УДК 681.3.06

МЕТОД ГЕНЕРАЦИИ ПЕРЕСТАНОВОК НА ОСНОВЕ ФАКТОРИАЛЬНЫХ ЧИСЕЛ С ИСПОЛЬЗОВАНИЕМ ДОПОЛНЯЮЩЕГО МАССИВА

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

В статье производится оценка быстродействия известных алгоритмов генерации перестановок на основе факториальных чисел. Предлагается алгоритм, обладающий более высоким быстродействием за счёт снижения количества операций преобразования факториального числа в перестановку.

Ключевые слова: *генерация перестановок, методы, алгоритмы, быстродействие, факториальная система счисления.*

ПОСТАНОВКА ЗАДАЧИ

Перестановки часто используются на практике для решения различных задач, среди которых - задачи комбинаторной оптимизации, помехоустойчивой передачи данных и их защиты от несанкционированного доступа [1]. Существует большое количество методов получения перестановок. Одним из способов построения перестановок является использование факториальных чисел, близких к перестановкам по своей структуре и свойствам [2]. Методы, использующие для генерации перестановок факториальную систему счисления, обладают рядом преимуществ, таких как способность получения перестановок большой длины, возможность формирования случайных перестановок и перечисления всех перестановок заданной длины.

Известные методы генерации перестановок на основе факториальных чисел, рассмотренные в [3], обладают высоким быстродействием за счёт уменьшения количества операций сравнения, необходимых для преобразования элементов перестановок. Однако в том случае, когда сортировку элементов перестановки невозможно осуществлять параллельно преобразованию, появляются значительные задержки, необходимые для выполнения вспомогательных операций.

РЕШЕНИЕ ЗАДАЧИ

Определим общее число циклов преобразования факториального числа в перестановку при последовательном выполнении всех операций для метода, рассмотренного в [3]. Для оценки зависимости данной величины от длины n перестановки будем считать, что время, необходимое для выполнения всех основных операций преобразования, является постоянной величиной.

Количество операций сравнения будет определяться согласно [3] по формулам (1) и (2).

Для случая минимального количества операций

$$C_{ГСЭП} = n - 1 . \qquad (1)$$

Для случая максимального количества операций

$$C_{ГСЭП\max} = (n-1) + (n-2) + \ldots + 2 + 1 = n \cdot (n-1)/2 . \qquad (2)$$

В количество циклов, необходимых для сортировки, будут входить цикл записи числа в массив сортировки и циклы сдвига записанных в массив чисел. Количество циклов сдвига будет различным как для разных перестановок, так и для разных элементов в одной перестановке. Максимальное количество циклов сдвига будет наблюдаться в случае, когда каждый раз новое число будет записываться на место наименьшего записанного числа, а все записанные в массив числа будут при этом сдвигаться на 1 позицию. Этому случаю соответствует преобразование факториального числа F = (n–1 n–2 ... 2 1 0) в перестановку P = (n–1 n–2 ... 2 1 0). При этом в массив сортировки будет сначала записываться число n–1, далее на его место запишется n–2, а n–1 при этом перепишется в следующую ячейку массива, на следующем цикле преобразования на место n–2 запишется число n–3, а n–2 и n–1 сдвинутся на 1 позицию в массиве и т.д. Общее количество циклов записи W и сдвига T для данного случая будет

$$Q_{ГСЭП\_WT} = W_{ГСЭП} + T_{ГСЭП} + \ldots + T_{ГСЭПi} + \ldots + T_{ГСЭП(n-2)},$$

где $W_{ГСЭП}$ – количество циклов записи, $W_{\text{ГСЭП}} = n - 1$;

$T_{ГСЭПi}$ – количество циклов сдвига для каждого записанного числа, $T_{ГСЭПi} = i - 1$; i = 1, 2 ... n – 1.

$$Q_{ГСЭП\_WT\max} = (n-1) + ((1-1) + (2-1) + \ldots + (n-1-1)) =$$
$$= 1 + 2 + \ldots + (n-2) + (n-1) = n \cdot (n-1)/2.$$

