

УДК 681.322

РЕКУРСИВНОЕ ПОСТРОЕНИЕ НЕЛИНЕЙНЫХ КОРРЕКТИРУЮЩИХ КОДОВ НА ОСНОВЕ БЛОК-СХЕМ

Ткаченко В.Г., Кокорев А.В.

*Одесская национальная академия связи им. А.С. Попова
Одесса, ул. Кузнечная, 1
kokorev.av@onat.edu.ua*

РЕКУРСИВНА ПОБУДОВА НЕЛІНІЙНИХ КОРЕГУВАЛЬНИХ КОДІВ НА ОСНОВІ БЛОК-СХЕМ

Ткаченко В.Г., Кокорев О.В.

*Одеська національна академія зв'язку ім. О.С. Попова
Одеса, вул. Ковальського 1
kokorev.av@onat.edu.ua*

RECURSIVE CONSTRUCTION OF NONLINEAR CORRECTING CODES ON THE BASIS OF BLOCK DESIGN

Tkachenco V.G., Kokorev A.V.

*Odessa national academy of telecommunication n.a. O.S. Popov
Odessa, str. Kuznehnaya 1
kokorev.av@onat.edu.ua*

Аннотация. В статье определены блочные нелинейные k -угольные коды. Рассмотрены способы построения некоторых n -угольных кодов и предложен эффективный универсальный рекурсивный метод построения кодов большой длины на основе блок-схем для криптосистем с коррекцией заданного числа ошибок. Среди кодов с заданной длиной кодового слова и заданным числом единиц в этом слове эти коды содержат максимальное число кодовых слов. Достоинствами этих кодов является быстрота шифрации и дешифрации, а также возможность быстрой смены кода без изменения таблиц шифрации и дешифрации. Возможно использование этих кодов в криптосистемах.

Ключевые слова: корректирующие коды, нелинейные k -угольные коды, криптосистема, штейнеровы системы, аффинная плоскость, проективная плоскость.

Анотація. У статті визначено блокові нелінійні k -кутові коди. Розглянуто способи побудови деяких k -кутових кодів та запропоновано ефективний універсальний рекурсивний метод побудови кодів більшої довжини на основі блок-схем для криптосистем з коригуванням заданої кількості помилок. Серед кодів із заданою довжиною кодового слова і заданим числом одиниць у цьому слові ці коди містять максимальне число кодових слів. Перевагами цих кодів є швидкість цифрації та дешифрації, а також можливість швидкої зміни коду без зміни таблиць цифрації та дешифрації. Можливе використання цих кодів у криптосистемах.

Ключові слова: коригувальні коди, нелінійні k -кутові коди, криптосистема, штейнерови системи, афінна площина, проективна площина.

Abstract. In the article are defined nonlinear k -gonal block codes. The methods of constructing n -gonal codes are considered. Efficient universal recursive methods of constructing codes great length on the basis of block design for any predetermined number of errors are suggested. Among the codes with a predetermined length codeword and a predetermined number of units in the word, these codes will have a maximum number of codewords. Dignity of these codes is speed of encoding and decoding. Also possibility of fast change of a code without change of tables of encoding and decoding. This makes it possible to use these in cryptosystems.

Key word: correcting codes, nonlinear k -gonal codes, cryptosystem, Steiner system, affine plane, projective plane.

В процессе передачи информации в криптосистемах по телекоммуникационным сетям связи возникает проблема коррекции ошибок. Контроль целостности данных и коррекции ошибок – важные задачи на многих уровнях работы с информацией. Одним из средств решения этих задач является применение помехоустойчивых кодов, лежащих в основе криптосистем.

К настоящему времени разработано много различных помехоустойчивых кодов для криптосистем, отличающихся друг от друга расстоянием, избыточностью, структурой, функциональным назначением, корреляционными свойствами, алгоритмами кодирования и декодирования, формой частотного спектра ([1...4]). На основе монотонных булевых функций построен ряд криптосистем [5...9], с коррекцией ошибок. В частности, в системе на основе треугольных кодов для построения кодов большой длины использовались рекурсивные методы [6, 9].

Однако рекурсивные методы, используемые в [6, 9] не позволяют строить коды, если число единиц в кодовом слове больше 3.

Целью данной работы является разработка рекурсивного метода для построения кодов большой длины и мощности, быстрой шифрацией, дешифрацией и сменой кода для криптосистем с коррекцией заданного числа ошибок.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ k -УГОЛЬНЫХ КОДОВ

В данной статье в качестве кодовых слов будем рассматривать векторы длины n $\tilde{p} = (p_1, \dots, p_i, \dots, p_n)$, компоненты которых принимают значения из множества $\{0,1\}$, и количество единичных компонент в векторе равно k . Такие кодовые слова имеют вес Хэмминга (количество единиц в кодовом слове) равный k . Расстоянием Хэмминга (кодовым расстоянием) между двумя кодовыми словами \tilde{p} и \tilde{s} называется число $\rho(\tilde{p}, \tilde{s})$ равное количеству компонент, в которых они различаются [1]. Длиной кода назовём длину кодового слова. Всего таких кодовых слов с весом k могут быть C_n^k . Кодовые расстояния между различными словами в этом случае могут быть $2, 4, 6, \dots, 2k$. Для корректирующих кодов применимы только кодовые слова с расстоянием $4, 6, \dots, 2k$. Количество кодовых слов называется мощностью кода. Такие коды с кодовым расстоянием $2k$ малоинтересны, поскольку их мощность мала и всегда равна $[n/k]$. В любой такой паре кодовых слов нет совпадающих единичных бит. В дальнейшем будем рассматривать максимальные коды с $\rho(\tilde{p}, \tilde{s}) \geq 2k - 2$, поскольку они исправляют максимальное количество ошибок. Из определения расстояния Хэмминга следует, что в таких кодах для каждой пары кодовых слов общей может быть только одна единица. Такие коды легко представить в виде монотонных булевых функций ранга n , веса 1 и мощности m , где m равно мощности кода. [6...9].

