Отзыв

о статье А. Н. Рыбалова

«О генерической сложности проблемы проверки тождеств в конечных группах и моноидах»

Рецензируемая статья не может быть рекомендована к публикации. Прежде всего, бóльшая часть результатов этой статьи уже опубликована автором в работе ‘A generic algorithm for the identity problem in finite groups and monoids’ (Journal of Physics: Conference Series **1546** (2020), article no. 012101, `doi:10.1088/1742-6596/1546/1/012101`). А именно, теоремы 1 и 2 рецензируемой статьи совпадают соответственно с теоремами 1 и 2 работы из Journal of Physics: Conference Series. Отмечу, что в рецензируемой статье нет ссылки на указанную работу.

Новой по сравнению с работой из Journal of Physics: Conference Series является только теорема 3. Эта теорема утверждает, что проблема проверки тождеств генерически полиномиально разрешима во всех конечных моноидах Брандта. Однако на самом деле при том подходе к определению множества входов проблемы проверки тождеств, который использует автор, нетрудно доказать более общий факт: *проблема проверки тождеств генерически полиномиально разрешима во всех конечных моноидах.*

Действительно, автор считает входом размера n пару слов (p, q) над фиксированным алфавитом из n букв, такую, что $|p| + |q| = n$. Нетрудно подсчитать, что число T_n таких входов равно $n^n(n+1)$ — на каждую позицию в слове длины n можно поставить любую из n букв и есть $n+1$ способ разбить слово длины n на два куска p и q (один из которых может быть пустым). Назовем множество букв, участвующих в записи некоторого слова, *содержанием* этого слова и оценим число S_n входов, в которых содержания слов p и q совпадают. Для таких входов в записи более короткого из этих двух слов может участвовать максимум $\lfloor \frac{n}{2} \rfloor$ букв, поэтому S_n заведомо не больше, чем число Q_n всех тех входов, в записи которых участвует $\lfloor \frac{n}{2} \rfloor$ букв. Понятно, что $Q_n = \binom{n}{\lfloor \frac{n}{2} \rfloor} \lfloor \frac{n}{2} \rfloor^n (n+1)$ — есть $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ способов выбрать $\lfloor \frac{n}{2} \rfloor$ букв из n букв данного алфавита, после чего на каждую позицию в слове длины n можно поставить любую из выбранных $\lfloor \frac{n}{2} \rfloor$ букв и разбить слово длины n на два куска p и q (один из которых может быть пустым), для чего есть $n+1$ способ. Используя верную при всех $n \geq 1$ оценку для среднего биномиального коэффициента $\binom{2n}{n} \leq \frac{4^n}{\sqrt{\pi n}}$, получаем

$$Q_n = \binom{n}{\lfloor \frac{n}{2} \rfloor} \left\lfloor \frac{n}{2} \right\rfloor^n (n+1) \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} \left(\frac{n}{2}\right)^n (n+1) \leq \frac{4^{\frac{n}{2}}}{\sqrt{\pi \frac{n}{2}}} \frac{n^n}{2^n}(n+1) = \frac{T_n}{\sqrt{\pi \frac{n}{2}}}.$$

Поэтому частное $\frac{Q_n}{T_n} \leq \frac{1}{\sqrt{\pi \frac{n}{2}}}$ стремится к 0 при $n \to \infty$, откуда и частное $\frac{S_n}{T_n} \leq \frac{Q_n}{T_n}$ стремится к 0 при $n \to \infty$. В терминологии автора это означает, что множество входов, в которых содержания слов p и q совпадают, пренебрежимо.

Пусть теперь M произвольный конечный моноид. Если M одноэлементен, то в M выполнено любое тождество. Если M содержит неодноэлементную подгруппу, то проблема проверки тождеств в M генерически полиномиально разрешима по теореме 2 упомянутой выше работы автора из Journal of Physics: Conference Series. Наконец, если моноид M неодноэлементен, а все подгруппы в M одноэлементны, то множество $M \setminus \{1\}$ образует непустой идеал в M и фактормоноид Риса по этому идеалу изоморфен моноиду $\{0, 1\}$, где 0 и 1 перемножаются обычным образом. Хорошо известно (и легко проверяется), что тождество $p = q$ выполняется в последнем моноиде тогда и только тогда, когда содержания слов p и q совпадают. Теперь рассмотрим следующий алгоритм для проверки тождеств в M: на входе $p = q$ алгоритм возвращает НЕТ, если содержания слов p и q не совпадают, и НЕ ЗНАЮ в противном случае. Тогда множество входов, на которых алгоритм возвращает НЕ ЗНАЮ, пренебрежимо, а те входы, на которых алгоритм возвращает НЕТ, отвечают тождествам, не выполняющимся в моноиде $\{0, 1\}$ и тем более в моноиде M. Итак, описанный алгоритм генерически полиномиален.