УДК 004.021

Алгоритм вычисления минимальных кодовых расстояний CRC как блочного кода

А. А. Блюдов, Г. Ю. Пронин

Петербургский государственный университет путей сообщения Императора Александра I, Россия, 190031, Санкт-Петербург, Московский пр., 9

Для цитирования: *Блюдов А. А., Пронин Г. Ю.* Алгоритм вычисления минимальных кодовых расстояний CRC как блочного кода // Бюллетень результатов научных исследований. 2026. Вып. 2. С. 176–186. DOI: 10.20295/2223-9987-2026-2-176-186

Аннотация

Цель: разработать алгоритм, позволяющий определить минимальное кодовое расстояние CRC как блочного кода для различных значений длин информационной части. Разработать способ, позволяющий определить целесообразность применения CRC в качестве блочного помехозащитного кода (в данной статье имеется в виду, что для определенного количества информационных разрядов минимальное кодовое расстояние будет равняться двум). **Методы:** для проведения экспериментальных исследований использовалось компьютерное моделирование с использованием интерпретируемого программного языка общего назначения Python. Для теоретических исследований применены метод аналитического обзора, теория помехозащитного кодирования. **Результаты:** в качестве вспомогательного инструмента описан и применен способ определения верхних границ минимальных кодовых расстояний для кодов CRC. Описан способ определения количества информационных разрядов, при котором применение CRC в качестве помехозащитного кода перестает быть эффективным. Предложен и описан алгоритм расчета минимальных кодовых расстояний CRC как блочного кода для различного количества информационных разрядов. Результатом работы алгоритма являются параметры кодов с различными минимальными расстояниями Хэмминга, для которых отношение минимального кодового расстояния к количеству информационных разрядов является максимально возможным для заданного полинома. Получены параметры блочных кодов для популярных полиномов CRC8. **Практическая значимость:** получен алгоритм, позволяющий определить параметры искомых кодов, образованных полиномами от CRC до CRC32 включительно за разумное время. Это позволяет определить минимальные кодовые расстояния для другого количества информационных разрядов, при условии что минимальное кодовое расстояние больше двух. Приведены результаты применения алгоритма для популярных полиномов CRC8.

Ключевые слова: помехозащитное кодирование, циклический избыточный код, CRC, минимальное кодовое расстояние, разделимые коды

Введение

CRC-коды получили широкое распространение в различных областях техники [1–3]. В современных системах автоматики, в том числе железнодорожной, для обнаружения ошибок в процессе приема-передачи информации применяются блочные CRC-коды [4, 5]. Несмотря на их широкое распространение в системах передачи информации, ряд вопросов, связанных с применением CRC, остается нерешенным [6–8]. На данный момент при проектировании системы передачи информации у инженеров есть выбор из множества образующих полиномов, но в общем случае нет ответа на вопрос «Какое минимальное кодовое расстояние даст этот полином, если закодировать n бит?». Современные вычислительные мощности позволяют решить эту задачу путем полного перебора. В случае если длина информационного вектора и образующего полинома невелика, то это не займет много времени. В случае использования CRC16 и CRC32 количество полиномов, пригодных для использования, возрастает, а вместе с ним значительно увеличивается и время выбора полинома. Это приводит к тому, что применяется какой-либо распространенный полином, а защитные свойства кода не исследуются.

В данной статье изучены способы вычисления минимального кодового расстояния в зависимости от количества информационных разрядов для произвольных полиномов.

Под CRC понимается Cyclic Redundancy Code, образуемый по правилу [9]:

$$R(x) = P(x) \cdot x^N \mathrm{mod} G(x),$$

где $R(x)$ — полином, представляющий значение CRC;
$P(x)$ — полином, представляющий информационный вектор;
$G(x)$ — порождающий полином;
N — степень порождающего полинома.

Дополнительные манипуляции, такие как ненулевое стартовое значение, отражение векторов до и после вычисления, а также сложение результата вычислений с константой, не рассматриваются.

Определение границы эффективности для минимального кодового расстояния 2

Для определения целесообразности применения CRC как блочного кода определим количество информационных битов в коде, при котором минимальное кодовое расстояние [10] $d = 2$. Такое расстояние Хэмминга может быть получено путем применения бита четности/нечетности, что говорит о неэффективности применения CRC.