Для исследования таких кодов можно использовать блок-схемы.

В [10...12] приведены следующие определения блок-схемы, ВІВ блок-схемы, аффинной и проективной плоскостей.

Определение. Уравновешенной неполной блок-схемой (или просто блок-схемой) $B(v, b, r, k, \lambda)$ называется такое размещение v различных элементов по b блокам, что каждый блок содержит точно k различных элементов, каждый элемент появляется точно в r различных блоках и каждая пара различных элементов b_i, b_j появляется точно в λ блоках.

ПРИМЕР 1. Для $v = 7, b = 7, r = 3, k = 3, \lambda = 1$ имеем такие блоки:

$b_0:$	(0, 1, 3)	$b_3:$	(3, 4, 6)	$b_6:$	(6, 0, 2)
$b_1:$	(1, 2, 4)	$b_4:$	(4, 5, 0)		
$b_2:$	(2, 3, 5)	$b_5:$	(5, 6, 1)		

Определение. Уравновешенной относительно пар (элементов) блок-схемой $VIB(v, (b_1, \dots, b_m), (k_1, \dots, k_m), \lambda)$ называется такое размещение v элементов по $b = \sum_1^m b_i$ блокам,

что: 1) b_i блоков содержит по $k_i < v$ различных элементов при некотором $i = 1, \dots, m$; 2) каждая пара элементов появляется вместе точно в λ блоках.

Любая блок-схема или BIB блок-схема является кодом. В этом случае номера единичных битов кодовых слов соответствуют элементам блока, а сами кодовые слова соответствуют блокам в этой блок-схеме. Очевидно, что число λ соответствует расстоянию Хэмминга, а именно: $\rho(\tilde{a}, \tilde{b}) = 2(k - \lambda)$.

Определение. Корректирующая способность – характеристика кода, которая равна максимальному количеству исправляемых ошибок в кодовых словах. Корректирующая способность равна $[(d-1)/2]$, где d – минимальное расстояние между кодовыми словами.

Так как число кодовых слов, у которых $\rho(\tilde{a}, \tilde{b}) = 2k$ мало, то в реальных кодах наибольшая корректирующая способность кода достигается, когда $\lambda = 1$ и равна $2(k-1) = [(2k-3)/2]$.

В дальнейшем рассматриваются только блок-схемы с $\lambda = 1$, т.е. штейнеровы системы.

В предложенном методе построения корректирующих кодов будут использованы проективная и аффинная плоскости.

Определение. Система $PG(2, n)$, имеющая конечное количество точек называется проективной плоскостью порядка n , если удовлетворяет следующим аксиомам:

1. Через две различные точки P и Q плоскости проходит прямая, причем, только одна.
2. Любые две прямые имеют общую точку.
3. Существуют три точки, не лежащие на одной прямой.
4. Каждая прямая содержит не менее трёх точек

В общем случае проективная плоскость порядка n имеет $n^2 + n + 1$ точек и столько же прямых. Каждая линия содержит $n + 1$ точек, и каждая точка принадлежит $n + 1$ прямой.

Определение. Система $EG(2, n)$, имеющая конечное количество точек называется аффинной плоскостью порядка n , если удовлетворяет следующим аксиомам:

1. Для любых двух различных точек существует только одна прямая, содержащая эти точки.
2. Пересечение двух различных прямых содержит ровно одну точку.
3. Существует множество из четырёх точек, никакие три из которых не принадлежат одной прямой.

В общем случае проективная плоскость порядка n имеет n^2 точек и $n^2 + n$ прямых. Каждая линия содержит n точек, и каждая точка принадлежит $n + 1$ прямой.

Аффинная и проективная плоскости являются блок-схемами, в которых каждый блок состоит из номеров точек находящихся на некоторой прямой.

Дадим определение k -угольного кода.

Определение 1. k -угольным кодом называется штейнерова система, в каждом блоке которой содержится k элементов.

Эти коды являются блоковыми нелинейными, поскольку разность любых двух кодовых слов не является кодовым словом.

Перед тем как описать рекурсивный метод построения кодов на основе блок-схем введём следующие определения.

Определение 2. Проективным расширением штейнеровой системы $A0(v, b, r, k)$ называется штейнерова система $C0$, полученная объединением блоков b проективных плоскостей $B0(k(k-1)+1, k(k-1)+1, k, k) = PG(2, k-1)$, построенных для каждого блока штейнеровой системы $A0$.

Определение 3. Аффинным расширением штейнеровой системы $A0(v, b, r, k)$ называется штейнерова система $C0$, полученная объединением блоков b аффинных плоскостей $B0((k-1)(k-1), k(k-1), k, k-1) = EG(2, k-1)$, построенных для каждого блока штейнеровой системы $A0$.

