В. В. Гоцуленко, Формализация комбинаторных чисел в терминах целочисленных решений систем линейных диофантовых уравнений, *ПДМ. Приложение*, 2014, выпуск 7, 157–160

тей, нахождение наибольшей клики, вычисление хроматического числа, определение наибольшего независимого множества вершин графа, поиск наименьшего пополнения графа до хордального, распознавание класса совершенных графов и др. Большинство из этих задач являются NP-трудными.

В работе атомарное представление графа применено к двум оптимизационным задачам: вычислению кратчайших путей для всех пар вершин взвешенного графа (All-Pairs Shortest-Path, APSP) и нахождению наибольшей клики графа (Maximum-Clique-Problem, MCP). Первая задача полиномиально разрешимая, а вторая NP-трудная. Совместное использование алгоритма Флойда — Уоршолла [7] и атомарного представления входного n-вершинного графа позволяет находить точное решение задачи APSP за время $O(nk^3)$. Применение алгоритма Уилфа [7] к каждому атому и связывание решений, полученных для всех атомов входного графа, приводит к точному решению задачи MCP за время $O(n \cdot 1{,}39^k)$. Заметим, что в обоих случаях время нахождения решения линейно зависит от n. Кроме того, чем меньше значение k, т. е. чем более разреженным является входной граф, тем быстрее работает алгоритм.

Таким образом, предложенный декомпозиционный подход даёт возможность создавать алгоритмы, способные за реальное время обрабатывать разреженные графы большой размерности.

ЛИТЕРАТУРА

1. *Gardiner E., Willett P., and Artymiuk P.* Graph-theoretic techniques for macromolecular docking // J. Chem. Inf. Comput. 2000. No. 40. P. 273–279.
2. *Broder A., Kumar R., Maghoul F., et al.* Graph structure in the Web // Comput. Networks. 2000. V. 33. P. 309–320.
3. *Boginski V., Butenko S., and Pardalos P. M.* Mining market data: A network approach // Comput. & Operat. Res. 2006. No. 33. P. 3171–3184.
4. *Колчин В. Ф.* Случайные графы. М.: Физматлит, 2004.
5. *Быкова В. В.* О разложении гиперграфа кликовыми минимальными сепараторами // Журнал Сибирского федерального университета. Математика и физика. 2012. № 1(5). С. 36–45.
6. *Быкова В. В.* FPT-алгоритмы на графах ограниченной древовидной ширины // Прикладная дискретная математика. 2012. № 2(16). С. 65–78.
7. *Емеличев В. А., Мельников О. И., Сарванов В.И., Тышкевич Р. И.* Лекции по теории графов. М.: Книжный дом «ЛИБРОКОМ», 2012.

УДК 519.1

ФОРМАЛИЗАЦИЯ КОМБИНАТОРНЫХ ЧИСЕЛ В ТЕРМИНАХ ЦЕЛОЧИСЛЕННЫХ РЕШЕНИЙ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ

В. В. Гоцуленко

Рассмотрены некоторые обобщения числа размещений с повторениями при различных типах ограничений. Подсчёт данных комбинаторных чисел приводит к определению числа целых неотрицательных решений систем линейных диофантовых уравнений при соответствующих дополнительных ограничениях. Получены производящие функции и интегральные формулы для вычисления введённых

комбинаторных чисел и рассмотрены различные задачи, которые решаются с их применением.

