Math-Net.Ru

Общероссийский математический портал

С. П. Струнков, О последовательностях в периодических группах, *Дискрет. матем.*, 2007, том 19, выпуск 2, 74–77

DOI: <https://doi.org/10.4213/dm22>

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: 54.166.219.16

26 апреля 2023 г., 05:45:37

О последовательностях в периодических группах

© 2007 г. С. П. Струнков

Вычисляются мощности некоторых множеств неприводимых последовательностей в бесконечных конечно порожденных периодических группах.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 05-01-01018, и ГУ-ВШЭ, грант 06-01-0107.

В работе рассматриваются последовательности в периодических группах с конечным числом образующих. В последнее время теоретические исследования этих объектов комбинаторной теории групп получили дополнительный стимул ввиду возрастающей практической потребности таких различных областей деятельности как вычисления методами Монте-Карло, криптография, техника использования радаров, а также различного рода датчики псевдослучайных чисел и слов [1]. Алгебраический подход, при котором алгебраические объекты являются поставщиками последовательностей, играет важную роль [2]. Выбор периодической группы в качестве источника последовательностей продиктован тем, что рассматриваемые здесь неприводимые последовательности на периодической группе не могут быть периодическими, что является их достоинством [3].

Пусть G — бесконечная периодическая группа, порожденная образующими $a_1, \dots, a_n$. Слово $w = a_{i_1} a_{i_2} \dots a_{i_k}$ длины $|w| = k$ называется неприводимым, если соответствующий элемент $g = a_{i_1} a_{i_2} \dots a_{i_k}$ группы G не может быть представлен в виде произведения $g = a_{j_1} a_{j_2} \dots a_{j_l}$, которому соответствует слово $a_{j_1} a_{j_2} \dots a_{j_l}$ меньшей длины. Отметим, что два слова $a_{i_1} a_{i_2} \dots a_{i_k}$ и $a_{j_1} a_{j_2} \dots a_{j_l}$ называются равными, если $k = l$ и $a_{i_s} = a_{j_s}$ для любого $s = 1, 2, \dots, k$. Бесконечная последовательность $a_{i_1}, a_{i_2}, \dots$ называется неприводимой, если любое ее конечное слово $a_{i_1}, a_{i_2}, \dots, a_{i_k}$ является неприводимым. Бесконечные неприводимые последовательности существуют в любой конечно порожденной бесконечной периодической группе $G = \langle a_1, \dots, a_n \rangle$. Именно, любой точке полного накопления $(a_{i_1}, a_{i_2}, \dots)$ множества W всех неприводимых конечных слов на G , рассматриваемого как подмножество тихоновского произведения T счетного множества конечных пространств $\{a_1, \dots, a_n\}$ (см. [4]), соответствует бесконечная неприводимая последовательность $C = a_{i_1}, a_{i_2}, \dots$. Нас в первую очередь будут интересовать асимптотические свойства множеств неприводимых слов, в частности, вопрос о том, как много различных неприводимых последовательностей в рассматриваемых периодических группах.

Пусть $C = C_0 = a_{i_1}, a_{i_2}, \dots$ — некоторая бесконечная последовательность в группе $G = \langle a_1, \dots, a_n \rangle$. Ее подпоследовательностью индекса k будем называть последовательность $C_k = a_{i_{k+1}}, a_{i_{k+2}}, \dots$. Очевидно, что если последовательность

$C = C_0$ неприводима, то любая ее подпоследовательность также неприводима. Множество $C = \{C_0, C_1, C_2, \dots\}$ всех подпоследовательностей последовательности $C = C_0$ будем обозначать $\langle C \rangle$. Множество $\langle C \rangle$ счетно и при этом естественным образом линейно упорядочено.

Конечное слово $w = a_{j_1}, \dots, a_{j_k}$ бесконечной последовательности $C = a_{i_1}, a_{i_2}, \dots$ называется бесконечно продолжаемым в C , если в C существует бесконечно много подпоследовательностей, начинающихся со слова w . Если число таких подпоследовательностей для слова w в последовательности C конечно, то слово w называется конечно продолжаемым.

