УДК 621.3.037.37

АЛГОРИТМ ГЕНЕРИРОВАНИЯ ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ НА ОСНОВЕ МИНИМАЛЬНЫХ СИСТЕМ КОДООБРАЗУЮЩИХ ОГРАНИЧЕНИЙ

И.А. Кулик, В.Б. Чередниченко*, С.В. Костель
Сумский государственный университет, г. Сумы
**Сумский филиал Харьковского национального университета внутренних дел, г. Сумы*

В статье предлагается новый алгоритм генерирования двоичных биномиальных чисел на основе минимальных систем кодообразующих ограничений. Минимальные системы ограничений для биномиальных чисел были выведены из биномиальной числовой функции. Разработанный алгоритм является более быстродействующим по сравнению с алгоритмами биномиального счета.

ПОСТАНОВКА ПРОБЛЕМЫ

На сегодняшний день генерирование двоичных биномиальных чисел, используемых в задачах комбинаторного кодирования и оптимизации, возможно только или табличным способом, или на основе существующих процедур биномиального счета. При этом под биномиальным счетом понимается последовательный перебор биномиальных чисел в возрастающем или убывающем порядке, в котором численное значение (номер) последующей биномиальной комбинации отличается от предыдущей на единицу [1]. Указанные два способа генерирования биномиальных чисел отличаются крайними граничными значениями таких сложностных параметров, как время получения необходимого биномиального числа и объем аппаратно-программных затрат, требуемый при практической реализации.

Табличный способ заключается в том, что по входному двоичному номеру всего за один временной шаг получаем из таблицы искомое двоичное биномиальное число. Но при больших параметрах n и k двоичных биномиальных чисел практическое применение такого способа является весьма затруднительным из-за значительного объема памяти, требуемой для хранения таблицы чисел. Значение емкости памяти здесь находится в полиномиальной зависимости от числового диапазона $P = C_n^k$ биномиальной системы счисления.

С другой стороны, способ последовательного перебора двоичных биномиальных чисел для нахождения искомого числа не требует столь существенных аппаратно-программных затрат. Но генерирование одного или нескольких чисел в рамках данного способа приводит к значительным временным издержкам, объем которых также растет полиномиально в зависимости от параметров n и k. В этом случае максимальное число шагов без учета времени на исполнение инициализирующих команд в лучшем случае может быть равным значению C_n^k.

Все эти вышеприведенные трудности по применению существующих способов порождения двоичных биномиальных чисел снижают эффективность методов комбинаторного кодирования и оптимизации, в которых они используются, и сдерживают их широкое распространение [2, 3]. Таким образом, актуальной является задача разработки алгоритмов генерирования двоичных биномиальных чисел, сложностные характеристики которых удовлетворяют следующим требованиям:

– максимальное число $N_{\max}$ шагов для получения двоичного биномиального числа: $N_{\max} < C_n^k$;
– объем V аппаратно-программных затрат при реализации алгоритмов на практике: $V < r_{\max} C_n^k$, где $r_{\max}$ – максимальная длина двоичного биномиального числа.

1 ВЫВОД МИНИМАЛЬНОЙ СИСТЕМЫ КОДООБРАЗУЮЩИХ ОГРАНИЧЕНИЙ ДЛЯ ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

Пусть имеется полное множество X двоичных биномиальных чисел, задаваемых двоичной биномиальной системой счисления с параметрами n и k. Мощность такого полного множества $P = |X| = C_n^k$. В соответствии с числовой функцией десятичный количественный эквивалент F_j двоичного биномиального числа $X_j \in X$, $X_j = x_1 x_2 \ldots x_i \ldots x_r$ определяется как

$$F_j = \operatorname{dec} X_j = \sum_{i=1}^{r} x_i C_{n-i}^{k-q_i}, \qquad (1)$$

