

УДК 621.391

МЕТОД ВИЗНАЧЕННЯ СТЕПЕНІВ УТВОРЮЮЧИХ ПОЛІНОМІВ ПСЕВДОВИПАДКОВИХ ДВІЙКОВИХ ПОСЛІДОВНОСТЕЙ

Олещук Д.В., Бондар Д.В.

e-mail: denys.oleshchuk@nure.ua, e-mail: dmytro.bondar@nure.ua

Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

This work is devoted to the description of the method of programmatic determination of the powers of the generating polynomials of pseudo-random binary sequences, according to which the cell numbers of the shift register of the sequence generator are selected. The algorithms for creating tuples of register bit numbers and selecting from them those that can be used to generate pseudo-random binary sequences are considered. There is a link to the developed software module. The advantages and disadvantages of the considered method are formulated.

Сучасна телекомунікаційна техніка працює, спираючись на цифрові технології обробки та передачі інформації. Безпосередня увага приділяється двійковим кодам та двійковим послідовностям.

Важливе місце між двійкових послідовностей займають псевдовипадкові двійкові послідовності максимальної довжини, які ще мають назву m -послідовностей. Ці послідовності застосовують для вирішення багатьох задач, зокрема: розширення спектру інформаційних сигналів, скремблювання двійкових потоків, шифрування, утворення кодів різноманітного призначення тощо.

Основним методом формування m -послідовностей є побудова генератору на основі двійкового регістру зсуву, охопленого лінійним зворотним зв'язком. Тракт зворотного зв'язку складається з блоку суматора за модулем два, на вхід якого надходять сигнали з виходів чарунок регістру зсуву. Вихідний сигнал з блоку суматора за модулем два подається на вхід регістру зсуву, замикаючи тим самим коло зворотного зв'язку. Таким чином є можливість утворення m -послідовностей довжина яких визначається кількістю чарунок регістру відповідно до виразу $2^n - 1$, де n – кількість чарунок регістру. Означені послідовності є періодичними з означеним вище періодом.

При побудові генератора m -послідовності треба так визначити виходи чарунок регістру, щоб в результаті роботи в регістрі утворилися всі можливі $2^n - 1$ двійкові комбінації окрім повністю нульової. Вибір визначальних чарунок здійснюється, спираючись на теорію утворюючих поліномів, але

можна запропонувати альтернативний спосіб за допомогою програмної реалізації відповідного алгоритму.

На першому етапі слід сформулювати вимоги до визначення кількості чарунок, виходи яких треба завести на вхід тракту зворотного зв'язку. Ці вимоги полягають в наступному. Якщо регістр складається з n чарунок, то всього можливо 2^n варіантів обрання. Далеко не всі з цих варіантів підійдуть. По-перше, не слід обирати вихід тільки однієї чарунки із зрозумілих причин. По-друге, неможна обирати непарну кількість чарунок, оскільки це призведе до зациклювання генератора на стані, коли всі чарунки встановлені в одиницю, який є обов'язковим для утворення саме послідовності максимальної довжини. По-третє, на вхід тракту зворотного зв'язку обов'язково потрібно заводити сигнал з вихідної чарунки регістру, інакше довжина m -послідовності буде скорочена практично в два рази.

На другому етапі необхідно створити матриці з номерів чарунок регістрів, які дозволять згенерувати m -послідовність. З цією метою слід зробити наступне. По-перше, згенерувати всі можливі комбінації номерів чарунок в межах довжини регістру парної кількості з обов'язковою присутністю номеру вихідної чарунки. По-друге, провести відсіювання тих комбінацій, які не забезпечують утворення послідовності максимальної довжини.

Реалізація другого етапу вимагає використання алгоритму генерування всіх сполучень вигляду C_n^k , де $k \leq n \wedge k \oplus 2 = 0$. Можна генерувати всі сполучення вигляду C_{n-1}^k , де $k \leq n-1 \wedge k \oplus 2 = 1$, при умові, що до утворених кортежів буде додано номер вихідної чарунки регістру n .

Відсіювання треба проводити на підставі задоволення двох умов: збалансованості та періодичності послідовності.

Перевірка збалансованості полягає в підрахунку одиниць в одному періоді послідовності. Одиничних символів повинно бути більше ніж нульових символів рівно на один символ.

Перевірка періодичності полягає в посимвольному порівнянні двох суміжних сегментів згенерованої послідовності довжиною $2^n - 1$ двійкових символів кожна. Всі символи повинні співпадати.

На третьому етапі можна створити програмний модуль, що реалізує запропонований метод. Одна з версій цього програмного модуля реалізована в середовищі пакету MathCad та надає коректні результати.

Переваги методу полягають у можливості створення не великого за об'ємом та складністю програмного додатку та не шукати довідникові дані.

Недоліком є те, що достатність двох критеріїв відсіювання, отриманих емпірично, надана як гіпотеза та не є доведеною теоретично. Також слід

зауважити, що збільшення довжини m -послідовності тягне зростання часу роботи додатку, що може обмежувати його використання.

Список використаних джерел:

1. Склад Б. Цифровая связь. Теоретические основы и практическое применение: Издательский дом «Вильямс», 2003. – 1104 с.