УДК 621.391.15

С.Н. НИКОЛАЕВ, А.Н. РОМАНОВ

МЕТОД РАСПОЗНАВАНИЯ ПАРАМЕТРОВ ПОМЕХОУСТОЙЧИВЫХ БЛОЧНЫХ ЦИКЛИЧЕСКИХ КОДОВ ПО ОБРАЗУЮЩЕМУ ПОЛИНОМУ

Аннотация. Описана суть помехоустойчивого блочного циклического кодирования. Рассмотрен метод распознавания параметров такого кода полным перебором при отсутствии априорной информации. Определено количество необходимых для этого вычислений. Показано, что использование такого метода в реальных условиях затруднительно. Исследованы известные образующие полиномы, применение которых наиболее вероятно. Сформировано множество таких полиномов и соответствующих параметров. Предложен метод распознавания параметров помехоустойчивых блочных циклических кодов среди известного множества, что позволяет значительно сократить количество необходимых вычислений.

Ключевые слова: битовый поток, помехоустойчивый блочный циклический код, образующий полином кода, остаток от полиномиального деления, матрица.

ВВЕДЕНИЕ

Для декодирования данных по существующим методам, алгоритмам и стандартам в программно-технических комплексах должны быть известны вид и параметры кода [1]. В случае отсутствия такой информации необходимо предварительно провести анализ битового потока для их определения [2], что является сложной научно-технической задачей. Такие задачи, как правило, решаются при оценивании характеристик каналов связи, радиомониторинге, анализе производительности сетей передачи данных. Однако развитию методического аппарата анализа битовых потоков, проводимого перед декодированием, уделяется недостаточно внимания [3]. Под битовым потоком (bitstream) будем понимать поток битов (цифровой поток) в виде нулей и единиц, полученный из канала связи после демодулятора, содержащий в закодированном виде сообщение и обладающий некоторой избыточностью.

Вследствие эффективности [4] наиболее распространенными видами помехоустойчивых кодов в современных системах связи и передачи данных являются блочные и сверточные коды, а также их комбинации [2, 5, 6]. Среди помехоустойчивых блочных кодов, используемых на практике, многие коды циклические [7–10]. Исключение составляют широко применяемые благодаря корректирующим возможностям блочные LDPC-коды [11], которые в общем случае не являются циклическими.

Анализ результатов исследований показал развитость методического аппарата анализа сетевых протоколов передачи данных и их цепочек на высших уровнях модели OSI, оперирующих кадрами [12, 13], а также определения вида модуляции на первом уровне этой модели [14]. Однако методический аппарат остальных аспектов анализа битовых потоков на первом уровне иерархии модели OSI разработан недостаточно: существуют разрозненные подходы к определению вида кода [15], анализу помехоустойчивых сверточных [15] и блочных [2, 15, 16] кодов. К известным методам анализа битовых потоков для определения параметров помехоустойчивых блочных циклических кодов относится метод, использующий корреляционные функции [2, 17, 18]. Его недостатком является необходимость проведения значительного количества вычислений для распознавания блочных кодов большой длины [15].

Таким образом, исследование методов определения параметров помехоустойчивых блочных циклических кодов, с помощью которых поиск выполняется за более короткое время, — актуальная задача. В данной статье предложен метод распознавания параметров помехоустойчивых блочных циклических кодов в масштабе реального времени.

ПОМЕХОУСТОЙЧИВОЕ БЛОЧНОЕ ЦИКЛИЧЕСКОЕ КОДИРОВАНИЕ

Основными параметрами помехоустойчивого блочного циклического кода, однозначно определяющими его возможности по обнаружению и исправлению ошибок, являются длина кода n, количество информационных бит k, количество проверочных бит $n-k$, минимальное кодовое расстояние $d_{\min}$ и образующий полином $g(z)$ [7–10, 16]. Степень образующего полинома равна количеству проверочных битов.

Каждое кодовое слово $\mathbf{X}$ длиной n бит представляет собой конкатенацию двух матриц-векторов: $\mathbf{K}$ длиной k бит и $\mathbf{G}$ длиной $n-k$ бит (рис. 1),

$$\mathbf{X} = \{\mathbf{K}, \mathbf{G}\}, \tag{1}$$

где $\{\}$ — знак конкатенации.

Информационная часть кодового слова представлена в виде матрицы-вектора $\mathbf{K} = (x_0, x_1, \ldots, x_{k-1})$ и содержит биты данных $x_i \in (0,1)$, как правило, в виде кода ASCII (8 бит), Unicode (16 бит), реже — в виде других кодов.

Суть кодирования заключается в формировании проверочной части кодового слова при наличии информационной части и правила выполнения проверок, заданного в образующем полиноме.

