ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА

(повне найменування закладу вищої освіти)

Факультет математики, фізики та інформаційних технологій

(повне найменування факультету)

Кафедра алгебри, геометрії та диференціальних рівнянь

(повна назва кафедри)

Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

«Інверсний генератор псевдовипадкових чисел другого порядку»

(тема кваліфікаційної роботи українською мовою)

«Inversive generator of pseudorandom numbers of second order»

(тема кваліфікаційної роботи англійською мовою)

Виконав: здобувач денної форми навчання

спеціальності 111 Математика

(код, назва спеціальності)

Освітня програма Математика

(назва)

Кисельов Даниїл Олегович

(прізвище, ім'я, по-батькові здобувача)

Керівник доктор фіз.-мат. наук, професор, Варбанець С.П.

(науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент кандидат технічних наук, доцент, Якімова Н.А.

(науковий ступінь, вчене звання, прізвище, ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри

№____від .....20____р.

Завідувач(ка) кафедри

(підпис) (прізвище,ім'я)

Захищено на засіданні ЕК № _____
протокол №___від .....20____р.

Оцінка_____/_____/_____
(за національною шкалою/шкалою ECTS/ бали)

Голова ЕК

(підпис) (прізвище, ім'я)

Одеса 2024

ЗМІСТ

ВСТУП

В магістерській роботі розглядаються питання побудови генераторів послідовностей псевдовипадкових чисел, а також оцінка згенерованих послідовностей.

Саме тому перший розділ роботи описує апарат випадкових (псевдовипадкових) чисел, а також спеціальний чисельний метод Монте-Карло.

В другому розділі ми розглядаємо елементи теорії генерації псевдовипадкових послідовностей. Надаємо опис існуючих генераторів, методів на яких вони засновані, а також їх ефективність та застосовуваність в різних сферах, зокрема, в криптографії.

Для оцінки якості згенерованих послідовностей існує багато різних методів. Зокрема в теорії чисел одним із таких методів є компіляція методу тригонометричних сум разом із так званим s-мірним тестом на непередбачуваність елементів послідовності. А тому огляду тригонометричних сум, застосуванню методу тригонометричних сум, їх оцінці також присвячено окремий третій розділ дипломної роботи.

За допомогою відомої нерівності Турана-Ердьоша-Коксми свого часу була встановлена відповідність між послідовностями псевдовипадкових чисел і тригонометричними сумами шляхом оцінки так званої дискріпантної функції/дискріпансії відповідної послідовності саме за допомогою оцінок тригонометричних сум. Оцінкам функції дикріпансії та суміжним поняттям (таким як рівнорозподілена послідовність псевдовипадкових чисел) присвячено четвертий розділ дипломної роботи.

Нарешті останній і основний розділ, який власно і був метою магістерської роботи, присвячений побудові інверсних конгруентних генераторів другого порядку, оцінка послідовності псевдовипадкових чисел, яка генерується даним генератором за допомогою s-мірного тесту на непередбачуваність.

РОЗДІЛ 1

Псевдовипадкові числа і їх застосування

В літературі, яка так чи інакше пов’язана з математичною статистикою, часто наводяться так звані «таблиці випадкових чисел». Також наразі, із зростанням обчислювальних потужностей, інтерес до питань, що пов’язані з випадковими та псевдовипадковими числами стрімко зростає. Це стається тому, що наразі в багатьох різних науках активно використовується моделювання. Основою будь-якого моделювання є модель, яка зазвичай є багатофакторною. Проте, «паливом» для різноманітних моделей є саме випадкові та псевдовипадкові числа з різноманітними властивостями. Загалом їх основне завдання наближено відобразити реальні умови. Надамо визначення випадкових чисел

Випадкові числа це отримана послідовність реалізацій випадкової величини із заданим законом розподілу.

До методів отримання випадкових чисел відносять:

- за допомогою таблиць випадкових чисел;
- за допомогою спеціальних пристроїв – генераторів випадкових чисел(зазвичай їх називають фізичними генераторами випадкових чисел);

Загалом, послідовність випадкових чисел може бути отримана як штучним чином так і фізичним і спочатку в науці намагались використовувати випадкові числа, отримані саме за допомогою так званих фізичних генераторів випадкових чисел. Насамперед фізичними генераторами є фізичні шуми, до яких можна віднести іонізуючу радіацію, пуасонівський шум в резисторі, космічне випромінювання тощо. Проте у фізичних генераторів випадкових чисел існує ряд досить великих недоліків:

1) час та трудовитрати на встановлення та обслуговування фізичного генератора;
2) ціна відповідних комплектуючих та загальна ціна фізичного генератора;
3) час, який витрачається на генерацію послідовності випадкових чисел;
4) неможливість відтворення раніше згенерованої послідовності випадкових чисел.

Тож, аналізуючи всі переваги і недоліки з’являється ідея, про отримання чисел, які за своїми властивостями подібні до випадкових, проте уникають проблем, з якими стикаються наприклад фізичні генератори випадкових чисел. Надамо визначення псевдовипадкового числа

Псевдовипадкове число — це елемент числової послідовності, створеної за певним алгоритмом, властивості якої наближаються до випадкових.

Числова послідовність, що утворена певним алгоритмом, елементом якої є псевдовипадкове число називається послідовністю псевдовипадкових чисел.

Як вже було зазначено, основним споживачем випадкових та псевдовипадкових чисел є моделювання у різних галузях. Для того аби використовувати як випадкові так і псевдовипадкові числа у моделюванні, вони повинні відповідати наступним критеріям:

- Досить точно відтворювати поведінку випадкової величини з визначеним розподілом.
- Використовувати якомога менше машинних операцій для генерації одного числа.

Проте окрім моделювання є ще 2 постійних споживача псевдовипадкових чисел: це рандомізація умов експериментів та метод вибіркових обстежень. Рандомізація умов експериментів за своєю сутністю є першим кроком в історії застосування псевдовипадкових чисел. В науку концепцію рандомізації вніс видатний англійський вчений Рональд Фішер. Він розглядав випадковість як механізм захисту результатів експерименту від впливу зовнішніх факторів і як механізм появи певних подій з певною вірогідністю.

Наступний великий крок в розвитку псевдовипадкових чисел був пов'язаний з виникненням так званого методів Монте-Карло. Вважається, що самі методи з’явились завдяки роботам вчених Д. Неймана, С. Улама, М. Метрополіса та інших вчених, що працювали в 1940-х роках у Лос-Алмосі. На сьогоднішній день не існує загальноприйнятого визначення методів Монте-Карло. Зазвичай вони розуміються як чисельні методи розв’язання математичних задач за допомогою випадкових величин. При такому визначенні до методів Монте-Карло можна віднести і деякі інші методи, як наприклад стохастичні наближення або випадковий пошук, які в традиційній

класифікації розглядаються окремо. Водночас варто відзначити декілька ключових моментів що стосуються методів Монте-Карло, а саме:

- вони можуть конкурувати лише тільки з класичними чисельними методами, а не з аналітичними, бо за своєю сутністю є чисельними методами;
- методи Монте-Карло можна використовувати при розв’язанні різноманітних задач, зокрема тих, що мають ймовірнісний характер і пов’язані з випадковими величинами.

Не дивлячись на те, що саму назву методи отримали в 1940-х роках, самі методи почали застосовуватись набагато раніше. Так наприклад в 1850 р. метод Монте-Карло був застосований для обчислення ірраціонального числа π за допомогою експерименту, основою для якого стала відома класична задача під назвою «Задача Бюффона».

Методи Монте-Карло розвивалися й надалі. Так у 1970-х роках у новій галузі математики — теорії обчислювальної складності — було доведено, що існує клас задач, складність (кількість обчислень, необхідних для отримання точного результату) яких зростає експоненційно з розміром задачі. Іноді можна знайти алгоритм, який буде менш складним, жертвуючи точністю, але для багатьох задач цього зробити не вдається (наприклад, задача визначення об'єму випуклого тіла в n-вимірному евклідовому просторі або, в загальному, обчислення n-вимірних інтегралів). У таких випадках метод Монте-Карло стає єдиним способом отримати достатньо точну відповідь за прийнятний час. Наразі основні зусилля дослідників спрямовані на розробку ефективних алгоритмів Монте-Карло для моделювання різних фізичних, хімічних і соціальних процесів, адаптованих до паралельних обчислювальних систем. Детальніше про методи Монте-Карло можна дізнатись наприклад з [4].

РОЗДІЛ 2

Огляд генераторів послідовностей псевдовипадкових чисел

Для отримання псевдовипадкових послідовностей чисел використовуються так звані генератори псевдовипадкових чисел (далі ГПСЧ).

Генератор псевдовипадкових чисел — це алгоритм, який створює послідовність чисел, елементи якої майже незалежні один від одного та підпорядковуються певному розподілу (зазвичай дискретному рівномірному).

Для того аби називати деякий алгоритм, ГПСЧ до нього висуваються наступні якісні характеристики:

1. Достатньо тривалий період — це гарантія відсутності зациклювання послідовності в межах розв'язуваної задачі. Довжину періоду потрібно математично обґрунтувати.
2. Ефективність — швидкість роботи алгоритму та невеликі витрати пам'яті.
3. Відтворюваність — можливість повторно відтворити раніше згенеровану послідовність чисел будь-яку кількість разів.
4. Портативність — однакове функціонування на різному обладнанні та операційних системах.
5. Швидкість отримання X_{n+i} елемента послідовності чисел, коли відомий X_n елемент для і будь-якого значення; це дозволяє розділяти послідовність на декілька потоків (послідовностей чисел).

Історично засновником підходів, які застосовуються у ГПСЧ та загалом їх перших форм вважається Джон фон Нейман. Джон фон Нейман вважав використання фізичних генераторів випадкових чисел у комп'ютерах неприпустимим, оскільки для перевірки розрахунків повторення попередніх дій вимагало б відтворення вже отриманого випадкового числа, а створювати нові випадкові числа було б недоцільно. Запис і зберігання згенерованих випадкових

чисел потребували б можливості їх зчитування. Проте механізми зчитування даних були одним із найвразливіших елементів обчислювальних машин 1940-х років. Фон Нейман вважав генератори випадкових чисел на апаратному рівні непридатними, оскільки, якщо вони не реєстрували вихідні дані, їх не можна було б перевірити на помилки. Якщо вони реєстрували свій вихід, це виснажувало б обмежену пам'ять комп'ютера, що впливало на здатність комп'ютера зчитувати та записувати числа. Якщо числа записувалися на картки, це займало б набагато більше часу для запису та зчитування. На комп'ютері ENIAC, яким він користувався, метод «середнього квадрата» генерував числа в кілька сотень разів швидше, ніж зчитування чисел з перфокарт.

Ранній комп'ютерний генератор псевдовипадкових чисел, запропонований Джоном фон Нейманом у 1946 році, відомий як метод «середнього квадрата». Алгоритм полягає в наступному: візьмемо будь-яке число, піднесемо його до квадрату, видалимо середні цифри отриманого числа, які і вважатимемо псевдовипадковим числом, а потім використаймо це число як початкове для наступної ітерації. Наприклад, підносячи число «1111» до квадрату, ми отримаємо «1234321», яке можна записати як «01234321». Це дає «2343» як псевдовипадкове число. Повторюючи цю процедуру, на наступному кроці ми отримаємо «4896» як наступний результат псевдовипадкового числа і так далі. Єдина відмінність нашого запропонованого ГПСЧ від того, який запропонував фон Нейман полягає в тому, що Нейман у своєму алгоритмі використовував 10-значні числа. [21]

Основним недоліком методу "середнього квадрата" полягає в тому, що множина псевдовипадкових чисел є обмеженою – вона може занадто швидко зациклюватись. Так наприклад якщо на деякому кроці ми отримали число, середні цифри якого є нулями, то отримали зациклену послідовність з нулів.

Наступним етапом розвитку ГПСЧ вважається так званий лінійний когруентний метод, який був запропонований у 1951 р. Д.Г. Лемером, [14] суть якого полягає

в заданні послідовності псевдовипадкових цілих чисел наступною рекурсивною формулою

$$X_{n+1} = (aX_n + c)\ mod\ m\ , (2.1)$$

де $a, m, c \in Z: 1 < m, 0 < a < m, 0 < c < m, X_0 < m$

Основним недоліком цього методу генерації псевдовипадкових чисел є залежність X_n від X_0 для n > 0 бо, $X_n = \left(a^n X_0 + \frac{c(a^n-1)}{(a-1)}\right) mod\ m$

Також варто відмітити той факт, що даний метод генерації псевдовипадкових чисел також досить швидко зациклюється.

