# Захист інформації

УДК 004.056.4

А.А. Борисенко, А.Е. Горячев

*Сумский государственный университет, Сумы*

## ИСПРАВЛЕНИЕ ОШИБОК В ПЕРЕСТАНОВКАХ

*В работе исследуются помехоустойчивые коды на перестановках с целью применения их для достоверной передачи и хранения информации. Предлагаются методы обнаружения и исправления ошибок в перестановках, использующие их структурную избыточность. Исправление ошибок с помощью этих методов осуществляется на стороне приемника и не требует повторной передачи ошибочных элементов перестановок.*

***Ключевые слова:*** *перестановки, помехоустойчивые коды, обнаружение ошибок, исправление ошибок.*

### Введение

С ростом объёмов информации, передаваемой в телекоммуникационных сетях, важной задачей является обеспечение ее высокой помехозащищенности. Одним из подходов к решению такой задачи является применение помехоустойчивых кодов, которые могут обнаруживать и при необходимости исправлять ошибки. Важным требованием к ним является простота, которая позволяет упростить кодирующие и декодирующие устройства, увеличив при этом скорость преобразования обычных кодов в помехоустойчивые коды и обратно. Самыми простыми помехоустойчивыми кодами являются коды со сложением по модулю два. Они широко используются в сетях передачи данных для защиты от ошибок, а также при аппаратной реализации цифровых устройств. Однако явный недостаток этих кодов – небольшая глубина контроля, не всегда дает возможность эффективного их применения. В настоящее время разработано много других помехоустойчивых кодов, которые в той или иной мере удовлетворяют современным требованиям к ним, таким как умеренная избыточность информации и возможность выявления и исправления с их помощью как одиночных, так и пакетов ошибок [1 – 6].

Среди этих кодов особенно выделяются систематические коды, а среди них – групповые коды [1 – 6]. Они обладают повышенной помехозащищенностью и не только способны обнаруживать ошибки, а при необходимости и исправлять их, причем как одиночные ошибки, так и их пакеты. Эти коды в значительной мере рассчитаны на аппаратную реализацию, что позволяет поднять быстродействие операций кодирования и декодирования защищаемых массивов информации, хотя вполне эффективно их можно применять и при программной реализации.

К недостаткам этих кодов можно отнести то, что они до получения всего массива информации не могут обнаружить или исправить ошибку. В этом отношении более перспективными являются, например, сверточные коды, которые способны исправлять ошибки в процессе передачи массива информации. Однако их главный недостаток – большая избыточность информации, что значительно снижает скорость передачи сообщений [2]. Также их алгоритмы кодирования и декодирования достаточно сложны для практической реализации.

На практике также используются неразделимые коды, в комбинациях которых отсутствует деление на информационную и контрольную часть. Примером таких кодов являются равновесные коды, в которых признаком правильности комбинации является равенство числа единиц в ней некоторому заданному числу [1, 4]. Главным достоинством этих кодов является простота их алгоритмов кодирования и декодирования и возможность адаптации к параметрам помех. Их недостаток – отсутствие возможности исправления ошибок и необходимость дополнительного преобразования исходных массивов информации в равновесные коды и обратно.

К неразделимым кодам относятся также коды, основанные на простейших комбинаторных комбинациях – перестановках, размещениях, сочетаниях. Это, например, сменно посылочные коды или сменно качественные коды [4]. В данной работе исследуются неразделимые коды на перестановках, с целью передачи на их основе сообщений с повышенной достоверностью в системах телекоммуникации.

**Постановка задачи.** Перестановками называют соединения (последовательности, слова, комбинации), получаемые расположением $n$ разных элементов в различном порядке. Так, например, последовательность различных элементов *abc*, состоящая из трех различных элементов, в соответствии с вышеприведенным определением, будет являться перестановкой. Множество, состоящее из перестановок *abc, acb, bac, bca, cab, cba*, образует код на перестановках.

Множество перестановок длины $n$, в которых каждому элементу присвоен определённый номер от 0 до $n$-1, назовем числовым кодом на перестановках. Например, последовательность элементов длины $n = 3$, состоящая из трех цифр «0 1 2», в соответствии с определением, будет являться перестановкой числового

кода. Перестановками числового кода, при их длине $n = 3$, будут комбинации 012, 021, 102, 120, 201, 210.

Код на перестановках, в котором каждый элемент представлен в двоичном виде, назовем двоичным кодом на перестановках, а соответствующие перестановки – двоичными перестановками. Ими будут для $n = 3$ следующие комбинации: 00 01 10, 00 10 01, 01 10 00, 01 00 10, 10 01 00, 10 00 01.

