Math-Net.Ru

Общероссийский математический портал

В. С. Губа, О некоторых свойствах периодических слов, *Матем. заметки*, 2002, том 72, выпуск 3, 330–337

DOI: <https://doi.org/10.4213/mzm425>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.80.73.141

26 апреля 2023 г., 14:15:20

УДК 519.4

О НЕКОТОРЫХ СВОЙСТВАХ ПЕРИОДИЧЕСКИХ СЛОВ

В. С. Губа

В статье доказывается, что куб простого слова нельзя разложить в произведение слов с периодами меньшей длины. Исследован также вопрос о разложении квадрата простого слова в произведение слов с меньшими периодами. Утверждения подобного рода, касающиеся свойств периодических слов, представляют интерес в связи с исследованием групп и полугрупп, заданных при помощи периодических определяющих соотношений.

Библиография: 7 названий.

В настоящей заметке рассматриваются некоторые свойства периодических слов. Думается, что они, во-первых, представляют самостоятельный интерес, а во-вторых, подобного рода утверждения о свойствах периодических слов часто оказываются полезными при изучении групп и полугрупп, заданных при помощи периодических соотношений. По этому поводу см., например, [1]–[3].

Знак равенства “=” используется в качестве обозначения для графического (побуквенного) равенства слов. Длина слова X обозначается через $|X|$. Если $X = YZ$, то слово Y называется *началом* слова X , а слово Z – *концом* слова X . Если при этом Y (Z) не совпадает с X , то оно называется *собственным* началом (концом). Слово X называется *истинной степенью*, если существует такое слово Y и такое натуральное число $n > 1$, что $X = Y^n$. В противном случае слово называется *простым*. Любое непустое слово X представимо в виде $X = Y^n$, где Y – простое слово, n – натуральное число. Если T – непустое слово, то произвольное подслово степени слова T мы будем называть *T -периодическим словом*. Ясно, что если W есть T -периодическое слово, то оно будет также S -периодическим для некоторого простого слова S , степенью которого является T . Слова X, Y называются *сопряженными*, если существуют такие слова A, B , что $X = AB, Y = BA$. Иначе говоря, слова сопряжены, если одно из них является циклическим сдвигом другого. Очевидно, что если слово T -периодично, то оно будет S -периодично для любого слова S , сопряженного T . Для любого непустого слова X рассмотрим такое слово T минимальной длины, что X является T -периодическим. Легко видеть, что слово T с этим свойством всегда существует и определено однозначно с точностью до циклического сдвига. Оно называется *минимальным периодом* слова X .

Работа [4] посвящена описаниям решений уравнений $x^k y^l = z^m$ в свободной группе, где $k, l, m \geq 2$. Доказывается, что если (X, Y, Z) – решение, то X, Y, Z принадлежат одной циклической подгруппе. Такие решения мы будем называть *циклическими*.

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований, грант № 99-01-00894.

Частным случаем рассматриваемой ситуации является описание решений этого уравнения в свободной полугруппе. Пусть $k, l, m \geq 2$, и пусть имеет место равенство $X^k Y^l = Z^m$ для некоторых слов X, Y, Z . Из работы [4] следует, что при этом существует слово T , степенями которого являются X, Y и Z . Можно считать, что слово T при этом является простым. Легко понять, что данный факт эквивалентен следующему: если (X, Y, Z) – решение уравнения $x^k y^l = z^m$ ($k, l, m \geq 2$), и слова X, Y, Z простые, то $X = Y = Z$ в свободной полугруппе. Можно привести и такую формулировку: если T – простое слово, и $m \geq 2$, то слово T^m нельзя представить в виде произведения степеней (простых) слов X и Y таких, что $|X| < |T|, |Y| < |T|$.

Рассмотрим следующее обобщение. Пусть T – простое слово, $m \geq 2$. Нас интересует возможность представить слово T^m в виде произведения X -периодического и Y -периодического слов, где X, Y – простые слова такие, что $|X| < |T|, |Y| < |T|$. На языке уравнений, речь идет об уравнении вида $(x_1 x_2)^k x_1 y_2 (y_1 y_2)^l = z^m$, которое можно рассматривать как обобщение уравнения Линдона–Шюттенберге в свободной полугруппе (точнее, в свободном моноиде).

