УДК 681.3.06

ПЕРЕСТАНОВКИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

А. А. Борисенко, *д-р техн. наук, профессор,*
А. Е. Горячев, *ассистент;*
Б. К. Лопатченко, *канд. техн. наук, доцент,*
О. М. Кобяков, *канд. техн. наук, доцент,*
Сумский государственный университет,
ул. Римского-Корсакова, 2, г. Сумы, 40007, Украина
E-mail: alevgor@gmail.com

Одним из подходов к решению задачи повышения достоверности передачи информации является применение помехоустойчивых кодов. К ним относятся коды, использующие в своей основе перестановки. В статье рассматриваются основные свойства перестановок, которые могут применяться для решения задач повышения достоверности передачи данных в телекоммуникационных сетях.

Ключевые слова: *перестановки, достоверность передачи информации, свойства перестановок, избыточность*

ВВЕДЕНИЕ

С ростом объёмов информации, передаваемых в телекоммуникационных сетях, важной задачей является обеспечение ее высокой достоверности. Одним из подходов к решению такой задачи является применение помехоустойчивых кодов, которые могут обнаруживать и при необходимости исправлять ошибки. Все помехоустойчивые коды являются подмножествами некоего множества, которое является *универсальным множеством или универсальным кодом*. Важным требованием к помехоустойчивым кодам является простота их алгоритмов кодирования и декодирования, что позволяет строить соответствующих устройства с повышенной скоростью их получения. К кодам с простыми алгоритмами кодирования и декодирования относятся рассматриваемые в статье коды, использующие в своей основе перестановки.

Перестановками называют соединения, получаемые расположением n разных элементов в различном порядке [1, 2].

Так, например, последовательность элементов *abc*, состоящая из трех различных элементов, в соответствии с вышеприведенным определением, будет являться перестановкой.

Множество перестановок и операции над ними образует *код на перестановках*. Например, множество, состоящее из перестановок *abc*, *acb*, *bac*, *bca*, *cab*, *cba*, образует код на перестановках.

Множество перестановок длины n, в которых каждому их элементу присвоен определённый номер от 0 до n-1, назовем *числовым кодом на перестановках*. Например, последовательность элементов длины $n = 3$, состоящая из трех цифр 012, в соответствии с определением 2, будет являться перестановкой числового кода. Перестановками числового кода, при их длине $n = 3$, будут также комбинации 021, 102, 120, 201, 210. В дальнейшем, если не будет специально оговорено, под кодом на перестановках будет пониматься их числовой код, в котором числа будут представляться в виде номеров.

Код на перестановках, в которых каждый элемент представлен в двоичном виде, назовем *двоичным кодом на перестановках*, а соответствующие перестановки – *двоичными перестановками*. Ими,

например, будут для $n = 3$ комбинации 00 01 10, 00 10 01, 01 00 10, 01 10 00, 10 00 01, 10 01 00.

ПОСТАНОВКА ЗАДАЧИ

Перестановки широко применяются в различных науках, таких, например, как комбинаторная математика, абстрактная алгебра, криптография и для решения специальных задач [2–5]. Однако применение перестановок для повышения достоверности передачи данных на практике встречается редко, так как получение перестановок большой длины требует довольно сложных алгоритмов преобразования, а при малой длине они содержат относительно большую избыточность и поэтому обладают невысокой скоростью передачи информации. Получить же большую длину перестановок, при которой они превосходили бы по эффективности известные помехоустойчивые коды, до настоящего времени было затруднительно, так как не были известны достаточно простые методы преобразования исходных массивов информации в перестановки и обратно. В настоящее время предлагается решение этой задачи путем применения факториальной системы счисления [6, 7]. При этом наряду с повышением достоверности передаваемой информации в этом случае решается еще и задача скрытности передачи информации, что на сегодня является также важной задачей [8–11]. Существенно, также и то, что эти две задачи решаются по сути одним и тем же методом.

Однако применение перестановок в задачах передачи информации в телекоммуникационных сетях требует предварительного всестороннего исследования их свойств. В данной статье как раз и решается эта задача.

ИССЛЕДОВАНИЕ ОСНОВНЫХ СВОЙСТВ ПЕРЕСТАНОВОК

В основе изучаемых в работах [12, 13] методов обнаружения и исправления ошибок в перестановках, используемых в телекоммуникационных системах, лежат следующие их свойства:

Свойство 1. Число перестановок длины n в их коде равно $n! = 1\times2...\times n$ (n факториал) [1–4].

