнення 2D і 3D просторів та зменшення похибки інтегрування в методі Монте-Карло. Серед алгоритмічних генераторів для подальшої модифікації обрано алгоритм Xorshift через його швидкість та простоту інтеграції в інформаційну систему. Запропоновано рішення, що базується на вдосконаленні алгоритму генерації псевдовипадкових чисел Xorshift за рахунок бітного реверсування, що дозволило покращити характеристики згенерованої послідовності. Проведено статистичні тести для запропонованого генератора та здійснено порівняння його результатів з початковим базовим генератором Xorshift. Результати статистичного аналізу показали відсутність значущих відхилень від ідеального рівномірного розподілу. Доведено, що реверсування бітів може суттєво покращувати 2D-проекції й зменшити надмірну щільність точок чи навпаки прогалини. Зауважено крапчасту рівномірність покриття площини світла та швидшу збіжність Монте-Карло інтеграла для генератора з реверсування бітів та відзначено його перспективність для задач рендерингу світла і тіней. Зроблено висновок, що реверсування бітів є простою, але ефективною технікою підвищення якості генератора псевдовипадкових послідовностей. Запропонований генератор має практичне значення для задач Монте-Карло, комп'ютерного моделювання та 3D-візуалізації, де вимоги до рівномірності вибірки у багатовимірному просторі є особливо критичними.

Ключові слова: генератор псевдовипадкових чисел, регістри зсуву, статистичний аналіз.

M. V. SEMANKIV

Candidate of Technical Sciences,

Associate Professor at the Department of Computer Science

Vasyl Stefanyk Carpathian National University

ORCID: 0000-0002-1314-8923

IMPROVEMENT OF A PSEUDORANDOM NUMBER GENERATOR BASED ON A LINEAR FEEDBACK SHIFT REGISTER AND INVESTIGATION OF ITS CHARACTERISTICS

This article examines the use of pseudo random number generators in Monte Carlo methods and in computer simulations, in 2D and 3D rendering. Their characteristics are analyzed, with particular attention given to one of the most important properties of such generators – the quality of distribution uniformity, i.e., how evenly the generated points or directions are distributed in space. It is noted that a high-quality random number generator in 3D modeling and rendering is essential for achieving accurate results, fast convergence, and visually clean images. A review of recent publications on improving the properties of pseudo random number generators is presented. The analysis shows that many existing solutions involve combining classical fast generators or adding extra operations to ensure uniform coverage of 2D and 3D spaces and to reduce Monte Carlo integration error. Among algorithmic generators, Xorshift was selected for further modification due to its speed and ease of integration into an information system. A solution is proposed that builds upon the Xorshift pseudo random number generation algorithm by incorporating bit reversal, which improved the statistical properties of the generated sequence. Statistical tests were performed on the proposed generator, and its results were compared with those of the baseline Xorshift generator. The statistical analysis showed no significant deviations from an ideal uniform distribution. It was demonstrated that bit reversal can substantially improve 2D projections and reduce both excessive clustering of points and gaps. Improved uniformity in light-plane sampling and faster convergence of the Monte

Carlo integral were observed for the bit-reversed generator, highlighting its potential for light and shadow rendering tasks. It is concluded that bit reversal is a simple yet effective technique for improving the quality of pseudo random sequences. This has practical importance for Monte Carlo methods, computer simulation, and 3D visualization, where uniformity of sampling in multidimensional space is especially critical.

Key words: *pseudo random number generator; linear feedback shift register; statistical analysis.*

Постановка проблеми

Генератори псевдовипадкових чисел (ГПЧ) застосовуються в дуже багатьох сферах: для методу Монте-Карло, в машинному навчанні, в комп'ютерній графіці та іграх, для тестування програм і систем та т.д. У рендерингу, комп'ютерних симуляціях і будь-яких методах Монте-Карло якісні ГПЧ мають критично важливе значення, оскільки саме вони визначають, наскільки рівномірно будуть розподілені точки у просторі. Якщо генератор «слабкий», то випадкові точки можуть утворювати скупчення й залишати прогалини, що візуально проявляється у вигляді шуму, смуг або плям у зображенні. Натомість надійні генератори забезпечують рівномірне покриття простору, відсутність кореляцій і закономірних візерунків, швидку генерацію мільйонів чисел [1].

