

Кукунин Д.С.

Руководство к курсовой работе

«Цикловое фазирование в системе передачи данных при помощи *M*-последовательностей»

СОДЕРЖАНИЕ

Раздел 1. Цели и задачи курсовой работы.....	3
1.1. Цель.....	3
1.2. Задачи	3
1.2.1. Построение поля Гауа	4
1.2.2. Определение элементов двойственного базиса поля Гауа	5
1.2.3. Построение рекуррентных M -последовательностей и КЦФ.....	6
1.2.4. Внесение ошибок в КЦФ	7
1.2.5. Обработка M -последовательностей при помощи двойственного базиса поля Гауа	7
1.3. Варианты заданий.....	12
1.4. Содержание и форма отчета	12
Раздел 2. Пример отчета по выполненной курсовой работе	14
2.1. Исходные данные	14
2.2. Проведение расчетов.....	14
2.2.1. Построение поля Гауа	14
2.2.2. Вычисление элементов двойственного базиса поля Гауа	15
2.2.3. Формирование M -последовательностей.....	15
2.2.4. Выделение КЦФ	17
2.2.5. Выводы по результатам выполнения курсовой работы.....	18
ЛИТЕРАТУРА	20

Раздел 1. Цели и задачи курсовой работы

1.1. Цель

Целью курсовой работы является изучение вопросов, связанных с методами циклового фазирования в синхронных и асинхронных системах передачи данных. В результате ее выполнения студенты приобретают опыт работы с математическим аппаратом, который в полной мере затрагивает теорию полей Галуа, теорию двойственного базиса поля Галуа, теорию кодирования, а также теорию рекуррентных регистров сдвига.

Навыки, полученные при проведении расчетов, будут полезны при проектировании и изучении современных систем передачи данных, в которых особое место отведено рекуррентным последовательностям.

1.2. Задачи

Основной задачей циклового фазирования в системе передачи данных является выделение специальной комбинации цикловой фазы (КЦФ), в качестве которой может выступать рекуррентная M -последовательность с известными начальными элементами.

Выбор M -последовательностей в качестве КЦФ обусловлен их хорошими корреляционными свойствами.

При синхронной передаче данных процедура циклового фазирования во времени состоит из двух этапов: на первом этапе осуществляется поиск (обнаружение или распознавание) КЦФ, а на втором – контроль и поддержание синхронизма. Передача информации осуществляется циклами длиной N , в каждом из которых в начале следует КЦФ, а затем поле данных (рис. 1).

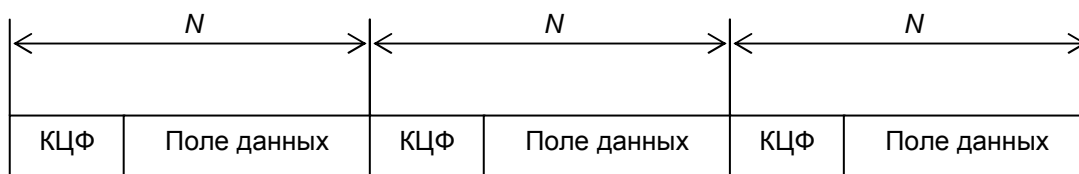


Рис. 1. Структура циклов в синхронной системе передачи данных

При асинхронной передаче данных циклы разделены во времени, каждый блок данных также сопровождается КЦФ, которую необходимо определить, но поддержка синхронизма не требуется (рис 2).



Рис. 2. Структура циклов в асинхронной системе передачи данных

В обоих случаях необходимо решать задачу поиска и распознавания КЦФ при том, что начало по времени данной комбинации на приемной стороне не известно.

Поиск КЦФ предполагает обработку участков M -последовательности при помощи двойственного базиса поля Галуа, поэтому одной из основных задач курсовой работы является определение элементов двойственного базиса.

В данной курсовой работе предполагается провести анализ системы передачи данных в течение одного цикла. Цикловое фазирование обеспечивается появлением КЦФ, которая передается по каналу связи с ошибками. Ошибочные разряды определяются в задании на курсовую работу (п. 2).

Таким образом, требуется сгенерировать соответствующую КЦФ. Для этого сначала необходимо построить поле Галуа, что является первой задачей курсовой работы.

Обработка M -последовательностей двойственным базисом производится с целью определения конечного элемента КЦФ и момента начала приема блока данных.

1.2.1. Построение поля Галуа

Поле называется коммутативное кольцо с единичным элементом относительно умножения, в котором каждый ненулевой элемент имеет мультипликативный обратный элемент (обратный по умножению).

Поля с конечным числом элементов q называют полями Галуа и обозначают $GF(q)$. Число элементов поля q называют порядком поля. В зависимости от значения q различают простые или расширенные поля. Поле называется простым, если q – простое число. В данной работе из простых полей используется только двоичное поле $GF(2)$, образованное двумя единичными элементами: “0” – относительно операции сложения и “1” – относительно операции умножения. Из расширенных полей $GF(p^k)$, где характеристика p является простым числом, в данной работе рассматриваются конечные поля $GF(2^k)$.

Ненулевые элементы поля $GF(2^k)$ образуют ряд:

$$1, \varepsilon, \varepsilon^2, \varepsilon^3, \dots, \varepsilon^{2^k-2}. \quad (1)$$

Каждый ненулевой элемент поля Галуа можно представить в виде степени первообразного элемента ε , который, в свою очередь, является корнем характеристического многочлена:

$$P(x) = p_0x^k + p_1x^{k-1} + \dots + p_{k-1}x + p_k, p_j \in \text{GF}(2). \quad (2)$$

Многочлен (2) является неприводимым примитивным многочленом, входящим в разложение двучлена $(x^{2^k} - 1 + 1)$ на неприводимые сомножители.

Часть характеристического многочлена без старшей степени называется вычетом и непосредственно используется при построении поля Галуа, как показано в примере выполнения курсовой работы (Раздел 2).