Вначале напомним формулировки трех лемм. Все они хорошо известны и часто используются при работе со словами. Для доказательств см., например, [5, гл. 11, § 5].

ЛЕММА 1. Пусть $XY = YX$ для некоторых слов X, Y . Тогда эти слова являются степенями одного и того же слова, т.е. существует слово P и целые неотрицательные числа k, l такие, что $X = P^k, Y = P^l$.

ЛЕММА 2. Пусть X, Y – простые слова, и предположим, что слово W является X -периодическим и Y -периодическим. Если $|W| \geq |X| + |Y|$, то X и Y сопряжены.

Если заранее известно, что простые слова X и Y имеют разные длины, то всякое слово, являющееся как X -периодическим, так и Y -периодическим, будет иметь длину $< |X| + |Y|$. Именно в такой форме эта лемма будет часто использоваться в дальнейшем.

ЛЕММА 3. Пусть X, Y, Z – такие слова, что $XY = YZ$, и предположим, что X, Z непусты. Тогда существуют слова P, Q и целое число $d \geq 0$ такие, что $X = PQ, Z = QP, Y = (PQ)^d P$.

ОПРЕДЕЛЕНИЕ. Пусть W – некоторое T -периодическое слово, где T простое. Мы говорим, что W – вырожденное T -периодическое слово, если W также является U -периодическим для некоторого (простого) слова U со свойством $|U| < |T|$.

Из леммы 2 легко следует, что если $|W| \geq |T^2|$, где T простое, то W – невырожденное T -периодическое слово. Действительно, если W также U -периодично, где U – простое слово, более короткое, чем T , то U и T не сопряжены, и $|W| < |T| + |U| < |T^2|$. Отсюда очевидно, что при $m \geq 4$ слово T^m , где T простое, не представимо в виде произведения двух вырожденных T -периодических слов.

Рассмотрим следующий пример. Пусть $T = a^n b a$, где a, b – буквы некоторого алфавита. Очевидно, T простое. Мы можем представить слово T^2 в виде $a^n b a^n \cdot a b a$, где $a^n b a^n$ есть вырожденное T -периодическое слово, так как имеет период $a^n b$ более короткий, чем T . Но $|a^n b a^n|/|T^2| \rightarrow 1$ при $n \rightarrow \infty$. Поэтому оценка $|W| \geq |T^2|$ в этом смысле является точной.

Сформулируем первый из наших основных результатов.

ТЕОРЕМА 1. Пусть T – простое слово. Если $T^3 = XY$ для некоторых X, Y , то либо X , либо Y есть невырожденное T -периодическое слово. Иными словами, куб простого слова нельзя разложить в произведение периодических слов с более короткими периодами.

ДОКАЗАТЕЛЬСТВО. Предположим, что это не так. Пусть X – U -периодическое слово, и Y – V -периодическое, где U, V – простые и $|U| < |T|, |V| < |T|$.

По лемме 2 мы имеем $|X| < |T| + |U| < |T^2|$, т.е. $|Y| > |T|$. Аналогично, $|Y| < |T| + |V| < |T^2|$, и $|X| > |T|$. Таким образом, можно положить $X = TX', Y = Y'T$, и $T = X'Y'$.

Без ограничения общности пусть $T = U^k U'$ для некоторого $k \geq 1$, где U' есть непустое начало U . Пусть $U = U'U''$. Полагаем $A = U', B = U''U^{k-1}$. Тогда $T = ABA$, и X есть начало некоторой степени слова AB . Так как $|X| < |T| + |U|$, мы получаем $|X'| < |U| \leq |AB|$. Итак, X' есть начало слова BA .

Аналогично, мы можем положить $T = CDC$, где DC есть степень V , а Y' есть конец CD , причем $|Y'| < |DC|$. Легко видеть, что A, B, C, D – непустые слова.

Мы имеем $ABA = CDC$. Рассмотрим два случая.

