ACTA ARITHMETICA
XLIX (1987)

О построении нормального базиса конечного поля

С. А. Степанов, И. Е. Шпарлинский (Москва)

Семидесятипятилетию профессора Пауля Эрдёша посвящается

Пусть n — натуральное, q — степень простого числа, $F = \mathrm{GF}(q)$ и $K = \mathrm{GF}(q^n)$ — конечные поля из q и q^n элементов соответственно.

Базис $\theta_1, \ldots, \theta_n$ поля K, рассматриваемого как n-мерное векторное пространство над полем F, называется *нормальным*, если при некотором $\theta \in K$ он имеет вид $\theta_1 = \theta$, $\theta_2 = \theta^q, \ldots, \theta_n = \theta^{q^{n-1}}$. Существование нормального базиса было впервые доказано К. Гензелем (историю вопроса и доказательство можно найти в [1]).

Базисы такого вида возникают в различных вопросах теории кодирования, позволяют существенно ускорить процедуру декодирования некоторых кодов (см. [2], [3]).

В настоящей работе в случае $(n, q) = 1$ предложен алгоритм построения нормального базиса поля K, время работы которого ограничено полиномом от n и $\ln q$. В частности, в наиболее важном для приложений случае фиксированного q и растущего n время работы алгоритма ограничено полиномом от n.

Теорема. *При* $(n, q) = 1$ *нормальный базис поля* K *может быть построен за время, ограниченное полиномом от* n *и* $\ln q$.

Пусть $\omega_1, \ldots, \omega_n$ произвольный базис поля K. Матрицу $A = (a_{ij})_{i,j=1}^n$ с элементами из поля F определим равенствами

$$\omega_i^q = a_{i1}\omega_1 + \ldots + a_{in}\omega_n, \quad i = 1, \ldots, n. \tag{1}$$

Таким образом

$$(\omega_1^q, \ldots, \omega_n^q)^T = A(\omega_1, \ldots, \omega_n)^T.$$

Возводя обе части (1) в степень q^{j-1}, получаем

$$\omega_i^{q^j} = a_{i1}\omega_1^{q^{j-1}} + \ldots + a_{in}\omega_n^{q^{j-1}}.$$

Отсюда вытекает, что

$$(\omega_1^{q^j}, \ldots, \omega_n^{q^j})^T = A^j(\omega_1, \ldots, \omega_n)^T. \tag{2}$$

Учитывая, что $\omega^{q^n} = \omega$ при $\omega \in K$ и, что $\omega_1, \ldots, \omega_n$ — базис поля K, получаем отсюда равенство $A^n = E$, где E — единичная матрица.

Так как $(n, q) = 1$, то характеристический многочлен $f(\lambda) = \lambda^n - 1$ матрицы A не имеет кратных корней. Пусть

$$f(\lambda) = \prod_{v=1}^{m} f_v(\lambda) \tag{3}$$

его разложение на неприводимые над F многочлены $f_1, \ldots, f_m$, степени которых $d_1, \ldots, d_m$.

Через $\lambda_{v1}, \ldots, \lambda_{vd_v}$ обозначим собственные значения матрицы A, которые являются корнями многочлена $f_v(\lambda)$. Найдем собственный вектор z_{v1}, матрицы A, соответствующий λ_{v1}. Для этого необходимо найти в поле $\mathrm{GF}(q^{d_v})$ ненулевое решение системы линейных уравнений

$$z_{v1}(A - \lambda_{v1} E) = 0. \tag{4}$$

Если $z_{v1} = (z_{v1}(1), \ldots, z_{v1}(n))$, то векторы

$$z_{vr} = (z_{v1}(1)^{q^r}, \ldots, z_{v1}(n)^{q^r}), \quad r = 1, \ldots, d_v, \tag{5}$$

будут собственными векторами, соответствующими остальным корням многочлена f_v. Тогда, очевидно, что векторы

$$z_v = z_{v1} + \ldots + z_{vd_v}, \quad v = 1, \ldots, m \tag{6}$$

имеют координаты из поля F. Следовательно, вектор

$$x = (x_1, \ldots, x_n) = z_1 + \ldots + z_m \tag{7}$$

также имеет координаты из поля F.

Положим

$$\theta = x_1\omega_1 + \ldots + x_n\omega_n. \tag{8}$$

Лемма 1. *Элемент θ, определяемый соотношениями* (1), (3)–(8), *порождает нормальный базис поля K и может быть вычислен за время, ограниченное полиномом от n и q.*

Доказательство. Из (2) и (8) вытекает, что

$$\theta^{q^j} = xA^j(\omega_1, \ldots, \omega_n)^T, \quad j = 0, 1, \ldots, n-1.$$

Покажем, что векторы $x, xA, \ldots, xA^{n-1}$ линейно независимы над полем F. В самом деле, в силу (7), вектор x имеет вид $x = y_1 + \ldots + y_n$, где $y_1, \ldots, y_n$ — собственные векторы матрицы A, соответствующие попарно различным собственным значениям $\mu_1, \ldots, \mu_n$. Тогда

$$xA^j = \mu_1^j y_1 + \ldots + \mu_n^j y_n, \quad j = 0, 1, \ldots, n-1.$$

Отсюда вытекает линейная независимость этих векторов. Следовательно θ порождает нормальный базис поля K.

Легко проверить, что все вымисления по формулам (1), (3)–(8) могут быть выполнены за полиномиальное от n и q время (см. [4] и [5]). Лемма доказана.

Пусть теперь $q > n$. Выберем в поле F произвольное подмножество $\Lambda \subset F$ мощности $|\Lambda| = n+1$. Обозначим через $e_i = (0, \ldots, 1, \ldots, 0)$, $i = 1, \ldots, n$, единичные n-мерные векторы.