Проверочная часть кодового слова $\mathbf{G} = (x_k, x_{k+1}, \ldots, x_{n-1})$ содержит проверочные биты $x_i \in (0,1)$ и представлена в виде остатка от деления сдвинутой на $n-k$ бит влево информационной части кодового слова длиной k, дополненной справа нулями, на образующий полином $g(z) = a_{n-k} z^{n-k} + a_{n-k-1} z^{n-k-1} + a_{n-k-2} z^{n-k-2} + \ldots + a_1 z^1 + a_0 z^0$. Полином $g(z)$ имеет множители при аргументе: $a_0 = 1$; $a_i \in (0,1)$, $i \in (1, \ldots, n-k-1)$; $a_{n-k} = 1$. Выбор конкретного значения множителя a_i при аргументе z^i и составляет суть построения образующего полинома, от которого зависит качество помехоустойчивого кода [7–10]. Например, среди образующих полиномов 16-й степени для двоичных кодов наиболее предпочтительны следующие [16]:

$$g(z) = z^{16} + z^{15} + z^2 + 1 = 1100000000000101_2 = 98309_{10} = 18005_{16};$$

$$g(z) = z^{16} + z^{12} + z^5 + 1 = 10001000000100001_2 = 69665_{10} = 11021_{16};$$

$$g(z) = z^{16} + z^{12} + z^3 + z + 1 = 10001000000001011_2 = 69643_{10} = 1100B_{16};$$

$$g(z) = z^{16} + z^{13} + z^{12} + z^{11} + z^{10} + z^8 + z^6 + z^5 + z^2 + 1 = 10011110101100101_2 =$$

$$= 81253_{10} = 13D65_{16};$$

$$g(z) = z^{16} + z^{14} + z^{13} + z^{11} + z^{10} + z^9 + z^8 + z^6 + z^5 + z + 1 =$$

$$= 10110111101100011_2 = 94051_{10} = 16F63_{16}.$$

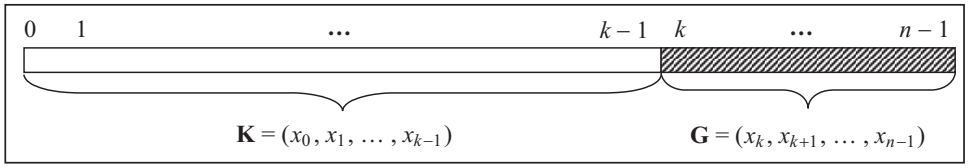

Рис. 1. Кодовое слово $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$ длиной n бит

При фиксированных параметрах n и k основным параметром кода, определяющим правило формирования проверочных битов, является образующий полином $g(z)$. Если известен образующий полином кода, известен и код [7–10]. Поэтому для отыскания параметров такого помехоустойчивого кода достаточно найти его образующий полином. Для этого можно применить метод, который основан на полном переборе всех возможных вариантов.

РАСПОЗНАВАНИЕ ПАРАМЕТРОВ КОДА ПОЛНЫМ ПЕРЕБОРОМ

Суть метода распознавания параметров помехоустойчивого блочного циклического кода полным перебором заключается в разбиении всего анализируемого битового потока $\mathbf{Y}$ длиной M бит на m_j гипотетических кодовых слов длиной n_j бит каждое с k_j информационными битами (рис. 2) так, что $M = m_j n_j + l_j$, где l_j — остаток, в общем случае $0 \le l_j < n_j$. Битовый поток разбивается всего на J вариантов. Каждый j-й вариант разбиения, $j \in [0 \dots J-1]$, соответствует конкретному значению длины гипотетического кодового слова n_j (от $n_{\min}$ до $n_{\max}$), количеству информационных бит k_j (от $k_{\min}$ до $k_{\max}$), количеству гипотетических кодовых слов $m_j = \left\lfloor \dfrac{M}{n_j} \right\rfloor$ и степени образующего полинома $n_j - k_j$. Для каждой гипотетической длины кодового слова n_j определяется минимально и максимально возможная степень образующего полинома $g_{\min} = n_j - k_{\max}$ и $g_{\max} = n_j - k_{\min}$ в зависимости от максимально $k_{\max}$ и минимально $k_{\min}$ возможного количества информационных битов.

Весь набор кодовых слов, состоящий из M бит, представляется в виде конкатенации кодовых слов $\mathbf{X}_i$ (1) длиной n_j бит каждое (остаток отбрасывается):

$$\mathbf{Y} = \{\mathbf{X}_0, \mathbf{X}_1, \dots, \mathbf{X}_{m_j-1}\}. \tag{2}$$

В общем случае матрицы-векторы $\mathbf{X}_i$ имеют одинаковую длину n_j и не равны между собой, так как наполнены разными выборками битового потока $x_i \in (0,1)$.

Каждое гипотетическое кодовое слово полиномиально делится на значение гипотетического полинома $g(z)$, получаемое последовательным инкрементированием на единицу младшего разряда:

$$\frac{\mathbf{X}_i}{g(z)} = q(z) + \frac{r(z)}{g(z)}, \tag{3}$$

где $q(z)$ — частное от деления; $r(z)$ — остаток от деления. Деление (3) выполняется в пределах конкретного разбиения j в матрице-векторе $\mathbf{Y}$ (2) для текущих значений n_j, k_j для каждого $\mathbf{X}_i$.

