# Новый алгоритм синтеза всех неприводимых многочленов над заданным конечным полем

***Леухин А. Н., Бахтин С. А.***
inf@marstu.mari.ru
Йошкар-Ола, ГОУ ВПО Марийский гос. тех. университет

Проведен обзор проблемы синтеза неприводимых и примитивных многочленов над заданным конечным полем. Предложен новый быстрый детерминированный алгоритм синтеза всех неприводимых многочленов над конечным полем $F_p$ заданной степени $n$, основанный на модифицированном быстром методе Крылова для вычисления характеристического многочлена матрицы Фробениуса, сопровождающей неприводимый многочлен над заданным конечным полем.

Теория многочленов степени $n$ от одной переменной, неприводимых над конечными полями $F_p$, представляет существенный интерес как для исследования алгебраической структуры конечных полей $F_{q=p^n}$, так и для многочисленных приложений в современной теории передачи информации. Такие многочлены имеют большое значение при синтезе шумоподобных кодовых последовательностей, в теории помехоустойчивого кодирования, в криптографии при решении задачи дискретного логарифмирования (к которой сводится задача логарифмирования на эллиптической кривой), в теории кольцевых счетчиков, и т. д.

Первое крупное исследование о неприводимых многочленах от одной переменной над полем $F_q$ проведено в работе [1]. Фундаментальный обзор результатов по теории конечных полей, включающий и теорию неприводимых многочленов, приводится в работе [2]. Однако, несмотря на достигнутые успехи в теории синтеза неприводимых многочленов, имеется ряд важнейших проблем, которые до сих пор не поддаются решению. Одной из них является проблема построения неприводимых многочленов заданной степени в явном виде, а также определения периодов элементов поля — корней этих многочленов.

По существу, все подходы к синтезу неприводимых многочленов можно разделить на три большие группы. К первой группе можно отнести аналитические методы построения, позволяющие в явном виде сразу записать выражения для неприводимых многочленов. В роли таких многочленов чаще всего выступают полиномы с малым числом слагаемых — двучлены, трехчлены и четырехчлены.

В работе [2] приводятся теоремы для неприводимых двучленов и трехчленов. Конкретные примеры аналитических выражений для неприводимых многочленов, удовлетворяющие приведенным теоремам, приводятся в работе [3]. Конструкции неприводимых многочленов над полем $F_2$ степени $4 \cdot 3^k \cdot 5^l$, над полем $F_3$ степени $4 \cdot 2^k \cdot 5^l$, над полем $F_p$ $(p > 3)$ степени

$2 \cdot 2^k \cdot 3^l$ можно найти в работе [4]. Другие аналитические конструкции неприводимых многочленов над конечными полями в явном виде приведены в работах [5, 6].

К сожалению, в явном виде не удается получить выражения для неприводимых многочленов произвольной степени $n$ над полем $F_q$. Кроме того, в явном виде невозможно записать все неприводимые многочлены заданной степени $n$.

Следующая группа методов синтеза основана на идее факторизации многочлена произвольно заданной степени $n$ в конечном поле $F_q$ . Неприводимость многочлена устанавливается по результатам факторизации. Первые существенны результаты получены в работе [7], опираясь на которые, в работе [8] синтезирован улучшенный и эффективный в вычислительном плане метод. В дальнейшем на основе методов факторизации появились вероятностные [9] и детерминированные [10] алгоритмы-тесты на неприводимость многочлена произвольной степени $n$ над полем $F_q$, позволяющие решать задачу за полиномиальное время.