Генератори випадкових і псевдовипадкових чисел мають низку проблем, серед яких ключовими є обмежена якість випадковості (кореляції між послідовними значеннями, нерівномірність розподілу, низька ентропія), скінченний період, що призводить до повторюваності послідовностей у довгих симуляціях, а також передбачуваність, що є критичним для криптографічних застосувань. Додатково виникають питання продуктивності, адже якісні генератори можуть бути повільними, та питання відтворюваності результатів, що важливо у наукових розрахунках. Також можливі програмні помилки у реалізації або фізичні зсуви в апаратних генераторах, що викликає статистичні відхилення та спотворює результати моделювання чи рендерингу [1, 2].

Аналіз останніх досліджень і публікацій

Лінійні регістри зі зворотним зсувом (LFSR) мають кілька характерних проблем: вони генерують повністю детерміновані послідовності з обмеженим періодом, що легко прогнозуються після спостереження невеликої кількості вихідних бітів, тому не підходять для криптографії [2]. Їхня лінійність призводить до слабкої статистичної випадковості – у спектрі з'являються помітні кореляції, відсутні певні бітові комбінації, а розподіл може відхилятися від рівномірного [3]. LFSR також чутливі до початкового стану: за нульової ініціалізації регістр «зависає» у нулях. Хоч вони дуже швидкі й прості в апаратній реалізації, але у задачах моделювання, рендерингу або криптографії їх часто комбінують або нелінійно перетворюють, щоб покращити статистичні властивості й приховати передбачуваність [4].

Для покращення статистичних властивостей і рівномірності розподілу у генераторів на основі лінійного зворотного зсувного регістра здійснюють комбінування декількох генераторів, що дозволяє збільшити періодичність та зменшує лінійність [3]. Для згладження нерівномірності в генераторах даного типу використовують перестановку вивідних бітів [5].

Формулювання мети дослідження

Метою роботи є вдосконалення алгоритму генерації псевдовипадкових чисел на регістрах зсуву зворотного зв'язку (Xorshift) за рахунок введення дії реверсу на кожен 32/64-бітну вибірку та дослідження статистичних характеристик запропонованого генератора псевдовипадкових чисел.

Викладення основного матеріалу дослідження

Розглянемо популярний ГПЧ, що є базовим генератором для тестування методів інтеграції у Монте-Карло рендерингу – генератор Xorshift, що відкритий Джорджем Марсальєю [2]. Він є підмножиною генераторів лінійного регістра зсуву зворотного зв'язку. Метод Xorshift генерує випадкові числа за допомогою багаторазового використання побітових операторів виключне-або (XOR, $\oplus$) та бітових зсувів ($\ll$ для лівого та $\gg$ для правого). Це робить його дуже швидким в сучасних комп'ютерних архітектурах. Він вимагає дуже малого розміру коду та стану, але він не проходить всі статистичні тести без вдосконалення, одним зі способів виправити це – поєднання їх з нелінійними функціями або включити додаткову операцію [4].

Розглянемо детальніше Xorshift64. Нехай x_n – 64-бітне ціле число, що згенеровано на n кроці. Наступне число формується на основі рекурентної формули:

$$\begin{aligned} x_{n+1} &= T(x_n); \\ T(x) &= (((x \oplus (x \ll a)) \oplus ((x \oplus (x \ll a)) \gg b)) \oplus \\ &\oplus (((x \oplus (x \ll a)) \oplus ((x \oplus (x \ll a)) \gg b)) \ll c)) \bmod 2^{64}, \end{aligned}$$

де $\oplus$ – побітове XOR, $\ll k$ – циклічний зсув на вліво k бітів, $\gg k$ – зсув вправо на k бітів, $a, b, c \in N$ – три параметри-зсуви [2].

Усі операції виконуються за модулем 2^{64} .