Если $r(z) = 0$, то такое гипотетическое кодовое слово становится возможным кодовым словом и в строку матрицы заносятся его значения m_j, n_j, k_j, а также текущее значение образующего полинома $g(z)$. Если для выбранных значений n_j и k_j проверены все возможные образующие полиномы и истинный полином не найден,

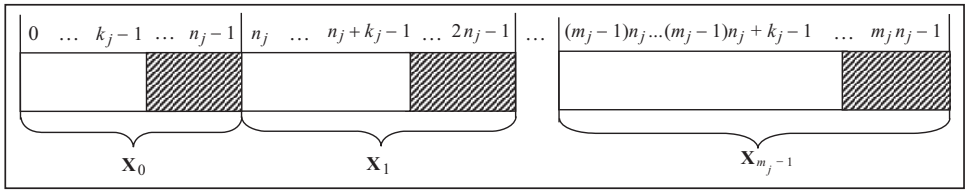

Рис. 2. Разбиение битового потока длиной M бит на m_j гипотетических кодовых слов $\mathbf{X}_i$, каждое по n_j бит, $l_j = 0$

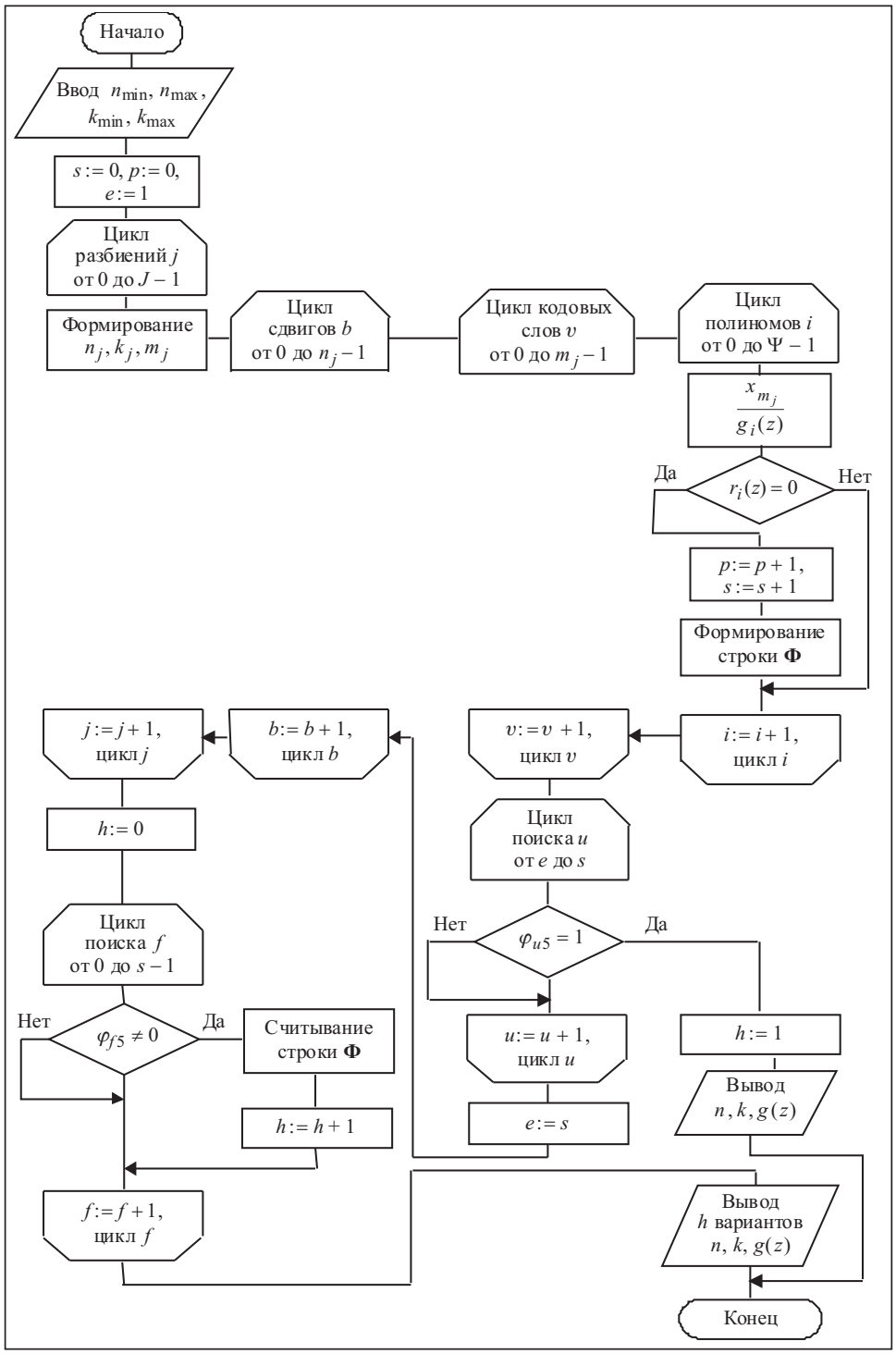

Рис. 3. Алгоритм работы метода распознавания параметров помехоустойчивых блочных циклических кодов по образующему полиному полным перебором