1.2.2. Определение элементов двойственного базиса поля Галуа

Любые k элементов ряда (1) являются линейно-независимыми над $\text{GF}(2)$ и могут образовывать базис поля $\text{GF}(2^k)$:

$$[\varepsilon^g, \varepsilon^{g+1}, \varepsilon^{g+2}, \dots, \varepsilon^{g+k-1}]. \quad (3)$$

Таким образом, любой элемент поля $\text{GF}(2^k)$ можно выразить через различные базисы, в том числе левый степенной и двойственный ему базис.

Левый степенной базис поля $\text{GF}(2^k)$ представляет собой набор из k последовательных элементов ряда (3) при $g=0$:

$$[1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{k-1}]. \quad (4)$$

Произвольный элемент ε^j поля $\text{GF}(2^k)$ выражается через левый степенной базис следующим образом:

$$\varepsilon^j = a_0 + a_1\varepsilon + a_2\varepsilon^2 + \dots + a_{k-1}\varepsilon^{k-1}, a_i \in \text{GF}(2). \quad (5)$$

Последовательность элементов левого степенного базиса (4), через которые выражен элемент ε^j поля $\text{GF}(2^k)$, можно записать в виде индексированного ряда, где каждому элементу соответствует α_i :

$$\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k. \quad (6)$$

Для перехода к рассмотрению базиса, двойственного левому степенному (6), введем понятие функции след.

Пусть построено поле $\text{GF}(2^k)$. Для любого элемента ε из этого поля функция след $T(\varepsilon)$ определяется по формуле [1]:

$$T(\varepsilon) = \varepsilon + \varepsilon^2 + \varepsilon^{2^2} + \dots + \varepsilon^{2^{k-1}}. \quad (7)$$

Для базиса (6) существует двойственный базис:

$$\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_k. \quad (8)$$

Этот базис можно построить с учетом свойства [4]:

$$T(\lambda_i \alpha_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}. \quad (9)$$

Для левого степенного базиса поля $GF(2^k)$ (6) элементы двойственного базиса λ_ρ определяется по формуле [1]:

$$\lambda_\rho = \frac{\sum_{l=0}^{k-\rho} p_{k-\rho-l} \varepsilon^l}{P'(\varepsilon)}, \quad GF(2^k), \rho=1, 2, \dots, k, \quad (10)$$

где $P'(\varepsilon)$ – значение производной характеристического многочлена $P(x)$ в точке, соответствующей примитивному элементу поля $GF(2^k)$.

Таким образом, любой элемент ε^j поля $GF(2^k)$ можно выразить не только через левый степенной (6), а также через двойственный ему базис:

$$\varepsilon^j = b_0 \lambda_1 + b_1 \lambda_2 + b_2 \lambda_3 + \dots + b_{k-1} \lambda_k, \quad b_i \in GF(2). \quad (11)$$

Элементы двойственного базиса поля Галуа в дальнейшем будут использованы при обработке M -последовательностей.

1.2.3. Построение рекуррентных M -последовательностей и КЦФ

Любая M -последовательность $\{S\}$ может быть построена при помощи характеристического многочлена $P(x)$ степени k (2) и является циклическим $(2^k-1, k)$ -кодом, каждая комбинация которого удовлетворяет рекуррентному уравнению:

$$S_{l+m} = p_1 S_{l+m-1} + p_2 S_{l+m-2} + \dots + p_m S_l, \quad l = 0, 1, 2, \dots \quad (12)$$

Генератор последовательности $\{S\}$ может быть построен на основе простого регистра с вынесенными сумматорами, как показано в примере выполнения курсовой работы (Раздел 2).

Рекуррентная последовательность $\{S\}$ также может быть построена на основе функций след от подряд идущих элементов поля:

$$\{S\} = [T(\varepsilon^g), T(\varepsilon^{g+1}), T(\varepsilon^{g+2}), \dots, T(\varepsilon^{g+2^k-2})], \quad (13)$$

где элемент ε^g является так называемой начальной фазой рекуррентной последовательности. В случае, если в формуле (13) $g=0$, мы получаем каноническую рекуррентную последовательность:

$$\{S\} = [T(1), T(\varepsilon), T(\varepsilon^2), \dots, T(\varepsilon^{2^k-2})]. \quad (14)$$

Построенная рекуррентная последовательность с заданной начальной фазой может быть выбрана в качестве КЦФ. При этом необходимо учесть, что приемная часть не обладает информацией о моменте поступления на вход рекуррентной последовательности и не знает, когда завершится ее период. Поэтому система ведет постоянный поиск КЦФ и

производит обработку двойственным базисом поступающих на вход k -элементных участков, пока не будет принято решение о появлении КЦФ.

Рекуррентная M -последовательность является циклически замкнутой комбинацией и содержит n возможных k -элементных участков. Для их последовательной обработки дополним период КЦФ следующими $k-1$ элементами так, что КЦФ будет иметь вид:

$$\{S\}_{КЦФ} = [T(\varepsilon^g), T(\varepsilon^{g+1}), T(\varepsilon^{g+2}), \dots, T(\varepsilon^{g+2^k-2}), T(\varepsilon^g), T(\varepsilon^{g+1}), \dots, T(\varepsilon^{g+k-1})], \quad (15)$$

где элемент ε^g является начальной фазой КЦФ. Это позволит обработать полный период M -последовательности без знания ее границ.

1.2.4. Внесение ошибок в КЦФ

В соответствии с заданием для каждого варианта определена КЦФ. При передаче по каналу КЦФ подвергается воздействию ошибок. Так по заданию для КЦФ указаны ошибочные разряды (от 0 до $n+k-2$). Рекуррентная последовательность $\{S\}_{КЦФ}$ должна быть сложена с вектором ошибки $\{e\}$ по mod 2:

$$\{H\} = \{S\}_{КЦФ} \oplus \{e\}. \quad (16)$$

В дополнение к этому по заданию в начало КЦФ добавляются случайные разряды, которые обеспечивают случайный порядок появления КЦФ и блока данных. Полученная в (16) последовательность $\{H\}$ подвергается обработке двойственным базисом поля Галуа.

