УДК 621.396

АЛГОРИТМ ДИАГНОСТИКИ ЦИКЛИЧЕСКИХ КОДОВ НА ОСНОВЕ НЕПОСРЕДСТВЕННОГО ВЫЧИСЛЕНИЯ ПРОСТЫХ ПОЛИНОМОВ

Корнеева Наталья Николаевна
старший преподаватель кафедры радиотехники и радиосистем ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».
E-mail: korneevanata@list.ru.

Никитин Олег Рафаилович
доктор технических наук, профессор, заведующий кафедрой радиотехники и радиосистем ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».
E-mail: olnikitin@mail.ru.

Полушин Петр Алексеевич
доктор технических наук, профессор кафедры радиотехники и радиосистем ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».
E-mail: polushin.p@mail.ru.
Адрес: 600000, г. Владимир, ул. Горького, 87.

Аннотация: Диагностика циклических кодов состоит в определении общего множителя всех рассматриваемых кодовых блоков. Рассмотрен и исследован алгоритм диагностики циклических кодов, который основан на непосредственном вычисления простых полиномов, которые являются множителями полинома, описывающего кодовый блок. Данный диагностический алгоритм позволяет определять параметры циклических кодов в ситуации, когда информация о параметрах кодеров либо утрачена, либо неполная, либо отсутствует изначально. В результате использования описываемого алгоритма диагностики можно обеспечить требуемую помехоустойчивость и качество передачи информации. Представлены результаты исследования свойств диагностического алгоритма, при использовании количества наборов кодовых блоков N=6, и значения порождающего полинома: $\mathbf{g}=11_{10}=1011=X^3+X+1$. Показано сколько и каких полиномов-делителей обнаружено в каждом из шести кодовых слов. Представлен конечный результат работы диагностического алгоритма, т.е. правильно определён простой полином, содержащийся во всех кодовых блоках. Определены достоинства и недостатки данного алгоритма. Рассмотрена вероятность неправильной диагностики.

Ключевые слова: циклические коды, кодовый блок, простые полиномы, порождающие полиномы.

Постановка задачи

Значительное количество эксплуатируемых и проектируемых систем передачи информации в настоящее время использует цифровые сигналы. Это в определённой степени даёт возможности повышения качества передачи. Известны много методов кодирования, имеющих различные возможности по исправлению ошибок и требующие при практической реализации разного уровня усложнения аппаратуры приёмников и передатчиков. Если предположить, что вид и параметры кодирования, используемые в передатчике, на приёмной стороне полностью известны, то на их основе осуществляется соответствующая процедура декодирования. А если информация о кодере отсутствует или неполная, то процесс декодирования может стать проблемным и, как следствие - невозможность обеспечения требуемой помехоустойчивости и качества передачи информации. Известно, что процесс кодирования вносит определённые связи между передаваемыми закодированными символами. При этом последовательность ранее независимых символов становится структурированной [1-5]. Анализируя эти связи можно восстановить информацию об используемых параметрах кодера, которая раньше отсутствовала. Найденные

связи позволят восстанавливать структуру кодера на приёмной стороне и, как следствие, увеличивать помехоустойчивость передачи.

Так как в блоковых кодах все блоки сформированы с помощью одного кодера и по одинаковым правилам, то взаимосвязи между проверочными и информационными символами имеют одинаковый характер. Анализируя определённое количество блоков можно выявить эти взаимосвязи и восстановить структуру кода. При использовании циклических кодов кодирование заключается в применении порождающего полинома. Поэтому при сравнении определённого числа кодовых блоков можно определить общую часть их полиномов. Именно она описывает порождающий полином, используемый при кодировании в передатчике. Задача диагностики циклических кодов решается нахождением общего множителя всех рассматриваемых кодовых блоков. Наиболее простым вариантом для вычислений является определение для каждого полинома, описывающего кодовый блок, всех его полиномов, как сомножителей. Каждый кодовый блок может быть описан в виде полинома, который в свою очередь, разложен на простые множители – простые полиномы. Тот набор простых полиномов, которые описывают изменяющуюся информационную часть блока, различается в каждом блоке, а тот набор полиномов, произведение которых составляет искомый порождающий полином, является общим для всех кодовых блоков.

