## Секция «Математика и механика»

### Некоторые нетривиальные верхние оценки в задаче быстрого возведения в степень при ограничениях на объём используемой памяти

***Балакин Константин Сергеевич***
*Аспирант*
*Московский государственный университет имени М.В. Ломоносова,*
*Механико-математический факультет, Москва, Россия*
*E-mail: bal_ks@mail.ru*

В качестве отправной точки рассматривается классическая задача о сложности возведения в степень - нахождении минимального числа операций умножения, достаточного для возведения некоторого числа $x$ в некоторую степень $n$ (обозначается $l(n)$). Известен результат [3] о том, что эта функция асимптотически равна $\log_2 n$, но при этом алгоритм доказательства требует возрастающего с ростом $n$ числа ячеек памяти. Возникает естественный вопрос об исследовании сложности возведения в степень в случае фиксированного числа ячеек памяти.

Известно [1], что для любого фиксированного числа ячеек памяти $t$ найдётся такое $\varepsilon = \varepsilon(t) > 0$, что минимальное число операций умножения, достаточного для возведения некоторого числа $x$ произвольную степень $n$ (обозначается $l_t(n)$), для почти всех чисел $n$ не менее $(1+\varepsilon)\log_2 n$.

Что касается верхних оценок, то достаточно легко получается, что, при $t = 2^k + 1$ для некоторого $k \geq 0$, $l_t(n) \leq (1 + \frac{1}{1+k})\log_2 n$. Соответственно интерес представляет получение нетривиальных оценок (тривиальные получаются из того факта, что $l_t(n)$ не возрастает с ростом $t$) на функцию $l_t(n)$, когда $t \neq 2^k + 1$. Минимальным таким $t$ является $t = 4$.

***

В работе показано, что $l_4(n) < (\frac{3}{2} - \varepsilon)\log_2 n$ для некоторого $\varepsilon > 0$. Также приводятся оценки на значение $\varepsilon$.

### Литература

1. Балакин К.С. О сложности возведения в степень при ограничениях на используемую память //Материалы X Международного семинара "Дискретная математика и ее приложения М.,2010, с.85-87.

2. Кнут Д.Е. Искусство программирования для ЭВМ. Т.2. М., 1977.

3. Brauer A. On addition chains // Bull. Amer. Math. Soc. - 1939. - V.45 - pp.736-739

### Слова благодарности

Автор выражает глубочайшую благодарность своему научному руководителю В.В. Кочергину за ценные замечания в процессе работы.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863).