Определение 4. Проективно-аффинным расширением $B1B$ штейнеровой системы $A0(v, b1, b2), (k, k+1)$ называется штейнерова система $C0$, полученная объединением блоков $b1$ проективных плоскостей $B0(k(k-1)+1, k(k-1)+1, k, k) = PG(2, k-1)$, построенных для каждого блока из k элементов, и $b2$ аффинных плоскостей $B0(k \cdot k, k(k+1), k+1, k) = EG(2, k)$, построенных для каждого блока из $k+1$ элемента $B1B$ штейнеровой системы $A0$.

РЕКУРСИВНЫЕ МЕТОДЫ ПОСТРОЕНИЯ k -УГОЛЬНЫХ КОДОВ

Опишем рекурсивный метод построения блок-схем на примере построения кода длиной 64 из кода длиной 21.

ПРИМЕР 2. В качестве блок-схемы $A0$ длины 21 возьмем проективную плоскость 4-го порядка $PG(2,4)$ $v = 21, b = 21, r = 5, k = 5, \lambda = 1$

1) (1,2,7,9,19)	7) (3,6,7,12,14)	(9,12,13,18,20) 14)	(3,5,15,18,19) 20)
2) (2,3,8,10,20)	8) (4,7,8,13,15)	(0,10,13,14,19) 15)	(4,6,16,19,20) 21)
3) (0,3,4,9,11)	9) (5,8,9,14,16)	(1,11,14,15,20) 16)	(0,5,7,17,20)
4) (0,1,6,8,18)	10) (6,9,10,15,17) 11)	(0,2,12,15,16)	
5) (1,4,5,10,12)	(7,10,11,16,18) 12)	17) (1,3,13,16,17) 18)	
6) (2,5,6,11,13)	(8,11,12,17,19) 13)	(2,4,14,17,18) 19)	

Пусть множество E , состоит из точки 0 и пар (x, y) , где $0 \leq x \leq 20, 0 \leq y \leq 2$. Построим блоки, содержащие 0, следующим образом: $(0, (x, 0), (x, 1), (x, 2))$. Будем такие блоки называть выделенными блоками. В парах (x, y) в качестве элементов x возьмём элементы блока 1 блок-схемы $A0$: (1,2,7,9). В результате получим 16-элементное множество $E1$. Перенумеруем все пары (x,y) следующим образом $(0,0) = 1, (1,0) = 2, \dots, (0,1) = 22, \dots, (20,2) = 63$. В результате получим такое множество $E1 = \{0, 1, 2, 7, 9, 19, 22, 23, 28, 30, 40, 43, 44, 49, 51, 61\}$. На этом множестве построим блок-схему $B1$ – аффинную плоскость 4-го порядка $EG(2,4)$ $v = 16, b = 20, r = 5, k = 4, \lambda = 1$.

1.1) (0,1,22,43)	1.6) (1,2,9,28)	1.11) (7,22,30,44)	1.16) (28,40,44,51)
1.2) (0,2,23,44)	1.7) (2,7,40,43)	1.12) (23,43,49,51)	1.17) (1,44,49,61)
1.3) (0,7,28,49)	1.8) (7,9,23,61)	1.13) (9,19,43,44)	1.18) (2,19,30,49)
1.4) (0,9,30,51)	1.9) (1,23,30,40)	1.14) (9,22,40,49)	1.19) (1,7,19,51)
1.5) (0,19,40,61)	1.10) (2,22,51,61)	1.15) (28,30,43,61)	1.20) (19,22,23,28)

Выделенными блоками в блок-схеме $B1$ являются блоки, содержащие 0, т.е. с номерами 1.1...1.5.

Аналогично по блоку 2 блок-схемы $A0$ $PG(2,4)$ строим множество $E2 = \{0, 2, 3, 8, 10, 20, 23, 24, 29, 31, 41, 44, 45, 50, 52, 62\}$. На этом множестве построим блок-схему $B2$ – аффинную плоскость 4-го порядка $EG(2,4)$ $v = 16, b = 20, r = 5, k = 4, \lambda = 1$ с помощью такой замены элементов блок-схемы $B1$ (согласно лемме 3):

$1 \rightarrow 2 \rightarrow 3, 7 \rightarrow 8, 9 \rightarrow 10, 19 \rightarrow 20, 22 \rightarrow 23 \rightarrow 24, 28 \rightarrow 29, 30 \rightarrow 31, 40 \rightarrow 41,$
 $43 \rightarrow 44 \rightarrow 45, 49 \rightarrow 50, 51 \rightarrow 52, 61 \rightarrow 62$

2.1) (0,2,23,44) 2.2)	2.6) (2,3,10,29) 2.7)	2.11) (3,20,31,50)	2.16) (10,23,41,50)
(0,3,24,45) 2.3)	(2,8,20,52) 2.8)	2.12) (3,23,52,62)	2.17) (20,23,24,29)
(0,8,29,50) 2.4)	(2,24,31,41)	2.13) (8,10,24,62)	2.18) (24,44,50,52)
(0,10,31,52) 2.5)	2.9) (2,45,50,62) 2.10)	2.14) (8,23,31,45)	2.19) (29,31,44,62)
(0,20,41,62)	(3,8,41,44)	2.15) (10,20,44,45)	2.20) (29,41,45,52)

