УДК 681.3.06

ОБНАРУЖЕНИЕ ОШИБОК В ПЕРЕСТАНОВКАХ

А.Е. Горячев, *аспирант*
Сумский государственный университет, г. Сумы

В статье рассматриваются возможные ошибки, возникающие при передаче перестановок, а также способы их обнаружения и исправления. На основе предложенных методов разрабатываются алгоритмы обнаружения ошибок в перестановках, исследуются их быстродействие и надёжность.

Ключевые слова: *перестановки, помехоустойчивость, обнаружение ошибок, надёжные алгоритмы.*

При передачі перестановок по каналу зв'язку можливе виникнення неприпустимих помилок, отже, необхідно розробляти способи їх виявлення і виправлення. На основі запропонованих у статті методів виявлення помилок у перестановках розробляються відповідні алгоритми, досліджуються їх швидкодія та надійність.

Ключові слова: *перестановки, завадостійкість, виявлення помилок, надійні алгоритми.*

ПОСТАНОВКА ЗАДАЧИ

На практике широко используется такой комбинаторный объект, как перестановка. Перестановки используются для решения задач комбинаторной оптимизации, например, задачи поиска оптимального решения, а также при помехоустойчивой передаче данных и защите их от несанкционированного доступа [1]. Существует множество методов получения перестановок. Одним из таких методов является генерация перестановок на основе факториальных чисел [2]. В случае, когда после получения перестановки требуется её передача по каналу связи с шумом, при передаче могут возникнуть ошибки, и перестановка будет принята неверно. Это является неприемлемым, так как может привести к потере данных в устройствах защиты и передачи информации либо к ошибочным результатам при решении комбинаторных задач.

В данной работе ставится задача оценки помехоустойчивости перестановок, а также разработки методов, обеспечивающих обнаружение ошибок, возникающих при передаче перестановок по каналу связи с шумом и не требующих внесения дополнительной избыточности в передаваемые перестановки.

РЕШЕНИЕ ЗАДАЧИ

При передаче перестановки по каналу связи с шумом в общем случае могут возникнуть следующие ошибки: в одном из элементов:

1. Переход одного из элементов перестановки в другой разрешённый элемент.

Пример: Перестановка 145302 при передаче перешла в 345302. В конечной перестановке один из элементов «3» является ошибочным, так как не может повторяться в правильно записанной перестановке.

2. Переход одного из элементов перестановки в запрещённый элемент.

Пример: Перестановка 145302 при передаче перешла в 145702. Элемент конечной перестановки «7» является запрещённым, так как не удовлетворяет следующему условию: n-разрядная перестановка содержит элементы 0, 1, ..., n. В нашем случае $n = 6$, $7 > n$.

1. Ошибки, связанные с переходом одного из элементов перестановки в другой разрешённый элемент

Рассмотрим случай, когда при передаче перестановки возможно возникновение только ошибки первого вида с переходом одного разрешённого элемента в другой. Данный случай предполагает наименьшую (нулевую) избыточность кода, используемого при передаче элементов перестановки. В случае использования двоичного кода это является возможным, когда число элементов перестановки длины n будет равным 2^n. Число всех возможных комбинаций элементов перестановки на входе приёмника будет равняться числу размещений с повторениями из n по n элементов [3]:

$$N_O = n^n, \tag{1}$$

где n – число элементов (порядок) перестановки.

Число разрешённых комбинаций элементов – число перестановок длины n, определяется как

$$N_P = n!. \tag{2}$$

Следовательно, число запрещённых комбинаций будет равняться

$$N_З = N_O - N_P = n^n - n! \tag{3}$$

Ошибки, возникающие при передаче перестановки, могут быть обнаружены при переходе разрешённой комбинации в запрещённую комбинацию, то есть в комбинацию, не являющуюся перестановкой. При переходе одной разрешённой комбинации в другую разрешённую комбинацию ошибка может быть обнаружена только в случае использования дополнительных средств, повышающих помехоустойчивость передающихся данных.