1.2.5. Обработка M -последовательностей при помощи двойственного базиса поля Галуа

Рассмотрим алгоритм обработки M -последовательности, позволяющий определить ее конечный элемент, за которым следует блок данных.

Суть предлагаемого метода построена на свойстве M -последовательности и заключается в том, что начальный элемент c , порождающий данную последовательность, может быть определен по произвольному k -элементному участку $(S_g S_{g+1} \dots S_{g+k-1})$ как [1]:

$$c = \varepsilon^{-g} \sum_{i=1}^k \lambda_i S_{g+i-1}, \quad (17)$$

где g – определяет расстояние k -элементного участка от начала M -последовательности.

Учитывая тот факт, что начало и конец КЦФ на приемной стороне заранее не известны, для их определения необходимо решить две задачи:

- определение участка поступившей на вход последовательности $\{H\}$, обладающего свойствами рекуррентности по заданному характеристическому многочлену $P(x)$;
- оценка длины рекуррентного участка по заданному пороговому значению и принятие решения об обнаружении КЦФ;
- определение конечного элемента КЦФ и начала блока данных.

Таким образом, методика выделения КЦФ сводится к последовательной обработке двойственным базисом k -элементных участков поступившей на вход комбинации, вычислению элементов поля c_j и анализу их распределения:

$$c_j = \sum_{i=1}^k \lambda_i H_{t+i-1}, \quad t=0, 1, 2, \dots; j=1, 2, \dots, \quad (18)$$

где j – порядковый номер обработанного k -элементного участка, вместе с тем номер такта обработки последовательности $\{H\}$ двойственным базисом.

Последовательно принимая k -элементные участки и вычисляя c_j , определим степени элементов путем нахождения дискретного логарифма:

$$z_j = \log_{\varepsilon} c_j, \quad j=1, 2, \dots \quad (19)$$

Полученный набор значений (19) позволяет сделать заключение о наличии рекуррентного участка в принятой последовательности.

Рассмотрим данный метод на примере обработки M -последовательности с характеристическим многочленом $P(x)=x^4+x+1$. В качестве исходного выбран вектор (111000100110101111), имеющий длину $n+k-1$ бит за счет циклического дополнения к M -последовательности следующих $k-1$ разрядов. Данный вектор может быть использован в качестве $\{S\}_{КЦФ}$ с начальным элементом ε^{12} поля $GF(2^4)$.

Применяя формулу (18) для обработки замкнутой в кольцо комбинации $\{S\}_{КЦФ}$, последовательно умножаем ее k -элементные участки на элементы двойственного базиса $\{\varepsilon^{14}, \varepsilon^2, \varepsilon, 1\}$, вычисленного ранее для выбранного $P(x)$.

$c_1 = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{12}$	$z_1 = 12$
$c_2 = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{13}$	$z_2 = 13$
$c_3 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{14}$	$z_3 = 14$
$c_4 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = 1$	$z_4 = 0$
$c_5 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon$	$z_5 = 1$
$c_6 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^2$	$z_6 = 2$
$c_7 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^3$	$z_7 = 3$
$c_8 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_8 = 4$

$$\begin{aligned}
c_9 &= 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^5 & z_9 &= 5 \\
c_{10} &= 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^6 & z_{10} &= 6 \\
c_{11} &= 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^7 & z_{11} &= 7 \\
c_{12} &= 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^8 & z_{12} &= 8 \\
c_{13} &= 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^9 & z_{13} &= 9 \\
c_{14} &= 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{10} & z_{14} &= 10 \\
c_{15} &= 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{11} & z_{15} &= 11
\end{aligned}$$

По результатам обработки рекуррентной последовательности, не содержащей ошибок, построим график (рис. 3), представляющий собой шаблон.

