Исследование возможности декодирования сложных кодовых последовательностей

© А.С. Косолапов, А.В. Галев

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Шумоподобные сигналы широко применяются для передачи полезной информации и обеспечения синхронизации. Представляет интерес разработка метода декодирования широкого класса шумоподобных сигналов, формируемых комбинированием нескольких исходных компонентных М-последовательностей по тому или иному правилу. Проведенные исследования основаны на положениях теории полей Галуа и на структурных свойствах шумоподобных сигналов. Показано, что разложение комбинированных кодовых последовательностей на компоненты возможно путем решения системы уравнений, связывающих между собой координаты элементов поля Галуа и входные символы декодируемой кодовой последовательности.

Ключевые слова: шумоподобные сигналы, поля Галуа, сопровождающая матрица полинома, векторы-столбцы координат.

Введение. Для передачи информации в современных системах связи широко применяют шумоподобные сигналы (ШПС). Часто в таких системах канал синхронизации совмещают с информационным каналом. Длину кода при этом выбирают в соответствии с требуемыми точностью и скоростью вхождения в синхронизм и достоверностью передаваемой информации. При заданных вероятностных характеристиках бывает технически сложно и даже нецелесообразно применять алгоритмы декодирования, для реализации которых необходимо использовать целое кодовое слово.

Интерес представляют алгоритмы, которые позволяют восстанавливать кодовое слово по отдельным правильно принятым символам (информационной совокупности). Такие алгоритмы декодирования наиболее просто реализовать с помощью циклических кодов. Наибольшее распространение получили коды максимальной длины (M-последовательности). Для декодирования M-последовательностей применяют, в частности, известный метод последовательной оценки.

В многоадресных системах использование M-последовательностей не представляется возможным ввиду малого ансамбля сигналов и неудовлетворительных взаимнокорреляционных функций сигналов. В таких системах используются кодовые последовательности с большим ансамблем сигналов, каждый из которых предназначен для определенного абонента системы. Сигналы могут быть построены на основе двух M-последовательностей или более [1]. Разделение сигналов абонентов проводится на основе различий в структуре широко-

полосных сигналов. Известны двоичные кодовые последовательности, образованные путем комбинации нескольких кодовых M-последовательностей [2, 3].

Успешное решение задач распознавания и синхронизации при использовании таких последовательностей может быть найдено, если входные кодовые последовательности разложить на компоненты. Последующая обработка этих компонент позволит различать входную кодовую последовательность и определять ее фазу.

Предлагаемая методика декодирования двоичных кодовых последовательностей представляет собой процедуру разложения входной последовательности на компоненты. Данная методика универсальна, т.е. ее можно применять для обработки различных кодовых последовательностей, сформированных на основе двух и более M-последовательностей любой длины.

Методика декодирования. На примере обработки входных сигналов, представляющих собой последовательности Голда и последовательности малого семейства Касами, рассмотрим методику декодирования. Исходными компонентами, формирующими эти последовательности, являются две M-последовательности, которые описываются соответствующими первообразными, неприводимыми полиномами $f_1(x)$ и $f_2(x)$. При формировании последовательности Голда порождающие M-последовательности имеют одинаковую длину, при формировании последовательности Касами — разную длину.

В общем виде первообразный, неприводимый над полем $GF(2^n)$ полином f(x) степени n и его сопровождающая матрица имеют вид [4]:

$$f(x) = C_n x^n + C_{n-1} x^{n-1} + \dots + C_1 x + C_0;$$

$$H = \begin{vmatrix} 0 & 0 & \cdots & 0 & C_0 \\ 1 & 0 & \cdots & 0 & C_1 \\ 0 & 1 & \cdots & 0 & C_2 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \cdots & 1 & C_{n-1} \end{vmatrix},$$
(1)

где C — весовые коэффициенты, принимающие значения 0 или 1 и определяющие конкретный вид полинома f(x).

