

ГЕНЕРАТОРИ ВИПАДКОВИХ ЧИСЕЛ В СКЛАДІ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЮВАЧА МОНТЕ-КАРЛО

Семаньків М.В.

Державний вищий навчальний заклад «Прикарпатський національний університет імені Василя Стефаника», м. Івано-Франківськ

Статистичне моделювання систем потребує формування значень випадкових величин, що реалізуються з допомогою генераторів випадкових або псевдовипадкових чисел. Важливим класом псевдовипадкових послідовностей є послідовності, які формуються генераторами на основі регістрів зсуву з лінійними зворотними зв'язками. Основними перевагами таких генераторів є: простота апаратної і програмної реалізації; висока швидкодія; достатньо високі статистичні властивості сформованих послідовностей; можливість побудови на їх основі генераторів, що формують послідовність довільної довжини або послідовність псевдовипадкових чисел з довільним законом розподілу.

Запропоновано метод генерування псевдовипадкових чисел Галуа на основі циклічних зсувів, який реалізовано програмно і апаратно. Конструктивно апаратна реалізація методу відносно проста, пристрій генерування псевдовипадкових чисел функціонує в циклічному режимі, з використанням генератора тактових імпульсів, тригерів регістру зсуву, логічних елементів І, логічних елементів сумування за модулем два та інвертора. Підвищення розрядності псевдовипадкових чисел при апаратній реалізації спричинить тільки до розширення кількості розрядів регістру зсуву та елементів зворотного зв'язку.

Результати досліджень вказали на ефективність теоретико-числових перетворень із застосуванням теорії полів Галуа, які дозволяють реалізувати швидкі прямі алгоритми обчислень, що зумовлені простотою апаратної реалізації на базі процедур зсуву. Коди Галуа володіють одними із кращих характеристиками кодової дистанції (для розрядності кодового слова $n > 6$, де $n = \log_2 N$, N – модуль системи числення) і кореляційних функцій, а також множинністю алгоритмів декодування, які реалізуються на основі високорегулярних послідовних структур.

Проведено дослідження статистичних характеристик генерованих послідовностей з допомогою пакетів статистичних тестів NIST, Diehard та згідно критеріїв χ^2 та Пірсона. Результати проведених досліджень на визначення типу розподілу послідовності псевдовипадкових чисел, генерованих зазначеним методом, показали високу якість рівномірності розподілу та ефективність використання даного генератора в складі аналого-цифрового перетворювача Монте-Карло. Використання запропонованого методу генерування псевдовипадкових чисел Галуа на основі циклічних зсувів дозволило регуляризувати структуру АЦП Монте-Карло, підвищити швидкодію та технологічність виробництва і зменшити вартість продукту.