Так как CRC — это линейный код [9], то любое кодовое слово может быть получено путем линейной комбинации (сложения по модулю 2) двух разрешенных кодовых слов. При этом не существует такой пары разрешенных кодовых слов, что их линейная комбинация не будет входить в код. Таким образом, чтобы двукратная ошибка привела к необнаруживаемому искажению, ее вектор должен совпадать с разрешенным кодовым словом. Поскольку при использовании вышеописанного правила расчета CRC-код будет включать нулевое кодовое слово, то для заданного полинома нахождение кода с параметрами (n, k, 2) сводится к поиску разрешенного кодового слова, в котором будет две единицы.

Так как CRC представляет собой разделимый код, то существует три возможных распределения единиц между информационной и контрольной частями:

1. Две единицы в кодовой части — невозможно для используемого правила расчета CRC.

2. Одна единица в информационной части; одна единица в контрольной части.

3. Две единицы в информационной части.

Рассмотрим второй случай: одна единица в информационной и одна в контрольной частях. Рассчитаем контрольные векторы от информационных с весом 1. Количество остатков от деления не может превышать 2^{N-1} (для CRC8 это 256), а значит, начнут повторяться. В качестве примера выберем полином 0b100111001 (0x139), так как в его случае первое повторение контрольного вектора начинается после 17-го информационного вектора. Рассчитаем контрольное значение от информационных слов с весом 1 для полинома 0x139. Результаты расчета приведены в табл. 1.

ТАБЛИЦА 1. Контрольные векторы для полинома 0x139

k	$P(x)$	$R(x)$	$d(R(x), 0)$
1	1	00111001	4
2	10	01110010	4
3	100	11100100	4
4	1000	11110001	4
5	10000	11011011	5
6	100000	10001111	5
7	1000000	00100111	4
8	10000000	01001110	4
9	100000000	10011100	4
10	1000000000	00000001	2
11	10000000000	00000010	2
12	100000000000	00000100	2
13	1000000000000	00001000	2
14	10000000000000	00010000	2
15	100000000000000	00100000	2
16	1000000000000000	01000000	2
17	10000000000000000	10000000	2

В данной таблице рассмотрены 17 кодовых слов, так как при дальнейшем расчете при $P(x)$ = 100000000000000000 (k = 18), $R(x)$ = 00111001. Все дальнейшие значения контрольной части будут циклически повторяться [9]. Длина этого цикла отличается для полиномов с одинаковым числом бит и не превышает максимальное возможное количество контрольных значений $2^N - 1$. Вычисление следующего значения $R(x)$ в таблице эквивалентно следующей операции:

$$\text{если } \deg\left(x \cdot R(x)_{t-1}\right) \neq N, \text{ то } R(x)_t = x \cdot R(x);$$

$$\text{если } \deg\left(x \cdot R(x)_{t-1}\right) = N, \text{ то } R(x)_t = x \cdot R(x) \oplus P(x).$$

Данная таблица заканчивается на 00000001, 00000010, 00000100, 00001000, 00010000, 00100000, 01000000, 10000000. Аналогично будут заканчиваться все таблицы [9]. Таким образом, для каждого полинома можно найти параметры кода, при котором минимальное кодовое расстояние равно двум. В данном случае это (18, 10, 2). Из табл. 1 видно, что для того чтобы кодовое расстояние было равно 2, а вес контрольной части равнялся нулю, то $P(x)$ = 100000000000000001. Из этого можно сделать вывод, что длина кодового слова, вес информационной и контрольной частей которого равен 1, будет всегда меньше. Значит, этим способом можно определить количество информационных разрядов, при котором минимальное кодовое расстояние будет равно 2, а применение CRC в качестве блочного кода будет нецелесообразным.

