ПРЕОБРАЗОВАНИЕ ДВОИЧНЫХ КОДОВ В ПЕРЕСТАНОВКИ НА ОСНОВЕ ФАКТОРИАЛЬНОЙ СИСТЕМЫ СЧИСЛЕНИЯ

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

На практике распространена задача преобразования двоичных чисел в различные комбинаторные объекты. Среди этих объектов особое место занимают перестановки, так как они используются в задачах защиты информации от несанкционированного доступа, комбинаторной оптимизации, контроля ошибок [1]. Последняя задача особо интересна при контроле ошибок в массивах данных большой длины, так как в этом случае можно достичь высокой скорости передачи информации за счёт высокой помехоустойчивости [2].

В стандартах шифрования данных перестановки используются для перемешивания шифруемой информации. Среди задач комбинаторной оптимизации наиболее известна задача коммивояжёра, которая также требует получения перестановок, на которых ищется целевая функция. Перечисленные задачи требуют разработки эффективного метода преобразования двоичных чисел в перестановки, причём эта задача должна решаться для чисел большой длины. Исходя из этого, предлагается метод преобразования двоичных последовательностей в перестановки на основе факториальной системы счисления [1]. Суть метода состоит в том, что вначале двоичное число преобразуется в факториальное число, которое далее преобразуется в перестановку [1].

Предлагаются следующие усовершенствования данного метода. Для преобразования двоичных чисел в факториальные числа деление двоичных чисел на основания заменяется делением на факториалы оснований, а при преобразовании факториальных чисел в перестановки используется сортировка элементов перестановки. Это повышает быстродействие преобразований за счёт сокращения количества операций преобразования, а также за счёт получения готовых цифр факториального числа и элементов перестановки до окончания процесса преобразования.

1. О.А. Борисенко, І.А. Кулик, О.Є. Горячев, *Вісник СумДУ. Тех. н.* No**1,** 183 (2007).
2. А.Е. Горячев, *Вісник СумДУ. Тех. н.* No**3,** 169 (2009).