В третью группу методов синтеза неприводимых полиномов входят алгоритмы построения неприводимых и примитивных многочленов, использующих алгебраическую структуру и внутреннее строение полей Галуа. В отличии от двух предыдущих случаев, данные методы позволяют синтезировать сразу все возможные неприводимые или примитивные многочлены степени $n$ над $F_q$. Первый алгоритм — алгоритм решета — является прямым методом синтеза неприводимых многочленов [2], и для его реализации нет необходимости в использовании «начального» неприводимого многочлена. Однако этот алгоритм имеет низкую вычислительную производительность и может использоваться для малых размерностей степени многочлена $n$ и характеристики $p$ поля. Второй алгоритм [2] основан на свойствах минимальных многочленов степени $n$ поля $F_q$. Для его реализации требуется один «начальный» неприводимый полином степени $n$ над $F_q$ для задания внутренней структуры поля. В работе [11] описан метод построения новых неприводимых многочленов над полем, исходя из данного неприводимого многочлена.

В ходе исследовательской работы нами был получен алгоритм синтеза всех возможных примитивных многочленов степени $n$ над полем $F_p$. На первом шаге формируется матрица Фробениуса, сопровождающая «начальный» примитивный многочлен. На втором шаге определяются подмножества коэффициентов $p$-сопряженных элементов поля $F_{p^n}$, и на их основе формируются множество кооффициентов, содержащее любой из элементов каждого подмножества. На третьем шаге исходная матрица возводится в степень коэффициента множества. На четверттом шаге с использованием метода Крылова формируется матрица, по кото-

рой будет вычисляться характеристический многочлен в конечном поле. Для ее формирования в качестве нулевого вектора используется вектор вида $u_0 = 1,\ u_1 = 0,\ u_2 = 0,\ \ldots,\ u_{n-1} = 0$. На пятом шаге с помощью модифицированного метода исключения Гаусса, позволяющего проводить триангуляцию матрицы даже с нулевыми элементами на главной диагонали, с учетом выполнения операций деления в конечном поле $F_p$, формируется матрица Крылова. Последний элемент $A_{n,n}$ этой матрицы представляет собой искомый неприводимый многочлен над полем $F_{p^n}$. Отметим, что процедуры возведения матрицы в степень выполняются дихотомическим способом.

Отличие предлагаемого алгоритма от рассмотренных выше заключается в том, что для его реализации не требуется введение трудоёмких в вычислительном плане операций умножения и деления многочленов в конечном поле $F_{p^n}$. Все операции выполняются в поле $F_p$, при этом возрастает производительность и снижаются требования к объёму используемой памяти.

Программная реализация предлагаемого в работе быстрого алгоритма показала удовлетворительные результаты при сравнительном анализе быстродействия с аналогичными специализированными математическими продуктами GAP 4.4.6 группы разработчиков Gap Group и MAGMA 2.12 группы разработчиков Computational Algebra Group.

С помощью такого быстрого алгоритма синтеза, реализованного на современной элементной базе, могут быть успешно решены задачи помехоустойчивого приёма информации, кодового разделения каналов передачи информации и задач криптографии.

Работа выполнена при поддержке РФФИ, проект №07-07-00285, и гранта Президента РФ МД-63.2007.9.

**Литература**

[1] *Dickson L. E.* Linear Groups with an Exposition of the Galois Field Theory. — New York: 1958.

[2] *Лиддл Р., Ниддерайтер Г.* Конечные поля. — М.: Мир. Т.1,2. 1988

[3] *Gao Sh., Panario D.* Foundations of Computational Mathematics. — Springer. 1997. P.346.

[4] *Shparlinski I.* Apl. Alg. Eng. Comm. 1993. v.4. P.263.

[5] *Gao S., Mullen G.* J. Number Theory. 1994. v.49. P.118.

[6] *Menezes A., Blake I., Gao X., Mullin R., Vanstone S., Yaghoobian T.* Applications of Finite Fields. Kluwer Academic Publisher. 1993.

[7] *Butler M.* Quart. J. Math. Oxford Ser. (2). 1954. v.5. P.102.

[8] *Berlekamp E. R.* Math. Comp. 1970. v.24. P.713-735.

[9] *Rabin M. O.* SIAM J. Comp. 9. 1980. P.273.

[10] *Shoup V.* J. Symb. Comp. 20. 1996. P.363.

[11] *Варшамов Р. Р., Антонян А. М.* Докл. АН АрмССР. т.66. №4. 1978. С.197.