то начало поиска в битовом потоке длиной M бит сдвигается вправо на 1 бит. Количество битовых сдвигов b может принимать значения от 0 до $n_j - 1$. Для каждого полиномиального деления, если $r(z) = 0$, формируется строка матрицы

$$\mathbf{\Phi} = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \varphi_{13} & \varphi_{14} & \varphi_{15} \\ \dots & \dots & \dots & \dots & \dots \\ \varphi_{s1} & \varphi_{s2} & \varphi_{s3} & \varphi_{s4} & \varphi_{s5} \end{pmatrix}, \tag{4}$$

где $\varphi_{s1} = n_j$ — длина кодового слова; $\varphi_{s2} = k_j$ — количество информационных битов; $\varphi_{s3} = g(z)$ — образующий полином кода в виде целого числа; $\varphi_{s4} = b$ — битовый сдвиг в пределах матрицы-вектора $\mathbf{Y}$, $0 \le b \le n_j - 1$; $\varphi_{s5} = p / m_j$ — нормированное количество поделившихся нацело кодовых слов в пределах матрицы-вектора $\mathbf{Y}$, $0 \le p / m_j \le 1$; s — общее количество возможных вариантов параметров кода в пределах всего битового потока из M бит, равное количеству строк матрицы $\mathbf{\Phi}$.

В результате обработки всего битового потока из M бит заполняется s строк матрицы $\mathbf{\Phi}$, где только одна строка содержит правильные параметры кода (является истинной). По окончании всех итераций полиномиального деления C найденный максимум среди элементов пятого столбца матрицы $\mathbf{\Phi}$ позволяет окончательно установить истинные параметры блочного циклического кода, которым закодирован битовый поток из M бит. Возможны два случая: $\varphi_{s5} = 1$ и $\varphi_{s5} < 1$. Для первого случая принимается гипотеза о соответствии образующего полинома $g(z)$ и параметров n_j, k_j помехоустойчивого блочного циклического кода, которые содержатся в s-й строке матрицы $\mathbf{\Phi}$, истинному полиному и поиск прекращается. Для второго случая ($\varphi_{s5} < 1$), характерного для реальных битовых потоков, выполняется поиск s-й строки матрицы $\mathbf{\Phi}$, для которой φ_{s5} максимально приближено к единице (в общем случае для битового потока из M бит возможно h вариантов параметров кода, $0 \le h \le s$).

Рассмотренный метод назовем методом распознавания параметров блочных циклических помехоустойчивых кодов по образующему полиному полным перебором. Алгоритм [19, 20], описывающий работу метода, представлен на рис. 3.

ОЦЕНКА ЭФФЕКТИВНОСТИ РАСПОЗНАВАНИЯ ПАРАМЕТРОВ КОДА ПОЛНЫМ ПЕРЕБОРОМ

Очевидными недостатками такого метода является необходимость проведения большого количества вычислений и соответственно низкая скорость распознавания. Проанализировав алгоритм (см. рис. 3), получим следующие формулы для оценки эффективности описанного метода. Общее количество итераций C алгоритма без учета возможного досрочного отыскания истинного образующего полинома можно получить, выполнив циклы разбиений j, сдвигов b, кодовых слов υ и полиномов i (см. рис. 3):

$$C = \sum_{n=n_{\min}}^{n_{\max}} \left(\left\lfloor \frac{n-4}{2} \right\rfloor nm \sum_{k=k_{\min}}^{k_{\max}} 2^{n-k-1} \right), \tag{5}$$

где $n_{\min} = 10$ — минимальная длина кодового слова; $n_{\max}$ = 32716 — максимальная длина кодового слова, ограниченная вычислительными возможностями для чисел с плавающей точкой ($1{,}1 \cdot 10^{4932}$); m — количество гипотетических кодовых слов в пределах одного разбиения;

$$k_{\min} = \begin{cases} 0{,}5\,n, & n \wedge 1 = 0, \\ 0{,}5\,n + 1, & n \wedge 1 \ne 0; \end{cases} \quad k_{\max} = \begin{cases} n - 3, & n \in [10, 29], \\ 0{,}9\,n, & n \in [30, 99], \\ 0{,}96\,n, & n \in [100, 999], \\ 0{,}99\,n, & n \in [1000, 32716]. \end{cases}$$

Количество разбиений J при построении возможных вариантов матрицы-вектора $\mathbf{Y}$ можно вычислить по эмпирической формуле

$$J = \sum_{n=n_{\min}}^{n_{\max}} \left\lfloor \frac{n-4}{2} \right\rfloor. \tag{6}$$

Следует заметить, что при переходе от одной итерации алгоритма к другой многие полиномы повторяются, так как их структура при полном переборе определяется лишь степенью $2^{n_j - k_j}$ (числом проверочных битов). Поэтому общее количество образующих полиномов $g(z)$, используемых на всех итерациях C, соответствует числу проверочных битов для каждого разбиения j и его можно записать в таком виде:

$$\Psi = 2^{3-1} + 2^{4-1} + \ldots + 2^{0,5n_{\max}} = \sum_{i=3}^{0,5n_{\max}} 2^{i-1}. \tag{7}$$

Графики зависимостей количества разбиений J, итераций C и образующих полиномов Ψ от длины кодового слова для $n_{\min} = 10$ и $n_{\max} = 300$, рассчитанные по формулам (5)–(7) при $m = 3$, приведены на рис. 4 и рис. 5.