Необхідно зазначити також, що неабиякий вплив на сучасні ГПСЧ зробив алгоритм, відомий під назвою генератор Фібоначчі або так звані адитивні генератори.[22] На відміну від генераторів, які використовують лінійний конгруентний алгоритм, фібоначчієві генератори можна застосовувати в статистичних алгоритмах, які вимагають високої точності. З цієї причини лінійний конгруентний алгоритм поступово втрачав свою популярність, і його місце займало сімейство фібоначчієвих алгоритмів, які можуть бути рекомендовані для використання в алгоритмах, де важлива висока якість псевдовипадкових чисел.

Послідовністю Фібоначчі називається послідовність, в якій X_{n+1}залежить більше ніж від одного з попередніх значень і визначається за формулою$X_{n+1} = (X_n + + X_{n-1})\ mod\ (2^m)$

Спочатку вивчався саме даний алгоритм, проте було виявлено що даний ГПСЧ не є достатньо ефективним, тому було запропоновано допрацьована формула послідовності у вигляді $X_{n+1} = (X_n + X_{n-k})\ mod\ (2^m)$

Виявилось, що даний алгоритм є ефективним для $k \geq 16$

Очевидною перевагою адитивних генераторів є те, що вони використовують операцію додавання, а не множення, що є значно повільнішою операцією, а також період даного генератора (період має бути $\geq 2^m$).

Наступним етапом в розвитку ГПСЧ став генератор Блюма-Шуба [7]. Його практична цінність полягає в його криптографічній стійкості, а також в застосуванні підходів теорії чисел при генерації послідовності псевдовипадкових чисел. Також за цей алгоритм була отримана премія Тьюрінга в 1995 році.

Алгоритм виглядає наступним чином:

$$x_{n+1} = x_n^2 mod\ M (2.2)$$

де $M = pq$ (p і q достатньо великі прості числа)

Також $p \equiv q \equiv 3\ mod\ 4$ (це гарантує, що кожен квадратний лишок має тільки один корінь, котрий також є квадратичним лишком) і $gcd(p-1, q-1)$ повинен бути достатньо малим для того, аби період був достатньо великим.

Цікавою особливістю даного алгоритму є те, що для отримання x_n не потрібно вираховувати всі попередні значення. Якщо відомий початковий стан генератора x_0 і числа p та q, то n-е псевдовипадкове число може бути знайдене за формулою (2.3)

$$x_n = x_0^{2^n\ mod\ \lambda(M)}\ mod\ M, (2.3)$$

де λ – функція Кармайкла:

$$\lambda(M) = \lambda(pq) = \text{НСК}(p-1, q-1)$$

Цей генератор підходить для використання в криптографії, але не в моделюванні, оскільки його швидкість недостатня. Проте він має надзвичайно високу стійкість, що забезпечується якістю генератора, враховуючи обчислювальну складність задачі факторизації чисел. Коли прості числа обрані ретельно, і кожен біт xnx_nxn є вихідними даними з оцінкою $O(\log\log M)$, то межа для M швидко зростає, і обчислення вихідних бітів стає настільки складним, як і сам процес факторизації числа M.

Якщо факторизація цілих чисел є настільки складною, як припускається, то генератор з великим M буде видавати послідовність, яка не містить жодних виявлених не випадкових шаблонів, навіть при значних обсягах обчислень. Однак існує ймовірність розробки швидкого алгоритму для факторизації, що ставить під сумнів гарантовану надійність алгоритму.

Проте розвиток ГПСЧ не зупинився, а продовжується і надалі. Так, наприклад, у 2020 році з'явився так званий генератор випадкових чисел на основі лічильника. Це тип генератора псевдовипадкових чисел, який використовує виключно цілочисельний лічильник для зберігання свого внутрішнього стану. Такі генератори часто застосовуються для створення псевдовипадкових чисел для великих паралельних обчислень.

Генератор псевдовипадкових чисел можна уявити як функцію, що перетворює серію бітів, яка є початковим станом, на новий стан і випадкове число. Інакше кажучи, маючи функцію ГПСЧ і початковий стан $state_0$, ми можемо багаторазово застосовувати ГПСЧ для отримання послідовності нових станів і випадкових чисел:

$$\text{ГПСЧ}(state_0) = state_1, num_1$$

$$\text{ГПСЧ}(state_1) = state_2, num_2$$

$$\text{ГПСЧ}(state_2) = \cdots$$

У деяких ГПСЧ, таких як наприклад вихр Мерсена, стан є великим і складає більше 2048 байт. В інших, наприклад, у xorshift, стан і кількість параметрів є тим самим, тому стан є меншим — лише 4, 8 або 16 байтів, в залежності від розміру генерованих чисел. Однак у обох випадках, як і в більшості традиційних ГПСЧ, стан змінюється непередбачувано. Тому, якщо потрібно обчислити певний $state_i$, починаючи з початкового стану $state_0$, необхідно по черзі обчислювати $state_1$, $state_2$ і так далі, повторно застосовуючи ГПСЧ і разів. Такі алгоритми, за своєю природою, є послідовними і не можуть бути ефективно використані на паралельних машинах, таких як багатоядерні процесори чи графічні процесори.

На відміну від них, генератор псевдовипадкових чисел на основі лічильника є алгоритмом, у якому стан змінюється дуже просто: $state_i = i$. Завдяки цьому кожне число можна генерувати незалежно, без необхідності знати результат попереднього виклику ГПСЧ.

Ця особливість дозволяє ефективно запускати генератор псевдовипадкових чисел на основі лічильника на кількох потоках ЦП або графічного процесора. Наприклад, для генерації nnn випадкових чисел на GPU можна створити n потоків, кожен з яких обчислюватиме ГПСЧ(i).

Загалом більшість детермінованих ГПСЧ відповідають структурі, яка була запропонована П. Лекуером у 1994 році [16]: (S, μ, f, V, g) – детермінований ГПСЧ, де S – кінцевий набір станів, μ – ймовірнісний розподіл в просторі станів S, яке використовується для обрання початкового стану s_0, $f: S \to S$ – функція переходу, V – простір вихідних значень, $g: S \to V$.

Зазвичай $V = (0,1)$, а стан генератора задається формулою $s_i = f(s_{i-1})$ де $i \geq 1$.

Вихідне значення генератора $v_i = g(s_i) \in V;\ v_0, v_1, v_2, \ldots$ - послідовність псевдовипадкових чисел. Так як S скінченна множина, то повинні існувати деякі числа $k \geq 0$ та $m > 0$: $s_{k+m} = s_k$. Тому для всіх $i \geq k$, будуть виконуватись умови $s_{i+m} = s_i$ $v_{i+m} = v_i$ тому що функції f та g детерміновані. Таким чином

також отримали визначення періоду ГПСЧ: в даному контексті періодом ГПСЧ називається мінімальне додатнє число m.

Проте ГПСЧ мають і певні недоліки. Жоден детермінований алгоритм не може генерувати повністю випадкові числа, він може лише апроксимувати деякі їхні властивості. Як сказав Джон фон Нейман: «Кожен, хто відчуває слабкість до арифметичних методів отримання випадкових чисел, безсумнівно є грішником».

Будь-який ГПСЧ з обмеженими ресурсами рано чи пізно зациклюється — починає повторювати одну й ту ж послідовність чисел. Довжина циклів ГПСЧ залежить від самого генератора і складає близько $2^{\frac{n}{2}}$, де n — розмір внутрішнього стану в бітах, хоча лінійні конгруентні та РСЛОС-генератори мають максимальні цикли порядку 2^n. Якщо породжена послідовність ГПСЧ сходиться до занадто коротких циклів, такий ГПСЧ стає передбачуваним і непридатним для практичного застосування.

Більшість простих арифметичних генераторів, хоча і володіють великою швидкістю, страждають від численних серйозних недоліків:

- Занадто короткий період.
- Послідовні значення не є незалежними.
- Деякі біти є «менш випадковими», ніж інші.
- Нерівномірний одномірний розподіл.
- Зворотність.

РОЗДІЛ 3

Апарат тригонометричних сум

На початку цього розділу надамо визначення тригонометричної суми в загальному вигляді.

Сума вигляду $S\big(f(x)\big) = \sum_{x\in A} e^{2\pi i f(x)}$ називається тригонометричною, де $f(x)$ – дійснозначна функція на множині A, множина A – скінченна підмножина n-вимірного дійсного або комплексного простору.

Першим, хто став розглядати тригонометричні суми найпростішого вигляду, був Гаус; він досліджував важливі властивості суми, яка сьогодні носить його ім’я (сума Гауса):

$$S\left(\frac{ax^2}{P}\right) = \sum_{x=1}^{P} e^{2\pi i\frac{ax^2}{P}} \quad (3.1)$$

де $(a, P) = 1$

Гаус по суті був першим, хто показав цінність тригонометричних сум в контексті розв’язання задач з теорії чисел (наприклад, використовуючи властивості суми Гауса, він побудував одне з власних доведень квадратичного закону взаємності)

В подальшому тригонометричні суми, хоча й більш загального вигляду ніж суми Гауса, стали потужним інструментом розв’язання цілого ряду важливих питань теорії чисел. При цьому основною в розрізі таких сум стала проблема знаходження більш точної верхньої оцінки (тобто більш точна верхня границя їх модуля).

Для суми Гауса ця проблема була повністю розв’язана безпосередньо самим Гаусом. Він дав наступні точні значення для модуля цієї суми:

$$\left|S\left(\frac{ax^2}{P}\right)\right| = \sqrt{P}, \text{якщо } P \equiv 1\ (mod\ 2)$$

$$\left|S\left(\frac{ax^2}{P}\right)\right| = P, \text{якщо } P \equiv 2\ (mod\ 4)$$

$$\left|S\left(\frac{ax^2}{P}\right)\right| = \sqrt{2P}, \text{якщо } P \equiv 0\ (mod\ 4)$$

Ідея отримання даних виразів наступна: для прикладу розглянемо випадок $P \equiv 1\ (mod\ 2)$. Тоді

$$\left|S\left(\frac{ax^2}{P}\right)\right|^2 = \sum_{y=1}^{P}\sum_{x=1}^{P} e^{2\pi i\frac{a(y^2-x^2)}{P}} = \sum_{h=0}^{P-1} S_h$$

за умови що $y \equiv x + h\ (mod\ P)$

Звідси S_h може бути представлена у вигляді

$$S_h = \sum_{x=1}^{P} e^{2\pi i\frac{a(2xh+h^2)}{P}}$$

При $h = 0$, $S_h = P$, а при $h > 0$ $S_h = 0$. Тому

$$\left|S\left(\frac{ax^2}{P}\right)\right|^2 = P \ \rightarrow\ \left|S\left(\frac{ax^2}{P}\right)\right| = \sqrt{P}$$

Сума Гауса є окремим випадком більш загальної, так званої раціональної тригонометричної суми $S\left(\frac{\alpha(x)}{P}\right)$, де $\alpha(x) = a_1x + \cdots + a_nx^n$ – многочлен степені $n > 1$ з умовою $(a_1, \dots, a_n, P) = 1$

Для тригонометричної суми даного вигляду, вичерпну оцінку надав Вейль, довівши що

$$\left|S\left(\frac{\alpha(x)}{P}\right)\right| < n\sqrt{P} \quad (3.2)$$

Оцінка Вейля в сенсі порядку зростання зі зростанням P, при фіксованому n, є найкращою – можна вказати необмежене число випадків, коли модуль суми буде не менше ніж $\sqrt{P}$.

Найкращу оцінку суми $S\left(\frac{\alpha(x)}{P}\right)$ в загальному вигляді встановив Хуа. Він довів нерівність $\left|S\left(\frac{\alpha(x)}{P}\right)\right| \leq c(n)P^{1-\frac{1}{n}}$

Ця нерівність є особливою цікавою тим, що при фіксованому n, в сенсі зростання порядку правої частини зі зростанням P, дана нерівність не може бути замінена істотно кращою. Дана твердження випливає з існування при будь-якому простому p з умови $(n,p) = 1$ сум вигляду $S\left(\frac{ax^n}{p^n}\right)$, де $(a,p) = 1$ кожна з яких дорівнює $P^{1-\frac{1}{n}}$ $(P = p^n)$

Дійсно, будемо вважати, що $x = zp^{n-1} + y$. Тоді маємо

$$S\left(\frac{ax^n}{p^n}\right) = \sum_{y=1}^{p^{n-1}} \sum_{z=0}^{p-1} e^{2\pi i \frac{a(y^n + ny^{n-1}p^{n-1}z)}{p^n}} = \sum_{y=1}^{p^{n-1}} S_y$$

Але $S_y = p$, якщо $y \vdots p$, а в іншому випадку $S_y = 0$, тому $S\left(\frac{ax^n}{p^n}\right) = p^{n-2}p = p^{n-1} = P^{1-\frac{1}{n}}$

Раціональна тригонометрична сума входить як окремий випадок до ще більш загального класу сум вигляду

$$T = T(a_1, \dots, a_n) = \sum_{0<x\leq P} e^{2\pi i f(x)}, \text{де } f(x) = a_1 x + \cdots a_n x^n, a_1, \dots, a_n \in R$$

Перший загальний метод знаходження нетривіальних оцінок сум такого вигляду дав Вейль тому даним сумам присвоєна назва суми Вейля.