где $j = \overline{1, C_n^k}$, x_i – двоичные разряды числа r – длина двоичного биномиального числа,

$$q_i = \sum_{t=1}^{i-1} x_t . \qquad (2)$$

Системы ограничений, определяющих двоичные биномиальные числа, выглядят следующим образом [1]:

$$\begin{cases} n-k = r-q \\ 0 \le q \le k-1 \\ x_r = 0 \end{cases}, \qquad (3)$$

$$\begin{cases} k \le r \le n-1 \\ q = k \\ x_r = 1 \end{cases}. \qquad (4)$$

Биномиальные числа, удовлетворяющие системе (3) ограничений, составляют первый класс A чисел. При этом в зависимости от значения числа q содержащихся в числах единиц различают подклассы A_q:

$$A = \bigcup_{\alpha=0}^{k-1} A_q, \; A_q \cap A_d = \varnothing, \; 0 \le q, d \le k-1, \; q \ne d$$

Биномиальные числа, удовлетворяющие системе (4) ограничений, составляют второй класс B чисел. При этом в зависимости от значения числа l содержащихся в числах нулей различают подклассы B_l:

$$B = \bigcup_{\beta=0}^{n-k-1} B_l, \; B_l \cap B_c = \varnothing, \; 0 \le l, c \le n-k-1, \; l \ne c$$

Решение сформулированной задачи по разработке нового алгоритма предлагается на основе рассмотрения систем ограничений прежде всего как систем, порождающих биномиальные числа. До проведения данной

научной работы приведенные системы ограничений использовались только для проверки соответствия двоичных комбинаций классу двоичных биномиальных чисел [1]. В этой связи числовую функцию (1) двоичной биномиальной системы счисления необходимо проанализировать с точки зрения функции, порождающей числа в соответствии с ограничениями, которые она на них накладывает. Результаты такого анализа составляют две нижеследующие теоремы.

Теорема 1 Максимальная длина $r_{\max}$ двоичных биномиальных чисел с параметрами n и k:

$$r_{\max} = n - 1 . \tag{5}$$

Доказательство. В соответствии с числовой функцией (1) двоичной биномиальной системы счисления с параметрами n и k значения весовых коэффициентов должны быть

$$C_{n-i}^{k-q_i} > 0 ,$$

что возможно только при $0 \le k - q_i \le n - i$, где $i = 0, 1, \ldots, r$. Данное неравенство может выполняться, когда $i = r = n$, то есть возможное максимальное значение длины r, большее $n-1$, может быть $r_{\max} = n$. Тогда согласно (2) существуют два случая:

1) $0 \le q_n \le k$, если $x_n = 0$;

2) $0 \le q_n \le k - 1$, если $x_n = 1$.

Для первого случая последнее слагаемое функции F для любых значений q_n из заданного диапазона всегда равно нулю:

$$x_n C_{n-n}^{k-q_n} = 0 \cdot C_{n-n}^{k-q_n} = 0 .$$

Для второго случая равенство нулю последнего слагаемого функции F является следствием $C_0^{k-q_n} = 0$ для всех $0 \le q_n \le k - 1$ [5]:

$$x_n C_{n-n}^{k-q_n} = 1 \cdot C_{n-n}^{k-q_n} = 1 \cdot C_0^{k-q_n} = 0 .$$

Следовательно, ни в первом, ни во втором случаях последнее слагаемое не вносит никакого вклада в значение F двоичного биномиального числа. Тогда длины двоичных биномиальных чисел $r \le n - 1$, то есть $r_{\max} = n - 1$.

Теорема доказана.

Теорема 2 Системы кодообразующих ограничений для двоичных биномиальных чисел имеют вид:

$$\begin{cases} l = n - k \\ x_r = 0 \end{cases} , \tag{6}$$

$$\begin{cases} q = k \\ x_r = 1 \end{cases} \tag{7}$$

где q и l – количество двоичных единиц и нулей в двоичном биномиальном числе соответственно.

