

УДК 621.382(07) + 681.32(07)

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ РОЗПОДІЛІВ НА ОСНОВІ КОДІВ ГАЛУА

Лаврів М.В., аспірант каф. Інформатики
Прикарпатського національного університету ім.
В.Стефаника (м. Івано-Франківськ) dlya_marii@mail.ru

Одним із ефективних шляхів розширення смуги спектру сигналу, аналого-цифрового перетворення на основі інтегрального методу є використання методу статистичних досліджень Монте-Карло. Широке застосування останнього обмежувалось складністю якісних алгоритмів і засобів генерування псевдовипадкових сигналів та значними коштами виготовлення, що і визначило актуальність здійснення досліджень по розробці таких генераторів, які б володіли конкуруючими техніко-економічними характеристиками.

Запропоновано метод і розроблено генератор псевдовипадкових чисел на основі циклічних кодів типу послідовностей максимальної довжини, який полягає в тому, що в кодовій послідовності всі елементи володіють рекурсивною взаємозалежністю, а кожен із n -розрядних кодових фрагментів та їх аналогове представлення має псевдовипадковий характер розподілу на одиничному періоді. Технічна реалізація такого генератора полягає у застосуванні регістра зсуву, охопленого логічним зворотним зв'язком згідно примітивних невірджених поліномів, до цифрових виходів якого підключено цифро-аналоговий перетворювач, що по аналоговому виходу формує аналогову розгортку псевдовипадкового сигналу.

Здійснено оцінку якості псевдовипадкового розподілу за допомогою емпіричних та теоретичних методів

тестування. Зокрема, у групі емпіричних тестів проведено:

- перевірку рівномірності розподілу між нулем і одиницею;
- перевірку серій, згідно якої досліджується рівномірність і незалежність пар суміжних випадкових чисел;
- перевірку інтервалів між моментами появи суміжних значень;
- перевірку комбінацій, що досліджує розподіл n груп із k наступних один за одним чисел і обчислює число груп, в яких міститься r різних чисел;
- перевірку перестановок, що розділяє початкову послідовність на n груп з t елементів в кожній і визначає скільки раз зустрічається кожне розміщення, після чого застосовується критерій χ^2 .

З метою визначення потенційної верхньої спектральної частотної складової проведено спектральне тестування отриманого розподілу.

За допомогою графічних тестів, зокрема гістограми розподілу елементів оцінено рівномірність розподілу символів у послідовності та визначено частоту їх появи. Тест оцінки розподілу на площині дозволив визначити залежності між елементами досліджуваної послідовності, а перевірки на монотонність - рівномірність розподілу символів. За допомогою графічного спектрального тестування здійснено перевірку послідовності на розподіл 0 і 1 в досліджуваній послідовності на основі аналізу висоти викидів перетворення Фур'є.

За допомогою статистичних критеріїв, зокрема χ^2 та Колмогорова - Смірнова проведено статистичні дослідження отриманих розподілів для визначення закону розподілу випадкових чисел, які дозволили визначити тип емпіричного розподілу як рівномірний, а сукупність всіх наведених тестів ствердити високі якісні показники у порівнянні з відомими методами генерування псевдовипадкових розподілів за співвідношенням критеріїв "якість розподілу – вартість реалізації".