Ідея методу Вейля полягає в наступному. Вона заснована на виразі $(y = x + h)$:

$$|T|^2 = \sum_{y=1}^{P}\sum_{x=1}^{P} e^{2\pi i\left(f(y)-f(x)\right)} = \sum_{h=1-P}^{P-1} S_h, \text{ де}$$

$$S_h = \sum_{\max(1,1-h)\le x\le \min\,(P,P-h)} e^{2\pi i\left(f(x+h)-f(x)\right)}$$

Як ми бачимо, $|T|^2$ заміняється доданками вигляду S_h у кількості $< 2P$, при чому сума S_h аналогічна сумі T, проте є більш простою. Дійсно, число доданків суми S_h не перевищує P, а в показнику кожного доданку замість $f(x)$ стоїть різниця $f(x+h)-f(x)$, що дорівнює 0 при $h=0$, а в іншому випадку є многочленом степені $n-1$.

Оцінка суми T, що отримана за допомогою матоду Вейля може бути сформульована у вигляді наступної теореми:

Нехай $a_n = \frac{a}{q} + \frac{\theta t}{q^2}$, де $(a,q) = 1, 0 < q \le P^n, 1 \le |t| \le q$, θ – дійсне число, модуль якого не перевищує 1

Тоді при деякому $\mathrm{c}(\mathrm{n},\varepsilon) \le 1$ має місце нерівність:

$$|T| \le \mathrm{c}(\mathrm{n},\varepsilon)P^{1+\varepsilon}(P^{-1} + tq^{-1} + tP^{1-n} + qP^{-n})^k, lt\ k = \frac{1}{2^{n-1}}$$

Суттєвий недолік даної оцінки полягає швидка втрата точності зі зростанням n. Права частина нерівності значно більше степені P^{1-k}, показник якої, зі зростанням n досить швидко наближається до одиниці, через те що k, яка є величиною порядку 2^{-n} відносно n, досить швидко наближається до нуля.

Тим не менш, дана оцінка зіграла неабияку роль в розвитку теорії чисел: вона дозволила дати перші, хоча й не найкращі рішення певного ряду важливих задач в цьому розділі математики.

Одною з таких задач є задача розподілення дробових частин значень многочлену $Q(x) = a_1 x + \cdots + a_n x^n$. Її рішення було отримано в наступному вигляді:

Нехай $a_n = \frac{a}{q} + \frac{\theta}{q^2}, (a,q) = 1, 0 < q \leq P^n,$

і нехай σ – будь-яке число, що має властивість $0 < \sigma \leq 1$. Тоді представляючи число $D(\sigma)$ чисел ряду $1, \dots, P$ з умовою $0 \leq \{Q(x)\} < \sigma$ у вигляді $D(\sigma) = P(\sigma) + + \lambda(\sigma)$

для числа $\lambda(\sigma)$ маємо нерівність вигляду

$$|\lambda(\sigma)| \leq \mathrm{c(n,\varepsilon)} P^{1+\varepsilon}(P^{-1} + q^{-1} + qP^{-n})^k, \text{де } k = \frac{1}{2^{n-1}}$$

Іншою задачею, в якій суттєво допомогла оцінка, отримана за допомогою методою Вейля, стала задача Варинга. Варинг у 1770 році стверджував, що при кожному цілому $n > 1$, існує таке $r = r(n)$, що будь-яке ціле додатнє число N може бути представлене у вигляді $N = x_1^n + \dots + x_r^n$ з цілими невід'ємними коефіцієнтами $x_1, \dots, x_r$.

Дана задача була вирішена Гільбертом у 1909 році, проте Харді та Літлвуд в 1919 році розробили новий метод вирішення задачі Воринга, який є непорівняно більш загальним та точним, ніж метод Гільберта.

Зокрема, Харді та Літлвуд розглянули функцію $G(n)$, що являє собою найменше значення r при якому всі цілі N, представляються у вигляді, запропонованим Варингом. Для цієї функції вони вивели нерівності

$$n < G(n) \leq n2^{n-1}h, \text{де } \lim_{n\to\infty} h = 1$$

Найважливішим було те, що Харді та Літлвуд при $r > 2^{n-1}(n-2) + 5$ для числа $I(N)$ представлень числа N у вигляді, запропонованим Варингом, знайшли асимптотичну формулу виду

$$I(N) = \frac{\left(\Gamma(1+\nu)\right)^n}{\Gamma(r\nu)} N^{r\nu-1}\omega + O(N^{r\nu-1-c(n,r)}) \quad (3.3)$$

де ω – деякий «особливий ряд». сума якого, як воно довели згодом, не перевищує деяке число $c_1(n,r)$.

В наступному схема доведення Харді та Літлвуда була замінена близькою за ідеєю, але більш простою схемою Виноградова. При цьому був досліджений ряд адитивних задач, котрим можна дати «узагальнення задачі Варинга». Серед таких задач, зокрема, виявилася і сформульована Гільбертом задача в 1900 році задача про розв'язність системи

$$\begin{cases} x_1 + \cdots + x_r = N_1 \\ \cdots \\ x_1^n + \cdots + x_r^n = N_n \end{cases}$$

в цілих невід'ємних значеннях $x_1, \ldots, x_r$ (при достатньо великому $r = r(n)$ і при наявності доволі жорстких природних нерівностей, які обмежують $N_1, \ldots, N_n$). Асимптотичну формулу для кількості розв'язків цієї системи при $r > 2^{2n} n! \, (n+1)^3$ вперше знайшов Марджанішвілі в 1937 році (існування розв'язків при достатньо великому $r = r(n)$ раніше цього, в 1921 році, довів Камке за допомогою узагальнення методу Гільберта в задачі Варинга).

Оцінка для суми T, а також знайдені Корпутом (за допомогою видозміненого методу Вейля) оцінки для узагальненої суми T, на випадок, коли функція $f(x)$, не будучи многочленом степені n, в деякому відношенні близька до такого многочлену, отримали застосування в інших питаннях теорії чисел. Наприклад, дані оцінки були використані в теорії розподілу простих чисел: в питанні про потрапляння простих чисел малої довжини (поглиблене доведеного Чебишевим постулата Бертрана про те, що при $N > 1$ між N і $2N$ завжди знайдеться просте число) і в задачі про число $\pi(N)$ простих чисел, що не перевищують N.

В 1934 році Виноградов розробив новий метод в аналітичній теорії чисел. В розробці та застосуванні методу Виноградова брали участь Ван дер Корпут, Чудаков, Хуа та інші. Важливий p-адичний варіант цього методу, удосконалений Карацубою, дав Линник.

Важливими теоремами, що отримані за допомогою методу Виноградова, є теореми, що дають при достатньо великому цілому b, що більше за

$\frac{1}{4}n(n+1)$, оцінку інтеграла $I = \int_0^1 \dots \int_0^1 |T|^{2b} da_1 \dots da_n$

Одна з теорем дає таку оцінку для значень b деякого загального вигляду, а інша теорема – для деякого окремого b, при чому, як і очікувалось друга теорема є більш простою:

Нехай n – фіксоване, $n \geq 12, b = 2r_1, r_1 = [n^2(2\ln n + \ln\ln n + 2.6)]$

Тоді маємо $I \ll P^{2b-\left(\frac{n(n+1)}{2}\right)}$

Наслідком першої з цих теорем (для узагальненого випадку) є нові оцінки суми Вейля. При отриманні нових оцінок нема потреби використовувати метод Виноградова в точках $(a_1, \dots, a_n)$, що належать малим областям, які обмежують точки $\left(\frac{a_1}{q_1}, \dots, \frac{a_n}{q_n}\right)$ маючи координатами нескоротні дроби зі спільним знаменником, що не перевищує P^ν, так як в цих точках сума T може бути оцінена за допомогою простіших методів. Для точок області H, що залишаються після виділення з області n-мірного простору вказаних малих областей, метод Виноградова дає оцінку виду

$|T| \leq \mathrm{c(n)}P^{1-\tau}$, де $\tau = \frac{1}{8n^2(\ln n + 0.5\ln\ln n + 1.3)}$ (3.4)

Порівнюючи цю оцінку з недосяжною для методу Вейля оцінкою $|T| \leq P^{1-k}$, де $k = \frac{1}{2^{n-1}}$ ми бачимо, що при зростанні n перша з них хоча й погіршується (в сенсі порядку зростання зі зростанням P), проте стається це набагато повільніше, ніж друга (тому що τ прямує до нуля набагато повільніше ніж k).

Проте, варто відмітити, що метод Виноградова починає давати кращі оцінки суми T ніж метод Вейля починаючи лише приблизно з $n = 12$. Зрозуміло, що нові оцінки сум Вейля за допомогою метода Виноградова.

По перше це торкнулось задачі розподілу дробових частин значень многочлену. Для залишкового члену ряду $\lambda(\sigma)$ в області H була отримана оцінка виду $|\lambda(\sigma)| \leq \mathrm{c(n)}P^{1-\tau}$, де $\tau = \frac{1}{8n^2(\ln n + 0.5 \ln\ln n + 1.4)}$

яка краще попередньої приблизно в тому ж обсязі, в якій оцінки сум Вейля за допомогою методу Виноградова були краще за попередні.

В задачі Варингу за допомогою нового методу Виноградова була отримана наступна нерівність для функції $G(n)$

$G(n) < 2n \ln n\,(1 + \delta_n')$, де $\lim\limits_{n\to\infty} \delta_n' = 0$.

А за допомогою сформульованої теореми про оцінку інтеграла I і отриманих Виноградовим оцінок сум Вейля доводиться що асимптотична формула Харді і Літлвуда справедлива за умови якщо

$r > 4n^2 \ln n\,(1 + \delta_n'')$, де $\lim\limits_{n\to\infty} \delta_n'' = 0$.

Також за даної умови за допомогою метода Виноградова виводиться асимптотична формула для кількості рішень для задачі Гільберта про розв'язність системи.

В теорії розподілу простих чисел в задачі про потрапляння простих чисел в інтервал малої довжини за допомогою методу Виноградова доведено існування простих чисел p в інтервалі $N \leq p \leq N + N^{\delta}$ при $\delta = \frac{3}{5}$. Таким чином ми побачили структуру розвитку апарату тригонометричних сум і приклади його застосування в конкретних задачах теорії чисел.

Розглянувши апарат тригонометричних сум, варто зазначити, що в нашій роботі він розглядається у компіляції з так званим s-мірним тестом на непередбачуваність. Даний тест дозволяє оцінити «якість» згенерованої послідовності псевдовипадкових чисел і дати відповідь на питання чи досить вона близька за своїми властивостями до послідовності випадкових чисел.

Говорячи загалом, даний тест являє собою набір процедур, заснованих на перевірці однорідності розподіли шаблонів заданих довжин. Цей тест перевіряє частоту всіх можливих m-бітових шаблонів, що перекриваються, протягом усієї послідовності. Його мета — оцінити, чи відповідає частота появи $2m$ можливих m-бітових шаблонів, що перекриваються, приблизно такій, як можна було б очікувати у випадковій послідовності. У випадковій послідовності розподіл рівномірний, тобто кожен m-бітовий шаблон має рівну ймовірність появи, як і будь-який інший m-бітовий шаблон. Зокрема, для $i_1 \dots i_m$ проходячи через набір усіх 2^m можливих $(0,1)$ векторів довжини m, нехай $\nu_{i_1 \dots i_m}$позначає частоту шаблону $i_1 \dots i_m$ у «зацикленому» рядку бітів $(\varepsilon_1, \dots, \varepsilon_n, \varepsilon_1, \dots, \varepsilon_{m-1})$.

Нехай

$$\psi_m^2 = \frac{2^m}{n} \sum_{i_1 \dots i_m} \left(\nu_{i_1 \dots i_m} - \frac{n}{2^m} \right)^2 = \frac{2^m}{n} \sum_{i_1 \dots i_m} {\nu_{i_1 \dots i_m}}^2 - n.$$

Тут варто зазначити, що досить розповсюдженою помилкою є припущення про те, що ψ_m^2 має розподіл хі-квадрат. Але насправді, частоти шаблонів $\nu_{i_1 \dots i_m}$ не є незалежними величинами.