Перестановки широко применяются в различных науках, таких, например, как комбинаторная математика, абстрактная алгебра, криптография [6 – 8]. Однако до настоящего времени для повышения достоверности передачи данных применялись они не часто, невзирая на простоту обнаружения и исправления с их помощью ошибок. Это объясняется тем, что при малой длине перестановок они имеют большую относительную избыточность информации и поэтому проигрывают другим помехоустойчивым кодам в скорости передачи информации. Получить же большую длину перестановок, при которой они превосходили бы по эффективности известные помехоустойчивые коды, раньше было затруднительно, так как не были известны достаточно простые методы преобразования исходных массивов информации в перестановки и обратно. В настоящее время имеется решение этой задачи, заключающееся в применении факториальной системы счисления [9]. Переход от массивов информации к факториальным числам, которые близки по своей структуре к перестановкам, является промежуточным шагом при преобразовании массивов информации в перестановки. При этом наряду с повышением достоверности передаваемой информации решается еще и задача скрытности передачи информации, что на сегодня является важной задачей. Существенно также и то, что эти две задачи решаются по сути одним и тем же методом [10, 11].

Применение перестановок для повышения достоверности передачи данных требует разработки новых эффективных методов обнаружения и исправления ошибок в перестановках, что является задачей данной статьи.

## Методы исправления ошибок

**1. Метод контрольных сумм с индикацией ошибочных элементов.**

Метод предназначен для обнаружения и исправления пакетов ошибок в отдельных элементах перестановки. Суть метода основывается на том факте, что если один из элементов перестановки ошибочен и имеется индикатор, который указывает на этот элемент, то его можно вычислить, найдя разность между контрольной суммой и суммой всех элементов перестановки за исключением ошибочного. После этого необходимо заменить элемент с ошибкой на вычисленный элемент. Однако при использовании данного метода появляется необходимость индикации ошибочного элемента, так как контрольная сумма дает информацию только о том, что в переданной перестановке имеется ошибка. Для такой индикации необходимо в каждый двоичный номер элемента перестановки ввести дополнительные избыточные разряды и произвести контроль этих номеров на наличие в них ошибки с помощью какого-либо известного кода. Например, таким кодом может быть контроль чётности или код Хэмминга.

Достоинством данного метода исправления ошибок является его простота и то, что он может исправлять пакеты ошибок в количестве, равном приведенному к целой величине двоичному логарифму, взятому от длины перестановки $n$. К недостаткам метода следует отнести необходимость дополнительного избыточного искусственного кодирования элементов массива, что увеличивает не только время кодирования, а и время передачи информации, и возможность исправления ошибки только в одном двоичном номере элемента перестановки. Очевидно, что количество дополнительных бит, вводимых искусственно в перестановку, будет равно $n$, и с ростом ее длины оно линейно увеличивается. Так для перестановки с 1024 элементами количество искусственно вводимых дополнительных бит равно 1024, что составляет 10 процентов от общего количества информации, передаваемой перестановкой, что по сравнению с большинством используемых на практике кодов вполне экономично. Для сравнения, сверточные коды используют искусственную избыточность в размере 50% от величины передаваемой информации, то есть в 5 раз больше [2].

*Пример.* В процессе передачи перестановки произошла ошибка и на приемном конце была получена комбинация 41022. Причем дополнительное кодирование показало, что ошибочной будет последняя двойка. Необходимо восстановить ошибочный элемент. Заранее известно, что контрольная сумма равна 10. Из этой контрольной суммы вычитаем сумму первых четырех элементов, то есть 7. Результат 10 – 7 = 3. Значит, правильная перестановка будет 41023. При этом максимальная длина пакета исправляемых двоичных ошибок равна 3.

**2. Метод перекрестного контроля элементов перестановок.**

Исправляет одиночные ошибки в одном из элементов перестановки и обнаруживает пакеты ошибок в них с возможностью их дальнейшего переспроса. Данный метод является улучшенным аналогом хорошо известного и проверенного на практике итеративного кода [1, 3]. Его достоинство – высокое быстродействие процессов кодирования и декодирования, простота их реализации как аппаратным, так и программным способом и относительно небольшая избыточность информации, особенно при больших длинах перестановок (10 – 15%).

В предлагаемом методе находится контрольная сумма элементов перестановки по модулю два. Так как для разных перестановок определенной длины $n$ она одна и та же, то она предварительно не формируется каждый раз перед передачей, как это происходит в итеративном коде и, соответственно, не передается по каналу связи на приемный конец. Кон-

трольная сумма в предлагаемом методе получается один раз на приемном конце канала связи и при передаче разных перестановок не изменяется.

Наряду с используемой в методе контрольной суммой в каждый элемент перестановки вводится операция сложения по модулю два, что приводит к появлению в них дополнительных контрольных разрядов. В результате получается код, в котором не может быть двух одинаковых строк. Ошибка в нем находится и исправляется также как и в итеративном коде на пересечении искаженной строки и столбца.