Доля обнаруживаемых ошибочных комбинаций [3]:

$$Z = \frac{N_P \cdot N_З}{N_P \cdot N_O} = 1 - \frac{N_P}{N_O} = 1 - \frac{n!}{n^n}. \tag{4}$$

Из формулы (4) видно, что при увеличении порядка перестановки возрастает количество обнаруживаемых переходов и соответственно увеличивается доля обнаруживаемых ошибочных комбинаций. Это иллюстрирует таблица 1, в которой показаны значения параметра Z для перестановок различной длины. Данные таблицы 1 графически изображены на рисунке 1.

Таблица 1. Зависимость доли обнаруживаемых комбинаций Z от порядка перестановки n

n	2	3	4	5	6	7	8	9	10
Z	0,5	0,7778	0,9063	0,9616	0,9846	0,9939	0,9976	0,9991	0,9996

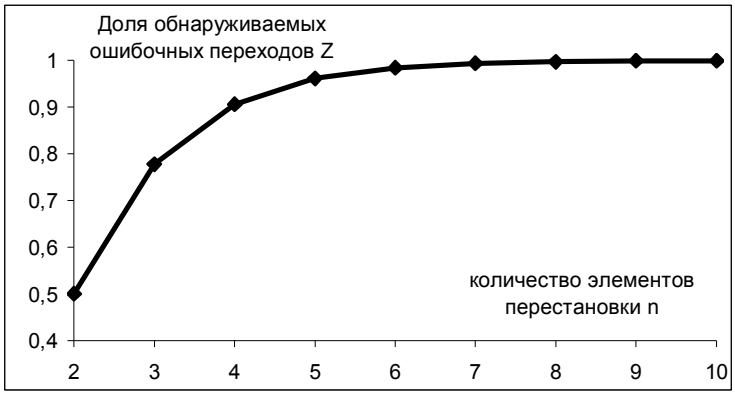

Рисунок 1 – Зависимость доли обнаруживаемых ошибочных комбинаций от порядка перестановки

2. Ошибки, связанные с переходом одного из элементов перестановки в запрещённый элемент

Частота возникновения ошибок с переходом элемента перестановки в запрещённый элемент зависит от отношения числа таких переходов и переходов одного из элементов перестановки в другой разрешённый элемент. Данное отношение, в свою очередь, определяется числом неиспользуемых для обозначения элементов перестановки двоичных комбинаций. Число запрещённых двоичных комбинаций можно определить из следующего соотношения:

$$n_З = 2^{\lceil \log_2 n \rceil} - n,$$

где n – порядок перестановки;

$\lceil \log_2 n \rceil$ – длина элемента перестановки в виде двоичного кода.

Из формулы видно, что наименьшее (нулевое) число переходов в запрещённый элемент для длины двоичного представления элемента перестановки i будет в случае, когда n будет равняться 2^i, наибольшее – при n, равном $2^{i-1}+1$.

При расчёте помехоустойчивости перестановки с учётом переходов в запрещённые комбинации необходимо в формулах (1-4) использовать не порядок перестановки, а количество всех возможных двоичных комбинаций, равное сумме n и $n_З$. Доля обнаруживаемых ошибочных комбинаций в этом случае

$$Z = 1 - \frac{(n+n_З)!}{(n+n_З)^{(n+n_З)}} = \frac{(2^{\lceil \log_2 n \rceil})!}{2^{\lceil \log_2 n \rceil \cdot 2^{\lceil \log_2 n \rceil}}}. \qquad (5)$$

В случае, когда $\lceil \log_2 n \rceil = \log_2 n$, формула (5) аналогична формуле (4).

3. Способы обнаружения ошибок при переходе одного из элементов перестановки в другой разрешённый элемент

1) Метод контроля суммы элементов перестановки на стороне приёмника.

Сумма всех элементов перестановки может быть вычислена в

соответствии со следующим выражением:

$$P = n + (n-1) + \ldots + 2 + 1 = \frac{n \cdot (n+1)}{2}. \qquad (6)$$

Пример: Найти сумму элементов 20-элементной перестановки.