Теоретическая часть

Алгоритм диагностики представлен на рис. 1.

Первоначально производится отбор N кодовых блоков $y_1 \div y_N$. Затем полиномы этих блоков подаются поочерёдно на процедуру разделения на простые полиномы. Данная процедура носит частично циклический характер. Поочерёдно перебираются значения полиномов γ_k, начиная с наиболее простого, равного X (двоичное число 2) до $X^{n-1}+X^{n-2}+\ldots X+1$ (двоичное число, равное 2^n-1). Полином $\mathbf{y}_i$ очередного кодового слова проверяется на делимость на полином γ_k, и если он делится нацело, то делитель запоминается (деление производится в соответствии с правилами операций в полях Галуа). После этого частное от деления проверяется на равенство единице, и в случае неравенства опять повторяется деление на γ_k. Если же устанавливается, что полученный полином $\mathbf{y}_i/\gamma_k$ нацело на γ_k не делится, то происходит проверка делимости полинома $\mathbf{y}_i$ на следующий делитель γ_{k+1}.

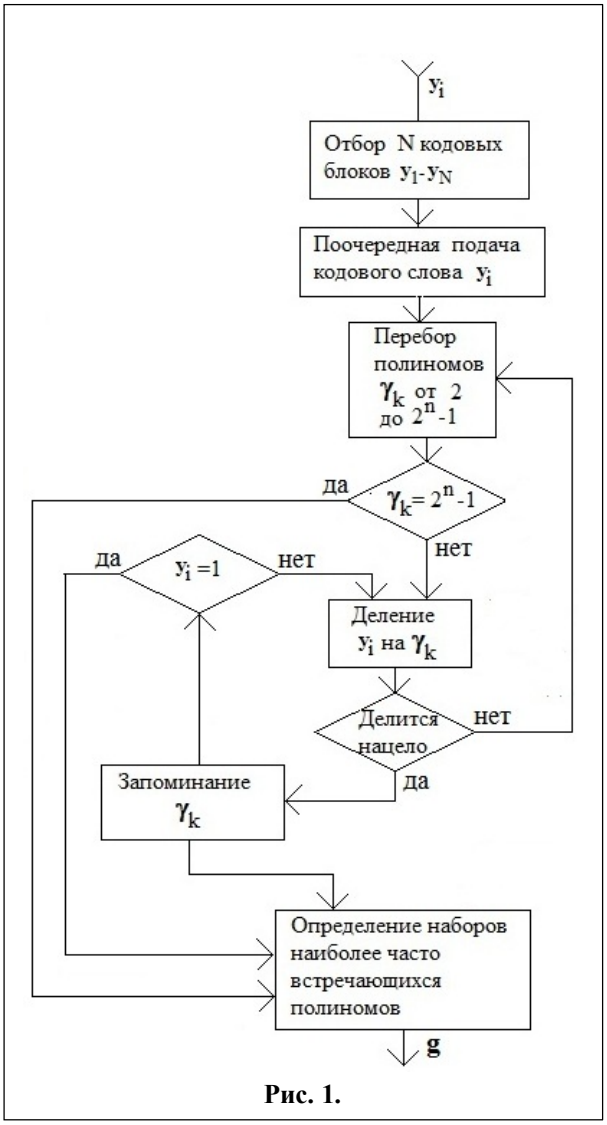

Рис. 1.

После декомпозиции на сомножители всех выбранных N кодовых блоков определяются наиболее часто встречающиеся простые полиномы, как делители. И хотя в информационных блоках некоторые простые полиномы тоже будут встречаться часто, но тем не менее, не во всех кодовых блоках. А те полиномы,

которые составляют порождающий полином, будут встречаться во всех блоках, поэтому чаще, чем все возможные другие. В результате именно их количество после окончания всей процедуры будет запомнено наибольшим. Таким образом, последняя операция анализа определит именно их, и представит как результат диагностики.