Определение параметров граничных кодов для других минимальных кодовых расстояний

Максимальное возможное кодовое расстояние, которое можно получить с помощью образующего полинома, равно количеству единиц в этом полиноме. Это видно, если рассмотреть код, в котором один информационный бит. Для рассматриваемого в качестве примера полинома 0x139 это будут два кодовых слова 000000000 и 100111001, а параметры кода (9, 1, 5). При увеличении количества информационных разрядов минимальное кодовое расстояние будет уменьшаться. Важно отметить, что в общем случае необязательно существуют коды с минимальными кодовыми расстояниями от N до 2. Перед непосредственным поиском кодовых алфавитов определим граничные параметры. Для этого в табл. 2 посчитаем количество единиц в кодовых словах для полинома 0b111010111 (0x1D7), так как этот пример нагляднее предыдущего.

ТАБЛИЦА 2. Контрольные векторы для полинома 0x1D7

k	$R(x)$	$d(R(x), 0)$
1	11010111	7
2	01111001	6
3	11110010	6

Окончание табл. 2

k	$R(x)$	$d(R(x), 0)$
4	00110011	5
5	01100110	5
6	11001100	5
7	01001111	6
8	10011110	6
9	11101011	7
10	00000001	2
11	00000010	2
12	00000100	2
13	00001000	2
14	00010000	2
15	00100000	2
16	01000000	2
17	10000000	2

Так как в табл. 1 и 2 фактически приведены контрольные части кодовых слов от информационных векторов весом 1, то можно сделать вывод, что минимальное кодовое расстояние в коде с количеством информационных разрядов весом k не может превышать сумму весов соответствующего контрольного и информационного векторов. На основании данных, приведенных в табл. 2, определим максимально возможное количество информационных разрядов в кодовых алфавитах, образованных полиномом 0x1D7, для минимальных кодовых расстояний (2, 7). Для этого запишем минимальное количество информационных разрядов для соответствующих кодовых расстояний. В случае если кодовое расстояние отсутствует, ему присваивается значение, соответствующие следующему минимальному кодовому расстоянию.

ТАБЛИЦА 3. Верхние границы информационных разрядов для минимальных кодовых расстояний блочного CRC 0x1D7

d	$k_{max}(d)$
7	1
6	2
5	4
4	10
3	10
2	10

Алгоритм поиска кодовых слов с минимальным кодовым расстоянием

При поиске кодовых слов с минимальным кодовым расстоянием будем исходить из следующих предпосылок:

1. Всех минимальных кодовых расстояний в отрезке (2, N) может не существовать.

2. В случае если вес информационного вектора больше, чем минимальное кодовое расстояние, то проверка бессмысленна.

Алгоритм поиска кодовых слов с минимальным кодовым расстоянием (см. рисунок):

1. Выбирается и фиксируется проверяемый полином $G(x)$.

2. По формуле $R(x) = P(x) \cdot x^N \mathrm{mod} G(x)$ рассчитывается первый контрольный полином от информационного полинома $P(x) = 1$.

3. Выбирается следующий информационный полином $P(x)_{t+1} = x \cdot P(x)_t$.

4. От него рассчитывается следующий контрольный полином.

