АННОТАЦИЯ

Расчетно-пояснительная записка состоит из страниц, 4 раздела, рисунков, таблиц, использованных источника.

Сегодня экстенсивное развитие информационных технологий приводит к значительному увеличению нагрузки на цифровые системы передачи данных. В силу ограниченных возможностей развития этих систем, чрезвычайную важность представляют вопросы увеличения скорости передачи данных, что в свою очередь сказывается на вероятности появления ошибок в каналах передачи. Целью этой работы является разработка метода декодирования кодов Рида-Соломона, применяемого в ЦССС. Объектом исследования выступает непосредственно цифровой поток.

В работе проанализировано место и роль кодов, исправляющих ошибки, в схеме функционирования типовой системы цифровой связи, обобщены достоинства и недостатки кодов Рида-Соломона, рассмотрены математические основы их кодирования и декодирования. Разработан метод декодирования кодов Рида-Соломона в реальном времени. На основе данного метода, создано программное решение. Проведены исследования скорости и надежности работы разработанного решения.

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ **4**

ВВЕДЕНИЕ **5**

Аналитический раздел **7**

Помехоустойчивое кодирование 7

Основные параметры помехоустойчивых кодов 8

Избыточность корректирующего кода 9

Кодовое расстояние 9

Кратности ошибок 10

Классификация помехоустойчивых кодов 11

Коды Рида-Соломона 14

Декодирование кодов Рида-Соломона 16

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ

k	число входных символов
n	число выходных символов
r	абсолютная избыточность
$R_{\text{отн}}$	относительная избыточность
d	расстояние Хэмминга
t	количество гарантированно исправляемых ошибок
GF(q)	поле Галуа, где q - число элементов
$g(x)$	порождающий многочлен
$h(x)$	проверочный многочлен
$S(x)$	многочлен синдромов
$\Gamma(x)$	многочоен значений ошибок
$\Lambda(x)$	многочлен локаторов ошибок

ВВЕДЕНИЕ

На сегодняшней день быстрый рост телекомоционной отрасли преводит к динамичному технологическому переходу на цифровые системы обработки и передачи информации, что создает значительный круг проблем при проектирование совремменных систем информатики и телекоммуникации. Одной из важнейших задач которые при этом необходимо решать во всех подобных системах является обеспечение высокой достоверности передачи данных, которую в текущих условиях достигается все сложнее, так как интенсивная скорость развития приводит и к нежелательным явлениям, в виде возникновения различных ошибок и помех в передаваемых файлах, вызванных повышением зашумленности каналов связи, а также проблемами демодуляции.

Наиболее эффективными методам обеспечения высокого качества цифровой передачи в этих обстоятельствах являются алгоритмы корректирующих (помехоустойчивых) кодов. За годы интенсивного развития в технику связи были успешно внедрены многие из них. При этом одними из самых распространенных сейчас являются коды Рида-Соломона.

Эффект от их применения может выражаться в том, что в системе связи они позволяют при прочих равных условиях многократно увеличивать скорость или дальность передачи, снижать размеры дорогостоящих антенн или работать при существенно сниженном уровне полезного сигнала. Применение кодирования можно рассматривать и просто как способ многократного увеличения КПД спутниковых и прочих цифровых каналов связи.

Однако требования к алгоритмам исправления ошибок в каналах с шумами, в частности, спутниковых каналах, непрерывно растут, и главная проблема - декодирования с эффективностью близкой к оптимальной по энергетике канала, но при минимальной скорости обработки, еще далека от своего успешного решения.

Разработка такого метода декодирования описано в этой работе. Предметом исследования являются цифровые системы связи

Цель работы: разработать метод декодирования кодов Рида-Соломона, применяемых в ЦССС.

Задачи, решаемые в работе:

- обзор места помехоустойчивого кодирования в структуре цифровой системы передачи данных;
- анализ математических основ кодов Рида-Соломона, их достоинства и недостатки
- разработка метода их декодирования, применяемых в ЦССС;
- разработка программного обеспечения, реализующего данный метод;
- проведение серии экспериментов с использованием разработанного программного обеспечения.

Аналитический раздел

Помехоустойчивое кодирование

Помехоустойчивое кодирование (англ. Error Correcting Coding, ECC) — процесс преобразования информации, предоставляющий возможность обнаружить и исправить ошибки, возникающие при передаче информации по каналам передачи данных.

Процесс помехоустойчивого кодирования заключается во введении избыточности, т. е. для передачи информации используется код, у которого используются не все возможные комбинации, а только некоторые из них. Такие коды называют избыточными или корректирующими.

