Октябрь 18, 2006 at 16:04

ТЕЗИСЫ

Том 1, стр. 1–10 (2006) УДК 512.54
MSC 00A00

ТЕОРИЯ ДЕЛИМОСТИ В ГРУППЕ ТОМПСОНА И ЕЕ ПРИЛОЖЕНИЯ.

Е.С. ЕСЫП

Abstract. The objective of this paper is to construct divisibility theory for the R.Thompson group and its application to the decision of decomposition problem.

1. Введение.

Мы продолжаем исследование теории делимости в группах. Следуя идеям теории делимости для положительных Артиновых полугрупп [1], подобная теория была сделана для частично комутативных групп в статье [2].

Настоящая работа касается группы Р.Томпсона

$$F =< x_0, x_1, x_2, ...|x_i^{-1}x_kx_i = x_{k+1}(k > i) >,$$

а так же полугруппы положительных элементов

$$F^+ =< x_0, x_1, x_2...|x_kx_i = x_ix_{k+1}(k > i) > .$$

Группа F впервые встречается в статье Маккензи и Томпсона [3]. Подробное исследование этой группы приведено в статье [4]. Там, в частности, доказано, что группа F имеет конечное представление:

$$F \simeq< a, b|[ab^{-1}, a^{-1}ba] = [ab^{-1}, a^{-2}ba^2] = 1 > .$$

На элементах полугруппы F^+ определим длину l. Длина $l(w)$ равна числу букв в записи слова w. Дадим общие определения делимости.

Определение. *Делителем* (левым) элемента w в полугруппе F^+ называется такой элемент $u \in F^+$, для которого существует элемент $v \in F^+$, такой что выполнены условия: $w = uv$, $l(w) = l(u) + l(v)$.

(Условие $l(w) = l(u)+l(v)$ в записи произведения элементов обозначают символом $\circ$, т.е. пишут $w = u \circ v$.) Аналогично определяются правые делители. Основная цель данной работы - найти способы (алгоритмы)

Есып Е.С., Теория делимости в группе Томпсона и ее приложения.

Работа поддержана РФФИ (грант 05-01-00057).

нахождения делителей элементов полугруппы F^+, проверки условия делимости и решение связанных с этим проблем.

2. Теория делимости в группе.

2.1. **Нормальные формы.** Любой элемент F^+ может быть единственным образом записан в нормальной форме:

$$x_{i_0}x_{i_1}...x_{i_m}, \tag{1}$$

где $i_0 \leqslant i_1 \leqslant i_2 \leqslant ... \leqslant i_k$.

Можно расширить эту нормальную форму на всю группу F. В [4] доказано, что любой элемент F может быть однозначно записан в нормальной форме

$$x_{i_1}...x_{i_m}x_{j_l}^{-1}...x_{j_1}^{-1}$$

где $i_1 \leq ... \leq i_m, j_1 \leq ... \leq j_l$, если встречаются элементы x_k и x_k^{-1}, то встречается либо x_{k+1} либо x_{k+1}^{-1}. Соответствующие правила Кнута Бендикса:

- $x_i^{-1}x_k \longrightarrow x_{k+1}x_i^{-1}$
- $x_k^{-1}x_i \longrightarrow x_ix_{k+1}^{-1}$
- $x_kx_i \longrightarrow x_ix_{k+1}$
- $x_i^{-1}x_k^{-1} \longrightarrow x_{k+1}^{-1}x_i^{-1}$
- $x_ix_i^{-1} \longrightarrow 1$
- $x_i^{-1}x_i \longrightarrow 1$
- $x_iwx_i^{-1} \longrightarrow w$

где $i < k$, $x_iw = wx_i$, w в нормальной форме.

2.2. **Косокоммутирование.** Определим *оператор, увеличивающий (уменьшающий) индексы* $\delta_k : F \to F$, следующим образом: $\delta_k(x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}) = x_{i_1+k}^{\varepsilon_1}...x_{i_m+k}^{\varepsilon_m}$.