1) $|A| = |C|$. Тогда $A = C, B = D$. Слово $T = X'Y'$ есть произведение некоторого начала слова BA и некоторого конца слова AB . Мы знаем, что $|X'| < |AB|$ и $|Y'| < |BA|$. Тогда $|X'| > |A|, |Y'| > |A|$. Мы видим, что $X' = AB_1, Y' = B_2A, B = B_1B_2$, где B_1, B_2 непусты.

Так как X' есть начало $BA = B_1B_2A$ и $|X'| > |B_1|$, то $X' = B_1X''$ для некоторого X'' , где $|X''| = |A|$. Аналогично, $Y' = Y''B_2$, где $|Y''| = |A|$.

Так как $X' = B_1X''$ есть начало $BA = B_1B_2A$, то X'' есть начало B_2A . Но $B_2A = Y' = Y''B_2$, и это слово начинается с Y'' . Слова X'' и Y'' имеют одну и ту же длину, поэтому $X'' = Y''$. Итак, мы получаем

$$AB = AB_1B_2 = X'B_2 = B_1X''B_2 = B_1Y''B_2 = B_1Y' = B_1B_2A = BA.$$

По лемме 1 слова A, B – степени некоторого P . Это влечет, что $T = ABA$ есть истинная степень P , поэтому мы имеем противоречие.

2) Если $|A| \neq |C|$, то без ограничения общности $|A| < |C|$. Так как $ABA = CDC$, мы имеем $C = AE = FA$ для некоторых непустых E, F и $B = EDF$. Лемма 3 влечет существование слов P, Q и числа $k \geq 0$ таких, что $E = QP, F = PQ, A = (PQ)^k P$.

Так как $|Y| < |V| + |T| \leq |DC| + |T|$, мы получаем $|X| > |T^2| - |DC| = |TAE|$. Тогда X' начинается с $AE = (PQ)^{k+1}P$, и поэтому PQ есть начало X' . Но с X' также начинается слово $BA = QPDF A$, и потому QP есть начало X' . Мы получаем, что $PQ = QP$, и P, Q – степени одного и того же (простого) слова S по лемме 1. Итак, для некоторых m, n мы получаем $A = S^m$ и $E = F = S^n$. Тогда $C = S^{m+n}, B = S^n D S^n$. (Ясно, что m и n положительны.)

Рассмотрим слово $T = X'Y'$. Заметим, что $|X'| < |AB|$ и $|Y'| < |DC|$. Поэтому $|X'| > |C|, |Y'| > |A|$.

Проверим, что $|Y'| > |C|$. Предположим противное. Тогда $|X'| = |T| - |Y'| \geq |CD|$. Тем самым оказывается, что X' начинается с $CD = S^{m+n}D$. Но X' есть начало слова $BA = S^n D S^{m+n}$, и мы получаем $S^{m+n}D = S^n D S^m$. Тогда $S^m D = D S^m$. Так как S простое, легко заключить (используя леммы 1, 2), что D есть степень S (см. [5]). Это приводит к противоречию, так как $T = ABA = S^{m+n} D S^{m+n}$ не есть истинная степень.

Мы имеем $|X'| < |CD|$ и $|Y'| > |C|$. Можно записать $X' = CD_1, Y' = D_2C, D = D_1D_2$, где D_1, D_2 непусты. Напомним, что слово $X' = CD_1 = S^{m+n}D_1$ есть

начало $BA = S^n DS^{m+n}$, и слово $Y' = D_2 S^{m+n}$ есть конец $CD = S^{m+n} D$. Это влечет, что $S^m D_1$ есть начало слова DS^{m+n} (а также начало DS^m).

Пусть $t \geq 0$ – максимальное целое число такое, что $D_1 = S^{mt} D'_1$ для некоторого D'_1 . Тогда $S^m D_1 = S^m S^{mt} D'_1$ есть начало слова $DS^m = S^{mt} D'_1 D_2 S^m$. Мы заключаем, что $S^m D'_1$ есть начало $D'_1 D_2 S^m$. Так как t максимально, слово D'_1 не может начинаться с S^m . Итак, $S^m = D'_1 R$ для некоторого R .