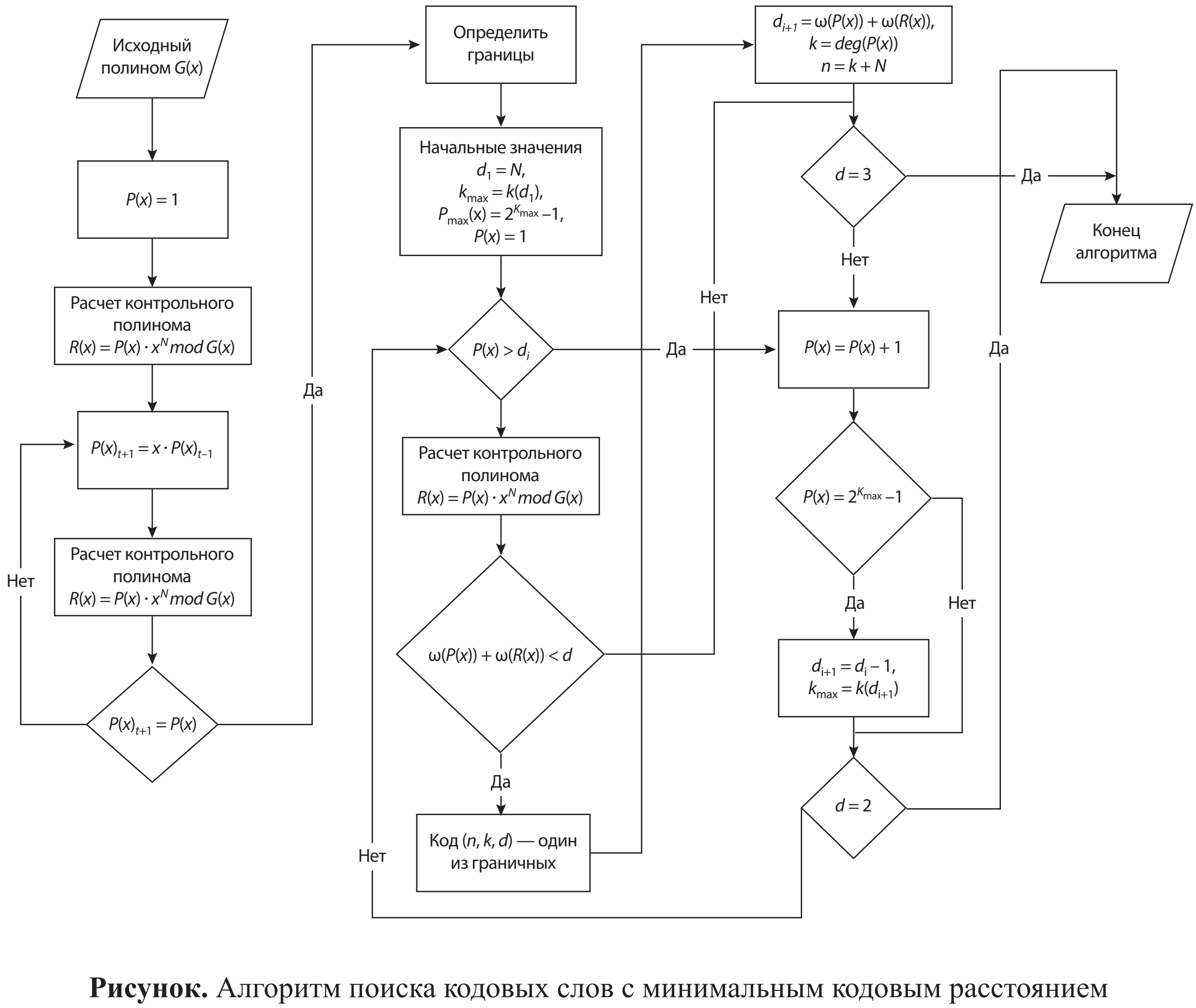

Рисунок. Алгоритм поиска кодовых слов с минимальным кодовым расстоянием

5. Пункты 3 и 4 повторяются до тех пор, пока значение контрольного полинома не совпадет с первым полиномом.

6. Определить границы. Для минимальных кодовых расстояний от N до 2 определяются максимальное возможное количество информационных разрядов.

7. Определить начальные значения $d_1 = N$, $k_{max} = k(d_1)$, $P_{max}(x) = 2^{k_{max}} - 1$, $P(x) = 1$.

8. Если вес информационного полинома больше искомого, перейти к пункту 12.

9. Рассчитать контрольный полином.

10. Если $\omega(P(x) + \omega(R(x)) < d$, то $d_{i+1} = \omega(P(x)) + \omega(R(x))$, $k = \deg(P(x))$, $n = k + N$, то запомнить код с параметрами (n, k, d).

11. Если $d = 3$, то перейти к пункту 16.

12. Увеличить $P(x)$ на единицу.

13. Если $P(x) = 2^{k_{max}} - 1$, то $d_{i+1} = d_i - 1$, $k_{max} = k(d_{i+1})$.

14. Если $d = 2$, то перейти к пункту 16.

15. Перейти к пункту 8.

16. Конец алгоритма.

Далее приводятся результаты использования алгоритма (табл. 4). Для облегчения восприятия для каждого полинома приведен код с $k = 1$.