Опишемо запропоновану для генератора операцію реверсування порядку бітів. Нехай $x \in \{0, 1, \dots, 2^{b-1}\}$ – ціле число, що подано у двійковій формі:

$$x = \sum_{i=0}^{b-1} x_i 2^i, \quad x_i \in \{0,1\}, \quad x_0 - \text{молодший біт}, \quad x_{b-1} - \text{старший}.$$

Тоді операція реверсу має вигляд:

$$\text{rev } x_b(x) = \sum_{i=0}^{b-1} x_i 2^{b-1-i},$$

тобто індекс біта змінюється з i на $b-1-i$.

Операція перестановки бітів не змінює періоду, і в бінарному сенсі вона залишається лінійною. В числовому поданні вона змінює розподіл старших/молодших бітів. Запропонований генератор Xorshift з реверсуванням порядку бітів в подальшому буде згадуватись як реверсивний Xorshift або Xorshift з реверсуванням бітів.

Одним із методів аналізу генераторів випадкових чисел є створення візуалізації згенерованих чисел [6]. Побудовано точкові діаграми з нормалізацією точок у діапазоні $[0,1]$ для генератора Xorshift64 та запропонованого реверсивного генератора (рис. 1).

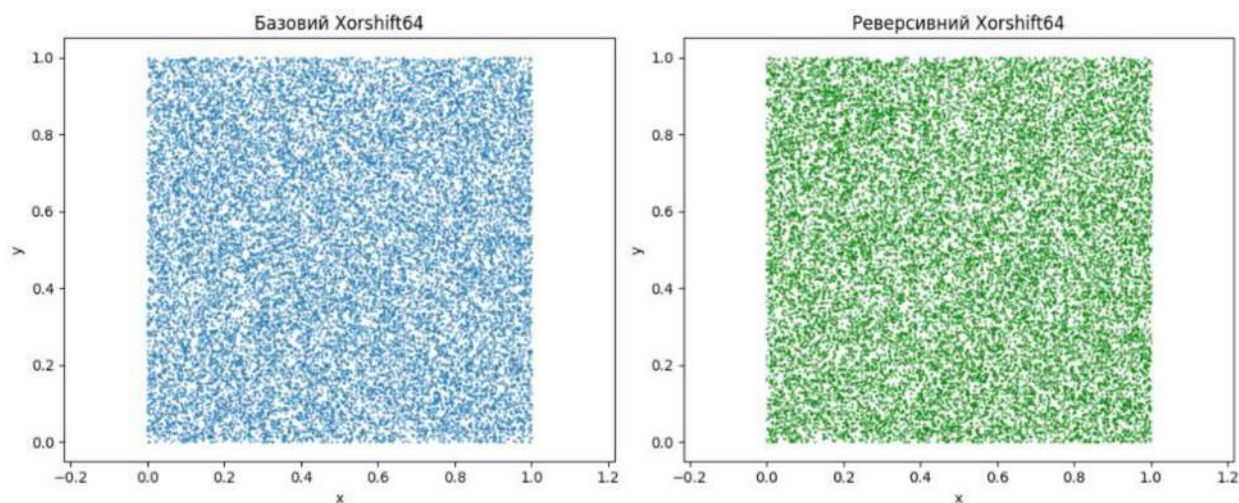


Рис. 1. Візуалізація розподілу згенерованих точок на площині

Статистичний аналіз

Проведено статистичне дослідження [6] послідовностей згенерованих базовим генератором Xorshift та реверсивним Xorshift, проведено наступні тести та отримано результати:

1. Осьові тести для перевірки розподілу кожної координати окремо – X , Y та Z . Кожна координата є 1D-вибіркою, і для неї використано тест Колмогорова-Смірнова і χ^2 -критерій.

