

ПОМЕХОУСТОЙЧИВАЯ ПЕРЕДАЧА ИНФОРМАЦИИ НА ОСНОВЕ МНОГОЗНАЧНЫХ БИНОМИАЛЬНЫХ КОДОВ

А. А. Борисенко, д-р техн. наук, профессор;
Т. А. Протасова, ст. преподаватель;
Е. А. Протасова, аспирант;
О. В. Бережная, канд. техн. наук, доцент,
Сумский государственный университет,
ул. Римского-Корсакова, 2, г. Сумы, 40007, Украина

В статье рассматривается применение многозначных биномиальных чисел в качестве помехоустойчивого кода. Рассматриваются методы обнаружения ошибок на их основе. Дана оценка помехоустойчивости.

Ключевые слова: *многозначные биномиальные коды, криптография, биномиальная система счисления, диапазон многозначных биномиальных чисел, универсальное множество.*

Обеспечение повышенной помехоустойчивости при передаче информации в настоящее время остается актуальной задачей. На сегодня известно достаточно большое количество различных помехоустойчивых кодов, среди которых выделяются коды с обнаружением ошибок, применяемые в системах передачи данных с переспросом, которые на сегодня довольно широко распространены. Используемые в них коды хотя и обладают достаточной помехоустойчивостью, однако в ряде случаев имеют повышенную сложность кодирования и декодирования кодовых комбинаций, особенно при обнаружении в них пакетов ошибок. Как следствие, реализация кодирующих и декодирующих устройств в системах передачи информации приводит к повышенным аппаратным затратам, а сами устройства, при этом, часто не обладают возможностью самоконтроля, и поэтому могут стать источником дополнительных ошибок.

Эти недостатки можно устранить, используя многозначные биномиальные коды, важным достоинством которых при помехоустойчивой передаче информации является простота алгоритмов обнаружения ошибок, а также возможность самоконтроля кодирующих и декодирующих устройств.

В данной работе рассматривается многозначная l -ичная [1] биномиальная система счисления, которая характеризуется тем, что:

- а) ее диапазон и весовые значения разрядов задаются биномиальными коэффициентами;
- б) максимальное число разрядов в биномиальных числах равно k ;
- в) количество r информационных разрядов для различных биномиальных чисел является переменным;
- г) алфавит используемых цифр с учетом нуля содержит $m \cdot k$ цифр, где m -параметр системы счисления, влияющий на ее диапазон;
- д) вес разряда зависит от его местоположения в числе, стоящей в нем цифры и предшествующих цифр;
- е) содержит контрольное число $l = m \cdot k$, превышение которого в биномиальном числе приводит к появлению в нем ошибки.

Помехоустойчивый биномиальный код, применяемый в системах обработки информации, строится на основе следующей числовой функции:

$$F^l = \sum_{i=0}^{X_1-1} C_{mi-1, X_{r-0}}^{k1} + \sum_{i=0}^{X_2-1} C_{mi-2, X_{r-0}-X_{r-1}}^{k2} + \dots + \sum_{i=0}^{X_j-1} C_{mi-j, q_j}^{kj} + \dots + \sum_{i=0}^{X_r-1} C_{mi-r, q_r}^{kr} = \sum_{j=0}^{k-1} A_j. \quad (1)$$

Многочленная l -ичная биномиальная система счисления характеризуется наличием в ней параметров m и k , которые задают диапазон многозначных биномиальных чисел, образующих биномиальный код:

$$C_m^k = \frac{m!}{k!(m-k)!}. \quad (2)$$

При этом параметр k определяет количество разрядов чисел многозначного биномиального кода, а параметр m вместе с k задает контрольное число $l = m - k$, превышение которого суммой цифр многозначного биномиального числа свидетельствует об ошибке [1, 2].