Пример. Дана перестановка 4 1 3 0 2 . Ее длина равна 5. Тогда число перестановок в коде, к которому принадлежит данная перестановка, будет равно 5! = 120.

Для n, изменяющегося от 1 до 10, значения факториалов приведены в таблице 1. Как видим, они быстро нарастают с увеличением n.

Таблица 1 – значения количества перестановок в коде в зависимости от n

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5040	40320	362880	3628800

Свойство 2. Сумма номеров элементов перестановки длины n

$$S = \frac{n \cdot (n-1)}{2}. \qquad (1)$$

Следует из того, что по определению любая перестановка содержит элементы с номерами от 0 до n-1, взятые в разном порядке. Отсюда, сумма номеров всех элементов будет равняться $0 + 1 + ... + n\text{-}1$, что, как известно, равно $n\cdot(n\text{-}1)/2$ [1].

Пример. Дана перестановка 4 1 3 0 2 длины 5. Тогда сумма её элементов S согласно формуле (1) $S = 5 \cdot (5-1)/2 = 10$. Действительно, просуммировав элементы перестановки, получим тот же результат: $4 + 1 + 3 + 0 + 2 = 10$.

В табл. 2 показана зависимость суммы номеров элементов перестановок S от значения n. Графически данные таблицы 2 представлены на рис. 1.

Таблица 2 –Суммы номеров элементов перестановок в зависимости от n

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	1	3	6	10	15	21	28	36	45	55	66	78	91	105

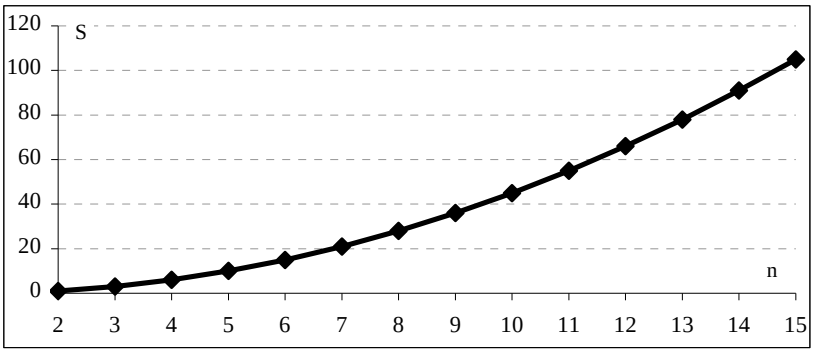

Рисунок 1 - График зависимости суммы номеров элементов перестановок S от длины перестановок n

Свойство 3. Среди номеров перестановки не может быть два таких p_j и p_i, ($j, i = 0,1, \ldots n\text{-}1, j \neq i$), что $p_j = p_i$.

Следует из определения перестановки, в которой не могут быть два или больше одинаковых элемента.

Пример. Комбинация, состоящая из 4 номеров, 1 0 2 2 не является перестановкой, так как значения двух последних элементов в ней (2 2) являются одинаковыми.

Свойство 4. Минимальное количество информации, требуемое для кодирования перестановки, равно $\log_2 n!$ бит.

Следует из того, что число всех перестановок в их коде равно $n!$ и соответственно, чтобы идентифицировать перестановку требуется $\log_2 n!$ бит информации. Можно также исходить и из того, что выбор первого элемента перестановки потребует число $\log_2 n$ бит информации, второго $\log_2(n-1)$ и, наконец, последнего $\log_2 1 = 0$. Произведя суммирование количеств информации по всем разрядам, получим требуемое значение – $\log_2 n!$.

Пример. Допустим, что дана двоичная перестановка, содержащая 4 элементы – 0 1 2 3. Тогда количество информации, содержащейся в ней, очевидно, будет $\log_2 4 + \log_2 3 + \log_2 2 + \log_2 1 = \log_2 4 \cdot 3 \cdot 2 \cdot 1$ бит.

Свойство 5. Количество информации, требуемое для кодирования перестановки в универсальном коде, равно $n \cdot \log_2 n$.

Вытекает из того, что перестановки входят в универсальное множество, состоящее из Z = n^n комбинаций. Применительно к нему получим требуемый результат, логарифмируя Z. Можно исходить и из рассуждения, что каждый элемент перестановки требует для своей идентификации максимально $\log_2 n$ бит. Тогда умножив число элементов n на $\log_2 n$, получим необходимый результат.