Таблиця 1

Результати тестів Колмогорова-Смірнова і χ^2 -критерію

Генератори	Осі	KS-тест	χ^2 -критерій
Генератор Xorshift	X	stat = 0.0040, $p = 0.9032$	stat = 53.28 ($df = 63$), $p = 0.8036$
	Y	stat = 0.0076, $p = 0.1920$	stat = 68.25 ($df = 63$), $p = 0.3035$
	Z	stat = 0.0042, $p = 0.8749$	stat = 50.35 ($df = 63$), $p = 0.8754$
Реверсивний Xorshift	X	stat = 0.0093, $p = 0.0618$	stat = 67.22 ($df = 63$), $p = 0.3347$
	Y	stat = 0.0053, $p = 0.6189$	stat = 52.96 ($df = 63$), $p = 0.8124$
	Z	stat = 0.0073, $p = 0.2304$	stat = 61.55 ($df = 63$), $p = 0.5282$

Обидва генератори (Xorshift64 і з реверсуванням бітів) демонструють розподіл, що близький до рівномірного за всіма осями. Проте операція реверсування бітів дала невелике покращення статистичних показників. Вищі p -значення у тесті Колмогорова-Смірнова і χ^2 -тесті вказують на зменшення прихованих кореляцій і більш «гладке» заповнення простору. У практичних задачах, таких як моделювання, Монте-Карло, 3D-рендеринг, такий реверсивний генератор може бути корисним для покращення якості випадкової вибірки.

2. Тест Пірсона парних кореляцій між осями. Його використовують, щоб перевірити, чи не виникають систематичні залежності між координатами випадково згенерованих точок. У випадку справді рівномірного тривимірного розподілу очікується, що значення X , Y і Z мають бути статистично незалежними, тобто їхня кореляція

повинна бути близькою до нуля. Даний тест допомагає виявити приховані залежності, які не завжди видно на гістограмах або χ^2 -тестах.

Таблиця 2

Тест Пірсона парних кореляцій між осями

Генератори	Площини	Результати тесту
Генератор Xorshift	XY	0.004512102657454674
	XZ	0.0025055279677412643
	YZ	-0.004825255314985926
Реверсивний Xorshift	XY	-0.01779539191410323
	XZ	0.013988626760637064
	YZ	-0.002869986540511929

Аналіз парних кореляцій між координатами XY , ZX , Y , Z показав, що для базового генератора Xorshift значення залишаються майже нульовими ($|r| < 0.005$), що свідчить про практичну незалежність координат і відсутність осьових залежностей, тобто точки в просторі розподілені рівномірно й ізотропно. Натомість у випадку з реверсуванням бітів кореляції зростають за модулем ($|r| \approx 0.014 - 0.018$), що вказує на появу слабких, але помітних взаємозалежностей між координатами, зокрема негативної кореляції в площині XY . Хоча такі величини все ще невеликі й не призводять до різкого порушення рівномірності, вони можуть формувати приховані діагональні структури в хмарі точок, що потенційно знижує статистичну ефективність при застосуванні у прикладних задачах, де критичною є саме незалежність координат і відсутність латентних закономірностей.

3. Покриття на сітці (2D/3D χ^2). Цей тест потрібен для того, щоб перевірити наскільки рівномірно точки покривають простір не лише вздовж однієї осі, а й у взаємодії між осями.

Таблиця 3

Покриття на сітці (2D/3D χ^2)

Сітка	Xorshift	Реверсивний метод
2D χ^2	$XY: \chi^2 = 242.10, p = 0.7094$	$XY: \chi^2 = 255.87, p = 0.4729$
	$XZ: \chi^2 = 260.99, p = 0.3849$	$XZ: \chi^2 = 272.31, p = 0.2180$
	$YZ: \chi^2 = 297.96, p = 0.0333$	$YZ: \chi^2 = 233.55, p = 0.8285$
3D χ^2	$\chi^2 = 485.27, p = 0.7875$	$\chi^2 = 550.04, p = 0.1127$

Отримані результати χ^2 -тестів свідчать, що рівномірність покриття простору суттєво залежить від способу генерації. Для генератора Xorshift у проекції YZ зафіксовано значне відхилення від рівномірного розподілу ($p \approx 0.033$), що вказує на наявність прихованих кореляцій чи кластеризації. Використання реверсування бітів помітно зменшило цю проблему ($p \approx 0.8285$), забезпечивши значно більш рівномірне покриття в цій площині. Водночас у повному 3D просторі реверсивний Xorshift показав гірший результат ($p \approx 0.11$ проти 0.79), що означає надлишкову регулярність і менш природну імітацію випадковості. Таким чином, реверсування бітів може суттєво покращувати 2D-проекції й зменшувати локальні артефакти, проте у задачах, де критична саме глобальна тривимірна рівномірність, базовий Xorshift або низькодисперсні послідовності можуть залишатися кращими.

