УДК 621.391

АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ УКОРОЧЕННЫХ АЛЬТЕРНАНТНЫХ КОДОВ

к.т.н. А.В. Северинов, к.т.н. Н.В. Пастухов, С.Л. Городецкий
(представил д.т.н., проф. Ю.В. Стасев)

В статье проводится анализ методов укорочения альтернантных кодов для построения помехоустойчивой системы автоматизированного управления.

В условиях постоянного совершенствования систем автоматизированного управления войсками, одной из задач их функционирования является обеспечение помехоустойчивости передаваемой информации. Решение этой задачи возможно на основе использования укороченных альтернантных кодов, обладающих наилучшими характеристиками в классе линейных блочных кодов [1]. Применение укороченных альтернантных кодов позволяет строить помехоустойчивые системы передачи данных с изменяемыми параметрами: длиной кодового блока **n** и числом информационных символов **k**.

Пусть линейный (**n**, **k**) - код имеет порождающую матрицу, **i** столбцов которой являются линейно независимыми (**i**<**k**). Множество векторов длины **n-i**, полученных удалением **i** компонент из кодовых векторов, образуют линейный (**n-i**, **k-i**) - код. Эта процедура называется укорочением, а код - укороченным кодом [1]. Порождающая матрица укороченного кода получается из порождающей матрицы исходного кода удалением **i** строк и **i** столбцов. При укорочении кода выбрасываемые символы полагаются равными нулю и не передаются, а на приемной они восстанавливаются и декодирование осуществляется на полной длине кода. При этом минимальное расстояние укороченного кода не меньше минимального расстояния исходного кода.

Укорочение кодов часто приводит к кодам с наилучшими параметрами. В [1] доказано, что при больших **n** укороченные коды достигают нижней границы Варшамова-Гилберта. Например, укороченный (55,16,19) - альтернантный код, задаваемый многочленом **G(x)** степени 9, является лучшим среди соответствующих кодов из таблиц [1].

Укороченные альтернантные коды строятся на элементах поля **L**, определенного на $\mathbf{GF(q^m)} - \{\alpha_1, \alpha_2, \ldots, \alpha_p\}$, где $\alpha_i \in \overline{GF}(q^m)$, **i=1,p** [2]. Имеется два варианта построения укороченного кода. В первом случае в качестве порождающего многочлена **G(x)** выбирается многочлен, имеющий некратные корни в поле $\mathbf{GF(q^m)}$ и при укорочении выбрасываются

нулевые частоты на позициях корней многочлена **G(x)**. Длина укороченного кода в этом случае будет равна (**n-p**), где **p** – количество корней порождающего многочлена. Во втором случае в качестве **G(x)** выбирается неприводимый многочлен, а из поля **GF(q^m)** выбрасываются некоторые частоты. Тогда длина кода уменьшится на количество выбрасываемых частот.

В случае построения укороченного альтернантного кода на основе порождающего многочлена, имеющего некратные корни, количество корней **p**, а следовательно и символов укорочения, будет определять степень многочлена **t** (**t** = **p**) и соответственно кодовое расстояние кода **d**. Поэтому в данном случае количество информационных символов укороченного кода равно

$$\mathbf{k' = k - p \geq n - mt - p = n - p(m + 1).}$$

В табл. 1 представлены параметры укороченных кодов для порождающих многочленов с различным количеством корней.

Таблица 1

Параметры альтернантных кодов для многочленов с корнями

Количество корней	Размерность поля			
	GF(32)	**GF**(64)	**GF**(128)	**GF**(256)
2	30,25,5	62,50,5	126,112,5	254,238,5
3	29,14,7	61,43,7	125,104,7	253,229,7
4	28,8,9	60,36,9	124,96,9	252,220,9
5	27,4,11	59,29,11	123,88,11	251,211,11
6	26,2,13	58,22,13 58,23,13	122,80,13	250,202,13
7	-	57,15,15 57,16,15 57,17,15	121,72,15	249,193,15

Анализ данных параметров показывает, что значительное изменение информационной длины кода и кодового расстояния при укорочении на один символ не позволяет гибко менять параметры альтернантного кода.

Для альтернантных кодов, построенных на основе неприводимых порождающих многочленов, известно три метода укорочения.

Метод укорочения №1. Пусть альтернантный код **Y**(**n**, **k**, **d**), **N** = $\mathbf{2^k}$, имеет проверочную матрицу **H**. Тогда матрица **H** с вычеркнутыми **p** столбцами является проверочной матрицей кода **Y'**(**n'**, **k'**, **d**) с параметрами: **n'** = **n - p**, **k'** = **k - p**.

Метод укорочения №2. Пусть альтернантный код **Y**(**n**, **k**, **d**), **N** = $\mathbf{2^k}$, имеет проверочную матрицу **H** и некоторое множество **P** из **p** позиций покрывают полностью **h** векторов из матрицы **H** (то есть все ненулевые позиции этих **h** векторов принадлежат множеству **P**). Тогда множество слов с вычеркнутыми **p** позициями множества **P** образуют код **Y'**(**n'**, **k'**, **d**) с параметрами: **n'** = **n - p**, **k'** = **k - p** + **h** [3].

