

УДК 621.396

Декодирование составных кодовых последовательностей

Второв А.В., дипломант

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Радиоэлектронные системы и устройства»*

Научный руководитель: Косолапов А.С., к.т.н., доцент

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

a.s.kosolapov@mail.ru

main@rl1-11.bmstu.ru

Работа многих радиотехнических систем возможна только после обеспечения синхронизации всех звеньев системы. Процедура синхронизации обычно заключается в поиске сигнала на временной оси и определении его задержки по отношению к сигналу местного опорного генератора на приемной стороне [1]. Применительно к двоичным псевдослучайным последовательностям процесс вхождения в синхронизм заключается в определении фазы принимаемой последовательности.

Существует метод последовательной оценки Уорда [2]. Данный метод основан на алгебраических особенностях псевдослучайных сигналов и заключается в определении принятых подряд символов входной последовательности и в их использовании в качестве начальных условий опорного генератора на приёмной стороне. Критерием правильности принятых символов опорной выборки является работа генератора в фазе с приходящим сигналом. Если оценка символов была сделана неверно, например, была допущена ошибка в оценке хотя бы одного символа, то делается новая попытка установления синхронизации. Каждая загрузка генератора в методе последовательной оценки требует большого времени анализа, что увеличивает время вхождения в синхронизм. Можно увеличить эффективность метода, используя структурные свойства псевдослучайных последовательностей. Так для оценки принимаемых символов M -последовательности, достаточно принять отрезок последовательности длиной N символов и использовать его в качестве начальных условий опорного генератора [1].

Метод последовательной оценки является весьма эффективным при средних значениях отношения $\frac{\text{сигнал}}{\text{шум}}$ и не высоких скоростях процесса вхождения в синхронизм. По-

казано [2], что значительное сокращение времени распознавания при использовании данного метода наблюдается для значений отношения $\frac{\text{сигнал}}{\text{шум}}$ вплоть до -15 дБ.

Но метод, предложенный Уордом, не пригоден для декодирования составных кодовых последовательностей, таких как последовательности Голда, последовательности Касами и др. [3]. В работах [4], [5] рассмотрен метод синхронизации и распознавания составных кодовых последовательностей, основанный на использовании основных положений теории полей Галуа. Известно, что полная система вычетов по двойному модулю $\text{modd}(f(x), p)$ образует расширенное поле Галуа, содержащее p^n элементов, которое обозначают через $GF(q^s)$, где $q = p^n$, p – простое число, s – расширение поля [6], [7]. При $s = 1$ $GF(p^n)$ и поле в этом случае называется простым. В случае двоичных М-последовательностей $p = 2$, а элементами простого поля являются числа 0 и 1. Элементами $GF(2^n)$ являются многочлены степени не выше $n-1$ с коэффициентами из поля $GF(2)$:

$$R(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0.$$

Элементы поля Галуа $GF(2^n)$ можно записать в виде многочленов $R(x)$ и в виде степеней первообразного элемента θ^i , $i=0, 1, \dots, 2^n-2$. Первообразный элемент имеет максимально возможный период, а его степени пробегают все ненулевые элементы поля. Нулевой элемент поля не входит в мультипликативную группу поля.

Каждый элемент поля может быть представлен в виде:

$$c = \omega_0x_0 + \omega_1x_1 + \omega_{n-1}x_{n-1},$$

где x_i ; $i=0, 1, \dots, n-1$ – координаты элемента c в заданном базисе $\Omega = (\omega_0, \omega_1, \dots, \omega_{n-1})$.

Если Ω состоит из элементов $\omega_i = \theta^i$, $i=0, 1, \dots, n-1$, где θ – корень первообразного неприводимого над полем $GF(2^n)$ полинома $f(x)$ степени n , то $\Omega = (\theta^0, \theta^1, \dots, \theta^{n-1})$ называется натуральным базисом поля $GF(2^n)$.