Минимальное количество циклов сдвига соответствует случаю, когда каждое следующее число будет записываться в массив сортировки на новую позицию. Величина $Q_{\text{ГСЭП\_WT}}$ при этом будет определяться только количеством операций $W_{\text{ГСЭП}}$, все $T_{\text{ГСЭПi}}$ будут равны нулю:

$$Q_{ГСЭП\_WT\min} = W_{ГСЭП} = n - 1 .$$

Данный случай соответствует преобразованию факториального числа F = (0 0 0 ... 0 0) в перестановку P = (0 1 2 ... n–2 n–1). Все остальные значения $Q_{ГСЭП\_WT}$ будут находиться между $Q_{ГСЭП\_WT\min}$ и $Q_{ГСЭП\_WT\max}$.

Далее необходимо учесть циклы инкрементирования I преобразуемого элемента перестановки. Количество этих циклов будет наибольшим при преобразовании числа F = (0 0 0 ... 0 0) в перестановку P = (0 1 2 ... n–2 n–1) и наименьшим при преобразовании числа F = (n–1 n–2 ... 2 1 0) в перестановку P = (n n–1 ... 2 1 0).

$$I_{ГСЭП} = I_{ГСЭП(n-1)} + I_{ГСЭП(n-2)} + \ldots + I_{ГСЭП1} + I_{ГСЭП0},$$

где $I_{\text{ГСЭПk}}$ – количество циклов инкрементирования k-го элемента перестановки, k = 0, 1, ..., n–1.

$$I_{ГСЭП\max} = 0 + 1 + 2 + \ldots + (n-1) = n \cdot (n-1)/2 ,$$

$$I_{ГСЭП\min} = 0 .$$

Общее количество циклов преобразования

$$Q_{ГСЭП} = C_{ГСЭП} + Q_{ГСЭП\_WT} + I_{ГСЭП}.$$

Для случая перехода F = (0 0 0 ... 0 0) в P = (0 1 2 ... n−2 n−1)

$$\begin{aligned} Q_{ГСЭП0} &= C_{ГСЭП\,\max} + Q_{ГСЭП\_WT\,\min} + I_{ГСЭП\,\max} = \\ &= n \cdot (n-1)/2 + (n-1) + n \cdot (n-1)/2 = (n-1) \cdot (n+2). \end{aligned} \quad (3)$$

Для случая перехода F = (n−1 n−2 ... 2 1 0) в P = (n−1 n−2 ... 2 1 0)

$$\begin{aligned} Q_{ГСЭП(n-1)} &= C_{ГСЭП\,\min} + Q_{ГСЭП\_WT\,\max} + I_{ГСЭП\,\min} = \\ &= (n-1) + n \cdot (n-1)/2 = n \cdot (n+1)/2 - 1. \end{aligned} \quad (4)$$

Результаты сравнения полученных значений количества циклов преобразования (3), (4) с величинами, полученными при использовании алгоритма генерации перестановок на основе факториальных чисел с использованием сортировки элементов перестановки по (1) и (2), свидетельствуют о значительном увеличении времени, требуемого для преобразования факториального числа в перестановку (табл. 1).

Таблица 1 – Количество циклов полного преобразования факториального числа в перестановку и количество циклов сравнения элементов в зависимости от длины перестановки для метода ГСЭП

n	2	3	4	5	6	7	8	9	10
$Q_{ГСЭП\ 0}$	3	8	15	24	35	48	63	80	99
$C_{ГСЭП\ max}$	1	3	6	10	15	21	28	36	45
$Q_{ГСЭП\ n-1}$	2	5	9	14	20	27	35	44	54
$C_{ГСЭП\ min}$	1	2	3	4	5	6	7	8	9

Наиболее заметное отличие наблюдается для величин $C_{ГСЭПmin}$ и $Q_{ГСЭП\_n-1}$. При росте длины перестановки наблюдается значительное смещение графиков $Q_{ГСЭП\_0}$ и $Q_{ГСЭП\_n-1}$ относительно $C_{ГСЭПmax}$ и $C_{ГСЭПmin}$ соответственно в сторону увеличения количества циклов преобразования, а также более заметная разница между максимальным $Q_{ГСЭП\_0}$ и минимальным $Q_{ГСЭП\_n-1}$ значением количества циклов преобразования и (рис. 1). Полученные результаты показывают, что существует необходимость разработки метода преобразования факториальных чисел в перестановки, отличающегося увеличенным быстродействием за счёт сокращения общего количества операций [3].