Соответственно, процесс введения избыточности (преобразование информационных символов в кодовое слово) называется *кодированием*, а обратный процесс восстановления информации из кодового слова, возможно содержащего ошибки — *декодированием*.

Еще одним важным свойством помехоустойчивого кодирования является эффект *усреднения шума*, который достигается за счет того, что избыточные символы зависят от нескольких информационных символов.

В рамках цифровой системы передачи данных задачи кодирования и декодирования возложены на *кодер* и *декодер* соответственно. Структура цифровой системы передачи данных показана на рисунке 1.

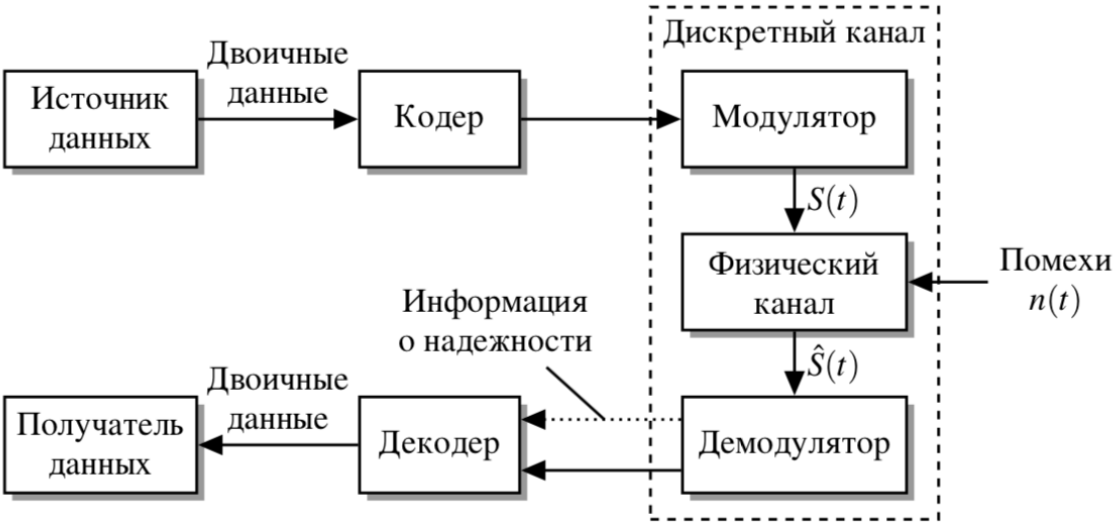

Рисунок 1. Структура цифровой системы передачи данных

На нем также показано, что часто декодеру доступна информация, указывающая на надежность решений, принимаемых о различных символах кодового слова. Такая информация часто может быть использована для упрощения процесса декодирования, либо для улучшения его характеристик.

В целом, способность помехоустойчивых кодов определять и исправлять ошибки — их корректирующие свойства — зависят от правил построения этих кодов и параметров кода (числа разрядов, избыточности и др.), а также от используемых алгоритмов декодирования.

Основные параметры помехоустойчивых кодов

Основными параметрами, характеризующими корректирующие свойства кодов являются

1. Избыточность кода.
2. Кодовое расстояние.
3. Кратность гарантированно обнаруживаемых ошибок.
4. Кратность гарантированно исправляемых ошибок.

Избыточность корректирующего кода

Избыточность корректирующего кода может быть абсолютной и отно- сительной. Под *абсолютной избыточностью r* понимают число вводимых дополнительных разрядов:

$$r = n - k, \tag{1.1}$$

где *n* — число кодовых символов на выходе кодера, соответствующих *k* информационных символов на его входе.

Относительной избыточностью корректирующего кода называют величину $R_{\text{отн}}$:

$$R_{\text{отн}} = \frac{r}{n} = \frac{n-k}{n} = 1 - \frac{k}{n} \tag{1.2}$$

С ней связана так называемая *относительная скорость передачи информации* или *скорость кода*, которая показывает, какую часть общего числа символов кодовой комбинации составляют информационные символы.

$$\frac{k}{n} = 1 - R_{\text{отн}} \tag{1.3}$$

Если производительность источника равна *H* символов в секунду, то скорость передачи после кодирования этой информации будет равна:

$$R = H * \frac{k}{n}. \tag{1.4}$$

Кодовое расстояние

Кодовое расстояние d или *расстояние Хемминга* характеризует степень различия любых двух кодовых комбинаций. Оно выражается числом символов, которыми комбинации отличаются одна от другой.

