УДК 621.391.15

ОЦЕНКА ПОТЕНЦИАЛЬНОЙ ПОМЕХОУСТОЙЧИВОСТИ АЛГОРИТМА ДЕКОДИРОВАНИЯ НА ОСНОВЕ ПАССИВНОЙ СОГЛАСОВАННОЙ ФИЛЬТРАЦИИ ПСЕВДОСЛУЧАЙНЫХ КОДОВ

Константин Александрович МОРДАСОВ родился в 1983 г. в городе Чебоксары. Аспирант Московского государственного института электронной техники. Основные научные интересы — в области теории информации и помехоустойчивого кодирования. Автор пяти научных работ. E-mail: kosmor@mail.ru

Konstantin A. MORDASOV, was born in 1983, in Cheboksary. He is a Postgraduate Student at the Moscow Institute of Electronic Technology (MIET). His research interests are in information theory and noise-immune coding. He has published 5 technical papers. E-mail: kosmor@mail.ru

Рассматривается алгоритм, предложенный автором для быстрого декодирования длинных псевдослучайных кодов. Дается аналитическая оценка потенциальной помехоустойчивости алгоритма. Представлены результаты компьютерного моделирования алгоритма в дискретном симметричном канале для симплексного блокового кода (1023, 10), образованного циклическими сдвигами одного периода линейной рекуррентной последовательности максимальной длины. Дается сравнение результатов моделирования с аналитической оценкой, которое показало необходимость дальнейшего развития рассмотренного подхода к декодированию псевдослучайных кодов для приближения к его потенциальным возможностям.

An algorithm is suggested to decode rapidly long pseudo-random codes. An analytical estimation is considered for a potential noise immunity of the algorithm. Computer simulation results are presented for the algorithm operating in discrete symmetric channel using simplex block code (1023, 10) generated by means of circular shifts for one period of linear recurrent sequence with maximum length. The simulation results are compared with analytical ones. The comparison demonstrates a necessity to improve the pseudo-random code decoding algorithm to reveal its useful potential capabilities.

Ключевые слова: код максимальной длины; алгоритм; декодирование; помехоустойчивость.

Key words: maximum-length code, algorithm, decoding, noise immunity.

Введение

В статье [1] показана актуальность проблемы декодирования ансамблей длинных псевдослучайных кодов, которые используются для повышения помехозащищенности радиосистем передачи информации в условиях радиоэлектронной борьбы. Авторами этой же статьи [1] предложен новый подход к декодированию этих ансамблей, основанный на пассивной согласованной фильтрации, который обладает логарифмической сложностью декодирующего устройства в отличие от линейной сложности известных алгоритмов. В результате предложенный подход снимает ограничения на реализацию декодера при обработке сверхдлинных кодов в режиме реального времени, что позволяет использовать его для цифровой обработки шумоподобных сигналов с большой базой в системах широкополосной радиосвязи. Будем далее называть такой подход быстрым декодированием (БДК). В настоящей статье выводится аналитическая формула нижней границы блоковой ошибки декодирования для алгоритма БДК в дискретном симметричном канале и на примере симплексного кода максимальной длины (1023, 10) демонстрируется помехоустойчивость алгоритма БДК, которую потенциально можно достичь, развивая идеи данного подхода.

Оценка потенциальной помехоустойчивости

Алгоритм БДК предназначен для декодирования кодов, образованных линейными рекуррентными последовательностями. Рекурсивная зависимость кодовых символов позволяет по отрезку из m безошибочных символов кодового слова восстановить целиком все кодовое слово, где m — память кода. Алгоритм БДК основан на поиске в кодовом слове, принятом из канала с ошибками, сегмента из $L = m + J$ безошибочных символов. Будем называть такой сегмент чистым окном шириной L. Причем m символов чистого окна используются для восстановления кодового слова и декодирования m сим-

волов информационной последовательности, а J символов используются для проверки первых m символов чистого окна. Очевидно, чем больше глубина проверки J, тем достовернее алгоритм БДК отличает чистые окна от кодовых сегментов, содержащих канальные ошибки. Однако увеличение глубины проверки уменьшает возможность найти чистое окно на длине кодового слова. Таким образом, возникает задача достижения компромисса между достоверностью обнаружения чистого окна и возможностью найти такое окно в кодовом слове.

