ВОССТАНОВЛЕНИЕ СТРУКТУРЫ ПОМЕХОУСТОЙЧИВЫХ КОДОВ**С.В. Овсянкин, С.Ю. Костомаров***Академия ФСО России, Орел, Российская Федерация*

Исследована проблема анализа кодированных последовательностей современных систем связи с использованием алгебраических методов. Рассмотрены условия применения различных методов определения параметров помехоустойчивых кодов. Для случаев невозможности их определения предложен способ декодирования помехоустойчивого кода на основе построения обобщенной проверочной матрицы. Обоснована возможность построения обобщенной проверочной матрицы, корректно учитывающей влияние структурных элементов кодера, и применения к ней алгоритма итеративного распространения доверия.

Ключевые слова: декодирование, помехоустойчивый код, алгебраический метод, обобщенная проверочная матрица, алгоритм итеративного распространения доверия.

STRUCTURE RECOVERY OF ERROR-CONTROL CODES**S.V. Ovsyankin, S.Yu. Kostomarov***Academy FGS of Russia, Orel, Russian Federation*

The problem of the analysis of coded sequences of modern communication systems using algebraic methods is investigated. Conditions of application of various methods for determining parameters of error-correcting codes are considered. For cases of impossibility of their definition, the method for decoding an error-correcting code based on construction of the generalized verification matrix is offered. The possibility of constructing a generalized verification matrix that correctly takes into account the influence of the structural elements of the encoder and the application of the iterative confidence propagation algorithm to it is substantiated.

Keywords: decoding, error-correcting code, algebraic method, generalized verification matrix, iterative confidence propagation algorithm.

1. Постановка проблемы

Одной из основных тенденций развития современных систем связи является усложнение методов формирования сигнально-кодовых конструкций с целью повышения удельной скорости передачи при минимизации ширины пропускания и мощности передатчика. Разработчики систем связи стремятся к повышению информационной эффективности систем связи и зачастую используют собственные разработки в области проектирования и построения телекоммуникационного оборудования, что ведет к широкому распространению уникальных методов модуляции и кодирования, многостанционного доступа. К последним можно отнести технологию множественного доступа с совмещением несущих, применение низкоплотностных кодов, турбокодов.

Собственные разработки крупнейших фирм-производителей, отсутствие рекомендаций и подробного описания структуры используемых сигнально-кодовых конструкций приводит к росту числа сигналов с неустановленными параметрами, большая часть которых связана с априорной неопределенностью относительно структуры помехоустойчивого кодера.

В связи этим актуализируется задача по разработке комплексов радиоконтроля, которые выполняют следующие функции: выявление неиспользуемых частот и незарегистрированных радиостанций в контролируемом диапазоне; выявление источников помех и обследование электромагнитной обстановки; измерение параметров излучений с целью установ-

ления соответствия условиям использования частот, определенным в разрешительных и нормативных документах.

Данные комплексы радиоконтроля являются неотъемлемой составной частью общегосударственной системы управления использованием радиочастотного спектра, а также могут быть использованы операторами связи.

Следовательно, разработка алгоритмов анализа и определения параметров кодированных сигналов является актуальной задачей, решение которой приведет к повышению эффективности ведения радиоконтроля.

2. Известные методы определения параметров помехоустойчивых кодов

Задача определения параметров и характеристик сигнально-кодовых конструкций существенно зависит от наличия априорной информации о структуре кодера. Разнообразие возможных исходных данных о его структуре порождает необходимость разработки и применения различных методов анализа, определяемых сочетанием неизвестных параметров.

Среди известных на сегодняшний день подходов к решению задачи определения параметров помехоустойчивых кодов и кодеров можно выделить следующие: метод полного перебора, статистический метод, алгебраический метод.

Метод полного перебора – метод определения параметров кодера путем перебора всех возможных параметров схемы кодера с последующим пробным декодированием и принятием решения на основе критерия $\min(P_{\text{ош}})$.

Статистический метод – метод определения параметров кодера, представляющий собой частный случай метода полного перебора, и основанный на анализе результатов пробного декодирования кодовых слов, составленных из фрагмента исследуемого цифрового потока для всего известного набора применяемых помехоустойчивых кодов.