Доказательство. Воспользовавшись условием симметрии для чисел сочетаний [5], весовой коэффициент общего вида функции (1) можно представить как

$$C_{n-i}^{k-q_i} = C_{n-i}^{n-i-(k-q_i)}. \qquad (8)$$

Следовательно, для получения весовых коэффициентов (8) числовой функции (1), больших 0 (только в этом случае имеет смысл наличие соответствующих разрядов в записи биномиального числа), необходимо выполнение неравенства

$$k - q_i \le n - i \text{ или } n - i - k + q_i \le n - i. \qquad (9)$$

После выполнения преобразований, целью которых является перенос переменных величин, зависящих от номера разряда, в левые части, а постоянных величин в правые части неравенств (9), в результате получаем

$$\begin{cases} i - q_i \le n - k \\ q_i \le k \end{cases}. \qquad (10)$$

С целью выявления случаев выполнения неравенств (10) для двоичных биномиальных чисел проанализируем их левые части. Следует отметить, что разность $i - q_i$ представляет собой число l_i нулей от первого разряда до $(i-1)$-го включительно, то есть

$$l_i = i - q_i = \sum_{t=1}^{i-1} \overline{x}_t .$$

Вид первого и второго неравенств (10) показывает, что в области задания номера i разряда и суммы q_i возможны два случая – генерирование $(n-k)$-го нуля и генерирование k-й единицы.

В первом случае – генерирование $(n-k)$-го нуля – при формировании двоичного биномиального числа после некоторого $x_z = 1$, $z < i \le n-1$ порождаются только двоичные нули:

$$\begin{cases} x_z = 1 \\ z < i \le n-1 \\ q_i = \text{const} \end{cases}.$$

Тогда из первого неравенства (10) следует

$$r - q_r = n - k.$$

Это означает, что в двоичном биномиальном числе содержится постоянное число $l = n - k$ нулей и число заканчивается нулем $x_r = 0$.

Следовательно, для первого случая получается следующая система кодообразующих ограничений:

$$\begin{cases} l = n - k \\ x_r = 0 \end{cases}.$$

Во втором случае – генерирование k-й единицы – при формировании двоичного биномиального числа после некоторого $x_z = 0$, $z < i \le n-1$ порождаются только двоичные единицы:

$$\begin{cases} x_z = 0 \\ z < i \le n-1 \\ q_{i+1} = q_i + 1 \end{cases}.$$

Тогда из второго неравенства (10) следует

$$q_r = k - 1 .$$

Это означает, что двоичное биномиальное число заканчивается единицей $x_r = 1$ и в числе присутствует постоянное число $q = q_r + x_r = q_r + 1 = k$ единиц.

Таким образом, для второго случая имеем следующую систему кодообразующих ограничений:

$$\begin{cases} q = k \\ x_r = 1 \end{cases}.$$

В результате кодобразующие ограничения, генерирующие вместе с числовой функцией двоичные биномиальные числа с параметрами n и k:

$$\begin{cases} l = n - k \\ x_r = 0 \end{cases} \text{ и } \begin{cases} q = k \\ x_r = 1 \end{cases}.$$

Теорема доказана.

Следствие 1 Минимальная длина $r^0_{\min}$ двоичных биномиальных чисел, удовлетворяющих ограничениям (6):

$$r^0_{\min} = n - k .$$

Следствие 2 Минимальная длина $r^1_{\min}$ двоичных биномиальных чисел, удовлетворяющих ограничениям (7):

$$r^1_{\min} = k .$$

Следствие 3 Минимальная длина $r_{\min}$ двоичных биномиальных чисел с параметрами n и k:

$$r_{\min} = \min\left(r^0_{\min}, r^1_{\min}\right) = \min\left(n - k, k\right).$$

Приведенные минимальные (неизбыточные) системы (6, 7) кодобразующих ограничений позволяют построить новый алгоритм генерирования двоичных биномиальных чисел. Из этих систем ограничений следует, что неравномерные двоичные биномиальные числа представляют собой конкатенацию сочетаний нулей и единиц и последнего, имеющего фиксированное значение, разряда x_r (для первого класса $x_r = 0$, для второго – $x_r = 1$). Согласно первой системе (6) ограничений биномиальные числа из подкласса A_q могут быть получены путем присоединения справа двоичного нуля к сочетанию q двоичных единиц по $r = l + q - 1$ разрядам, $0 \le q \le k - 1$. В соответствии со второй системой (7) биномиальные числа из подкласса B_l получаются, если справа к сочетанию $q = k - 1$ двоичных единиц по $r = l + k - 1$ разрядам добавить двоичную единицу, $0 \le l \le n - k - 1$.