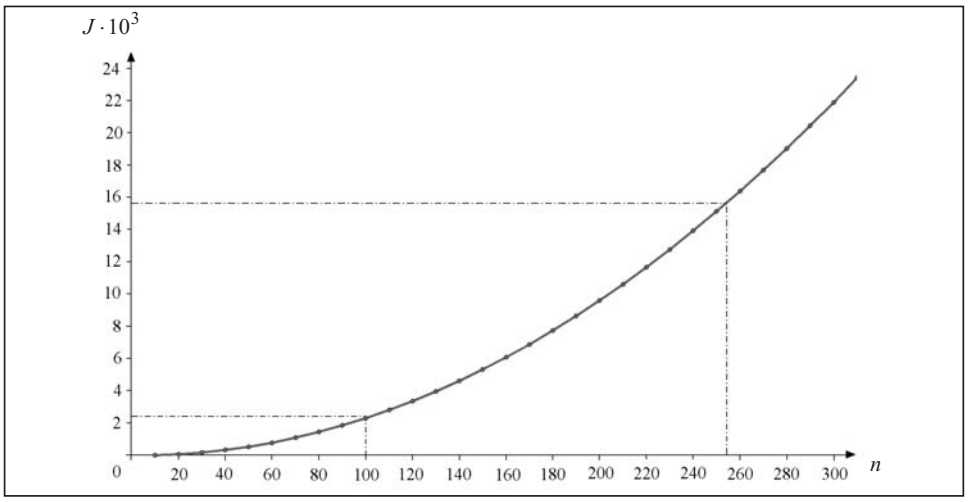

Рис. 4. График зависимости количества разбиений J от длины кодового слова n

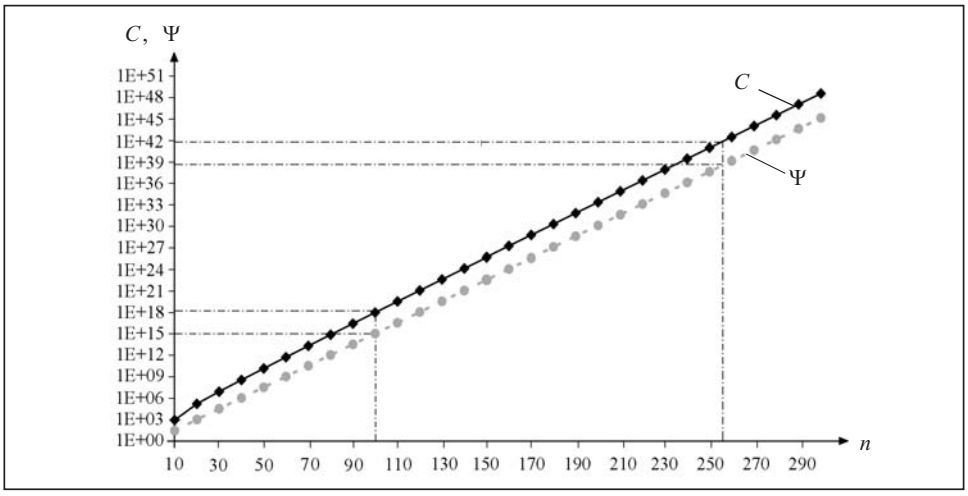

Рис. 5. Графики зависимости количества итераций C и количества образующих полиномов Ψ от длины кодового слова n

Результаты оценки количества разбиений J, итераций C и полиномов Ψ по формулам (5)–(7) свидетельствуют, что оба параметра экспоненциально возрастают с ростом длины кодового слова. Например, для $n=100$, $m=3$ количество разбиений $J=2298$, количество итераций алгоритма (фактически количество полиномиальных делений) $C=9{,}89\cdot10^{17}$ и количество образующих полиномов $\Psi=1{,}13\cdot10^{15}$. В реальных условиях количество кодовых слов m больше трех, что приводит к большему увеличению количества итераций C. Для известного кода Рида–Соломона при $n=255$ [21] имеем $J=15744$, $C=5{,}16\cdot10^{41}$, $\Psi=1{,}7\cdot10^{38}$. Очевидно, что применение рассмотренного метода в реальных условиях затруднительно.

ФОРМИРОВАНИЕ МНОЖЕСТВА ХОРОШИХ ОБРАЗУЮЩИХ ПОЛИНОМОВ

Для приведенного примера со степенью образующего полинома $n-k=16$ теоретически возможно использование $2^{15}=32768$ значений образующих полиномов (все нечетные значения от 1000000000000001_2 до 1111111111111111_2 включительно). Очевидно, что не все эти значения реально применяются, так как в системах связи и передачи данных в качестве образующих полиномов помехоустойчивых блочных циклических кодов используются лишь известные хорошие образующие полиномы, позволяющие получить помехоустойчивые коды с необходимыми свойствами. Поиск только среди этих полиномов может позволить значительно сократить количество итераций алгоритма, приведенного на рис. 3 [16, 19, 20].

