

文章编号: 0583-1431(2005)05-0947-08

文献标识码: A

有限域上最优正规基的乘法表

廖群英

四川大学数学学院 成都 610064
四川师范大学数学与软件科学学院 成都 610066
E-mail: Liao_qunying@yahoo.com.cn

孙 琦

四川大学数学学院 成都 610064
E-mail: Qisun126@sohu.com

摘要 本文给出了有限域上最优正规基乘法表的一个计算方法, 改进了孙琦的相应结果. 在有限域上椭圆曲线密码体制的应用中, 本文给出的算法是非常有效的.

关键词 有限域上的正规基; 最优正规基; 正规基的乘法表

MR(2000) 主题分类 12E20

中图分类 O156.1

On Multiplication Tables of Optimal Normal Bases over Finite Fields

Qun Ying LIAO

Mathematical College, Sichuan University, Chengdu 610064, P. R. China
Mathematical and Soft-Ware Scientific College, Sichuan Normal University,
Chengdu 610066, P. R. China
E-mail: Liao_qunying@yahoo.com.cn

Qi SUN

Mathematical College, Sichuan University, Chengdu 610064, P. R. China
E-mail: Qisun126@sohu.com

Abstract The authors propose an algorithm for computing multiplication tables of optimal normal bases over finite fields, which is better than those corresponding results of Sun. In particular, this algorithm is very helpful to elliptic curves public-key cryptic systems.

Keywords Normal bases over finite fields; Optimal normal bases; Multiplication tables of optimal normal bases over finite fields

MR(2000) Subject Classification 12E20

Chinese Library Classification O156.1

1 引言及定理

设 q 为素数幂, $F = F_{q^n}$ 是有限域 F_q 的 n 次扩域, $N = \{\alpha_i \mid i = 0, 1, \dots, n-1\}$ 是 F

收稿日期: 2003-09-28; 接受日期: 2004-09-02

基金项目: 国家自然科学基金资助项目 (10128103); 基础数学重点学科建设项目 (SJD0406)

在 F_q 上的一组正规基, 其中 $\alpha_i = \alpha^{q^i}$, $i = 0, 1, \dots, n-1$. 对 $\forall A \in F$ 和 $\forall B \in F$, 可设 $A = \sum_{i=0}^{n-1} a_i \alpha_i$, $B = \sum_{j=0}^{n-1} b_j \alpha_j$, $a_i, b_j \in F_q$. 显然 $F \cong F_q^n$, 故可记 $A = (a_0, \dots, a_{n-1})$, $B = (b_0, \dots, b_{n-1})$. 设 $AB = C = (c_0, \dots, c_{n-1})$, 熟知 $c_l = A^{q^{-l}} T_0 (B^{q^{-l}})^T$, $l = 0, 1, \dots, n-1$, 而 $T_0 = (t_{i,j}^{(0)})$ 由下式给出

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{i,j}^{(k)} \alpha_k, t_{i,j}^{(k)} = t_{j,i}^{(k)} \in F_q.$$

令 $\alpha = \alpha_0$, $\alpha \alpha_i = \sum_{j=0}^{n-1} t_{i,j} \alpha_j$, $0 \leq i \leq n-1$, $t_{i,j} \in F_q$, 则称 $T = (t_{i,j})$ 为正规基 N 的乘法表. 易知 $t_{i,j}^{(0)} = t_{i-j, n-j}$, $0 \leq i, j \leq n-1$. 可见, $T_0 = (t_{i,j}^{(0)})$ 可由乘法表 $T = (t_{i,j})$ 唯一确定, 而 $AB = C$ 又可由 $T_0 = (t_{i,j}^{(0)})$ 得到. 显然 T 和 T_0 中非零元的个数相等, T 中的非零元越少, F 中乘法运算的计算量也就越小. Mullin 等人在文 [1] 中引入了 $T = (t_{i,j})$ 的复杂度 C_N 为 T 中非零元的个数, 并证明了 $C_N \geq 2n-1$. 当 $C_N = 2n-1$ 时, 称 N 为最优正规基.