ТАБЛИЦА 4. Таблица зависимости минимального кодового расстояния от длины

Полином в двоичном виде	Полином в шестнадцатеричном виде	Граничные коды n, k, d
100011011	1B	(9, 1, 5) (30, 22, 4) (52, 44, 2)
100011101	1D	(9, 1, 5) (15, 7, 4) (26, 18, 3) (256, 248, 2)
100101011	2B	(9, 1, 5) (21, 13, 4) (68, 60, 3) (256, 248, 2)
100101101	2D	(9, 1, 5) (12, 8, 4) (39, 31, 3) (256, 248, 2)
100111111	3F	(9, 1, 7) (12, 8, 6) (13, 5, 5) (18, 10, 4) (28, 20, 3) (86, 78, 2)
101001101	4D	(9, 1, 5) (24, 16, 3) (256, 248, 2)
101011111	5F	(9, 1, 7) (11, 8, 4) (49, 41, 3) (256, 248, 2)
101100011	63	(9, 1, 5) (13, 5, 4) (24, 16, 3) (256, 248, 2)
101100101	65	(9, 1, 5) (31, 23, 4) (41, 33, 3) (256, 248, 2)
101101001	69	(9, 1, 5) (17, 8, 3) (256, 248, 2)
101110001	71	(9, 1, 5) (16, 8, 4) (36, 28, 3) (256, 248, 2)
101110111	77	(9, 1, 7) (11, 3, 6) (12, 4, 3) (86, 78, 2)
101111011	7B	(9, 1, 7) (11, 3, 6) (12, 4, 5) (17, 8, 3) (86, 78, 2)

Окончание табл. 4

Полином в двоичном виде	Полином в шестнадцатеричном виде	Граничные коды n, k, d
110000111	87	(9, 1, 5) (10, 8, 4) (88, 80, 3) (256, 248, 2)
110001011	8B	(9, 1, 5) (22, 14, 4) (86, 78, 2)
110001101	8D	(9, 1, 5) (22, 14, 4) (60, 52, 3) (256, 248, 2)
110011111	9F	(9, 1, 7) (10, 2, 4) (52, 44, 2)
110100011	A3	(9, 1, 5) (13, 5, 4) (86, 78, 2)
110101001	A9	(9, 1, 5) (14, 6, 3) (256, 248, 2)
110110001	B1	(9, 1, 5) (15, 7, 4) (52, 44, 2)
110111101	BD	(9, 1, 7) (10, 2, 6) (11, 3, 5) (14, 6, 4) (26, 18, 3) (86, 78, 2)
111000011	C3	(9, 1, 5) (10, 2, 4) (54, 46, 3) (256, 248, 2)
111001111	CF	(9, 1, 7) (10, 2, 4) (28, 20, 3) (256, 248, 2)
111010111	D7	(9, 1, 7) (10, 2, 6) (12, 4, 5) (18, 10, 2)
111011101	DD	(9, 1, 7) (10, 2, 6) (12, 4, 3) (86, 78, 2)
111100111	E7	(9, 1, 7) (10, 2, 4) (116, 108, 3) (256, 248, 2)
111110011	F3	(9, 1, 7) (10, 2, 4) (52, 44, 2)
111110101	F5	(9, 1, 7) (10, 2, 6) (14, 6, 3) (256, 248, 2)
111111001	F9	(9, 1, 7) (10, 2, 4) (29, 21, 3) (86, 78, 2)

Заключение

В статье описан и предложен алгоритм вычисления минимальных кодовых расстояний CRC как блочного кода. Он определяет параметры кодов с минимальным отношением информационных разрядов к минимальному кодовому расстоянию для заданного полинома. Описанный в статье процесс вычисления параметров кодов применим только к классическому методу вычисления CRC. В случае если в процессе расчета применяются какие-либо модификации (например, ненулевое стартовое значение, отражение векторов до и после вычисления, а также сложение результата вычислений с константой), то результаты применения алгоритма могут быть недостоверны. В случае если анализируется классический метод расчета, то в качестве объекта исследования может быть использован любой полином вне зависимости от его длины и простоты.