Алгебраический метод – метод определения параметров кода, основанный на свойствах линейного векторного пространства, образованного кодовыми словами, заключающийся в преобразовании матрицы, составленной из кодовых слов, к каноническому виду. Данный подход является наиболее общим из всех известных.

Наиболее предпочтительным на практике является алгебраический метод, поскольку обладает невысокой вычислительной сложностью по сравнению с методом полного перебора. В зависимости от значений вероятности ошибки в канале связи можно выделить несколько областей применения алгебраического метода:

1) определение параметров помехоустойчивого кода при достаточном объеме выборки кодированной последовательности и нулевой вероятности ошибки на выходе канала связи $P_{\text{ош}} = 0$;

2) определение параметров помехоустойчивого кода при достаточном объеме выборки кодированной последовательности и ненулевой вероятности ошибки на выходе канала связи $0 < P_{\text{ош}} < P_{\text{ош}}^{\text{гран}}$, где $P_{\text{ош}}^{\text{гран}}$ – граничное значение вероятности ошибки, больше которого невозможно определение параметров сигнально-кодовой конструкции;

3) применение алгоритмов декодирования по полученной обобщенной проверочной матрице кода.

При реализации первого подхода необходимо составление матрицы из кодовых слов, не содержащих ошибки, иначе будет вычислен базис расширенного подпространства, образованного объединением векторов кодовых слов искомого линейного блочного кода и векторов ошибок. Необходимо отметить, что указанный метод предполагает наличие априорной информации относительно длины кодового слова n . В противном случае требуется организация дополнительной процедуры перебора значений указанных параметров кода.

Второй подход применяется для определения параметров в случае ненулевой вероятности ошибки на выходе канала связи. В данном случае возможно использование метода

статистического накопления оценок проверочных матриц, метода селекции выборки с использованием схемы со стиранием, метода итеративного исключения проверочной части, модифицированного алгоритма итеративного исключения проверочной части с использованием дополнительной информации от декодера.

В случае невозможности определения параметров помехоустойчивого кода следует применять алгоритмы декодирования, использующие проверочную матрицу кода.

3. Алгоритмы декодирования по проверочной матрице кода

В настоящее время существуют различные алгоритмы декодирования помехоустойчивых кодов по проверочной матрице кода. Условно их можно разделить на две группы: с мягким решением и с жестким решением. Как правило, алгоритм с жестким решением является частным случаем алгоритма с мягким решением. Поэтому остановимся на рассмотрении алгоритмов с мягким решением. В основе мягкого декодирования лежат два правила, основанных на применении критериев оптимальности. Первое состоит в выборе кодового слова, минимизирующего евклидово расстояние от кодового слова до принятой последовательности. Это правило минимизирует вероятность ошибки в последовательности, и реализующий его декодер является декодером максимального правдоподобия. Второе правило заключается в декодировании каждого символа кодового слова с минимизацией средней вероятности ошибки на символ. Характеристики декодеров, реализующие эти два правила, по существу, совпадают, поскольку минимизация вероятности ошибки символа ведет к минимизации вероятности ошибки последовательности и наоборот. Все используемые в настоящее время методы мягкого декодирования более длинных кодов представляют собой попытки аппроксимировать одно из указанных правил.

Наиболее важным среди алгоритмов декодирования, в которых делается попытка минимизировать вероятность ошибки символа, является алгоритм вероятностного декодирования, предложенный Галлагером, оптимальный алгоритм посимвольного декодирования Хартмана-Рудольфа, а также алгоритм Чейза.

Для сравнительной оценки рассмотренных алгоритмов декодирования произведен расчет необходимых вычислительных ресурсов для реализации декодера сверточного турбокода (ТКС). Расчет производился для параметров ТКС современных систем спутниковой связи *DVB-RCS*, *ArcLight*, *Surfbeam*. В табл. 1 представлено количество логических элементов (*Logic*) и ячеек памяти (*Mem*), необходимых для реализации рассмотренных алгоритмов декодирования в зависимости от длины кодового слова n , длины информационной части k , кодового расстояния d .