Відповідні загальні статистичні величини для перевірки випадковості виглядають наступним чином $\nabla\psi_m^2 = \psi_m^2 - \psi_{m-1}^2$ та $\nabla^2\psi_m^2 = \psi_m^2 - 2\psi_{m-1}^2 + {} + \psi_{m-2}^2$ $(\psi_0^2 = \psi_{-1}^2 = 0)$.

Виходячи з цього, $\nabla\psi_m^2$ має розподіл хі-квадрат із 2^{m-1} ступенями свободи і $\nabla^2\psi_m^2$ має розподіл хі-квадрат із 2^{m-2}. Таким чином, для малих значень m, $\mathrm{m\,m} < \lfloor \log_2 n \rfloor - 2$, можна знайти відповідні $2m$ P-значення за стандартними формулами $P_1 = \gamma(2^{m-2}, \nabla\psi_m^2)$ та $P_2 = \gamma(2^{m-3}, \nabla^2\psi_m^2)$ відповідно.

До речі, доведення того, що $\nabla\psi_m^2$ збігається до хі розподілу було дано в 1953 році.

Опишемо покроково схему даного тесту:

Послідовність (m, n), де:

m – довжина в бітах кожного блоку.

n – довжина бітового рядка в бітах.

Варто зазначити, що рекомендується обирати такі значення, що $m < \lfloor \log_2 n \rfloor - 2$

Додаткові вхідні дані, які використовуються функцією, але надаються тестовим кодом:

ε - послідовність бітів, згенерована генератором псевдовипадкових чисел, що тестується; $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$.

$\nabla\psi_m^2$ та $\nabla^2\psi_m^2$ – міра вимірювання того, наскільки добре збігаються спостережувані частоти m-бітових шаблонів із очікуваними частотами m-бітових шаблонів.

1) Сформувати розширену послідовність ε': розширити послідовність, додавши перші $m-1$ бітів до кінця послідовності для різних значень n.

2) Визначити частоту всіх можливих m-бітових блоків, що перекриваються, усі можливі перекриття $(m-1)$-бітових блоків та всі можливі $(m-2)$-бітові блоки, що перекриваються. Нехай $\nu_{i_1 \ldots i_m}$ позначає частоту m-бітового шаблону $i_1 \ldots i_m$; нехай $\nu_{i_1 \ldots i_{m-1}}$ позначає частоту $(m-1)$-бітового шаблону $i_1 \ldots i_{m-1}$; і нехай $\nu_{i_1 \ldots i_{m-2}}$позначає частоту $(m-2)$-бітового шаблону $i_1 \ldots i_{m-2}$.

3) Порахувати

$$\psi_m^2 = \frac{2^m}{n} \sum_{i_1 \ldots i_m} \left(\nu_{i_1 \ldots i_m} - \frac{n}{2^m}\right)^2 = \frac{2^m}{n} \sum_{i_1 \ldots i_m} {\nu_{i_1 \ldots i_m}}^2 - n$$

Аналогічно для ψ_{m-1}^2та ψ_{m-2}^2.

4) Порахувати

$$\nabla\psi_m^2 = \psi_m^2 - \psi_{m-1}^2 \text{ та } \nabla^2\psi_m^2 = \psi_m^2 - 2\psi_{m-1}^2 + \psi_{m-2}^2$$

5) Порахувати P_1та P_2:

$$P_1 = \gamma(2^{m-2}, \nabla\psi_m^2), P_2 = \gamma(2^{m-3}, \nabla^2\psi_m^2)$$

Таким чином, якщо пораховані $P_1, P_2 < \frac{1}{100}$ то ми робимо висновок, що згенерована послідовність псевдовипадкових чисел за своїми властивостями не нагадують випадкову.

Приклад використання даного тесту на реальному прикладі послідовності псевдовипадкових чисел можна знайти в [6].

РОЗДІЛ 4

Функція дискріпансії

Загалом розглянувши наразі послідовності псевдовипадкових чисел та апарат тригонометричних сум хочеться отримати зв'язок між цими двома поняттями. Дане питання вирішується шляхом оцінки, так званої функції дискріпансії/дискріпантної функції, якій загалом і буде присвячено даний розділ.

Наразі варто зазначити що послідовність псевдовипадкових чисел має мати ще одну важливу характеристику аби бути придатною для використання наприклад у криптографії. Дана характеристика носить назву рівномірної розподіленості/рівнорозподіленості. Надамо визначення рівномірно розподіленої послідовності

Послідовність дійсних чисел $(k_1, k_2, k_3 \dots)$ називається рівномірно розподіленою на невиродженому відрізку [a, b] якщо, для будь-якого підвідрізка $[c, d]$ відрізку $[a, b]$ маємо

$$\lim_{n\to\infty} \frac{|\{k_1,\dots,k_n\}\cap[c,d]|}{n} = \frac{d-c}{b-a} \quad (4.1)$$

де $|\{k_1, \dots, k_n\}\cap[c, d]| = \varphi(n)$ - позначає кількість елементів з перших n елементів послідовності, які знаходяться між c і d.

Наприклад, розглянемо послідовність, яка рівномірно розподілена на відрізку $[0, 3]$. Оскільки підвідрізок $[1, 2]$ займає $1/3$ загальної довжини відрізку $[0, 3]$, у міру збільшення кількості членів у послідовності частка перших n членів, які потрапляють між 1 і 2, повинна наближатися до $1/3$. Іншими словами, кожен член послідовності з однаковою ймовірністю потрапить у будь-яке місце на відрізку $[0, 3]$. Однак це не означає, що послідовність є набором випадкових

величин; скоріше, це конкретна, заздалегідь визначена послідовність дійсних чисел.

Використовуючи визначення рівномірно розподіленої послідовності ми можемо дати визначення дискріпансії для даної послідовності.

Тож для послідовності $(k_1, k_2, k_3 \dots)$ відносно відрізка $[a, b]$ дискріпансія визначається наступним чином

$$D_N = \sup_{a \le c \le d \le b} \left| \frac{|\{k_1, \dots, k_n\} \cap [c,d]|}{n} - \frac{d-c}{b-a} \right| \quad (4.2)$$

Таким чином ми бачимо, що послідовність рівномірно розподілена якщо дискріпансія прямує до нуля, коли N прямує до нескінченності.

Незважаючи на свою назву, рівномірний розподіл послідовності є відносно слабким критерієм для опису послідовності, яка заповнює сегмент, не залишаючи прогалин. Наприклад, значення, отримані з випадкової змінної, рівномірно розподіленої по відрізку, будуть рівномірно розподілені в цьому відрізку, але вони можуть залишати значні прогалини. Це контрастує з послідовністю, яка спочатку перераховує кратні невеликого значення ε в межах відрізку, а потім поступово розглядає менші значення ε у ретельно вибраний спосіб.

Для визначення того, чи є послідовність рівномірно розподіленою користуються так званими критеріями для рівномірної розподіленості. Нагадаємо, що якщо f – функція, яка інтегрована за Ріманом на відрізку $[a, b]$, його інтеграл є межею сум Рімана. Таким чином, якщо послідовність рівнорозподілена в $[a, b]$, очікується, що цю послідовність можна використовувати для обчислення інтеграла функції, інтегрованої за Ріманом. Це призводить до наступного критерію рівнорозподіленої послідовності, який має назву інтегральний критерій Рімана:

Нехай $(k_1, k_2, k_3 \dots)$ послідовність, яка міститься у відрізку $[a, b]$. Тоді наступні 2 умови еквівалентні:

1) Послідовність рівномірно розподілена.

2) Для будь-якої функції f, що інтегрована за Ріманом, $f\colon [a, b] \to \mathbb{C}$ має місце наступна границя:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(k_n) = \frac{1}{b-a} \int_a^b f(x)\, dx$$

Цей критерій дає початок концепції інтегрування Монте-Карло, де інтеграли оцінюються шляхом вибірки функції з використанням послідовності випадкових величин, які рівномірно розподілені в межах відрізку.

Після цього виникає питання стосовно узагальнення даного критерію, проте інтегральний критерій Рімана не може бути поширений на більш широкий клас функцій, окрім інтегрованих за Ріманом. Наприклад, при розгляді інтеграла Лебега та взяття f з L^1, критерій не виконується. До прикладу, якщо f є індикаторною функцією рівнорозподіленої послідовності, ліва частина критерію завжди дорівнює 1, тоді як права частина дорівнює 0, оскільки послідовність є зліченною, тобто f майже всюди дорівнює нулю. До речі цікаво, що насправді існує теорема де Брейна–Поста забезпечує протилежність критерію вище: якщо f – функція, для якої інтегральний критерій Рімана виконується для всіх рівнорозподілених послідовностей у $[a, b]$, тоді f інтегровна за Ріманом на відрізку $[a, b]$.

Для того аби детальніше розглянути поняття дискрипансії та тісно пов’язаних з ним понять необхідно ввести ще одне поняття, яке носить назву послідовність, що рівномірно розподілена за модулем 1.

Послідовність дійсних чисел $(s_1, s_2, s_3, \dots)$ називаються рівномірно розподіленою за модулем 1, якщо послідовність дробових частин чисел s_n, що

позначається як (s_n) рівномірно розподілена на відрізку $[0,1]$. Наведемо декілька прикладів таких послідовностей:

- послідовність усіх кратних ірраціонального числа a рівномірно розподілена за модулем 1 (даний факт є наслідком з інтегрального критерію Рімана). Більш загально, якщо p – многочлен із принаймні одним ірраціональним коефіцієнтом, відмінним від постійного доданка, то послідовність $p(n)$ рівномірно розподілена за модулем 1;

- послідовність усіх кратних ірраціонального а на послідовні прості числа, $2a, 3a, 5a, 7a, 11a, \ldots$ рівнорозподілена за модулем 1.

Для рівномірно розподілених послідовностей за модулем 1 також існує критерій що дозволяє зрозуміти, чи є дана послідовність ріваномірно розподіленою за модулем 1. Даний критерій носить назву критерій Вейля і він стверджує наступне:

$$s_n \text{ є рівнорозподіленою за модулем } 1 \Leftrightarrow \forall k \in \mathbb{Z}\colon \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i k s_j} = 0$$

Даний критерії є надважливим в контексті вивчення послідовностей псевдовипадкових чисел, тому що він явно демонструє нам використання тригонометричної суми в контексті виявлення важливої для послідовності псевдовипадкових чисел характеристики. Враховуючи важливість даного доведення наведемo його схематичне доведення

$(\rightarrow)$

Якщо s_n є рівнорозподіленою за модулем 1, то ми можемо використати інтегральний критерій Рімана для функції $f(x) = e^{2\pi i k x}$, яка має нульовий інтеграл на відрізку $[0,1]$.

$(\leftarrow)$

Нехай справджується критерій Вейля. Тоді інтегральний критерій Рімана виконується для функцій f, як зазначено в 1 пункті доведення. Через лінійність інтегрального критерія Рімана він виконується також для тригонометричних ммногочленів. За теоремою Вейєрштрасса-Стоуна та аргументом наближення це поширюється на будь-яку неперервну функцію f.

Нарешті, нехай f є індикаторною функцією відрізку. Зверху і знизу f можна затиснути двома неперервними функціями на відрізку, інтеграли яких відрізняються на довільне ε. Даний результат можна поширити результат на будь-яку індикаторну функцію f, тим самим довівши рівномірний розподіл послідовності за модулем 1 даної послідовності.

Критерій Вейля природним чином узагальнюється віщі вимірності, припускаючи природнє узагальнення поняття рівнорозподіленості за модулем 1:

Послідовність векторів $v_n \subset R^k$ рівнорозподілена за модулем 1

$$\Leftrightarrow \forall \text{ "ненульового вектору" } l \in Z^k \colon \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i l v_j} = 0$$

Розглянемо застосування критерію Вейля в контексті тригонометричних сум. Для цього доведемо наступну теорему:

Послідовність кратних: $(0, a, 2a, 3a, \dots)$ для деякого $a \in \mathbb{R}$ рівнорозподілена за модулем 1 $\Leftrightarrow a \in \mathbb{R}/\mathbb{Q}$

$(\leftarrow)$

Нехай а ірраціональне число. Перепишемо нашу послідовність у вигляді $b_j = ja$, де j = 0,1,2… . Нехай $l \neq 0$ і $l \in \mathbb{Z}$. Так як $a \in \mathbb{R}/\mathbb{Q} \Longrightarrow la \notin \mathbb{Z} \Longrightarrow e^{2\pi i l a} \neq 1$. Тоді маємо

$$\left|\sum_{j=0}^{n-1} e^{2\pi i l j a}\right| = \left|\sum_{j=0}^{n-1} e^{(2\pi i l a)^j}\right| = \left|\frac{1 - e^{2\pi i l n a}}{1 - e^{2\pi i l a}}\right| \leq \frac{2}{|1 - e^{2\pi i l a}|}$$

Як ми бачимо, верхня межа не залежить від n. Тоді після ділення на n та умови, що n прямує до нескінченності, ліва частина нерівності прямує до нуля і виконується критерій Вейля.