Пример. Дана перестановка, состоящая из 4 элементов – 0 1 2 3. Количество информации необходимое для ее представления в универсальном коде равно $n \cdot \log_2 n = 4 \log_2 4$ бит.

Свойство 6. Абсолютная избыточность информации в элементах перестановок изменяется от

$i_0 = \log_2 n - \log_2 n = 0$ бит для первого элемента,

$i_1 = \log_2 n - \log_2 (n-1)$ бит для второго элемента

до значения

$i_n = \log_2 n - \log_2 1 = \log_2 n$ бит для последнего n-го элемента.

Данное свойство вытекает из того, что первый элемент выбирается из n элементов, второй из n-1 и т. д., до n - го элемента, который остается один.

Пример. Изменение величины абсолютной избыточности i для каждого элемента перестановки p_j (j = 1, 2, ... 16), при их числе n = 16, показано в табл. 3 и на графике рис. 2.

Таблица 3 –значения избыточности элементов перестановок при длине перестановок n = 16

p_j	1	2	3	4	5	6	7	8
i	0	0,093	0,193	0,3	0,415	0,541	0,678	0,83

p_j	9	10	11	12	13	14	15	16
i	1	1,193	1,415	1,678	2	2,415	3	4

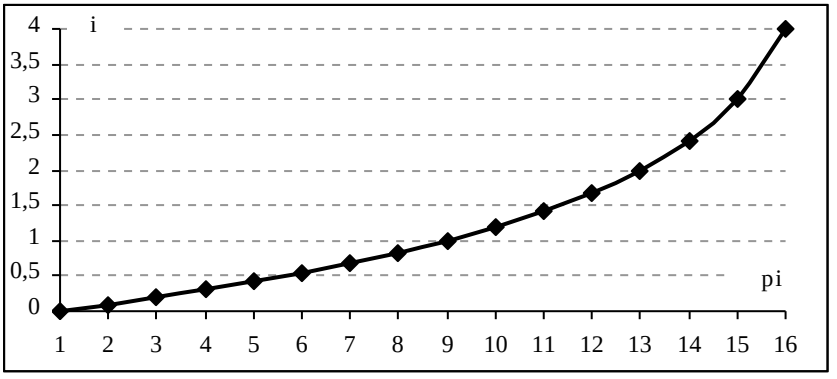

Рисунок 2 - График изменения абсолютной избыточности i для каждого элемента перестановки при длине перестановок n = 16

Свойство 7. Величина абсолютной избыточности, содержащейся в перестановках, равна

$$I = n \cdot \log_2 n - \log_2 n! \text{ бит.} \qquad (2)$$

Пример. Изменение величины абсолютной избыточности I для перестановок с изменением их длины n, показано в табл. 4 и на графике рис. 3.

Таблица 4 – значения абсолютной избыточности перестановок различной длины

n	2	3	4	5	6	7	8	9
I	1	2,170	3,415	4,703	6,018	7,352	8,701	10,06

n	10	11	12	13	14	15	16
I	11,428	12,803	14,184	15,570	16,96	18,353	19,75

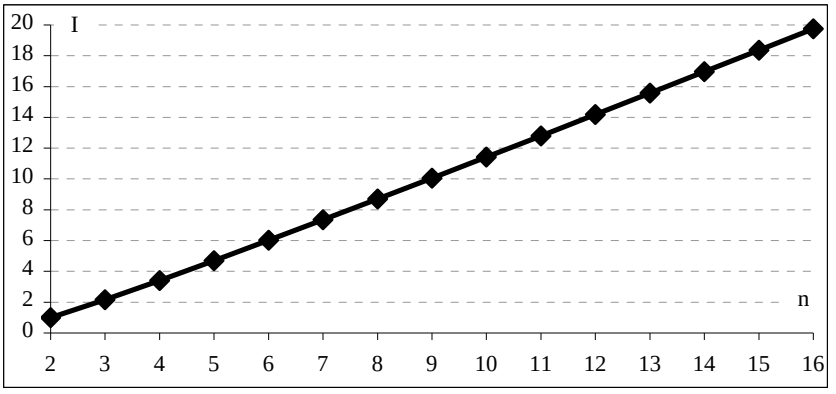

Рисунок 3 - График изменения абсолютной избыточности перестановок I в зависимости от длины перестановок n

