

РЕФЕРАТ

Актуальність теми. Випадкові числа використовуються давно і досить широко. Нагадаємо деякі області їх застосування:

- Соціологічні та наукові дослідження. Підготовка випадкових вибірок при зборі даних, опитуванні думок або в дослідженні фізичних явищ з випадковим вибором результатів експериментів.

- Моделювання. У комп'ютерному моделюванні фізичних явищ. Крім того, математичне моделювання використовує випадкові числа як один з інструментів чисельного аналізу.

- Криптографія та інформаційна безпека. Випадкові числа можуть використовуватися в тестуванні коректності або ефективності алгоритмів і програм. Багато алгоритмів використовують генерацію псевдовипадкових чисел для вирішення прикладних завдань (наприклад, криптографічні алгоритми шифрування, генерація унікальних ідентифікаторів та ін.).

Теорія побудови генераторів псевдовипадкових чисел (ГПВЧ) глибоко і добре вивчена. Однак у тій же інженерній практиці виникає необхідність у генерації якихось спеціальних послідовностей певної підмножини векторів довжини n . Прикладом може бути область тестування цифрової апаратури

Об'єктом дослідження є процес побудови гамільтонових циклів на основі сформованих векторів.

Предметом дослідження є спосіб формування гамільтонових циклів для генераторів псевдовипадкових чисел з різною вагою.

Мета роботи: Проаналізувати можливість побудови гамільтонового циклу для генератора псевдовипадкових двійкових векторів з вагами $p_1 \dots p_k$ (послідовно розташованих на числовій осі) на основі стандартної схеми: n -розрядний регістр зсуву зі зворотним зв'язком.

Наукова новизна полягає в наступному:

Розроблено спосіб пошуку усіх гамільтонових циклів для заданого набору векторів з вагами $p_1 \dots p_k$.

Практична цінність У роботі розглядаються теоретичні аспекти проблеми побудови генератора псевдовипадкових двійкових векторів з кількома вагами, що йдуть на основі класичної схеми: зсувний регістр зі зворотним зв'язком у вигляді схеми, що реалізує певну булеву функцію. Показується, що це можливо, доводиться існування гамільтонова циклу у графі переходів генератора. У випадку нелінійної функції оберненого зв'язку. Розглядається можливість пошуку різних гамільтонових циклів графа, втілення яких призводить до різних генераторів, які можуть серйозно відрізнятися в плані складності реалізації булевої функції зворотного зв'язку та за якістю імовірнісних характеристик послідовності, що генерується двійкових векторів. Це розширює можливості розробника під час побудови генератора.

Апробація роботи. Основні положення і результати роботи були представлені та обговорювались на XV конференцію молодих вчених ПМК-2022 року (Київ, 16-18 листопада 2022 р.); Тези до доповіді на IX Міжнародній науково-технічній Internet-конференції 2022 року.

Структура та обсяг роботи. Магістерська дисертація складається з вступу, чотирьох розділів та висновків.

У *вступі* подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень, показано наукову новизну отриманих результатів і практичну цінність роботи, наведено відомості про апробацію результатів і їхнє впровадження.

У *першому розділі* розглянуто загальні відомості про ГПВЧ, а також проведений аналіз, який дає змогу визначити основні переваги та недоліки цих способів.

У *другому розділі* аналізуються існуючі генератори псевдовипадкових та реальних чисел.

У третьому розділі наведено види та критерії тестів для статичних властивостей генераторів псевдовипадкових чисел.

У четвертому розділі представлений спосіб формування векторів з різною вагою згідно заданих параметрів, та пошуку для них гамільтонових циклів.

У висновках представлені результати проведеної роботи.

Робота представлена на 80 аркушах, містить посилання на список використаних літературних джерел.

Ключові слова: ГПВЧ, перетворення, вектори, генератори, графи.