Выделенными блоками в блок-схеме $B2$ являются блоки 2.1...2.5

Используя таким образом все 21 блок блок-схемы A_0 , мы получим 21 аффинную плоскость, в которые будут входить 420 блоков. При этом невыделенные блоки не будут иметь повторяющихся пар таких блоков будет $15 \cdot 21 = 315$. Теперь, мы добавим блоки, по которым происходят пересечения блок-схем B_i и B_j , $1 \leq i, j \leq 21$, $i \neq j$. Такие пересечения будут происходить только по выделенным блокам (лемма 1). таких блоков во всех B_j будет $21 \cdot 5 = 105$. Но по лемме таких блоков будет 21. Поэтому будем иметь в сумме $315 + 21 = 336$ непесекающихся блоков. Таким образом, мы получили все блоки штейнеровой системы C_0 с параметрами $v = 64$, $b = 336$, $r = 21$, $k = 4$.

Для распространения построения из примера 1 на произвольные штейнеровы системы предварительно докажем три леммы.

ЛЕММА 1. Любой невыделенный блок может входить только в одну из штейнеровых систем B_i .

Доказательство. Так как в качестве A_0 рассматривается штейнерова система, то любые два блока a_i и a_j из A_0 либо не пересекаются, либо имеют один общий элемент. В первом случае множества E_i и E_j имеют один общий элемент, равный 0, а значит штейнеровы системы B_i и B_j , построенные из элементов этих множеств, не имеют общих блоков. Во втором случае блоки a_i и a_j имеют общий элемент x , а множества E_i и E_j имеют в качестве общих элементов 0 и пары (x, y) , где x постоянно, а y может принимать все допустимые значения. Всего общих элементов в E_i и E_j столько, сколько их содержится в одном блоке штейнеровых систем B_i и B_j . Все эти общие элементы входят в один выделенный блок, общий для штейнеровых систем B_i и B_j . Это доказывает, что B_i и B_j не имеют общих невыделенных блоков.

ЛЕММА 2. Любые два несовпадающих блока штейнеровых систем B_i и B_j не содержат общую пару элементов.

Доказательство. По построению выделенные блоки не имеют общей пары и никакая пара из выделенного блока не может входить в невыделенный блок. Допустим 2 невыделенных блока из B_i и B_j содержат общую пару элементов. Тогда эта пара является общей для множеств E_i и E_j , а значит согласно лемме 1 входит в выделенный блок, общий для B_i и B_j . Тогда B_i содержит выделенный и невыделенный блоки с общей парой элементов. Это противоречит тому, что B_i является штейнеровой системой. Лемма доказана.

ЛЕММА 3. Любая штейнерова система B_i получается перенумерацией элементов штейнеровой системы B_1 .

Доказательство. Штейнеровы системы B_1 и B_i строятся из блоков a_1 и a_i штейнеровой системы A_0 . Однозначно отобразим элементы блока a_1 на элементы блока a_i . При этом общий элемент два блока (если он есть) отображается на себя. Элементам блоков a_1 и a_i соответствуют компоненты x в парах (x, y) , принадлежащих множествам E_1 и E_i . При таком отображении получается однозначная перенумерация элементов множества E_1 в элементы множества E_i . При этом из штейнеровой системы B_1 получается штейнерова система B_i .

В доказательстве лемм 1...3 не используется то, что в примере 1 в качестве B_i и B_j берутся аффинные плоскости. Поэтому леммы 1...3 справедливы, когда B_i и B_j являются штейнеровыми системами

Распространим построение из примера 2 на случай произвольных v и k .

Теорема 1. Если существует штейнерова система $A_0(v, b, r, k)$ и существует аффинная плоскость $k-1$ -го порядка $B_0((k-1)^2, k(k-1), k, k-1) = EG(2, k-1)$, то существует аффинное расширение $C_0(v(k-2)+1, b \cdot k(k-2) + v, v, k-1)$ штейнеровой системы A_0 . Аффинные плоскости B_i существуют для $k-1$ вида p^i , где p – простое число.

Доказательство. Согласно лемме 1 в b аффинных плоскостях B_i присутствуют $b \cdot k(k-1) - b \cdot k$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в аффинном расширении C_0 штейнеровой системы A_0 содержится $b \cdot k(k-2) + v$ блоков. Во все эти блоки по построению входят $v(k-2)+1$ элементов, так как x в парах (x, y) меняется в об-

щем случае от 0 до $v-1$, а y от 0 до $k-3$. Каждая пара (x, y) входит в $r \cdot (k-1)$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r \cdot (k-1) + 1 = v$, то каждый элемент аффинного расширения $C0$ входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b \cdot k(k-2) + v$ блоках содержится

$b \cdot k(k-2) \cdot (k-1) \cdot (k-2)/2 + v \cdot (k-1) \cdot (k-2)/2$ пар. Поскольку для блок-схем $b \cdot k = v \cdot r$, то количество пар равно $v \cdot (v-1) \cdot (k-2)^2/2 + v \cdot (k-1) \cdot (k-2)/2 = v^2 \cdot (k-2)^2/2 + v \cdot (k-2)/2$, т.е. количеству пар, которые образуют $v(k-2) + 1$ элементов. Это доказывает, что $C0$ штейнерова система.