Тогда $c = \Omega \cdot X$, где $X = (x_0, x_1, \dots, x_{n-1})^T$ – n -мерный вектор-столбец координат.

Справедливо матричное уравнение:

$$X_{i+l} = H^l \cdot X_i \quad (1)$$

где X_{i+l} и X_i – n -мерные векторы-столбцы координат элементов θ^{i+l} и θ^i поля $GF(2^n)$, H – невырожденная сопровождающая матрица порядка n полинома $f(x)$ в натуральном базисе, с помощью которой можно найти координаты $(i+l)$ -го элемента, если известны координаты i -го элемента.

Матричное уравнение (1) можно представить в виде:

$$\begin{pmatrix} x_{i+l}^0 \\ x_{i+l}^1 \\ \dots \\ x_{i+l}^k \\ \dots \\ x_{i+l}^{n-1} \end{pmatrix} = H^l \cdot \begin{pmatrix} x_i^0 \\ x_i^1 \\ \dots \\ x_i^k \\ \dots \\ x_i^{n-1} \end{pmatrix}, \quad (2)$$

где X_{i+l} и X_i записаны в виде n -мерных векторов-столбцов координат, причём k -я координата любого элемента принимает значение 0 или 1.

Выражение для матрицы H в натуральном базисе имеет вид:

$$H = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ 0 & 0 & 1 & \dots & 0 & a_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix},$$

где a_i ; $i=0, 1, \dots, n-1$ – коэффициенты при степенях x^j ; $j=0, 1, \dots, n$ многочлена $f(x)$ степени n :

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Выражение (2) показывает, что каждый элемент поля $GF(2^n)$ характеризуется своим персональным вектором-столбцом координат, а все элементы поля взаимосвязаны.

Нулевые координаты ненулевых элементов поля являются символами М-последовательности, причем $x_i^0 = b_i$, где b_i – символ последовательности.

Задача синхронизации должна решаться за время поступления на вход приёмного устройства ограниченного числа символов М-последовательности. Однако для этого недостаточно знать только некоторую совокупность принятых символов, т.к. по ней невозможно определить номера текущих символов. Известно, что по совокупности n символов М-последовательности при условии, что эти символы распознаны без ошибок, можно сформировать поступающую на вход М-последовательность [3]. Однако её фаза не будет определена. Ненулевые элементы поля $GF(2^n)$ обладают n -мерными векторами координат $X = (x_0, x_1, \dots, x_{n-1})^T$. Тогда для определения номера символа М-последовательности, а следовательно и её фазы целесообразно воспользоваться не только значениями принимаемых символов, но и совокупностью значений всех координат этих символов, как элементов поля $GF(2^n)$.

Таким образом, задача определения фазы принимаемой М-последовательности сводится к определению вектора-столбца координат принимаемого символа последовательности и последующего определения по этому вектору номера символа.

Текущие значения векторов-столбцов координат должны быть связаны с предшествующими значениями, исходя из матричного уравнения (1). Следовательно, критерием правильного распознавания входной последовательности является упорядоченный характер серии векторов-столбцов координат.

Из-за воздействия помех оценка принимаемых символов М-последовательности может оказаться ошибочной. Это в свою очередь приводит к ошибкам в определении векторов-столбцов координат. Для минимизации этих ошибок можно использовать мажоритарную оценку входных символов. Значение каждого символа принимается по большинству, исходя из проверочных уравнений, составляемых для этого символа на длине последовательности в специальном блоке проверочных уравнений (БПУ) [8]. Максимальное

количество проверочных уравнений m_{max} определяется по формуле $m_{max} = \frac{N-1}{2}$, где

$N = 2^n - 1$ – длина последовательности.

Вероятность ошибочной оценки символов на выходе БПУ определяется выражением:

$$P_y = 2P_3(1 - P_3),$$

где P_3 – вероятность ошибочной оценки принимаемых символов.