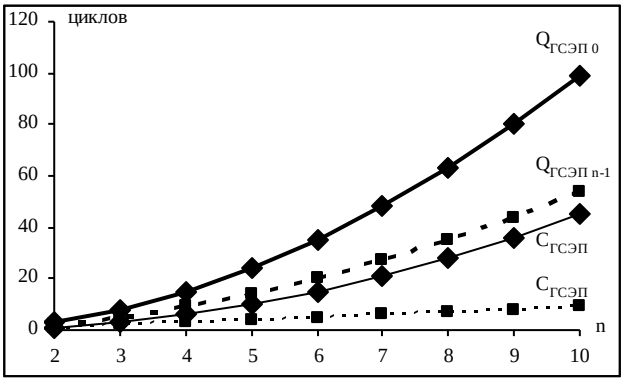

Рисунок 1 - Сравнение количества циклов преобразования факториального числа в перестановку и циклов сравнения элементов перестановок для метода ГСЭП при различной длине перестановок

Значительная потеря быстродействия происходит за счёт транспозиций при сортировке преобразованных элементов перестановки. При этом отсортированные элементы располагаются в массиве сортировки в порядке возрастания их значений. Поэтому предлагается записывать полученные элементы перестановки в ячейках массива, номера которых соответствуют значениям этих элементов, то есть, к примеру, элемент со значением 1 записывается в первую ячейку, 5 – в пятую и т.п. Таким образом, сохраняется возрастающий порядок элементов в массиве и отпадает необходимость в дополнительных перемещениях элементов внутри массива. В процессе преобразования в данном случае необходимо пропускать пустые ячейки массива сортировки и сравнивать преобразуемый элемент со значениями элементов в заполненных ячейках, начиная с ячейки с наименьшим номером.

Далее, поскольку значения хранимых в ячейках массива сортировки чисел будут соответствовать номерам этих ячеек, нет необходимости записывать в ячейки данные числа, достаточно отметить те из них, которые должны быть заполнены, единицами, в то время как пустые ячейки будут заполнены нулями. Массив сортировки, заполненный согласно данному рассуждению, будем называть дополняющим массивом $M_{\text{доп}}$. Согласно методу генерации перестановок преобразуемый элемент увеличивается на единицу в случае, когда элемент, с которым он сравнивается, меньше его либо равен ему [2]. Следовательно, для перехода от цифры факториального числа f_{i} к элементу перестановки p_{i} необходимо добавить к этой цифре все единицы из ячеек массива $M_{\text{доп}}$, начиная с наименьшей ячейки $m_{доп\_0}$ и заканчивая ячейкой с номером, равным величине преобразуемой цифры $m_{доп\_f_i}$. После этого, если цифра f_{i} увеличилась на некоторое число единиц k, необходимо добавить к f_{i} все единицы ячеек $M_{\text{доп}}$ из интервала от $m_{доп\_f_i}$ до $m_{доп\_(f_i+k)}$. Данные операции суммирования прерываются при выполнении одного из двух следующих условий:

К f_{i} прибавлены все единицы из массива $M_{\text{доп}}$. Их количество ограничивается числом преобразованных ранее элементов перестановки. Для перестановки длины n количество единиц в массиве $M_{\text{доп}}$ будет равно $n - i - 1$. В этом случае элемент перестановки $p_{\text{i}} = f_{\text{i}} + n - i - 1$.

В рассматриваемом интервале ячеек $M_{\text{доп}}$ нет ни одной единицы. При этом f_{i} остаётся неизменным и записывается как элемент перестановки p_{i}.

Алгоритм, реализующий метод генерации перестановок с использованием дополняющего массива (метод ГДМ), содержит следующие шаги:

Шаг 1. Запись исходного n-разрядного факториального числа F. Установка в нулевое значение ячеек m_0 ... m_{n-2} дополняющего массива $M_{\text{доп}}$.