При исследованиях работы алгоритма задаётся длина k информационной части кодовых блоков и вид порождающего полинома g. Также задаётся различное число N кодовых блоков в анализируемом наборе. После этого информационная часть блоков имитируется случайной последовательностью нулей и единиц длиной k, в которой появление обоих вариантов значения символов равновероятно.

После этого производится блоковое кодирование, и полученный набор кодовых слов подвергается обработке с помощью описываемого алгоритма. Выявляются общие для всех блоков простые множители и из их произведения формируется оценка порождающего полинома.

Примеры результатов исследования свойств представлены на рис. 2-9, количество наборов кодовых блоков равняется N=6. Рис. 2-9 относятся к значению порождающего полинома: $\mathbf{g}=11_{10}=1011=X^3+X+1$. Рис. 2-7, показывают, сколько и каких полиномов-делителей обнаружено в каждом из шести кодовых слов. По горизонтальной оси рисунка отложена величина полиномов в десятичном выражении, по вертикальной оси отложено количество полиномов-делителей каждого значения.

Рис. 8, показывает полученные результаты в наглядной форме. Он сведён в матрицу, которая интерпретирована, как изображение. По горизонтальной оси отложены значения полиномов-делителей, соответствующие номерам столбцов матрицы, по вертикальной оси отложены номера кодовых блоков в наборе, соответствующие номерам строк матрицы. Цвет соответствующего элемента матрицы показывает количество полинома данного вида (потемнение от белого к черному указывает на возрастание значения элемента матрицы.)

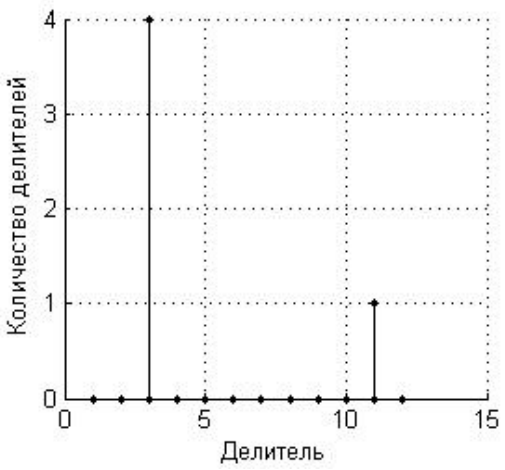

Рис. 2.

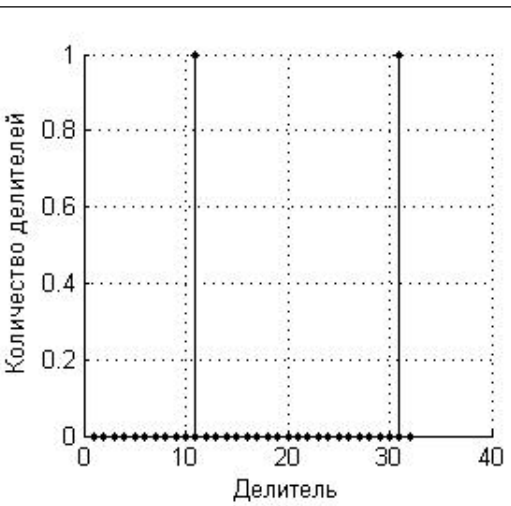

Рис. 3.

