УДК 681.3.06

Борисенко А. А., профессор кафедры электроники и компьютерной техники Сумского государственного университета

Горячев А. Е., инженер кафедры электроники и компьютерной техники Сумского государственного университета

ОБНАРУЖЕНИЕ ОШИБОК НА ОСНОВЕ ПЕРЕСТАНОВОК

В статье рассматриваются два способа обнаружения ошибок в перестановках, и производится оценка их эффективности. Перестановки представляются в форме итеративного кода, выгодно отличающегося от обычного представления.

Ключевые слова: перестановки, обнаружение ошибок, кодовое расстояние, доля обнаруживаемых ошибок

Borisenko A.A., professor of Electronics and Computers Department, Sumy State University

Goryachev A.E., Engineer of Electronics and Computers Department, Sumy State University

ERROR DETECTION BASED ON PERMUTATIONS

The article discusses two ways of errors detection in permutations, and their effectiveness is evaluated. The permutations are presented in the form of an iterative code which benefits comparing to the ordinary concept.

Keywords: permutations, error detection, code distance, detected errors percentage

ВВЕДЕНИЕ

Сегодня, как никогда, в связи с широким распространением телекоммуникационных систем стоит задача дальнейшего повышения помехоустойчивости передачи и хранения информации. Существующие методы в большинстве случаев достаточно эффективно справляются с этой задачей. Однако дальнейший рост требований к помехоустойчивости приводит к необходимости поиска новых методов, которые бы повышали помехоустойчивость передаваемых и хранимых сообщений. При этом они должны минимально снижать скорость передачи информации и приводить к простым методам ее кодирования и декодирования.

В работах [1 – 3] для помехоустойчивой передачи и хранения информации предлагается использовать коды на основе перестановок, представляющие собой последовательностей различных элементов, являющиеся по своей природе неразделимыми кодами [4]. Как известно, число возможных перестановок из числа n элементов, представляющего их

длину, равно $n! = 1 \cdot 2, \ldots, n$. Например, число перестановок длины $n = 5$ будет равно $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. В данной работе предполагается, что элементы перестановок кодированы положительными целыми числами, начиная с нуля, – 0, 1, 2, …, n-1. Такое кодирование перестановок будем называть *простейшим*, а соответствующий код *простейшим* кодом. Так как этот код формируется с помощью натурального ряда чисел с нулем в его начале, то в нем всегда найдется два элемента, отличающиеся между собой на 1. Например, одной из 120 перестановок простейшего кода длины $n = 5$ будет последовательность чисел 1 0 4 2 3. В ней для каждого элемента найдется еще один элемент, отличающийся от него на 1. Однако ничто не мешает произвести и более сложное кодирование элементов перестановок, например, четными целыми положительными числами. Количество возможных перестановок в этом случае остается прежним – $n!$. Тогда представленная выше перестановка простейшего кода 1 0 4 2 3 будет иметь вид 2 0 8 4 6.

На практике элементы перестановок удобно представлять в двоичной форме. Такое их представление будет называться *двоично-кодированным*. Тогда перестановка 1 0 4 2 3 в двоично-кодированной форме будет иметь вид: 010 000 100 010 011. Хотя возможно и троично-кодированное, и десятично-кодированное представление, и многие другие способы представления элементов перестановок.

Число двоичных разрядов в двоично-кодированных элементах перестановок определяется как целый логарифм от числа элементов n:

$$m = \lceil \log_2 n \rceil. \qquad (1)$$

В приведенном выше примере 1 0 4 2 3 перестановка использует только 5 из 8 возможных двоичных комбинаций из трех разрядов, остальные комбинации 101, 110, 111 не используются. В дальнейшем для помехоустойчивого кодирования, с целью его упрощения и уменьшения избыточности информации, будут использоваться только перестановки, содержащие число элементов равное степени двойки, то есть 2, 4, 8, 16, …, 2^n. Такое кодирование перестановок будет называться *полным*.

Так как все перестановки содержат одни и те же элементы, только заданные в различном порядке, то сумма двоичных чисел, кодирующих элементы перестановок, должна оставаться постоянной, образуя собой контрольную сумму, одинаковую для всех перестановок, равную

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

Ее можно использовать для выявления ошибочных комбинаций среди правильных перестановок. Для приведенного выше примера перестановки 1 0 4 2 3, такая контрольная сумма равна $5 \cdot (5\text{-}1)/2 = 10$. И как бы мы не

переставляли элементы данной перестановки, их сумма не изменится и останется равной 10.