4. Тест найближчого сусіда потрібен для оцінки того, наскільки «щільно» і рівномірно розташовані точки в просторі. Якщо точки дійсно рівномірні, то відстані до найближчих сусідів повинні мати відносно стабільний розподіл – без надто великої кількості дуже маленьких відстаней (кластерів) чи надто великих прогалів.

Таблиця 4

Тест найближчого сусіда

Генератори	Середнє значення	Стандартне відхилення
Генератор Xorshift	mean = 21.1720	std = 7.8514
Реверсивний Xorshift	mean = 21.1019	std = 7.9206

Аналіз результатів тесту найближчого сусіда для генераторів Xorshift звичайного та з реверсування бітів показав, що обидві послідовності формують просторові конфігурації точок зі статистично подібними характеристиками локальної щільності. Середні значення відстаней між найближчими точками (близько 21.1–21.2) практично збігаються, що свідчить про аналогічний масштаб заповнення тривимірного простору для обох генераторів. Стандартні відхилення (приблизно 7.9) також майже однакові, що вказує на відсутність значущих відмінностей у варіативності міжпунктових відстаней та, відповідно, на схожу тенденцію до рівномірного розподілу без явних кластерів чи «порожніх зон».

5. 2D-/3D-KS альтернативи (енергетична відстань EnergyDist, максимальна середня розбіжність MMD) є тестами для оцінки рівномірності заповнення простору вищих вимірів. Вони допомагають зрозуміти, чи дійсно генератор підходить для задач, де важливе рівномірне покриття.

Таблиця 5

2D-/3D-KS альтернативи

Генератори	Тест	2D	3D
Генератор Xorshift	EnergyDist	0.00277	0.00374
	MMD	0.00009	0.00009
Реверсивний Xorshift	EnergyDist	0.00221	0.00453
	MMD	0.00010	0.00011

Отримані результати показують, що у площинних проекціях (2D) енергетична відстань для вибірки згенерованої реверсивним Xorshift є меншою, ніж для базованої, що свідчить про більш рівномірне покриття й зменшення локальних кластерів; однак у повному 3D просторі реверсування бітів демонструє гірші показники (вища EnergyDist), тобто він створює приховану регулярність, яка знижує глобальну випадковість. Значення MMD для обох методів залишаються дуже малими й близькими, що означає загалом добру апроксимацію рівномірного розподілу. На основі даного тесту можна зробити висновок, що реверсивний метод корисний для задач, де важлива якість 2D-проекцій (наприклад, рендеринг світла і тіней), тоді як звичайний Xorshift більш надійний у тривимірних симуляціях. Даний тест підтвердив результати тесту покриття на сітці ($2D/3D\chi^2$).

Автокореляція (ACF) по осі перевіряє наскільки послідовні значення генератора випадкових чисел залежать від попередніх.