Справедливо матричное уравнение

$$X_{i+1} = H^l X_i, \tag{2}$$

где X_{i+1} и X_i — n-мерные векторы-столбцы координат в натуральном базисе i-го элемента поля Γ алуа $\mathrm{GF}(2^n)$.

Матричное уравнение (2) можно записать в виде:

$$\begin{pmatrix}
x_{i+l}^{0} \\
x_{i}^{1} \\
x_{i+l}^{1} \\
\dots \\
x_{i+l}^{k} \\
\dots \\
x_{i+l}^{n-1}
\end{pmatrix} = H^{l} \begin{pmatrix}
x_{i}^{0} \\
x_{i}^{1} \\
\dots \\
x_{i}^{k} \\
\dots \\
x_{i}^{n-1} \\
\dots \\
x_{i}^{n-1}
\end{pmatrix},$$
(3)

где x^{k}_{i} — k-я координата i-го элемента поля Галуа.

Иногда M-последовательностью называют упорядоченную периодическую последовательность нулевых координат ненулевых элементов поля $\mathrm{GF}(2^n)$:

$$M = (x_0^0, x_1^0, \dots, x_i^0, \dots, x_{2^n-2}^0)$$

Откуда непосредственно следует, что $x^0_i = a_i$, т.е. a_i -й символ M-последовательности совпадает со значением нулевой координаты i-го элемента поля $GF(2^n)$. Нулевым по порядку следования символом M-последовательности удобно считать значение нулевой координаты элемента поля $a^0 = 1$, первым символом — a^1 и так далее до a^{2^n-2} ; a — первообразный элемент поля $GF(2^n)$.

Используя сопровождающую матрицу H полинома f(x), можно получить следующие соотношения:

$$x_{i}^{n-1} = x_{i+1}^{0} = a_{i+1};$$

$$x_{i+1}^{n-1} = x_{i+2}^{0} = a_{i+2} = x_{i}^{n-2} + C_{n-1} x_{i}^{n-1};$$

$$x_{i+2}^{n-2} = a_{i+2} + C_{n-1} a_{i+1};$$

$$x_{i+2}^{n-1} = x_{i+3}^{0} = a_{i+3} = x_{i+1}^{n-2} + C_{n-1} x_{i+1}^{n-1};$$

$$x_{i+1}^{n-2} = x_{i}^{n-3} + C_{n-2} x_{i}^{n-1};$$

$$x_{i}^{n-3} = a_{i+3} + C_{n-1} a_{i+2} + C_{n-2} a_{i+1};$$

$$x_{i+3}^{n-1} = x_{i+4}^{0} = a_{i+4} = x_{i+2}^{n-2} + C_{n-1} x_{i+2}^{n-1};$$

$$x_{i+2}^{n-2} = x_{i+1}^{n-3} + C_{n-2} x_{i+1}^{n-1};$$

$$(6)$$

$$x_{i+1}^{n-3} = x_i^{n-4} + C_{n-3} x_i^{n-1};$$

$$x_i^{n-4} = a_{i+4} + C_{n-1} a_{i+3} + C_{n-2} a_{i+2} + C_{n-3} a_{i+1}.$$
(7)

Продолжая подобные расчеты, для (n-1)-й координаты некоторого i-го символа можно записать рекуррентное уравнение:

$$x_i^{n-l} = a_{i+l} + C_{n-1}a_{i+l-1} + C_{n-2}a_{i+l-2} + \cdots$$
 (8)

Для любого многочлена f(x) уравнение (8) можно записать в виде

$$x_i^k = \sum_{j=0}^{n-k-1} C_{n-j} a_{i+n-k-j},$$
(9)

причем k = 0, 1, ..., n - 1. Координаты x_i^0 и x_i^{n-1} можно определять с помощью выражений:

$$x_i^0 = a_i;$$
$$x_i^{n-1} = a_{i+1}.$$

Из выражений (4) — (7) следует, что координаты соседних символов произвольного отрезка M-последовательности связаны между собой рекуррентным соотношением:

$$x_{i+1}^k = x_i^{k-1} + C_k x_i^{n-1} , (10)$$

причем $x_i^0 = a_i$.