Пусть $w_1 = a_{p_1}, \dots, a_{p_k}$, $w_2 = a_{q_1}, \dots, a_{q_l}$ — некоторые конечные слова бесконечной последовательности $C = a_{i_1}, a_{i_2}, \dots$. Через w_1, w_2 будем обозначать слово $w = a_{p_1}, \dots, a_{p_k}, a_{q_1}, \dots, a_{q_l}$, если оно является словом последовательности C . В противном случае эта операция приписывания w_2 к w_1 не определена. Для удобства считаем, что последовательность C содержит пустое слово w_0 и $w, w_0 = w_0, w = w$ для любого слова $w \in C$. Операция приписывания w_1, w_2, w_3 для трех (и более) слов w_1, w_2, w_3 последовательности C определяется естественным способом.

Неприводимые последовательности в бесконечной конечно порожденной группе G формально могут быть двух типов. Последовательность C назовем неоднородной, если для любого ее бесконечно продолжаемого слова w_1 существует слово w_2 такое, что слово w_1, w_2 бесконечно продолжаемо, и при этом для любого слова w_3 такого, что w_1, w_2, w_3 бесконечно продолжаемо в C , выполняется условие, заключающееся в том, что для любого слова w'_3 такого, что $|w'_3| = |w_3|$, $w'_3 \neq w_3$, слово w_1, w_2, w'_3 конечно продолжаемо, либо не является словом последовательности C . Все остальные последовательности на группе G будем называть однородными. Неоднородные последовательности мало интересны для криптографии ввиду значительного отличия частот появления слов w_1, w_2, w_3 и w_1, w_2, w'_3 в них. Алгебраический смысл однородных и неоднородных последовательностей легко можно усмотреть из их определения.

Пусть S — некоторое множество бесконечных последовательностей группы G . Замыканием множества S будем называть такое множество $\bar{S}$, что для любой последовательности $D = a_{i_1}, a_{i_2}, \dots \in \bar{S}$ и любого ее конечного слова $w = a_{i_1}, a_{i_2}, \dots, a_{i_k}$ в множестве S найдется некоторая последовательность $C = a_{i_1}, a_{i_2}, \dots$, начинающаяся со слова $w = a_{i_1}, a_{i_2}, \dots, a_{i_k}$. Другими словами, если S рассматривать как подмножество тихоновского произведения T счетного множества конечных пространств $\{a_1, \dots, a_n\}$, то множество $\bar{S}$ является замыканием множества S в топологическом пространстве T . Легко видеть, что если все последовательности множества S неприводимы, то и все последовательности множества $\bar{S}$ также неприводимы.

Нашей целью является доказательство следующих утверждений.

Теорема 1. Пусть $G = \langle a_1, \dots, a_n \rangle$ — бесконечная периодическая группа. Тогда замыкание $\langle C \rangle$ множества всех подпоследовательностей $\langle C \rangle$ любой неприводимой однородной последовательности C группы G имеет мощность континуума.

Доказательство. Последовательности $C = a_{i_1}, a_{i_2}, \dots$ и $D = a_{j_1}, a_{j_2}, \dots$ назовем равными, если для всех k слова $a_{i_1}, a_{i_2}, \dots, a_{i_k}$ и $a_{j_1}, a_{j_2}, \dots, a_{j_k}$ равны. Заметим, что из периодичности группы G вытекает, что последовательность $C = C_0$ не может быть равной никакой своей подпоследовательности. Так как множество всех подпоследовательностей последовательности C линейно упорядочено, то есть для любых двух подпоследовательностей последовательности C одна из них является подпоследовательностью другой, то никакие подпоследовательности последовательности C не равны между собой.