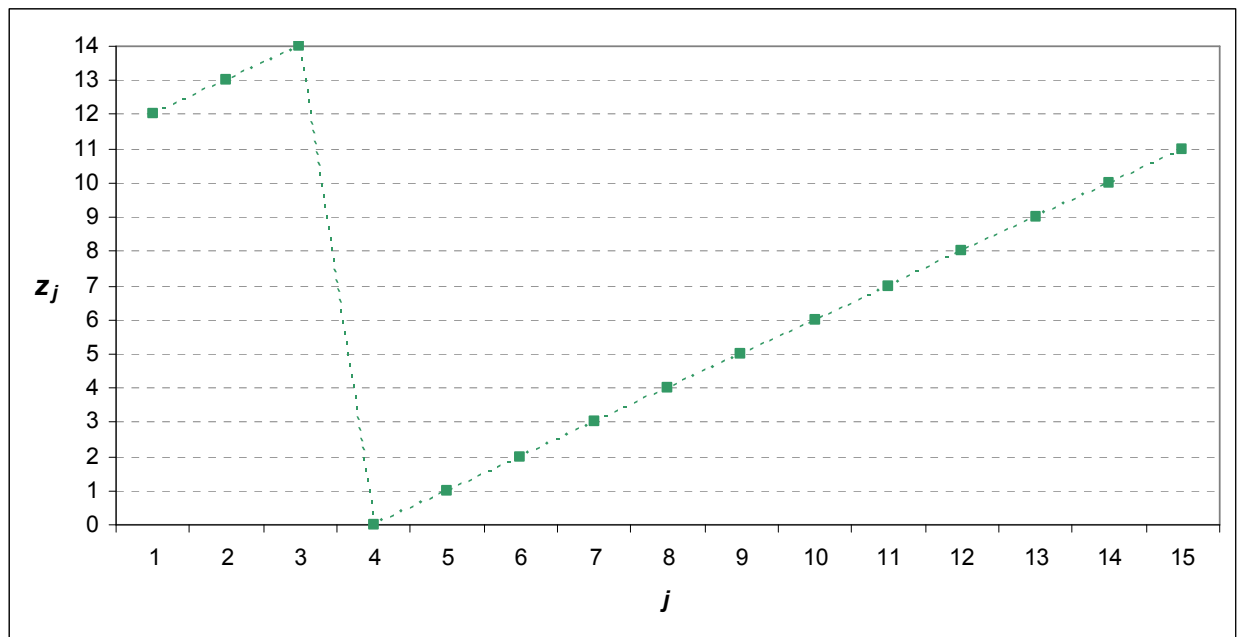


Рис. 3. Обработка рекуррентной последовательности двойственным базисом

Из рис. 3 видно, что точки, соответствующие степеням элементов поля, линейно зависят от сдвига фазы предполагаемой рекуррентной последовательности (лежат на одной прямой шаблона с учетом равенства $z_j = z_j \bmod n$). Другими словами, при обработке полного периода M -последовательности (с учетом добавленных элементов) были получены все элементы поля в последовательном порядке.

Выделив КЦФ, не составляет труда определить конечный участок КЦФ – (1111), соответствующий элементу ε^{11} . Этот участок определяет место, с которого начинается поле данных.

Очевидно, что при низкой вероятности ошибки решение можно принимать, не производя обработку полного периода целиком. Наличие достаточно большого количества последовательных точек z_j , совпадающих с шаблоном, позволяет сделать заключение о правильном выделении КЦФ. Такой подход предполагает использование

некоторого порогового значения зачетного участка рекуррентности. При этом все участки рекуррентности, имеющие меньшую длину [1] будут игнорироваться.

Значение порога, то есть длины зачетного участка, для каждого варианта указано в задании на курсовую работу. Таким образом, одной из задач в работе является определение числа тактов, необходимых для выделения КЦФ с учетом заданного порогового значения длины зачетного участка.

Отметим, что ошибки, возникающие при передаче КЦФ по каналу связи, нарушают рекуррентные связи в ней, а также могут формировать новые рекуррентные участки, которые в свою очередь способны привести к ложному решению.

Для примера внесем ошибку $\{e\}=(000001000000000000)$ в данную последовательность и добавим дополнительные разряды (100) в начало. Тогда обрабатываемый вектор $\{H\}$ будет иметь вид (100111001100110101111). Зададим пороговое значение длины зачетного участка рекуррентности $J = 8$.

Осуществим поиск КЦФ. Произведем обработку k -элементных участков предполагаемой рекуррентной последовательности, сдвигая начало искомой комбинации вправо.

Получим набор элементов поля:

$c_1 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^3$	$z_1 = 3$
$c_2 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_2 = 4$
$c_3 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{10}$	$z_3 = 10$
$c_4 = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{12}$	$z_4 = 12$
$c_5 = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{13}$	$z_5 = 13$
$c_6 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^3$	$z_6 = 3$
$c_7 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_7 = 4$
$c_8 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^5$	$z_8 = 5$
$c_9 = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{13}$	$z_9 = 13$
$c_{10} = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^3$	$z_{10} = 3$
$c_{11} = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_{11} = 4$
$c_{12} = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^5$	$z_{12} = 5$
$c_{13} = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^6$	$z_{13} = 6$
$c_{14} = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^7$	$z_{14} = 7$
$c_{15} = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^8$	$z_{15} = 8$
$c_{16} = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^9$	$z_{16} = 9$
$c_{17} = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{10}$	$z_{17} = 10$
$c_{18} = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{11}$	$z_{18} = 11$

На основании результатов обработки 18 k -элементных участков последовательности $\{H\}$ двойственным базисом построим график (рис. 4).

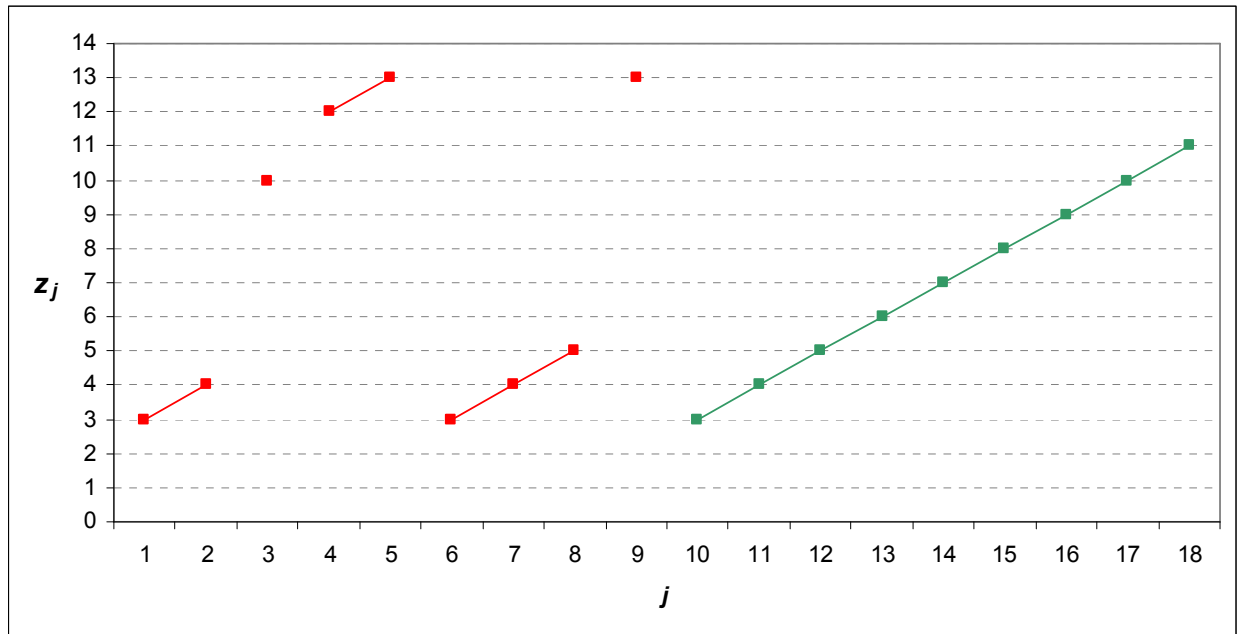


Рис. 4. Обработка последовательности (100111001100110101111) двойственным базисом