Свойство 8. Элементы перестановки длины n, представленные в двоичном коде, по отношению к универсальному коду содержат избыточную информацию

$$I_d = n \cdot \left\lceil \log_2 n \right\rceil - n \cdot \log_2 n \,. \qquad (3)$$

Пример. Дана перестановка, состоящая из 5 элементов – 01234. При представлении каждого из них в двоичном коде будет получена двоичная перестановка 000 001 010 011 100, содержащая избыточность информации по отношению к универсальному коду

$$I_d = n \cdot \left\lceil \log_2 n \right\rceil - n \cdot \log_2 n = 5 \log_2 8 - 5 \log_2 5 \text{ бит.}$$

В табл. 5 и на графике рис. 4 показан пример изменения величины избыточности двоичных перестановок по отношению к перестановкам универсального кода.

Таблица 5 – значения избыточности двоичных перестановок относительно универсального кода

n	2	3	4	5	6	7	8	9
I_b	0,000	1,245	0,000	3,390	2,490	1,349	0,000	7,471

n	10	11	12	13	14	15	16
I_b	6,781	5,946	4,980	3,894	2,697	1,397	0,000

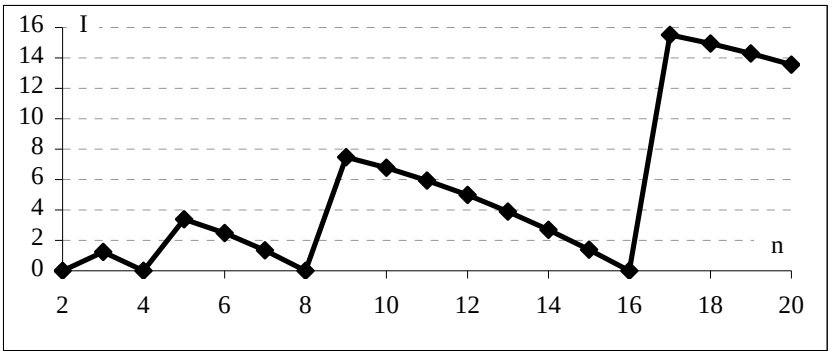

Рисунок 4 - График зависимости избыточности двоичных перестановок относительно перестановок универсального кода

Свойство 9. Значение абсолютной избыточности двоичных перестановок по отношению к перестановкам с минимальной избыточностью

$$I_{\Sigma} = n \cdot \left\lceil \log_2 n \right\rceil - \log_2 n! . \qquad (4)$$

В табл. 6 показано изменение абсолютной избыточности двоичных перестановок в зависимости от их длин n.

Таблица 6 – значения абсолютной избыточности двоичного представления перестановок в зависимости от длины перестановок n

n	2	3	4	5	6	7	8	9
I_{Σ}	1	3,415	3,415	8,093	8,508	8,701	8,701	17,531

n	10	11	12	13	14	15	16
I_{Σ}	18,209	18,750	19,165	19,464	19,657	19,750	19,750

На графике рис. 5 показано изменение I_{Σ}, I_b, I в зависимости от длины перестановок n.

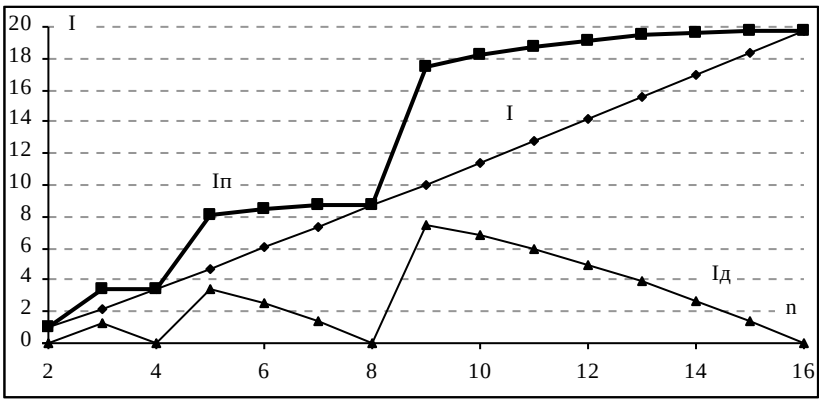

Рисунок 5 - График изменения избыточности перестановок

Свойство 10. При длине перестановок n, кратной степени двойки, любой из элементов двоичной перестановки может быть получен путём сложения по модулю два значений разрядов остальных её n-1 элементов.