Таблица 1

Ресурсоемкость декодеров

Система связи, скорость кодирования	n	k	$n-k$	Вероятностный		Чейза		Хартмана-Рудольфа	
				<i>Mem</i>	<i>Logic</i>	<i>Mem</i>	<i>Logic</i>	<i>Mem</i>	<i>Logic</i>
DVB-RCS (48 пар), 1/3	288	96	192	$5 \cdot 10^4$	$7 \cdot 10^5$	$7 \cdot 10^{57}$	2^d	$5 \cdot 10^4$	$8 \cdot 10^{58}$
DVB-RCS (48 пар), 6/7	122	96	26	$3 \cdot 10^3$	$4 \cdot 10^4$	$7 \cdot 10^6$	2^d	$3 \cdot 10^3$	$9 \cdot 10^7$
DVB-RCS (220 пар), 2/3	660	440	220	$2 \cdot 10^5$	$3 \cdot 10^6$	$2 \cdot 10^{66}$	2^d	$2 \cdot 10^5$	$4 \cdot 10^{67}$
DVB-RCS (864 пары), 1/3	5184	1728	3456	$2 \cdot 10^7$	$4 \cdot 10^8$	$3 \cdot 10^{1040}$	2^d	$2 \cdot 10^7$	$5 \cdot 10^{1041}$
DVB-RCS (48 пар), 6/7	2220	1728	492	$1 \cdot 10^6$	$3 \cdot 10^6$	$2 \cdot 10^{148}$	2^d	$1 \cdot 10^6$	$4 \cdot 10^{147}$
ArcLight (ЦС), 1/3	24592	8192	16400	$4 \cdot 10^8$	$5 \cdot 10^9$	$8 \cdot 10^{4936}$	2^d	$4 \cdot 10^8$	$1 \cdot 10^{4938}$
ArcLight (AC), 1/3	1272	424	848	$1 \cdot 10^6$	$2 \cdot 10^7$	$2 \cdot 10^{255}$	2^d	$1 \cdot 10^6$	$4 \cdot 10^{256}$
SurfBeam, 1/2	5128	2556	2574	$2 \cdot 10^7$	$3 \cdot 10^8$	$7 \cdot 10^{774}$	2^d	$2 \cdot 10^7$	$9 \cdot 10^{775}$
SurfBeam, 3/4	5128	3830	1298	$6 \cdot 10^6$	$8 \cdot 10^7$	$6 \cdot 10^{390}$	2^d	$6 \cdot 10^6$	$7 \cdot 10^{391}$
SurfBeam, 7/8	5128	4470	658	$3 \cdot 10^6$	$4 \cdot 10^7$	$1 \cdot 10^{198}$	2^d	$3 \cdot 10^6$	$3 \cdot 10^{199}$

Для алгоритма Чейза и посимвольного декодирования характерен экспоненциальный рост вычислительной сложности с увеличением длины кодового слова, что говорит о невозможности их применения для современных систем связи.

Анализ результатов расчета ресурсоемкости, представленных в табл. 1, показывает, что для декодирования по проверочной матрице наилучшим с точки зрения минимизации затрат ресурсов является алгоритм вероятностного декодирования, предложенный Галлагером.

4. Обобщенная порождающая матрица кода

Кодер сверточного турбокода представляет собой схему параллельного либо последовательного соединения ветвей турбокода. На рис. 1 представлена схема j -й ветви турбокода, $j = 1 \dots N$.

Рис. 1. Ветвь турбокода

Под *ветвью* турбокода понимается последовательное соединение перемежителя, компонентного кодера и перфоратора. В конструкции турбокодов для простоты аппаратной реализации декодера как правило используются элементарные компонентные сверточные кодеры с разрядностью регистра сдвига L , $L = 1 \dots 4$. Обобщенная схема формирования турбокода с использованием N ветвей представлена на рис. 2.

