В формуле (6) содержится порядка 2^{3n} дизъюнкций длины 3 и n.

На основе полученных формул генерируется входной файл для SAT-решателя. Формулы можно также использовать для тестирования работы новых SAT-решателей, созданных для криптографических задач.

ЛИТЕРАТУРА

1. *Огородников Ю. Ю.* Комбинированная атака на алгоритм RSA с использованием SAT-подхода // Динамика систем, механизмов и машин. Омск: ОмГТУ, 2016. С. 276–284.
2. *Заикин О. С., Отпущенников И. В., Семёнов А. А.* Оценки стойкости шифров семейства Trivium к криптоанализу на основе алгоритмов решения проблемы булевой выполнимости // Прикладная дискретная математика. Приложение. 2016. № 9. С. 46–48.
3. *Schmittner S. E.* A SAT-based Public Key Cryptography Scheme. IACR Cryptol. ePrint Arch. 2015. `https://eprint.iacr.org/2015/771.pdf`.
4. *Wille R., Lye A., and Niemann P.* Checking reversibility of Boolean functions // LNCS. 2016. V. 9720. P. 322–337.

УДК 519.688 DOI 10.17223/2226308X/13/39

О ВЫЧИСЛЕНИИ СИСТЕМЫ ПЕРЕПИСЫВАЮЩИХ ПРАВИЛ В КОНЕЧНОЙ ГРУППЕ

А. А. Кузнецов

Представлен алгоритм, определяющий переписывающую систему конечной группы, заданной фиксированным порождающим множеством. Необходимым условием эффективной реализации алгоритма является наличие быстрой процедуры умножения элементов в группе. Такой групповой операцией может быть композиция подстановок, умножение матриц, вычисление полиномов Холла и т. д. Алгоритм был применён для исследования переписывающих систем в конечных двупорождённых группах периода 5.

Ключевые слова: *система переписывающих правил, группа Бернсайда.*

Решение некоторых задач теории кодирования и криптографии сводится к исследованию подходящих графов Кэли, например открытая проблема эффективного восстановления вершин в графе Хэмминга [1].

Поиск кратчайших путей в графах Кэли является труднорешаемой проблемой, поэтому исследователям приходится идти на различные уловки и приёмы, чтобы получить решение за приемлемое время. Например, в [2] сначала определяют автоматическую структуру группы, которая порождает соответствующий граф Кэли. Автоматическая структура группы состоит из конечных автоматов специального вида [3]. Для их вычисления требуется определить множество соотношений в группе, используя известный алгоритм Кнута — Бендикса [4].

Зачастую алгоритм Кнута — Бендикса работает недопустимо долго, например в конечных группах, заданных коммутаторными соотношениями. В этом случае разворачивание коммутаторных соотношений приводит к очень длинным словам, что катастрофически замедляет работу алгоритма.

Настоящая работа представляет собой попытку устранить указанный недостаток. Остановимся подробнее на основных определениях.

Пусть $G = \langle X \rangle$ — конечная группа, порождённая упорядоченным множеством $X = \{x_1 \prec x_2 \prec \ldots \prec x_m\}$, которое также называют алфавитом. Множество всех слов (строк) над алфавитом X будем обозначать X^*. Пусть $w = x_1x_2\dots x_l$ — слово над X и $|w| = l$ — его длина. На множестве X^* также определим отношение порядка. Пусть v и w — два произвольных слова в алфавите X. Тогда $v \prec w$, если $|v| < |w|$, а в случае равенства длин меньшее слово определяется согласно введённому лексикографическому порядку на порождающих. Если необходимо подчеркнуть, что строка $v \in X^*$ соответствует элементу $g \in G$, то будем писать v_g. Строку v будем называть минимальным словом элемента g, если для всех других $w \in X^*$, таких, что $v_g = w_g$, выполняется $v \prec w$. Очевидно, что каждому $g \in G$ соответствует уникальное минимальное слово. Единице группы e соответствует пустое слово ε: $|\varepsilon| = 0$.

Пусть R — система переписывающих правил (переписывающая система), состоящая из множества пар вида (u, v), где $u_g = v_g$ и $u \succ v$ [4]. При этом слово u называют левой стороной правила, а строку v — правой. Иногда правила записывают в виде $u \to v$. Действие системы R над некоторым словом w означает осуществление замен вида $xuy \to xvy$ до тех пор, пока не будет получено несократимое относительно R слово w', т. е. $R(w) = w'$.

Если изменение порядка применения правил не влияет на конечный результат, то R называют *конфлюэнтной*.

Переписывающую систему R называют *несократимой*, если для любой пары $(u, v) \in R$ выполняется $R'(u) = u$ и $R'(v) = v$, где $R' = R \setminus \{(u, v)\}$.