С помощью рекуррентного уравнения (9) можно определить все координаты произвольного i-го элемента, используя значения n следующих подряд символов M-последовательности.

Из структуры уравнения (9) следует, что устройство, определяющее координаты текущих элементов поля, номера которых совпадают с номерами, соответствующих символов M-последовательности, представляет собой простую совокупность сумматоров по модулю два. На n входов такого устройства поступает опорная выборка из n символов последовательности.

Согласно изложенному выше, опорная выборка из n символов M-последовательности позволяет определить вектор координат одного элемента поля (символа), а затем и его номер. Однако ошибки в оценке символов опорной выборки, возникающие в результате воздействия помех, приведут к ошибочному вычислению вектора координат, а следовательно, и номера символа M-последовательности. Для установления факта неправильного определения номера можно

учитывать, что значения векторов координат соседних элементов поля связаны между собой соотношением (3).

Решение о наличии на входе полезного сигнала с заданной фазой может быть сделано, если последующие независимые измерения дают результаты, логически вытекающие из предыдущих. Таким образом, упорядоченный характер серии определяемых векторов координат может служить не только критерием правильного распознавания входного сигнала, но и критерием правильного нахождения его фазы.

Рассмотрим процедуру декодирования последовательностей Голда, формируемых на основе пары порождающих полиномов $f_1(x) = x^9 + x^8 + x^7 + x^2 + 1$ и $f_2(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Ансамбль последовательностей Голда состоит из $L = 2^9 - 1 = 511$ кодовых последовательностей.

По входным символам последовательности Голда устройство декодирования должно определить символы компонент M-последовательностей, описываемых полиномами $f_1(x)$ и $f_2(x)$, а также координаты ненулевых элементов поля $GF(2^n)$, т. е. символов этих компонент. Первообразные полиномы $f_1(x)$ и $f_2(x)$ в данном случае имеют сопровождающие матрицы

а векторы-столбцы координат i-го и j-го символов первой и второй компонент в общем случае имеют вид:

$$X_i = (x_i^0, x_i^1, ..., x_i^{n-1}), X_j = (x_j^0, x_j^1, ..., x_j^{n-1}),$$

где x_i^k и x_j^k — k-е координаты i-го и j-го символов первой и второй компонент соответственно. Символы последовательности Голда являются результатом суммирования по модулю два символов двух сдвинутых относительно друг друга порождающих M-последовательностей

$$a_k = b_i + b_j,$$

где a_k — k-й символ последовательности Голда; b_i и b_j символы M-последовательностей. Можно составить систему из 2n уравнений

$$a_{k} = b_{i} + b_{j};$$

$$a_{k+1} = b_{i+1} + b_{j+1};$$
......
$$a_{k+l} = b_{i+l} + b_{j+l};$$
.....
$$a_{k+2n-1} = b_{i+2n-1} + b_{j+2n-1},$$
(11)

где каждый из символов M-последовательностей в правых частях уравнений определяется с помощью матриц H_1 и H_2 через совокупность координат i-го и j-го символов последовательностей. Используя значение первых строк матриц H_1 и H_2 , в некоторой степени l, соответствующей номеру уравнения в системе из 2n уравнений, можно записать:

$$a_{k+l} = H_{1,1}^l X_i + H_{2,1}^l X_j , \qquad (12)$$

где $H_{1,1}^l$ и $H_{2,1}^l$ — первые строки матриц H_1 и H_2 соответственно.

С учетом того, что $b_{i+1} = x_{i+1}^0$, $b_{j+1} = x_{j+1}^0$ для любого l, решение системы уравнений позволяет определить значение текущих символов порождающих M-последовательностей через совокупность входных символов последовательности Голда, т.е. решить задачу декодирования этой последовательности. Так, символы M-последовательностей, описываемые полиномами $f_1(x)$ и $f_2(x)$, находят с помощью выражений

$$\begin{split} b_i &= x_i^0 = D_{13} a_{k+13} \oplus D_{10} a_{k+10} \oplus D_6 a_{k+6} \oplus D_5 a_{k+5} \oplus D_4 a_{k+4} \oplus D_3 a_{k+3} \oplus D_0 a_k; \\ b_j &= x_j^0 = D_{13} a_{k+13} \oplus D_{10} a_{k+10} \oplus D_6 a_{k+6} \oplus D_5 a_{k+5} \oplus D_4 a_{k+4} \oplus D_3 a_{k+3}, \end{split}$$

где D — весовые коэффициенты.