$(\rightarrow)$

Припустимо, що $a \in \mathbb{Q}$. Тоді послідовність не є рівномірно розподіленою за модулем 1, тому що є тільки скінченна кількість дробових частин чисел b_j.

Для більш строгих критеріїв і методів побудови послідовностей, які розподілені більш рівномірно, необхідно розглядати послідовності з низькою дискріпансією.

Послідовність з низькою дискріпансією це послідовність з властивістю що при будь-яких значеннях N, її підпослідовність $k_1, \ldots, k_N$має низьку дискріпансію. Загалом, дискріпансія послідовності вважається низькою, якщо частка точок у послідовності, які потрапляють у даний набір B точно відповідає мірі B, як і очікувалося в середньому для рівномірно розподіленої послідовності (хоча не для конкретних прикладів). Різні визначення дискріпансії різняться з точки зору вибору B (наприклад, гіперсфери, гіперкуби тощо), а також метод, який використовується для обчислення та комбінування дискріпансії для кожного набору B (зазвичай шляхом нормалізації та вибору найгіршого значення).

Послідовності з низькою дискріпансією часто називають квазівипадковими послідовностями, оскільки вони зазвичай використовуються як замінники рівномірно розподілених випадкових чисел. Термін «квазі» підкреслює, що ці послідовності не є ані справді випадковими, ані псевдовипадковими, але вони демонструють певні характеристики випадкових змінних. У конкретних застосуваннях, таких як метод Квазі-Монте-Карло[12], їх менша дискріпансія загалом забезпечує значну перевагу. Квазівипадкові числа мають перевагу перед чисто випадковими числами, оскільки вони охоплюють область інтересу ефективніше та рівномірніше. Два помітних застосування квазівипадкових чисел полягають у визначенні характеристичної функції щільності ймовірності та

обчисленні похідної детермінованої функції з мінімальним шумом. Квазівипадкові числа дозволяють швидко і дуже точно обчислювати моменти вищого порядку.

Застосування, які не потребують сортування, включають обчислення середнього значення, стандартного відхилення, асиметрії статистичного розподілу, а також знаходження інтегралу, глобальних максимумів і мінімумів складних детермінованих функцій. Квазівипадкові числа також можуть служити відправними точками для детермінованих алгоритмів, які працюють локально, наприклад для методу Ньютона–Рафсона.

Крім того, квазівипадкові числа можна інтегрувати з алгоритмами пошуку. У цьому контексті вони можуть допомогти визначити моду, медіану, довірчі інтервали та кумулятивний розподіл статистичного розподілу, а також ідентифікувати всі локальні мінімуми та рішення детермінованих функцій.

Послідовності з низькою розбіжністю активно застосовуються в чисельному інтегруванні, що цікаво з точки зору методі Монте-Карло. Різні методи числового інтегрування можна описати як методи наближення інтеграла функції f на деякому відрізку (до прикладу $[0,1]$), як середнє функції визначене на множині $\{x_1, \dots, x_N\}$ на цьому відрізку: $\int_0^1 f(u)du \approx \frac{1}{N}\sum_{i=1}^{N} f(x_i)$

Тут, в залежності від того як обирають точки, даний метод має різні назви: якщо точки розподілені випадково або псевдовипадково, то це метод Монте-Карло, а якщо точки обрані з елементів послідовності з низькою дискріпансією, то це квазі-метод Монте-Карло. Важливим результатом в цьому контексті є нерівність Главки-Коксми яка показує, що помилка даного методу може бути обмежена добутком лише двох членів, один з яких залежить від f, а інший – дискріпансія множини $\{x_1, \dots, x_N\}$.

Тож наведемо визначення дискріпансії за допомогою нотації Нідеррайтера [18]:

Дискріпансія множини $X = \{x_1, \dots, x_N\}$ визначається як

$$D_N(X) = \sup_{B \in J} \left| \frac{A(B;X)}{N} - \lambda_s(B) \right| \quad (4.3)$$

де λ_s- s-мірна міра Лебега, $A(B;X)$ кількість точок X що потрапляють в B та J це множина s мірних полуінтервалів форми

$$\prod_{i=1}^{s} [a_i, b_i] = \{x \in R^s : a_i \leq x_i \leq b_i\} \quad (4.4)$$

де $0 \leq a_i < b_i \leq 1$.

Також ще одне необхідне нам визначення носить назву дискріпансія з зірочкою і позначається $D_N^*(X)$. Загалом дане поняття визначається ідентичним до минулого визначення чином, лише з тою відмінністю, що супремум береться по множині J^* полуінтервалів виду $\prod_{i=1}^{s} [0, u_i]$, де u_i знаходиться в полуінтервалі $[0,1]$.

Звичайна дискріпансія та дискріпансія із зірочкою пов'язаються одна з одною за допомогою наступної нерівності $D_N^* \leq D_N \leq 2^s D_N^*$

У цих визначеннях дискріпансія стосується максимального відхилення щільності точок від рівномірного розподілу. Однак інші вимірювання помилок також є доречними, що призводить до альтернативних визначень і варіацій дискріпансії. Наприклад, L^2-дискріпансія часто використовується для оцінки якості однорідних наборів точок. До речі оцінювати такий вид дискріпансії легше для достатньо великих N та s.

Часто, при будь-яких обчисленнях, важко знайти точне значення не виключенням є й функція дискріпансії великих наборів точок. Дану задачу

вирішує нерівність Турана-Ердьоша-Коксми, яка дає верхню межу функції дискріпансії.

Передує даній нерівності так звана нерівність Турана-Ердьоша. Ця нерівність обмежує відстань між імовірнісною мірою на колі та мірою Лебега в термінах коефіцієнтів Фур'є. Це було доведено Паулем Ердешем і Палом Тураном у 1948 році. Наведемо формулювання нерівності Турана-Ердьоша:

Нехай μ імовірнісна міра на одиничному колі $\mathbb{R}/\mathbb{Z}$. Нерівність Турана-Ердьоша стверджує, що для будь-якого натурального n

$$\sup_A |\mu(A) - mes(A)| \leq C\left(\frac{1}{n} + \sum_{k=1}^{n} \frac{|\widehat{\mu(k)}|}{k}\right) \quad (4.5)$$

де супремум береться по всім дугам $A \subset \mathbb{R}/\mathbb{Z}$ одиничного кола, mes – міра Лебега, $\widehat{\mu(k)} = \int e^{2\pi i k\theta}\, d\mu(\theta)$ коефіцієнти ряду Фур'є μ, $C > 0$ – константа.

Нехай $s_1, s_2, \ldots \in \mathbb{R}$ рівнорозподілена послідовність за модулем 1. Тоді нерівність Турана-Ердьоша застосована до міри $\mu_m(S) = \frac{1}{m}\, \varphi_n[a, b]$ дає наступну верхню межу для дискріпансії

$$D(m) \leq C\left(\frac{1}{n} + \frac{1}{m}\sum_{k=1}^{n} \frac{1}{k} \left| \sum_{j=1}^{m} e^{2\pi i s_j k} \right|\right)$$

Дана нерівність справджується для довільних натуральних m, n та надає множинну форму для критерію Вейля про рівномірно розподілену послідовність за модулем 1. Багатовимірний варіант даної оцінки і називається нерівністю Турана-Ердьоша-Коксми. Вона формулюється наступним чином

Нехай $x_1, \ldots, x_N$ точки в $I^s = [0,1]^s$ і H – довільне натуральне число. Тоді

$$D_N^*(x_1, \dots, x_N) \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \sum_{0<||h||_\infty \leq H} \frac{1}{r(h)} \left|\frac{1}{N} \sum_{n=1}^{N} e^{2\pi i \langle h, x_n \rangle}\right|\right) \quad (4.6)$$

де $r(h) = \prod_{i=1}^{s} \max\{1, |h_i|\}$ для $h = (h_1, \dots, h_s) \in \mathbb{Z}^s$.

Таким чином, ми бачимо, що від оцінки функції дискріпансії зверху можна перейти до оцінки тригонометричних сум за допомогою нерівності Турана-Ердьоша Коксми.

Наведемо дві основні конструкції, які стосуються оцінки функції дискріпансії знизу.

1) Існує константа c_s, яка залежить тільки від розмірності s, така що

$D_N^*(x_1, \dots, x_N) \geq c_s \frac{(\ln N)^{s-1}}{N}$ для будь-якого скінченного набору точок $(x_1, \dots, x_N)$.

2) Існує константа c_s', яка залежить тільки від розмірності s, така що

$D_N^*(x_1, \dots, x_N) \geq c'_s \frac{(\ln N)^s}{N}$ для нескінченного числа N і для будь-якої нескінченної послідовності $x_1, \dots$

Насправді ці дві конструкції є еквівалентними. Вони були доведені Шмідтом для $s \leq 2$.

Для довільних розмірностей $s > 1$ Рот довів наступну нижню оцінку для функції дискріпансії: $D_N^*(x_1, \dots, x_N) \geq \frac{1}{2^{4s}} \frac{1}{((s-1)\ln 2)^{\frac{s-1}{2}}} \frac{\ln^{\frac{s-1}{2}} N}{N}$ для будь-якого скінченного набору точок $(x_1, \dots, x_N)$.

Йозеф Бек встановив подвійне логарифмічне покращення цього результату в трьох вимірах. Це було вдосконалено Д. Біликом і М. Т. Лейсі до степеня одного логарифма. Найбільш відома оцінка для $s > 2$ належить Д. Білику, М. Т. Лейсі

та А. Вагаршакяну. Для $(x_1, \dots, x_N)$ існує $t = 0$ таке що $D_N^*(x_1, \dots, x_N) \geq t \frac{\ln^{\frac{s-1}{2}+t} N}{N}$ для будь-якого скінченного набору точок $(x_1, \dots, x_N)$.

РОЗДІЛ 5

Інверсні конгруентні генератори другого порядку

Інверсні конгруентні генератори є одним з видів генераторів псевдовипадкових чисел. Найбільш відомі види інверсних генераторів визначаються за допомогою конгруентних рекурсій.

Нехай F_q – скінченне поле, що складається з q елементів і $a, b, y_0 \in F_q$. Покладемо

$$\bar{y} = \begin{cases} 0, \text{якщо } y = 0, \\ \text{мультиплікативно зворотній до } y \in F_q^*. \end{cases}$$

Тоді рекурсія вигляду $y_{n+1} = a\bar{y} + b$, n = 0, 1,… представляє інверсний конгруентний генератор над полем F_q.

Інверсні генератори визначаються не лише над скінченними полями, а й, наприклад, над кільцем Z_{p^m}.

Нехай p – просте число і $m > 1$ – натуральне число. Розглянемо рекурсію наступного вигляду

$$y_{n+1} \equiv a y_n^{-1} + b \ (mod\ p^m),\ a, b \in Z,\ \text{n} = 0, 1, \ldots \quad (5.1)$$

де y_n^{-1}- мультиплікативно зворотній за модулем p^mдля y_n, якщо $(y_n, p) = 1$. Параметри a, b, y_0 називаються множником, зсувом та початковим значенням відповідно. Даний вид генератора називається інверсним генератором з постійним зсувом.

В роботах [9,10,19] було доведено, інверсний генератор з постійним зсувом, генерує послідовність $\{x_n\}, x_n = \frac{y_n}{p^m}$, яка проходить s-мірний тест на рівномірну

розподіленість та статистичну незалежність для $s = 1,2,3,4$ якщо умови на параметри a, b, y_0 виконуються.

Варто зазначити, що даний генератор є надзвичайно корисним в контексті квазі-методів Монте-Карло. Якщо говорити про криптографічні застосування, то тепер початкове значення y_0 та константи a, b вважаються секретними ключами, а потоковий шифр це вихідні дані генератора. Проте загалом послідовності псевдовипадкових чисел, що згенеровані інверсним конгруентним генератором з постійним зсувом, не можна використовувати в криптографії, оскільки a і b можуть бути обчислені лише з трьох послідовних елементів за умови, що відомий p^m.

