УДК 621.3.037.37

ЕЛЕКТРОННА СИСТЕМА ГЕНЕРАЦІЇ ПЕРЕСТАНОВОК НА БАЗІ ФАКТОРІАЛЬНИХ ЧИСЕЛ

О.А. Борисенко, І.А. Кулик, О.Є. Горячев
Сумський державний університет

У статті розглядається факторіальна система числення з метою отримання більш простих алгоритмів та електронних систем для генерації перестановок. Отримання факторіальних чисел є проміжним кроком при переході від степеневих чисел до перестановок і зворотному переході. Як результат часові витрати при породженні перестановок і їх нумерації зменшуються, а практична реалізація відповідних електронних пристроїв і систем спрощується.

СТАН ПРОБЛЕМИ

Такий клас комбінаторних об'єктів, як перестановки, широко і ефективно застосовується на практиці для вирішення відомих задач: 1) захисту даних від несанкціонованого доступу; 2) перешкодостійкої передачі даних; 3) комбінаторної оптимізації. Так, наприклад, для побудови гнучких та швидких блокових апаратних шифрів з метою захисту інформаційно-телекомунікаційних систем використовуються перестановки, які управляються, фіксовані перестановки та перестановки, вигляд яких залежить від даних, що перетворюються [1, 2]. З урахуванням розташування і значень елементів перестановок вони з успіхом можуть бути застосовані для виявлення та корекції помилок в даних, які передаються по каналах зв'язку [3]. Випадково породжені перестановки як вхідні конфігурації вихідних даних необхідні для оцінки складності і ефективності алгоритмів, наприклад, методом Монте-Карло [4].

Загальним методом породження різних комбінаторних об'єктів, у тому числі перестановок, є метод, який базується на пошуку з поверненням [4]. Безпосереднє застосування цього методу, як правило, призводить до алгоритмів, час роботи яких неприпустимо великий. Щоб знизити ці часові витрати при породженні перестановок, необхідно адаптувати цей загальний метод до конкретної задачі. В даній роботі пропонується для генерування перестановок використовувати факторіальні числа, які близькі до них за своєю структурою і властивостями.

Таким чином, цілями цієї роботи є:

1) розроблення алгоритмів породження перестановок і зворотного перетворювання на базі факторіальних чисел;

2) розроблення структур електронних систем, які реалізують алгоритми породження перестановок і зворотного перетворювання на базі факторіальних чисел.

Структури електронних пристроїв, які реалізують розроблені алгоритми, мають бути ефективними в системах захисту інформації від несанкціонованого доступу, системах зв'язку для завадостійкої передачі даних, комбінаторних системах оптимального управління і регулювання.

1 Загальні відомості

Факторіальні системи числення відносяться до систем зі змішаною основою.

Як правило, під факторіальною системою числення розуміють вираз, який має вигляд

$$F_{<ф>} = X_n \cdot n! + X_{n-1} \cdot (n-1)! + \ldots + X_l \cdot l! + \ldots + X_1 \cdot 1! + X_0 \cdot 0!, \qquad (1)$$

де $l = 0,1,\ldots, n$; $0 \le X_l \le l$.

Він має назву нумераційної чи числової функції.

Максимальне число $F_{\max}$ в факторіальній системі має вигляд $n(n-1)\ldots l\ldots 10$. Тоді

$$F_{<ф>\max} = (n+1)! - 1. \qquad (2)$$

Це випливає з наведених нижче перетворювань над $F_{<ф>}$ (1), коли $X_l = l$, де $0 \le X_l \le l$. У цьому разі

$$\begin{aligned} F = F_{\max} &= (n+1-1)\cdot n! + \big((n-1)+1-1\big)\cdot(n-1)! + \ldots \\ &\ldots + (l+1-1)\cdot l! + \ldots + (1+1-1)\cdot 1! + (0+1-1)\cdot 0! = \\ &= (n+1)! - n! + n! - (n-1)! + \ldots + (l+1)! - l! + \ldots \\ &\ldots + 2! - 1! + 1 - 1! = (n+1)! - 1. \end{aligned}$$

Мінімальне число $00\ldots0\ldots0$ в факторіальній системі числення $F_{\min} = 0$. Дійсно, якщо всі розряди $X_l = 0$, то

$$F = F_{\min} = 0 \cdot n! + 0 \cdot (n-1)! + \ldots + 0 \cdot l! + \ldots + 0 \cdot 1! + 0 \cdot 0! = 0.$$

Діапазон факторіальних чисел

$$P = F_{\max} + 1. \qquad (3)$$

Для його знаходження враховується, крім максимального числа, ще й нуль.