Соотношения для символов b M-последовательностей можно записать в общей для этих символов компактной форме

$$b = \sum_{l=0}^{2n-1} D_l a_{k+l}. \tag{13}$$

Причем из развернутых соотношений для b_i и b_j следует, что символы M-последовательности, описываемой первым полиномом, определяются с помощью весовых коэффициентов $D_l = 1$ при l = 0, 3, 4, 5, 6, 10, 13, а символы второй <math>M-последовательности, описываемой вторым полиномом, определяются с помощью коэффициентов $D_l = 1$

при l = 3, 4, 5, 6, 10, 13. Для других значений l весовые коэффициенты равны нулю для обеих компонент.

Последовательности малого семейства Касами формируются путем суммирования по модулю два двухкомпонентных M-последовательностей с разными по величине периодами N_1 и N_2 . Длина M-последовательности с меньшим периодом кратна длине M-последовательности с бо́льшим периодом, поэтому период последовательностей малого семейства Касами равен периоду M-последовательности с большим периодом.

Рассмотрим процедуру разложения на компоненты последовательности Касами длиной $2^{10}-1=1023$, (n=10). Всего существует 60 полиномов десятой степени и шесть полиномов пятой степени, порождающих M-последовательности. Возьмем один из 60 полиномов 10-й степени $f(x)=x^{10}+x^3+1$ и рассмотрим шесть полиномов степени n/2=5, которые имеют вид:

$$f(x) = x^{5} + x^{2} + 1;$$

$$f(x) = x^{5} + x^{3} + 1;$$

$$f(x) = x^{5} + x^{3} + x^{2} + x + 1;$$

$$f(x) = x^{5} + x^{4} + x^{2} + x + 1;$$

$$f(x) = x^{5} + x^{4} + x^{3} + x + 1;$$

$$f(x) = x^{5} + x^{4} + x^{3} + x^{2} + 1.$$

Каждая пара полинома десятой степени и одного из полиномов шестой степени порождает малое семейство последовательностей Касами, состоящее из $2^5-1=31$ кодовой последовательности длиной $N=2^{10}-1=1023$ элемента.

Сопровождающие матрицы H_1 и H_2 для порождающих полиномов $x^{10} + x^3 + 1$ и $x^5 + x^4 + x^2 + x + 1$ (четвертый по порядку полином 5-й степени), соответственно, имеют вид:

Возводя матрицы H_1 и H_2 последовательно в степени от 2 до 14, можно получить необходимые в данном случае 3n:2-1=14 первых строк каждой матрицы: $H_{1,1};H_{1,1}^2;...;H_{1,1}^{14}$ и $H_{2,1};H_{2,1}^2;...;H_{2,1}^{14}$. Умножив первые строки матриц H_1 и H_2 в соответствующей степени на векторы-столбцы

$$X_{i} = (x_{i}^{0}, x_{i}^{1}, x_{i}^{2}, x_{i}^{3}, x_{i}^{4}, x_{i}^{5}, x_{i}^{6}, x_{i}^{7}, x_{i}^{8}, x_{i}^{9}), X_{i} = (x_{i}^{0}, x_{i}^{1}, x_{i}^{2}, x_{i}^{3}, x_{i}^{4}),$$