Алгоритм перебора многозначных биномиальных чисел имеет следующие шаги. Из [2, 3] следует, что многозначные биномиальные числа получаются на основе условия, что сумма цифр в биномиальном числе будет меньше или равной контрольному числу $l = m - k$. Тогда, очевидно, что первое многозначное биномиальное число, состоящее из нулей, всегда отвечает этому условию, так как сумма нулей в нем равна 0. Если контрольное число l равно 0, то на этом процесс перебора биномиальных чисел заканчивается. Если же l не равно 0, то второе число получается добавлением в младший разряд биномиального числа единицы. Если после этого сумма цифр в нем не стала равной l , то в младший разряд снова добавляется единица, и так идет до тех пор, пока не будет получена в младшем разряде цифра равная контрольному числу. По приходе следующей единицы младший разряд обнуляется, а в соседний старший разряд заносится единица. Если после этого сумма единиц в числе не стала равняться l , то снова происходит добавление 1 в младший разряд и цикл повторяется до тех пор, пока во втором разряде не будет получено контрольное число. Затем происходит перенос единицы в соседний старший разряд и так идет счет далее до появления числа l в старшем разряде биномиального числа, что соответствует признаку окончания процедуры счета. В этом случае будут перебраны все C_m^k многозначных биномиальных чисел для данных параметров m и k . Если же в процессе счета появится суммарное число во всех разрядах счетчика большее l , то это значит, что произошла ошибка и процесс счета следует прекратить.

Процесс преобразования может быть проиллюстрирован блок-схемой алгоритма, приведенной на рисунке 1.

Например, контрольным числом l для значений параметров $k = 3$ и $m = 5$ будет число 2. При этом диапазон соответствующих многозначных биномиальных чисел будет равен

$$C_5^3 = \frac{5!}{3!2!} = 10.$$

В него входят числа 000 001 002 010 011 020 100 101 110 200. В этих числах используются только цифры 0, 1, 2, сумма значений которых в многозначных биномиальных числах не должна превышать контрольное число 2. Его превышение означает, что произошла ошибка.

Многозначные биномиальные цифры могут быть представлены двоичными числами с разрядностью, равной округленному до целой величины логарифму от числа $l + 1$. В примере – это будет два разряда,

кодирующие цифры 0, 1, 2 – 00, 01, 10. Ошибка при передаче информации может произойти как в нескольких, так и во всех разрядах двоичного числа, кодирующего биномиальные цифры. Независимо от этого при превышении суммой цифр биномиального числа контрольного числа ошибка в нем будет обнаружена, в том числе и при наличии пакетов ошибок, что является одним из достоинств данного метода помехоустойчивого кодирования.

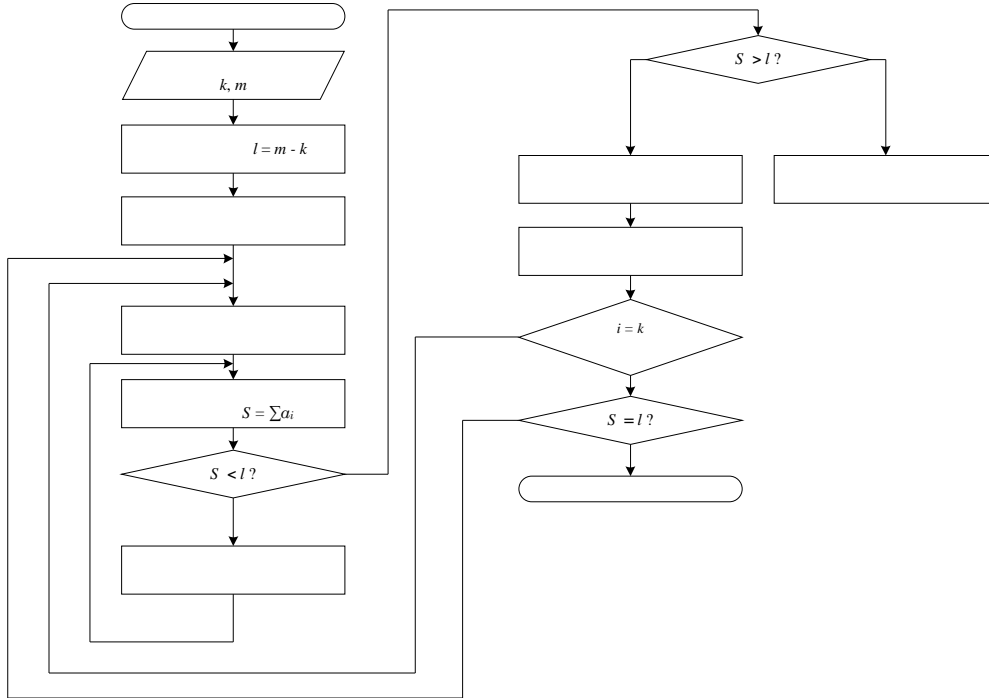


Рисунок 1 – Блок-схема алгоритма перебора многозначных биномиальных чисел

Многозначные биномиальные числа образуют подмножество C_m^k разрешенных чисел из их универсального множества, содержащего $(l+1)^k$ чисел, а разность $(l+1)^k - C_m^k$ образуют подмножество запрещенных чисел. Очевидно, что