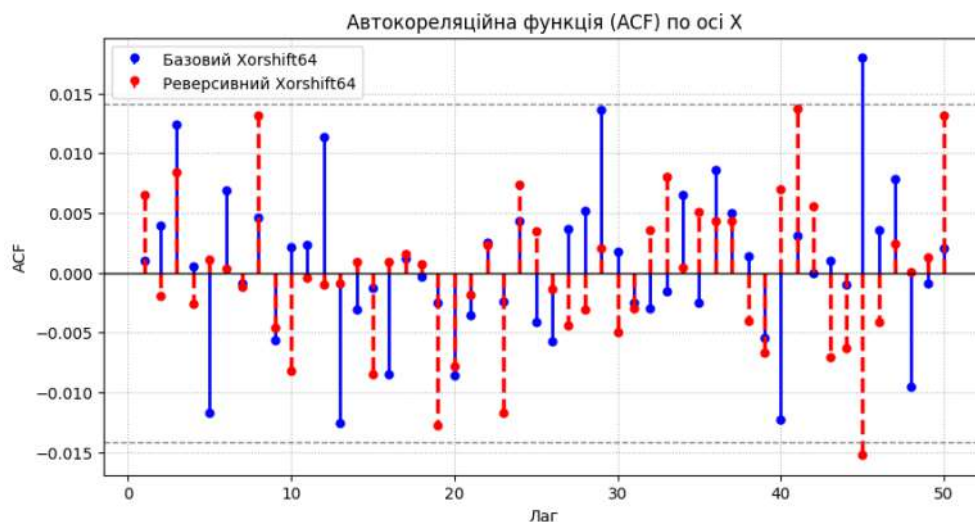


Рис. 2. Результати тесту на автокореляцію

На основі рис. 2 можна зробити висновок, що в обох випадках значення автокореляцій залишаються дуже близькими до нуля і майже завжди лежать у межах довірчого інтервалу 95 %. Це свідчить про відсутність суттєвої лінійної залежності між сусідніми елементами послідовності. У реверсивного генератора (пунктирна лінія) може бути трохи більша варіативність, ніж у базованого (суцільна), але відхилення все одно не перевищують статистично значущих меж. Таким чином, реверсування бітів не погіршило якість випадковості, ані не додало систематичних залежностей. Отже, обидва варіанти, як базовий Xorshift, так і реверсивний, демонструють відсутність автокореляцій на низьких лагах, що є ознакою хорошої властивості випадкових послідовностей у задачах Монте-Карло та моделювання.

Використання генераторів для рендерингу

У сучасних системах рендеринг часто використовує Монте-Карло інтеграцію і тому він потребує якісні генератори псевдовипадкових чисел, бо саме вони визначають, наскільки рівномірно в просторі будуть вибиратися напрямки променів, точки вибірки на поверхнях та у середовищі. Вони є фундаментом для того, щоб результати обчислень і зображення були точними, швидко збіжними та візуально чистими. Тому проведено ряд тестів для визначення ефективності запропонованого генератора для практичного застосування для рендерингу [7].

1) перевірка якості освітлення й тіней у графічних рушіях чи рендерах показує наскільки правильно система відтворює м'які тіні від протяжних джерел світла. RMSE як міра точності визначить наскільки якість тіні, створеної апроксимацією, відрізняється від еталонного фізично коректного рендерингу.

Для базового генератора RMSE становить 0.006878 (при $spp = 16$), для реверсивного 0.005971 ($spp = 16$). Ці результати означають, що при використанні 16 променів на піксель (spp) метод із реверсування бітів дав меншу похибку середньоквадратичного відхилення ($RMSE = 0.005971$), ніж базовий Xorshift ($RMSE = 0.006878$). Тобто згенероване зображення за допомогою генератора з реверсом бітів виявилося трохи точнішим у відтворенні сталонного результату. Така перевага свідчить, що реверс бітів може краще «розкидати» вибірки по просторі, зменшуючи локальні кластери й прогалини, що критично для задач рендерингу світла та тіней, де важлива рівномірність покриття інтегральної області.

Тест прямого освітлення з використанням MIS (Multiple Importance Sampling, багатокритеріальне вибіркве інтегрування) перевіряє, наскільки правильно і ефективно алгоритм рендерингу відтворює пряме освітлення. Він показує, наскільки добре рендер знижує шум, чи правильно балансує ваги між різними PDF , чи збігається результат з еталонним рендерингом.

MIS direct lighting RMSE для базового генератора становить 0.002684 (при $spp = 16$), для реверсивного MIS direct lighting RMSE дорівнює 0.002714 ($spp = 16$). Отримані результати показують, що при використанні MIS для прямого освітлення різниці між генератором Xorshift64 та його варіантом із реверсією бітів практично відсутня: значення RMSE для обох випадків дуже близькі, що відповідає лише $\approx 1\%$ відносної різниці і може бути пояснене випадковими статистичними флуктуаціями. Це означає, що реверсування бітів у даній задачі не дає ані помітної переваги, ані шкоди – точність обчислення в першу чергу визначається самим методом MIS і геометрією сцени, а не деталями генератора псевдовипадкових чисел.