Из графика (рис. 4) видно, что последний рекуррентный участок содержит 9 точек, это удовлетворяет заданному пороговому значению зачетного участка ($J=8$). Предыдущие рекуррентные участки оказались слишком короткими и были проигнорированы. Только после 17 тактов обработки последовательности $\{H\}$ удалось сделать заключение о появлении КЦФ. Учитывая, что начальная фаза КЦФ должна быть ε^{12} , не составляет труда определить конечную точку. Это должен быть участок, сформированный элементом ε^{11} . Так как последний элемент, полученный при обработке длинного рекуррентного участка на 17 такте – ε^{10} , можно заключить, что КЦФ должна закончиться через один такт, после чего начнется передача данных.

Устройство, реализующее данный алгоритм подробно описано в работе [1].

1.3. Варианты заданий

Варианты заданий к курсовой работе приведены в табл.1.

Таблица 1

Вариант	$P(x)$	Начальная фаза КЦФ	Изменения в КЦФ		Пороговое значение зачетного участка
			Ошибочные разряды	Дополнительные начальные элементы	
1	x^5+x^2+1	ε	3, 4	100	10
2	$x^5+x^4+x^3+x^2+1$	ε^2	5, 6	101	12
3	$x^5+x^4+x^2+x+1$	ε^3	6, 7	010	11
4	$x^5+x^3+x^2+x+1$	ε^4	4, 5, 6	000	15
5	$x^5+x^4+x^3+x+1$	ε^5	11, 12, 13	111	16
6	x^5+x^3+1	ε^6	6, 11	001	19
7	x^5+x^2+1	ε^7	5, 12, 15	101	11
8	$x^5+x^4+x^3+x^2+1$	ε^8	1, 3, 5	100	15
9	$x^5+x^4+x^2+x+1$	ε^9	2, 10	010	14
10	$x^5+x^3+x^2+x+1$	ε^{10}	1, 9	000	24
11	$x^5+x^4+x^3+x+1$	ε^{11}	12, 14	100	16
12	x^5+x^3+1	ε^{12}	4, 8, 13	111	6
13	x^5+x^2+1	ε^{13}	1, 3	001	15
14	$x^5+x^4+x^3+x^2+1$	ε^{14}	15, 16	111	10
15	$x^5+x^4+x^2+x+1$	ε^{15}	3, 6	000	17
16	$x^5+x^3+x^2+x+1$	ε^{16}	5, 7, 9	110	14
17	$x^5+x^4+x^3+x+1$	ε^{17}	10, 11, 12	010	8
18	x^5+x^3+1	ε^{18}	3, 4	100	24

1.4. Содержание и форма отчета

Выполненная курсовая работа предоставляется в бумажном и электронном виде. Электронный образец курсовой работы должен быть записан на оптический компакт-диск в формате PDF. На компакт-диске должна быть указана дисциплина, по которой выполнена курсовая работа, фамилия, имя студента, группа и дата выполнения работы.

Отчет должен содержать результаты решения следующих задач:

- Построено поле Галуа по выбранному характеристическому многочлену;
- Вычислены элементы двойственного базиса поля Галуа;

- Построена схема генератора M -последовательностей на основе регистра сдвига с вынесенными сумматорами;
- При помощи функции след сформирована КЦФ с заданной начальной фазой;
- По заданию проведено наложение полиномов ошибок на сформированную КЦФ, добавлены дополнительные начальные разряды;
- Проведена обработка последовательности, содержащей КЦФ с ошибками;
- Графически представлены результаты обработки последовательности, содержащей КЦФ;
- Сделаны выводы о правильности выделения КЦФ и количестве тактов обработки, необходимых для ее определения с учетом заданного порогового значения зачетного участка.

Бумажный вариант курсовой работы должен соответствовать следующим техническим требованиям к оформлению документа:

- Кегль 12;
- Межстрочный интервал 1;
- Левое поле 3 см;
- Правое поле 1 см;
- Верхнее поле 2 см;
- Нижнее поле 2 см;
- Выравнивание текста по ширине страницы.

Раздел 2. Пример отчета по выполненной курсовой работе

Приведен пример выполнения курсовой работы.

2.1. Исходные данные

Таблица 2

$P(x)$	Начальная фаза КЦФ	Ошибочные разряды	Дополнительные начальные элементы	Пороговое значение зачетного участка
x^4+x+1	ε^6	0, 3, 5	101	8

2.2. Проведение расчетов

2.2.1. Построение поля Галуа

Для построения поля Галуа $GF(2^4)$ используется многочлен $P(x)=1+x+x^4$

Вычет имеет вид: 1100

Результат построения поля представлен в табл.3.