Чтобы получить кодовое расстояние между двумя комбинациями двоичного кода, достаточно подсчитать число единиц в сумме этих комбинаций по модулю 2, к примеру:

$$10011 \oplus 11001 = 01010 \Rightarrow d = 2.$$

Кодовое расстояние может быть различным. Так, в первичном натуральном безызбыточном коде это расстояние для различных комбинаций может различаться от единицы до *n*, где *n* — значность/длина кода.

Для помехоустойчивого кода наиболее важным является *минимальное кодовое расстояние* d_{min} — наименьшее кодовое расстояние из всех между всеми парами кодовых комбинаций.

В безызбыточном коде все комбинации являются разрешенными, $d_{min} = 1$. Достаточно только исказиться одному символу, и будет ошибка в сообщении.

Кратности ошибок

Эти параметры напрямую зависят от минимального кодового расстояния. Под *кратностью* понимается количество поражённых ошибкой символов кодовой комбинации.

В общем случае при необходимости обнаруживать ошибки кратности $t_{\text{обн}}$ минимальное кодовое расстояние должно быть, по крайней мере, на единицу больше $t_{\text{обн}}$, то есть:

$$d_{min} \geq t_{\text{обн}} + 1 \qquad (1.5)$$

Соответственно, *кратность гарантированно обнаруживаемой кодом ошибки* равна:

$$t_{\text{обн}} \leq d_{min} - 1 \tag{1.6}$$

Кратность гарантированно исправляемой кодом ошибки вычисляется по формуле:

$$t \leq \frac{d_{min}-1}{2} \tag{1.7}$$

Таким образом, код, имеющий минимальное кодовое расстояние $d_{min} = 3$, позволяет гарантированно обнаружить $t_{\text{обн}} = 2$ и менее ошибок и гарантированно исправить $t = 1$ ошибку.

Классификация помехоустойчивых кодов

Помехоустойчивые коды классифицируются по различным признакам. Одной из основных классификаций является деление кодов на *блочные* и *непрерывные*.

Блочный (блоковый) код является *кодом без памяти*. Кодер блочного кода отображает подающийся на вход блок информационных символов длиной k в кодовую последовательность из n выходных символов. Термин «без памяти» указывает, что каждый блок из n символов зависит только от соответствующего блока из k символов и не зависит от других блоков.

Основными параметрами блочных кодов являются длина информационного блока k, длина кодового слова n, скорость кода $\frac{k}{n}$ и минимальное кодовое расстояние d_{min}.

Непрерывные или *древовидные* коды — это коды, исправляющие ошибки, которые используют непрерывную или последовательную обработку информации короткими фрагментами (блоками). Чаще всего используются линейные древовидные коды, называемые *сверточными*. Кодер древовидного кода является устройством *с памятью*. На вход поступают наборы из k входных информационных символов, а на выходе появляются наборы из n кодовых символов. Каждый набор n кодовых символов зависит от текущего входного набора и от v предыдущих входных символов. Следовательно кодер должен содержать устройство памяти на m входных символов:

$$m = k + v \tag{1.8}$$

Параметр m часто называют *длиной кодового ограничения* кода.

Также *непрерывные* коды характеризуются скоростью кода $\frac{k}{n}$ и свободным расстоянием $d_{\text{св}}$

Особое место в такой классификации занимают каскадные коды и турбо коды, представляющие из себя комбинации блочных и/или непрерывных кодов.

Другой подход к классификации делит коды на *линейные* и *нелинейные*. Линейные коды образуют векторное пространство. Два кодовых слова линейного кода при сложении по определенному правилу дают в результате третье кодовое слово.

Практически все применяемые на практике схемы кодирования основаны на использовании линейных кодов. Двоичные линейные блоковые коды часто называют *групповыми* кодами, так как их кодовые слова образуют математическую структуру, называемую *группа*.

По способу кодирования коды делятся на *систематические* и *несистематические*. В первом случае информационные символы передаются на выход декодера без изменения и к ним добавляются проверочные символы. В случае несистематического кодирования информационные символы в явном виде в кодовом слове отсутствуют. Подклассом систематических кодов являются циклические коды, подразумевающие, что каждая циклическая перестановка кодового слова также является кодовым словом. Полная классификация помехоустойчивых кодов представлена на рисунке 2.