Пример. Для двоичной перестановки длины $n = 2^3 = 8$ известны значения 7 элементов: 000 111 001 011 010 100 101. Определить значение недостающего элемента этой перестановки можно, просуммировав по модулю два 7 известных значения ее двоичных элементов: $000 \oplus 111 \oplus 001 \oplus 011 \oplus 010 \oplus 100 \oplus 101 = 110$. В результате получим значение неизвестного 8 элемента $110_{<2>} = 6_{<10>}$.

ВЫВОДЫ

Таким образом, имеется 10 свойств перестановок, которые могут быть использованы для повышения достоверности передачи информации в телекоммуникационных системах.

ПЕРЕСТАНОВКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

О. А. Борисенко, О. Є. Горячев, Б. К. Лопатченко, О. М. Кобяков,
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007, Україна,
E-mail: alevgor@gmail.com

Одним з підходів до вирішення завдання підвищення достовірності передачі інформації є застосування завадостійких кодів. До них відносять коди, що використовують у своїй основі перестановки. У статті розглядаються властивості перестановок, які можуть бути використані для підвищення достовірності передачі інформації в телекомунікаційних системах.

Ключові слова: перестановки, достовірність передачі інформації, властивості перестановок, надмірність.

PERMUTATIONS IN TELECOMMUNICATION NETWORKS

A. A. Borisenko, A. E. Goryachev, B. K. Lopatchenko, O. M. Kobyakov,
Sumy State University,
2, Rimsky-Korsakov Str., 40007 Sumy, Ukraine
E-mail: alevgor@gmail.com

One of the approaches to solving the problem of increasing the reliability of data transmission is the use of error-correcting codes. These are codes based on permutations. The article deals with the properties of permutations that can be used to improve the reliability of data transmission in telecommunication systems.

Key words: permutations, reliability of data transmission, properties of permutations, redundancy.

СПИСОК ЛИТЕРАТУРЫ

1. Андерсон Дж. Дискретная математика и комбинаторика / Дж. Андерсон. – М.: Вильямс, 2006. – 960 с
2. Кнут Д. Искусство программирования. Том 1. Основные алгоритмы, 3-е изд. : уч. пос. / Д. Кнут. – М. : Изд. дом «Вильямс». – 2000. – 720 с.
3. Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М. : Мир, 1980. – 476 с.
4. Липский В. Комбинаторика для программиста / В. Липский. – М. : Мир, 1988. – 213 с.
5. Борисенко А. А. Подход к решению задачи коммивояжёра на основе факториальных чисел / А. А. Борисенко, А. Е. Горячев // Актуальні проблеми економіки. – 2009. – № 10 (100). – С. 150 – 154.
6. Борисенко А. А. Электронная система генерации перестановок на базе факториальных чисел / А. А. Борисенко, И. А.Кулик, А. Е. Горячев // Вісник СумДУ. Серія Технічні науки. – 2007. – № 1. – С. 183 – 188.
7. Borisenko A. A. Generation of Permutations Based Upon Factorial Numbers / A. A. Borisenko, V. V. Kalashnikov, I. A. Kulik, A. E. Goryachev // Eighth International Conference on Intelligent Systems Design and Applications. – Kaohiung, Taiwan, 2008. – P. 57 – 61.
8. Мартин Д. Системный анализ передачи данных / Д. Мартин. – М. : Мир, 1975. – Т. 1.– 256 с.
9. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2001. – 672 с.
10. Таненбаум Э. Компьютерные сети. 4-е изд. / Э. Таненбаум. – СПб.: Питер, 2009. – 992 с.
11. Чернега В. Компьютерные сети : учеб. пособие / В. Чернега, Б. Платтнер. – Изд-во СевНТУ, 2006. – 500 с.
12. Горячев А. Е. Обнаружение ошибок в перестановках / А. Е. Горячев // Вісник СумДУ. Серія Технічні науки. – 2009. – № 3. – С.169. – 174.
13. Борисенко А. А. Обнаружение и исправление ошибок в перестановках / А. А. Борисенко, А. Е. Горячев, Е. Л. Онанченко // Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерна інженерія". Вінниця, 19-21 травня 2010. – ВНТУ, 2010. – С. 348-350.

Поступила в редакцию 20 марта 2013 г.