Теперь

$$S^{m+n} D = S^{m+n} D_1 D_2 = S^{mt} S^m S^n D'_1 D_2 = S^{mt} D'_1 R S^n D'_1 D_2 = D_1 R S^n D'_1 D_2.$$

Ясно, что $|R S^n D'_1 D_2| = |S^{m+n} D| - |D_1| = |D_2 S^{m+n}|$. Но слово $D_2 S^{m+n}$ есть конец $S^{m+n} D$, поэтому имеем

$$R S^n D'_1 D_2 = D_2 S^{m+n} \quad \text{и} \quad S^{m+n} D = D_1 R S^n D'_1 D_2 = D_1 D_2 S^{m+n} = D S^{m+n}.$$

Теперь получается, что D, S – степени одного слова, что является противоречием.

Теорема доказана.

Отметим тот очевидный факт, что в формулировке теоремы 1 вместо слова T^3 можно взять произвольное T -периодическое слово W , длина которого не меньше $|T^3|$. В самом деле, если W разложено в произведение двух слов с периодами, каждый из которых по длине короче слова T , то этот же факт верен относительно начала слова W , имеющего длину $|T^3|$. Можно еще несколько усилить формулировку, допустив, что слова X, Y могут перекрываться, т.е. X – начало W , Y – конец W , и при этом $|X| + |Y| \geq |W|$.

Теорема 1 была доказана автором в [6], см. также [7]. Отметим, что из этой теоремы легко следует тот известный факт, что уравнение Линдона–Шютценберже в свободной полугруппе имеет только циклические решения. Действительно, пусть X, Y, Z – простые слова, $k, l, m \geq 2$, и $X^k Y^l = Z^m$. Выведем, что $X = Y = Z$. Рассуждая от противного, предполагаем, что $X \neq Z, Y \neq Z$. Из леммы 2 выводим, что $|X^k| < |X| + |Z|$, откуда $|X| \leq |X^{k-1}| < |Z|$. Неравенство $|Y| < |Z|$ доказывается так же. Теперь ясно, что $|X^k| < |Z^2|, |Y^l| < |Z^2|$, откуда $m \leq 3$. При $m = 3$ (основной случай) получаем противоречие с теоремой 1. Осталось рассмотреть случай $m = 2$. Применим индукцию по $|Z|$. Пусть $X^k Y^l = Z^2$. Без ограничения общности $|X^k| > |Z|$, откуда $X^k = ZV, Z = VY^l$. Слово $V^2 Y^l = VZ$ есть, очевидно, циклический сдвиг слова $ZV = X^k$, поэтому оно равно $(X')^k$, где X' – циклический сдвиг X . При этом возникает уравнение $V^2 Y^l = (X')^k$. Можно считать, что $k = 2$, так как в противном случае уравнение имеет лишь циклические решения. Теперь можно применить предположение индукции, так как $|X'| = |X| < |Z|$. Следовательно, уравнение имеет только циклические решения, т.е. V должно быть степенью Y , а потому и Z будет собственной степенью Y , что невозможно.

Непустое слово T называется *гиперпростым*, если никакое его собственное непустое начало не может являться его же концом. Если слово T не гиперпросто, то выделим кратчайшее из его непустых начал X , которое является концом этого же слова. Слово X обязано быть гиперпростым (в противном случае оно не будет кратчайшим). Из определения следует, что различные вхождения одного и того же гиперпростого слова не могут перекрываться, поэтому T имеет вид XYX , где X непусто. Ясно, что мы тем самым приходим к эквивалентному определению гиперпростого слова. Можно предложить еще одну эквивалентную формулировку: простое слово T гиперпросто тогда и только тогда, когда оно является невырожденным T -периодическим.

