УДК 621.391

С. В. ФЕДОРЕНКО

МОДИФИКАЦИЯ АЛГОРИТМА ГЕРЦЕЛЯ—БЛЕЙХУТА

Рассматриваются классический алгоритм Герцеля—Блейхута вычисления дискретного преобразования Фурье над конечным полем, а также его модификации. Показано, что модифицированный алгоритм относится скорее к классу быстрых алгоритмов вычисления дискретного преобразование Фурье, чем к классу полубыстрых.

Ключевые слова: *дискретное преобразование Фурье, быстрое преобразование Фурье, сложность алгоритма, быстрый алгоритм, полубыстрый алгоритм, конечное поле.*

Быстрый алгоритм — это вычислительная процедура, которая значительно сокращает число необходимых операций сложения и умножения по сравнению с прямым метод вычисления. Быстрое преобразование Фурье (БПФ) — это метод вычисления n-точечного преобразования, который использует около $n \log n$ операций умножения и около $n \log n$ операций сложения в поле вычисления преобразования Фурье [1].

Полубыстрый алгоритм — это вычислительная процедура, позволяющая значительно сократить число необходимых операций умножения по сравнению с прямым метод вычисления, не уменьшая число сложений. Полубыстрый алгоритм вычисления преобразования Фурье —

это метод вычисления n-точечного преобразования Фурье, который использует около $n \log n$ операций умножения и около n^2 операций сложения в поле вычисления преобразования Фурье [1].

Дискретное преобразование Фурье (ДПФ) длины n вектора $\mathbf{f} = (f_i)$, $i \in [0, n-1]$, $n \mid (q-1)$, в конечном поле $GF(q)$ есть вектор $\mathbf{F} = (F_j)$,

$$F_j = \sum_{i=0}^{n-1} f_i \alpha^{ij}, \qquad j \in [0, n-1],$$

где α (ядро ДПФ) является элементом порядка n в конечном поле $GF(q)$.

Далее предполагается, что длина n-точечного преобразования Фурье над $GF(2^m)$ есть $n = 2^m - 1$. Произвольный вектор $\mathbf{f} = (f_i)$, $i \in [0, n-1]$, свяжем с многочленом $f(x) = \sum_{i=0}^{n-1} f_i x^i$ и получим $F_j = f(\alpha^j)$. Поле вычисления преобразования Фурье есть конечное поле $GF(2^m)$, а α — примитивный элемент поля $GF(2^m)$. Все логарифмы вычисляются по основанию 2.

Алгоритм Герцеля—Блейхута. Рассмотрим модификацию [2, 3] алгоритма для вычисления ДПФ над конечными полями [4, 5].

Алгоритм Герцеля—Блейхута состоит из двух шагов. На первом шаге выполняется деление с остатком многочлена $f(x)$ на каждый минимальный многочлен $M_k(x)$:

$$\begin{cases} f(x) = M_k(x)\, q_k(x) + r_k(x), \\ \deg r_k(x) < \deg M_k(x) = m_k, \\ k \in [0, l-1], \end{cases}$$

где $r_k(x) = \sum_{j=0}^{m_k-1} r_{j,k} x^j$, l — число двоичных классов сопряженности.

На втором шаге выполняется вычисление значений $r_k(x)$ во всех элементах конечного поля:

$$\begin{cases} F_i = f(\alpha^i) = r_k(\alpha^i) = \sum_{j=0}^{m_k-1} r_{j,k} \alpha^{ij}, \\ i \in [0, n-1], \end{cases}$$

где элемент α^i — корень минимального многочлена $M_k(x)$.

Алгоритм Герцеля—Блейхута принадлежит к классу полубыстрых и имеет сложность порядка $n \log n$ операций умножения и порядка n^2 операций сложения над элементами поля $GF(2^m)$ [2].

Модификация первого шага алгоритма Герцеля—Блейхута. В работе [6] предложен способ улучшения первого шага алгоритма Герцеля—Блейхута, в ней показано, что асимптотическая сложность этого шага составляет $O(n\ (\log n)^2 \log \log n)$ операций над элементами поля $GF(2^m)$.