Рис. 2. Обобщенная схема формирования сигналов с турбокодированием:
а – параллельный турбокод; б – последовательный турбокод

Операция кодирования в матричной форме может быть представлена умножением информационного вектора u на порождающую матрицу кода G :

$$c = uG. \quad (1)$$

Порождающая матрица кода в систематическом виде представляет собой конкатенацию единичной и проверочной подматриц и в классическом случае не отражает процедуры канального кодирования на различных этапах преобразования сигнала:

$$G = (I|P). \quad (2)$$

Процедуры перемежения и перфорации преобразуют сигнал на выходе схемы сверточного турбокодера, поэтому их влияние необходимо учитывать при получении обобщенной порождающей матрицы турбокода.

Обобщенная порождающая матрица $G_{\text{обобщ}}$ турбокода для схемы, представленной на рис. 3, может быть выражена через функцию матриц ветвей сверточного турбокода:

$$G_{\text{обобщ}} = \Psi(G_{\text{ветвь } 1}, G_{\text{ветвь } 2}, \dots, G_{\text{ветвь } N}), \quad (3)$$

где $G_{\text{ветвь } j}$ – матрица j -й ветви турбокода.

Матрица j -й ветви турбокода, зависит от порождающей матрицы компонентного кода $G_{\text{кодер } j}$, матрицы перемежителя $\Pi_{\text{перем } j}$ и матрицы перфоратора $M_{\text{перф } j}$:

$$G_{\text{ветвь } j} = f(G_{\text{кодер } j}, \Pi_{\text{перем } j}, M_{\text{перф } j}). \quad (4)$$

В качестве компонентного кодера в сверточных турбокодах применяется сверточный код, порождающая матрица $G^{\text{канон}}$ которого определяется канонической *ленточной матрицей* с шириной ленты, равной $(L+1)n$ для кода памяти L и скорости $1/N$. Первая строка является *образующей*, так как все остальные строки ленточной матрицы получены путем сдвига первой строки на символ вправо.

$$G^{\text{канон}} = \begin{pmatrix} g_0^1 & g_0^2 & \dots & \dots & \dots & g_0^N & \dots & \dots & \dots & g_L^1 & g_L^2 & \dots & \dots & \dots & g_L^N & 0 & 0 & 0 & \dots \\ 0 & g_0^1 & g_0^2 & \dots & \dots & g_0^N & \dots & \dots & \dots & g_L^1 & g_L^2 & \dots & \dots & \dots & g_L^N & 0 & 0 & \dots \\ 0 & 0 & g_0^1 & g_0^2 & \dots & \dots & g_0^N & \dots & \dots & g_L^1 & g_L^2 & \dots & \dots & \dots & g_L^N & 0 & \dots \\ 0 & 0 & 0 & \ddots & \dots & \dots & \dots & \dots & \dots & g_L^1 & g_L^2 & \dots & \dots & \dots & g_L^N & \ddots & \ddots \end{pmatrix}, \quad (5)$$

где g_i^j – i -й коэффициент j -го порождающего полинома сверточного кода.

Для систематического рекурсивного сверточного кода (СРСК) со скоростью k/n и длиной информационной части k порождающая матрица в систематическом виде $G^{\text{сист}}$ принимает вид:

$$G^{\text{сист}} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & p_1 & p_2 & p_3 & \dots & p_{n-k-1} & p_{n-k} \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 & p_1 & p_2 & \dots & p_{n-k-2} & p_{n-k-1} \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & p_1 & \dots & p_{n-k-3} & p_{n-k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 & \dots & p_1 & p_2 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & \dots & 0 & p_1 \end{pmatrix}. \quad (6)$$

Перемежитель – устройство, осуществляющее блочную перестановку позиций информационных бит в исходной последовательности. Блочная перестановка может быть описана с помощью биективной функции $\pi(\bullet): \{1, \dots, k\} \rightarrow \{1, \dots, k\}$. Действие перемежителя может быть представлено умножением информационного вектора u на матрицу перемежения Π , которая формируется из единичной матрицы I перестановкой столбцов согласно закону перемежения π :

$$\Pi_{i,j} = I_{i,\pi(j)}. \quad (7)$$

Перфоратор – устройство, реализующее функцию удаления по заданному закону $\mu(\bullet): \{1, 2, \dots, n\} \rightarrow \{0, 1\}$ бит базового кода для получения кода с более высокой скоростью. В работе показано, что результат действия перфоратора можно представить умножением кодового вектора на матрицу перфорации M , которая может быть получена из единичной матрицы I размером $n \times n$, путем удаления столбцов, соответствующих выкалываемым битам по закону μ :

$$M = \mu(I), \quad M_{i,z} = I_{i,j}, \quad z = \sum_{l=1}^j \mu(l). \quad (8)$$