Таблица 3

Элементы	(a_0, a_1, a_2, a_3)	Выражение через левый степенной базис
1	1000	1
ε	0100	ε
ε^2	0010	ε^2
ε^3	0001	ε^3
ε^4	1100	$1+\varepsilon$
ε^5	0110	$\varepsilon+\varepsilon^2$
ε^6	0011	$\varepsilon^2+\varepsilon^3$
ε^7	1101	$1+\varepsilon+\varepsilon^3$
ε^8	1010	$1+\varepsilon^2$
ε^9	0101	$\varepsilon+\varepsilon^3$
ε^{10}	1110	$1+\varepsilon+\varepsilon^2$
ε^{11}	0111	$\varepsilon+\varepsilon^2+\varepsilon^3$
ε^{12}	1111	$1+\varepsilon+\varepsilon^2+\varepsilon^3$
ε^{13}	1011	$1+\varepsilon^2+\varepsilon^3$
ε^{14}	1001	$1+\varepsilon^3$

2.2.2. Вычисление элементов двойственного базиса поля Галуа

Определим коэффициенты характеристического многочлена (2).

$$P(x) = p_0x^4 + p_1x^3 + p_2x^2 + p_3x + p_4$$

$$p_0 = 1$$

$$p_1 = 0$$

$$p_2 = 0$$

$$p_3 = 1$$

$$p_4 = 1$$

Определим значение производной характеристического многочлена.

$$P'(\varepsilon) = 4\varepsilon^3 + 1 = 1$$

Для вычисления элементов двойственного базиса используем формулу (10),

$$\lambda_1 = \frac{\sum_{l=0}^{k-1} p_{k-1-l} \varepsilon^l}{P'(\varepsilon)} = \sum_{l=0}^3 p_{3-l} \varepsilon^l = p_3 + p_2 \varepsilon + p_1 \varepsilon^2 + p_0 \varepsilon^3 = 1 + \varepsilon^3 = \varepsilon^{14}$$

$$\lambda_2 = \frac{\sum_{l=0}^{k-2} p_{k-2-l} \varepsilon^l}{P'(\varepsilon)} = \sum_{l=0}^2 p_{2-l} \varepsilon^l = p_2 + p_1 \varepsilon + p_0 \varepsilon^2 = \varepsilon^2$$

$$\lambda_3 = \frac{\sum_{l=0}^{k-3} p_{k-3-l} \varepsilon^l}{P'(\varepsilon)} = \sum_{l=0}^1 p_{1-l} \varepsilon^l = p_1 + p_0 \varepsilon = \varepsilon$$

$$\lambda_4 = \frac{\sum_{l=0}^{k-4} p_{k-4-l} \varepsilon^l}{P'(\varepsilon)} = p_0 = 1$$

Таким образом, базис, двойственный левому степенному, имеет вид $\{\varepsilon^{14}, \varepsilon^2, \varepsilon, 1\}$.

2.2.3. Формирование M -последовательностей

Построим генератор последовательностей $\{S\}$ для характеристического многочлена $P(x) = x^4 + x + 1$ на основе регистра сдвига с вынесенным сумматором (рис. 5).

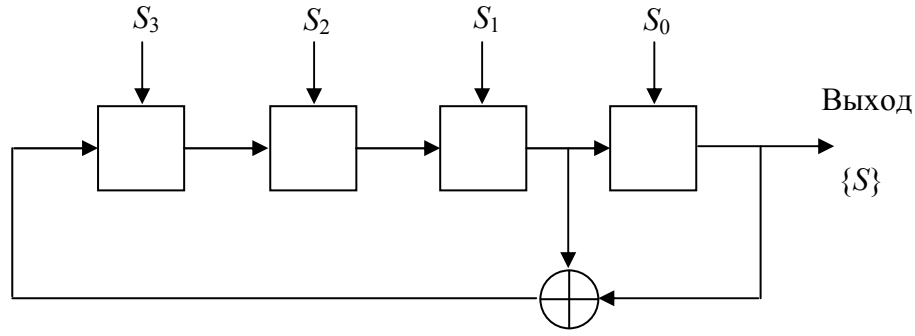


Рис. 5. Генератор М-последовательности для $P(x)=x^4+x+1$
на основе регистра сдвига с вынесенным сумматором

Построим каноническую последовательность $\{S\}$ на основании функций след от подряд идущих элементов поля:

$$\{S\}=[T(1),T(\varepsilon),T(\varepsilon^2),T(\varepsilon^3),T(\varepsilon^4),T(\varepsilon^5),T(\varepsilon^6),T(\varepsilon^7),T(\varepsilon^8),T(\varepsilon^9),T(\varepsilon^{10}),T(\varepsilon^{11}),T(\varepsilon^{12}),T(\varepsilon^{13}),T(\varepsilon^{14})]$$

$$T(1) = 1 + 1^2 + 1^4 + 1^8 = 0$$

$$T(\varepsilon) = \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = 0$$

$$T(\varepsilon^2) = \varepsilon^2 + (\varepsilon^2)^2 + (\varepsilon^2)^4 + (\varepsilon^2)^8 = \varepsilon^2 + \varepsilon^4 + \varepsilon^8 + \varepsilon^{16} = \varepsilon^2 + \varepsilon^4 + \varepsilon^8 + \varepsilon = 0$$

$$T(\varepsilon^3) = \varepsilon^3 + (\varepsilon^3)^2 + (\varepsilon^3)^4 + (\varepsilon^3)^8 = \varepsilon^3 + \varepsilon^6 + \varepsilon^{12} + \varepsilon^{24} = \varepsilon^3 + \varepsilon^6 + \varepsilon^{12} + \varepsilon^9 = 1$$

$$T(\varepsilon^4) = \varepsilon^4 + (\varepsilon^4)^2 + (\varepsilon^4)^4 + (\varepsilon^4)^8 = \varepsilon^4 + \varepsilon^8 + \varepsilon^{16} + \varepsilon^{32} = \varepsilon^4 + \varepsilon^8 + \varepsilon + \varepsilon^2 = 0$$

$$T(\varepsilon^5) = \varepsilon^5 + (\varepsilon^5)^2 + (\varepsilon^5)^4 + (\varepsilon^5)^8 = \varepsilon^5 + \varepsilon^{10} + \varepsilon^{20} + \varepsilon^{40} = \varepsilon^5 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{10} = 0$$