Очевидно, что появление в перестановке, в процессе ее передачи или хранения, двух и более одинаковых элементов, преобразует ее в ошибочную перестановку – запрещенную последовательность элементов, не являющуюся перестановкой. Тогда сравнивая на приемном конце элементы передаваемых последовательностей между собой можно установить, являются ли они перестановками или нет. И первое, и второе рассмотренное свойство перестановок можно использовать для разработки соответствующих методов контроля ошибок передаваемых сообщений и тем самым повысить помехоустойчивость передачи и хранения информации в телекоммуникационных системах [3].

Но кроме указанных свойств перестановки обладают и другими полезными свойствами, позволяющими выявлять в них ошибки. Изучение таких свойств и реализация на их основе методов контроля ошибок и является основной задачей данной работы.

АНАЛИЗ ОШИБКООБНАРУЖИВАЮЩИХ СВОЙСТВ ПЕРЕСТАНОВОК

Зададим с помощью таблицы 1 пример из трех простейших перестановок, представленных в виде трех таблиц. В первой таблице в первой колонке слева представлена перестановка 0 1 2 3 4 5 6 7 в соседней таблице перестановка в аналогичной колонке 1 0 3 2 5 4 7 6 и в соответствующем колонке, следующей за ней таблицы, перестановка 7 6 5 4 3 2 1 0. Последняя третья колонка справа, состоящая из трех столбцов, в каждой из указанных таблиц отображает соответствующую двоично-кодированную форму простейших перестановок. Все эти формы являются полными, так как содержат все 8 возможных комбинаций из 3 разрядов.

Таблица 1 – Варианты перестановок

0	0	000
1	1	001
2	1	010
3	0	011
4	1	100
5	0	101
6	0	110
7	1	111

1	1	001
0	0	000
3	0	011
2	1	010
5	0	101
4	1	100
7	1	111
6	0	110

7	1	111
6	0	110
5	0	101
4	1	100
3	0	011
2	1	010
1	1	001
0	0	000

Подобных перестановок и соответствующих им таблиц можно записать 8! = 40320. Соответственно, каждая из этих перестановок, при их равновероятном генерировании, несет около 16 бит информации и соответственно ее можно использовать для передачи такого же количества

информации. Количество информации, содержащееся в каждой из данных перестановок, как это с очевидностью следует из табл. 1, равно 24 битам, что говорит о содержащейся в ней почти 30-процентной избыточной информации в количестве 8 бит, которая может быть использована для обнаружения ошибок. Эта избыточность, являющаяся абсолютной, с ростом длины перестановок увеличивается, но при этом относительная избыточность уменьшается и с неограниченным ростом n в пределе стремится к 0 [3]. Это значит, что при больших длинах перестановок реальная скорость передачи информации приближается к максимально возможной величине – энтропии источника информации. При этом количество ошибок, обнаруживаемых в перестановках, стремится к 100 процентам [3].

Терема 1. *Минимальное кодовое расстояние в числовом коде на перестановках равно* 2.

Доказательство. Очевидно, что переменой мест двух элементов любой перестановки можно получить новую перестановку. Среди всех возможных элементов простейшей числовой перестановки, в силу ее определения, обязательно найдутся два элемента, которые отличаются на 1 и, при этом, ничто не мешает получить перестановкой этих элементов новую перестановку. В результате будут получены две перестановки, кодовое расстояние между которыми будет равно 2, так как каждому из двух элементов одной перестановки в противопоставляемой ей другой перестановке будет соответствовать элемент, отличающийся от него на 1. Так как остальные противостоящие элементы будут одинаковыми, то весовая разница между ними будет равняться 0.

Очевидно, что таких пар перестановок с кодовым расстоянием равным 1 можно получить столько, сколько имеется пар элементов, отличающихся друг от друга на 1. Другие пары перестановок, кроме рассмотренных выше пар, в противостоящих элементах должны будут иметь весовую разницу большую 1 и поэтому кодовое расстояние у них будет больше 2. Значит, минимальное кодовое расстояние для кода на перестановках будет равно 2. **Теорема доказана**.