Рассмотрим случаи, которые могут привести к ложному декодированию при использовании алгоритма БДК.

1. Если при определенной реализации канальных ошибок в кодовом слове апостериори отсутствует чистое окно шириной m, алгоритм БДК в идеальном случае должен выдавать отказ от декодирования, так как в описанной ситуации отсутствует возможность правильно декодировать принятое слово. В этом случае положительное решение декодера БДК о наличии чистого окна всегда приводит к ложному декодированию.

2. В канальном слове присутствует чистое окно шириной не менее m символов. В этом случае существует возможность правильного декодирования, однако встает задача правильного выбора m безошибочных символов для декодирования. Так как декодер БДК принимает решение о наличии чистого окна по J проверкам, отсутствие апостериори такого окна шириной $L = m + J$ всегда приводит к ложному решению о его наличии. В этом случае существует вероятность ошибки в выбранных для декодирования m символах, что приводит к ложному декодированию. Если же апостериори есть чистое окно шириной не менее $L = m + J$ символов, решение декодера БДК о его наличии может быть правильным.

Таким образом, приходим к выводу, что возможность правильного декодирования кодового слова практически полностью определяется наличием чистого окна из $L = m + J$ и более символов в кодовом слове.

Теперь, если рассмотреть идеальный декодер БДК, который при заданном уровне канальных ошибок всегда правильно обнаруживает чистое окно шириной $L = m + J$ символов и всегда выдает отказ от декодирования, если такого окна нет, можно считать, что вероятность $P_{\text{пр}}$ правильного декодирования определяется вероятностью события A ={“В канальном слове есть хотя бы одно чистое окно шириной L или более символов”}. Это и будет потенциальной помехоустойчивостью декодера БДК. Для реального декодер БДК существует вероятность $P_{\text{лож}}$ ложного обнаружения чистого окна, что приводит к ложному декодированию и снижает помехоустойчивость метода. Вероятность $P_{\text{лож}}$ определяется глубиной проверок J и законом таких проверок, т. е. схемой конкретного декодера БДК. Аналитическое изучение зависимости $P_{\text{лож}}$ от схемы декодера БДК представляется затруднительным, поэтому автор исследовал такую зависимость с помощью компьютерного моделирования декодера в дискретном симметричном канале (ДСК). Для сравнения результатов моделирования с потенциальными возможностями декодера БДК автором была выведена аналитическая формула, определяющая нижнюю границу вероятности блоковой ошибки декодирования в ДСК. При этом под блоковой ошибкой декодирования подразумевались события, связанные с отказом от декодирования (вероятность $P_{\text{отк}}$) и ложным декодированием кодового блока (вероятность $P_{\text{лож}}$). Для идеального декодера БДК ложное декодирование отсутствует ($P_{\text{лож}} = 0$).

Нижнюю границу $Q_{\min}$ вероятности блоковой ошибки декодера БДК можно оценить блоковой ошибкой идеального декодера БДК. Тогда, если вероятность события A равна P_A, по формуле полной вероятности событий получаем

$$P_{\text{лож}} + P_{\text{отк}} + P_{\text{пр}} = Q_{\min} + P_{\text{пр}} = Q_{\min} + P_A = 1. \quad (1)$$

Пусть вероятность канальной ошибки на символ равна q, а декодеру БДК для восстановления кодового слова необходимо определить положение чистого окна шириной $L = m + J$ символов в кодовом слове из n символов. Вероятность P_A определяется суммарной вероятностью различных конфигураций случайных ошибок в канале, приводящих к наступлению события A.