График зависимости вероятности ошибочной оценки символов М-последовательности на выходе БПУ от вероятности ошибочной оценки входных символов представлен на рисунке 1.

С выхода блока проверочных уравнений символы поступают на мажоритарный элемент, который уменьшает вероятность ошибочной оценки символов до величины:

$$P_{мэ} = \sum_{r=\frac{m+1}{2}}^m C_m^r P_y^r (1 - P_y)^{m-r}, \quad (3)$$

где $P_{мэ}$ – вероятность ошибочной оценки символов на выходе мажоритарного элемента,

C_m^r – число сочетаний из m по r (биномиальный коэффициент).

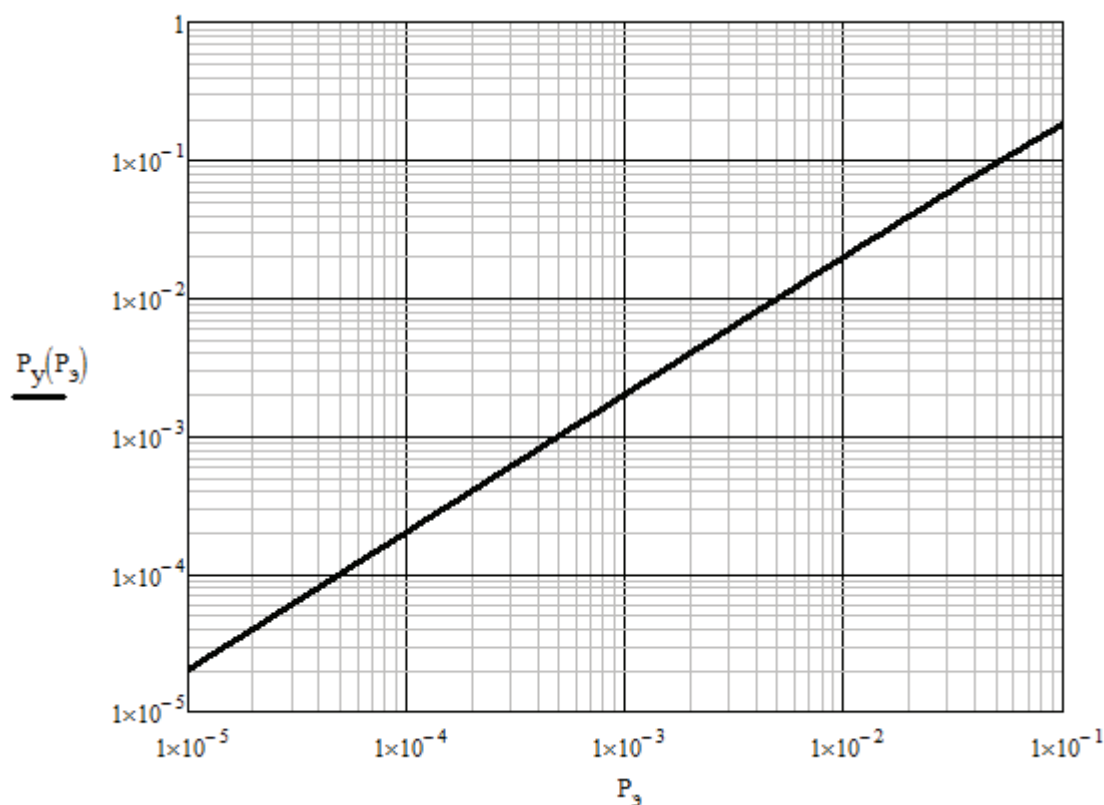


Рис. 1. Зависимость вероятности ошибочной оценки символов на выходе БПУ от вероятности ошибочной оценки принимаемых символов

На рисунке 2 представлена зависимость вероятности ошибочной оценки символов на выходе мажоритарного элемента от количества проверочных уравнений m при значе-

ниях $P_{\varepsilon} = 10^{-5} \div 10^{-1}$. Из выражения (3) видно, что количество проверочных уравнений должно быть нечетным. Очевидно, что при уменьшении вероятности ошибочной оценки принимаемых символов значения $P_{\text{мэ}}$ будут также уменьшаться, причем на более высокие порядки.