2 Арифметичні операції

Під час виконання арифметичних операцій додавання і віднімання в факторіальній системі числення в нульовому розряді використовують правила унарної (одиничної) системи числення, в першому – двійкової, у другому – трійкової і т.д. Операції множення і ділення виконуються з допомогою операцій додавання і віднімання за загальними правилами для однорідних систем числення.

Приклад 1 Виконати операції додавання і віднімання факторіальних чисел $A_{<ф>} = 23110$ і $B_{<ф>} = 12200$ і знайти величину максимального числа.

Розв'язання. Застосовуючи вираз (1), максимальне число

$$F_{\max} = 4 \cdot 4! + 3 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 119.$$

Згідно з (3) діапазон факторіальних чисел для даного випадку

$$P = F_{\max} + 1 = 120.$$

Додавання і віднімання чисел виконується так:

$$\begin{array}{r} 23110 \\ +\ 12200 \\ \hline 12200 \end{array} \qquad \begin{array}{r} 23110 \\ -\ 12200 \\ \hline 10210 \end{array} .$$

Перевірка:

$23110_{<ф>} = 2 \cdot 4! + 3 \cdot 3! + 1 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 69_{<10>}$;

$12200_{<ф>} = 1 \cdot 4! + 2 \cdot 3! + 2 \cdot 2! + 0 \cdot 1! + 0 \cdot 0! = 40_{<10>}$;

$42010_{<ф>} = 4 \cdot 4! + 2 \cdot 3! + 0 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 69_{<10>} + 40_{<10>} = 109_{<10>}$;

$10210_{<ф>} = 1 \cdot 4! + 0 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 69_{<10>} - 40_{<10>} = 29_{<10>}$.

3 Перетворення факторіальних чисел в числа степеневих систем числення

Перетворення факторіального числа в степеневе виконується шляхом підстановки факторіального числа в числову (нумераційну) функцію для факторіальних систем числення. При цьому виконуються всі вказані в цій функції операції множення і додавання.

Приклад 2 Перетворити факторіальне число $F_{<ф>} = 232200$ в десяткову систему числення.

Розв'язання:

$$F_{<ф>} = 2 \cdot 5! + 3 \cdot 4! + 2 \cdot 3! + 2 \cdot 2! + 0 \cdot 1! + 0 \cdot 0! = 240 + 72 + 12 + 4 = 328_{<10>}.$$

4 Виявлення помилок

У факторіальній системі числення можуть бути одержані помилкові числа, які можуть бути виявлені. Ознакою помилок буде порушення обмежень на величину цифр X_l, де $0 \le X_l \le l$.

Наприклад, факторіальне число 23210 є правильним, а число 23220 – помилковим, тому що в першому розряді цього числа порушено обмеження на величину цифри 1, яка повинна бути не більше 1, тобто дорівнювати 0 або1.

5 Перетворення степеневих чисел в числа факторіальної системи числення

Перетворення числа із степеневої системи числення в факторіальну відбувається в такій послідовності.

Першим кроком буде ділення числа, яке перетворюється на 1. Якщо знайдена частка буде більше 1, то наступним кроком буде ділення його на двійку, і тоді отриманий залишок від ділення запишеться як цифра першого розряду факторіального числа. Потім аналізується величина отриманої при діленні на двійку частки. Якщо вона менше 3, то в другий розряд факторіального числа записується її значення, а у всі старші розряди – нулі. Якщо більше 3, то виконується ділення цієї частки на 3 і далі виконується із залишком і часткою такі самі операції, як і на другому кроці. Ця процедура продовжується до того часу, поки частка не стане менше свого дільника. Потім справа наліво виписуються всі отримані раніше залишки. Їх послідовність створює шукане число.

Приклад 3 Перетворити десяткове число $D = 69_{<10>}$ у факторіальне число $F_{<ф>}$.

Розв'язання. Процес перетворення степеневого числа $69_{<10>}$ відображено на рисунку 1.

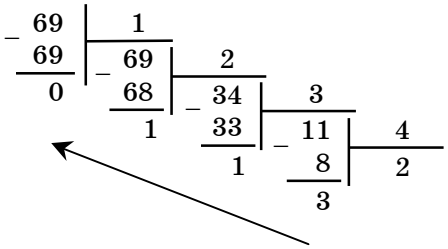

Рисунок 1 – Перетворення $69_{<10>}$ *в* $23110_{<ф>}$

Відповідь. $F_{<ф>} = 23110_{<ф>}$.