Пусть $\overline{E} = \langle e_1 e_2 \ldots e_n \rangle$ — случайный вектор (конфигурация) ошибок в кодовом слове. Элемент $e_i = 1$ в векторе $\overline{E}$ соответствует наличию ошибки в i-м символе кодового слова, а элемент $e_i = 0$ — отсутствию ошибки в этом символе. Вероятность события $\{e_i = 1\}$ равна q, а вероятность события $\{e_i = 0\}$ равна $p = 1 - q$. По определению канала ДСК события $\{e_i = 1\}$ и $\{e_i = 0\}$ независимы. Примером реализации вектора $\overline{E}$ может служить исход $\overline{E} = \langle 010 \rangle$, который показывает, что во 2-м символе слова из трех символов произошла ошибка, а все остальные

символы приняты без ошибок. В случае, когда реализация вектора ошибок содержит повторяющиеся элементы, будем использовать краткую запись, отображая кратность элемента в нижнем индексе, например $\overline{E} = \langle 001110000 = 0_2 1_3 0_4 \rangle$. В силу независимости случайных элементов вектора ошибок вероятность отдельной реализации вектора $\overline{E}$ равна произведению вероятностей реализации его элементов:

$$P\left(\overline{E} = \langle e_1 e_2 ... e_n \rangle\right) = P(e_1) P(e_2) ... P(e_n) = p^{n_0} q^{n_1}, \quad (2)$$

где n_0 — количество элементов $\{e_i = 0\}$ в векторе $\overline{E}$; n_1 — количество элементов $\{e_i = 1\}$ в векторе $\overline{E}$, причем $n_0 + n_1 = n$.

Множество различных реализаций случайного вектора $\overline{E}$ будем называть группой исходов вектора $\overline{E}$ и обозначать $\bar{G}_E$. Представим $\bar{G}_E$ в виде суммы реализаций вектора $\overline{E}$:

$$\bar{G}_E = \bar{E}_1 + \bar{E}_2 + ... + \bar{E}_k = \langle e_1 e_2 ... e_n \rangle.$$

Например, две реализации $\bar{E}_1 = \langle 010 \rangle$ и $\bar{E}_2 = \langle 000 \rangle$ можно объединить в группу исходов:

$$\bar{G}_E = \langle 010 \rangle + \langle 000 \rangle = \langle 0(0+1)0 \rangle = \langle 0x0 \rangle.$$

В случае, когда наличие или отсутствие ошибки в определенном символе кодового слова не имеет значения, будем помечать позицию такого символа в записи $\bar{G}_E$ элементом *x*. Ясно, что вероятность события $\{e_i = x\}$ равна 1. Суммарная вероятность реализаций вектора ошибок, входящих в группу $\bar{G}_E$, определяется как $P\left(\bar{G}_E\right) = \sum_{i=1}^{i=k} P\left(\bar{E}_i\right)$. По аналогии с формулой (2) получаем альтернативное выражение для $P\left(\bar{G}_E\right)$:

$$P\left(\bar{G}_E = \langle e_1 e_2 ... e_n \rangle\right) = p^{n_0} q^{n_1} 1^{n_x} = p^{n_0} q^{n_1}, \quad (3)$$

где $n_0 + n_1 + n_x = n$; n_x — количество элементов $e_i = x$ в векторе $\bar{G}_E$. Пусть группа исходов $\bar{G}_E$ представляет собой объединение $\{\bar{G}_{E,1}, \bar{G}_{E,2}, ..., \bar{G}_{E,k}\}$ различных групп исходов (т. е. групп, которые не имеют общих реализаций вектора ошибок), тогда суммарная вероятность реализаций группы $\bar{G}_E$ равна

$$P\left(\bar{G}_E = \bar{G}_{E,1} + \bar{G}_{E,2} + ... + \bar{G}_{E,k}\right) = \sum_{i=1}^{i=k} P\left(\bar{G}_{E,i}\right). \quad (4)$$