ОБНАРУЖЕНИЕ ОШИБОК В ПЕРЕСТАНОВКАХ ПО МОДУЛЮ 2

Обнаружение ошибок в двоично-кодированных столбцах полных перестановок возможно на основе того, что сумма единиц и нулей в них всегда одинакова и равна $n/2$. Поэтому сложение по модулю 2 по столбцам на четность дает для любых двоично-кодированных полных перестановок один и тот же результат – 0 (см. табл. 1). Это значит, что при передаче информации в перестановку не нужно добавлять избыточный разряд, содержащий информацию о результате сложения двоичных значений

разрядов по модулю 2 в соответствующем столбце, и в результате отпадает необходимость в кодирующей программе или устройстве. Тем самым ускоряется как процесс кодирования информации, так и процесс ее передачи. Кроме того, вероятность ошибки в передаваемом или хранимом сообщении, хотя и незначительно, но уменьшается за счет отсутствия необходимости передачи контрольного разряда, который тоже может исказиться в процессе передачи. Важно также и то для рассматриваемого метода кодирования перестановок, что после обнаружения ошибки в одном или двух столбцах двоично-кодированной перестановки надо переспрашивать не всю двоично-кодированную перестановку, а только отдельные ее двоичные столбцы, что значительно повышает скорость передачи информации.

Ошибочными переходами комбинаций, стоящих в столбцах, при сложении по модулю 2 на четность могут быть только переходы в двоичные комбинации с нечетным числом 1, 3, …, n-1 единиц. Число таких комбинаций, будет равно сумме биномиальных коэффициентов $C_n^1 + C_n^3 + ... + C_n^{n-1}$. Поэтому доля обнаруживаемых ошибочных переходов двоичных комбинаций, стоящих в столбцах перестановок, по отношению к общему числу комбинаций 2^n

$$D_o = \frac{C_n^1 + C_n^3 + ... + C_n^{n-1}}{2^n}. \qquad (3)$$

Количество не обнаруживаемых ошибочных переходов, с учетом правильно переданной комбинации, в столбце перестановки определяется суммой $C_n^0 + C_n^2 + ... + C_n^n$ биномиальными коэффициентов, задающих числа переходов двоичных комбинаций в столбцах в двоичные комбинации с четным числом единиц 0, 2, …, n. Поэтому доля не обнаруживаемых ошибочных переходов, без учета правильно переданной комбинации, взятая по отношению к общему числу возможных переходов двоичных комбинаций в столбцах 2^n,

$$D_н = \frac{C_n^0 + C_n^2 + ... + C_n^n - 1}{2^n}. \qquad (4)$$

В сумме биномиальные коэффициенты для нечетных и четных ошибочных переходов дадут число комбинаций равное величине 2^n - 1. Поэтому

$$D_o = 1 - D_н - \frac{1}{2^n}. \quad (5)$$

Критерий оценки помехоустойчивости кодов в виде доли обнаруживаемых ошибочных переходов широко используется в соответствующей литературе, например, в [5]. Его несомненное достоинство – простота. Однако он не учитывает реальных вероятностей переходов единиц в нули и обратно нулей в единицы в кодовых комбинациях под воздействием помех непосредственно в системах связи. Но оценка по доли обнаруживаемых переходов дает возможность сравнивать между собой помехоустойчивые коды по числу запрещенных и разрешенных состояний безотносительно к выбранному каналу связи. Такую возможность следует рассматривать как достоинство данного критерия.

ВЫЯВЛЕНИЕ ОШИБОК В ПЕРАСТАНОВКАХ НА ОСНОВЕ РАВНОВЕСНОГО ДЕКОДИРОВАНИЯ ИХ СТОЛБЦОВ

Указанные выше достоинства метода помехоустойчивого кодирования на основе сложения по модулю 2 для обнаружения ошибок в перестановках делает его применение из-за простоты и высокой скорости декодирования в ряде случаев достаточно эффективным. Однако обнаружение им только ошибок нечетной кратности заставляет искать и применять на практике другие более сложные методы обнаружения ошибок в перестановках.