Были проведены исследования использования известных образующих полиномов $g(z)$ на практике в блочных циклических кодах и описанных в фундаментальных трудах по теории кодирования [1, 4, 7–10, 22–26], применение которых является наиболее вероятным. Образующие полиномы целесообразно искать для следующих видов двоичных блочных циклических кодов: Боуза–Чоудхури–Хоквингема [9, 10, 23], мажоритарных $M(n, k)$ [22], Голея [22, 23], с постоянным весом [24], Файра [22], Касами [8, 10], Рида–Соломона [21], низкоплотностных LDPC-кодов [11, 26] и многих других [25].

Формальная постановка задачи исследования заключается в том, чтобы за счет уменьшения значения Ψ, определяемого по формуле (7), снизить количество итераций C (5), что эквивалентно уменьшению количества полиномиальных делений (3), и построить матрицу $\mathbf{\Phi}$.

Результаты поиска хороших образующих полиномов $g(z)$ для длин кодов от $n_{\min}=10$ до $n_{\max}=300$ позволили сформировать множество $\mathbf{\Omega}$ из 600 таких полиномов, соответствующих им значений n и k, а также предложить метод распознавания параметров помехоустойчивых блочных циклических кодов по образующему полиному среди известного множества.

РАСПОЗНАВАНИЕ ПАРАМЕТРОВ КОДОВ СРЕДИ ИЗВЕСТНОГО МНОЖЕСТВА

Сокращение количества итераций в усовершенствованном методе достигается при условии, что в (5) второе суммирование выполняется лишь в случае $g(z)\in\mathbf{\Omega}$. Представим множество $\mathbf{\Omega}$ в виде матрицы:

$$\mathbf{\Omega}=\begin{pmatrix}\omega_{11} & \omega_{12} & \omega_{13}\\ \dots & \dots & \dots\\ \omega_{d1} & \omega_{d2} & \omega_{d3}\end{pmatrix}, \tag{8}$$

где d — общее количество возможных кодов ($d=600$); значения ω_{d1}, ω_{d2}, ω_{d3} аналогичны значениям φ_{s1}, φ_{s2}, φ_{s3} из выражения (4). Количество строк d в матрице (8) в общем случае существенно меньше, чем количество строк s в матри-

це (4). Множество $\mathbf{\Omega}$ рассчитано заранее и при обработке не изменяется, тогда как матрица $\mathbf{\Phi}$ вычисляется согласно (4).

В процессе построчного заполнения матрицы $\mathbf{\Phi}$ для каждого значения $2^{n-k-1} = \omega_{d1} - \omega_{d2}$ из формулы (5) и матрицы (8) осуществляется подстановка значения ω_{d3} в качестве делителя в формулу полиномиального деления (3). Дальнейшая обработка возможных образующих полиномов, на которые гипотетические кодовые слова поделились без остатка, проводится так же, как в методе полного перебора. При отыскании истинного образующего полинома процедура может быть прекращена.

На рис. 6 показан видоизмененный цикл полиномов i из рис. 3, ограниченный пределами от 1 до 600, в котором используется проверка $g(z) \in \mathbf{\Omega}$. Применение этого цикла в алгоритме, представленном на рис. 3, приводит к алгоритму, реализующему метод распознавания параметров помехоустойчивых блочных циклических кодов по образующему полиному среди известного множества. Приведем основные элементы алгоритма, описывающего работу метода.

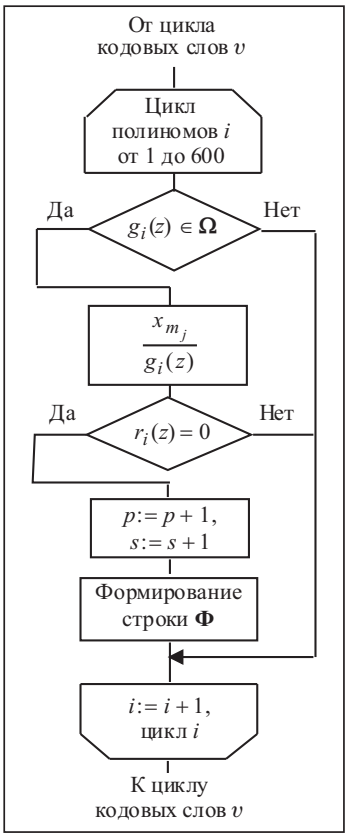

Рис. 6. Видоизмененный цикл полиномов i для метода распознавания параметров помехоустойчивых блочных циклических кодов по образующему полиному среди известного множества

1. Разбиение битового потока длиной M бит на J вариантов.

2. Цикл битовых сдвигов b от 0 до $n_j - 1$.

3. Цикл кодовых слов v от 0 до $m_j - 1$.