В случае когда $v=40$, то эту теорему применить нельзя. Из блок-схемы с $v=13$ построить блок-схему $v=40$ можно с помощью проективной плоскости.

Теорема 2. Если существует штейнерова система $A0(v, b, r, k)$ и существует проективная плоскость $k-1$ -го порядка $B0(k(k-1) + 1, k(k-1) + 1, k, k) = PG(2, k-1)$, то существует проективное расширение $C0(v(k-1) + 1, b(k-1) \cdot (k-1) + v, v, k)$ штейнеровой системы $A0$. Проективная плоскость $B0$ существует для $k-1$ вида p^i , где p – простое число. Штейнерова система $B0$ симметрична.

Доказательство. Согласно лемме 1 в b проективных плоскостях Bi присутствуют $b \cdot (k(k-1) + 1) - b \cdot k$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в проективном расширении $C0$ блок-схемы $A0$ содержится $b(k-1)^2 + v$ блоков. Во все эти блоки по построению входят $v(k-1) + 1$ элементов, так как x в парах (x, y) меняется в общем случае от 0 до $v-1$, а y от 0 до $k-3$. Каждая пара (x, y) входит в $r \cdot (k-1)$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r \cdot (k-1) + 1 = v$, то каждый элемент проективного расширения $C0$ входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b(k-1)^2 + v$ блоках содержится $b(k-1)^2 \cdot k(k-1)/2 + v \cdot k(k-1)/2$ пар. Поскольку для блок-схем $b \cdot k = v \cdot r$, то количество пар равно $v \cdot (v-1) \cdot (k-1)^2/2 + v \cdot k(k-1)/2 = v \cdot (k-1)(v \cdot (k-1) + 1)/2$, т.е. количеству пар, которые образуют $v(k-1) + 1$ элементов. Это доказывает, что $C0$ штейнерова система.

ПРИМЕР 3. Из блок-схемы $A0(13, 13, 4, 4)$ и такой же блок-схемы $B0(13, 13, 4, 4)$ получим блок-схему $C0(40, 130, 13, 4)$. Пусть блок-схемы $A0$ и $B0$ такие:

1)	(1, 2, 3, 4)	5)	(2, 5, 8, 11)	9)	(3, 5, 9, 13)
2)	(1, 5, 6, 7)	6)	(2, 6, 9, 12)	10)	(3, 7, 8, 12)
3)	(1, 8, 9, 10)	7)	(2, 7, 10, 13)	11)	(4, 5, 10, 12)
4)	(1, 11, 12, 13)	8)	(3, 6, 10, 11)	12)	(4, 6, 8, 13)
				13)	(4, 7, 9, 11)

Из блока 1 получим так же как в примере 2 блок-схему $B1(13, 13, 4, 4)$. Из неё перенумерацией элементов получим блок-схемы $B2 - B13$. В результате получим 117 невыделенных и 13 выделенных блоков блок-схемы $C0$.

Повторно применяя теорему 2 к $C0(40, 130, 13, 4) = A1$ получим бесконечную последовательность штейнеровых систем:

$$A0(13, 13, 4, 4) \Rightarrow A1(40, 130, 13, 4) \Rightarrow \dots \Rightarrow A3(364, 11011, 121, 4) \Rightarrow \\ \Rightarrow \dots \Rightarrow Ai(9841, 8069620, 3280, 4) \Rightarrow \dots$$

В случае, когда $v=52$ теоремы 1 и 2 применить нельзя. Зато можно построить штейнерову систему с $v=52$, используя $B1B$ штейнерову систему $A0$.

Теорема 3. Если существует $B1B$ штейнерова система $A0(v, (b1, b2), (k, k+1))$, существует проективная плоскость $k-1$ -го порядка $B0(k(k-1) + 1, k(k-1) + 1, k, k) = PG(2, k-1)$ и существует аффинная плоскость k -го порядка $D0(k \cdot k, k(k+1), k+1, k) = EG(2, k)$, то существует проективно-аффинное расширение $C0(v(k-1) + 1, b1(k-1)(k-1) + b2(k \cdot k - 1) + v, v, k)$

BIB штейнеровой системы A_0 . Обе плоскости существуют для $k-1$ вида $p_1^{k-1} \cdot i1$ и k вида p_2^{k-1} , где p_1 и p_2 – простые числа.

Доказательство. Согласно лемме 1 в $b1$ проективных и $b2$ аффинных плоскостях B_i присутствуют $b1 \cdot (k(k-1) + 1) - b1 \cdot k + b2 \cdot k(k+1) - b2 \cdot (k+1)$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в проективно-аффинном расширении C_0 блок-схемы A_0 содержится $b1(k-1)^2 + b2(k^2-1) + v$ блоков. Во все эти блоки по построению входят $v(k-1) + 1$ элементов, так как x в парах (x, y) меняется в общем случае от 0 до $v-1$, а y от 0 до $k-2$. Каждая пара (x, y) входит в $r(k-1) + k$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r \cdot (k-1) + 1 = v$, то каждый элемент проективного расширения C_0 входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b1(k-1)^2 + b2(k^2-1) + v$ блоках содержится $b1(k-1)^2 \cdot k \cdot (k-1)/2 + b2(k^2-1) \cdot k \cdot (k-1)/2 + v \cdot k \cdot (k-1)/2$ пар. Поскольку для блок-схем $(b1 + b2) \cdot k = v \cdot r$, то количество пар равно $v \cdot (v-1) \cdot (k-1)^2/2 + v \cdot k \cdot (k-1)/2 = v \cdot (k-1) \cdot (v \cdot (k-1) + 1)/2$, т.е. количеству пар, которые образуют $v(k-1) + 1$ элементов. Это доказывает, что C_0 штейнерова система.