Нам понадобится одна лемма, представляющая самостоятельный интерес. Пусть T – простое слово. Напомним, что слово T^2 является невырожденным T -периодическим. Мы хотим отсечь от слова T^2 некоторый его конец так, чтобы оставшееся слово было невырожденным T -периодическим. Если T гиперпросто, то можно отсечь от T^2 слово T . Допустим, что T не гиперпросто. Представим его в виде XYX , где X непусто. Ясно, что Y также непусто, так как T простое. Мы утверждаем, что в этом случае можно отсечь X справа, т.е. слово $XYXXY$ будет невырожденным T -периодическим. На самом деле от T^2 справа можно отсечь любое слово X , которое является собственным началом и концом слова T . Чтобы сделать наше утверждение более наглядным, введем следующие обозначения. Если T просто, но не гиперпросто, то рассмотрим минимальный период U слова T . При этом будем также считать, что T начинается словом U . Пусть k – наибольшее число, при котором T начинается словом U^k . Ясно, что $k \geq 1$. Положим $T = U^k X$. Очевидно, что X есть непустое начало слова U . Положим $U = XY$. В итоге имеем равенство $T = (XY)^k X$, где XY простое, X и Y непусты, $k \geq 1$. Мы утверждаем, что от слова T^2 можно отсечь $(XY)^{k-1} X$ справа, т.е. TXY будет невырожденным T -периодическим. (Можно также сказать, что если слово A является собственным началом и концом простого слова T , то отсечение справа слова A от слова T^2 приводит к невырожденному T -периодическому слову.)

ЛЕММА 4. Пусть T – простое слово, имеющее вид $T = (XY)^k X$, где X, Y – непустые слова, $k \geq 1$. Тогда начало TXY слова T^2 будет невырожденным T -периодическим.

ДОКАЗАТЕЛЬСТВО. Допустим противное, т.е. предположим, что TXY имеет некоторый (простой) период U , где $|U| < |T|$. Лемма 2 позволяет заключить, что $|TXY| < |T| + |U|$, откуда $|XY| < |U|$. Поскольку слово T является как U -периодическим, так и XY -периодическим, то та же лемма позволяет сделать вывод, что $|T| < |U| + |XY|$. (Применяя эту лемму, нужно иметь в виду, что XY есть степень некоторого простого слова V . Следовательно, $|T| < |U| + |V| \leq |U| + |XY|$.) В результате получаем, что $|(XY)^{k-1} X| < |U|$. Заменяя при необходимости слово U на его циклический сдвиг, будем далее считать, что T начинается с U . Рассмотрим два случая.

Случай 1. $|(XY)^k| < |U|$. В этом случае U содержит $(XY)^k$ в качестве собственного начала и при этом само является собственным началом слова $T = (XY)^k X$. Следовательно, X представимо в виде произведения двух непустых слов $X = X_1 X_2$ таким образом, что $U = (XY)^k X_1$. По условию, $TXY = UX_2 X_1 X_2 Y$ есть начало некоторой степени слова U . Следовательно, этим же свойством обладает и слово $X_2 X_1 X_2 Y$, получаемое отсечением от TXY слова U слева. Однако ввиду $k \geq 1$ слово U начинается с $X = X_1 X_2$, и потому выполняется равенство $X_1 X_2 = X_2 X_1$. По лемме 1 найдется простое слово P и натуральные числа m, n такие, что $X_1 = P^m$, $X_2 = P^n$. В результате мы знаем, что слово $X_2 X_1 X_2 Y = P^{m+2n} Y$ есть начало степени слова U . Если $k \geq 2$, то U начинается с XYX . Если $k = 1$, то рассмотрим слово $U^2 = XYX_1 XYX_1$, которое также начинается с XYX ввиду того, что $X_1 X = X X_1$. Итак, в любом случае U^2 начинается с $XYX = P^{m+n} Y P^n P^m$. Отсюда следует, что $P^{m+2n} Y$ должно совпадать с началом слова XYX той же длины, т.е. $P^{m+2n} Y = P^{m+n} Y P^n$. Таким образом, $P^n Y = Y P^n$, и ввиду леммы 1 и простоты слова P оказывается, что Y есть степень P . Это приводит к противоречию, так как слово T при этом было бы истинной степенью.