В роботі [23] було надано два узагальнення для інверсного генератора з постійним зсувом. Перше узагальнення стосується рекурентного відношення

$$y_{n+1} \equiv a y_n^{-1} + b + cF(n+1)y_0 \ (mod\ p^m)$$

за умов $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 \ (mod\ p)$, $F(n)$ – многочлен над $Z[n]$.

Даний вид генератора носить назву інверсний конгруентний генератор із змінним зсувом $b + cF(n+1)y_0$. Обчислювальна складність генератора із змінним зсувом така ж сама, що й для генератора з постійним зсувом, але реконструкція параметрів a, b, c, y_0, n і многочлена $F(n)$ є важкою задачею, навіть якщо кілька послідовних значень $y_n, y_{n+1}, \dots, y_{n+N}$ буде знайдено(наприклад, відновлення навіть тричленного многочлена $F(n)$ великого невідомого степеня є дуже важкою задачею, оскільки відновлення многочлена за його значеннями в k-точках неможлива, якщо його степінь більший за k). Таким чином генератор із змінним зсувом, на відміну від генератора з постійним зсувом, можна використовувати в криптографічних алгоритмах. зауважимо, що умови $(a, p) = (y_0, p) = 1$ та $b \equiv c \equiv 0 \ (mod\ p)$ гарантують, що рекурсія виробляє нескінченну послідовність $\{y_n\}$.

Друге узагальнення стосується конгруентної рекурсії вигляду

$$y_{n+1} \equiv ay_n^{-1} + b + cy_n \ (mod\ p^m), \text{ для } (a,p) = 1, b \equiv c \equiv 0 \ (mod\ p)$$

і має назву лінійний інверсний конгруентний генератор.

Для випадку $p = 2$ Като, Ву, Янагіхара досліджували лінійний інверсний конгруентний генератор [13,14].

Ці автори довели, що відповідна послідовність $\{x_n\}$ псевдовипадкових чисел має період $\tau = 2^{m-1}$ тоді і тільки тоді, коли $a + c \equiv 1 \ (mod\ 4)$ і $b \equiv 3 \ (mod\ 4)$.

В даному розділі ми будемо розглядати лінійно інверсний конгруентний генератор другого порядку, що задається за допомогою рекурсію виду

$$y_{n+1} \equiv a(y_{n-1}y_n)^{-1} + b \ (mod\ p^m), \ (5.2)$$

де $(a,p) = (y_0,p) = (y_1,p) = 1,\ b \equiv 0(mod\ p)$

В даному розділі, ми хочемо довести, що послідовність псевдовипадкових чисел, яка згенерована даним генератором проходить s-мірний тест на непередбачуваність та статистичну незалежність, а тому дані послідовності можуть бути використані в криптографії та/або в моделюваннях процесів.

В цьому розділі ми будемо використовувати наступні позначення: буква p позначає просте число, $p \geq 3$. Для $m \in N$ позначення Z_{p^m} (відповідно $Z_{p^m}^*$) позначає повну (відповідно скорочена) система лишків за модулем p^m. Для $z \in Z, (z,p) = 1$ нехай z^{-1} буде мультиплікативним оберненим до z за модулем p^m. Напишемо $\nu_p(A) = \alpha$, якщо $A \vdots p^\alpha$, але $\mathrm{p}^{\alpha+1} \nmid A$.

Для цілого числа t використовується скорочення $e_m(t) = e^{\frac{2\pi it}{p^m}}$.

Сформулюємо необхідні нам теореми у вигляді лем.

Лема 1. *Нехай* $p > 2$, $f(x)$ *та* $g(x)$ *– многочлени над* Z

$$f(x) = A_1x + A_2x^2 + \cdots, g(x) = B_1x + B_2x^2 + \cdots,$$

$\nu_p(A_j) = \lambda_j, \nu_p(B_j) = \mu_j, j = 1,2,3, \ldots$ *і, крім того,*

$$\alpha = \lambda_2 \leq \lambda_3 \leq \cdots, 0 = = \mu_1 < \mu_2 \leq \mu_3 \leq \cdots.$$

Тоді для $m \geq 2$ *справджується наступна оцінка*

$$\left| \sum_{x \in Z_{p^m}} e_m(f(x)) \right| \leq \begin{cases} 2p^{\frac{m+\alpha}{2}} & \text{якщо } \nu_p(A_1) \geq \alpha, \\ 0 & \text{якщо } \nu_p(A_1) \geq \alpha; \end{cases}$$

$$\left| \sum_{x \in Z_{p^m}^*} e_m(f(x) + g(x^{-1})) \right| \leq I(p^m)p^{\frac{m}{2}}$$

де $I(p^m)$ *– розв'язок конгруенції* $f'(y) \equiv g(y^{-1}) * y^{-1} \ (mod\ p^{m-m_0})$.

Для цілих чисел $q \geq 2$ і $d \geq 1$, нехай $C_q(d)$ – множина всіх ненульових точок решітки: $(h_1, \ldots, h_d) \in Z^d$ з $-\frac{q}{2} < h_j \leq \frac{q}{2}, 1 \leq j \leq d$. Ми визначаємо

$$r(h,q) = \begin{cases} q \sin\frac{\pi|h|}{q} & \text{якщо } h \in C_1(q) \\ 1 & \text{якщо } h = 0 \end{cases}$$

і

$$r(\mathfrak{h},q) = \prod_{j=1}^{d} r(h_j,q), \text{для } \mathfrak{h} = (h_1, \ldots, h_d) \in \mathrm{C}_d(q).$$

Лема 2 (Нідерайтер [9]). *Нехай* $N \geq 1$ і $q \geq 2$ *цілі числа. Для* N *довільних точок* $t_0, \ldots, t_{N-1} \in [0,1)^d$, *дискрепансія* $D(t_0, \ldots, t_{N-1})$ *задовільняє нерівності*

$$D_N(t_0, \ldots, t_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathfrak{h} \in C_d(q)} \frac{1}{r(\mathfrak{h},q)} \left| \sum_{n=0}^{N-1} e(\mathfrak{h} * t_n) \right|.$$

Лема 3. *Нехай* $\{\mathfrak{n}_k\}, \mathfrak{n}_k \in \{0, \dots, q-1\}^d$, *періодична послідовність з періодом* τ. *Тоді для дискрiпансії точок* $t_k = \frac{\mathfrak{n}_k}{q} \in [0,1)^d, k = 0, \dots, N-1; N \leq \tau$ *справджується наступна нерівність*

$$D_N(t_0, \dots, t_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathfrak{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{\tau}{2}, \frac{\tau}{2}\right]} r^{-1}(\mathfrak{h}, q)\, r^{-1}(h_0, \tau) * |\mathfrak{S}|$$

де

$$\mathfrak{S} := \sum_{k=0}^{\tau-1} e\left(\mathfrak{h} * t_k + \frac{k h_0}{\tau}\right).$$

Тепер отримаємо представлення y_n у вигляді раціональної функції від y_0. Позначимо $\nu_p(b) = \nu_0$. За допомогою прямих обчислень рекурсії, що відповідає за інверсний лінійний конгруентний генератор другого порядку, за модулем $p^{3\nu_0}$ отримаємо

$$y_2 = \frac{a + b y_0 y_1}{y_0 y_1}, \qquad y_3 = \frac{(a y_0 + ab + b^2 y_0 y_1)}{a y_0 y_1 + a b y_0 + a b^2}, \; y_4 = \frac{a y_0 y_1 + a b y_0 + a b^2}{a y_0 + ab + b^2 y_0 y_1}$$

Дані отримані співвідношення породжують припущення про те, що представлення y_n може бути визначено як

$$y_n = \frac{({A_0}^{(n)} + {A_1}^{(n)} y_0 + {A_2}^{(n)} y_0 y)}{{B_0}^{(n)} + {B_1}^{(n)} y_0 + {B_2}^{(n)} y_0 y_1}$$

де $A_j^{(n)}, B_j^{(n)}$ – многочлени із $Z[n]$. З даного припущення маємо

$$y_{n+2} = \\ = \frac{(a{B_0}^{(n)} + b{A_0}^{(n+1)}) + (a{B_1}^{(n)} + b{A_1}^{(n+1)}) y_0 + (a{B_2}^{(n)} + b{A_2}^{(n+1)}) y_0 y_1}{{A_0}^{(n+1)} + {A_1}^{(n+1)} y_0 + {A_2}^{(n+1)} y_0 y_1}$$

Тепер, за допомогою прямих обчислень за модулем $p^{3\nu_0}$ отримаємо

$$\begin{cases} A_0^{(3k-1)} \equiv a^{\mathrm{k}}, A^{1(3\mathrm{k}-1)} \equiv (k^2 - 3k + 3)a^{\mathrm{k}-1}b^2, \\ A_2^{(3k-1)} \equiv ka^{\mathrm{k}-1}b + 6(k-3)a^{\mathrm{k}-2}b^2; \\ \mathrm{B}_0{}^{(3k-1)} = \left(\frac{k(k-1)}{2}\right)a^{\mathrm{k}-1}b^2, \ B^{1(3\mathrm{k}-1)} = (3k-1) - 2(k-2)a^{\mathrm{k}-1}b, \\ B_2^{(3k-1)} = a^{\mathrm{k}-1} + 6a^{\mathrm{k}-2}b; \end{cases}$$

$$\begin{cases} A_0{}^{(3\mathrm{k})} \equiv ka^{\mathrm{k}}, \ A_1{}^{(3\mathrm{k})} \equiv 2a^{\mathrm{k}}, \ A_2{}^{(3\mathrm{k})} \equiv \left(\frac{k(k+1)}{2}\right)a^{\mathrm{k}-1}b^2; \\ B_0{}^{(3\mathrm{k})} \equiv a^{\mathrm{k}}, \ B_1{}^{(3\mathrm{k})} \equiv (k^2 - 3k + 3)a^{\mathrm{k}-1}b^2; \\ B_2{}^{(3\mathrm{k})} \equiv ka^{\mathrm{k}-1}b + 6(k-3)a^{\mathrm{k}-2}b^2. \end{cases}$$

$$\begin{cases} A_0^{(3k+1)} = a^{k+1} + ka^k b^2, A_1^{(3k+1)} = (k^2 - 3k + 3)a^k b^2 + 2a^k b \\ A_2^{(3k+1)} = ka^k b + 6(k-3)a^{k-1}b^2 \\ B_0^{(3k+1)} = ka^2 b, B_1^{(3k+1)} = 2a^k; B_2^{(3k+1)} = a^{k-1}b^2 \end{cases}$$

Справедливість даних формул встановлюється за допомогою методу математичної індукції, а остання випливає з рекурсії для генератора другого порядку. Інші доданки $A_j^n, j = 0,1,2; n = \{3k-1 \text{ або } 3k \text{ або } 3k+1\}$, які за модулем $p^{3\nu_0}$ дорівнюють 0, можуть бути представлені многочленами від Z[n](випливає з представлення y_{n+2}). Тож маємо

$$A_0^{(3k-1)} = a^k + p^{3\nu_0}F_0(k), \dots, B_2^{3k-1} = a^{k-1} + 6(k-3)a^{k-2}b^2 + p^{3\nu_0}G_2(k)$$

Відношення для y_n показує, що для будь-якого $k = 0,1,2, \dots$ числівник та знаменник мають доданок, яки взаємно простий з p. Помножимо чисельник і знаменник на мультиплікативний обернений $\mathrm{mod}\, p^m$ на відповідний доданок знаменника та застосуємо розширення $(1+pu)^{-1} = 1 - pu + p^2u^2 - \dots + +(-1)^{m-1}(pu)^{m-1}(\mathrm{mod}p^m)$, ми отримуємо представлення y_k у степеневому розкладі k з коефіцієнтами, які залежать лише від y_0, y_1 і $(a^{-1})^j, 0 \le j \le m$, де $a \cdot a^{-1} \equiv 1(\mathrm{mod}p^m)$.