Решение: Согласно формуле (6) сумма всех элементов перестановки будет равняться

$$P = 20 \cdot (20+1)/2 = 210.$$

Если сумма элементов перестановки после передачи не равна P, значит, произошла ошибка. В этом случае исправить ошибку можно с помощью повторной передачи всей перестановки.

Алгоритм работы метода контроля суммы элементов перестановки:

1. Установка начального значения суммы принятых элементов перестановки P_0 в ноль, установка контрольной суммы P в соответствии с формулой (6).
2. Приём элемента перестановки p_i.
3. Прибавление значения принятого элемента перестановки p_i к сумме P_0.
4. Проверка, был ли принят последний элемент перестановки. Если нет, то переход к п.2. Если да, то происходит сравнение значений суммы принятых элементов перестановки P_0 и контрольной суммы P.
5. Если $P_0 \neq P$, значит, обнаружена ошибка при передаче, происходит запрос на повторную передачу перестановки. Если $P_0 = P$, то перестановка принята верно, к источнику посылается сигнал успешного приёма.

Для проверки работы метода проводилось программное моделирование алгоритма его работы. При этом оценивалось быстродействие алгоритма, а также доля обнаруживаемых переходов в сравнении с расчётными значениями, которые приводились ранее в таблице 1.

В результате исследования доли обнаруживаемых ошибок при использовании метода контроля суммы элементов перестановки получены следующие данные (таблица 2):

Таблица 2 - Зависимость доли обнаруживаемых ошибочных комбинаций для метода контроля суммы элементов перестановки от числа элементов перестановки при разном количестве испытаний

Длина перестановки	Количество испытаний				
	10	100	1000	10000	100000
2	0,4	0,5	0,499	0,505	0,503
3	0,8	0,66	0,748	0,74	0,741
4	0,8	0,73	0,817	0,83	0,829
5	0,9	0,88	0,877	0,879	0,879
6	0,8	0,92	0,897	0,91	0,906
7	1	0,92	0,924	0,929	0,928
8	1	0,97	0,949	0,941	0,939
9	1	0,97	0,947	0,95	0,95
10	1	0,93	0,951	0,96	0,96

Из результатов исследований, приведенных в таблице 2, следует, что рассматриваемый метод позволяет выявлять не все возможные запрещённые комбинации. Это объясняется тем, что проверка суммы элементов перестановки, помимо переходов в разрешённые комбинации вида 12345 → 12354, не выявляет ошибки при переходах вида 12345 → 13344, так как в обоих случаях сумма элементов на выходе равна P.

В таблице 3 показана оценка быстродействия метода контроля суммы элементов в зависимости от длины перестановки и количества проверяемых перестановок.

Таблица 3 - Зависимость времени проверки перестановок на наличие ошибок методом контроля суммы элементов перестановки (в секундах) от числа элементов перестановки и количества проверяемых перестановок

Длина перестановки	Количество перестановок				
	200000	400000	600000	800000	1000000
100	0,77	1,48	2,36	3,08	3,85
200	1,54	3,02	4,56	5,93	7,58
300	2,2	4,51	6,92	9,23	11,48
400	3,08	6,15	9,23	12,31	15,33
500	3,85	7,69	11,43	15,44	19,18

Графически данные таблицы 3 показаны на рисунке 2. Анализируя полученные результаты, можно сделать вывод, что время, необходимое на проверку перестановок на наличие ошибок методом контроля суммы элементов перестановки, линейно зависит как от длины перестановки, так и от количества проверяемых перестановок. Метод показывает хорошее быстродействие даже при больших значениях входных величин.