Построим дерево делителей. На самом нижнем уровне находятся l минимальных многочленов. Предположим, что l есть степень числа 2, иначе дополним множество минимальных многочленов до степени числа 2 фиктивными многочленами, равными единице. На следующем уровне располагаются $l/2$ произведений пар минимальных многочленов. Далее на

каждом уровне располагаются произведения пар многочленов из предыдущего уровня. В корне дерева находится двучлен $x^{2^m-1}-1$. Алгоритм состоит в последовательном вычислении остатков от деления, начиная с исходного многочлена $f(x)$, на все делители из каждого уровня дерева сверху вниз. Известно, например [7], что сложность деления многочлена степени $2s$ на многочлен степени s имеет порядок $D(s)=O(s\ \log s\ \log\log s)$ операций. Из очевидного неравенства $pD(s/p)\le D(s)$ следует, что для каждого уровня дерева сложность вычисления всех остатков от делений не превышает $D(n)$. Число уровней в дереве делителей есть $\log\ l=O\left(\log\ \frac{n}{m}\right)=O(\log\ n)$. Тогда общее число операций имеет порядок $D(n)\ \log\ l=O(n\ (\log n)^2\ \log\log n)$. Заметим, что приведенная оценка сложности алгоритма явно завышена.

Модификация второго шага алгоритма Герцеля—Блейхута. Предложим вариант улучшения второго шага алгоритма Герцеля—Блейхута. Из работ [8, 9] следует, что второй шаг алгоритма можно свести к вычислению l m-точечных циклических сверток. Конструктивный метод построения циклических сверток для длин $m=2^i$, $i\ge 0,$ имеющий сложность порядка $\frac{1}{2}\ m\log m$ операций умножения и $m\log m$ операций сложения, введен автором настоящей статьи. Таким образом, верхняя оценка асимптотической сложности второго шага алгоритма имеет порядок $O(l\ m^2)=O\left(\frac{n}{m}\ m^2\right)=O(n\ \log n)$ операций сложения и умножения над элементами поля $GF(2^m)$.

Заключение. В работе показано, что модификация алгоритма Герцеля—Блейхута с общей сложностью порядка $O(n\ (\log n)^2\ \log\log n)$ операций над элементами поля $GF(2^m)$ относится скорее к классу быстрых алгоритмов вычисления ДПФ, чем к классу полубыстрых алгоритмов.

Автор выражает признательность фонду имени Александра фон Гумбольдта (Германия) за многолетнюю поддержку научных исследований.

СПИСОК ЛИТЕРАТУРЫ

1. *Blahut R. E.* Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach. Cambridge, UK: Cambridge University Press, 2008. 543 p.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
3. *Blahut R. E.* Fast Algorithms for Signal Processing. Cambridge, UK: Cambridge University Press, 2010. 453 p.
4. *Goertzel G.* An algorithm for the evaluation of finite trigonometric series // The American Mathematical Monthly. 1958. Vol. 65, N 1. P. 34—35.
5. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1989. 448 с.
6. *Trifonov P.* On the additive complexity of the cyclotomic FFT algorithm // Proc. of the IEEE Information Theory Workshop. Lausanne, Switzerland, 2012. P. 537—541.
7. *von zur Gathen J., Gerhard J.* Modern computer algebra. Cambridge, UK: Cambridge University Press, 1999.
8. *Трифонов П. В., Федоренко С. В.* Метод быстрого вычисления преобразования Фурье над конечным полем // Проблемы передачи информации. 2003. Т. 39, № 3. С. 3—10.
9. *Fedorenko S. V.* The discrete Fourier transform over a finite field with reduced multiplicative complexity // Proc. of the IEEE Intern. Symp. on Information Theory. St. Petersburg, 2011. P. 1200—1204.

Сведения об авторе

Сергей Валентинович Федоренко — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: sfedorenko@ieee.org

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.