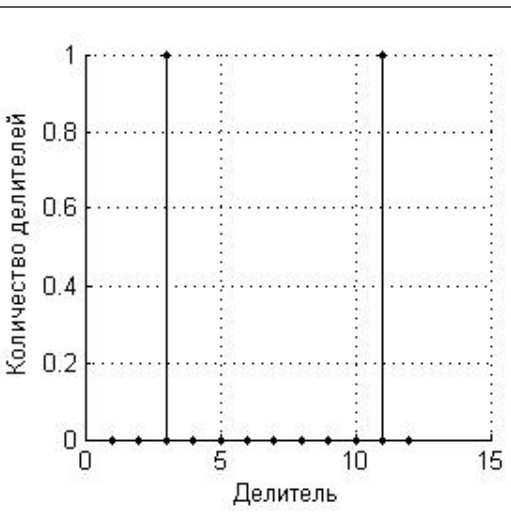

Рис. 4.

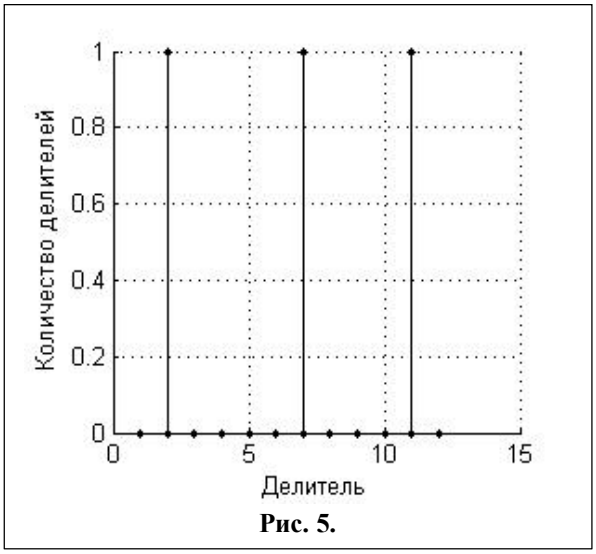

Рис. 5.

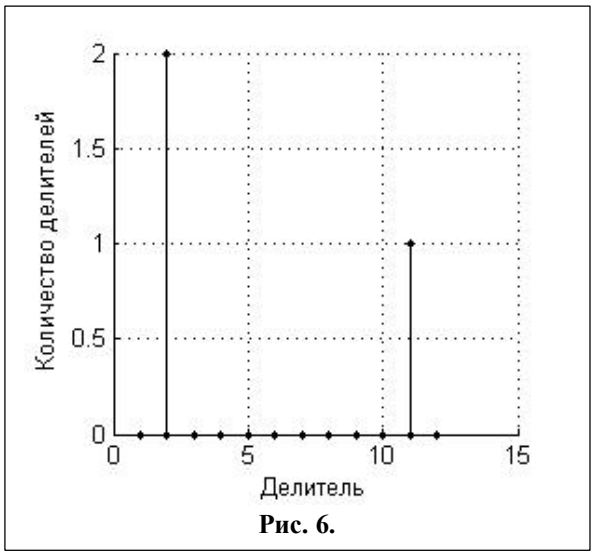

Рис. 6.

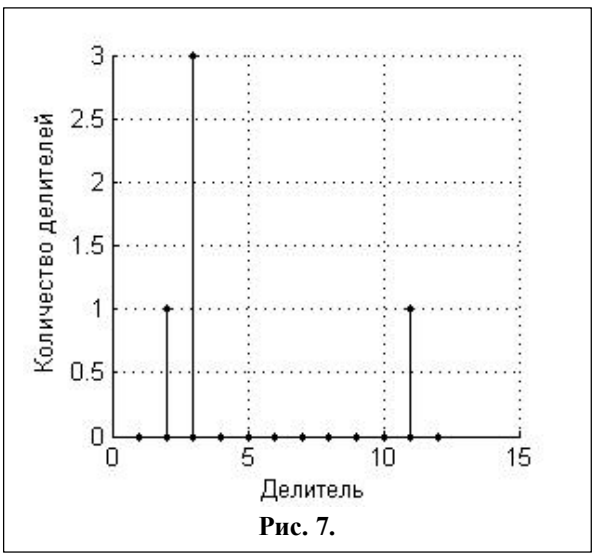

Рис. 7.