Ключевые слова: *комбинаторные числа, системы линейных диофантовых уравнений, производящие функции.*

В работе вводятся в рассмотрение комбинаторные числа размещений с повторениями при различных дополнительных ограничениях [1]. Формулировка достаточно общей комбинаторной задачи, приводящей к размещениям с повторениями при рассматриваемых ограничениях, может быть следующей [2]. Предположим, что имеется N различных ящиков, в каждом из которых находится достаточно большое (например, бесконечное) число конфет q различных видов. Конфеты упакованы по коробкам. Известно, что в i-м ящике $(i = 1, \ldots, N)$ конфеты j-го вида $(j = 1, \ldots, q)$ упакованы в коробки вместительностью по $r_{i,s}^{j}$ $(s = 1, \ldots, n_{ij})$ штук, где n_{ij} — число объёмов коробок i-го ящика, в которых находятся конфеты j-го вида. Путь также имеется R детей, которым необходимо дать конфеты из этих N ящиков. При этом k-му ребёнку $(k = 1, \ldots, R)$ необходимо дать ровно m_{jk} конфет j-го вида. Необходимо, чтобы суммарное число конфет всех коробок, взятых из i-го ящика для k-го ребёнка, было равно p_{ik}, где p_{ik} — фиксированные целые неотрицательные числа. Также требуется, чтобы суммарное число всех конфет j-го вида, розданных всем детям из i-го ящика, было равно наперёд заданному целому неотрицательному числу d_{ij}. Любое допустимое распределение конфет q видов R детям из N различных ящиков будем называть обобщённым q-размещением из N по R при жёстких ограничениях.

Если безразлично, сколько конфет каждого вида необходимо раздать детям из каждого ящика, то допустимое распределение конфет q видов R детям из N различных ящиков будем называть обобщённым q-размещением из N по R при мягких ограничениях. В последнем случае будем предполагать, что для k-го ребёнка $(k = 1, \ldots, R)$ задано число конфет m_k, которые необходимо ему дать из всех N ящиков. Также предполагается заранее заданным p_i — суммарное число конфет, которое разрешается взять из i-го ящика $(i = 1, \ldots, N)$.

Как в первом, так и во втором случаях на выборку конфет из ящиков возможны различные ограничения. Рассмотрим следующие три типа ограничений:

A) Конфеты во всех ящиках находятся не в коробках, а россыпью (т. е. $r_{i,s}^{j} = 1$ для всех i, j, s) и из каждого ящика разрешается брать любое допустимое число конфет.

B) Из каждого ящика разрешается брать не более одной допустимой коробки конфет каждого вида.

C) Разрешается брать любое число допустимых коробок конфет каждого вида из любого ящика.

Обозначим через x_{ijk} число конфет j-го вида, взятых из i-го ящика k-му ребёнку. Тогда при жёстких ограничениях приходим к следующей системе линейных диофантовых уравнений $(i = 1, \ldots, N,\ j = 1, \ldots, q,\ k = 1, \ldots, R)$:

$$\sum_{i=1}^{N} x_{ijk} = m_{jk};\ \ \sum_{j=1}^{q} x_{ijk} = p_{ik};\ \ \sum_{k=1}^{R} x_{ijk} = d_{ij}. \tag{1}$$

При мягких ограничениях получается система уравнений

$$\sum_{i=1}^{N}\sum_{j=1}^{q} x_{ijk} = m_k;\ \ \sum_{j=1}^{q}\sum_{k=1}^{R} x_{ijk} = p_i,\ i = 1, \ldots, N,\ k = 1, \ldots, R. \tag{2}$$

В случае «B» областью допустимых значений для (1) и (2) являются множества

$$x_{ijk} \in \left\{r_{i,s}^{j} : 1 \leqslant s \leqslant n_{ij}\right\} \cup \{0\},\ i = 1, \ldots, N,\ j = 1, \ldots, q,\ k = 1, \ldots, R. \tag{3}$$

Введём в рассмотрение множества целых чисел ($i = 1, \ldots, N,\ j = 1, \ldots, q$)

$$I_{ij} = I_{ij}\left(\left\{r_{is}^{j}\right\}_{N \times n_{ij}}^{q}\right) = \left\{\sum_{s=1}^{n_{ij}} \alpha_s r_{i,s}^{j} : \alpha_s \in \mathbb{N} \cup \{0\},\ s = 1, \ldots, n_{ij}\right\},$$

$$J_{ij} = J_{ij}\left(P, \left\{r_{is}^{j}\right\}_{N \times n_{ij}}^{q}\right) = \left\{r \in I_{ij}\left(\left\{r_{is}^{j}\right\}_{N \times n_{ij}}^{q}\right) : r \leqslant P\right\},\ P \in \mathbb{N}.$$