$$T(\varepsilon^6) = \varepsilon^6 + (\varepsilon^6)^2 + (\varepsilon^6)^4 + (\varepsilon^6)^8 = \varepsilon^6 + \varepsilon^{12} + \varepsilon^{24} + \varepsilon^{48} = \varepsilon^6 + \varepsilon^{12} + \varepsilon^9 + \varepsilon^3 = 1$$

$$T(\varepsilon^7) = \varepsilon^7 + (\varepsilon^7)^2 + (\varepsilon^7)^4 + (\varepsilon^7)^8 = \varepsilon^7 + \varepsilon^{14} + \varepsilon^{28} + \varepsilon^{56} = \varepsilon^7 + \varepsilon^{14} + \varepsilon^{13} + \varepsilon^{11} = 1$$

$$T(\varepsilon^8) = \varepsilon^8 + (\varepsilon^8)^2 + (\varepsilon^8)^4 + (\varepsilon^8)^8 = \varepsilon^8 + \varepsilon^{16} + \varepsilon^{32} + \varepsilon^{64} = \varepsilon^8 + \varepsilon + \varepsilon^2 + \varepsilon^4 = 0$$

$$T(\varepsilon^9) = \varepsilon^9 + (\varepsilon^9)^2 + (\varepsilon^9)^4 + (\varepsilon^9)^8 = \varepsilon^9 + \varepsilon^{18} + \varepsilon^{36} + \varepsilon^{72} = \varepsilon^9 + \varepsilon^3 + \varepsilon^6 + \varepsilon^{12} = 1$$

$$T(\varepsilon^{10}) = \varepsilon^{10} + (\varepsilon^{10})^2 + (\varepsilon^{10})^4 + (\varepsilon^{10})^8 = \varepsilon^{10} + \varepsilon^{20} + \varepsilon^{40} + \varepsilon^{80} = \varepsilon^{10} + \varepsilon^5 + \varepsilon^{10} + \varepsilon^5 = 0$$

$$T(\varepsilon^{11}) = \varepsilon^{11} + (\varepsilon^{11})^2 + (\varepsilon^{11})^4 + (\varepsilon^{11})^8 = \varepsilon^{11} + \varepsilon^{22} + \varepsilon^{44} + \varepsilon^{88} = \varepsilon^{11} + \varepsilon^7 + \varepsilon^{14} + \varepsilon^{13} = 1$$

$$T(\varepsilon^{12}) = \varepsilon^{12} + (\varepsilon^{12})^2 + (\varepsilon^{12})^4 + (\varepsilon^{12})^8 = \varepsilon^{12} + \varepsilon^{24} + \varepsilon^{48} + \varepsilon^{96} = \varepsilon^{12} + \varepsilon^9 + \varepsilon^3 + \varepsilon^6 = 1$$

$$T(\varepsilon^{13}) = \varepsilon^{13} + (\varepsilon^{13})^2 + (\varepsilon^{13})^4 + (\varepsilon^{13})^8 = \varepsilon^{13} + \varepsilon^{26} + \varepsilon^{52} + \varepsilon^{104} = \varepsilon^{13} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^{14} = 1$$

$$T(\varepsilon^{14}) = \varepsilon^{14} + (\varepsilon^{14})^2 + (\varepsilon^{14})^4 + (\varepsilon^{14})^8 = \varepsilon^{14} + \varepsilon^{28} + \varepsilon^{56} + \varepsilon^{112} = \varepsilon^{14} + \varepsilon^{13} + \varepsilon^{11} + \varepsilon^7 = 1$$

Таким образом, каноническая последовательность $\{S\}$ будет иметь вид:

$$\{S\} = (000100110101111)$$

На основе канонической последовательности $\{S\}$ сформируем КЦФ

Начальная фаза КЦФ – ε^6 .

$$\{S\}=[T(\varepsilon^6),T(\varepsilon^7),T(\varepsilon^8),T(\varepsilon^9),T(\varepsilon^{10}),T(\varepsilon^{11}),T(\varepsilon^{12}),T(\varepsilon^{13}),T(\varepsilon^{14}),T(1),T(\varepsilon),T(\varepsilon^2),T(\varepsilon^3),T(\varepsilon^4),T(\varepsilon^5)]$$

Дополняем период $\{S\}$ следующими $k-1$ разрядами - (110).

$$\{S\}_{КЦФ}=(110101111000100110)$$

Внесем ошибки в КЦФ в соответствии с исходными данными.

$$\{H\} = \{S\}_{КЦФ} + \{e\} = (110101111000100110) \oplus (100101000000000000) = (010000111000100110)$$

Добавляем дополнительные начальные элементы (101)

$$\{H\} = (101010000111000100110)$$

2.2.4. Выделение КЦФ

Произведем обработку 18 k -элементных участков последовательности (101010000111000100110) двойственным базисом с учетом сдвига принятой последовательности вправо. Получим набор элементов поля:

$c_1 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^7$	$z_1 = 7$
$c_2 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^8$	$z_2 = 8$
$c_3 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^7$	$z_3 = 7$
$c_4 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^2$	$z_4 = 2$
$c_5 = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{14}$	$z_5 = 14$
$c_6 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = 0$	$z_6 = \text{не существует}$
$c_7 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = 1$	$z_7 = 0$
$c_8 = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_8 = 4$
$c_9 = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^{10}$	$z_9 = 10$
$c_{10} = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{12}$	$z_{10} = 12$
$c_{11} = 1 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{13}$	$z_{11} = 13$
$c_{12} = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^{14}$	$z_{12} = 14$
$c_{13} = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = 1$	$z_{13} = 0$
$c_{14} = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon$	$z_{14} = 1$
$c_{15} = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^2$	$z_{15} = 2$
$c_{16} = 1 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 0 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^3$	$z_{16} = 3$
$c_{17} = 0 \cdot \varepsilon^{14} + 0 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 1 \cdot 1 = \varepsilon^4$	$z_{17} = 4$
$c_{18} = 0 \cdot \varepsilon^{14} + 1 \cdot \varepsilon^2 + 1 \cdot \varepsilon + 0 \cdot 1 = \varepsilon^5$	$z_{18} = 5$

Результаты обработки комбинации $\{H\}$ представим в графическом виде (рис. 6).