4. Цикл полиномов i, в котором полиномиальное деление выполняется лишь при условии $g(z) \in \mathbf{\Omega}$.

5. Формирование строки матрицы $\mathbf{\Phi}$.

6. Цикл поиска u от e до s, в матрице $\mathbf{\Phi}$ которого находится $\varphi_{s5} = 1$ (условие досрочного прекращения поиска, $h = 1$).

7. Цикл поиска f от 0 до $s-1$, в матрице $\mathbf{\Phi}$ которого находятся значения φ_{s5}, максимально приближенные к единице (формируются h вариантов параметров кода). Истинный полином считается найденным, если отношение вычисленного максимального значения φ_{s5} к следующему по величине значению φ_{s5} составляет не менее 10, иначе принимается решение о том, что образующий полином не найден.

Очевидно, что количество итераций алгоритма C (5) при использовании метода распознавания параметров помехоустойчивых блочных циклических кодов по образующему полиному среди известного множества (без учета досрочного прекращения поиска) значительно сократится.

ЗАКЛЮЧЕНИЕ

Предложенный метод распознавания параметров помехоустойчивых блочных циклических кодов, используемых в системах связи и передачи данных, отличается от известных методов выполнением поиска параметров лишь среди множества известных образующих полиномов. Существенное сокращение времени вычисления достигается за счет поиска только среди известных хороших об-

разующих полиномов, применение которых для формирования кодов в сигналах систем связи и передачи данных наиболее вероятно. Предполагается, что программные или программно-аппаратные реализации предложенного метода или его разновидностей в программно-технических комплексах позволят значительно повысить эффективность анализа битовых потоков за счет распознавания параметров помехоустойчивых блочных циклических кодов, используемых в системах связи и передачи данных.

СПИСОК ЛИТЕРАТУРЫ

1. Morelos-Zaragoza R.H. The art of error correcting coding. 2nd ed. Chichester: John Wiley & Sons, 2006. 278 p.
2. Котюбін В.Ю., Романов О.М., Бурлак Д.Ю. Особливості визначення періодичності у інформаційній послідовності при проведенні технічного аналізу сигналів. *Теорія та практика створення, розвитку і застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції*: тези доп. XXII Всеукр. наук.-практ. конф. (26–27 квітня 2018, Житомир). Житомир: ЖВІ імені С. П. Корольова, 2018. С. 153.
3. Романов О.М. Особливості розробки комплексів аналізу цифрових послідовностей. *Створення та модернізація озброєння і військової техніки в сучасних умовах*: зб. тез доп. 17 наук.-техн. конф. (7–8 вересня 2017, Чернігів). Чернігів: ДНВЦ ЗС України, 2017. С. 309–310.
4. Зубарев Ю.Б., Овечкин Г.В. Помехоустойчивое кодирование в цифровых системах передачи данных. *Электросвязь*. 2008. № 12. С. 58–61. URL: http://mtdbest.ru/articles/obzor_dvoichnie_kodi_2.pdf.
5. TC Synchronization and Channel Coding. Recommended Standard CCSDS 231.0-B-3. Washington: CCSDS, 2017. 50 p. https://public.ccsds.org/Pubs/231x0b3.pdf.
6. Сидоркина Ю.А., Шахтарин Б.И., Балахонов К.А. Анализ эффективности современных помехоустойчивых кодов. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*. 2014. № 6. С. 108–116. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sovremennyh-pomehoustoychivyh-kodov.
7. Blahut R.E. Theory and practice of error control codes. Corr. ed. Boston: Addison-Wesley, 1983. 452 p.
8. Касами Т., Токура Н., Ивадари Ё., Инагаки Я. Теория кодирования. Москва: Мир, 1978. 576 с.
9. Peterson W.W., Weldon E.J. Error-correcting codes. 2nd ed. Cambridge: MIT Press, 1972. 560 p.
10. Berlekamp E.R. Algebraic coding theory. New York: McGraw-Hill, 1968. 466 p.
11. Mostari L., Taleb-Ahmed A. High performance short-block binary regular LDPC codes. *Alexandria Engineering Journal*. 2018. Vol. 57, Iss. 4. P. 2633–2639. https://doi.org/10.1016/j.aej.2017.09.016.
12. Романов О.М. Застосування аналізаторів протоколів при технічному аналізі сигналів систем зв'язку. *Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Матеріали доп. II наук.-практ. конф.* (23–24 березня 2017, Київ). К.: КНУ ім. Тараса Шевченка, 2017. С. 177–179.
13. Маркин Ю.В. Методы и средства углубленного анализа сетевого трафика: автореф. дис. … канд. техн. наук. Москва: ИСП РАН, 2017. 30 с. URL: https://www.ispras.ru/dcouncil/docs/diss/2017/markin/autoref-markin-publ.pdf.
14. Воробьева Е.И., Немцов Р.А., Чураков П.П. Распознавание вида модуляции сигналов в системах радиомониторинга. *Вестн. Воронеж. гос. техн. ун-та*. 2015. Т. 11, № 4. С. 72–75.
15. Ревуцкий В.А. Устойчивые к мешающим факторам алгоритмы распознавания вида помехоустойчивых кодов в радиотехнических системах: автореф. дис. … канд. техн. наук. Рязань: РГРТУ, 2013. 19 с.
16. Куляниця О.Й., Ніколаєв С.М., Ратанін Є.Г. Аналіз циклічних кодів сучасних систем радіозв'язку КХ діапазону. *Праці ВІТІ НТУУ «КПІ»*. 2002. № 4. С. 95–98.
17. Ifeachor E.C., Jervis B.W. Digital signal processing: A practical approach. 2nd ed. Harlow; New York: Prentice Hall, 2002. 933 p.
18. Sklar B. Digital communications: Fundamentals and applications. 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2001. 1104 p.