Тогда для задачи «C» множествами допустимых решений для (1) и (2) являются

$$x_{ijk} \in J_{ij}\left(\min\left\{m_{jk}, p_{ik}, d_{ij}\right\}, \left\{r_{is}^{j}\right\}_{N \times n_{ij}}^{q}\right),\ i = 1, \ldots, N,\ j = 1, \ldots, q,\ k = 1, \ldots, R. \tag{4}$$

Таким образом, вычисление введённых комбинаторных чисел сводится к определению числа целых неотрицательных решений систем уравнений (1) или (2) без ограничений, а также при ограничениях (3) или (4). Установлено, что число всех целых неотрицательных решений системы уравнений (1) равно коэффициенту при $t_1^{b_1} t_2^{b_2} \ldots t_K^{b_K}$ в разложении по возрастающим показателям степеней $t_1^{r_1} t_2^{r_2} \ldots t_K^{r_K}$ следующей производящей функции ($\alpha = 1, \ldots, K, \beta = 1, \ldots, M$):

$$\Psi\left(t_1, t_2, \ldots, t_K\right) = \prod_{\beta=1}^{M}\left(1 - \prod_{\alpha=1}^{K} t_\alpha^{a_{\alpha\beta}}\right)^{-1},\ \text{где } M = NqR,\ K = Nq + qR + NR, \tag{5}$$

$$\nu_{n_1,n_2}(r) = (r_1, r_2),\ r_1 = 1 + \left[\frac{r-1}{n_2}\right],\ r_2 = 1 + n_2\left\{\frac{r-1}{n_2}\right\},\ r = 1, \ldots, n_1 n_2,$$

$$\psi(\beta) = (i, j, k), \psi_1(\beta) = i, \psi_2(\beta) = j, \psi_3(\beta) = k, \psi_{21}(\beta) = (j, k), \psi_{22}(\beta) = (i, k),$$

$$\psi_{23}(\beta) = (i, j), i = 1 + \left[\frac{1}{q}\left[\frac{\beta-1}{R}\right]\right], j = 1 + q\left\{\frac{1}{q}\left[\frac{\beta-1}{R}\right]\right\}, k = 1 + R\left\{\frac{\beta-1}{R}\right\}.$$

$$a_{\alpha\beta} = \begin{cases} 1,\ \text{если } 1 \leqslant \alpha \leqslant qR,\ \nu_{q,R}(\alpha) = \psi_{21}(\beta), \\ 1,\ \text{если } qR + 1 \leqslant \alpha \leqslant qR + NR,\ \nu_{N,R}(\alpha - qR) = \psi_{22}(\beta), \\ 1,\ \text{если } qR + NR + 1 \leqslant \alpha \leqslant qR + NR + Nq,\ \nu_{N,q}(\alpha - qR - NR) = \psi_{23}(\beta), \\ 0 \text{ в остальных случаях;} \end{cases}$$

$$b_\alpha = \begin{cases} m_{jk},\ \text{если } 1 \leqslant \alpha \leqslant qR,\ \nu_{q,R}(\alpha) = (j, k), \\ p_{ik},\ \text{если } qR + 1 \leqslant \alpha \leqslant qR + NR,\ \nu_{N,R}(\alpha - qR) = (i, k), \\ d_{ij},\ \text{если } qR + NR + 1 \leqslant \alpha \leqslant qR + NR + Nq,\ \nu_{N,q}(\alpha - qR - NR) = (i, j). \end{cases}$$