有许多论文研究有限域的正规基, 可参阅专著 [2] 和 [3]. 由于在有限域的椭圆曲线密码体制的快速实现当中, 通常都采用最优正规基表示有限域的元, 这就更加促进了对有限域的正规基, 特别是对最优正规基的研究 [4, 5]. 熟知, I型和 II型最优正规基的如下构造 (证明请参见文 [1]):

I型最优正规基的构造定理 设 $n+1$ 是一个素数, q 是模 $n+1$ 的一个原根, 则 $F = F_q$ 上 n 个非单位元的 $n+1$ 次单位根是线性无关的, 且组成 $F = F_{q^n}$ 到 F_q 上的一组最优正规基, 记为 $N = \{\alpha^{q^i} \mid i = 0, \dots, n-1\} = \{\alpha^j \mid j = 1, \dots, n\}$, 这里 α 是一个 $n+1$ 次本原单位根, 称 N 为 F 到 F_q 上的一组 I型最优正规基.

II型最优正规基的构造定理 设 $2n+1$ 是一个素数, 假设

- (a) 2 为模 $2n+1$ 的一个原根, 或
- (b) $2n+1 \equiv 3 \pmod{4}$, 且 2 模 $2n+1$ 的次数为 n ,

则 $\alpha = r + r^{-1}$ 生成一个 $F = F_{2^n}$ 到 F_2 上的一组最优正规基, 这里 r 是一个 $2n+1$ 次本原单位根, 记为 $N = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\} = \{\alpha = r + r^{-1}, r^2 + r^{-2}, \dots, r^n + r^{-n}\}$, 称为 $F = F_{2^n}$ 到 F_2 上的一组 II型最优正规基.

另一方面, 若 N 为 F 到 F_q 上的一组最优正规基, $\forall a \in F_q^*$, 易知 $aN = \{a\alpha \mid \alpha \in N\}$ 也是 F 到 F_q 上的一组最优正规基, 此时我们称正规基 N 与 aN 等价. 高绪洪和 Lenstra 在文 [6] 中证明了: 一个有限域上的最优正规基与 I型最优正规基等价或与 II型最优正规基等价. 由此立得: $F = F_{2^n}$ 在 F_2 上的最优正规基只有 I型与 II型两种. Agnew 等在文 [4] 中指出有限域中元的乘法的执行硬件与正规基的复杂度有着密切的关系. 也就是说, T_0 中的非零元越少, 有限域的乘法就越简单. 因此, 计算最优正规基的乘法表 T 是快速实现有限域上的椭圆曲线密码体制重要的一环. 最近孙琦在 [7] 中给出了特征为 2 的有限域上的 I型最优正规基乘法表的一个算法, 他证明了下述结果: 设 F_q 的特征为 2, $n \geq 2$, $N = \{\alpha_i \mid i = 0, 1, \dots, n-1\}$ 是 F 到 F_q 上的一组 I型最优正规基, 则

- (a) 正规基 N 的乘法表 $T = (t_{i,j}) = UV$, 其中 V 是 n 阶循环矩阵

$$C[\underbrace{1, \dots, 1}_{\frac{n}{2}}, 0, 1, \dots, 1],$$

U 中的元为 $\text{Tr}(\alpha \alpha_i \alpha_j)$, $0 \leq i, j \leq n-1$, $\text{Tr}(\alpha)$ 表示 F 上元 α 在 F_q 上的迹函数.

(b) 如果 $q = 2$, 对于 U 中的元 $\text{Tr}(\alpha\alpha_i\alpha_j)$, $0 \leq i, j \leq n - 1$, 当 $i = j$ 时, 有

$$\text{Tr}(\alpha\alpha_i^2) = \begin{cases} 0, & \text{若 } i = \frac{n}{2} - 1 \\ 1, & \text{否则.} \end{cases}$$

当 $i \neq j$, $0 \leq i, j \leq n - 1$ 时, 有

$$\text{Tr}(\alpha\alpha_i\alpha_j) = \begin{cases} 0, & \text{若 } 2^i + 2^j \equiv n \pmod{n+1} \\ 1, & \text{否则.} \end{cases}$$

本文给出了有限域上最优正规基的乘法表的一个计算方法. 对于 I 型最优正规基的乘法表, 新的算法比文 [7] 提出的算法更为有效. 文 [7] 中未讨论 II 型最优正规基的乘法表的计算方法, 本文对 II 型的情形, 也给出了一个有效的算法. 我们证明了下面的定理.