ПРИМЕР 4. Пусть задана *BIB* блок-схема $A_0(v=17, (b1=16, b2=4), (k=4, k+1=5))$:

$a1)$ (0, 1, 2, 3, 4)	$a8)$ (1, 8, 12, 16)	$a15)$ (3, 7, 9, 14)
$a2)$ (0, 5, 6, 7, 8)	$a9)$ (2, 5, 10, 15)	$a16)$ (3, 8, 10, 13)
$a3)$ (0, 9, 10, 11, 12)	$a10)$ (2, 6, 9, 16)	$a17)$ (4, 5, 12, 14)
$a4)$ (0, 13, 14, 15, 16)	$a11)$ (2, 7, 12, 13)	$a18)$ (4, 6, 11, 13)
$a5)$ (1, 5, 9, 13)	$a12)$ (2, 8, 11, 14)	$a19)$ (4, 7, 10, 16)
$a6)$ (1, 6, 10, 14)	$a13)$ (3, 5, 11, 16)	$a20)$ (4, 8, 9, 15)
$a7)$ (1, 7, 11, 15)	$a14)$ (3, 6, 12, 15),	

проективная плоскость 3-го порядка $B_0(13, 13, 4, 4)$ и аффинная плоскость 4-го порядка $D_0(16, 20, 5, 4)$. Из A_0, B_0 и D_0 можно построить проективно-аффинное расширение $C_0(52, 221, 17, 4)$. А именно, из блоков $a1 - a4$ блок-схемы A_0 получим 4 аффинных плоскости $D_1 - D_4(13, 13, 4, 4)$ (как в примере 2), которые дадут 144 невыделенных блока, а из остальных блоков схемы A_0 получим 16 проективных плоскостей $B_5 - B_{20}(16, 20, 5, 4)$ (как в примере 3), которые дадут 60 невыделенных и 17 выделенных блоков (по построению) проективно-аффинного расширения $C_0(52, 221, 17, 4)$.

Для отдельных случаев k могут существовать и другие рекуррентные способы построения кодов. В частности, для случая $k=3$ в [7] доказаны теорема А и теорема Б, а также приведена теорема Мура.

Теорема А. Пусть существует треугольный код со словами кодовой длины k (k нечётно и $k \not\equiv 5 \pmod{6}$) мощности $m = k(k-1)/6$. Тогда существует треугольный код со словами кодовой длины $n = 2k$ мощности $4m = n(n-2)/6$.

Теорема Б. Пусть существуют системы троек Штейнера порядков v_1 и v_2 : $S_1(v_1, b_1, r_1, 3)$ и $S_2(v_2, b_2, r_2, 3)$. Тогда существует штейнерова система $S\left(v_1 v_2, \frac{v_1 v_2 (v_1 v_2 - 1)}{6}, \frac{v_1 v_2 - 1}{2}, 3\right)$.

Теорема Мура. Пусть существуют системы троек Штейнера порядков v_1 и v_2 : $S_1(v_1, b_1, r_1, 3)$ и $S_2(v_2, b_2, r_2, 3)$. Пусть также либо $v_3 = 1$, либо v_3 является порядком системы троек Штейнера $S_3(v_3, b_3, r_3, 3)$, которая является подсистемой в S_2 . Тогда можно построить систему троек Штейнера $S(v, b, r, 3)$ с $v = v_3 + v_1(v_2 - v_3)$, содержащую v_1 подсистем порядка v_2 и по крайней мере по одной подсистеме порядков v_1 и v_3 (если v_3 не равно 1).

Для случая $k=4$ можно доказать теорему аналогичную теореме Б.

АЛГОРИТМЫ ШИФРАЦИИ И ДЕШИФРАЦИИ k -УГОЛЬНЫХ КОДОВ

Шифрацию и дешифрацию рассмотрим при $k = 4$. Так как расстояние Хэмминга между любыми кодовыми словами не меньше $2(k-1)$, то такой четырёхугольный код может исправлять $\lfloor (2k-3)/2 \rfloor$, символов передаваемого кодового слова. Кодовые слова в таблице шифрации (табл. 1) упорядочены по возрастанию.

Дешифрация проводится с помощью таблицы (двумерного массива), где в заголовках строк и столбцов будут записаны номера единичных битов, а в самой таблице номера кодовых слов. По номерам двух битов кодового слова мы определяем переданное информационное сообщение. При этом номера столбцов соответствуют младшему биту, а номера строк старшему биту передаваемого сообщения.