На рис. 9 представлен конечный результат анализа - обнаруженные общие для всех блоков множители. Рисунки указывают на правильный результат диагностики. Полином $\mathbf{g}=11_{10}$ является простым и на более короткие полиномы не разлагается.

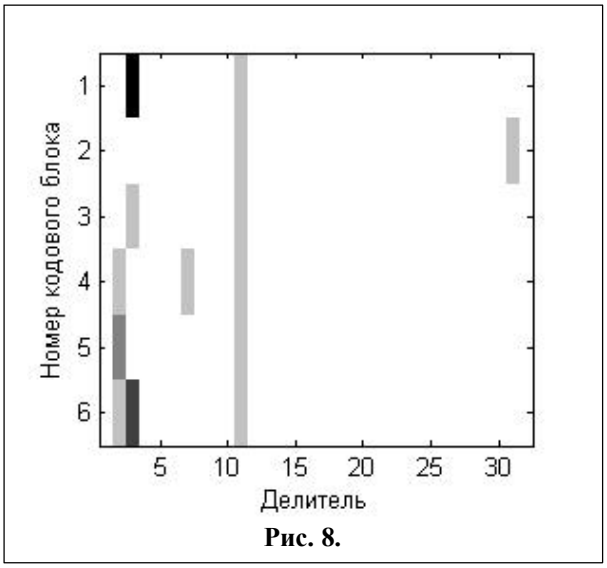

Рис. 8.

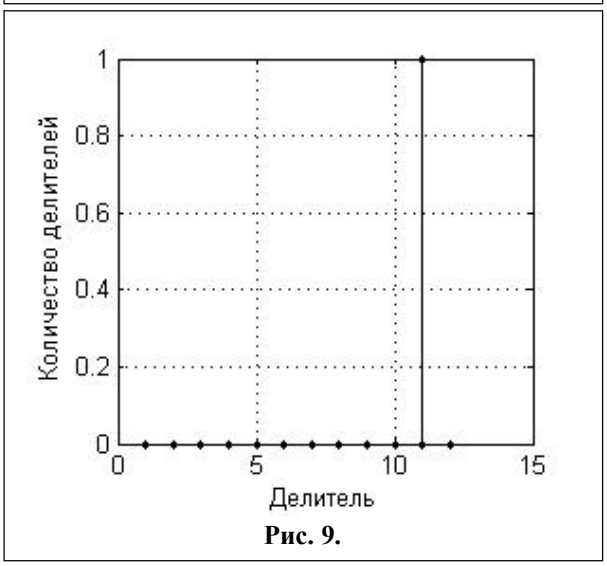

Рис. 9.

Рассмотрим вероятность неправильной диагностики. Поскольку в литературе не описана точная формула появления простых полиномов в возрастающем ряде полиномов, как и не известна соответствующая формула, относящаяся к натуральному ряду, будем использовать грубую оценку [6-13].

Ошибка появится, если во всех информационных частях кодовых блоков будет появляться один и тот же полином, не входящий в порождающий полином. Известно, что самым распространенным полиномом является полином, равный X (половина всех кодовых блоков делится на 2), то рассмотрим этот полином.

Вероятность того, что информационная часть конкретного кодового блока окажется четной, равна 1/2. Поэтому вероятность того, что в информационных частях N рассматриваемых блоков появится множитель 2, равна 2^{-N}. При увеличении количества анализируемых кодовых блоков эта величина быстро убывает, становясь меньше типового значения допустимой символьной ошибки.

Множители, большие, чем 2, появляются в полиномах, описывающих информационную часть кодовых блоков, с меньшей вероятностью, поэтому их влияние на появление диагностической ошибки существенно меньше.