Тож за модулем p^m маємо

$$y_{3k-1} = y_0^{-1}y_1^{-1} \cdot S_1 \cdot S_2,$$

де

$$S_1 = [a + (k^2 - 3k + 3)b^2 y_0 + (b + 6(k-3)a^{-1}b^2)y_0 y_1 + p^{3\nu_0} G(k, y_0, y_1)]$$

$$S_2 = \Big[1 - 6a^{-1}by_0y_1 - \frac{k(k-1)}{2}b^2 - (2k-4)b^2 - \\ -(2k-4)by_0 + 36a^{-2}b^2(y_0y_1)^2 + (2k-4)^2b^2y_0^2 + \\ +12(2k-4)a^{-1}b^2y_0^2y_1 + p^{3\nu_0}F(k, y_0, y_1)]$$

Звідси отримаємо

$$y_{3k-1} = y_0^{-1}y_1^{-1}\Big\{(a + bc_0) + kb(1 - 2ay_1^{-1}) + k^2b^2\left(y_0 - \frac{1}{2}ay_1^{-1} + 4ay_1^{-1}\right) + \\ + b^3H(k, y_0, y_1)\Big\}$$

де $c_0 = -6a^{-1}by_0y_1 + b^2(3y_0 + 8a + 36a^{-1}(y_0y_1)^2 + 16ay_0^2 - 48y_0^2y_1) + \\ +4by_0a$

За аналогією отримуємо

$$y_{3k} = [2y_0 - 3a^{-1}b^2y_0(1 - ba^{-1}y_1)] + kb(1 + bh(k)) + \\ +k^2b^2\left(-\frac{1}{2}a^{-1}y_0y_1 - 2a^{-1}y_0^2\right) + p^{3\nu_0}L(k, y_0, y_1)$$

де $h(k) = 6a^{-1}by_0^2 - 12a^{-1}by_0^2y_1$,

$$y_{3k+1} = 2^{-1}y_0^{-1}[a + 2by_0 + 3b^2y_0(1 - 6a^{-1}y_1)] + \\ +kb\big(y_0y_1 - 2^{-1}ay_0^{-1} + p^{3\nu_0}b(-3y_0)\big) + \\ +k^2b^2(y_0 + 2^{-1}ay_0^{-2} - 2^{-2}y_0^{-1} - 2^{-1}y_1^{-1}) + p^{3\nu_0}M(k, y_0, y_1)y_0^{-1}$$

З представлень y_{3k} та $y_{3k\pm1}$ випливає наступне твердження.

Твердження 1. *Нехай послідовність* $\{y_n\}$ *згенерована за допомогою лінійного інверсного конгруентного генератору другого порядку з*

$(a, p) = (y_0, p) = (y_1, p) = 1, \nu_p(b) = \nu_0 > 0$. *Тоді існують многочлени* $F_{-1}(x), F_0(x), F_1(x) \in Z[x]$ *з коефіцієнтами що залежать від* y_0, y_1, *такі що*

$$y_{3k-1} = y_0^{-1}y_1^{-1}\Big(\big(a + b(-6a^{-1}y_0y_1) + b^2B_0(y_0, y_1)\big) + \\ +kb\big(1 - 2ay_1^{-1} + bB_1(y_0, y_1)\big) + \\ + k^2b^2\left(y_0 - \frac{7}{2}ay_1^{-1} + bB_2(y_0, y_1)\right)\Big) + p^{3\nu_0}F_{-1}(k)$$

$$y_{3k} = \big(2y_0 + b^2C_0(y_0, y_1)\big) + kb\big(1 + bC_1(y_0, y_1)\big) + \\ +k^2b^2\left(-\frac{1}{2}a^{-1}y_0y_1 - 2a^{-1}y_0^2\right) + p^{3\nu_0}F_0(k)$$

$$y_{3k+1} = 2^{-1}y_0^{-1}\big(a + 2by_0 + 3b^2y_0(1 - ba^{-1}y_1)\big) + kb(y_0y_1 - 2^{-1}ay_0^{-1}) + \\ +k^2b^2(y_0 + 2^{-1}ay_0^{-2} - (2^{-1})^2y_0^{-1} - 2^{-1}y_1^{-1}) + p^{3\nu_0}F_1(k)$$

У процесі доведення твердження 1 отримуємо також такі наслідки.

Наслідок 1. *Для* $k \geq 2$ *маємо*

$$y_{3k-1} = (a + kb + 8ab^2)y_0^{-1}y_1^{-1} + \left(-2akb + \frac{7}{2}ak^2b^2\right)y_0^{-1}y_1^{-2} + \\ +(4ab + 3b^2 + k^2b^2)y_1^{-1} + 16ab^2y_0y_1^{-1} + 48b^2y_0 - 6a^{-1}b + p^{3\nu_0}f_{-1}(y_0, y_1)$$

$$y_{3k} = kb + (2 - 3a^{-1}b^2)y_0 + (18a^{-2}b^2)y_0y_1 + (6a^{-1}b^2k - 2a^{-1}b^2k^2)y_0^2 - \\ -12a^{-1}kb^2y_0y_1 + p^{3\nu_0}f_0(y_0, y_1)$$

$$y_{3k+1} = 2^{-1}ay_0^{-1} + (b + 2^{-1}k^2b + 3b^2) + (-3a^{-1}b^2 + kb)y_1 + \\ +(-2^{-2}abk - 2^{-2}k^2b^2)y_0^{-2} + (-2^{-3}k^2b^2)y_0^{-3} - 2^{-2}y_0^{-1}y_1^{-1} + p^{3\nu_0}f_1(y_0y_1)$$

де f_{-1}, f_0, f_1*- раціональні функції при* y_0, y_1.

Даний наслідок випливає з представлень y_{3k} та $y_{3k\pm1}$.

Наслідок 2. *Нехай* τ *– період послідовності* $\{y_n\}$*, що згенерована за допомогою лінійного інверсного конгруентного генератору другого порядку;* y_0, y_1 *– початкові значення і нехай* $\nu_p(b) = \nu_0 > 0$. *Тоді маємо*

(A) $\tau = 3p^{m-\nu_0}$ *тільки якщо* $4y_0^2 \equiv a\ (modp)$ *або* $y_1 \equiv 2(modp)$*;*

(B) $\tau = 3p^{m-\nu_0-\delta}$ *якщо* $min\left(\nu_p(4y_0^2 - a), \nu_p(y_1 - 2)\right) = \delta < m - \nu_0$

(C) $\tau \leq 3p^{m-\nu_0-\delta}$ *в інших випадках.*

Доведення: Нехай $4y_0^2 \equiv a(\mathrm{mod}p)$. Тоді припускаючи що $y_{3k} = y_{3\ell+1}(\mathrm{mod}p^m)$, ми отримуємо $2y_0 \equiv 2^{-1}ay_0^{-1}(\mathrm{mod}p)$, що призводить нас до протиріччя.

Так само, з того що $y_{3k-1} \equiv y_{3\ell+1}(\mathrm{mod}p^m)$ і $y_{3k} \equiv y_{3\ell+1}(\mathrm{mod}p^m)$ ми робимо висновок про $y_0^{-1}y_1^{-1}a \equiv 2^{-1}ay_0^{-1}(\mathrm{mod}p)$ і $2y_0 \equiv 2^{-1}ay_0^{-1}(\mathrm{mod}p)$ тобто

$$y_1 \equiv 2\ (\mathrm{mod}p) \text{ та } 4y_0^2 \equiv a(\mathrm{mod}p).$$

Нехай $n_1 \equiv n_2(\mathrm{mod}3)$. Тоді з твердження 1 випливає, що $y_{n_1} \equiv y_{n_2}(\mathrm{mod}p^m)$ тоді і тільки тоді, коли $n_1 \equiv n_2(\mathrm{mod}p^{m-\nu_0})$. Звідси $\tau = 3p^{m-\nu_0}$ (частини (B) та (C) доводяться аналогічно). ■

Тепер ми можемо довести основні теореми про експоненційно-тригонометричні суми на послідовності псевдовипадкових чисел $\{y_n\}$, яка згенерована за допомогою генератора другого порядку.

Нехай

$$\sigma_{k,\ell}(h_1, h_2; p^m) := \sum_{y_0 \in Z_{p^m}^*} e\left(\frac{h_1 y_k + h_2 y_\ell}{p^m}\right), (h_1, h_2 \in Z)$$

В даному випадку функції y_k, y_ℓ розглядаються як функції від початкових значень y_0, y_1, що згенеровані генератором другого порядку.

Теорема 1. *Нехай* $(h_1, h_2, p) = 1, \nu_p(h_1 + h_2) = \mu_1, \nu_p(h_1 k + h_2 \ell) = \mu_2,\ k, \ell \in Z_{\geq 0}$ *і нехай* $\{y_n\}$ *згенерована генератором другого порядку. Тоді справджуються наступні оцінки*

$$\left|\sigma_{k,\ell}(h_1,h_2;p^m)\right| \le \begin{cases} 0 & якщо\ k \not\equiv \ell(mod3), \nu_p(h_2) > 0 \\ 4p^{m+\nu_0} & якщо\ \nu_p(h_2) = 0, k \not\equiv \ell(mod3) \\ 0 & якщо\ \mu_1 = 0, k \equiv \ell(mod3), \\ 4p^{m+\nu_0} & якщо\ min(\mu_1,\mu_2) \ge \nu_0, k \equiv \ell(mod3) \end{cases}$$

Доведення: без обмеження загальності припустимо що $(h_1,h_2,p)=1$, та $(h_1,p)=1$. Розглянемо 2 випадки

(I) Нехай k та ℓ невід'ємні цілі числа з $k \not\equiv \ell(\mathrm{mod}3)$, тобто $k = 3k_1 \pm 1$, $\ell == 3\ell_1$ або $k = 3k_1 - 1, \ell = 3\ell_1 + 1$.

Для $k = 3k_1, \ell = 3\ell_1 + 1$, з наслідку 1 маємо

$$h_1 y_{3k_1} + h_2 y_{3\ell_1+1} =$$
$$= A_0 + A_1 y_0 + A_2 y_0^{-1} + b g_1(y_0^{-1}) + b B_1 y_1^{-1} + B_2 y_1^{-1} + b g_2(y_1^{-1})$$

де модуль p^{ν_0}.

$$A_1 = 2h_1, A_2 = 2^{-1}h_2, B_1 = h_2 k, B_2 = -2^{-2}y_0^{-1}.$$

Тоді з леми 1 слідує що,

$$\left|\sigma_{3k_1-1,3\ell}(h_1,h_2)\right| \le \begin{cases} 0 & \text{якщо } \nu_p(h_2) > 0 \\ 4p^{m+1} & \text{якщо } \nu_p(h_2) = 0 \end{cases}$$

Даний результат дає випадок $k = 3k_1, \ell = 3\ell_1 + 1$ або $k = 3k_1 - 1, \ell = 3\ell_1 + +1$.

(II) Нехай $k \equiv \ell(\mathrm{mod}3)$. Розглянемо випадок $k \equiv \ell \equiv 0\ (mod\ 3)$. Тоді з наслідку 1 маємо

$$\begin{aligned} h_1 y_{3k} + h_2 y_{3\ell} = {} & (h_1 k + h_2 \ell) b + (h_1 + h_2)(2 - 3a^{-1}b^2) y_0 + \\ & + (h_1 + h_2) 18 a^{-2} b^2 y_0 y_1 + 6a^{-1}b^2(h_1 k + h_2 \ell) - \\ & - 2a^{-1}b^2(h_1 k^2 + e_2 \ell^2) y_0^2 - 12 a^{-1} b^2 (h_1 k + h_2 \ell) y_0 y_1 + \\ & + p^{3\nu_0} \sum_{j=0}^{m_0} a_j \left(h_1 k^j + h_2 \ell^j\right) f_j(y_0, y_1). \end{aligned}$$

Аналогічно, з леми 1 маємо

$$\left|\sigma_{3k,3\ell}(h_1,h_2)\right| \le \begin{cases} 0 & \text{якщо } \mu_1 = 0, k \equiv \ell \pmod 3, \\ 4p^{m+1} & \text{якщо } \min(\mu_1,\mu_2) \ge \nu_0, k \equiv \ell \pmod 3 \end{cases}$$

В цих двох випадках ми враховуємо, що $I(p^m)$ дорівнюють 0 або 2. ■

Нехай τ – найменший період послідовності $\{y_n\}$.