*Пример.* При передаче перестановки на приемном конце была получена последовательность двоичных комбинаций, представляющих ее элементы, показанная на рис. 1, а в виде таблицы. Проверка контрольных сумм по ее строкам и столбцам показала, что в переданной перестановке, состоящей из двоичных элементов, произошла ошибка, которая представлена 1 на пересечении третьей строки и третьего столбца. Чтобы исправить ошибку, надо эту 1 преобразовать в 0. В результате исправления ошибки будет получена перестановка, показанная на рис. 1, б.

а)

| Σ | 1 | 0 | 0 |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |

б)

| Σ | 1 | 0 | 0 |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |

Рис. 1. Исправление ошибки методом перекрестного контроля

Достоинством метода перекрестного контроля элементов перестановок является простота его использования даже по сравнению с итеративным кодом, так как не требуется формирования контрольных сумм по столбцам и их передача, что повышает скорость передачи и уменьшает количество возможных ошибок. Также данный код за счет отсутствия одинаковых строк (элементов) повышает достоверность передачи информации в асимметричных каналах связи.

## Выводы

Коды на перестановках обладают простыми методами обнаружения и исправления ошибок, как одиночных, так и их пакетов, и при большой длине перестановок содержат в себе относительно небольшую избыточность информации, что приводит к росту скорости их передачи и числа обнаруживаемых и исправляемых ошибок. Основной недостаток кодов на перестановках, сложность получения перестановок большой длины, устраняется с помощью факториальной системы счисления, которые позволяют относительно просто преобразовывать исходные сообщения в перестановки и обратно – перестановки в исходные сообщения. Большая длина перестановок и при этом небольшая избыточность передаваемой информации позволяет эффективно защищать ее не только от помех, а и от несанкционированного доступа, что дает возможность одновременно реализовывать защиту информации от помех и осуществлять скрытность ее передачи.

## Список литературы


*1. Березюк Н.Т. Кодирование информации (двоичные коды) / Н.Т. Березюк, А.Г. Андрущенко, С.С. Мощицкий и др. – Х.: Вища школа, 1978. – 252 с.*

*2. Чернега В. Компьютерные сети: уч. пос. / В. Чернега, Б. Платтнер. – Изд-во СевНТУ, 2006. – 500 с.*

*3. Кузьмин И.В. Основы теории информации и кодирования / И.В. Кузьмин, В.А. Кедрус. – К.: Вища шк., 1977. – 279 с.*

*4. Цымбал В.П. Теория информации и кодирования / В.П. Цымбал. – К.: Вища школа, 1977. – 288 с.*

*5. Жураковський Ю.Л. Теорія інформації та кодування: підручник / Ю.Л. Жураковський, В.П. Полторак. – К.: Вища шк., 2001. – 332 с.*

*6. Амелькин В.А. Методы нумерационного кодирования / В.А. Амелькин. – Н.: Наука, 1986. – 155 с.*

*7. Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика: пер. с англ. / Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М.: Мир, 1980. – 476 с.*

*8. Кнут Д. Искусство программирования, т. 1. Основные алгоритмы / Д. Кнут. – М.: Вильямс, 2000. – 720 с.*

*9. Борисенко А.А. Электронная система генерации перестановок на базе факториальных чисел / А.А. Борисенко, И.А. Кулик, А.Е. Горячев // Вісник СумДУ. Технічні науки. – 2007. – № 1. – С. 183-188.*

*10. Generation of Permutations Based Upon Factorial Numbers / A.A. Borisenko, V.V. Kalashnikov, I.A. Kulik, A.E. Goryachev // Eighth International Conf. on Intelligent Systems Design and Applications. – Kaohiung, Taiwan. – 2008. – P. 57-61.*

*11. Горячев А.Е. Обнаружение ошибок в перестановках / А.Е. Горячев // Вісник СумДУ. Технічні науки. – 2009. – №3. – С. 169-174.*


*Поступила в редколлегию 6.02.2013*

**Рецензент:** д-р техн. наук, проф. С.И. Приходько, Украинская государственная академия железнодорожного транспорта, Харьков.

### МЕТОДИ ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК В ПЕРЕСТАНОВКАХ

О.А. Борисенко, О.Є. Горячев

*У роботі досліджуються завадостійкі коди на перестановках з метою застосування їх для достовірної передачі та зберігання інформації. Пропонуються методи виявлення та виправлення помилок в перестановках, що використовують їх структурну надмірність. Виправлення помилок за допомогою цих методів не вимагає повторної передачі помилкових елементів перестановок.*

***Ключові слова:*** *перестановки, завадостійкі коди, виявлення помилок, виправлення помилок.*

### METHODS OF ERROR DETECTION AND CORRECTION IN PERMUTATIONS

A.A. Borisenko, A.E. Goryachev

*In the paper we study the noise-resistant codes on permutations in order to use them for reliable information transfer and storage. Methods for detecting and correcting errors in permutations, using their structural redundancy, are proposed. Correction of errors with these methods does not require re-transmission of erroneous permutation elements.*

***Keywords:*** *permutations, noise-resistant codes, error detection, error correction.*