В общем формальном виде генерирование неравномерных двоичных биномиальных чисел X_j по вышеприведенному правилу выглядит следующим образом:

– для системы (6) кодообразующих ограничений:

$$X_i\left[n-k+q,q\right]=E\left[n-k+q-1,q\right]++\ 0\,, \tag{11}$$

– для системы (7) кодообразующих ограничений:

$$X_i\left[l+k,k\right]=E\left[l+k-1,k-1\right]++\ 1\,, \tag{12}$$

где "++" – операция присоединения (конкатенации);

$E\left[n-k+q-1,q\right]$ – сочетание q двоичных единиц длины $n-k+q-1$ разрядов;

$E\left[l+k-1,k-1\right]$ – сочетание $k-1$ двоичных единиц длины $l+k-1$ разрядов.

Практическая реализация операций (11) и (12) в виде алгоритма выглядит следующим образом.

1 [Задание параметров n и k генерируемых двоичных биномиальных чисел, $n\geq 2$, $1\leq k\leq n-1$].

$$n'\leftarrow n\,,\ k'\leftarrow k\,.$$

2 [Вычисление максимальной длины $r_{\max}$ двоичных биномиальных чисел X_j].

$$\max r\leftarrow n'-1\,.$$

3 [Переход по типу класса биномиальных чисел: если $x_r=0$, то переход к формированию чисел первого класса A, если $x_r=1$, то переход к формированию чисел второго класса B, где AC – счетчик шагов алгоритма].

Если $x_r\leftarrow 1$, то $AC\leftarrow 12$. В противном случае $AC\leftarrow 4$.

4 [Начало генерирования двоичных биномиальных чисел $X_j\in A$ и задание типа подкласса A_q, $0\leq q\leq k-1$].

$$q'\leftarrow q\,.$$

5 [Вычисление фиксированного числа l нулей в генерируемых числах $X_j\in A_q\subset A$].

$$l'\leftarrow n'-k'\,.$$

6 [Вычисление числа P двоичных биномиальных чисел $X_j\in A_q$].

$$P\leftarrow C^{q'}_{(l'-1)+q'}\,.$$

7 [Вычисление длины z соответствующей двоичной равновесной комбинации].

$$z'\leftarrow\left(l'-1\right)+q'\,.$$

8 [Формирование двоичной равновесной комбинации длины z и числом q единиц].

$$E\leftarrow x_1x_2\ldots x_z\,.$$

9 [Формирование соответствующего двоичного биномиального числа $X_j\in A_q$].

$$X \leftarrow E++\ 0 = x_1 x_2 \ldots x_z 0 .$$

10 [Декрементация переменной P – общего количества двоичных биномиальных чисел подкласса A_q].

$$P \leftarrow P - 1 .$$

11 [Проверка факта генерирования последнего двоичного биномиального числа $X_j \in A_q$].

Если $P = 0$, то $AC \leftarrow 19$. В противном случае $AC \leftarrow 8$.

12 [Начало генерирования двоичных биномиальных чисел $X_j \in B$ и задание типа подкласса B_l, $0 \le l \le n - k - 1$].

$$l' \leftarrow l .$$

13 [Вычисление числа P двоичных биномиальных чисел подкласса $X_j \in B_l$].

$$P \leftarrow C^{l'}_{(k-1)+l'} .$$

14 [Вычисление длины z соответствующей двоичной равновесной комбинации].

$$z' \leftarrow \left(k-1\right) + l' .$$

15 [Формирование двоичной равновесной комбинации длины z и числом $\left(k-1\right)$ единиц].

$$E \leftarrow x_1 x_2 \ldots x_z .$$

16 [Формирование соответствующего двоичного биномиального числа $X_j \in B_l$].

$$X \leftarrow E++\ 1 = x_1 x_2 \ldots x_z 1 .$$

17 [Декрементация переменной P – общего количества двоичных биномиальных чисел подкласса B_l].

$$P \leftarrow P - 1 .$$

18 [Проверка факта генерирования последнего двоичного биномиального числа $X_j \in B_l$].