Главным недостатком представленного алгоритма является существенное возрастание длительности вычислений при увеличении величины кодового слова n. Каждый кодовый блок длиной n символов должен быть проанализирован на декомпозицию на простые множители. Перебор чисел M от 2 до $M=2^n$ в отношении разложения на простые множители (число M представляется в двоичном варианте) покажет то, что некоторые числа будут простыми, а некоторые будут сложными, разлагаемыми на более простые полиномы. Эта операция занимает длительное время. Но даже если считать, что все операции занимают одинаковое время, то анализ каждого числа займет минимум $M=2^n$ элементарных операций разложения на множители.

Таким образом, с учётом сказанного, время обработки результатов возрастает минимально в пропорции к величине 2^n от длины n кодового блока [14-15]. В практическом применении время обработки при увеличении длины кодового блока растёт очень быстро.

Описанный алгоритм, который является естественным простым решением диагностической задачи, имеет смысл применять только при относительно коротких кодовых блоках. Для более длинных кодовых блоков необходимо использовать другие алгоритмы, укорачивающие время анализа.

Выводы

При осуществлении диагностики систематических и несистематических циклических кодов может быть использован алгоритм, использующий сравнение набора простых полиномов, на которые разлагаются кодовые блоки.

Поступила 15 декабря 2016 г.

Предлагаемый алгоритм желательно использовать только при относительно коротких кодовых блоках.

Литература

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение/ пер. с англ. – М.: Изд. дом “Вильямс”, 2003. – 1104с.

2. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2006. – 320 с.

3. Полушин П.А., Самойлов А.Г. Избыточность сигналов в радиосвязи. – М.: Радиотехника, 2007. – 256 с.

4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 593 с.

5.Никитин О.Р., Полушин П.А., Белов А.Д., Бессмертный М.Ю. О возможности определения параметров кодера по принимаемому цифровому сигналу/ Материалы МНТК «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2015» (REDS-2015), Москва, 2015. – С. 61-63.

6. Немировский А.С., Рыжков Е.В. Системы связи и радиорелейные линии. – М.: Связь, 1980. – 432 с.

7. Помехоустойчивость и эффективность систем передачи информации / А.Г. Зюко и др.; под ред. А.Г. Зюко. – М.: Радио и связь, 1985. – 272 с.

8. Сергиенко, А.Б. Цифровая обработка сигналов. – СПб.: Питер, 2003. – 604 с.

9. Massey, J.L. Threshold Decoding. – MIT Press, 1963. – 278 p.

10. Berou C., Glavieux A., Thitimajshima P. New Shannon Limit Error-Cjrrecting Coding and Decoding: Turbo Codes. // IEEE Proceedings of the Int. Conf. on Communications, Geneva, Switzerland, May, 1993. – pp. 1064-1070.

11. Clark G., Cain J. Error Correction Coding for Digital Communication // Plenum Press, 1981. – pp. 21-26.

12. Lin S., Costello D.J. Error Control Coding: Fundamentals and Applications. // Prentice-Hall, 1983.– 101 p.

13. Корнеева Н.Н., Никитин О.Р. Декодирование циклических кодов при неизвестной структуре кодера // 11-я МНТК «Перспективные технологии в средствах передачи информации – ПТСПИ-2015» – Владимир–ВлГУ–2015 – С.156-158.

14. Финк Л.М. Теория передачи дискретных сообщений. – М.: Советское радио, 1970. – 728 с.

15. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой.– М.: Связь, 1979.– 272 с.

English

Cyclic code diagnostic algorithm based on direct calculation of simple polynoms

Natalya Nikolaevna Korneeva – Senior Lecturer Department of Radio Engineering and Radio Systems "Vladimir State University named after Alexader Grigoryevich and Nickolay Grigoryevich Stoletovs".

Oleg Rafailovich Nikitin – Doctor of Engineering, Professor Head of the Department of Radio Engineering and Radio Systems "Vladimir State University named after Alexader Grigoryevich and Nickolay Grigoryevich Stoletovs".

Pyotr Alekseevich Polushin – Doctor of Engineering, Professor Department of Radio Engineering and Radio Systems "Vladimir State University named after Alexader Grigoryevich and Nickolay Grigoryevich Stoletovs".