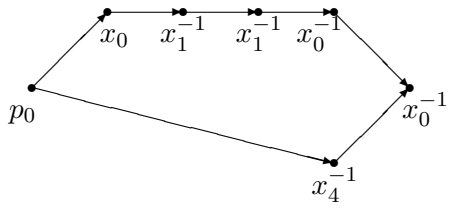
Определение. Слово $u \in F$ *косокоммутирует* с $v \in F$ тогда и только тогда выполняется одно из условий:

- $uv = \delta_{l(u)}(v)u$
- $uv = \delta_{-l(u)}(v)u$
- $uv = v\delta_{l(v)}(u)$
- $uv = v\delta_{-l(v)}(u)$.

2.3. **Пример нахождения множества делителей.** Элемент группы F:

$$w_0 := x_0x_4^{-1}x_1^{-1}x_1^{-1}x_0^{-1}x_0^{-1}$$

Граф этого элемента:



Ставим ребро тогда и только тогда, когда соответствующие вершинные элементы не косокоммутируют. Такой граф $\Gamma(w)$ можно построить для любого элемента w группы F.

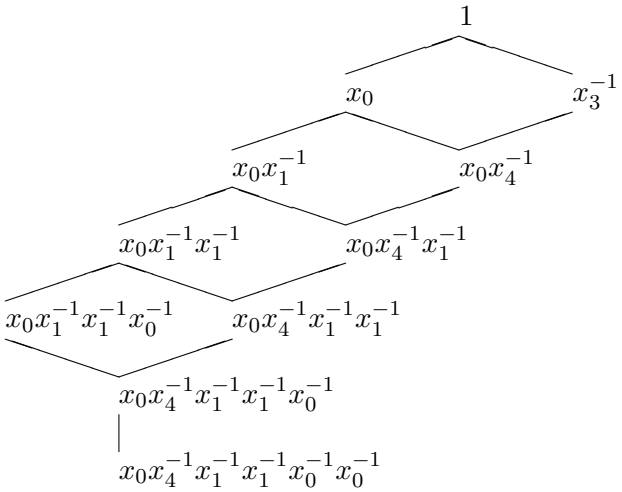
Предложение. Для любого элемента w группы F и любой вершины v графа $\Gamma(w)$, входит не более двух ребер и выходит не более двух ребер.

Доказательство. Достаточно проверить, что входит не более двух ребер. Список возможных ребер:

(1) $x_{i-1} \longrightarrow x_i^{-1}$
(2) $x_{i+1} \longrightarrow x_i^{-1}$
(3) $x_i^{-1} \longrightarrow x_i^{-1}$
(4) $x_{i+1}^{-1} \longrightarrow x_i^{-1}$
(5) $x_{i-1} \longrightarrow x_i$
(6) $x_i \longrightarrow x_i$

Из этого списка пары (1)-(3), (2)-(4) несовместны. □

Решетка делителей для элемента w_0:



Замечание. В группе не определено наименьшее общее кратное.

Пример: для элементов x_0 и x_0^{-1}.

3. Приложения.

Рассмотрим криптосистему, предложенную Шпильрайном и Ушаковым [6].

Протокол.

Зафиксируем число $s = 3..8$. Пусть A_s – группа порожденная $\{x_0x_1^{-1}, ..., x_0x_s^{-1}\}$, B_s – группа порожденная $\{x_{s+1}, ..., x_{2s}\}$. Группы A_s и B_s коммутируют.

(1) Открыто число s и слово $w \in T_{2s}$ длины m. Число m четное.
(2) Пользователь A выбирает два слова $a_1 \in A_s$ и $b_1 \in B_s$ длины m. Вычисляет нормальную форму слова $w_1 = a_1wb_1$ и отправляет ее пользователю B. Пользователь B выбирает два слова $b_2 \in B_s$ и $a_2 \in A_s$ длины m. Вычисляет нормальную форму слова $w_2 = b_2wa_2$ и отправляет ее пользователю A.
(3) Пользователь A вычисляет нормальную форму $a_1w_2b_1$. Пользователь B вычисляет нормальную форму $b_2w_1a_2$.
(4) Так как $a_1b_2wa_2b_1 = b_2a_1wb_1a_2 = w_{key}$, то оба пользователя получили общий ключ w_{key}.

Обозначение. Максимальный левый общий делитель, принадлежащий подгруппе H группы F для слова w обозначим через $lmd_H(w)$.