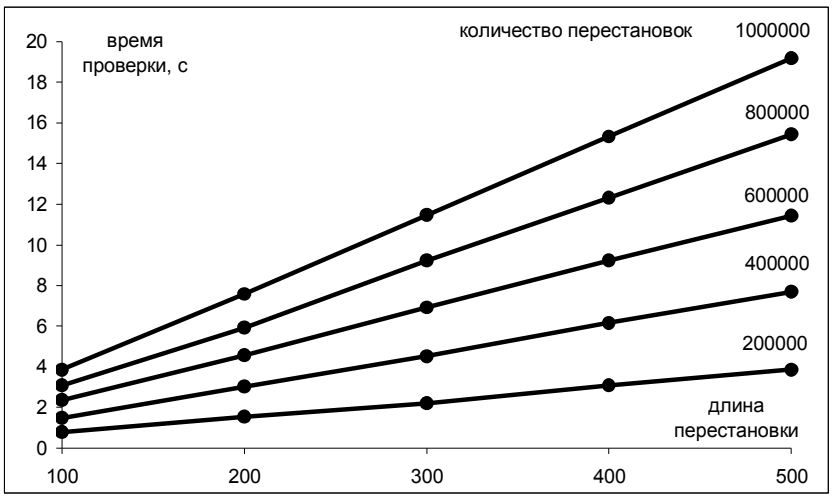

Рисунок 2 – Зависимость времени для перестановок на наличие ошибок методом контроля суммы элементов от длины перестановок при разном количестве проверок

2) Метод сравнения всех принятых элементов перестановки.

Если при сравнении принятых элементов перестановки обнаружены 2 одинаковых элемента, значит, один из них содержит ошибку. Достоинством данного метода является то, что для исправления ошибки достаточно осуществить повторную передачу только тех элементов, которые в перестановке на стороне приёмника получены как одинаковые. Для этого формируется вектор ошибки, представляющий собой двоичную комбинацию, в которой биты, номера которых соответствуют номерам правильно переданных элементов перестановки, принимают нулевые значения. В биты вектора ошибок, соответствующие повторяющимся элементам перестановки, записываются единицы.

Недостатком метода обнаружения ошибок в перестановке на основе сравнения её элементов является значительное увеличение числа операций сравнения элементов при возрастании количества элементов перестановки. Число операций сравнения элементов перестановки можно определить следующим образом: каждый следующий принятый элемент перестановки сравнивается со всеми предыдущими принятыми элементами. Следовательно, для первого принятого элемента не требуется проводить ни одной операции сравнения, второй принятый элемент сравнивается только с первым, третий – с первым и вторым и т.д. Последний n-й элемент перестановки сравнивается со всеми предыдущими, начиная с (n-1)-го и заканчивая первым. Общее число операций сравнения элементов будет вычисляться как сумма операций сравнения для каждого элемента перестановки. Для n-разрядной перестановки

$$Cp = (n-1) + (n-2)\ldots + 2 + 1 = \frac{n \cdot (n-1)}{2}. \qquad (7)$$

Пример: Найти число операций сравнения элементов при определении правильности передачи 100-элементной перестановки.

Решение: Согласно формуле (7) число операций сравнения элементов перестановки равняется

$$\text{Ср} = 100 \cdot (100-1)/2 = 4950.$$

Алгоритм работы метода обнаружения ошибок при передаче перестановки на основе сравнения её элементов:

1. Установка начального значения всех бит вектора ошибок в «0».
2. Приём элемента перестановки p_i.
3. Сравнение элемента перестановки p_i со всеми принятыми ранее элементами p_{i-1}, p_{i-2} … p_0.
4. Если обнаружены 2 элемента перестановки $p_i = p_j$, то происходит запись единиц в i-й и j-й биты вектора ошибок.
5. Проверка, был ли принят последний элемент перестановки. Если нет, то переход к п.2. Если да, то происходит проверка значения вектора ошибок.
6. Если значение вектора ошибок равно нулю, значит, перестановка принята верно, источнику и приёмнику отправляется сигнал о правильной передаче, в противном случае идёт переспрос ошибочно принятых элементов перестановки на основании значения вектора ошибок.

Аналогично предыдущему случаю было проведено программное моделирование рассматриваемого метода с целью оценить его быстродействие, а также способность обнаруживать ошибки в перестановках.