$$(l+1)^k = (m-k+1)^k \geq C_m^k. \quad (3)$$

Для приведенного выше примера с $k = 3$ и $m = 5$ запрещенные комбинации, которые являются ошибочными, приведены в таблице 1. Их число, очевидно, должно равняться разности между 27 и 10, то есть 17. Появление любого из этих чисел вместо многозначного биномиального числа говорит об ошибке.

Таблица 1 – Запрещенные комбинации для параметров $k = 3$ и $m = 5$

012	120	211
021	121	212
022	122	220
102	201	221
111	202	222
112	210	

Алгоритм обнаружения ошибок в биномиальных кодовых комбинациях содержит следующие шаги:

1. Подсчитывается сумма цифр S в биномиальном многозначном числе и сравнивается с контрольным числом $l = m - k$.
 2. Если S больше l , то в многозначном биномиальном числе произошла ошибка.
 3. Останов счета.
 4. Если S меньше или равно l , то процесс счета продолжается.
- Блок-схема алгоритма обнаружения ошибок в многозначных биномиальных числах приведена на рисунке 2.

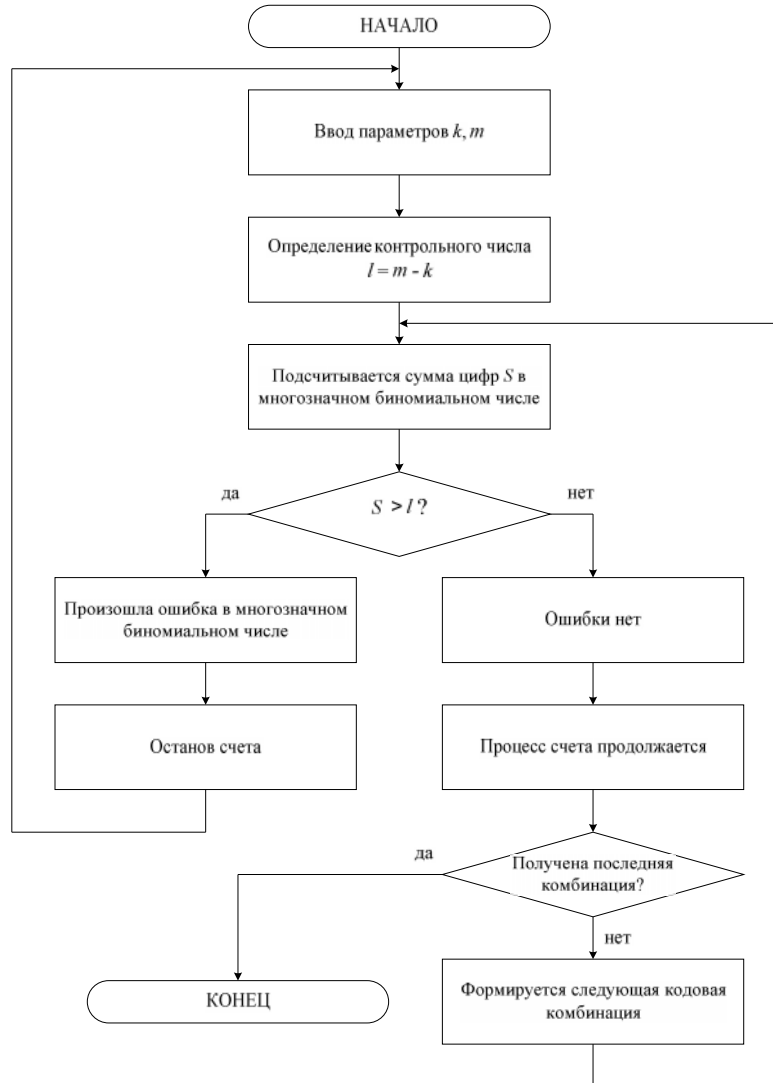


Рисунок 2 – Блок-схема алгоритма обнаружения ошибок в многозначных биномиальных числах