Количество вычислений, применяемое в процессе поиска параметров кодов для полиномов, использующихся на практике, делает его применение без ЭВМ неэффективным. Для ускорения вычислений выполняется предварительная подготовка, которая определяет верхнюю границу количества информационных разрядов для кодовых расстояний от количества единиц в образующем полиноме до $d = 3$, а также точные параметры кода $(n, k, 2)$, при которых отношение k / d

является максимально возможным. Также большая эффективность данного алгоритма по сравнению с непосредственным вычислением параметров кодов путем их перебора достигается за счет учета факта линейности CRC.

В статье приведены результаты применения алгоритма для 29 полиномов, которые могут использоваться в качестве образующих в CRC8. Данный алгоритм может быть применен для оценки эффективности полиномов, в случае если CRC используется как блочный код в информационных сетях, что позволит выбрать максимально эффективный из них в зависимости от количества информационных разрядов, использующихся для передачи данных.

Список источников

1. Гуртова К.С. Метод защиты информации цифровых документов с помощью невидимых цифровых меток и его реализация // Современные информационные технологии и ИТ-образование. 2022. №1.

2. Потапова К.А. Идентификация данных с помощью RFID-меток // Вестник науки. 2023. №10(67).

3. Андреев Р.А., Попова Т.С., Федоров А.С. Методика проведения сигнального тестирования устройств с поддержкой «ЭРА-ГЛОНАСС» // International Journal of Professional Science, 2022. № 5.

4. Прохорова Г.М. Оборудование станции устройствами микропроцессорной централизации ЭЦ-ЕМ с увязкой с системой диагностирования и мониторинга (АДК-СЦБ) // Форум молодых ученых. 2017. №6(10).

5. Калинин Т.С. Спектрально-сигнатурная диагностика микропроцессорных информационно-управляющих систем железнодорожной автоматики и телемеханики // Инженерный вестник Дона. 2012. № 1.

6. Семеренко В.П. Теория и практика CRC-кодов: новые результаты на основе автоматных моделей // Восточно-Европейский журнал передовых технологий. 2015. №9 (76).

7. Nuriddinov Q., Azizov A., Abdullaev R. Method of Optimization and Protection of Diagnostic Data in Monitoring Railway Automation Devices // Universum: Technical sciences. 2023. No. 5–7 (110).

8. Абдуллаев Р.Б. Определение числа необнаруживаемых ошибок циклическими кодами // Universum: технические науки. 2025. №10(139).

9. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / пер. с англ.; под ред. Р.Л. Добрушина, С.И. Самойленко. 2-е изд., перераб. и доп. М.: Мир, 1976.

10. Hamming R.W. Error Detecting and Error Correcting Codes // The Bell System Technical Journal. 1950. No. 2, vol. 29. DOI: 10.1002/j.1538–7305.1950.tb00463.x

Дата поступления: 05.04.2026
Решение о публикации: 24.05.2026

Контактная информация:
БЛЮДОВ Антон Александрович — кандидат техн. наук, доцент; bludov@pgups.ru
ПРОНИН Георгий Юрьевич — аспирант; georgiy3pronin@yandex.ru

Algorithm for Computing Minimum Code Distances of CRC as a Block Code

A. A. Blyudov, G. Yu. Pronin

Emperor Alexander I Petersburg State Transport University, 9 Moskovsky ave., Saint Petersburg, 190031, Russia

For citation: *Blyudov A. A., Pronin G. Yu.* Algorithm for Computing Minimum Code Distances of CRC as a Block Code // Bulletin of Scientific Research Results, 2026, iss. 2, pp. 176–186. DOI: 10.20295/2223-9987-2026-2-176-186 (In Russian)

Abstract

Objective: to develop an algorithm for determining the minimum code distance of a CRC as a block code for various data part lengths. To develop a method for determining the feasibility of using CRC as a block noise-protection code (in this article, it is implied that for a certain number of data bits, the minimum code distance will be equal to two). **Methods:** computer simulation using the general-purpose interpreted programming language Python was used for experimental studies. The analytical review method and the theory of noise-protection coding were applied for theoretical studies. **Results:** a method for determining the upper bounds of minimum code distances for CRC codes is described and applied as an auxiliary tool. A method for determining the number of data bits at which the use of CRC as a noise-protection code ceases to be effective is described. An algorithm for calculating the minimum code distances of a CRC as a block code for various numbers of data bits is proposed and described. The algorithm yields parameters for codes with different minimum Hamming distances, for which the ratio of the minimum code distance to the number of data bits is the maximum possible for a given polynomial. Parameters for block codes for popular CRC8 polynomials are obtained. **Practical significance:** an algorithm has been developed that allows one to determine the parameters of sought-after codes formed by CRC polynomials up to and including CRC32 in a reasonable time. This allows one to determine minimum code distances for a different number of data bits, provided that the minimum code distance is greater than two. Results from applying the algorithm to popular CRC8 polynomials are presented.