получаем систему из 15 уравнений, связывающую символы последовательностей малого семейства Касами с координатами i-го и j-го символов исходных M-последовательностей:

$$\begin{split} &a_{i} = x_{i}^{0} + x_{j}^{0}; \\ &a_{i+1} = x_{i}^{9} + x_{j}^{4}; \\ &a_{i+2} = x_{i}^{8} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+3} = x_{i}^{7} + x_{j}^{2} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+4} = x_{i}^{6} + x_{j}^{1} + x_{j}^{2} + x_{j}^{3}; \\ &a_{i+5} = x_{i}^{5} + x_{j}^{0} + x_{j}^{1} + x_{j}^{2}; \\ &a_{i+6} = x_{i}^{4} + x_{j}^{0} + x_{j}^{1} + x_{j}^{4}; \\ &a_{i+7} = x_{i}^{3} + x_{j}^{0} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+8} = x_{i}^{2} + x_{i}^{9} + x_{j}^{2} + x_{j}^{3}; \\ &a_{i+9} = x_{i}^{1} + x_{i}^{8} + x_{j}^{1} + x_{j}^{2} + x_{j}^{4}; \\ &a_{i+10} = x_{i}^{0} + x_{i}^{7} + x_{j}^{0} + x_{j}^{1} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+11} = x_{i}^{6} + x_{i}^{9} + x_{j}^{0} + x_{j}^{2} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+12} = x_{i}^{5} + x_{i}^{8} + x_{j}^{1} + x_{j}^{2} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+13} = x_{i}^{4} + x_{i}^{7} + x_{j}^{0} + x_{j}^{1} + x_{j}^{2} + x_{j}^{3} + x_{j}^{4}; \\ &a_{i+14} = x_{i}^{3} + x_{i}^{6} + x_{j}^{0} + x_{j}^{1} + x_{j}^{2} + x_{j}^{3}. \end{split}$$

Решение системы из 15 уравнений относительно x_i^0 и x_j^0 принимает вид

$$x_i^0 = b_i = a_{i+12} + a_{i+5} + a_{i+2} + a_i;$$

$$x_j^0 = b_j = a_{i+12} + a_{i+5} + a_{i+2}.$$
(14)

Из выражения (14) следует, что символы каждой из компонентных M-последовательностей определяются тремя или четырьмя символами входной последовательности малого семейства Касами. Таким образом, принятая последовательность малого семейства Касами может быть разложена на компоненты — исходные M-последовательности.

Решение системы для других пяти полиномов 5-й степени имеет вид:

$$\begin{split} x_i^0 &= b_i = a_{i+14} + a_{i+10} + a_{i+7} + a_{i+4} + a_{i+3}, \\ x_j^0 &= b_j = a_{i+14} + a_{i+10} + a_{i+7} + a_{i+4} + a_{i+3} + a_i; \\ x_i^0 &= b_i = a_{i+13} + a_{i+12} + a_{i+11} + a_{i+6} + a_{i+5} + a_{i+4} + a_{i+3} + a_{i+2} + a_{i+1} + a_i, \\ x_j^0 &= b_j = a_{i+13} + a_{i+12} + a_{i+11} + a_{i+6} + a_{i+5} + a_{i+4} + a_{i+3} + a_{i+2} + a_{i+1}; \\ x_i^0 &= b_i = a_{i+14} + a_{i+12} + a_{i+11} + a_{i+10} + a_{i+7} + a_{i+5} + a_{i+3} + a_{i+2} + a_{i+1}, \\ x_j^0 &= b_j = a_{i+14} + a_{i+12} + a_{i+11} + a_{i+10} + a_{i+7} + a_{i+5} + a_{i+3} + a_{i+2} + a_{i+1} + a_i; \\ x_i^0 &= b_i = a_{i+14} + a_{i+12} + a_{i+10} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+3} + a_{i+2}, \\ x_j^0 &= b_j = a_{i+14} + a_{i+12} + a_{i+10} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+3} + a_{i+2} + a_i; \\ x_i^0 &= b_i = a_{i+14} + a_{i+12} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+2} + a_i, \\ x_j^0 &= b_j = a_{i+14} + a_{i+12} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+2} + a_i, \\ x_j^0 &= b_j = a_{i+14} + a_{i+12} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+2} + a_i, \\ x_j^0 &= b_j = a_{i+14} + a_{i+12} + a_{i+7} + a_{i+5} + a_{i+4} + a_{i+2} + a_i. \end{split}$$

Выбранный вариант сигнала Касами при $f(x) = x^{10} + x^3 + 1$ и $f(x) = x^5 + x^4 + x^2 + x + 1$ с минимальным числом символов, равным трем и четырем, определяющих x^0_i и x^0_j соответственно, является оптимальным с точки зрения минимизации вероятности ошибочной оценки символов на выходах схемы разложения на компонентные M-последовательности.