ПРИМЕР 5. Обнаружение одной ошибки. Рассмотрим код с $k = 4$ и длиной n , по каналу криптосистемы передаётся два сообщения 2 и 1. Эти сообщения кодируются двумя кодовыми словами (по таблице 1): 0000...01110001 и 0000...00001111, т.е. всего передаётся $2n$ бита. Пусть были приняты два кодовых слова 0000...0110001 и 000...10001111. При приёме определяются номера битов кодовых слов для 1-го кодового слова это биты: 0, 4, 5, для 2-го – 0, 1, 2, 3, 7. Применим таблицу декодирования (табл. 2) для определения переданного сообщения соответствующего первому кодовому слову. Номер младшего единичного бита переданного слова равен 0, а номер старшего 5. На пересечении соответствующей строки и столбца стоит 2. Это значит, что передано сообщение 2. Ошибка передачи для 1-го кодового слова исправлена.

Рассмотрим, как происходит декодирование в случае, если вместо четырёх единичных битов было принято пять единичных битов, на примере второго кодового слова. Из единичных битов 2-го кодового слова можно образовать 10 пар: (0;1), (0;2), (0;3), (1;2), (1;3), (2;3), (0;7), (1;7), (2;7), (3;7). Этим парам в таблице декодирования соответствуют переданные сообщения: 1, 1, 1, 1, 1, 4, 6, 9, 10. Шесть из найденных в таблице сообщений одинаковы и равны 1. Это означает, что шесть первых пар битов образуют второе кодовое слово, т.е. было передано кодовое слово 0000...00001111. Ошибка передачи для 2-го кодового слова исправлена. Можно показать, что в случае приёма пять битов вместо четырех достаточно найти в таблицы для полученных пар два совпадающих сообщения, т.е. в приведенном примере вместо шесть пар достаточно было проверить только пары (0;1) и (0;2). В худшем случае достаточно проверить шесть пар, что требует шесть считываний из таблицы 1.

Несложно подсчитать, сколько в среднем нужно проверить пар в этом случае. Обозначим через x случайную величину – количество проверяемых пар, p – вероятности значений x . Значения p_i найдём по формуле $p_i = \frac{C_6^1 \cdot C_4^{i-2}}{C_{10}^{i-1}} \cdot \frac{5}{10-i+1}$. Имеем закон распределения этой случайной величины:

x_i	2	3	4	5	6
p_i	0,333333	0,333333	0,214286	0,095238	0,02381

Математическое ожидание $mx = 3,14$. Следовательно, в этом случае в среднем нужно проверить три пары битов.

ПРИМЕР 6. Обнаружение двух ошибок. В рассматриваемом примере возможны случаи когда:

1. Приняты две единицы, остальные нули.
2. Приняты четыре единицы, одна из которых находится не на своём месте.
3. Приняты шесть единиц.

В первом случае сразу по двум единицам определяем передаваемое кодовое слово.

Во втором случае имеем три верных (соответствуют одному передаваемому сообщению) и три неверных пары (соответствуют разным передаваемым сообщениям). Тогда достаточно найти две пары одного передаваемого сообщения.

Таблица 1 – Таблица шифрации

Передаваемое сообщение	Кодовое слово												
	Двоичный вид												
1	0	0	0	0	...	0	0	0	0	1	1	1	1
2	0	0	0	0	...	0	1	1	1	0	0	0	1
3	1	0	0	1	...	0	0	0	0	0	0	0	1
4	0	1	1	0	...	1	0	0	0	0	0	0	1
5	0	0	1	1	...	0	0	0	1	0	0	1	0
6	0	0	0	0	...	1	0	1	0	0	0	1	0
7	1	1	0	0	...	0	1	0	0	0	0	1	0
8	0	1	0	1	...	0	0	1	0	1	0	0	0
9	0	0	0	1	...	1	1	0	0	0	1	0	0
10	1	0	0	0	...	1	0	0	1	1	0	0	0
11	0	0	1	0	...	0	1	0	0	1	0	0	0
12	0	1	0	0	...	0	0	0	1	0	1	0	0
13	1	0	1	0	...	0	0	1	0	0	1	0	0
...
n	0	0	0	0	...	0	0	0	0	0	0	0	0

Таблица 2 – Таблица дешифрации

Биты	0	1	2	3	4	5	6	7	...	n
0	0	0	0	0	0	0	0	0	...	0
1	1	0	0	0	0	0	0	0	...	0
2	1	1	0	0	0	0	0	0	...	0
3	1	1	1	0	0	0	0	0	...	0
4	2	5	12	10	0	0	0	0	...	0
5	2	6	13	8	2	0	0	0	...	0
6	2	7	9	11	2	2	0	0	...	0
7	4	6	9	10	10	6	9	0	...	0
8	3	6	12	11	12	6	11	6	...	0
9	3	5	9	8	5	8	9	9	...	0
10	4	5	13	11	5	13	11	4	...	0
11	4	7	12	8	12	8	7	4	...	0
12	3	7	13	10	10	13	7	10	...	0
...	0
n	0	0	0	0	0	0	0	0	...	0

Для нахождения двух пар из одного передаваемого сообщения надо проверить минимум две и максимум пять пар. Подсчитаем, сколько в среднем нужно проверить пар битов. Пусть x случайная величина – количество проверяемых пар, p – вероятности значений x . Значения p_i найдём по формуле $p_i = \frac{C_3^1 \cdot C_3^{i-2}}{C_6^{i-1}} \cdot \frac{2}{6-i+1}$. Имеем закон распределения этой случайной величины:

x_i	2	3	4	5
p_i	0,2	0,3	0,3	0,2

Математическое ожидание $mx = 3,5$. Следовательно, в этом случае в среднем нужно проверить 3 – 4 пар битов.