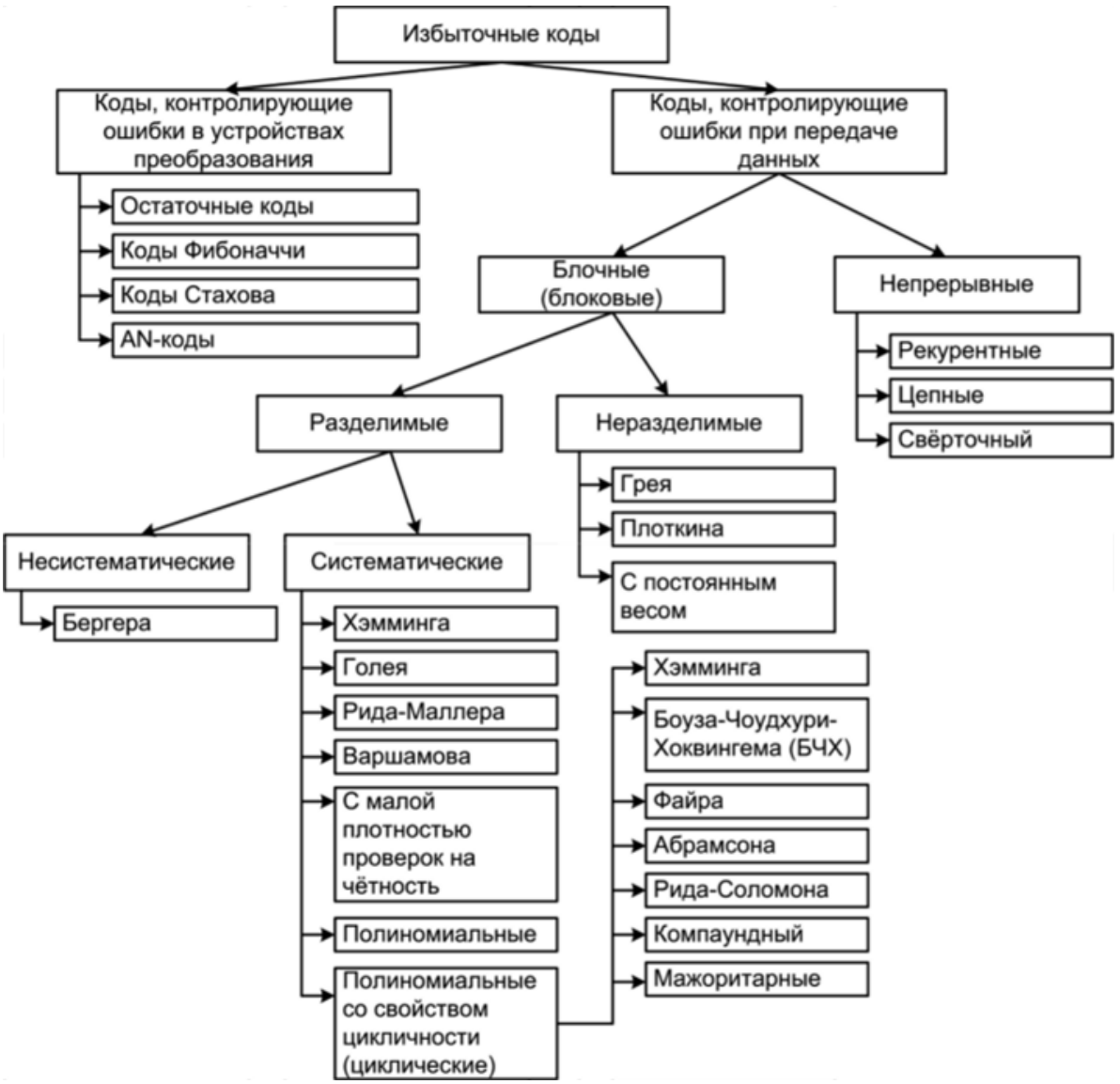

Рисунок 2. Классификация помехоустойчивых кодов

Ещё одним вариантом деления помехоустойчивых кодов является разделение их на *коды, исправляющие случайные ошибки*, и *коды, исправляющие пакеты (пачки) ошибок*. Хотя для исправления пачек ошибок было разработано большое количество кодов с хорошими характеристиками, часто оказывается выгодным использовать коды, исправляющие случайные ошибки, совместно с устройствами перемежения/деперемежения. Также стоит отметить, что существуют алгоритмы декодирования, позволяющие использовать коды, рассчитанные для исправления случайных ошибок, для исправления пачек ошибок без использования перемежителей.