В этом плане следует обратить внимание на то, что каждый столбец любой полной двоично-кодированной перестановки содержит кодовую комбинацию, содержащую $n/2$ единиц и столько же нулей. Такой код относится к равновесным кодам, содержащих в своих кодовых комбинациях постоянное число единиц. Этот код обнаруживает ошибки любой кратности за исключением комбинаций, содержащих $n/2$ единиц, получаемых из исходной двоичной комбинации с четным числом единиц путем взаимных переходов нулей в единицы и обратно.

Количество запрещенных кодовых комбинаций в равновесном коде с четным числом единиц определяется суммой биномиальных коэффициентов

$$C_n^0 + C_n^2 + \ldots + C_n^{(n/2)-1} + C_n^{(n/2)+1} + \ldots + C_n^n = \\ = 2^n - C_n^{n/2}. \quad (8)$$

Тогда доля обнаруживаемых ошибочных переходов определится как

$$D_o = 1 - \frac{C_n^{n/2}}{2^n}. \quad (9)$$

Соответственно доля не обнаруживаемых ошибочных переходов двоичных комбинаций в столбцах полных перестановках

$$D_н = \frac{C_n^{n/2} - 1}{2^n}. \qquad (10)$$

При этом скорость передачи информации остается такой же, как и при кодировании по модулю 2, так как какие-либо дополнительные избыточные разряды в столбцах перестановок отсутствуют. Важно также и то, что равновесные коды дают повышенный эффект по количеству обнаруживаемых ошибок в ассиметричных каналах связи, которые являются такими в большинстве практических применений. В ряде случаев при сильно выраженной асимметрии помех они могут обнаруживать практически все возникающие ошибки. Это возможно в некоторых радиоканалах, где наблюдаются, например, только ошибочные переходы 1 в 0 или 0 в 1 [6]. Недостаток равновесных кодов по сравнению с кодами по модулю 2 – это увеличенная сложность алгоритма обнаружения ошибок, требующего подсчета числа единиц в двоичной кодовой комбинации.

ПОЛУЧЕНИЕ ПЕРЕСТАНОВОК

Как видим, использование перестановок для помехоустойчивого кодирования может оказаться вполне эффективным. Однако возникает задача получения перестановок. Есть несколько путей ее решения. Перестановки после предварительного получения хранят в памяти, извлекают оттуда и при необходимости передают приемнику. Этот путь вполне подходит для различных систем автоматики. Другой путь – это получение перестановок в реальном масштабе времени, путем преобразования их из обычных двоичных кодов специальными методами [7]. Авторы для этой цели усовершенствовали метод преобразования, использующий факториальную систему счисления [1 – 3].

ВЫВОДЫ

Таким образом, в данной работе предложены два метода эффективного обнаружения ошибок на основе перестановок.

При этом метод сложения по модулю 2 позволяет более просто и с большим быстродействием реализовывать декодирующие устройства, чем метод равновесного декодирования столбцов. Однако он хуже работает в асимметричных каналах связи и позволяет обнаруживать только нечетное количество ошибок.

В отличие от него метод равновесного декодирования столбцов перестановок обнаруживает четные и нечетные числа ошибок любой

кратности и эффективно работает в ассиметричных каналах связи. В нем не обнаруживаются только взаимные переходы единиц в нули и нулей в единицы.

ЛИТЕРАТУРА

1. 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.
2. Борисенко А.А. Электронна система генерації перестановок на базі факторіальних чисел / А.А. Борисенко, И.А. Кулик, А.Е. Горячев // Вісник СумДУ. Технічні науки. – 2007. – №1. – с. 183 – 188.
3. Борисенко А.А. Завадостійка передача економічної інформації на базі перестановок / А.А. Борисенко, А.Е. Горячев // Актуальні проблеми економіки. – 2013. – №3(141). – с. 156 – 163.
4. Тутевич В.Н. Телемеханика. 2-е изд / В. Н. Тутевич – М.: Высшая школа, 1985 – 423 с.
5. Березюк Н.Т. Кодирование информации (двоичные коды) / Н.Т. Березюк, А.Г. Андрущенко, С.С. Мощицкий и др. – Харьков: Вища школа, – 1978. – 252с.
6. Статистика ошибок при передаче цифровой информации: Сборник статей / Перевод с англ. – М.: Мир, 1966. – 302с.
7. Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. Пер. с англ. – М.: Мир 1980. – 476 с.