Пряме освітлення від квадратного світла (без видимості), обчислення освітлення однієї точки від квадратного світильника.

Пряме освітлення (квадратне площинне джерело світла, без перевірки видимості)

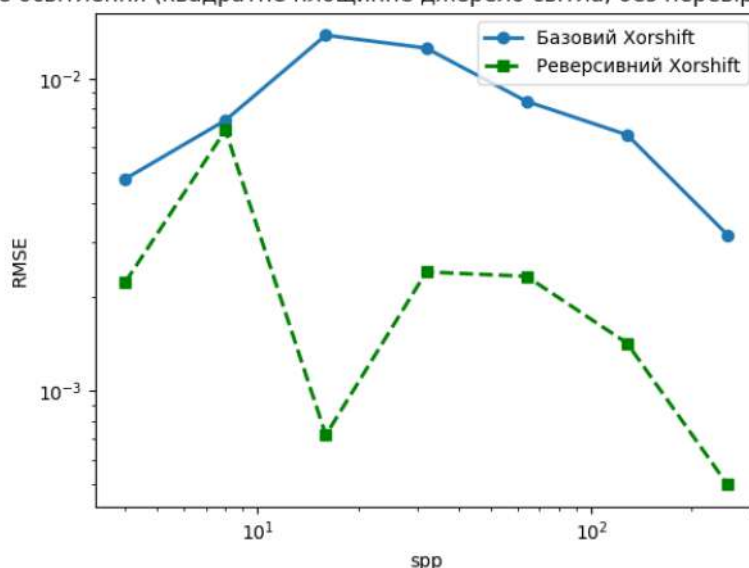


Рис. 3. Результати тесту Direct lighting

Крива показує, що для задачі прямого освітлення від квадратного джерела без видимості послідовність із реверсуванням бітів (пунктир) майже на всіх spp дає менший RMSE, ніж базовий Xorshift (суцільна), інколи істотно – отже, за однакової кількості семплів вона збігається швидше (краще покриває квадрат світла). Реверсивний генератор зменшує кластеризацію/прогалини у (u, v) і знижує дисперсію оцінки. Для рендерингу цей результат означає, що реверсування бітів дає кращі вибірки для інтеграції освітлення, ніж базовий Xorshift, коли мова йде про прості інтеграли на низькорозмірних областях. Отже, для прямого освітлення від площинних світильників реверсування зменшило шум і пришвидшило збіжність зображення при тому ж числі семплів. У випадку малих spp це особливо помітно – картинка буде виглядати більш «чистою» при тій самій кількості променів.

Висновки

Отримані результати статистичного аналізу дають підстави стверджувати, що як базовий генератор Xorshift64, так і модифікований варіант із реверсування бітів забезпечують рівномірність розподілу. Зокрема, значення p -value у тесті Колмогорова–Смирнова для всіх координатних осей перевищують критичні пороги, що свідчить про відсутність статистично значущих відхилень від ідеального рівномірного розподілу. χ^2 -статистики не перевищують ступені свободи, а p -value в більшості випадків розташовані у проміжку 0.5–0.75, що вказує на високу якість апроксимації. Слід відзначити, що реверсування бітів у згенерованих послідовностях призвела до незначного

покращення статистичних характеристик: середні χ^2 -статистики зменшились, а p -value тестів зросли, що означає більш рівномірне та «гладке» заповнення простору, зменшення латентних кореляцій між координатами та посилення імітаційних властивостей генератора.

Реверсивний метод має переваги в площинних 2D-проекціях, де він зменшує локальні аномалії, роблячи вибірку більш «рівномірною» та згладженою. Проте у повному 3D просторі він може створювати певну приховану регулярність, що трохи погіршує рівномірність розподілу. MMD показав, що в цілому обидва генератори досить близькі до рівномірного розподілу, але реверсування краще працює для 2D-випадків (наприклад, рендеринг тіней чи текстур), тоді як базовий Xorshift більш стабільний у 3D.

