Секция 6

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.1

НУМЕРАЦИЯ ИНВОЛЮЦИЙ

Л. Н. Андреева, В. А. Потеряева

Пусть задано конечное множество X. Отображение $q : X \to X$ со свойством инволютивности $\forall x, y \in X(q(x) = y \Rightarrow q(y) = x)$ называется *инволюцией*. Представим инволюцию

$$q = \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

вектором $(q_1, q_2, \dots, q_n)$, где $n = |X|$. Зададим на множестве всех инволюций на X лексикографический порядок, согласно которому каждой инволюции можно сопоставить порядковый номер. Возникают две задачи: построить инволюцию по заданному номеру и вычислить номер заданной инволюции [1].

Приведём примеры того, где возникают эти задачи. Если инволюция используется в качестве ключа шифра и требуется построить случайный ключ, то можно случайно сгенерировать число (номер инволюции), а затем по номеру восстановить саму инволюцию. Можно изучать свойства инволюций (в том числе и криптографические), используя параллельные вычисления. Нумерация позволяет разбить все инволюции на классы требуемой мощности и строить и изучать эти классы параллельно.

В данной работе предлагаются алгоритмы решения поставленных задач и приводятся результаты их испытаний.

Алгоритм 1 построения инволюции по заданному номеру

Вход: n — длина инволюции, I — номер инволюции.

Выход: вектор $(q_1, q_2, \dots, q_n)$, представляющий I-ю (в лексикографическом порядке) инволюцию.

Число всех инволюций длины n вычисляется по рекуррентной формуле $r_n = r_{n-1} + (n-1)r_{n-2}$, где $r_1 = 1$ и $r_2 = 2$ [2].

1. $Y = \{1, 2, \dots, n\}$, $t = 1$.
2. Если $t = n$, то переход в п. 5.
3. Если $I \leqslant r_{n-t}$, то $q_{y_1} = y_1$, $Y = Y \setminus \{y_1\}$, $t = t + 1$ и переход в п. 2;
   иначе если $t < n - 1$, то $k = \lceil (I - r_{n-t})/r_{n-t-1} \rceil + 1$, иначе $k = 2$.
4. $q_t = y_k$.
   Если $q_t = t$, то $t = t + 1$, $I = I - r_{n-t} - (k-2)r_{n-t-1}$, $Y = Y \setminus \{y_k\}$,
   иначе $q_{y_k} = t$, $I = I - r_{n-t} - (k-2)r_{n-t-1}$, $t = t + 2$, $Y = Y \setminus \{y_k, t\}$ и переход в п. 2.
5. $q_t = y_1$.

Алгоритм 2 вычисления номера заданной инволюции

Вход: n — длина инволюции, вектор $(q_1, q_2, \dots, q_n)$, представляющий инволюцию.

Выход: I — искомый номер инволюции.

1. $I = 1$, $t = n$.
2. Если $q_1 = 1$, то $t = t - 1$,
   иначе $I = I + r_{t-1} + (q_1 - 2)r_{t-2}$, $t = t - 2$.
3. $i = 1$.
4. Если $i = n$, то переход в п. 6,
   иначе если $q_i = i$, то $t = t - 1$ и переход в п. 5,
   иначе если $q_i > i$, то $I = I + r_{t-1} + (q_i - n + t - 1)r_t$, $t = t - 2$ и переход в п. 5.
5. $i = i + 1$ и переход в п. 4.
6. I — результат.

Приведённые алгоритмы реализованы программно на языке Си++ с использованием процессора Intel(R) Pentium(R) 4CPU, работающего с частотой 300 ГГц. В таблице приведено усреднённое по 10000 случайных примеров время работы алгоритмов для $25 \leqslant n \leqslant 31$.

n	Время работы алгоритма 1, с	Время работы алгоритма 2, с
25	0,0055	0,001261
26	0,008729	0,001902
27	0,013972	0,0032
28	0,022783	0,005199
29	0,037049	0,008263
30	0,057267	0,013038
31	0,091838	0,021003

ЛИТЕРАТУРА

1. *Тимошевская Н. Е.* Разработка и исследование параллельных комбинаторных алгоритмов // Прикладная дискретная математика. 2009. № 2(4). С. 96–103.
2. *Андреева Л. Н.* К криптоанализу инволютивных шифров инволюционной подстановки // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 43–44.

УДК 519.61

ОТСУТСТВИЕ ДИНАМИЧНОСТИ У МЕТОДА РЕШЕТА ЧИСЛОВОГО ПОЛЯ

Ю. Л. Зачёсов, А. М. Гришин

Под динамичностью метода будем понимать способность сохранять свои основные характеристики при существенном изменении входных параметров. Основными характеристиками являются трудоёмкость выполнения алгоритма, ограничения на требуемые вычислительные ресурсы и другие параметры. Характеристика входных параметров — это, как правило, их длина.

На сайте [1] можно найти данные об изменении трудоёмкости выполнения этапов алгоритма факторизации методом квадратичного решета [2] и NFS [3] с 1990 г. в зависимости от размера модуля факторизации. По представленным данным видно, что рассматриваемые алгоритмы требуют для своего выполнения существенных вычислительных ресурсов. Трудоёмкость выполнения алгоритма измеряется в MIPS years или в 1 ГГц CPU years. На сайте [4] можно посмотреть динамику изменения характеристик лучших мировых суперкомпьютеров. Их мощность измеряется в TFlop/s. Для того чтобы можно было сравнивать предлагаемые ресурсы и потребность в них алгоритмов, переведём всё в оценки, измеряемые в 10^k условных операций в секунду (опер/с),