Случай 2. $|U| \leq |(XY)^k|$. Сразу же заметим, что в этом случае $k \geq 2$ ввиду того, что $|XY| < |U|$. Поэтому U не равно $(XY)^k$, так как является простым. Отсю-

да и из неравенства $|(XY)^{k-1}X| < |U|$ следует, что U имеет $(XY)^{k-1}X$ собственным началом, являясь само собственным началом слова $(XY)^k = (XY)^{k-1}XY$. Поэтому можно разложить Y в произведение двух непустых слов $Y = Y_1Y_2$ так, что при этом $U = (XY)^{k-1}XY_1$. Тогда $THY = (XY)^kXHY = UY_2XXY_1Y_2$ есть начало степени слова U , и то же верно относительно слова $Y_2XXY_1Y_2$. Слово U (с учетом $k \geq 2$) начинается с $XYX = XY_1Y_2X$. Слова Y_2XXY_1 и XY_1Y_2X имеют одинаковую длину, поэтому обязаны совпадать, так как оба суть начала слова U . Это означает, что слова Y_2X и XY_1 коммутируют, поэтому лемма 1 дает возможность записать $Y_2X = P^m$, $XY_1 = P^n$, где P – простое слово, m и n – натуральные числа. В этих обозначениях слово $P^{m+n}Y_2$ является началом некоторой степени слова U . Заметим, что $XYX = XY_1Y_2X = P^{m+n}$.

Если $k \geq 3$, то U начинается словом $(XY)^2 = P^{m+n}Y$, и потому Y_2 есть начало Y . Тогда XY_2 является началом слова XY , которое, в свою очередь, есть начало слова P^{m+n} . Длина слова XY_2 равна $|Y_2X| = |P^m|$, откуда $XY_2 = P^m = Y_2X$. С использованием леммы 1 легко сделать вывод, что X и Y_2 суть степени слова P . Из этого следует, что степенью P будет и слово Y_1 , т.е. вновь приходим к противоречию с простотой слова T .

Теперь пусть $k = 2$. В этом случае $U^2 = (XYXY_1)^2$ начинается словом $P^{m+n}Y_1XY$. Слово $P^{m+n}Y_2$ короче по длине; следовательно, будучи началом степени слова U , оно будет началом слова $P^{m+n}Y_1XY$. Но тогда Y_1XY начинается словом Y_2 , а потому и XY_1XY имеет слово XY_2 своим началом. Остается заметить, что слово $XY_1XYX = P^{m+2n}$ также имеет XY_2 своим началом, а поскольку длина последнего равна длине слова P^m , то приходим к равенству $XY_2 = P^m = Y_2X$, что окончательно приводит к противоречию, как и в предыдущем абзаце.

Лемма доказана.

Теперь изучим вопрос о представлении слова T^2 , где T простое, в виде $T^2 = XY$, где X, Y – вырожденные T -периодические слова. Прежде всего отметим, что может иметь место следующий тривиальный случай. Если слово T не является гиперпростым, то T^2 есть произведение двух слов, равных T , каждое из которых является вырожденным T -периодическим. Минимальные периоды слов X и Y в этом случае оказываются сопряженными.

Несколько менее тривиальная ситуация возникает в следующем примере. Положим $T = (ab)^na(ab)^{2n}a$, где $n \geq 1$ произвольно, a, b – буквы. Легко видеть, что T – простое слово. Пусть $U = (ab)^na(ab)^n$, $V = ba$. Тогда U, V – простые слова, более короткие, чем T и не сопряженные друг другу. При этом

$$T^2 = (ab)^na(ab)^{2n}a(ab)^na(ab)^{2n}a = \underbrace{(ab)^na(ab)^n \cdot (ab)^na(ab)^n \cdot a \cdot a}_{X} \cdot \underbrace{(ba)^{2n}}_Y.$$

Здесь $|X| > |U^2|$, $|Y| > |V^{2n}|$, т.е. первый из сомножителей содержит более двух периодов U , а второй может содержать вообще сколь угодно много периодов V . Заметим, что слово X содержит менее трех периодов U . Сформулируем второй из наших основных результатов.