Данные, полученные в результате исследования доли обнаруживаемых в перестановках ошибок при использовании метода сравнения всех

принятых элементов перестановки, представлены в таблице 4. Исходя из этих данных, метод сравнения всех принятых элементов перестановки обладает более высокой способностью к обнаружению ошибок, чем рассмотренный ранее метод контроля суммы элементов перестановки, и позволяет выявлять все обнаруживаемые ошибки в перестановках. Доля обнаруживаемых ошибок для данного метода соответствует расчётному значению, полученному с помощью формулы (4) и представленному в таблице 1.

Таблица 4 - Зависимость доли обнаруживаемых ошибок для метода сравнения всех принятых элементов перестановки от длины перестановки при разном количестве испытаний

Длина перестановки	Количество испытаний				
	10	100	1000	10000	100000
2	0,5	0,5	0,512	0,498	0,503
3	0,7	0,79	0,763	0,781	0,778
4	0,8	0,9	0,927	0,91	0,906
5	0,9	0,94	0,967	0,962	0,962
6	0,9	0,98	0,981	0,985	0,983
7	1	0,99	0,992	0,995	0,994
8	1	1	0,996	0,998	0,998
9	1	1	0,999	0,999	0,999
10	1	1	1	0,9996	0,9996

Результаты оценки быстродействия рассматриваемого метода представлены в таблице 5 и на рисунке 3. Метод сравнения принятых элементов перестановки обладает гораздо более низким быстродействием по сравнению с методом контроля суммы элементов перестановки. Время, необходимое на обнаружение ошибок, с увеличением длины перестановок растёт быстрее, чем в случае метода контроля суммы элементов. Кроме того, зависимость времени проверки перестановок на наличие ошибок от длины перестановок нелинейна и определяется числом сравнений элементов перестановки согласно формуле (7). Зависимость же времени проверки от количества проверяемых перестановок линейна, как и в случае предыдущего метода.

Таблица 5 - Зависимость времени проверки перестановок на наличие ошибок методом сравнения всех принятых элементов перестановки (в секундах) от числа элементов перестановки и количества проверяемых перестановок

Длина перестановки	Количество перестановок				
	50000	100000	150000	200000	250000
100	3,41	6,87	10,22	13,68	17,09
200	13,08	26,41	39,89	52,25	65,27
300	28,96	57,86	86,87	115,11	143,79
400	50,82	101,87	152,75	204,07	254,4
500	78,85	158,57	237,57	316,7	395,88

Низкое быстродействие метода компенсируется более высокой долей

обнаруживаемых ошибок, а также возможностью снижения затрат времени на повторную передачу перестановок при обнаружении ошибки с помощью вектора ошибки.

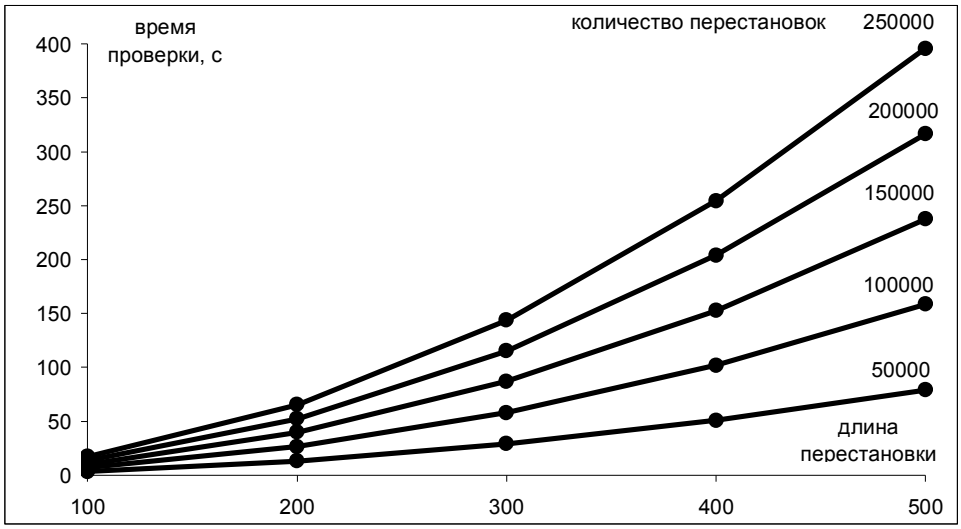

Рисунок 3 – зависимость времени проверки перестановок на наличие ошибок методом сравнения всех принятых элементов перестановки от длины перестановок при различном количестве проверок