定理 1 设 $N = \{\alpha^{q^i} \mid i = 0, \dots, n-1\} = \{\alpha, \alpha^2, \dots, \alpha^n\}$ (其中 α 为 $n+1$ 次本原单位根) 为 F 到 F_q 上的一组 I 型最优正规基, $T = (t_{i,j})$ 为其乘法表, 则当 $j = 0, 1, \dots, n-1$ 时, 有

$$t_{\frac{n}{2}, j} = -1; \quad (1)$$

当 $i = 0, 1, \dots, n-1$, 且 $i \neq \frac{n}{2}$, 时, 有

$$t_{i,j} = \begin{cases} 1, & \text{若 } q^j \equiv q^i + 1 \pmod{n+1}, \\ 0, & \text{否则.} \end{cases}$$

定理 2 设 $N = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\} = \{\alpha = r + r^{-1}, r^2 + r^{-2}, \dots, r^n + r^{-n}\}$ 为 F_{2^n} 到 F_2 上的一组 II 型最优正规基, $T = (t_{i,j})$ 为其乘法表, 则

$$t_{0,j} = \begin{cases} 1, & \text{若 } j = 1, \\ 0, & \text{否则.} \end{cases} \quad (3)$$

$$t_{n-1,j} = \begin{cases} 1, & \text{若 } j = n-1 \text{ 或 } 2^{j+1} \equiv \pm 3 \pmod{2n+1}, \\ 0, & \text{否则;} \end{cases} \quad (4)$$

而当 $i = 1, \dots, n-2$ 时, 有

$$t_{i,j} = \begin{cases} 1, & \text{若 } 2^j \equiv \pm(2^i \pm 1) \pmod{2n+1}, \\ 0, & \text{否则.} \end{cases} \quad (5)$$

不难看出, 定理 1 给出的计算方法比文 [7] 提出的算法简单. 因为, 本文的算法不需要计算两个 n 阶矩阵相乘.

2 定理的证明

定理 1 的证明 设 $N = \{\alpha^{q^i} \mid i = 0, 1, \dots, n-1\} = \{\alpha, \alpha^2, \dots, \alpha^n\}$ (其中 α 为 $n+1$ 次本原单位根) 为 F 到 F_q 上的一组 I 型最优正规基. 令

$$\alpha_i = \alpha^{q^i}, \quad \beta_i = \alpha^{i+1}, \quad 0 \leq i \leq n-1, \quad \beta = \beta_0 = \alpha = \alpha_0, \quad \beta\beta_i = \sum_{j=0}^{n-1} t_{i,j}^* \beta_j,$$

我们来证明 $T = (t_{i,j})$ 与 $T^* = (t_{i,j}^*)$ 之间有如下对应关系: 对 $\forall i, j = 0, 1, \dots, n-1$, 有

$$t_{i,j} = t_{s(i), s(j)}^*, \quad (6)$$

其中 $q^x \equiv s(x) + 1 \pmod{n+1}$, 且 $0 \leq s(i), s(j) \leq n-1$. 由 $N = \{\alpha^{q^i} \mid i = 0, \dots, n-1\} = \{\alpha, \alpha^2, \dots, \alpha^n\}$ 为一组基, 可得

$$\forall i = 0, 1, \dots, n-1, \exists s(i), 0 \leq s(i) \leq n-1,$$

使 $\alpha^{q^i} = \alpha^{s(i)+1}$, 即 $\alpha_i = \beta_{s(i)}$, 其中 $q^i \equiv s(i) + 1 \pmod{n+1}$, 故

$$\forall i = 0, 1, \dots, n-1, \sum_{j=0}^{n-1} t_{i,j} \beta_{s(j)} = \alpha \alpha_i = \beta \beta_{s(i)} = \sum_{j=0}^{n-1} t_{s(i), k}^* \beta_k.$$

从而 $\forall i, j = 0, 1, \dots, n-1$, $t_{i,j} = t_{s(i), s(j)}^*$, 其中 $q^x \equiv s(x) + 1 \pmod{n+1}$. 这就证明了 (6) 式.