Шаг 2. Цифра старшего разряда факториального числа $f_{\text{n-1}}$ считается первым элементом перестановки p_{n-1}, в ячейку памяти $m_{p_{n-1}}$ записывается единица.

Шаг 3. Происходит проверка, была ли преобразована последняя цифра факториального числа. Если да, то переход к п.10. Если нет, то происходит переход к преобразованию следующей цифры факториального числа.

Шаг 4. Предварительно элементу перестановки p_i присваивается значение f_{i}, где значение $i = n-2, \ldots 2, 1, 0$.

Шаг 5. Вычисляется сумма S единиц в ячейках m_0 ... m_{p_i}.

Шаг 6. Если полученное значение S равно нулю, элемент p_i остаётся без изменений, переход к п.3.

Шаг 7. Добавление значения S к значению элемента перестановки p_i.

Шаг 8. Если полученное значение p_i больше значения f_i на $n - i - 1$, то происходит переход к пункту 3.

Шаг 9. Вычисление суммы S единиц в ячейках $M_{доп}$, начиная с первой из незадействованных ранее и заканчивая ячейкой с номером, равным новому значению p_i. Переход к п.6.

Шаг 10. Вывод полученной перестановки.

Быстродействие метода будет определяться количеством операций сложения S значения преобразуемого элемента и содержимого ячеек дополняющего массива, а также количеством операций записи W в массив $M_{доп}$. Число операций записи для любой перестановки будет равно

$$W_{ГДМ} = n - 1.$$

Количество операций сложения будет разным для разных перестановок и определяется порядком заполнения массива, который, в свою очередь, зависит от порядка расположения элементов в перестановке. Минимальное количество единиц, прибавляемое к элементу перестановки, очевидно, будет равно 0, максимальное – $n - i - 1$, где i – номер разряда цифры факториального числа. Таким образом, для всех элементов перестановки число операций сложения $S_{ГДМ}$ будет ограничиваться минимальным $S_{ГДМ\ min}$ и максимальным $S_{ГДМ\ max}$ значением:

$$S_{ГДМ\,min} = 0,$$

$$S_{ГДМ\,max} = 0 + 1 + \ldots + (n-1) = n \cdot (n-1)/2.$$

В среднем для преобразования одного факториального числа в перестановку потребуется следующее количество операций сложения:

$$S_{ГДМср} = (S_{ГДМ\,min} + S_{ГДМ\,max})/2 = n \cdot (n-1)/4.$$

Общее количество операций, требующихся в среднем для преобразования факториального числа в перестановку с помощью метода ГДМ:

$$Q_{ГДМ} = S_{ГДМср} + W_{ГДМ} = (n-1) + n \cdot (n-1)/4 = (n-1) \cdot (n+4)/4.$$

Сравним полученные значения $S_{ГДМср}$ и $S_{ГДМ}$ со значениями среднего количества циклов преобразования для предыдущего метода (табл. 2). Величина $Q_{ГСЭП\_ср}$ в табл. 2 является средним значением величин $Q_{ГСЭП\_0}$ и $Q_{ГСЭП\_n\text{-}1}$, определяемых по (4):

$$Q_{ГСЭПср} = (Q_{ГСЭП\_0} + Q_{ГСЭП\_(n-1)})/2 = ((n-1) \cdot (n+1) + n \cdot (n+1)/2 - 1)/2 =$$
$$= (2n^2 - 2 + n^2 + n - 2)/4 = (n-1) \cdot (3n+4)/4.$$

Из полученных результатов (рис. 2) следует, что при последовательном выполнении операций рассматриваемый метод значительно превосходит по быстродействию метод ГСЭП, а при параллельном выполнении методы близки по значению быстродействия преобразования факториальных чисел в перестановки.