6 Практичне значення факторіальних систем числення

Факторіальні системи числення дають можливість побудови широкого класу комбінаторних конфігурацій, серед яких особливе значення мають перестановки. Їх можна породжувати за допомогою факторіальних чисел.

Розглянемо спочатку алгоритм побудови перестановок.

Для того щоб знайти відповідність між числом у факторіальній системі числення і перестановкою, необхідно цифру, яка стоїть в n-му розряді факторіального числа, залишити без змін і вважати її першим елементом перестановки. Наступну цифру $(n-1)$-го розряду числа необхідно порівняти з першим елементом перестановки, і якщо вона буде більшою, то треба збільшити цю цифру на 1, якщо ні – залишити без змін.

Далі цифру $(n-2)$-го розряду порівнюють спочатку з першим елементом перестановки, і якщо вона дорівнює йому або більше його, то збільшують цей елемент на 1, а якщо ні, то залишають без змін. Потім виконують порівняння скорегованої цифри з другим елементом перестановки, і якщо вона дорівнює йому або більше його, то знову збільшують її на 1. У протилежному разі залишають без змін.

Аналогічно проводять порівняння цифри $(n-3)$-го розряду і інших цифр факторіального числа аж до нульового розряду. При кожному збільшенні цифри на 1 її порівняння проводяться з всіма елементами перестановки, починаючи з першого.

Приклад 4 Дано факторіальне число $F_{<ф>} = 1200_{<ф>}$. Треба знайти перестановку $B_{<пер>}$ відповідну до цього факторіального числа.

Розв'язання. Згідно з факторіальним числом $1200_{<ф>}$ цифра 1 буде першим елементом перестановки, цифра 2 більше 1 і відповідно збільшується на 1. Це означає, що другий елемент перестановки буде дорівнювати 3. Далі 0 менший і цифри 1, і цифри 3. Отже, він залишається без змін. Тобто третім елементом перестановки буде 0. Остання цифра факторіального числа 0. Вона дорівнює третьому елементу перестановки. Тому збільшуємо цифру 0 на 1 і отримуємо 1. Ця цифра 1 дорівнює першому елементу перестановки. Тому збільшуємо її ще раз на 1 і отримуємо цифру 2. Ця цифра менше другого елемента перестановки і тому більше немає потреби збільшувати її на 1, тобто останній елемент перестановки буде дорівнювати 2. У результаті будемо мати перестановку $B_{<пер>}=1302_{<пер>}$. Таким чином, $1200_{<ф>} \to 1302_{<пер>}$.

Зворотний алгоритм переходу від перестановки до факторіального числа містить такі кроки: як цифру n-го розряду факторіального числа

береться старший n-й елемент перестановки. Наступна цифра факторіального числа повинна дорівнювати $(n-1)$-му елементу перестановки, якщо цей елемент менше n-го елемента перестановки або дорівнювати зменшеному на 1 його значення, якщо вона більше цього елемента n. Відповідно з l-го елемента перестановки віднімається стільки одиниць, скільки в перестановці буде менших попередніх йому елементів. Якщо таких елементів не буде, то цифра l факторіального числа буде дорівнювати l-му елементу перестановки.

Приклад 5 Дана перестановка $B_{<пер>} = 045321$. Треба знайти відповідне їй число $F_{<ф>}$ в факторіальній системі числення.

Розв'язання. Опираючись на розглянутий вище зворотний алгоритм перетворення перестановок в факторіальні числа, отримуємо, що

$$B_{<пер>} = 045321_{<пер>} \rightarrow F_{<ф>} = 033210_{<ф>}.$$

Також за допомогою факторіальних чисел розв'язується задача перетворення перестановок у відповідні їм числа степеневих систем числення, тобто виконується задача нумерації перестановок.

За допомогою факторіального числа $F_{<ф>}$ і числової факторіальної функції (1) легко одержати номер перестановки.

Приклад 6 Знайти номер перестановки $B_{<пер>} = 045321$.