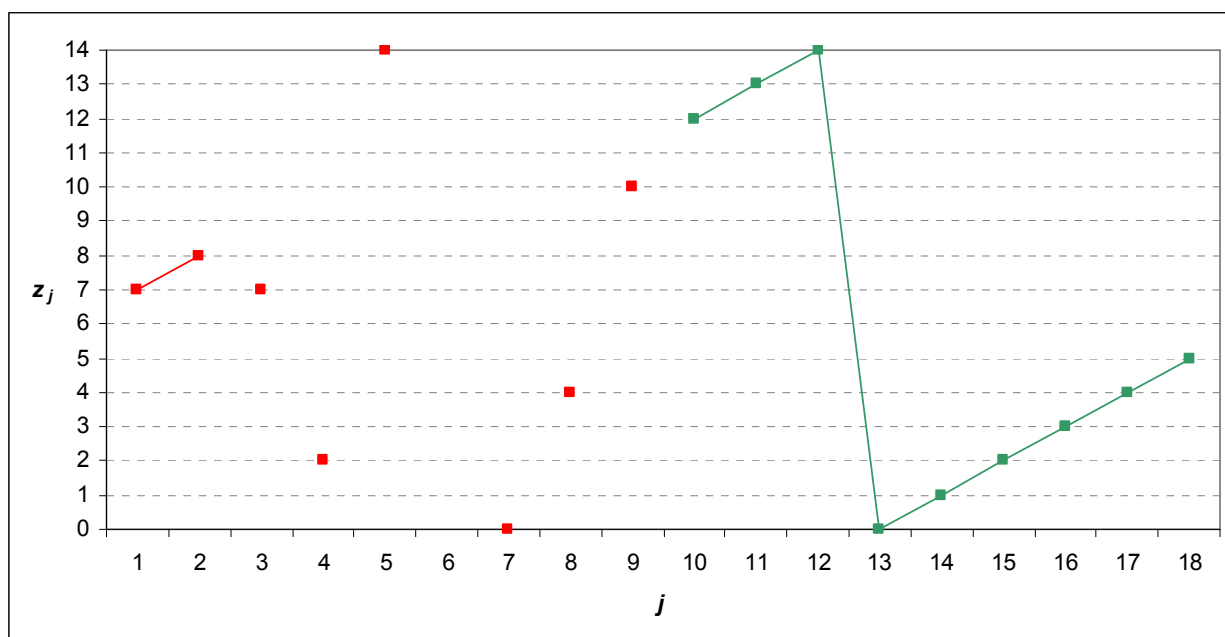


Рис. 6. Обработка последовательности (101010000111000100110) двойственным базисом

Из графика (рис. 6) видно, что для выявления КЦФ достаточно произвести 17 тактов обработки последовательности $\{H\}$ двойственным базисом. Так на 17 такте обработки длина рекуррентного участка будет содержать 8 точек, что удовлетворяет заданному пороговому значению зачетного участка ($J=8$). Предыдущие рекуррентные участки были проигнорированы, так как не удовлетворяли данному условию.

Учитывая, что обработка рекуррентного участка, на основании которого было принято решение о появлении КЦФ, закончилась на 17 такте с появлением элемента ε^4 , а начальная фаза КЦФ – ε^6 , то для завершения КЦФ системе нужно доработать еще один такт (чтобы принять участок, формируемый элементом ε^5). То есть следующий элемент в комбинации $\{H\}$ будет последним и начнется передача блока данных. Таким образом, можно сделать вывод, что, не смотря на искажения, внесенные при передаче данных по каналу связи, КЦФ была выделена правильно.

2.2.5. Выводы по результатам выполнения курсовой работы

В результате выполнения курсовой работы были решены следующие задачи:

- Построено поле Галуа по выбранному характеристическому многочлену;
- Вычислены элементы двойственного базиса поля Галуа;
- Построена схема генератора M -последовательностей на основе регистра сдвига с вынесенным сумматором;

- При помощи функции след сформирована M -последовательность с заданной начальной фазой ε^6 , сформирована КЦФ;
- Проведено наложение полинома ошибок на КЦФ, добавлены дополнительные разряды;
- Проведена обработка двойственным базисом поступившей на вход приемного устройства последовательности с целью выделения КЦФ;
- Результаты обработки представлены в графическом виде;
- Сделаны выводы о правильности выделения КЦФ и количестве тактов обработки, необходимых для ее определения.

ЛИТЕРАТУРА

1. *Когновицкий О.С.* Двойственный базис и его применение в телекоммуникациях. – СПб: Линк, 2009.
2. *Когновицкий О.С.* Алгебраический метод нахождения двойственного базиса в поле Галуа и его практическое применение // Сборник научных трудов учебных институтов связи, – Л., 1982.
3. *Когновицкий О.С., Кукунин Д.С.* Метод декодирования эквидистантных кодов // Труды учебных заведений связи / СПбГУТ. СПб, 2006. № 174. С. 45-52.
4. *Касами Т., Токура Н., Ивадари Ё., Инагаки Я.* Теория кодирования. – М., 1978.
5. *Кукунин Д.С.* Калькулятор Галуа с удаленным доступом через Интернет // 59-я НТК профессорско-преподавательского состава: мат-лы / СПбГУТ. СПб, 2007. С. 31.
6. *Когновицкий О.С.* Основы циклических кодов: Учеб. пособие. – Л., 1972.