Теорема 2. *Нехай інверсно-лінійний конгруентний генератор другого порядку має період τ і нехай $\nu_p(b) = \nu_0$ та $4y_0^2 \not\equiv a(mod p)$ або $y_1 \not\equiv 2(mod p)$*

Тоді справджуються наступні оцінки

$$|S_\tau(h,y_0)| \le \begin{cases} O(m) & \textit{якщо} \quad \delta > \nu_0, n_p(h) < m - 2\nu_0 - \delta, \\ 4p^{\frac{m+\nu_p(h)}{2}} & \textit{якщо} \quad \delta \ge \nu_0, \nu_p(h) < m - 2\nu_0, \\ \tau & \textit{в інших випадках.} \end{cases}$$

Доведення: без обмеження загальності можемо вважати, що послідовність $\{y_n\}$ має період $\tau = 3p^{m-\nu_0}$. З наслідку 2 маємо

$$|S_\tau(h,y_0,y_1)| = \left|\sum_{n=0}^{\tau-1} e_m(hy_n)\right| = \left|\sum_{n=0}^{3p^{m-\nu}-1} e_m(hy_n)\right| \le$$
$$\le \left|\sum_{k=1}^{p^{m_1}} e_m(hy_{3k-1})\right| = \left|\sum_{k=1}^{p^{m_1}} e_m(hy_{3k+1})\right| + O(m)$$

де $m_1 = m - \nu_0$ і

$$y_{3k-1} = F_{-1}(k) := A_0 + A_1 k + A_2 k^2 + \cdots$$
$$y_{3k} = F_0(k) := B_0 + B_1 k + B_2 k^2 + \cdots$$
$$y_{3k+1} = F_1(k) := C_0 + C_1 k + C_2 k^2 + \cdots$$

з A_i, B_i, C_i що визначені твердженням 1.

Звідси з леми 1 маємо

$$|S_\tau(h,y_0)| \le \begin{cases} O(m) & \text{якщо } \delta < \nu_0, \nu_p(h) < m-\nu_0-\delta \\ 4p^{\frac{m+\nu_p(h)}{2}} & \text{якщо } \delta \ge \nu_0, \nu_p(h) < m-2\nu_0 \\ \tau & \text{в інших випадках.} \end{cases}$$ ■

Теорема 3. *Нехай послідовність* $\{y_n\}$ *згенерована генератором другого порядку з параметрами* $a, b, y_0, y_1, (a,p) = (y_0 y_1, p) = 1, \nu_p(b) = p^{\nu_0}, \nu_0 \ge 1.$

Тоді для будь-якого $h \in Z$, $(h, p^m) = \mu \le m$ *маємо*

$$\bar{S}_N(h) = \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{y_0, y_1 \in Z_{p^m}^*} |S_N(h, y_0, y_1)| \le 12N^{\frac{1}{2}} + 12Np^{-\frac{m-\nu_0}{2}}$$

Доведення: Нехай $\nu_p(h) = 0$, тобто $(h,p) = 1$. З нерівності Коші-Шварца отримуємо

$$|\bar{S}_N(h)|^2 = \frac{1}{\left(\varphi(p^m)\right)^2} \left| \sum_{y_0, y_1 \in Z_{p^m}^*} \sum_{n=0}^{N-1} e_m(hy_n) \right|^2 =$$

$$= \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{y_0, y_1 \in Z_{p^m}^*} \sum_{k,\ell=0}^{N-1} e_m\big(h(y_k - y_\ell)\big) \le$$

$$\le \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{k,\ell=0}^{N-1} \big|\sigma_{k,\ell}(h,-h)\big| = \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{r=0}^{\infty} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=r}}^{N-1} \big|\sigma_{k,\ell}(h,-h)\big| =$$

$$= \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{t=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=t}}^{N-1} \big|\sigma_{k,\ell}(h,-h)\big| + \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{k=0}^{N-1} \big|\sigma_{k,k}(h,-h)\big| =$$

$$= N + \frac{1}{\left(\varphi(p^m)\right)^2} \sum_{t=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=t}}^{N-1} \big|\sigma_{k,\ell}(h,-h)\big|.$$

Використовуючи теорему 1 маємо

$$|\bar{S}_N(h)|^2 \le N + \frac{1}{\left(\varphi(p^m)\right)^2} \times$$

$$\times \sum_{r=0}^{m-1} \left(\sum_{\substack{k,\ell=0 \\ k\neq\ell \\ (\mathrm{mod}3) \\ \nu_p(k-\ell)=r}}^{N-1} \left|\sigma_{k,\ell}(h,-h)\right| + \sum_{\substack{k=\ell,\ell=0 \\ (\mathrm{mod}3) \\ \nu_p(k-\ell)=r}}^{N-1} \left|\sigma_{k,k}(h,-h)\right| \right) \leq$$

$$\leq N + \frac{1}{\left(\varphi(p^m)\right)^2} \times$$

$$\times \left[4p^m \sum_{r=0}^{m-1} \frac{N^2}{p^r} + \left(\sum_{r<m-\nu_0} + \sum_{m-\nu_0\leq r\leq m-1} \right) \sum_{k\equiv\ell,\ell(\mathrm{mod}3)}^{N-1} \left|\sigma_{k,\ell}(h,-h)\right| \right] \leq$$

$$\leq N + \frac{N}{\left(\varphi\left(p(^m)\right)\right)^2} \times$$

$$\times \left(4Np^m + \sum_{r<m-\nu_0} \frac{N}{p^r} p^{m+\nu_0+r} + p^m \sum_{r\geq m-\nu_0} \frac{N}{p^r} \right) \leq$$

$$\leq N + N^2 p^{-m} \cdot 11 p^{\nu_0}(m-\nu_0).$$

Тоді для $(h,p)=1$ маємо

$$|\bar{S}_N(h)| \leq N^{\frac{1}{2}} + 12Np^{-\frac{m-\nu_0}{2}} \qquad \blacksquare$$

Теореми 1-3 та леми 2-3 дозволяють отримати наступну оцінку для дискріпансії послідовності точок $\left\{\frac{y_n}{p^m}\right\} \in [0,1)$ і точок $X_n^{(s)} \in [0,1)^s$, $X_n^{(s)} = \left(\frac{y_n}{p^m}, \frac{y_{n+1}}{p^m}, \dots, \frac{y_{n+s-1}}{p^m}\right)$

Теорема 4. *Нехай* $p>2, y_0, y_1, a, b, m \in N, m \geq 3, (ay_0y_1, p)=1, \nu_p(b) == \nu_0 \geq 1$. *Тоді для послідовності* $\{x_n\}, x_n = \frac{y_n}{p^m}$, $n = 0,1, \dots$, *з періодом* τ, *що згенерована*

за допомогою лінійно-інверсного конгруентного генератора другого порядку, маємо для будь-яких $1 \le N \le \tau$

$$D_N(x_0, x_1, \dots, x_{N-1}) \le \frac{1}{p^m} + 3N^{-1}p^{\frac{m-\nu_0}{2}}\left(\frac{1}{p}\left(\frac{2}{\pi} log\, p^m + \frac{7}{5}\right)^2 + 1\right)$$

Теорема 5. *Тоді послідовність* $\left\{X_n^{(s)}\right\}$ *з періодом* $\tau = 3p^{m-\nu_0}$ *згенерована за допомогою лінійно-інверсного конгруентного генератора другого порядку. Тоді дискріпансія*

$$D_N^{(s)}\left(X_0^{(s)}, \dots, X_{\tau-s}^{(s)}\right) \le 2p^{-\frac{m}{2}+\nu_0}\left(\frac{1}{\pi} log\ p^{m-\nu_0} + \frac{3}{5}\right)^s + 2p^{-m+\nu_0}$$

для будь-яких $s = 1,2,3,4.$

Твердження теорем 4 та 5 є наслідками з теорем 2 і 3 та лем 2 і 3.

З теорем 4 та 5 ми отримуємо, що послідовність псевдовипадкових чисел, яка згенерована за допомогою лінійно-інверсного конгруентного генератора другого порядку проходить s-мірний тест на рівнорозподіленість та статистичну незалежність.

ВИСНОВКИ

Послідовності псевдовипадкових чисел є не тільки цікавими з теоретичної точки зору, а й надзвичайно корисні в прикладних аспектах. В нашій роботі було розглянуто їх використання наприклад у криптографії, моделюванні та окремих специфічних методах Монте-Карло. Провівши порівняння випадкових чисел із псевдовипадковими, можна із впевненістю стверджувати, що псевдовипадкові числа є більш оптимальними з точки зору використання.

Проте для того аби аналізувати дані послідовності було розглянуто апарат тригонометричних, та відповідні методи (метод Вейля, метод Виноградова тощо). Його поєднання із функцією дискріпансії, яка розглядається в контексті рівномірно розподілених послідовностей дозволяє оцінити «якість» згенерованої послідовності за допомогою певних алгоритмів, одним з яких є s-мірний тест.

Наостанок було розглянуто конкретний приклад побудови генератора псевдовипадкових чисел, а саме лінійно-інверсного конгруентного генератора другого порядку. Було доведено, що послідовність псевдовипадкових чисел, яка генерується даним генератором проходить s-мірний тест на рівномірну розподіленість та статистичну незалежність, що дозволяє використовувати даний генератор в прикладних аспектах.

СПИСОК ЛІТЕРАТУРИ

1. Варбанець С. П. Методи тригонометричних сум в теорії конгруентних генераторів псевдовипадкових чисел та асимптотичних задачах теорії чисел: дис. доктора фіз.-мат. наук / Варбанець Сергій Павлович. – Київ, 2021. – 285 с.
2. Виноградов І. М. Метод тригонометричних сум в теорії чисел. – М, 1971. – 160 с.
3. Іванова В. М. Випадкові числа і їх застосування. – М, 1984. – 108 с.
4. Соболь І. М. Чисельні методи Монте-Карло. – М, 1973. – 308 с.
5. Чанга М. Є. Методи аналітичної теорії чисел. – 2019. – 208 с.
6. Rukhin A. L., S. P. Smid, Y. T. Kolesnik, and A. J. Zukowski. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP) 800-22 Rev 1a. – 2010. – 131 p.
7. Blum L., Shub M. A Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing. – 1986. – Vol. 15, № 2. – P. 364-383.
8. Dick J., Pillichshammer F. Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration. – Cambridge University Press, 2010. – 68 p.
9. Eichenauer J., Lehn J., Topuzoğlu A. A Nonlinear Congruential Pseudorandom Number Generator with Power of Two Modulus. Math. of Comput. – 1988. – Vol. 51. – P. 757-759.
10. Eichenauer J., Grothe H. A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus. ACM Transactions of Modelling and Computer Simulation. – 1992. – Vol. 2, № 1. – P. 1-11.

11. Erdős P., Turán P. On a Problem in the Theory of Uniform Distribution. I. Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen. – 1948. – Vol. 51. – P. 1146-1154.

12. Erdős P., Turán P. On a Problem in the Theory of Uniform Distribution. II. Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen. – 1948. – Vol. 51. – P. 1262-1269.

13. Kato T., Wu L.-M., Yanagihara N. On a Nonlinear Congruential Pseudorandom Number Generator. Math. of Comput. – 1996. – Vol. 65, № 213. – P. 227-233.

14. Kato T., Wu L.-M., Yanagihara N. The Serial Test for a Nonlinear PRN's Generator. Math. Comput. – 1996. – Vol. 63, № 214. – P. 761-769.

15. Lehmer D. H. Mathematical Methods in Large-Scale Computing Units. Ann. Comput. Lab. Harvard Univ. – 1951. – Vol. 26. – P. 141-146.

16. L'Ecuyer P. Random Number Generation. In: Springer Handbooks of Computational Statistics. – 2007. – P. 93-137.

17. Niederreiter H. Random Number Generation and Quasi-Monte Carlo Methods. – Philadelphia: SIAM, 1992. – 241 p.

18. Niederreiter H. Low-Discrepancy and Low-Dispersion Sequences. J. Number Th. – 1987. – Vol. 30. – P. 51-70.

19. Niederreiter H., Shparlinski I. Exponential Sums and the Distribution of Inversive Congruential Pseudorandom Numbers with Prime-Power Modulus. Acta Arith. – 2000. – Vol. 90, № 1. – P. 89-98.

20. Varbanets P. D., Varbanets S. P. Inversive Generator of the Second Order for the Sequence of PRN's. Abstracts of X International Algebraic Conference in Ukraine Dedicated to 70th Anniversary of Yu. A. Drozd. – 2015. – P. 119.

21. Varbanets P. D., Varbanets S. P. Exponential Sums on the Sequences of Inversive Congruential Pseudorandom Numbers with Prime-Power Modulus. In:

VoronoI's Impact on Modern Science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1. – Kyiv, Ukraine, September 22-28, 2008. – P. 112-130.

22. Varbanets S. Generalizations of Inversive Congruential Generator. In: Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania. – 2012. – P. 265-282.

23. Varbanets S. Generalizations of Inversive Congruential Generator. In: Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania. – 2012. – P. 265-282.

24. Von Neumann J. Various Techniques Used in Connection with Random Digits. National Bureau of Standards Applied Mathematics Series. – 1951. – № 12. – P. 36-38.

25. Wrench J. Table Errata: The Art of Computer Programming, Vol. 2: Seminumerical Algorithms (Addison-Wesley, Reading, Mass., 1969) by Donald E. Knuth. Mathematics of Computation. – 1970. – Vol. 24, Iss. 110. – P. 504.