Начнем перебор всех различных групп исходов $\bar{G}_{E,j}$, которые приводят к наступлению события *A*. Пронумеруем группы $\bar{G}_{E,j}$, начиная с индекса $j = 0$. В качестве $\bar{G}_{E,0}$ рассмотрим чистое окно ширины *L* в начале кодового слова (т. е. первые *L* символов приняты без ошибок и не важно, как приняты все остальные символы). Тогда $\bar{G}_{E,0} = \langle 0_L x_{n-L} \rangle$. В дальнейшем, если вектор $\bar{G}_E$ содержит элементы *x* в конце, будем удалять их из краткой записи $\bar{G}_E$ и подразумевать, что они там есть. Следующие *L* групп выберем по закону $\bar{G}_{E,j} = \langle x_{j-1} 10_L \rangle$ (т. е. не важно, как приняты первые $j-1$ символов кодового слова, после которых следует одиночная ошибка в *j*-м символе; за ошибкой следует *L* безошибочных символов и не важно, как приняты все последующие символы). Нетрудно убедиться, что исходы каждой такой группы $\bar{G}_{E,j}$ отличаются от исходов всех предыдущих групп как минимум в *j*-м символе. Группы $\langle \bar{G}_{E,j} \rangle$ с индексами $j > L$ построим по закону $\bar{G}_{E,j} = \langle \overline{a_j} 10_L \rangle$, где вектор $\bar{a}_j = \langle e_1 e_2 ... e_{j-1} \rangle$ определяет конфигурации ошибок в первых $(j-1)$ символах кодового слова. Вектор $\bar{a}_j$ выбирается так, чтобы группа $\bar{G}_{E,j}$ не содержала в себе исходы, рассмотренные в предыдущих группах. Другими словами, каждый исход группы $\bar{G}_{E,j}$ должен отличаться как минимум одним символом от любого исхода из объединения $\bar{G}_{E,0} + \bar{G}_{E,1} + ... + \bar{G}_{E,j-1}$ всех предыдущих групп. Нетрудно убедиться, что исходы каждой группы $\bar{G}_{E,j}$ отличаются от исходов *L* предыдущих групп как минимум в *j*-м символе. Однако при определенном выборе $\bar{a}_j$ исходы $\bar{G}_{E,j}$ могут совпасть с исходами из объединения $\bar{G}_{E,0} + \bar{G}_{E,1} + ... + \bar{G}_{E,j-L-1}$ первых $(j-L)$ групп. Отсюда следует, что вектор $\bar{a}_j$ должен содержать конфигурации ошибок в первых $j-1$ символах кодово-

го слова, взятых из объединения $\bar{G}_{E,j-L} + \bar{G}_{E,j-L+1} + ... + \bar{G}_{E,j-1}$ предыдущих L групп. Построенная по такому закону группа $\bar{G}_{E,j}$ соответствует конфигурациям ошибок, для которых чистое окно шириной L не наблюдается в первых j символах кодового слова и возникает, начиная с $(j+1)$-го символа. Нетрудно убедиться, что последней группой $\bar{G}_{E,j}$, исходы которой могут привести к наступлению события A, будет группа с номером $j = n - L$. Рассмотренное правило построения групп $\bar{G}_{E,j}$ позволяет осуществить полный перебор всех реализаций вектора ошибок, приводящих к наступлению события A. Правило выбора вектора $\bar{a}_j = \langle e_1 e_2 ... e_{j-1} \rangle$ для группы $\bar{G}_{E,j} = \langle \bar{a}_j 10_L \rangle$ можно выразить аналитически через рекуррентную последовательность $\bar{a} = \bar{a}_1, \bar{a}_2, ..., \bar{a}_{n-L}$, элементы которой связаны правилом

$$\begin{aligned} &\bar{a}_j = \langle x_{j-1} \rangle, \quad j = 1,2,...L; \\ &\bar{a}_j = \sum_{k=1}^{k=L} \langle \bar{a}_{j-k} 10_{k-1} \rangle, \quad j > L. \end{aligned} \tag{5}$$

Например:

$$\bar{a}_{L+1} = \langle x_{L-1} 10_0 \rangle + ... + \langle x_0 10_{L-1} \rangle = \langle x_{L-1} 1 \rangle + ... + \langle 10_{L-1} \rangle.$$

Обобщая предыдущие рассуждения, получаем формулу перебора всех различных групп исходов, приводящих к наступлению события A:

$$\bar{G}_{E,j} = \begin{cases} \langle 0_L \rangle, & j = 0; \\ \langle x_{j-1} 10_L \rangle, & j = 1,2,...,L; \\ \langle \bar{a}_j 10_L \rangle, & j = L+1, L+2, ..., n-L, \end{cases} \tag{6}$$

где векторы $\bar{a}_j$ определяются правилом (5).