Если $P = 0$, то $AC \leftarrow 19$. В противном случае $AC \leftarrow 15$.

19 Останов.

Приведенный алгоритм за цикл своей работы позволяет получить двоичные биномиальные числа, принадлежащие заданным подклассам A_q или B_l. При этом получаемые биномиальные числа будут располагаться в лексикографическом порядке, но в рамках определенного подкласса. По сравнению с алгоритмом последовательного перебора двоичных биномиальных чисел [1] предлагаемый позволяет существенно сократить время получения необходимого биномиального числа. Для получения двоичного биномиального числа максимальное время работы приведенного алгоритма составляет $N_{\max} = \max\left(C^{q'}_{(l'-1)+q'}, C^{l'}_{(k-1)+l'}\right)$, что

значительно меньше значения C_n^k шагов. Поскольку алгоритм не использует числовые таблицы, то и объем V аппаратно-программных затрат при его практической реализации будет также меньше $r_{\max} C_n^k$. Следовательно, предложенный алгоритм генерирования двоичных биномиальных чисел удовлетворяет всем тем требованиям, которые необходимы для повышения эффективности методов комбинаторного кодирования и оптимизации, где эти числа используются.

ВЫВОДЫ

По результатам данной научной работы предложен новый алгоритм генерирования биномиальных чисел, основанный на том, что неравномерные двоичные биномиальные числа представляют собой конкатенацию сочетаний нулей и единиц и последнего, имеющего фиксированное значение, разряда. При равных объемах аппаратно-программных затрат полученный алгоритм является более быстродействующим по сравнению с известными алгоритмами биномиального счета. Кроме того, он предоставляет возможность получения биномиальных чисел, принадлежащих только одному подклассу чисел с одинаковым числом единиц или нулей. Таким образом, применение предлагаемого алгоритма для генерирования биномиальных чисел в методах комбинаторного кодирования и оптимизации позволит повысить их эффективность с точки зрения времени проведения операций и обеспечит их большую гибкость к изменяемым входным данным.

Следует отметить, что получение данного алгоритма стало возможным с выводом минимальных (неизбыточных) систем кодообразующих ограничений на основе математического анализа допустимых значений весовых коэффициентов биномиальной числовой функции.

SUMMARY

ALGORITHMS OF GENERATION OF BINARY BINOMIAL NUMBERS ON BASIS OF MINIMAL SYSTEMS OF CODE-FORMING RESTRICTIONS

Kulik I.A. ; Cherednichenko V.B. *; Kostel S.V.
Sumy State University
**Sumy Branch of Kharkov National University of Internal Affairs*

In the paper a new algorithm is proposed for generating binary binomial numbers on basis of minimal systems of code-forming restrictions. The minimal systems of restrictions are obtained of a binomial number function. The developed algorithm is more fast-acting in comparison with algorithms of binomial count.

СПИСОК ЛИТЕРАТУРЫ

1. Борисенко А.А. Биномиальный счет. Теория и практика: Монография. – Сумы: ИТД "Университетская книга", 2004. – 170 с.
2. Чередниченко В.Б. Метод сжатия двоичных кодов на основе биномиальных чисел // Вісник СумДУ. – 2006. – № 4(88). – С. 61–68.
3. Борисенко А.А. Защита информации на основе сжатия // Вісник СумДУ. – 2006. – № 4(88). – С. 53–55.
4. Кнут Д. Искусство программирования для ЭВМ. Т.1. Основные алгоритмы. – М.: Изд-во "Мир", 1976. – 736 с.

***Кулик И.А.**, канд. техн. наук, доцент;*
***Чередниченко В.Б.**, ст. преподаватель;*
***Костель С.В.**, аспирант*

Поступила в редакцию 30 мая 2008 г.