Так как множество вообще всех бесконечных последовательностей составленных из элементов $a_1, \dots, a_n$, имеет мощность континуума, для доказательства теоремы достаточно в множестве $\overline{\langle C \rangle}$ найти подмножество мощности континуум. Опишем процесс построения такого подмножества. Так как последовательность C однородна, в C существует такое бесконечно продолжаемое слово w_1 , что для любого слова w_2 такого, что слово w_1, w_2 бесконечно продолжаемо в C , в C найдутся по меньшей мере два различных слова одинаковой длины $w_3^{(1)}$ и $w_3^{(2)}$ такие, что слова $w_1, w_2, w_3^{(1)}$ и $w_1, w_2, w_3^{(2)}$ бесконечно продолжаемы в C . Для определенности будем ставить верхние индексы в словах $w_3^{(1)}$ и $w_3^{(2)}$ в соответствии с тем, какое из этих слов ближе расположено к началу. На первом шаге возьмем w_2 равным пустому слову. Существующие по определению однородной последовательности слова $w_3^{(1)}$ и $w_3^{(2)}$ обозначим через $w_{3,1}^{(1)}$ и $w_{3,1}^{(2)}$ соответственно. Поставим слову $w_1, w_{3,1}^{(1)}$ в соответствие число 1, а слову $w_1, w_{3,1}^{(2)}$ — число 2. Предположим, что для любой конечной последовательности $\{\varepsilon_1, \dots, \varepsilon_k\}$ длины k , в которой каждый элемент ε_i равен одному из чисел 1 или 2, в последовательности C построено бесконечно продолжаемое слово $w_1, w_{3,1}^{(\varepsilon_1)}, \dots, w_{3,k}^{(\varepsilon_k)}$. Возьмем $w_2 = w_{3,1}^{(\varepsilon_1)}, \dots, w_{3,k}^{(\varepsilon_k)}$. Тогда слово w_1, w_2 бесконечно продолжаемо в C . Следовательно, по определению однородной последовательности в C существуют два различных слова $w_{3,k+1}^{(1)}$ и $w_{3,k+1}^{(2)}$ одинаковой длины такие, что слова $w_1, w_{3,1}^{(\varepsilon_1)}, \dots, w_{3,k}^{(\varepsilon_k)}, w_{3,k+1}^{(1)}$ и $w_1, w_{3,1}^{(\varepsilon_1)}, \dots, w_{3,k}^{(\varepsilon_k)}, w_{3,k+1}^{(2)}$ бесконечно продолжаемы в C . Продолжая это построение, получаем соответствие между всеми бесконечными последовательностями $\varepsilon_1, \varepsilon_2, \dots$, составленными из чисел 1 и 2, и последовательностями $w_1, w_{3,1}^{(\varepsilon_1)}, w_{3,2}^{(\varepsilon_2)}, \dots$. Это соответствие является взаимно однозначным, так как если $\varepsilon_1, \varepsilon_2, \dots$ и $\varepsilon'_1, \varepsilon'_2, \dots$ — произвольные последовательности, составленные из чисел 1 и 2, и при этом $\varepsilon_i = \varepsilon'_i$ для $i = 1, \dots, k-1$, а $\varepsilon_k \neq \varepsilon'_k$, то $w_{3,i}^{(\varepsilon_i)} = w_{3,i}^{(\varepsilon'_i)}$ для всех $i = 1, \dots, k-1$, а $w_{3,k}^{(\varepsilon_k)} \neq w_{3,k}^{(\varepsilon'_k)}$ и при этом $|w_{3,k}^{(\varepsilon_k)}| = |w_{3,k}^{(\varepsilon'_k)}|$. Следовательно, последовательности $w_1, w_{3,1}^{(\varepsilon_1)}, w_{3,2}^{(\varepsilon_2)}, \dots$ и $w_1, w_{3,1}^{(\varepsilon'_1)}, w_{3,2}^{(\varepsilon'_2)}, \dots$ различны и соответствие между последовательностями $\varepsilon_1, \varepsilon_2, \dots$ и $w_1, w_{3,1}^{(\varepsilon_1)}, w_{3,2}^{(\varepsilon_2)}, \dots$ в самом деле взаимно однозначное. Так как все конечные слова $w_1, w_{3,1}^{(\varepsilon_1)}, \dots, w_{3,k}^{(\varepsilon_k)}$ являются словами последовательности C , все последовательности $w_1, w_{3,1}^{(\varepsilon_1)}, w_{3,2}^{(\varepsilon_2)}, \dots \in \overline{\langle C \rangle}$. Утверждение теоремы вытекает из того, что множество всех различных последовательностей $\varepsilon_1, \varepsilon_2, \dots$, составленных из чисел 1 и 2, имеет мощность континуума. Теорема доказана.

