УДК 004.056.55: 621.3.037.372.9: 621.3.083.72: 621.394.147

Ідентифікація імпульсних джерел повідомлень в системах автоматики

Л.Б. Петришин[1]

Abstract – **Mathematical identification bases of a impulsive information sources state on the recursive Galois coding base are resulted.**

Ключові слова – **перетворення, формування, код, рекурсія.**

I. Вступ

Реалізація системних функцій подання повідомлень в цифровій формі про стан інформаційного джерела є однією з актуальних задач первинного перетворення форми інформації. Поняття джерела повідомлень визначається як система засобів безпосереднього зчитування інформації про об'єкт та нормування значення по визначеному електричному параметру.

Засоби ідентифікації стану джерел повідомлень структурно складаються власне з джерела повідомлень та кодера чи транскодера із кінцевим вихідним кодом трансформації. Всі первинні перетворювачі, незалежно фізичній природі параметру перетворення, класифікуються по типу вихідного електричного сигналу на засоби із дискретним та аналоговим виходом. Причому дискретні перетворювачі підрозділяються на засоби із безпосередньо кодо-імпульсним виходом, як то первинні перетворювачі із число-імпульсним інтегральним, частотно-імпульсним, широтно-імпульсним, фазо-імпульсним та т.п. виходом та засоби із безпосередньо кодовим зчитуванням, як то перетворювачі переміщень на кодових шкалах. Якщо сигнали із перетворювачів з дискретним виходом можуть безпосередньо вводитись в цифрову систему із, за необхідності, проміжним дискретним перетворенням, то аналогові сигнали потребують попереднього перетворення, яке включає квантування по рівню та дискретизацію по часу із формуванням для кодування псевдоаналогового багатостабільного сигналу.

Виходячи з точки зору прикладного застосування теоретико-числових перетворень, системні функції інфотехнології: генерування, формування, перетворення, слідкування, аналого-цифрове перетворення, об'єднуються в єдиний клас засобів ідентифікації стану джерел повідомлень. Це дозволяє розглядати процедуру перетворення форми інформації з єдиних позицій математичного трактування та застосуванням єдиного математичного апарату дискретних міжбазисних трансформацій.

Проаналізуємо принципи та засоби формування і генерування рекурсивних послідовностей Галуа.

II. Основи ідентифікації імпульсних джерел повідомлень

В сучасних розподілених інфосистемах крім первинного перетворення інформації постає задача завадозахищеної дистанційної передачі повідомлень, часто в умовах значних промислових завад. Вибір методів зменшення надлишковості даних, кількості інформаційних та службових шин, застосування методів завадозахисту постає актуальною задачею. Перехід до нових базисів та методів теоретико-числових трансформацій забезпечує значне покращення техніко-економічних показників перетворювачів форми інформації.

Якщо повідомлення, представлені в певній кодовій системі, володіють внутрішніми кореляційними зв'язками, то завадостійкість коду підвищується за рахунок логіко-аналітичних зв'язків між кодовими символами. Якщо ці зв'язки слабкі, або невідомі, то між кодовими символами вводять штучні кореляційні зв'язки шляхом збільшенням числа символів в коді повідомлення, внаслідок чого форма представлення повідомлень стає надлишковою і кодова система теж визначається надлишковою. Одна із основних властивостей кодових систем Галуа - рекурсивне впорядкування кодових елементів, що забезпечує кореляційну взаємозалежність елементів в кодовій послідовності та дозволяє проводити високоефективне завадозахищене кодування повідомлень.

Технічні засоби завадозахищеної ідентифікації стану імпульсних джерел повідомлень ґрунтуються на використанні лінійних схем перемикання зі скінченим числом станів, які вміщують скінчене число пристроїв пам'яті, суматорів та засобів перемноження на константу і організовані послідовно в регістр зсуву, кожен із виходів якого через перемножувач підключений до суматора за модулем 2, сигнали із виходу якого формують вихідний сигнал рекурсивної кодової послідовності Галуа. Передбачається, що в лінійних схемах перемикання дані представлено за допомогою елементів поля Галуа $GF(2^n)$.

Вхід та вихід схеми є послідовними, причому на послідовній шині формуються тільки коефіцієнти поліному Галуа, які передаються, починаючи з вищих порядків. Так, поліном

$$A(x) = a_{n-1}\, x^{n-1} + a_{n-2}\, x^{n-2} + \ldots + a_0$$

буде сформовано по вихідній шині послідовністю п кодових елементів Галуа, починаючи із a_{n-1}.

При реалізації системної операції формування цифрових повідомлень процедура кодування передбачає

[1] AGH University of Science and Technology, ul. Gramatyka, 10, Kraków, 30-067, POLAND, E-mail: L.B.Petryshyn@gmail.com

векторне множення поліному повідомлення на фіксований поліном. Задамо повідомлення A(x) вектором $a_{n-1}, a_{n-2}, \ldots a_0$, та у вигляді поліному

$$A(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_0 .$$

Нехай поліном кодування

$$G(x) = g_{k-1} x^{k-1} + g_{k-2} x^{k-2} + \ldots + g_0 , \quad g_i(x) \in GF(2^k)$$

над повідомленням A(x) призводить до результату

$$B(x) = A(x)\, G(x) = b_{r-1} x^{r-1} + b_{r-2} x^{r-2} + \ldots + b_0 =$$
$$= a_{n-1} g_{k-1} x^{n+k-2} + (a_{n-2} g_{k-1} + a_{n-1} g_{k-2}) x^{n+k-3} + \ldots +$$
$$+ (a_0 g_2 + a_1 g_1 + a_2 g_0) x^2 + (a_0 g_1 + a_1 g_0) x + a_0 g_0,$$

де r = n + k.