Так как формула, определяющая диапазон разрешенных многозначных биномиальных слов, обладает свойством симметрии,

$$C_m^k = C_7^5 = C_7^2 = \frac{m!}{k!(m-k)!} = 21.$$

то для одинакового значения сочетаний могут быть сформированы различные биномиальные слова, например, приведенные в таблице 2.

Таблица 2 – Разрешенные биномиальные комбинации для параметров $m = 7, k = 5, l = 2$ и $k = 2, l = 5$ соответственно

$m = 7, k = 5, l = 2$			$m = 7, k = 2, l = 5$		
00000	00101	02000	00	11	23
00001	00110	10000	01	12	30
00002	00200	10001	02	13	31
00010	01000	10010	03	14	32
00011	01001	10100	04	20	40
00020	01010	11000	05	21	41
00100	01100	20000	10	22	50

На рисунке 3 приведены графики значений диапазонов для различных параметров m в зависимости от разрядности биномиального числа k .

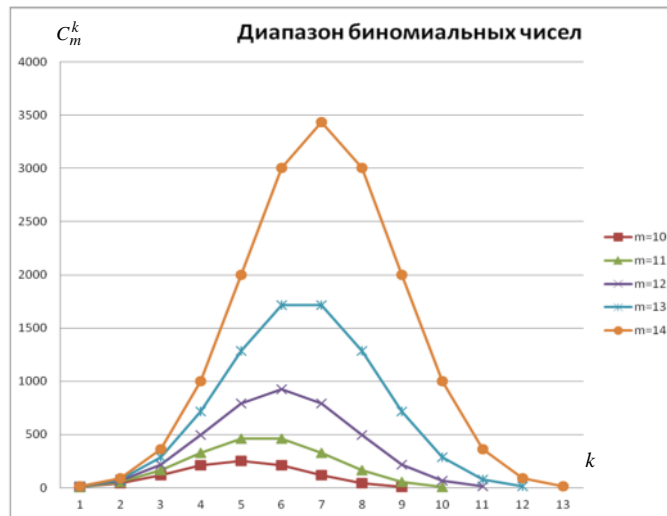


Рисунок 3 – График значений диапазонов для различных параметров m в зависимости от разрядности биномиального числа k

На рисунке 4 приведены графики значений диапазонов для различных k в зависимости от параметра биномиальной системы счисления m .

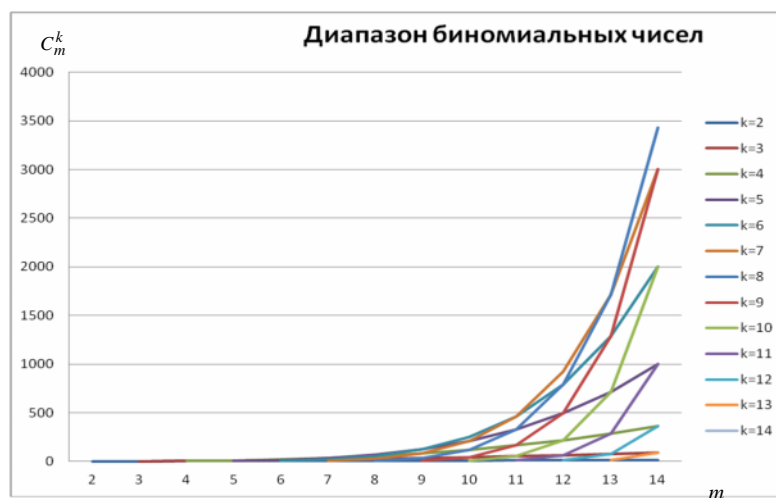


Рисунок 4 – График значений диапазонов для различных k в зависимости от параметра биномиальной системы счисления m

Диапазон биномиальных чисел влияет на степень обнаружения ошибок. Доля обнаруживаемых ошибок определяется по формуле [3]:

$$P = 1 - \frac{N_p}{N} = \frac{C_m^k}{(l+1)^k}, \quad (4)$$

где N_p – количество разрешенных комбинаций, N – количество возможных комбинаций.