ТЕОРЕМА 2. Пусть T – простое слово, и пусть $T^2 = XY$, где X и Y – соответственно U -периодическое и V -периодическое слова с минимальными периодами U ,

V , причем $|U| < |T|$ и $|V| < |T|$. Тогда из условия $|U| = |V|$ следует, что U и V сопряжены. Если $|U| > |V|$, то $|X| < |U^3|$, а из $|U| < |V|$ следует, что $|Y| < |V^3|$.

Перед доказательством заметим, что если слова U и V не сопряжены, то теорема накладывает ограничение либо на число периодов U , содержащихся в X , либо на число периодов V , содержащихся в Y . Если U и V сопряжены, то таких ограничений не имеется, как показывает пример периода вида $T = (ab)^n a$, где a, b – буквы.

ДОКАЗАТЕЛЬСТВО. Ясно, что хотя бы одно из неравенств $|X| \geq |T|$, $|Y| \geq |T|$ заведомо имеет место. Допустим, что $|X| \geq |T|$. Заменяя V на подходящий циклический сдвиг, будем считать, что Y начинается словом V . С учетом того, что $|X| \geq |T|$, можно рассмотреть сдвиг V как подслово в T -периодическом слове T^2 на период T влево. Поскольку V короче, чем T , результатом сдвига будет подслово, содержащееся в X . Поэтому слово V является U -периодическим. Из $|U| = |V|$ тогда немедленно следует сопряженность слов U и V , поэтому далее будем считать, что $|U| \neq |V|$.

ЗАМЕЧАНИЕ 1. Для дальнейшего заметим, что рассуждения предыдущего абзаца проходят безо всяких изменений, если вместо слова T^2 рассматривать произвольное T -периодическое слово, имеющее длину не меньше $|T^2|$.

По-прежнему предполагая без ограничения общности, что $|X| \geq |T|$, приходим к выводу, что Y есть подслово в T , а потому и в X . Следовательно, минимальный период слова Y не длиннее минимального периода слова X . Поэтому имеет место неравенство $|U| > |V|$. Достаточно доказать, что $|X| < |U^3|$. Предположим противное.

Можно записать $X = TZ$, откуда $T = ZY$. По лемме 2 $|X| < |T| + |U|$, т.е. $|Z| < |U|$. Ввиду $|X| \geq |U^3|$ имеем $|T| > |U^2|$. Поскольку Y является U -периодическим и V -периодическим одновременно, та же лемма дает неравенство $|Y| < |U| + |V|$. Отсюда $|T| = |Z| + |Y| < 2|U| + |V| < 3|U|$. Заменяя U на подходящий циклический сдвиг, можно считать, что T начинается словом U . Тогда X будет началом некоторой степени слова U . Из неравенств $|T| > |U^2|$, $|T| < |U^3|$ следует, что T имеет U^2 в качестве собственного начала, само являясь собственным началом слова U^3 . Следовательно, можно положить $T = U^2 A$, где A есть непустое собственное начало слова U . Имеем $U = AB$ для непустых слов A, B . Итак, $T = ABABA$. Поскольку X имеет $U^3 = (AB)^3$ своим началом, то Z начинается словом B . Это значит, что T также начинается словом B , откуда имеем равенство $AB = BC$ для некоторого C . По лемме 3 найдутся слова P, Q и целое неотрицательное число s такие, что $A = PQ$, $C = QP$, $B = (PQ)^s P$. Таким образом,

$$T^2 = (ABABA)^2 = (AB)^3 CABA = (AB)^3 QP(PQ)^{s+1} PPQ.$$

Отсюда понятно, что либо X начинается словом $(AB)^3 QP$, либо Y оканчивается словом $(PQ)^{s+1} PPQ$. Поскольку X есть начало степени $U = AB$, в первом случае оказалось бы, что $(AB)^3 QP$ совпало бы с $(AB)^3 A = (AB)^3 PQ$, т.е. $PQ = QP$. Из леммы 1 при этом сразу получается, что A и B – степени одного и того же слова, что противоречит простоте слова T .