另一方面, $T^* = (t_{i,j}^*)$ 中的元合条件 (见文 [1]):

$$\text{对 } \forall i = 0, 1, \dots, n-2, t_{i,j}^* = \begin{cases} 1, & \text{若 } j = i+1 \\ 0, & \text{否则;} \end{cases} \quad (7)$$

$$t_{n-1,j}^* = -1, \text{ 对 } \forall j = 0, 1, \dots, n-1. \quad (8)$$

由 I 型最正规基的构造定理知, q 为模 $n+1$ 的一个原根, 故 $q^{\frac{n}{2}} \equiv -1 \pmod{n+1}$, 从而 $s(\frac{n}{2}) = n-1$. 于是由 (6) 和 (8) 式, 得

$$t_{\frac{n}{2},j} = t_{s(\frac{n}{2}), s(j)}^* = t_{n-1,s(j)}^* = -1, \quad j = 0, 1, \dots, n-1.$$

这便证明了 (1) 式.

对 $\forall i = 0, 1, \dots, n-1$, 且 $i \neq \frac{n}{2}$, 由 (6) 和 (7) 式知

$$t_{i,j} = t_{s(i), s(j)}^* = \begin{cases} 1, & \text{若 } s(j) = s(i) + 1 \\ 0, & \text{否则.} \end{cases}$$

又 $q^x \equiv s(x) + 1 \pmod{n+1}$ 且 $s(j) = s(i) + 1 \iff q^j \equiv q^i + 1 \pmod{n+1}$, 这便证明了 (2). 定理 1 证毕.

定理 2 的证明 设 $N = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\} = \{\alpha = r + r^{-1}, r^2 + r^{-2}, \dots, r^n + r^{-n}\}$ 为 $F = F_{2^n}$ 到 F_2 上的一组 II 型最正规基. 令 $\alpha_i = \alpha^{2^i}$, $\beta = \beta_0 = \alpha = \alpha_0$, $\beta_i = r^{i+1} + r^{-i-1}$, $i = 0, 1, \dots, n-1$. 若

$$\alpha \alpha_i = \sum_{j=0}^{n-1} t_{i,j} \alpha_j, \quad \beta \beta_i = \sum_{j=0}^{n-1} t_{i,j}^* \beta_j,$$

我们来证明 $T = (t_{i,j})$ 与 $T^* = (t_{i,j}^*)$ 之间有如下对应关系: 对 $\forall i, j = 0, 1, \dots, n-1$, 有

$$t_{i,j} = t_{s(i), s(j)}^*, \quad (9)$$

其中

$$0 \leq s(i), s(j) \leq n-1, 2^x \equiv \pm(s(x) + 1) \pmod{2n+1}.$$

由 $N = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\} = \{\alpha = r + r^{-1}, r^2 + r^{-2}, \dots, r^n + r^{-n}\}$ 为一组基知

$$\forall i = 0, 1, \dots, n-1, \exists s(i), 0 \leq s(i) \leq n-1,$$

使 $\alpha_i = \alpha^{2^i} = \beta_{s(i)}$, 即 $r^{2^i} + r^{-2^i} = r^{s(i)+1} + r^{-s(i)-1}$, 可得 $r^{2^i} = r^{s(i)+1}$ 或 $r^{-s(i)-1}$, 故

$$2^i \equiv \pm(s(i) + 1) \pmod{2n+1},$$

而

$$\sum_{j=0}^{n-1} t_{i,j} \alpha_j = \alpha \alpha_i = \beta \beta_{s(i)} = \sum_{k=0}^{n-1} t_{s(i), k}^* \beta_k.$$

这就证明了(9)式.

