УДК003.26:51:004(075.8)

Программные аспекты нахождения примитивных полиномов больших степеней

Королева М.Н., Липницкий В.А.
Белорусский национальный технический университет
Военная академия Республики Беларусь

Конечные поля играют важнейшую роль в помехоустойчивом кодировании [1]. В теории конечных полей многочлены, а особенно неприводимые многочлены играют важнейшую роль. Всякое поле содержит минимальное подполе и является его расширением – векторным пространством. Фактор-кольца по максимальным идеалам являются источником полей, в том числе конечных полей. Всякое конечное (конечномерное, как векторное пространство) сепарабельное [2] расширение конкретной степени n изоморфно фактор-кольцу (Z/pZ)[x]/<q(x)> кольца полиномов Z/pZ[x] с коэффициентами из минимального подполя Z/pZ по его главному максимальному идеалу, порожденному неприводимым многочленом степени n [3]. Всякое поле Галуа состоит из p^n элементов $n \geq 1$, p – характеристика поля, Z/pZ минимальное подполе. Мультипликативная группа конечного поля – циклическая. Вычисления в полях Галуа $F(p^n)$ проводятся идеально при фиксации в них примитивных элементов – корней неприводимых примитивных полиномов. Ведь если α – примитивный элемент поля F(p^n), то все элементы этого поля исчерпываются множеством $\{0, \alpha, \alpha^2, \dots, \alpha^{p^n-1}=1\}$ и перемножать степени элементов значительно удобнее [4].

Таким образом, для работы в поле Галуа необходимо в первую очередь зафиксировать неприводимый примитивный полином с требуемыми параметрами.

К сожалению, данная проблема имеет релевантный характер, не имеет четких очертаний, и каждый раз требует серьёзных интеллектуальных и вычислительных усилий, с применением компьютерных технологий [5].

Литература

1. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
2. Ленг С. Алгебра – М., Мир, 1968.-572с.
3. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. Т. 1. Пер. с англ. – М.: Мир, 1988. – 413 с.
4. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. – Мн.: БГУИР, 2005. – 88 с.; 2-е издание: Мн.: БГУИР, 2006. – 88 с.