Установлено также, что число всех целочисленных решений системы уравнений (1) при условии (3) равно коэффициенту при $t_1^{b_1} t_2^{b_2} \ldots t_K^{b_K}$ в разложении по возрастающим показателям степеней $t_1^{r_1} t_2^{r_2} \ldots t_K^{r_K}$ следующей производящей функции:

$$\Psi\left(t_1, t_2, \ldots, t_K\right) = \prod_{\beta=1}^{M}\left(1 + \sum_{k=1}^{n_{\psi_1(\beta),\psi_2(\beta)}} \prod_{\alpha=1}^{K} t_\alpha^{a_{\alpha\beta} r_{\psi_1(\beta),k}^{\psi_2(\beta)}}\right). \tag{6}$$

Аналогично, производящей функцией для определения числа целых неотрицательных решений системы уравнений (1) при ограничениях (4) является функция

$$\Psi\left(t_1, t_2, \ldots, t_K\right) = \prod_{\beta=1}^{M} \sum_{r \in J_{\psi_{23}(\beta)}\left(D_{\psi(\beta)}, \left\{r_{is}^{j}\right\}_{N \times n_{ij}}^{q}\right)} \prod_{\alpha=1}^{K} t_\alpha^{a_{\alpha\beta} r}. \tag{7}$$

Полагая в (5)–(7) $K = R + N$, $M = RN$,

$$a_{\alpha\beta} = \begin{cases} 1, \text{ если } 1 \leqslant \alpha \leqslant R,\ \psi_3(\beta) = \alpha, \\ 1, \text{ если } R+1 \leqslant \alpha \leqslant R+N,\ \psi_1(\beta) = \alpha - R, \\ 0 \text{ в остальных случаях;} \end{cases}$$

$$b_\alpha = \begin{cases} m_i, \text{ если } 1 \leqslant \alpha \leqslant R,\ \alpha = i, \\ p_k, \text{ если } R+1 \leqslant \alpha \leqslant R+N,\ \alpha - R = k, \end{cases}$$

получим производящие функции для числа целых неотрицательных решений системы (2) без ограничений, а также соответственно при ограничениях (3) и (4).

ЛИТЕРАТУРА

1. *Яблонский С. В.* Введение в дискретную математику. М.: Наука, 1986. 384 с.
2. *Гоцуленко В. В.* Формула для числа сочетаний с повторениями при ограничениях и её применение // Прикладная дискретная математика. 2013. № 2(20). С. 71–77.

УДК 519.6

АЛГОРИТМ ГЕНЕРАЦИИ ПАРЫ ПРОСТЫХ ЧИСЕЛ СПЕЦИАЛЬНОГО ВИДА

К. Д. Жуков, А. С. Рыбаков

Рассматривается алгоритм генерации пары простых чисел p и q, таких, что числа $g = \frac{1}{2}(p-1, q-1)$ и $h = \frac{1}{2g}(pq-1)$ также простые. Такие простые числа впервые рассмотрены в 2006 г. М. Дж. Хинеком в связи с предложенной им модификацией криптосистемы RSA, устойчивой к атакам на малые секретные экспоненты. Приводятся экспериментальные данные о времени работы алгоритма.

Ключевые слова: *простые специального вида, Common Prime RSA.*

В 2006 г. М. Дж. Хинек предложил вариант криптосистемы RSA, устойчивой к атакам на малую секретную экспоненту, которая была названа Common Prime RSA. Простые сомножители p и q модуля Common Prime RSA выбираются такими, чтобы числа

$$g = \frac{1}{2}(p-1, q-1), \quad h = \frac{1}{2g}(pq-1) \tag{1}$$

были также простыми, причём число g должно быть достаточно большим.

Система Common Prime RSA не получила распространения. Этот факт связан с малым количеством публикаций по её анализу. Большинство атак на данную разновидность RSA были также предложены М. Дж. Хинеком (см., например, [2]). Не способствует распространению и отсутствие острой необходимости использовать малые секретные экспоненты; другим сдерживающим фактором использования Common Prime RSA является долгая генерация ключей.

Простейшая версия алгоритма генерации простых сомножителей модуля криптосистемы Common Prime RSA, предложенная в [1], описана ниже.