另一方面, 我们有(见文[1]或[2]) $T^* = (t_{i,j}^*)$ 中的元合条件: 当 $i = 1, \dots, n-2$ 时, 有

$$t_{i,j}^* = \begin{cases} 1, & \text{若 } j = i \pm 1 \\ 0, & \text{否则.} \end{cases} \quad (10)$$

以及

$$t_{n-1,j}^* = \begin{cases} 1, & \text{若 } j = n-1 \text{ 或 } j = n-2, \\ 0, & \text{否则;} \end{cases} \quad (11)$$

$$t_{0,j}^* = \begin{cases} 1, & \text{若 } j = 1, \\ 0, & \text{否则.} \end{cases} \quad (12)$$

显然,(3)式可由 $2^0 \equiv 0 + 1 \pmod{2n+1}$, $2 \equiv 1 + 1 \pmod{2n+1}$ 及(12)式立得.

由于当 n 为奇数时, 2 模 $2n+1$ 的次数为 n , 即 $2^n \equiv 1 \equiv -2n \pmod{2n+1}$, 从而 $2^{n-1} \equiv -n \pmod{2n+1}$, 故 $s(n-1) = n-1$; 当 n 为偶数时, 2 模 $2n+1$ 的次数为 $2n$, 即 $2^n \equiv -1 \equiv 2n \pmod{2n+1}$, 从而 $2^{n-1} \equiv n \pmod{2n+1}$, 仍有 $s(n-1) = n-1$. 进而, 由

$$s(j) = n-2 \iff 2^j \equiv \pm(n-1) \pmod{2n+1} \iff 2^{j+1} \equiv \pm 3 \pmod{2n+1}.$$

于是由(11)式便知(4)式成立. 又由(9)和(10)式, 可得

$$\forall i = 1, \dots, n-2, t_{i,j} = t_{s(i), s(j)}^* = \begin{cases} 1, & s(j) = s(i) \pm 1 \\ 0, & \text{否则,} \end{cases}$$

而

$$2^x \equiv \pm(s(x) + 1) \pmod{2n+1},$$

故(5)式得证. 定理2证毕.

注1 定理1, 2 分别给出了求有限域上I型和II型最优正规基的乘法表的一个计算方法.(1)和(2)式及(3)–(5)式表明: 当有限域 F_q 的扩域 F_{q^n} 的次数 n 较小时, 计算十分简单. 在有限域上椭圆曲线密码体制的实际应用中, 一般取 n 为三位数, 即使 n 是四位数, 计算也不复杂, 我们可以用下述算法(见三)计算(2)和(4), (5)式. 可见, 本文给出的计算有限域上I型和II型最优正规基的乘法表的算法, 在有限域上椭圆曲线密码体制的实现中是非常有效的.

3 应用举例

(i) I型最优正规基 N 的乘法表的算法

(方法一): 直接利用定理 1 中的公式 (1) 与 (2)

例 1 设 $n = 4, q = 2$, 由于 $n + 1 = 5$ 是素数, 2 是模 5 的一个原根, 由 I 型最优正规基的构造定理可知, 如果 α 是一个 5 次本原单位根, 则 α 生成 F_{2^4} 到 F_2 上一组 I 型最优正规基, 即

$$N = \{\alpha, \alpha^2, \alpha^4, \alpha^8\}.$$

由 (1) 式可得 $t_{\frac{n}{2}, j} = t_{2, j} = -1 = 1, j = 0, 1, 2, 3$;

另一方面, 由 $2^0 + 1 \equiv 2^1 \pmod{5}, 2^1 + 1 \equiv 3 \equiv 8 \equiv 2^3 \pmod{5}, 2^3 + 1 \equiv 9 \equiv 2^2 \pmod{5}$, 及 (2) 式知

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

(方法二): 由定理 1 的证明可得求 I 型最优正规基 N 的乘法表的步骤如下:

(a) 求出 $(i, s(i))$ 对使 $q^i \equiv s(i) + 1 \pmod{n+1}, \forall i = 0, 1, \dots, n-1$.