В третьем случае имеем шесть верных (соответствуют одному передаваемому сообщению) и девять неверных пар (соответствуют разным передаваемым сообщениям). Для нахождения двух пар из одного передаваемого сообщения надо проверить минимум две и максимум 11 пар.

Подсчитаем, сколько в среднем пар битов в этом случае надо проверить. Аналогично предыдущему, закон распределения для этой случайной величины:

x_i	2	3	4	5	6	7	8	9	10	11
p_i	0,142857	0,197802	0,197802	0,167832	0,125874	0,083916	0,048951	0,023976	0,008991	0,001998

Математическое ожидание $mx = 4,57$. Следовательно, в третьем случае в среднем нужно проверить четыре – пять пар битов.

ЗАКЛЮЧЕНИЕ

В заключение отметим следующее. Основным результатом работы является разработка универсального рекурсивного метода построения кодов большой длины на основе штейнеровых систем для криптосистем с коррекцией ошибок. Такие коды обладают максимальной мощностью и максимальной корректирующей способностью среди кодов с заданным числом единиц в кодовом слове. Доказан ряд свойств таких кодов, не описанных ранее в литературе. Построена криптосистема с простыми алгоритмами кодирования и декодирования и возможностью смены кода одной подстановкой.

ЛИТЕРАТУРА

1. Мак-Вильямс Ф.Д. Теория кодов, исправляющих ошибки / Ф.Д. Мак-Вильямс, Н.А. Слоэн. – М.: Связь, 1979. – 744 с.
2. Блейхут Р. Теория и практика кодов, контролируемых ошибки / Блейхут Р. – М.: Мир, 1986. – 576 с.
3. Берлекэмп Э. Алгебраическая теория кодирования / Берлекэмп Э. – М.: Мир, 1971. – 480 с.
4. David J.C. Information Theory, Inference, and Learning Algorithms / J.C. David, МакКай. – Cambridge University Press. – 2003.
5. Ткаченко В.Г. Перечисление типов монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2008. – № 2. – С. 54 – 69.
6. Ткаченко В.Г. Построение корректирующего кода для криптосистем на основе типов монотонных булевых функций / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2010. – № 1. – С. 85 – 92.
7. Ткаченко В.Г. Построение криптосистемы на основе треугольных кодов / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2012. – № 1. – С. 72 – 82.
8. Tkachenco V.G. Construction of cryptosystem on the basis quadrangular codes / Tkachenco V.G., Sinyavsky O.V. // Nauka i Studia. Przemysł. – 2013. – Т. 35 (103). – С. 18-28.
9. Tkachenco V.G. Construction of Cryptosystem on the Basis of Triangular Codes/ V.G. Tkachenco, O.V. Sinyavsky // Computer Science and Information Technology. – Horizon Research Publishing Corporation (HRPUB) – Alhambra, California. USA, 2014. – V.2, №7. – P. 300 – 307.
10. Холл М. Комбинаторика / Холл М. – М.: Мир, 1970. – 424 с.
11. Камерон П. Теория графов, теория кодирования и блок-схемы / П. Камерон, Дж. ван Линт. – М.: Наука, 1980. – 144 с.
12. Картеси Ф. Введение в конечные геометрии / Ф. Картеси. – М.: Наука, 1980. – 320 с.

REFERENCES

1. F.J. MacWilliams, N.J.A. Sloane. The theory of error-correcting codes, North-Holland Publishing Company, Amsterdam, 1977, 744.
2. R.E. Blahut. Theory and practice of error control codes, Addison-Wesley Publishing Company, London, 1983, 576.
3. E.R. Berlekamp. Algebraic coding theory, McGraw-Hill Book Company 1968, 480.
4. J.C. David, MacKay. Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003.
5. Tkachenco V.G. Enumeration monotonous Boolean function types upon synthesis digital circuits, Research works of ONAT n.a. O.S. Popov, №2, 54 – 69, 2008.
6. Tkachenco V.G., Sinyavsky O.V. Construction of error correcting code for cryptosystems on the basis of types monotonous Boolean functions, Research works of ONAT n.a. O.S. Popov, №1, 85 – 92, 2010.
7. Tkachenco V.G., Sinyavsky O.V. Construction of cryptosystem on the basis of triangular codes, Research works of ONAT n.a. O.S. Popov, №1, 72 – 82, 2012.
8. Tkachenco V.G., Sinyavsky O.V. Construction of cryptosystem on the basis quadrangular codes, Nauka i Studia. Przemysł, 35 (103), 18–28, 2013.
9. Tkachenco V.G., Sinyavsky O.V. Construction of Cryptosystem on the Basis of Triangular Codes, Computer Science and Information Technology. – Horizon Research Publishing Corporation (HRPUB) – Alhambra, California. USA, 2014. – V.2, №7. – P. 300 – 307.
10. Marshall Hall, Jr. Combinatorial theory, Blaisdell Publishing Company, Waltham (Massachusetts), 1967, 424.
11. P.J. Cameron, J.H. van Lint. Graph Theory and Block Designs, Cambridge University Press, 1975, 144.
12. F. Karteszi. Introduction to Finite Geometries, Akademiai Kiado, Budapest, 1976, 320.