Отримані результати для тесту прямого освітлення з площинним джерелом показують, що використання генератора з реверсування бітів замість стандартного генератора Xorshift дозволяє суттєво зменшити похибку при однаковій кількості семплів на піксель, особливо у випадку малих spp, коли шум у зображенні найбільш помітний. Це свідчить про кращу рівномірність покриття площини світла та, відповідно, швидшу збіжність Монте-Карло інтеграла, що робить метод реверсування бітів перспективним для задач рендерингу світла і тіней, зокрема для вибірки положень на джерелах світла або у просторі параметрів BRDF.

Таким чином, можна зробити висновок, що реверсування бітів є простою, але ефективною технікою підвищення якості псевдовипадкових послідовностей, що може мати практичне значення для задач Монте-Карло, комп'ютерного моделювання та 3D-візуалізації, де вимоги до рівномірності вибірки у багатовимірному просторі є особливо критичними.

Список використаної літератури

1. Pharr M., Jakob W., Humphreys G. *Physically Based Rendering: From Theory to Implementation*. 3rd ed. San Francisco: Morgan Kaufmann, 2016. 1266 с.
2. Xorshift RNGs. ResearchGate. URL: https://www.researchgate.net/publication/5142825_Xorshift_RNGs (дата звернення: 12.09.2025).
3. Pseudo Random Number Generation Using Linear Feedback Shift Registers. Analog devices. URL: https://www.analog.com/en/resources/design-notes/random-number-generation-using-lfsr.html?utm_source=chatgpt.com (дата звернення: 12.09.2025).
4. Alvarez R. Improving the Statistical Qualities of Pseudo Random Number Generators // *Symmetry*. 2022. Т. 14, № 2. С. 269. DOI: 10.3390/sym14020269
5. Condo C., Gross W.J. Pseudo-random Gaussian distribution through optimised LFSR permutations. 2012 IEEE Workshop on Signal Processing Systems. IEEE, 2012. С. 69–74. DOI: 10.1109/SiPS.2012.57
6. Knuth D.E. *The Art of Computer Programming*. Vol. 2: Seminumerical Algorithms. – Addison-Wesley, 1997.
7. Askar A., Shukirgaliyev B., Lukac N., Abdikamalov E. Evaluation of Pseudo-Random Number Generation on GPU Cards // *Computers*. 2021. Vol. 10, No. 12. P. 142. DOI: 10.3390/computers10120142

References

1. Pharr, M., Jakob, W., & Humphreys, G. (2016). *Physically based rendering: From theory to implementation* (3rd ed.). San Francisco, CA: Morgan Kaufmann.
2. Xorshift RNGs. (2003). *ResearchGate*. Retrieved from https://www.researchgate.net/publication/5142825_Xorshift_RNGs (accessed 12 September 2025).
3. Analog Devices. (n.d.). *Pseudo random number generation using linear feedback shift registers*. Retrieved from <https://www.analog.com/en/resources/design-notes/random-number-generation-using-lfsr.html> (accessed 12 September 2025).
4. Alvarez, R. (2022). Improving the statistical qualities of pseudo random number generators. *Symmetry*, 14(2), 269. <https://doi.org/10.3390/sym14020269>
5. Condo, C., & Gross, W. J. (2012). Pseudo-random Gaussian distribution through optimised LFSR permutations. In *2012 IEEE Workshop on Signal Processing Systems* (pp. 69–74). IEEE. <https://doi.org/10.1109/SiPS.2012.57>
6. Knuth, D. E. (1997). *The art of computer programming*. Vol. 2: *Seminumerical algorithms*. Addison-Wesley.
7. Askar, A., Shukirgaliyev, B., Lukac, N., & Abdikamalov, E. (2021). Evaluation of pseudo-random number generation on GPU cards. *Computers*, 10(12), 142. <https://doi.org/10.3390/computers10120142>

Дата першого надходження рукопису до видання: 18.09.2025
Дата прийнятого до друку рукопису після рецензування: 15.10.2025
Дата публікації: 28.11.2025