Теорема 2. Для любой неоднородной неприводимой последовательности C множество $\overline{\langle C \rangle}$ счетно.

Доказательство. Пусть $C' \in \overline{\langle C \rangle}$, где C — произвольная неприводимая последовательность. Покажем, что если C' содержит конечно продолжаемое слово w последовательности C , то C' равна некоторой подпоследовательности последовательности C . Пусть C_M — подпоследовательность последовательности C максимального индекса, в которой w является начальным словом. Тогда начальные слова достаточно большой длины, содержащие все слова w в C' , являются начальными словами подпоследовательностей последовательности C индексов, не превосходящих числа M . Следовательно, начиная с некоторого номера N , все начальные слова последовательности C' длины, большей или равной N , являются начальными словами некоторой подпоследовательности, индекс которой не превосходит числа M . Следовательно, вся последовательность C' совпадает с этой подпоследовательностью. Поэтому можно доказывать теорему для множества после-

довательностей, содержащихся в замыкании $\overline{\langle C \rangle}$, не содержащих конечно продолжаемых слов последовательности C .

Заметим, что для любого бесконечно продолжаемого слова w произвольной неприводимой последовательности C в C всегда существует слово $\tilde{w}$ любой заданной длины такое, что слово $w, \tilde{w}$ бесконечно продолжаемо в C .

Будем называть бесконечную неприводимую последовательность $C' \in \overline{\langle C \rangle}$ последовательностью первого рода, если в ней имеется бесконечно продолжаемое в C слово w , для которого в C существует единственное слово $\tilde{w}$ любой заданной длины такое, что все слова $w, \tilde{w}$ бесконечно продолжаемы в C . Так как C' не содержит конечно продолжаемых в C слов, слово w только один раз входит в слово C' . В противном случае бесконечные подпоследовательности, стоящие за словами w , находящимися на разных местах последовательности C' , будут равны и, следовательно, будут периодическими. Отсюда вытекает, что любая неприводимая последовательность $C' \in \overline{\langle C \rangle}$ имеет вид $C' = w_1, w, \tilde{w}, \dots$, где $\tilde{w}$ обозначает бесконечную неприводимую подпоследовательность в C' бесконечно продолжаемых в C слов, которую однозначно определило в C слово w , а w_1 — начальное слово последовательности C' .

Если последовательность $C' \in \overline{\langle C \rangle}$ является последовательностью второго рода, то есть для любого слова $w \in C'$ в C существуют по меньшей мере два разных слова $\tilde{w}$ и $\tilde{w}'$ одинаковой длины таких, что слова $w, \tilde{w}$ и $w, \tilde{w}'$ бесконечно продолжаемы в C , то C — однородная последовательность.

Таким образом, всякая неприводимая последовательность $C' \in \overline{\langle C \rangle}$, не содержащая конечно продолжаемых в C слов, является последовательностью первого рода. Но в этом случае она однозначно определяется упорядоченной парой слов w_1 и w . Так как множество вообще всех упорядоченных пар конечных слов w_1, w_2 счетно, множество всех последовательностей $C' \in \overline{\langle C \rangle}$ также счетно, что и требовалось доказать.

Список литературы

1. Ноден П., Китте Л., *Алгебраическая алгоритмика*. Мир, Москва, 1999.
2. Sánchez S., Criado R., Vega C., Recurrence sequences over residual rings. *Algebra Discrete Math.* (2005) №4, 81–92.
3. Sánchez S., Criado R., Vega C., A generator of pseudo-random numbers sequences with a very long period. *Math. Comput. Modelling* (2005) **42**, 809–816.
4. Понтрягин Л. С., *Непрерывные группы*. Наука, Москва, 1973.

Статья поступила 12.04.2006.