Коды Рида-Соломона

Исходя из предстввленной выше схемы, коды Рида-Соломона (РС) – недвоичные совершенные систематические линейные блочные коды, относящиеся к классу циклических кодов, рассматриваемые как подмножество кодов Боуза-Чоудхури-Хоквингем, символы которых представляют собой элементы поля Галуа GF(q), где $q = 2^m$— порядок поля, а m — степень поля Галуа. Коды РС *(n,k)* определены на всех m-битовых символах при всех n и k, для которых верно неравенство:

$$0 < k < n \leq 2^m - 1 \tag{1.9}$$

Для большинства *(n,k)* кодов РС:

$$(n, k) = (q - 1, q - 1 - 2t) \tag{1.10}$$

Если $n < q - 1$, то код РС называют укороченным, если $n = q$ или $n = q + 1$, то код РС называется расширенным на 1 или 2 символа, соответственно.

При этом для кодов РС:

$$d = n - k + 1, \tag{1.11}$$

что позволяет говорить о том, что эти коды являются разделяемым кодомами с максимальным расстоянием, другими словами, являются оптимальным в смысле границы Синглтона.

Это означает, что исходя из (1.6), (1.7), (1.10) и (1.11), добавление r контрольных байт позволяет обнаруживать $t_{\text{обн}} = r$ произвольным образом искаженных байт и гарантированно восстанавливая $t = r/2$ из них.

Для задания кодов РС используется порождающий многочлен *g(x)* степени $d_{min} - 1 = n - k = r$ вида:

$$g(x) = \prod_{j=b}^{b+2t-1} (x + \varepsilon^j), \tag{1.12}$$

где b — целое число. Обычно $b = \{0,1\}$.

Коды РС, у которых $b = 1$, то есть, образующий полином равен:

$$g(x) = (x + \varepsilon)(x + \varepsilon^2)\dots(x + \varepsilon^{n-k}), \tag{1.13}$$

называют кодами РС в узком смысле. В дальнейшем мы будем рассматривать только их.

На основе порождающего многочлена можно построить проверочный многочлен *h(x)* степени *k*, удовлетворяющий условию:

$$h(x)g(x) = 0(mod\, x^n + 1) \tag{1.14}$$

Декодирование кодов Рида-Соломона

Классическая процедура декодирования кодов Рида-Соломона над GF(q) основана на использовании вектора синдрома:

$$S_i = \sum_{j=0}^{n-1} y_j \alpha^{(b+i)j}, \quad 0 \le i < d - 1 \tag{1.15}$$

где, $(y_0,\dots, y_{n-1}) \in GF(q)$ — декодируемый вектор, причем $y_i = c_i + e_i$, где c_i— символы кодового слова и e_i — значения ошибок. Введем многочлен значений ошибок и стираний:

$$\Gamma(x) = \Lambda(x)S(x) \bmod x^{d-1}, \tag{1.16}$$

где $\Lambda(x) = \prod_{j=1}^{t}(1 - X_j x)$ — многочлен локаторов ошибок и стираний, $S(x) = \sum_{i=o}^{d-2} S_i x^i$ — синдромный многочлен, в которых $X_j = \alpha_{ij}$ — локатор j-ой ошибки, i_j — номер j-го ошибочного символа, $E_j = e_{ij}$. Исходя из этого, путем подстановки в (1.15) получим:

$$S(x) = \sum_{j=1}^{t} E_j X_j^b \sum_{i=0}^{d-2} (X_j x)^i = \sum_{j=1}^{t} \frac{E_j X_j^b}{1 - X_j x} \bmod x^{d-1}. \tag{1.17}$$

Отсюда следует, что значение j-ого ошибочного символа может быть найдено как:

$$E_j = \frac{X_j^{-b}\Gamma(X_j^{-1})}{\Pi_{l \ne j}(1 - X_l X_j^{-1})}. \tag{1.18}$$

Путем введения производной многочлена $\Lambda(x)$, из приведенных преобразований можно получить, что $deg(\Gamma(x)) \le t - 1$. Кроме того можно показать, что уравнение (1.16) имеет единственное решение $(\Lambda(x), \Gamma(x))$ при $t \le [(d - 1)/2]$. Из этого следует, что:

$$\sum_{j=1}^{t} \Lambda_j S_{i+t-j} = -S_{i+t},\ 0 \le i < d - t - 1. \qquad (1.19)$$

Тогда коэффициенты $\Lambda(x)$ задают некоторый регистр сдвига с линейной обратной связью, порождающий последовательность S_i, а сам $\Lambda(x)$ называют *многочленом связей* этого регистра. Эти коэффициенты могут быть найдены с помощью алгоритма Берлекэмпа-Месси, приведенного на рисунке 3. После нахождения $\Lambda(x)$ могут быть найдены его корни, которые задают местоположение ошибок.