4. Способы обнаружения ошибок при переходе одного из элементов перестановки в запрещённый элемент

Для обнаружения ошибок при переходе одного из элементов перестановки в запрещённый элемент может быть использован метод контроля суммы элементов перестановки аналогично случаю перехода элемента перестановки в разрешённый элемент. Данный метод является универсальным для обоих видов ошибок, поэтому алгоритм и устройство обнаружения ошибок, разработанные для него, могут быть применены без изменений для обнаружения ошибок в перестановках с запрещёнными элементами.

Метод сравнения элементов перестановки с максимальным значением элемента.

Любая запрещённая комбинация будет по значению больше максимального значения элемента перестановки. Следовательно, сравнивая все принятые элементы перестановки с максимальным значением элемента, можно обнаружить ошибочные элементы, являющиеся запрещёнными комбинациями. При этом, как и в методе сравнения всех принятых элементов перестановки для ошибок при переходе элемента перестановки в разрешённый элемент, формируется вектор ошибки, в котором единичные значения принимают биты, номера которых соответствуют номерам принятых запрещённых комбинаций.

Алгоритм данного метода выглядит следующим образом:

1. Установка начального значения всех битов вектора ошибок в «0».
2. Приём значения максимального элемента перестановки p_{max}.
3. Приём элемента перестановки p_i.
4. Сравнение элемента перестановки p_i со значением максимального элемента перестановки p_{max}. Если элемент перестановки $p_i > p_{max}$, то происходит запись единицы в i-й бит вектора ошибок.
5. Проверка, был ли принят последний элемент перестановки. Если

нет, то переход к п.3. Если да, то происходит проверка значения вектора ошибок.

6. Если значение вектора ошибок равно нулю, значит, перестановка принята верно, источнику и приёмнику отправляется сигнал о правильной передаче, в противном случае идёт переспрос ошибочно принятых элементов перестановки на основании значения вектора ошибок.

ВЫВОДЫ

Рассмотренная в работе зависимость доли обнаруживаемых ошибочных переходов от количества элементов перестановки позволяет сделать вывод, что число обнаруживаемых ошибок в перестановке растёт по мере увеличения её порядка.

Предложенные в работе методы и алгоритмы позволяют обнаруживать ошибки в перестановках при их передаче по каналу связи с шумом. При этом не требуется внесение дополнительной избыточности в передаваемые перестановки, что обеспечивает высокую скорость передачи. Выбор одного из алгоритмов для реализации в виде устройства обнаружения ошибок определяется требованиями, предъявляемыми к быстродействию и надёжности устройства.

SUMMARY

ERRORS DETECTION IN PERMUTATIONS

A.E. Goryachev
Sumy State University, Sumy

Transmission of a permutation may cause unacceptable errors therefore it's necessary to develop methods for their detection and correction. On the basis of the methods of detecting errors in the permutation proposed in the article appropriate algorithms are developed, their performance and reliability are researched.

Key words: *permutation, noise immunity, error detection, reliable algorithms.*

СПИСОК ЛИТЕРАТУРЫ

1. Рейнгольд Э. Комбинаторные алгоритмы: теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М.: Мир, 1980. – 477 с.
2. Борисенко А.А., Кулик И.А., Горячев А.Е. Электронная система генерации перестановок на базе факториальных чисел // Вісник СумДУ. Технічні науки. – 2007. – №1. – С.183 – 188.
3. Кодирование информации (двоичные коды) / Н.Т. Березюк, А.Г. Андрущенко, С.С. Мощицкий и др. - Харьков: Изд-во «Вища школа», 1978. – 252 с.

Поступила в редакцию 13 октября 2009 г.