Рассмотрим вторую из возможностей, т.е. допустим, что Y оканчивается словом $(PQ)^{s+1} PPQ$. Заметим, что $U = AB = (PQ)^{s+1} P$ – простое слово. Лемма 4 дает возможность сделать вывод, что слово $(PQ)^{s+1} PPQ$ не может иметь более короткий период, нежели U . Это приводит к противоречию с тем, что Y имеет период V , который короче периода U .

Теорема доказана.

Эта теорема допускает усиление того же сорта, что и теорема 1. А именно, можно заменить в формулировке слово T^2 на произвольное T -периодическое слово длиной не меньше $|T^2|$. Пусть такое слово имеет вид XY , где слова X, Y удовлетворяют условиям теоремы. Мы считаем, что XY начинается словом T .

Если $|U| = |V|$, то замечание 1 позволяет заключить, что U и V сопряжены. Допустим, что $|U| > |V|$. Отсюда следует, что $|X| > |T|$, поскольку в противном случае X содержалось бы в T , а Y содержало бы T . Тем самым X было бы V -периодическим, и слово U не было бы минимальным периодом для X . Рассмотрим начало W слова XY , имеющее длину $|T^2|$. Оно должно начинаться с X , поскольку является невырожденным T -периодическим. Полагая $W = XZ$ и замечая, что минимальный период слова Z не длиннее, чем у Y , мы можем применить к W утверждение теоремы, получая $|X| < |U^3|$. Случай $|U| < |V|$ рассматривается аналогично.

Допустимо и дальнейшее усиление, а именно, можно считать, что слова X, Y могут перекрываться. Пусть W есть T -периодическое слово с простым периодом T , содержащее не менее двух периодов. Пусть W начинается словом X , оканчивается словом Y , причем $|W| \leq |X| + |Y|$. Как и выше, слова U и V — это минимальные периоды слов X и Y соответственно, каждый из которых короче периода T . В рассмотрении нуждается лишь случай $|U| = |V|$. (Если, например, $|U| > |V|$, то W имеет вид XZ , где Z — конец Y . Тогда $|X| < |U^3|$, так как минимальный период слова Z не длиннее $|V|$.)

Итак, пусть $|U| = |V|$. Без ограничения общности предположим, что $|X| \geq |T|$. Представим W в виде $X'Y$. Если $|X'| \geq |T|$, то рассмотрим начало слова Y длиной $|V|$. Оно сопряжено слову V , а его образ при сдвиге на период T влево будет содержаться в X' , а потому и в X . Отсюда следует, что U и V сопряжены. Если $|X'| < |T|$, то начало слова X , имеющее длину $|U|$, при сдвиге на период T вправо попадет внутрь слова Y , откуда также следует сопряженность периодов.

Автор благодарит рецензента за ценные рекомендации.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Адян С. И. Проблема Бернсайда и тождества в группах. М.: Наука, 1975.
- [2] Guba V. S. The word problem for the relatively free semigroup satisfying $T^m = T^{m+n}$ with $m \geq 4$ or $m = 3, n = 1$ // Int. J. Algebra Comput. 1993. V. 3. № 2. P. 125–140.
- [3] Guba V. S. The word problem for the relatively free semigroup satisfying $T^m = T^{m+n}$ with $m \geq 3$ // Int. J. Algebra Comput. 1993. V. 3. № 3. P. 335–347.
- [4] Lyndon R. C. and Schützenberger M. P. The equation $a^M = b^N c^P$ in a free group // Michigan Math. J. 1962. V. 9. P. 289–298.
- [5] Лаллеман Ж. Полугруппы и комбинаторные приложения. М.: Мир, 1985.
- [6] Guba V. S. Some Properties of Periodic Words. Glasgow University Preprint Series. № 93/09. Glasgow, 1993.
- [7] Губа В. С. Некоторые свойства периодических слов // III Международная конференция по алгебре. Тезисы сообщений. Красноярск, 1993. С. 100.

Вологодский государственный педагогический университет
E-mail: guba@uni-vologda.ac.ru, guba@math.vanderbilt.edu

Поступило
19.11.1998
Исправленный вариант
10.09.2001