Выборка из n символов на выходе мажоритарного элемента может быть использована для определения координат текущего элемента поля $GF(2^n)$.

Описанный метод синхронизации и распознавания М-последовательностей также применим и для составных кодовых последовательностей, построенных на их основе, таких как последовательность Голда и Касами. При этом необходимо разложить составную последовательность на компоненты, которые затем могут быть обработаны каждая в своём канале в соответствии с вышеизложенным методом [9], [5]. Т.е. устройство синхронизации и распознавания становится многоканальным.

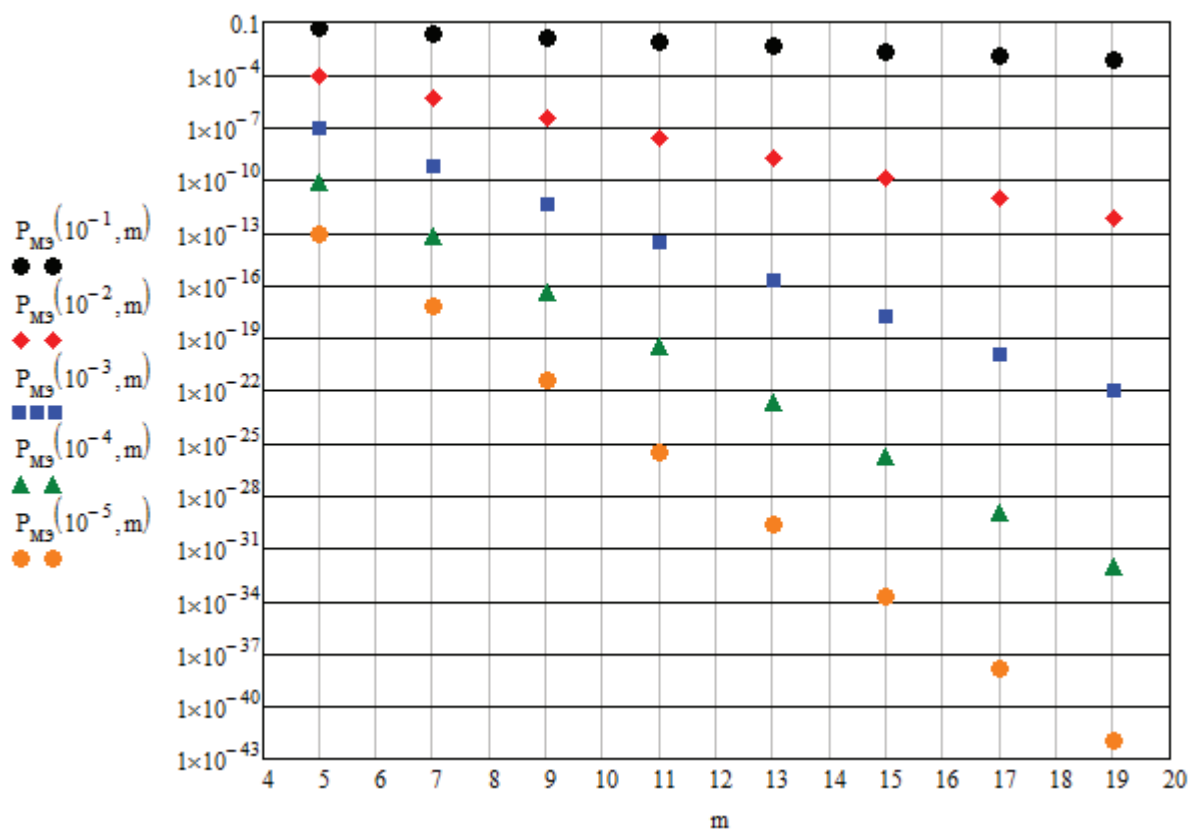


Рис. 2. Зависимость вероятности ошибочной оценки символов на выходе мажоритарного элемента от количества проверочных уравнений при различных значениях вероятности ошибочной оценки принимаемых символов