Алгоритм 1 определяет переписывающую систему конечной группы $G = \langle X, \circ\rangle$. Необходимым условием эффективной реализации алгоритма является наличие быстрой процедуры умножения элементов в группе. Например, групповой операцией $\circ$ может быть композиция подстановок, умножение матриц, вычисление полиномов Холла и т. д.

Алгоритм 1. $R =$ `RewritingSystem`$(G, X, \circ)$

Вход: $G = \langle X, \circ\rangle$.
Выход: система переписывающих правил R группы G.

$P_0 := \{\varepsilon\}$ — множество минимальных слов.
$K_0 := \{(e, \varepsilon)\}$ — словарь вида (элемент группы, его минимальное слово).
$R := \varnothing$.
Для всех $i = 1, 2, \dots, \infty$:
  $K_i := K_{i-1}$, $P_i := \varnothing$.
  Для всех $x \in X$ и $p \in P_{i-1}$:
    $u := xp$ — конкатенация слов,
    $g := x \circ p$ — групповое умножение.
    Если $g \in K_i$, **то**
      если $R(u) = u$, **то** $v := K_i[g]$, добавить (u, v) в R,
    иначе
      добавить u в P_i, добавить (g, u) в K_s.
  Если $P_i = \varnothing$, **то**
    Вернуть R.

Теорема 1. Пусть R — система переписывающих правил, полученная при помощи алгоритма 1, тогда R конфлюэнтна и несократима.

Рассмотрим примеры. Пусть $B_0(2, 5) = \langle a_1, a_2\rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34} [5]. Для каждого элемента данной группы существует уникальное коммутаторное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$, $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2. Определим фактор-группу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34}\rangle$. Очевидно, что $|B_k| = 5^k$.

Пусть R_k — переписывающая система группы B_k. На рис. 1 представлены графики роста R_k для минимального порождающего множества $X = \langle a_1, a_2\rangle$, а также симметричного $Y = \langle a_1, a_2, a_1^{-1}, a_2^{-1}\rangle$.

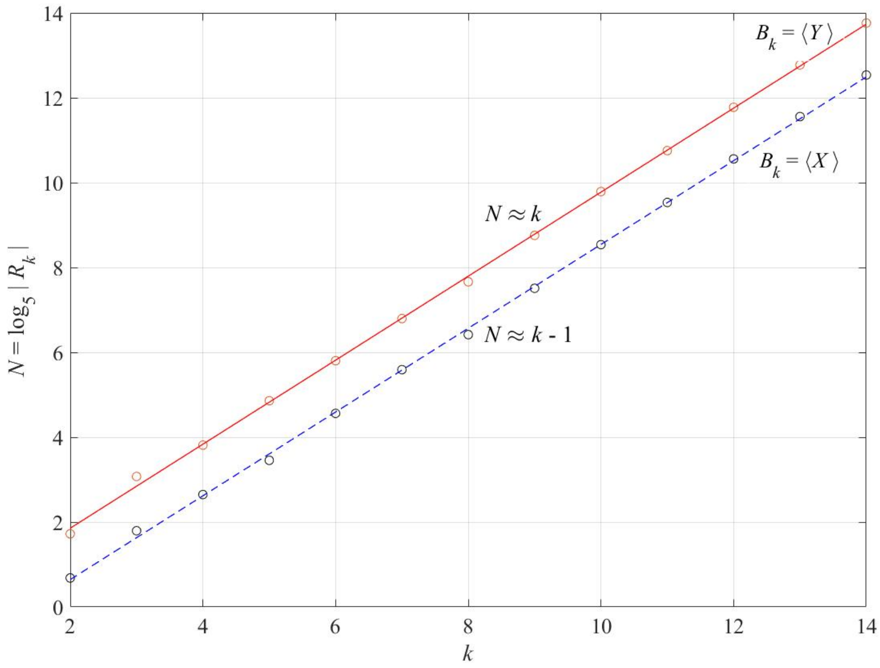

Рис. 1. Графики роста соотношений в B_k

ЛИТЕРАТУРА

1. *Константинова Е. В.* Комбинаторные задачи на графах Кэли. Новосибирск: НГУ, 2010. 110 с.
2. *Camelo M., Papadimitriou D., Fàbrega L., and Vilà P.* Efficient routing in Data Center with underlying Cayley graph // Proc. 5th Workshop Complex Networks CompleNet. 2014. P. 189–197.
3. *Epstein D., Paterson M., Cannon J., et al.* Word Processing in Groups. Boston: Jones and Barlett Publ., 1992. 330 p.
4. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
5. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.