Утверждение. *Для любого слова $w \in F$ элемент $lmd_{B_s}(w)$ существует и единственен.*

Доказательство. Выделим из слова w слева последовательно все буквенные делители, принадлежащие группе B_s. Получим разложение: $w = w_b \circ u$. Предположим $w = w'_b \circ u'$, где w'_b – некоторый элемент из B_s и $w'_b = w_b \circ v$, т.е., что w_b не максимальный, тогда $w = w_b \circ v \circ u$. В этом случае из слова $v \circ u$ мы можем выделить слева еще одну букву, принадлежащую B_s. Противоречие. Тогда w_b – это искомый $lmd_{B_s}(w)$. Единственность доказывается индукцией по длине w_b.

В случае с подгруппой A_s подобное доказательство не проходит, так как существуют слова из группы A_s, которые нельзя представить в виде несократимого произведения порождающих A_s. В случае, когда для подгруппы H существуют слова, которые нельзя представить в виде несократимого произведения порождающих, строим генерический алгоритм, вычисляющий $lmd_H(w)$.

Для успешного взлома достаточно найти хотя бы одно разложение w_2.

Атака. Вход: s, w, w_1, w_2. Выход: w_{key}.

(1) Вычисляем $b'_2 := lmd_{B_s}(w_b)lmd_{B_s}(w)^{-1}$. По экспериментальным данным в 50% случаев элемент $a'_2 := (b'_2w)^{-1}w_2$ принадлежит A_s, следовательно $w_{key} := b'_2w_1a'_2$. Проведено около 10^6 экспериментов для разных s и m.
(2) В элемент b'_2 может попасть часть слова a_2. В этом случае a'_2 может не принадлежать A_s. Вычисляем b''_2, w'', a''_2, где $b'_2wa'_2 = b''_2 \circ w'' \circ a''_2$ – остатки от сокращения. Добавляем к a''_2 слева слова вида $x_i...x_{i+j}x_{i+j+1}^{\varepsilon}x_{i+j}^{-1}...x_i^{-1}$, пока не получим разложение. Здесь i, j пробегают значения от 0 до $s + m$. В этом случае на 10^6 экспериментах получили разложение в 100% случаев.

Следует отметить, что существует более простое решение задачи декомпозиции для данных конкретных групп A_s и B_s, см. [7]. Однако, способ, использующий теорию делимости возможно расширить на любые

подгруппы группы Томпсона, так как он не использует особую структуру элемента подгрупп A_s и B_s, представленного в виде гомеоморфизма единичного отрезка, как это делается в [7].

Список литературы

[1] E.Brieskorn and K.Saito. *Artin-Gruppen und Coxeter-Gruppen*, Inventiones Math. 17(1972), 245-271.

[2] E.S.Esyp, I.V.Kazatchkov and V.N.Remeslennikov. *Divisibility theory and complexity of algorithms for free partially commutative groups.* Contemporary Mathematics, ISSN: 0271-4132, Vol. 378, 2005, 319-348pp.

[3] McKenzie R., Thompson R. J. *An elementary construction of unsolvable word problems in group theory, Word Problems* (W.W.Boone, F.B.Cannonito and R.C.Lyndon eds.), Studies in Logic and the Foundation of Mathematics. vol.71 North-Holland, Amsterdam, 1973, pp. 457-478.

[4] J. W. Cannon, W. J. Floyd, and W. R. Parry. *Introductory notes on Richard Thompson's groups.* Enseign. Math. (2), 42(3-4):215-256, 1996.

[5] D.Epstein and others.*Word processing in groups.*

[6] A.Ushakov, V.Shpilrain. *Thompson's group and public key cryptography.* Lecture Notes Comp. Sc., 3531:151-164, 2005.

[7] F. Matucci. *The Shpilrain-Ushakov protocol for Thompson's group F is always breakable.* http://arxiv.org/abs/math.GR/0607184

Евгений Семенович Есып
Омский филиал института математики им. С. Л. Соболева СО РАН,
ул. Певцова 13,
644000, Омск, Россия
E-mail address: esyp@iitam.omsk.net.ru, http://iitam.omsk.net.ru/~esyp