Рассмотрим процедуру разложения составной кодовой последовательности на примере последовательности малого семейства Касами. Символы данной последовательности получаются путём суммирования по модулю два символов двух М-последовательностей (со степенями порождающих многочленов n и $\frac{n}{2}$ соответственно):

$$a_k = b_i \oplus b_j, \quad (4)$$

где a_k – k -ый символ последовательности Касами, b_i – i -ый символ первой М-последовательности, b_j – j -ый символ второй М-последовательности.

Степень порождающего многочлена последовательности Касами определяется суммой степеней двух порождающих М-последовательности многочленов, т.е. равна $\frac{3n}{2}$.

На основании выражения (4) можно составить систему из $\frac{3n}{2}$ уравнений:

$$\begin{aligned} a_k &= b_i \oplus b_j; \\ a_{k+1} &= b_{i+1} \oplus b_{j+1}; \\ &\dots\dots\dots \\ a_{k+l} &= b_{i+l} \oplus b_{j+l}; \\ &\dots\dots\dots \\ a_{k+\frac{3n}{2}-1} &= b_{i+\frac{3n}{2}-1} \oplus b_{j+\frac{3n}{2}-1}; \end{aligned} \quad (5)$$

Символы b_i и b_j М-последовательностей представляют собой совокупность нулевых координат ненулевых элементов поля $GF(2^n)$. Тогда, используя матричное уравнение (1) и сопровождающие матрицы многочленов, можно записать:

$$\begin{aligned} b_{i+l} &= H_{1,1}^l \cdot X_i; \\ b_{j+l} &= H_{2,1}^l \cdot X_j, \end{aligned} \quad (6)$$

где $b_i = x_i^0$, $b_j = x_j^0$, $H_{1,1}^l$ и $H_{2,1}^l$ – первые строки матриц H_1 и H_2 в степени l компонентных М-последовательностей.

С учетом (6) перепишем систему уравнений (5):

$$\begin{aligned}
a_k &= b_i \oplus b_j; \\
a_{k+1} &= H_{1,1} X_i \oplus H_{2,1} X_j; \\
&\dots\dots\dots \\
a_{k+l} &= H_{1,1}^l X_i \oplus H_{2,1}^l X_j; \\
&\dots\dots\dots \\
a_{k+\frac{3n-1}{2}} &= H_{1,1}^{\frac{3n-1}{2}} X_i \oplus H_{2,1}^{\frac{3n-1}{2}} X_j.
\end{aligned} \tag{7}$$

Из системы уравнений (7) видно, что количество уравнений в системе равно суммарному количеству всех координат элементов полей $GF(2^n)$ и $GF\left(2^{\frac{n}{2}}\right)$, соответствующим двум М-последовательностям. Следовательно, можно решить систему уравнений (7) относительно нулевых координат $x_i^0 = b_i$ и $x_j^0 = b_j$.

Подобным образом решается задача разложения любой составной кодовой последовательности на компоненты.

Вероятность ошибочной оценки символов на выходе схемы разложения определяется следующей формулой:

$$P_p = \sum_{r=1}^{r \leq d} C_d^r P_{\text{ex}}^r (1 - P_{\text{ex}})^{d-r}, \tag{8}$$

где d – число символов последовательности Касами, определяющих нулевые координаты x_i^0 и x_j^0 двух М-последовательностей, r – нечетные числа от 1 до d ($r \leq d$), P_{ex} – вероятность ошибочной оценки символов на входе схемы разложения, C_d^r – число сочетаний из r по d . На рисунке 3 представлена зависимость вероятности ошибочной оценки символов на выходе схемы разложения от вероятности ошибочной оценки символов на входе при различных значениях d .

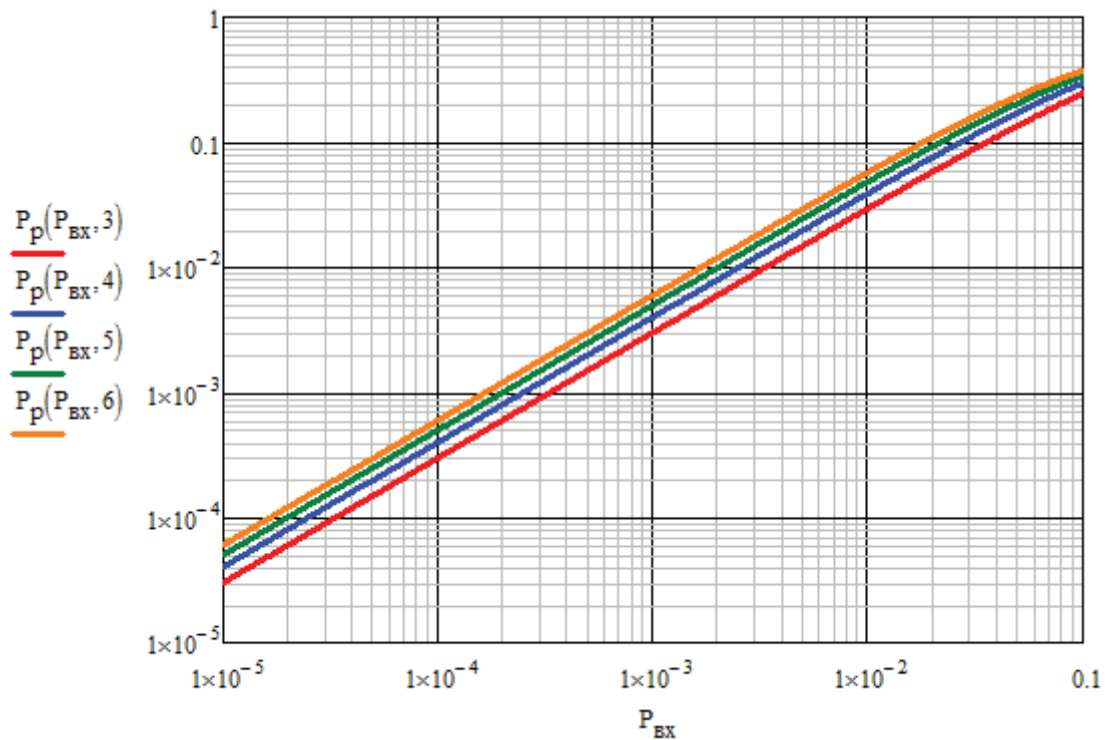


Рис. 3. Зависимость вероятности ошибочной оценки символов на выходе схемы разложения от вероятности ошибочной оценки символов на входе при $d = 3 \div 6$

Разложение последовательности Касами на компоненты увеличивает вероятность ошибочной оценки символов b_i и b_j компонентных М-последовательностей, по сравнению с вероятностью ошибочной оценки принимаемых символов последовательности Касами. Это видно из решения системы уравнений (7) и рисунка 3. Символы b_i и b_j определяются суммой входных символов последовательности Касами. С ростом числа символов последовательности Касами, определяющих нулевые координаты x_i^0 и x_j^0 , также растет и вероятность ошибочной оценки символов на выходе схемы разложения. Избежать увеличения вероятности ошибочной оценки символов b_i и b_j можно, применив мажоритарную оценку входных символов последовательности до процедуры её разложения на компоненты. Но это возможно не для всех пар М-последовательностей, формирующих последовательность Касами.

Рассмотрим последовательность малого семейства Касами, формируемого двумя М-последовательностями с порождающими многочленами: $f_1(x) = x^{10} + x^3 + 1$ и $f_2(x) = x^5 + x^4 + x^2 + x + 1$. Матрица H , соответствующая многочлену

$$f(x) = f_1(x) \cdot f_2(x) = x^{15} + x^{10} + x^9 + x^7 + x^3 + x^2 + 1$$

имеет вид:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

С помощью этой матрицы строятся векторы-столбцы координат всех элементов поля размерностью 2^{15} (но это не элементы поля $GF(2^{15})$). По аналогии с нумерацией элементов поля Галуа для М-последовательностей, начальный элемент введенного в рассмотрение поля обозначим вектором – столбцом координат

$$(1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)^T.$$

Последующие векторы-столбцы координат определяются с помощью выражения (2).

Для построенных векторов-столбцов координат проверялось существование проверочных уравнений. Оказалось, что можно построить 30 проверочных уравнений на длине последовательности Касами, равной 977 символов.

Всего насчитывается 60 многочленов, порождающих М-последовательности длиной $N_1 = 1023$ символа и 6 длиной $N_2 = 31$ символ, т.е. можно сформировать 360 семейств малых последовательностей Касами. Но не для всех из них существуют проверочные уравнения. Каждый многочлен 10-й степени со всеми многочленами 5-й степени образует три семейства, для которых не существует проверочных уравнений, для одного се-

мейства можно построить 15 проверочных уравнений и для двух семейств — 30 проверочных уравнений.

Функциональная схема устройства декодирования составных кодовых последовательности малого семейства Касами представлена на рис. 4. На вход РГ1 поступают символы последовательности Касами. Число записываемых в РГ1 символов последовательности определяется требуемым количеством проверочных уравнений. С выхода РГ1 символы поступают на вход блока проверочных уравнений (БПУ1), а затем на вход МЭ1, где производится мажоритарная оценка принятых символов. С выхода МЭ1 символы записываются в РГ2. В схеме используется блок разложения (БР), в котором на основе решения системы уравнений (5) определяются координаты x_i^0 и x_j^0 компонентных М-последовательностей. После блока разложения система становится двухканальной. Текущие символы М-последовательностей записываются в РГ3 и РГ4 для последующей обработки. В дальнейшем символы компонентных М-последовательностей, поступающие с выходов регистров РГ5 и РГ6 используются для синхронизации и распознавания составной кодовой последовательности Касами.

Учитывая, что последовательность малого семейства Касами формируется путем суммирования по модулю два двух М-последовательностей, причём более короткая М-последовательность сдвигается относительно другой, опорной М-последовательности, можно определить фазу последовательности Касами, измеряя её сдвиг по номеру i -го символа опорной М-последовательности.