Последовательность векторов $g_1, \ldots, g_n$ определим следующим образом. Положим $g_1 = e_1$. Если вектор g_i, $i < n$, определен, то для всех $\lambda \in \Lambda$ вычислим ранг системы векторов

$$r(\lambda) = \mathrm{rank}\{(g_i + \lambda e_{i+1}), (g_i + \lambda e_{i+1})A, \ldots, (g_i + \lambda e_{i+1})A^{n-1}\}. \tag{9}$$

Пусть его максимальное значение достигается при $\lambda = \lambda_0$,

$$r(\lambda_0) = \max_{\lambda \in \Lambda} r(\lambda), \tag{10}$$

тогда определим

$$g_{i+1} = g_i + \lambda_0 e_{i+1}. \tag{11}$$

Положим

$$x = (x_1, \ldots, x_n) = g_n. \tag{12}$$

Лемма 2. *При $q > n$ элемент θ, определяемый соотношениями* (8)–(12), *порождает нормальный базис поля K и может быть вычислен за время, ограниченное полиномом от n и* $\ln q$.

Доказательство. Пусть Ω — алгебраическое замыкание поля F; $y_1, \ldots, y_n$ полная система собственных векторов матрицы A. Разложим в поле Ω векторы $e_1, \ldots, e_n$ по векторам $y_1, \ldots, y_n$. Через I_v, $v = 1, \ldots, n$ обозначим множество индексов тех собственных векторов, которые входят в разложение e_v с ненулевыми коэффициентами. Аналогичным образом определим множества J_v, $v = 1, \ldots, n$, для векторов $g_1, \ldots, g_n$.

Очевидно, что

$$\bigcup_{v=1} I_v = \{1, \ldots, n\}.$$

Кроме того, учитывая, что $|\Lambda| > n+1$, в силу (9)–(11) получим

$$J_{v+1} = J_v \cup I_v, \quad v = 1, \ldots, n-1.$$

Следовательно $J_n = \{1, \ldots, n\}$ и $x = g_n$ имеет вид

$$x = \alpha_1 y_1 + \ldots + \alpha_n y_n,$$

где $\alpha_1, \ldots, \alpha_n$ — некоторые ненулевые элементы поля Ω.

Но тогда, как и при доказательстве леммы 1, получим, что векторы $x, xA, \ldots, xA^{n-1}$ линейно независимы над Ω и, следовательно, над F.

Вычисление матрицы A требует, очевидно, времени, ограниченного полиномом от n и $\ln q$, а вычисления по формулам (9)–(12) требуют времени, ограниченного полиномом только от n (см. [4]). Лемма доказана.

Доказательство теоремы. Применяя при $q < n$ лемму 1, а при $q > n$ лемму 2, получаем утверждение теоремы.

Литература

[1] R. Lidl and H. Niederreiter, *Finite fields*, Addison–Wesley, London 1983.

[2] Э. Р. Берлекемп, *Алгебраическая теория кодирования*, Мир, Москва 1971.

[3] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, Связь, Москва 1979.

[4] В. И. Солодовников, *Верхние оценки сложности решения систем линейных уравнений*, Зап. научн. семинаров ЛОМИ АН СССР, т. 118, с. 159–187.

[5] Д. Ю. Григорьев, *Разложение многочленов над конечным полем и решение систем алгебраических уравнений*, Зап. научн. семинаров ЛОМИ АН СССР, т. 137, с. 20–79.

Поступило 17.3.1986 (1606)

ACTA ARITHMETICA
XLIX (1987)

An awful problem about integers in base four

by

J. H. Loxton and A. J. van der Poorten (Macquarie)

To Paul Erdős on his 75th birthday

The set $\boldsymbol{Z}$ of all integers coincides with the language of all words on the symbols 0, 1, $\bar{1}$ and 2 interpreted as integers presented in base four; here $\bar{1}$ is a convenient contraction for the digit -1. We consider the subset $\boldsymbol{L}$ of $\boldsymbol{Z}$ omitting the digit 2; thus the language of all words on just the symbols 0, 1 and $\bar{1}$ interpreted as integers in base four. Our problem is this: *can every odd integer be written as a quotient of elements of* $\boldsymbol{L}$?

We will answer this question in the affirmative, but first we pause to remark that the matter is troublesome. For example, given an odd integer k it is not at all easy to find a nonzero multiplier m in $\boldsymbol{L}$ so that also km is in $\boldsymbol{L}$. The only method that seems efficient is exemplified by the following computation in which we discover the smallest (positive) multiplier for $k = 2\bar{1}2\bar{1}1$ $(= 477)$. We find

$$
\begin{array}{lll}
2\,\bar{1}\,2\,\bar{1}\,1 & & + \\
\quad 2\,\bar{1}\,2\,\bar{1}\,1 & & - \\
\hline
1\,1\,2\,1\,2\,\bar{1} & & \\
\quad\;\; 2\,\bar{1}\,2\,\bar{1}\,1 & & - \\
\hline
1\,1\,0\,2\,0\,0\,\bar{1} & & \\
\quad\;\;\; 2\,\bar{1}\,2\,\bar{1}\,1 & & + \\
\hline
1\,1\,1\,0\,\bar{1}\,1\,2\,1 & & \\
\quad\;\;\;\; 2\,\bar{1}\,2\,\bar{1}\,1 & & + \\
\hline
1\,1\,1\,0\,1\,1\,0\,0\,1 & &
\end{array}
$$

so that multiplying k by $1\bar{1}\bar{1}11$ $(= 181)$ yields a product in $\boldsymbol{L}$. Roughly, the strategy at each step is to multiply by 4 and to add or subtract k or to do nothing, all the while ensuring that no digit 2 remains trapped on the left. Another example, with $k = 2\bar{1}11$ $(= 117)$: