Секция «Математика и механика»

Оптимизация алгоритма умножения полиномов над кольцом

Лысов Михаил Андреевич
Аспирант
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Дзержинский, Россия
E-mail: sslys@yandex.ru

В настоящей работе построен алгоритм умножения многочленов с коэффициентами из алгебры над $\mathbb{F}_2$.

Теорема. Существует билинейный алгоритм, который для любой алгебры[1] *A над $\mathbb{F}_2$ вычисляет произведение любой пары многочленов из $A[x]$ степеней не выше n за $O(n \log n \log\log n)$ сложений в A и арифметических операций в $\mathbb{F}_2$ и $O(\frac{n \log n}{\log\log n} 2^{\log_2^* n})$ умножений в A.*

Итерированным логарифмом по основанию 2 называется $\log_2^* x = $
$= min\{i \geq 0 : \log_2^{(i)} x \leq 1\}$, где кратный логарифм кратности $k \geq 0$ определяется из соотношения $\log^{(k)} x = \log(\log^{(k-1)} x)$, где $\log^{(0)} x = x$.

В конце статьи проведено сравнение полученного алгоритма с лучшим предыдущим известным, и выделен случай, в котором построенный алгоритм эффективней.

Лучшим предыдущим известным результатом на эту тему является статья [1]. В ней доказано, что существует билинейный алгоритм, который для любого кольца R пару многочленов степеней n с коэффициентами из R перемножает за $O(n \log n \log\log n)$ аддитивных операций в R и $O(n \log n)$ мультипликативных. Теорема 1 улучшает этот результат в более узком классе колец: колец характеристики 2, поскольку алгебра над $\mathbb{F}_2$ и кольцо характеристики 2 – это одно и то же. Число сложений остаётся без изменения, добавляются арифметические операции в $\mathbb{F}_2$, которые можно считать проще сложений в кольце или принять за предвычисления. А число умножений в кольце уменьшается, поскольку $\log_2^* n$ растёт медленне любого кратного логарифма.

Для случая алгебры A, совпадающей с $\mathbb{F}_2$, применять данный алгоритм скорее всего бессмыслено, поскольку константа в $O()$ в аддитивных операциях больше, чем константа там же в теореме из [1]. При умножении матричных многочленов применять алгоритм из теоремы 1 эффективней. Такая задача возникает, как этап в некоторых алгоритмах решения разреженных систем линейных уравнений над $\mathbb{F}_2$. При достаточно больших размерах матриц, их умножение требует намного больше времени, чем сложение. Поэтому число умножений в алгебре становится главным параметром, влияющим на эффективность алгоритма умножения матричных многочленов, а теорема 1 именно этот параметр и улучшает.

Литература

1. D.Cantor, E.Kaltofen On fast multiplication of polynomials over arbitrary algebras // Acta Informatica 28, 693-701,1991.

[1]Здесь и далее под термином алгебра понимается не обязательно конечномерная, не обязательно коммутативная, не обязательно ассоциативная алгебра над полем.

2. Haining Fan, M. Anwar, Hasan Senior Member Comments on “five, Six, and Seven-Term Karatsuba-Like Formulae" // IEEE Transactions on Computers, volume 56, pages 716–717, 2007.

3. S.Gao, T.Mateer Additive Fast Fourier Transforms over finite fields // IEEE Transactions on information theory,2010.

4. S.Gao, D.Panario Tests and constructions of irreducible polynomials over finite fields // In Foundations of Computational Mathematics, ed. F. Cucker, M. Shub, 346-361, Springer Verlag, 1997.

5. Mateer, Todd D. Fast Fourier Transform Algorithms with Applications. PhD Dissertation. Доступна онлайн на http://cr.yp.to/f2mult.html.