Используя совместно формулы (3), (4) и (6), получаем формулу для вероятности $P_{A,j} = P\left(\bar{G}_{E,j-1}\right)$ встретить первое чистое окно шириной L или более символов, начиная с j-го кодового символа ($j = 1,2,...,n$):

$$P_{A,j} = \begin{cases} p^L, & j = 1; \\ qp^L, & j = 2,3,...,L+1; \\ b_{j-1} qp^L, & j = L+2,...,n-L+1; \\ 0, & j = n-L+2,...,n, \end{cases} \tag{7}$$

где множители b_j вычисляются по закону (8):

$$b_1 = ... = b_L = 1; \quad b_j = \sum_{k=1}^{k=L} qp^{k-1} b_{j-k}. \tag{8}$$

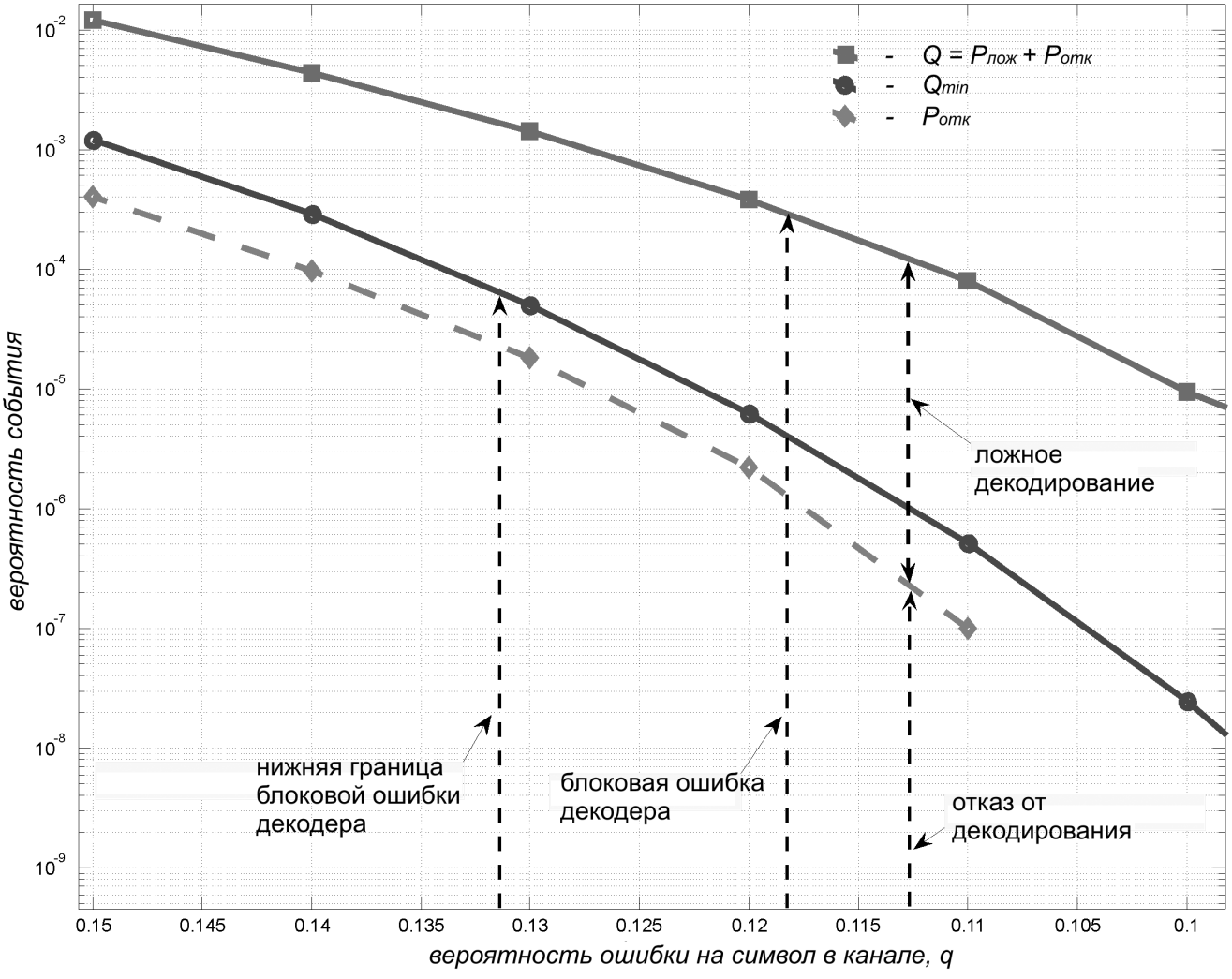
Используя формулы (1) и (7), получаем нижнюю границу $Q_{\min}$ вероятности блоковой ошибки декодера БДК:

$$Q_{\min} = 1 - \sum_{j=1}^{j=n-L+1} P_{A,j}. \tag{9}$$

Исследование помехоустойчивости

В качестве кода для исследования был выбран симплексный код, образованный циклическими сдвигами одного периода линейной рекуррентной последовательности максимального периода памяти m. Период такой последовательности равен $n = 2^m - 1$ и определяет длину кодового блока. К n сдвигам последовательности добавляется слово, состоящее из нулевых символов, в результате чего получает блоковый (n, m) код с объемом кодового пространства $V = 2^m$. В статье демонстрируются результаты исследования декодера БДК в ДСК для кода (1023, 10) с проверочным полиномом $g(x) = x^{10} + x^7 + 1$. Глубина проверки $J = 10$ (порог обнаружения фазы кода в работе [1]) и другие параметры алгоритма БДК (макс. база мажоритарного декодирования [1], равная 5) были выбраны для минимизации вероятности блоковой ошибки декодирования ($Q = P_{\text{лож}} + P_{\text{отк}}$) при вероятности $q = 10e-1$ ошибки на символ в канале. Для данного алгоритма путем компьютерного моделирования построена экспериментальная зависимость вероятностей Q, $P_{\text{отк}}$ и $P_{\text{лож}}$ от вероятности q. Результаты моделирования совместно с аналитической границей (9) для вероятности Q представлены на рисунке.

Из рисунка видно, что вероятность отказа от декодирования меньше, чем нижняя граница блоковой ошибки. Это можно объяснить тем, что в случаях, когда в канальном слове не было чистого окна, декодер ошибочно воспринимал искаженный кодовый сегмент за чистое окно, по которому ложно декодировал кодовое слово. Из рисунка видно, что вероятность блоковой ошибки исследуемого декодера превышает нижнюю границу блоковой ошибки. Это можно объяснить тем, что в случаях, когда в канальном слове было чистое окно, декодер выбирал вместо него искаженный ошибками кодовый сегмент, что приводило к ложному декодированию. В результате суммарная вероятность



Сравнение помехоустойчивости алгоритма БДК симплексного кода (1023, 10) с потенциальной нижней границей блоковой ошибки декодирования

отказов от декодирования и ложного декодирования превысила вероятность блоковой ошибки идеального декодера БДК. Также из рисунка видно, что блоковая ошибка практически полностью определятся ложным декодированием кодового блока, и, следовательно, низким качеством проверок, используемых декодером БДК для обнаружения чистого окна.

Выводы

Результаты проведенных исследований показали, что для достижения потенциальной границы (9) необходимо дальнейшее развитие критерия обнаружения чистого окна в алгоритме БДК. Причем критерий необходимо совершенствовать не за счет увеличения глубины проверок и, следовательно, роста числа отказов от декодирования, а за счет повышения качества этих проверок. Предварительно можно сообщить о возможности повысить помехоустойчивость подхода за счет использования проверочного полинома с большим числом слагаемых и за счет вынесения решения на базе нескольких чистых окон, обнаруженных декодером на длине кодового слова. В настоящее время автором статьи ведется работа в этом направление, по окончании которой достигнутые результаты будут представлены в виде публикации.

Библиографический список

Кузнецов В.С., Мордасов К.А. Быстрое декодирование на основе пассивной согласованной фильтрации длинных кодов Голда // Естественные и технические науки. 2009. № 4. С. 321—327.

Московский государственный институт электронной техники (технический университет)
Статья поступила в редакцию 8.10.2009