Address: 600000, Vladimir, st. of Gorky, 87.

Abstract: One of the main problems of communication is signal recovery in receiving. It is known that all blocks of the code block are formed according to the same rules and by the same coder. It can be assumed that interrelation between checking and information symbols are the same irrespective of the transmitted data. Thus recovery of the coder structure in the receiving part is possible when diagnosing the received code sequences. When using cyclic codes, diagnostics consists in possibility to reveal interrelations between checking and information symbols of each block. When comparing sufficient number of code blocks it is possible to define a common part. Here identical parts are those parts of code blocks which describe the generating polynom used for coding in the transmitter. Cyclic code diagnostic algorithm based on direct calculation of simple polynoms is described. In this case the length of information part of code blocks and the type of the generating polynom is defined. Also the different number of code blocks in the analyzed set is defined. Information part of blocks is imitated by random sequence of zeros and ones. The studied diagnostic algorithm involves calculation for each code block of simple polynoms set as multipliers into which this block is decomposed. Then information accumulating process follows about the frequency of emerging simple polynoms. Further the analysis of blocks and the choice of simple multipliers set is made. Examples of research results are given for the generating polynom value: **g=**11_{10}=1011=X^3+X+1, number of code blocks N=6, to value of the information sequence length equal to k=5. It is shown that the diagnostic result i.e. the multipliers, general for all blocks, are defined correctly. The probability of the wrong diagnostic is examined.

Key words: cyclic codes, the code block, simple polynoms, generating polynoms.

References

1. Sklar B. Digital Communications: Fundamentals and Applications. - Transl. from English - M.: Publ. house "Williams", 2003. – 1104p.
2. Morelos-Zaragoza, R. The art of error correcting coding. Methods, algorithms, application. - M.: Technosfera, 2006. - 320 p.
3. Polushin P.A., Samoylov A.G. Signal redundancy in radio communication. - M.: Radiotekhnika, 2007. - 256 p.
4. Peterson W., Weldon E. Error-Correcting Codes. - M.: Mir, 1976. - 593 p.
5. Nikitin O.R., Polushin P.A., Belov A.D., Bessmertny M.Yu. On possibility to define the coder parameters via received digital signal. - Materials of ISTC "Radio-electronic Devices and Systems for Infocommunication Technologies - REUS-2015" (REDS-2015), Moscow, 2015. – P. 61-63.
6. Nemirovskiy A.S., Ryzhkov E.V. Communication systems and radio relay lines. - M.: Svyaz 1980. - 432 p.
7. Noise resistance and efficiency of information transmission systems. Ed. by A.G. Zyuko. - M.: Radio i svyaz 1985. - 272 p.
8. Sergienko, A.B. Digital signal processing. - SPb.: Piter, 2003. - 604 p.
9. Massey J.L. Threshold Decoding. - MIT Press, 1963. - 278 p.
10. Berou C., Glavieux A., Thitimajshima P. New Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes. - IEEE Proceedings of the Int. Conf. on Communications, Geneva, Switzerland, May, 1993. - pp. 1064-1070.
11. Clark G., Cain J. Error Correction Coding for Digital Communication. - Plenum Press, 1981. - pp. 21-26.
12. Lin S., Costello D.J. Error Control Coding: Fundamentals and Applications. - Prentice-Hall, 1983. - 101 p.
13. Korneeva N.N., Nikitin O.R. Cyclic code decoding with the coder unknown structure. - the 11th IS TC "Perspective Technologies in Information Transmission Systems - PTSPI-2015" - Vladimir - VLGU-2015 – P. 156-158.
14. Fink L.M. Discrete-message Communication Theory. - M.: Sovetskoye radio, 1970. - 728 p.
15. Korzhik V.I., Fink L.M. Noise resistant coding of discrete messages in channels with random structure. - M.: Svyaz, 1979. - 272 p.