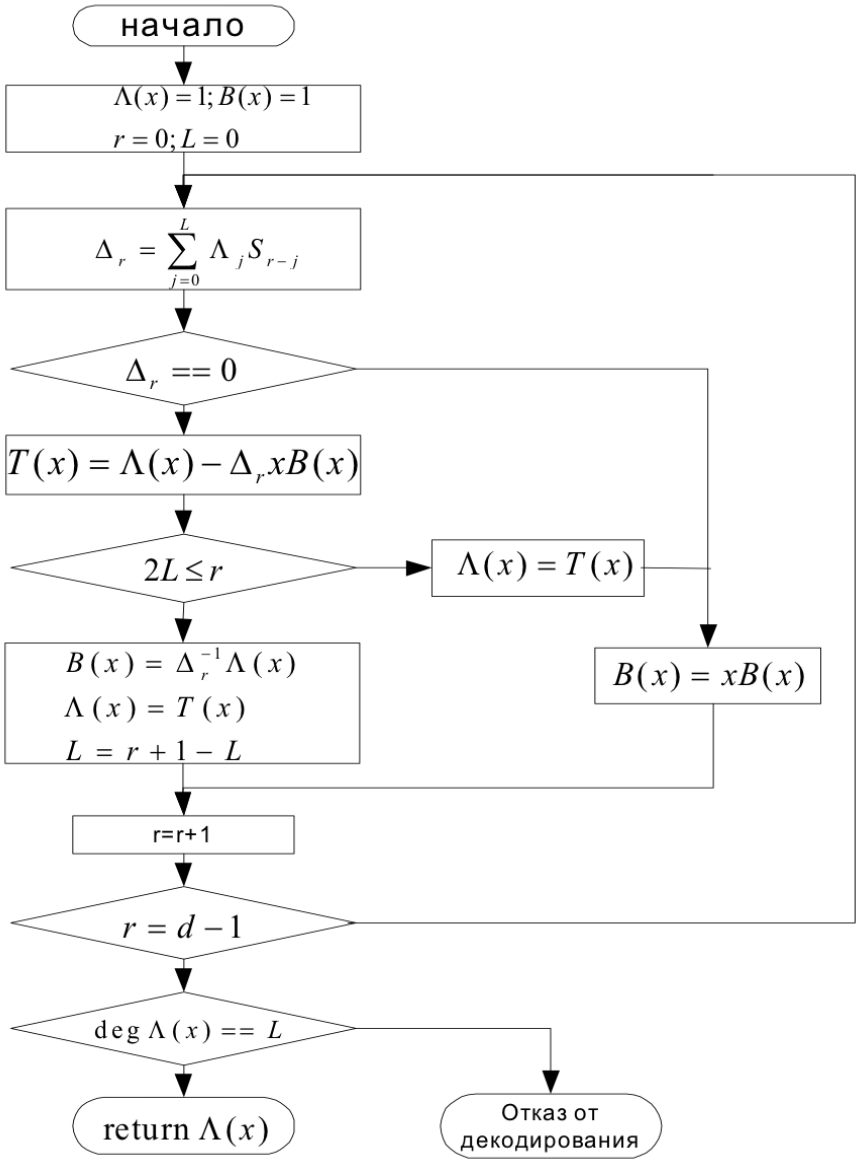

Рисунок 3. Алгоритм Берлекэмпа-Месси

Процедура вычисления синдрома, основанная на непосредственном применении (1.15), имеет сложность $O(dn)$, в то время как сложность алгоритма Берлекэмпа-Месси имеет сложность $O(d^2)$. Таким образом, вычисление синдрома и поиск корней многочлена локаторов ошибок являются наиболее трудоемкими этапами классической процедуры декодирования кодов Рида-Соломона.

Описанная процедура позволяет найти единственное кодовое слово кода (если оно существует), находящееся на расстоянии не более чем $[(d-1)/2]$ от декодируемого вектора. Однако на практике зачастую требуется исправление намного большего числа ошибок. В этом случае декодирование может быть неоднозначным, т.е. декодер может возвратить список. Следует также отметить, что ключевое уравнение может быть использовано и для исправления стираний. В этом случае можно считать, что i_j — номер j-го стертого символа, $y_{i_j} = 0$ и найти $\Gamma(x)$ непосредственно из (1.16).