УДК 621.3.037.37

О.А. Борисенко, О.Є. Горячев

Сумський державний університет, Суми

ЗАХИСТ ДАНИХ НА БАЗІ ФАКТОРІАЛЬНИХ ЧИСЕЛ

Вступ

Постановка задачі. Для вирішення задачі захисту даних від несанкціонованого доступу на практиці ефективно застосовується такий клас комбінаторних об'єктів, як перестановки. 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.

Загальним методом породження різних комбінаторних об'єктів, у тому числі перестановок, є метод, який базується на пошуку з поверненням. Безпосереднє застосування цього методу, як правило, призводить до алгоритмів, час роботи яких неприпустимо великий. Щоб знизити 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. Даний метод, крім забезпечення зменшення часових витрат на побудову перестановок, може застосовуватися безпосередньо для шифрування даних шляхом перетворення вхідних даних у вигляді двійкового коду спочатку на факторіальні числа, далі факторіальні числа – на перестановки.

Таким чином, метою цієї роботи є розроблення алгоритмів породження перестановок і їх зворотнє перетворювання на базі факторіальних чисел;

Структури електронних пристроїв, які реалізують розроблені алгоритми, мають бути ефективними в системах захисту інформації від несанкціонованого доступу.

Загальні положення. Факторіальні системи числення належать до систем зі змішаною основою.

Зазвичай під факторіальною системою числення розуміють вираз, який має вигляд:

$$F_{<Ф>} = X_n \cdot n! + X_{n-1} \cdot (n-1)! + .. + .X_j \cdot j! + ... \\ ... + X_1 \cdot 1! + X_0 \cdot 0!, \quad (1)$$

де $j = 0,1,\ldots,n;\ 0 \le X_j \le j$.

Цей вираз має назву нумераційної, або числової

функції. Максимальне число у факторіальній системі має вигляд

$$F_{max} = (n+1)!-1. \quad (2)$$

Це випливає з наведених нижче перетворень числової функції, коли $X_j = j$. Тоді

$$F = F_{max} = (n+1-1)\cdot n!+((n-1)+1-1)\cdot(n-1)!+$$
$$+...+(j+1-1)\cdot j!+...+(1+1-1)\cdot 1!+(0+1-1)\cdot 0!=$$
$$=(n+1)!-n!+n!-(n-1)!+...+(j+1)!-j!+2!-1!+1-1=$$
$$=(n+1)!-1.$$

Мінімальне число 00…0…0 у факторіальній системі числення $F_{min} = 0$.

Дійсно, якщо всі розряди $X_l = 0$, то

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

Діапазон факторіальних чисел

$$P = F_{max}+1=(n+1)!. \quad (3)$$

При його знаходженні враховується, крім максимального числа, ще й нуль.

Основний матеріал

Перетворення факторіальних чисел в однорідні числа. Перетворення факторіального числа в однорідне виконується шляхом підстановки факторіального числа в числову (нумераційну) функцію (1) для факторіальних систем числення. При цьому виконуються всі вказані в цій функції операції множення і додавання.

Перетворення однорідних чисел у факторіальні. Перетворення числа із однорідної системи числення у факторіальну відбувається в такій послідовності.

Першим кроком буде ділення числа, яке перетворюється, на 1. Залишок у цьому випадку буде створювати цифру нульового розряду. Очевидно, що вона дорівнює нулю, а частка – числу, яке перетворюється. Якщо це число і відповідно знайдена частка дорівнюють 0 або 1, то тоді в перший розряд відповідного числа записується 0 або 1 і перетворення закінчується. Якщо перетворюване число і відповідна частка після першого кроку ділення буде більшою за 1, то наступним (другим) кроком буде ділення її на двійку, і тоді отриманий залишок від ділення буде записано як цифра першого розряду факторіального числа. Потім аналізується величина отриманої при діленні на двійку частки. Якщо вона менше за 3, то в другий розряд факторіального числа записується її значення, а якщо дорівнює або більша за 3, то виконується ділення цієї частки на 3. Далі під час наступних кроків виконуються щодо залишку й частки такі ж самі операції, як і під час другого кроку. Відмінність полягає в тому, що під час четвертого кроку виконується ділення відповідно на 4, на п'ятому на 5 і так продовжується до того часу, поки частка не стане менша за свого дільника. Потім ця частка виписується і справа наліво за нею виписуються всі отримані раніше залишки. Їх послідовність створює число, яке потрібно було знайти.

Побудова перестановок на основі факторіальних чисел. Факторіальні системи числення дають можливість для побудови широкого класу комбінаторних конфігурацій, серед яких особливе значення мають перестановки.

Розглянемо алгоритм їх побудови. Для того, щоб знайти відповідність між числом у факторіальній системі числення й перестановкою, необхідно цифру, яка стоїть у n-му розряді факторіального числа залишити без змін і вважати її першим елементом перестановки. Наступну цифру (n – 1)-го розряду факторіального числа необхідно порівняти з першим елементом перестановки і, якщо вона буде дорівнювати йому або буде більшою від нього, то треба збільшити цю цифру на 1, а якщо ні, то залишити її без змін. В обох випадках буде отриманий другий елемент перестановки.

Далі цифру (n – 2)-го розряду факторіального числа порівнюють спочатку з меншим за величиною елементом серед двох елементів раніше сформованої частини перестановки і якщо вона дорівнює йому або більше його, то збільшують її на 1, а якщо ні, залишають без змін. У цьому випадку третій елемент перестановки буде сформований.

Якщо ж факторіальна цифра була збільшена на 1, виконують порівняння збільшеної на 1 цифри (n – 2)-го розряду з елементом перестановки, що залишився, і потім, якщо вона дорівнює йому або більше за нього, знову збільшують її на 1. У противному разі залишають її без змін. Отримана таким чином збільшена цифра факторіального числа буде третім елементом перестановки.

Аналогічно виконують порівняння цифри (n – 3)-го розряду й далі всіх цифр факторіального числа, які ще не порівнювались, аж до нульового розряду числа з елементами перестановки, яка будується.

Тобто в загальному випадку спочатку виконують порівняння цифри факторіального числа з найменшим елементом серед уже знайдених елементів перестановки. Якщо ця цифра дорівнює цьому найменшому елементу або більша за нього, то тоді вона збільшується на одиницю. У противному разі вона стає черговим елементом перестановки. Збільшена ж на одиницю цифра факторіального числа далі порівнюється з найменшим елементом сформованої частини перестановки, до якої не належить елемент, щодо якого вже відбулося порівняння, і далі цикл повторюється до того часу, поки не буде сформований елемент перестановки. Далі вибирають наступну цифру факторіального числа і з її допомогою за наведеним вище правилом знаходять новий елемент перестановки, і так буде продовжуватися до останньої цифри факторіального числа.

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.

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

1) знизити часові витрати на генерування перестановок у довільному або заданому порядку і, таким чином, скоротити час шифрування інформації;

2) застосовувати розроблені алгоритми та системи генерування перестановок для захисту даних від несанкціонованого доступу шляхом їх перетворення на факторіальні числа та перестановки.

Список літератури

1. Борисенко О.А. Електронна система генерації перестановок на базі факторіальних чисел / О.А. Борисенко, І.А. Кулик, О.Є. Горячев // Вісник СумДУ. Технічні науки. – 2007. – № 1. – С. 183-188.

2. 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.

3. Рейнгольд Э. Комбинаторные алгоритмы: теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М.: Мир, 1980. – 477 с.