Keywords: error-correcting coding, cyclic redundancy code, CRC; minimum code distance, separable codes

References

1. Gurtova K. S. Metod zashchity informatsii tsifrovykh dokumentov s pomoshch'yu nevidimykh tsifrovykh metok i ego realizatsiya [Method for Protecting Information of Digital Documents Using Invisible Digital Watermarks and Its Implementation], *Sovremennye informatsionnye tekhnologii i IT-obrazovanie [Modern Information Technologies and IT Education]*, 2022, no. 1. (In Russian)

2. Potapova K. A. Identifikatsiya dannykh s pomoshch'yu RFID-metok [Data Identification Using RFID Tags], *Vestnik nauki [Bulletin of Science]*, 2023, no. 10 (67). (In Russian)

3. Andreev R. A., Popova T. S., Fedorov A. S. Metodika provedeniya signal′nogo testirovaniya ustrojstv s podderzhkoj "ERA-GLONASS" [Methodology for Signal Testing of Devices Supporting ERA-GLONASS], *International Journal of Professional Science*, 2022, no. 5. (In Russian)

4. Prokhorova G. M. Oborudovanie stantsii ustrojstvami mikroprotsessornoj tsentralizatsii ETs-EM s uvyazkoj s sistemoj diagnostirovaniya i monitoringa (ADK-STSB) [Equipping a Station with Microprocessor Centralization Devices ETS-EM with Coordination with the Diagnostic and Monitoring System (ADC-SCB)], *Forum molodykh uchenykh [Forum of Young Scientists]*, 2017, no. 6 (10). (In Russian)

5. Kalinin T. S. Spektral′no-signaturnaya diagnostika mikroprotsessornykh informatsionno-upravlyayushchikh sistem zheleznodorozhnoj avtomatiki i telemekhaniki [Spectral-Signature Diagnostics of Microprocessor Information and Control Systems for Railway Automation and Telemechanics], *Inzhenernyj vestnik Dona [Engineering Bulletin of the Don]*, 2012, no. 1. (In Russian)

6. Semerenko V. P. Teoriya i praktika CRC-kodov: novye rezul′taty na osnove avtomatnykh modelej [Theory and Practice of CRC Codes: New Results Based on Automaton Models], *Vostochno-Evropejskij zhurnal peredovykh tekhnologij [Eastern-European Journal of Enterprise Technologies]*, 2015, no. 9 (76). (In Russian)

7. Nuriddinov Q., Azizov A., Abdullaev R. Method of Optimization and Protection of Diagnostic Data in Monitoring Railway Automation Devices, *Universum: Technical Sciences*, 2023, no. 5–7 (110).

8. Abdullaev R. B. Opredelenie chisla neobnaruzhivaemykh oshibok tsiklicheskimi kodami [Determination of the Number of Undetected Errors by Cyclic Codes], *Universum: Technical Sciences*, 2025, no. 10 (139). (In Russian)

9. Peterson W., Weldon E. Error-Correcting Codes; translated from English; edited by R. L. Dobrushin, S. I. Samoilenko, 2nd ed., revised and enlarged. M.: Mir, 1976, 594 p. (In Russian)

10. Hamming R. W. Error Detecting and Error Correcting Codes, *The Bell System Technical Journal*, 1950, vol. 29, no. 2, pp. 147–160. DOI: 10.1002/j.1538-7305.1950.tb00463.x

Received: April 05, 2026
Accepted: May 24, 2026

Author's information:
Anton A. BLYUDOV — PhD in Engineering, Associate Professor; bludov@pgups.ru
Georgiy Yu. PRONIN — Postgraduate Student; georgiy3pronin@yandex.ru