Коли на вхід схеми перемноження подається перший коефіцієнт a_{n-1} поліному A(x), то на виході генерується перший коефіцієнт добутку A(x) G(x), рівний $a_{n-1} g_{k-1}$. В цей момент усі комірки пристрою запам'ятовування вміщують нулі. На наступному такті вихід буде рівний коефіцієнту b_{r-2}, згідно виразу $a_{n-2} g_{k-1} + a_{n-1} g_{k-2}$, тобто значенню другого коефіцієнту добутку. Подальші рекурсивні операції здійснюються аналогічним чином. Після n+k-2 зсувів в комірках регістру перебуватимуть елементи 0, 0, ... , a_0, a_1, а вихід рівний $a_0 g_1 + a_1 g_0$, тобто передостанньому коефіцієнту добутку A(x) G(x). Після n+k-1 зсувів регістр вміщуватиме елементи 0, 0, ... , 0, a_0, а на виході буде сформовано останній коефіцієнт $a_0 g_0$ добутку. Таким чином, результат добутку двох поліномів отримано повністю.

Наведену лінійну структуру можна трактувати як пристрій перемноження довільних, поданих на вхід регістру зсуву поліномів Галуа A(x) на фіксований перемикачами зворотного зв'язку поліном G(x) із видачею на вихід схеми результату B(x) добутку.

Згідно іншого способу перемноження коефіцієнти добутку формуються в регістрі зсуву, тобто, сукупність k комірок пристрою пам'яті утворюють регістр, в якому на періоді перемноження умовно постійно записано заданий поліном G(x). Початково цей поліном рівний нулю. Подача на вхід коефіцієнта a_{n-1} додає до вмісту регістра поліном $a_{n-1} g(x)$. В результаті зсуву проводиться множення на x і на виході генерується перший коефіцієнт. Після подачі на вхід коефіцієнта a_{n-2} до полінома, записаного в регістр, додається поліном $a_{n-1} g(x)$, а при зсуві відбувається множення на x із видачею на вихід другого коефіцієнта добутку. Процедура повторюється аналогічно рекурсивно в часі на періоді n + k тактів до отримання останнього коефіцієнту результату перемноження.

Такий спосіб генерування характеризується вищою швидкодією та можливістю перемноження в полі Галуа більшої кількості поліномів.

На ґрунті наведених математичних засад виконання операцій над поліномами в полях Галуа базується апарат генерування кодових рекурсивних послідовностей Галуа, що слугує основою для розробки та побудови технічних засобів формування та генерування кодових систем Галуа.

Розглянемо рекурсивні співвідношення

$$\sum_{j=0}^{n-1} h_j a_{i+j} = 0, \quad \text{або} \quad a_{i+n} = -\sum_{j=0}^{n-1} h_j a_{i+j}, \qquad (1)$$

де $h_0 \neq 1$, $h_n = 1$ і кожне h_j належить полю $GF(2^n)$. Розв'язком цих рівнянь є послідовність $a_0, a_1, a_2, \ldots$ елементів поля $GF(2^n)$. Співвідношення (1) визначає правило обчислення a_n за заданими значеннями величин $a_{n-1}, a_{n-2}, \ldots a_0$. За відомими значеннями $a_n, a_{n-1}, \ldots a_1$ визначається a_{n+1} і так дальше. Оскільки рівняння лінійні, то довільна лінійна комбінація їх розв'язків знову є розв'язком, а всі розв'язки утворюють векторний простір. Сукупність із n розв'язків, для кожного із яких один із символів $a_{n-1}, a_{n-2}, \ldots a_0$ рівний 1, а всі решта рівні 0, породжує весь простір розв'язків. Відповідно, розмірність простору розв'язків не перевищує n.

Поліномний код з вектором кодування G(x) є матричним кодом з кодовою матрицею розмірності n×(n + k):

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & . & . & . & g_k & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & . & . & g_{k-1} & g_k & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & g_0 & g_1 & . & . & . & g_{k-1} & g_k \end{bmatrix}.$$

Ненульові елементи в j-й лінійці утворюють блок $g_0, g_1, \ldots, g_k$, розташований від j-го до j+k-го місця. Слід зауважити, що ненульові елементи чергової лінійки отримують зсувом вправо на одиницю із ненульових елементів попередньої лінійки. Для отримання кодових слів в кодовій системі Галуа використовують лінійні рекурсивні співвідношення.

З метою максимального використання обчислювальних апаратних ресурсів регістрів зсуву постає питання про отримання кодових послідовностей з максимально можливим періодом N. Найбільше можливе значення N для основи p та порядку n становить $N=p^n - 1$ при рекурсивному базисному упорядкуванні векторів, або ж $N=p^n$ при штучному вкладенні додатково 0 в генерований фрагмент із n - 1 нулів. Тобто, період, більший від $N=p^n - 1$ ($N=p^n$) не може бути реалізований для поліномів степені n над полем із p елементів. Виходячи з даної властивості, послідовні блоки довжини n на одному періоді $N=p^n - 1$ ($N=p^n$) складають множину всіх n-блоків тільки по одному разу, тому лінійні послідовності Галуа є ізоморфними повному довільному числовому полю однакової розмірності.

IV. Висновок

Таким чином, наведені теоретичні засади дозволяють розробки методи та схемотехнічні рішення побудови пристроїв завадозахищеного генерування та формування рекурсивних кодових послідовностей Галуа, що володіють мінімальною надлишковістю інформаційного обміну в розподілених мережах.