Заключение. В соответствии с изложенной выше методикой разложения кодовых последовательностей на компоненты устройство декодирования работает следующим образом. Входные символы принимаемой кодовой последовательности поступают на регистр, а затем с учетом результата решения системы уравнений (11) — на сумматоры по модулю два. Число сумматоров определяется числом компонент (порождающих *М*-последовательностей), формирующих на передающей стороне принимаемую кодовую последовательность. На выходе каждого из сумматоров проводится разложение принимаемой кодовой последовательности на компоненты (*М*-последовательности), т.е. определяются символы каждой из компонент. Для рассмотренного в работе примера с последовательностью Голда эти символы находят с помощью выражения (13). С выходов сумматоров

на дальнейшую обработку поступают символы компонентных M-последовательностей. Методика нахождения символов компонент универсальна, т.е. может быть использована для декодирования различных кодовых последовательностей, сформированных на основе двух и более M-последовательностей любой длины.

Проведенное исследование показало возможность декодирования сложных кодовых последовательностей. Предложенная методика декодирования позволяет разложить любую входную кодовую последовательность, сформированную на основе двух *М*-последовательностей и более, на компоненты. При последующей обработке символов компонент с учетом упорядоченного характера векторов координат этих символов может быть решена задача синхронизации и распознавания принимаемой входной последовательности. Результаты работы могут быть использованы для создания устройств обработки сигналов в системах передачи информации с шумоподобными сигналами.

ЛИТЕРАТУРА

- [1] Васин В.А. [др.]. Информационные технологии в радиотехнических системах. И.Б. Федоров, ред. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2003, 672 с.
- [2] Варакин Л.Е. Системы связи с шумоподобными сигналами. Москва, Радио и связь, 1985, 384 с.
- [3] Гантмахер В.Е., Быстров Н.Е., Чеботарев Г.В. ШПС: Анализ, синтез, обработка. Санкт-Петербург, Наука и техника, 2005, 400 с.
- [4] Свердлик М.Б. Оптимальные дискретные сигналы. Москва, Сов. радио, 1975, 199 с.

Статья поступила в редакцию 25.03.2013

Ссылку на эту статью просим оформлять следующим образом:

Косолапов А.С., Галев А.В. Исследование возможности декодирования сложных кодовых последовательностей. *Инженерный журнал: наука и инновации*, 2014, вып. 1. URL: http://engjournal.ru/catalog/pribor/radio/1170.html

Косолапов Андрей Сергеевич родился в 1939 г., окончил МВТУ им. Н.Э. Баумана в 1962 г. Канд. техн. наук, доцент кафедры «Радиоэлектронные системы и устройства» факультета «Радиоэлектроника и лазерная техника» МГТУ им. Н.Э. Баумана. Автор более 100 научных работ, изобретений и учебных пособий. Область научных интересов: исследование структурных свойств широкополосных сигналов и их обработка. e-mail: a.s.kosolapov@mail.ru

Галев Александр Викторович родился в 1946 г., окончил МВТУ им. Н.Э. Баумана в 1970 г. Канд. техн. наук, доцент кафедры «Радиоэлектронные системы и устройства» факультета «Радиоэлектроника и лазерная техника» МГТУ им. Н.Э. Баумана. Автор более 100 научных работ, изобретений и учебных пособий. Область научных интересов: исследование структурных помех при использовании широкополосных сигналов и их оценка. e-mail: agalev2@yandex.ru