Таблица 2 – Сравнение количества циклов преобразования факториального числа в перестановку для разных методов генерации перестановок

n	2	3	4	5	6	7
$S_{ГДМ\ ср}$	0,5	1,5	3	5	7,5	10,5
$Q_{ГДМ}$	1,5	3,5	6	9	12,5	16,5
$C_{ГСЭП\ ср}$	1	2,5	4,5	7	10	13,5
$Q_{ГСЭП\ ср}$	2,5	6,5	12	19	27,5	37,5
n	8	9	10	11	12	13
$S_{ГДМ\ ср}$	14	18	22,5	27,5	33	39
$Q_{ГДМ}$	21	26	31,5	37,5	44	51
$C_{ГСЭП\ ср}$	17,5	22	27	32,5	38,5	45
$Q_{ГСЭП\ ср}$	49	62	76,5	92,5	110	129

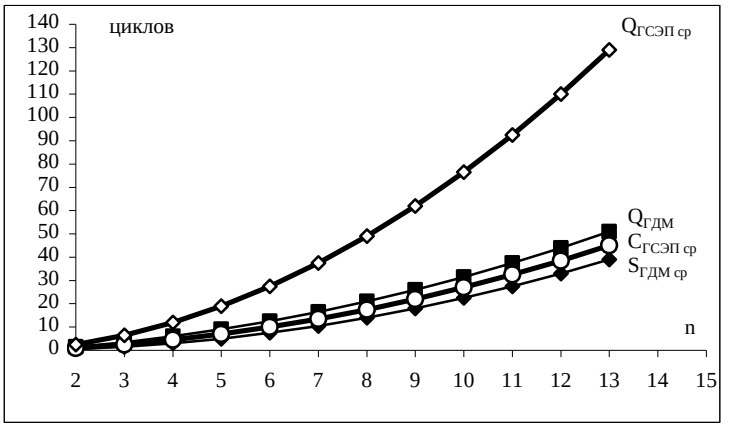

Рисунок 2 - График зависимости количества циклов преобразования факториального числа в перестановку от длины перестановок для разных методов генерации перестановок на основе факториальных чисел

В то же время необходимо учитывать возможность увеличения количества циклов преобразования для метода ГДМ в том случае, когда нет возможности выбирать из массива только единичные значения. В этом случае содержимое ячеек массива будет прибавляться к значению преобразуемого элемента подряд вне зависимости от его значения. Следовательно, для данного случая количество операций суммирования будет постоянно.

$$S_{ГДМ1} = S_{ГДМ\max} = 0 + 1 + \ldots + (n-1) = n * (n-1)/2\,,$$

$$Q_{ГДМ1} = S_{ГДМ1} + W_{ГДМ} = (n-1) + n \cdot (n-1)/2 = (n-1) \cdot (n+2)/2\,.$$

Для сравнения быстродействия методов генерации перестановок необходимо привести значения количества циклов преобразования $Q_{ГСЭП\_ср}$ для метода ГСЭП (см. табл. 2). Кроме того, необходимо определить число циклов преобразования для известного метода ГФЧ1. Для него ранее было найдено количество операций сравнения [3]. Кроме

этого, в процессе преобразования происходит некоторое количество операций инкрементирования элементов, различное для каждой перестановки. Это количество ограничено следующими значениями:

$$I_{ГФЧ1\_\min} = 0,$$

$$I_{ГФЧ1\_\max} = 0 + 1 + \ldots + n - 1 = n \cdot (n-1)/2.$$

Исходя из этих выражений, можно определить количество циклов преобразования в среднем для одной перестановки:

$$Q_{ГФЧ1\_ср} = (I_{ГФЧ1\_\min} + I_{ГФЧ1\_\max})/2 + C_{ГФЧ1} =$$
$$= n \cdot (n-1)/4 + n \cdot (n-1)/2 = 3n \cdot (n-1)/4.$$

Все полученные значения сведены для сравнения в табл. 3. Здесь $Q'_{ГДМ}$ – среднее количество циклов преобразования факториального числа в перестановку для метода ГДМ без учёта прибавления нулевых значений ячеек $M_{доп}$, $Q'_{ГДМ} = S'_{ГДМn}/n + W_{ГДМ}$, $Q'_{ГДМ1}$ – с учётом прибавления нулевых значений ячеек $M_{доп}$, $Q'_{ГДМ1} = S'_{ГДМ1n}/n! + W_{ГДМ}$.