На рисунке 5 приведены графики вероятностей обнаруживаемых ошибок в зависимости от длины чисел k для разных значений контрольного числа l . Как видим из графиков, при увеличении контрольного числа k вероятность ошибочных переходов, которые будут обнаружены, стремятся к единице.

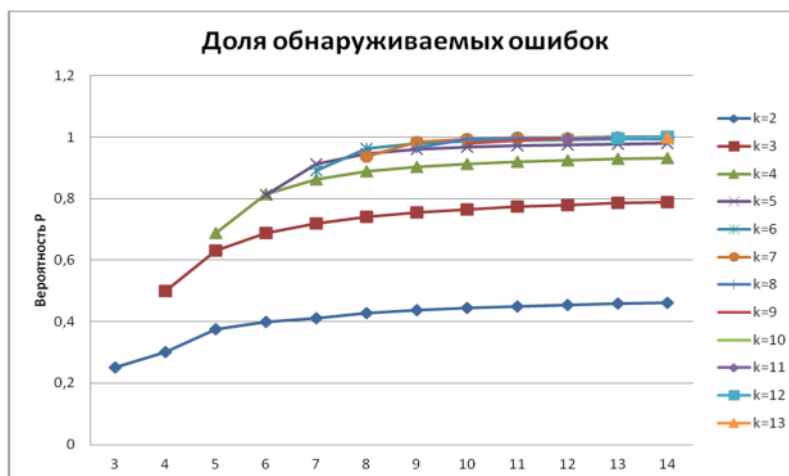


Рисунок 5 – Доля обнаруживаемых ошибок

ВЫВОДЫ

Таким образом применение биномиальных многозначных чисел позволяет с помощью простого алгоритма, использующего суммирование цифр этих чисел, эффективно обнаруживать одиночные ошибки и их пакеты. При этом с ростом длины биномиальных комбинаций эффективность помехоустойчивого кодирования увеличивается и в пределе вероятность обнаружения ошибок стремится к 1.

Работа выполнена в рамках бюджетной темы № 0113U000133.

SUMMARY

ANTI-JAMMING TRANSMISSION OF INFORMATION BASED ON MULTIVALUED BINOMIAL CODES

A. A. Borysenko, T. A. Protasova, E. A. Protasova, O. V. Berezhnaya,
Sumy State University,
2, Rymsky-Korsakov Str., 40007, Sumy, Ukraine

In the article the authors discuss the use of multivalued binomial numbers as error-correcting code, the methods of their formation and detection of errors in them and present the evaluation of noise immunity.

Keywords: multi-valued binomial codes, cryptography, binomial number system, a range of multi-valued binomial numbers, universal set.

РЕЗЮМЕ

ЗАВАДОСТІЙКА ПЕРЕДАЧА ІНФОРМАЦІЇ НА ОСНОВІ БАГАТОЗНАЧНИХ БІНОМІАЛЬНИХ КОДІВ

*О. А. Борисенко, Т. О. Протасова, К. О. Протасова, О. В. Бережна,
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007, Україна*

У статті розглядається застосування багатозначних біноміальних чисел в якості завадостійкого коду. Розглядаються методи виявлення помилок на їх основі. Дана оцінка завадостійкості.

Ключові слова: багатозначні біноміальні коди, криптографія, біноміальна система числення, діапазон біноміальних чисел, універсальна множина.

СПИСОК ЛІТЕРАТУРИ

1. Борисенко А. А. Системы счисления с биномиальным основанием / А. А. Борисенко, Е. Л. Онанченко, А. Н. Кобяков // Вестник СумГУ. – 1994. - №1. – С. 96-101.
2. Борисенко А. А. Биномиальный счет и счетчики: монография. – Сумы: СумГУ, 2008. – 152 с.
3. Кодирование информации. Двоичные коды: справочник/под ред. Н.Т. Березюка. – Х. : Вища шк..., Изд-во при Харьк. ун-те, 1978. – 252 с.

Поступила в редакцию 6 ноября 2013 г.