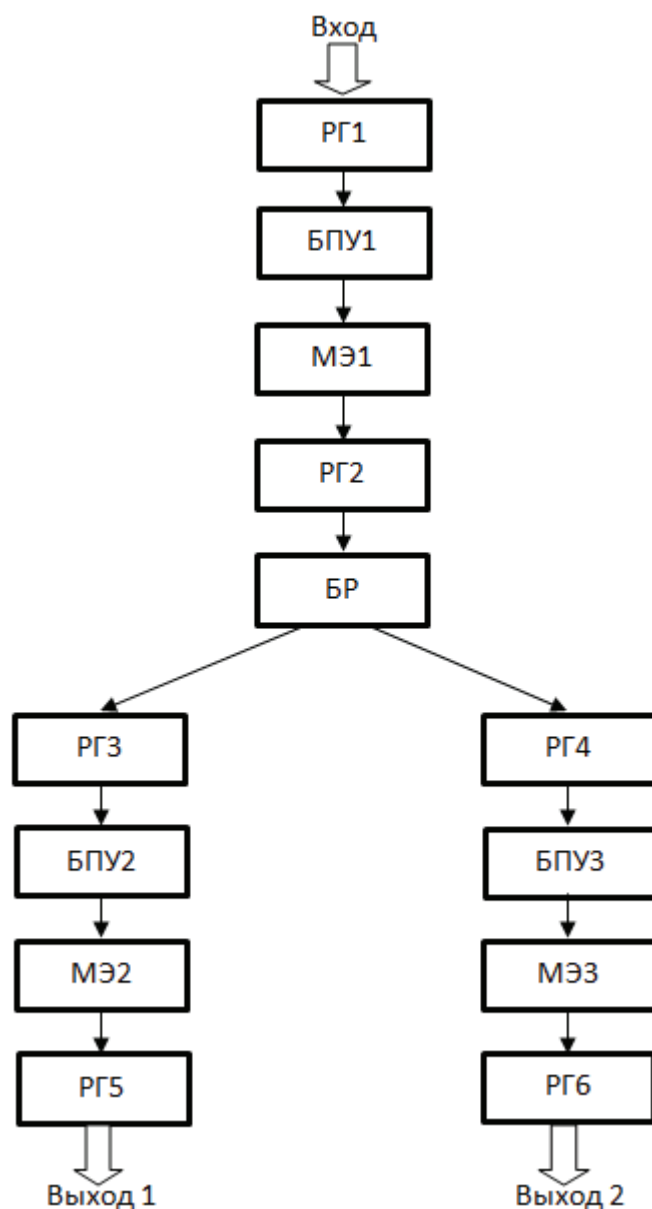


Рис. 4. Функциональная схема устройства декодирования кодовых последовательностей малого семейства Касами

Обозначив через j номер символа второй М-последовательности, рассчитанный в другом канале обработки, можно записать:

$$Z = [i - j(\text{mod } N_2)](\text{mod } N_2),$$

где Z – сдвиг между компонентными М-последовательностями, т.е. номер опознанной принятой последовательности Касами.

Таким образом решается задача синхронизации и распознавания принимаемой составной кодовой последовательности.

В работе рассмотрен метод декодирования составных кодовых последовательностей, основанный на использовании теории полей Галуа. Данный метод может использоваться для распознавания и синхронизации сигналов, обладающих сходной описанной в работе структурой, таких, как например последовательности малого и большого семейства Касами и последовательности Голда.

Список литературы

1. Лосев В.В. Методы синхронизации по задержке. (Обзор) // Изв. вузов СССР. Радиоэлектроника, 1979, т. 22, № 1. С. 3–13.
2. Уорд Р. Различение псевдошумовых сигналов методом последовательной оценки // За-рубежная радиоэлектроника, 1966, № 8, С. 20–37.
3. Варакин Л.Е. Системы связи с шумоподобными сигналами. — М.: Радио и связь. 1985. 384 с.
4. Косолапов А.С., Галев А.В. Исследование возможности декодирования сложных кодовых по-следовательностей // Инженерный журнал: наука и инновации, 2014, вып. 1. Режим досту-па: <http://engjournal.ru/catalog/pribor/radio/1170.html> (дата обращения: 20.01.2014).
5. Косолапов А.С., Тимошенков В.Ф., Наумкин С.И. О распознавании последовательно-сти Голда // Техника средств связи, серия техника связи. 1989. Вып. 1. С. 20–26.
6. Постников М.М. Теория Галуа. М.: Изд-во Физ-мат. литература, 1963. 220 с.
7. Чеботарев Н.Г. Основы теории Галуа. Ч.1. М.: Изд-во ЁЁ Медиа, 2012. 221 с.
8. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир. 1971.
9. А.с. 1295527 (СССР). Система декодирования двоичных последовательностей / А.С. Косолапов. Зарегистрировано в реестре изобретений СССР. 1986 г.