Таблица 3 – Среднее количество циклов преобразования факториального числа в перестановку для различных методов

n	2	3	4	5	6	7
$Q'_{ГДМ}$	1,5	3,5	6	9	12,5	16,5
$Q'_{ГДМ1}$	2	5	9	14	20	27
$Q_{ГСЭП\ ср}$	2,5	6,5	12	19	27,5	37,5
$Q_{ГФЧ1\ ср}$	1,5	4,5	9	15	22,5	31,5
n	8	9	10	11	12	13
$Q'_{ГДМ}$	21	26	31,5	37,5	44	51
$Q'_{ГДМ1}$	35	44	54	65	77	90
$Q_{ГСЭП\ ср}$	49	62	76,5	92,5	110	129
$Q_{ГФЧ1\ ср}$	42	54	67,5	82,5	99	117

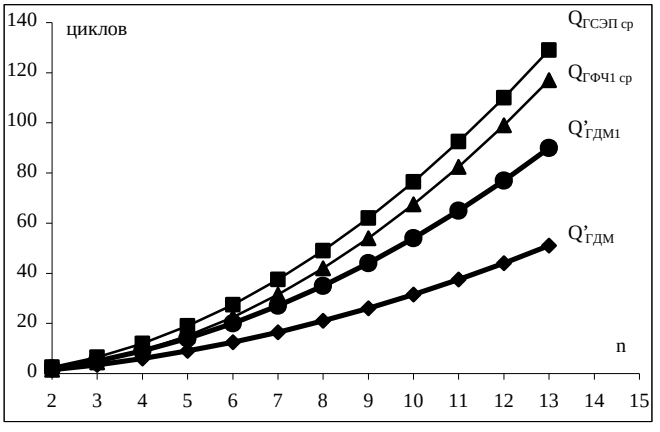

Рисунок 3 - Сравнение зависимости количества циклов преобразования факториального числа в перестановку от длины перестановок для различных методов

ВЫВОДЫ

Из полученных результатов исследования (рис. 3) можно сделать следующий вывод. Предложенный метод генерации перестановок, использующий дополняющий массив, при последовательном выполнении всех операций преобразования показывает более высокое быстродействие (меньшее количество операций) по сравнению с другими методами в обоих случаях – как при добавлении всех значений ячеек дополняющего массива, так и при выборе только единичных значений. Результаты, полученные с помощью моделирования работы метода, полностью совпадают с выведенной формулой, что позволяет использовать её для оценки быстродействия метода при большой длине перестановок.

МЕТОД ГЕНЕРАЦІЇ ПЕРЕСТАНОВОК НА БАЗІ ФАКТОРІАЛЬНИХ ЧИСЕЛ ІЗ ВИКОРИСТАННЯМ ДОПОВНЮВАЛЬНОГО МАСИВА

О. Є. Горячев, С. О. Дегтяр,
Сумський державний університет, м. Суми

Існують алгоритми генерації перестановок, що використовують факторіальні числа, які мають высоку швидкодію при паралельному виконанні операцій перетворення. У статті ставиться завдання визначення швидкодії цих алгоритмів при послідовному виконанні операцій, а також розроблення методу з підвищеною швидкодією за рахунок зменшення загальної кількості операцій перетворення.

Ключові слова: *генерація перестановок, методи, алгоритми, швидкодія, факторіальна система числення.*

THE METHOD OF GENERATING PERMUTATIONS BASED ON FACTORIAL NUMBERS USING SUPPLEMENTING ARRAY

A. E. Goryachev; S. O. Degtiar,
Sumy State University, Sumy

There are algorithms for permutations generation using the factorial numbers, which have a high-speed on condition of concurrency of transformation operations. The article describes the problem of the performance determination of these algorithms on condition of sequential operations, and develop a method of improvement of the performance by reducing the total number of conversion operations.

Key words: *generation of permutations, methods, algorithms, performance, factorial number system.*

СПИСОК ЛИТЕРАТУРЫ

1. Рейнгольд Э. Комбинаторные алгоритмы: теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. –М.: Изд-во “Мир”, 1980. – 477 с.
2. 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.
3. Горячев А.Е. Оценка быстродействия алгоритмов генерации перестановок на основе факториальных чисел / А.Е. Горячев // Вісник СумДУ. Технічні науки.– 2010.– № 1.– С. 62 -67.

Поступила в редакцию 31 августа 2012 г.