Для параллельной схемы, представленной на рис. 3 а, проверочная подматрица $P_{\text{обобщ}}$ будет представлять собой конкатенацию проверочных подматриц ветвей турбокода:

$$P_{\text{обобщ}} = (P'_1 | P'_2 | \dots | P'_N). \quad (9)$$

Для последовательной схемы, представленной на рис. 2, б, проверочная подматрица $P_{\text{обобщ}}$ образуется произведением проверочных подматриц ветвей турбокода:

$$P_{\text{обобщ}} = (P'_1 \times P'_2 \times \dots \times P'_N), \quad (10)$$

где P'_j – проверочная подматрица j -й ветви турбокода, представляющая собой произведение матриц элементов ветви – перемежителя, перфоратора и подматрицы компонентного кодера:

$$P'_j = (\Pi_{\text{перем } j} \times P_{\text{кодер } j} \times M_{\text{перф } j}). \quad (11)$$

Графический вид порождающей матрицы параллельного сверточного турбокода с двумя компонентными СРСК с параметрами $n = 96$ и $k = 64$, скоростью 2/3 представлен на рис. 3.

Рис. 3. Графический вид порождающей матрицы турбокода:
а – систематический вид; б – канонический вид

Для схемы турбокодера (рис. 3) получены следующие обобщенные проверочные матрицы:

$$H_{\text{парал}} = \left(\left[(\Pi_1 \times P_1 \times M_1) | (\Pi_2 \times P_2 \times M_2) | \dots | (\Pi_N \times P_N \times M_N) \right]^T | I_{(n-k) \times (n-k)} \right), \quad (12)$$

$$\mathbf{H}_{\text{послед}} = \left(\left[(\mathbf{P}_1 \times \mathbf{P}_1 \times \mathbf{M}_1) \times (\mathbf{P}_2 \times \mathbf{P}_2 \times \mathbf{M}_2) \times \dots \times (\mathbf{P}_N \times \mathbf{P}_N \times \mathbf{M}_N) \right]^T \mid \mathbf{I}_{(n-k) \times (n-k)} \right). \quad (13)$$

Полученные обобщенные проверочные матрицы (12–13) возможно использовать для исправления ошибок в цифровом потоке с помощью алгоритма итеративного распространения доверия:

Проведенное имитационное моделирование процесса декодирования сигнала стандарта *ArcLight* с применением предложенного алгоритма итеративного декодирования, использующего проверочные матрицы (12–13), показало выигрыш от применения данного подхода по сравнению с демультимплексированием информационной части кодового слова.

В табл. 2 представлена ресурсоемкость разработанного декодера сигналов с ТКС *ArcLight*.

Таблица 2

Ресурсоемкость декодера сигналов с ТКС *ArcLight*

Частота синтеза, МГц	Кол-во лог. ячеек, шт.			Кол-во умножителей, шт.			Объем памяти, кбит		
	Требуемое значение	Ресурс ПЛИС	%	Требуемое значение	Ресурс ПЛИС	%	Требуемое значение	Ресурс ПЛИС	%
248	245 606	314 880	78	1 102	1 344	82	18 500	25 344	73

Проведенный расчет ресурсоемкости разработанного алгоритма для аппаратной платформы цифровой обработки сигналов *Xilinx ML605* для приема сигналов стандарта *ArcLight* со скоростью до 5 МБод показал возможность реализации на ПЛИС средней степени интеграции.

СПИСОК ЛИТЕРАТУРЫ

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005.
2. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. М.: Радио и связь, 1987. 392 с.