Метод укорочения Хелгерта и Стинаффа. Пусть альтернантный

код **Y**(**n**, **k**, **d**), имеет порождающую (**k** × **n**) матрицу **G** вида

$$\mathbf{G} = \left(\frac{\mathbf{1\,1 \ldots 1}}{\mathbf{G_1}} \,\middle|\, \frac{\mathbf{0\,0 \ldots 0}}{\mathbf{G_2}} \right),$$

где число единиц в первой строке равно **d**. Тогда $\mathbf{G_2}$ является порождающей матрицей кода **Y'**(**n'**, **k'**, **d**) с параметрами $\mathbf{n'} = \mathbf{n} - \mathbf{d}$, $\mathbf{k'} = \mathbf{k} - \mathbf{1}$, $\mathbf{d'} \geq \lceil \mathbf{d/2} \rceil$ [1].

Рассмотрим данные методы укорочения на предмет использования их для построения помехоустойчивой системы управления.

Второй метод укорочения позволяет получить лучшие параметры кода. Однако для его применения необходимо знать количество единиц в любой строке проверочной матрицы **H** альтернантного кода **Y**(**n**, **k**, **d**), которое не меньше, чем минимальное расстояние **d'** дуального кода **Y'**. Для оценки дуального расстояния в основном используется частичный перебор на ЭВМ слов дуального кода [1, 3]. Однако для альтернантных кодов такие оценки неизвестны. Так как коды БЧХ являются подклассом альтернантных кодов, воспользуемся оценками дуального расстояния для кодов БЧХ. В табл. 2 представлены результаты расчета верхней оценки дуального расстояния, полученные согласно [3], для кодов БЧХ со скоростью **R** = 1/2.

Таблица 2

Верхняя оценка дуального расстояния для кодов БЧХ со скоростью **R**=1/2

n, **k**, **d**	511, 259, 57	255, 127, 33	127, 64, 19	63, 27, 13	31, 16, 7
d'	128	64	32	16	8

В табл. 3 представлены параметры укороченных двоичных альтернантных кодов (**n'**, **k'**), полученные на основе данного метода укорочения. В данном случае $\mathbf{d_1}$ обозначает минимальное количество единиц в одной строке, а $\mathbf{d_2}$ - в объединении двух строк проверочной матрицы **H** альтернантного кода.

Анализ представленных результатов показывает, что данный метод укорочения не позволяет укорачивать коды на малое количество символов. Следовательно, в этом случае невозможно гибко менять параметры кода, а также в большинстве случаев укорочение приводит к кодам, равным по длине кодам меньшего поля Галуа. А как известно, с увеличением размерности кода, при одинаковых **d**, скорость кода уменьшается, то есть значительное укорочение кода большего поля приводит к коду с меньшим числом информационных символов, чем укорочение на несколько бит кода меньшего поля.

Метод Хелгерта и Стинаффа позволяет укорачивать альтернантный код минимум на $\mathbf{d_{min}}$ символов. В табл. 4 представлено конструктивное кодовое расстояние некоторых альтернантных кодов со скоростью **R = 1/2**. Анализ данных табл. 4 показывает, что метод Хелгерта и Стинаффа имеет те же недостатки, что и второй метод укорочения.

Таблица 3

Параметры некоторых укороченных альтернантных кодов

M	**N, k, d**	$\mathbf{d_1}$	$\mathbf{d_2}$	$\mathbf{n'_1, к'_1, d}$	$\mathbf{n'_2, к'_2, d}$
7	127,92,11	≤32	≤48	95,61,11	76,46,11
	127,57,21	≤22		105,37,21	
	127,50,23	≤16	≤24	111,36,23	103,28,29
	127,36,29	≤14	≤24	113,23,29	103,14,29
8	255,223,9	≤96		159,128,9	
	255,191,17	≤64		191,128,17	
	255,159,25	≤48	≤99	207,112,25	156,62,25
	255,143,29	≤48	≤85	207,96,29	170,60,29
9	511,457,13	≤184		327,274,13	
	511,421,21511,385,	≤172		339,250,21	
	29	≤156		355,230,29	

Таблица 4

Конструктивное кодовое расстояние альтернантных кодов с **R** = 1/2

N	511	255	127	63	31
D	61	37	21	13	7

Следовательно, наиболее эффективным для построения помехоустойчивой системы является первый из методов укорочения, позволяющий укорачивать альтернантные коды на любое число символов и получать коды, обладающие заданными характеристиками по помехоустойчивости.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. / Под ред. Л.А. Бассалыго. – М.: Связь, – 1979. – 744 с.*
2. *Халимов Г.З., Северинов А.В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивого кодирования // Системы управления и связь. – Х. : НАНУ, ПАНИ, ХВУ. – 1996. – С. 116 - 119.*
3. *Зиновьев В.А., Лицын С.Н. Об укорочении кодов // Проблемы передачи информации. – 1984. – Т. 20, №1. – С. 3 - 11.*

Поступила 19.02.2002

***СЕВЕРИНОВ Александр Васильевич**, канд. техн. наук, зам. нач. кафедры Харьковского военного университета. В 1992 году окончил ХВВКИУРВ. Область научных интересов – применение помехоустойчивого кодирования в системах передачи данных.*

***ПАСТУХОВ Николай Васильевич**, канд. техн. наук, ст. преп. ХВУ. В 1991 году окончил ХВВКИУ. Область научных интересов – повышение помехозащищенности систем управления.*

***ГОРОДЕЦКИЙ Сергей Леонидович**, преп. ХВУ. В 1991 году окончил ХВВКИУ. Область научных интересов – применение помехоустойчивого кодирования в системах управления.*