19. Куляниця О.Й., Ніколаєв С.М., Павлюк С.В., Ратанін Є.Г. Алгоритм пошуку параметрів завадостійких кодів у сигналах систем радіозв'язку. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: тези доп. III наук.-практ. семінару* (8 грудня 2005, Київ). К.: ВІТІ НТУУ «КПІ», 2006. С. 64–65.
20. Ніколаєв С.М., Ратанін Є.Г. Алгоритм пошуку утворюючих поліномів завадостійких кодів в комплексах спеціального призначення. *Наукові проблеми розробки, модернізації та застосування інформаційно-вимірювальних систем космічного і наземного базування: тези доп. XV наук.-техн. конф.* (20–21 квітня 2006, Житомир). Житомир: ЖВІРЕ ім. С.П. Корольова, 2006. С. 173.
21. Типикин А.П., Петров В.В., Бабанин А.Г. Коррекция ошибок в оптических накопителях информации. К.: Наук. думка, 1990. 172 с.
22. Кодирование информации. Двоичные коды. Под ред. Березюка Н.Т. Харьков: Вища шк., 1978. 252 с.
23. Clark G.C., Cain J.B. Error-correction coding for digital communications. Applications of communications theory. New York: Springer, 1981. 435 p. https://doi.org/10.1007/978-1-4899-2174-1.
24. Злотник Б.М. Помехоустойчивые коды в системах связи. Москва: Радио и связь, 1989. 232 с.
25. Рахматкариев Э.У. Анализ избыточности помехоустойчивых кодов. *Кодирование в сложных системах*. Под ред. Самойленко С.И. Москва: Наука, 1974. С. 115–153.
26. Tomlinson M., Tjhai C.J., Ambroze M.A., Ahmed M., Jibril M. Error-correction coding and decoding. Bounds, codes, decoders, analysis and applications. Cham: Springer, 2017. 527 p. https://doi.org/10.1007/978-3-319-51103-0.

Надійшла до редакції 09.06.2020

С.М. Ніколаєв, О.М. Романов

МЕТОД РОЗПІЗНАВАННЯ ПАРАМЕТРІВ ЗАВАДОСТІЙКИХ БЛОКОВИХ ЦИКЛІЧНИХ КОДІВ ЗА УТВОРЮВАЛЬНИМ ПОЛІНОМОМ

Анотація. Описано суть завадостійкого блокового циклічного кодування. Розглянуто метод розпізнавання параметрів такого коду повним перебором. за відсутності апріорної інформації Визначено кількість необхідних для цього обчислень. Показано, що застосування такого методу в реальних умовах ускладнене. Досліджено відомі утворювальні поліноми, використання яких є найбільш ймовірним. Сформовано множину таких поліномів і відповідних параметрів. Запропоновано метод розпізнавання параметрів завадостійких блокових циклічних кодів серед відомої множини, що дає змогу значно скоротити кількість необхідних обчислень.

Ключові слова: бітовий потік, завадостійкий блоковий циклічний код, утворювальний поліном коду, залишок від поліноміального ділення, матриця.

S.N. Nikolaev, A.N. Romanov

ERROR-CORRECTING BLOCK CYCLIC CODE PARAMETER RECOGNITION METHOD BASED ON GENERATOR POLYNOMIAL

Abstract. The essence of the error-correcting block cyclic coding is described. A method for recognizing parameters of such a code in the absence of a priori information by a complete enumeration of parameters is considered. The amount of necessary calculation is determined. The application of the considered method in real conditions is shown to be difficult. The well-known generator polynomials whose practical use is most probable are investigated. A set of these polynomials and related parameters is generated. A method is proposed for recognizing parameters of error-correcting block cyclic codes among a known set, which can significantly reduce the amount of necessary calculation.

Keywords: bitstream, error-correcting block cyclic code, a generator polynomial of code, remainder of polynomial division, matrix.

Николаев Сергей Николаевич,
кандидат техн. наук, старший научный сотрудник, начальник научно-исследовательского управления Научно-исследовательского института Министерства обороны Украины, Киев, e-mail: divan24@i.ua.

Романов Алексей Николаевич,
кандидат техн. наук, заместитель начальника Научно-исследовательского института Министерства обороны Украины по научной работе, Киев, e-mail: rolex@i.ua.