Розв'язання. Згідно з прикладом 5 маємо $045321_{<пер>} \leftrightarrow 033210_{<ф>}$. Застосувавши факторіальну числову функцію (1) до числа $033210_{<ф>}$, отримуємо

$$033210_{<ф>} = 0 \cdot 5! + 3 \cdot 4! + 3 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! + 0 \cdot 0! = 95_{<10>}.$$

Структура системи формування перестановок на базі факторіальних чисел відображена на рисунку 1. Джерело 1 номерів генерує номери перестановок в довільному або заданому порядку, які надходять на перетворювач 2 номера в факторіальне число. Перетворювач 2 формує факторіальні числа згідно з алгоритмом перетворення чисел із степеневої системи числення в факторіальну. Далі факторіальне число надходить до перетворювача 3 факторіального числа в перестановку, результатом роботи якого є перестановка, згенерована відповідно до алгоритму побудови перестановок.

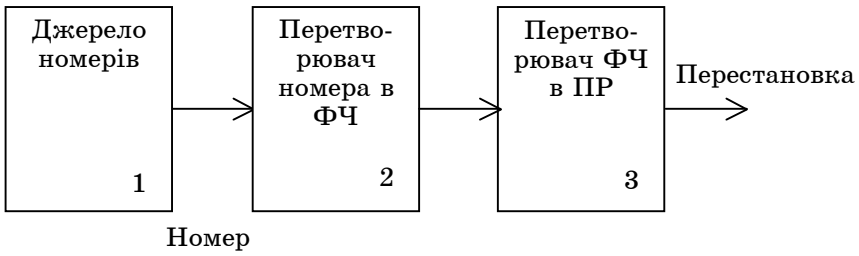

Рисунок 1 – Електронна система формування перестановок на базі факторіальних чисел, де ФЧ – факторіальне число; ПР – перестановка

Структура системи, яка розв'язує зворотну задачу формування номерів перестановок на базі факторіальних чисел, відображена на рисунку 2. Алгоритм роботи даної системи складає алгоритм зворотної задачі

перетворення перестановок в факторіальні числа, який реалізує блок 1, і алгоритм обчислювання номера згідно з числовою функцією (1), який реалізує блок 2.

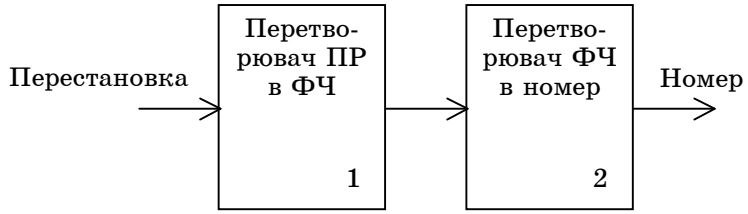

Рисунок 2 – Електронна система нумерації перестановок на базі факторіальних чисел, де ПР – перестановка; ФЧ – факторіальне число

ВИСНОВКИ

Розглянута вище факторіальна система числення є тільки одна з класу факторіальних систем. Вона породжує в даному випадку всі можливі перестановки. Але можуть бути отримані і інші, більш складні, які будуть породжувати факторіальні числа з іншою структурою і тим самим будувати перестановки з обмеженнями, тобто тільки частину перестановок із загального їх класу. Розроблення таких систем числення має науковий та практичний інтерес при розв'язанні деяких комбінаторних задач.

Запропоновані в роботі алгоритми породження перестановок і їх нумерації на базі факторіальних чисел дозволяють:

1) знизити часові витрати на генерування перестановок в довільному або заданому порядку;

2) спростити технічну реалізацію пристроїв і систем, які генерують перестановки.

SUMMARY

In the paper a factorial number system is considered to obtain more simple algorithms and electronic systems for generating permutations. Receipt of factorial numbers are an intermediate step at transferring from power numbers to permutations and vice versa. In result the time costs are decreased at generating permutations and their enumerating, practical realization of corresponding devices and systems is simplified.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян А.А. и др. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 244 с.
2. Введение в криптографию / Под общ. ред. В. В. Ященко. – М.: МЦНМО, 2000. – 272 с.
3. Цимбал В.П. Теория информации и кодирования. – К.: Вища школа, 1992. – 263 с.
4. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы: теория и практика. – М.: Изд-во "Мир", 1980. – 477 с.

О.А. Борисенко, д-р техн. наук, проф.,
Сумський державний університет;

И.А. Кулик, канд. техн. наук, доц.,
Сумський державний університет;

О.Є. Горячев, аспірант,
Сумський державний університет

Надійшла до редакції 26 березня 2007 р.