(b) 由于显然 $s(0) = 0$, 故把 $s(i)$ ($i = 0, 1, \dots, n-1$) 按由小到大的顺序排列得到序对 $(0, 0), (j_1, 1), \dots, (j_{n-2}, n-2), (j_{n-1}, n-1)$, 其中 $s(j_i) = i, j_i = 1, \dots, n-1$.

(c) 写出满足条件 $\forall k = 0, 1, \dots, n-1, s(l) = s(k) + 1$ 的 (k, l) 对为

$$(0, j_1), (j_1, j_2), \dots, (j_{n-2}, j_{n-1}).$$

(d) 在乘法表 $T = (t_{i,j})$ 中, 有

$$\forall k = 0, 1, \dots, n-1, k \neq \frac{n}{2}, t_{k,l} = 1; t_{\frac{n}{2}, j} = -1, \forall j = 0, 1, \dots, n-1.$$

而其余的 $t_{i,j}$ 取值为 0.

例 2 设 $n = 16, q = 3$, 由于 $n + 1 = 17$ 是素数, 3 是模 17 的一个原根, 由 I 型最优正规基的构造定理可知, 如果 α 是一个 17 次本原单位根, 则 α 生成 $F_{3^{16}}$ 到 F_3 上一组 I 型最优正规基, 即

$$N = \{\alpha^{3^i} | i = 0, 1, \dots, 15\}.$$

首先, 我们不难得到合条件

$$3^i \equiv s(i) + 1 \pmod{17}, \forall i = 0, 1, \dots, 15, i \neq \frac{n}{2} = 8$$

的 $(i, s(i))$ 对为: $(0, 0), (14, 1), (1, 2), (12, 3), (5, 4), (15, 5), (11, 6), (10, 7), (2, 8), (3, 9), (7, 10), (13, 11), (4, 12), (9, 13), (6, 14), (8, 15)$.

其次, 满足条件 $s(l) = s(k) + 1, \forall k = 0, 1, \dots, 15$, 的 (k, l) 对为: $(0, 14), (14, 1), (1, 12), (12, 5), (5, 15), (15, 11), (11, 10), (10, 2), (2, 3), (3, 7), (7, 13), (13, 4), (4, 9), (9, 6), (6, 8)$.

最后, 我们得到乘法表如下

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

(ii) II 型最优正规基 N 的乘法表的算法

(方法一): 直接利用定理 2 中的公式 (3), (4) 与 (5).

例 3 设 $n = 3$, 由于 $2n + 1 = 7$ 是素数, 2 模 7 的次数为 3, 由 II 型最优正规基的构造定理可知, 如果 r 是一个 7 次本原单位根, 则 $\alpha = r + r^{-1}$ 生成 F_{2^3} 到 F_2 上一组 II 型最优正规基, 即 $N = \{\alpha, \alpha^2, \alpha^4\}$.

由 (3) 式可得

$$t_{0,j} = \begin{cases} 1, & \text{若 } j = 1 \\ 0, & \text{否则.} \end{cases}$$

另一方面, 由 $2^{j+1} \equiv \pm 3 \pmod{7} \Rightarrow j = 1$, 故由 (4) 式得

$$t_{2,j} = \begin{cases} 1, & \text{若 } j = 1, 2 \\ 0, & \text{否则.} \end{cases}$$

又当 $i = 1$ 时, $2^1 - 1 \equiv 2^0 \pmod{7}, -(2^1 + 1) \equiv 2^2 \pmod{7}$, 故由 (5) 式, 可得

$$t_{1,j} = \begin{cases} 1, & \text{若 } j = 0, 2 \\ 0, & \text{否则.} \end{cases}$$

于是得乘法表如下

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

(方法二): 由定理 2 的证明可得求 II 型最优正规基 N 的乘法表的步骤如下:

(a) 求出 $(i, s(i))$ 对, 使 $2^i \equiv \pm(s(i) + 1) \pmod{2n + 1}, \forall i = 0, 1, \dots, n - 1$.

(b) 由于显然 $s(0) = 0$, 故把 $s(i)$ ($i = 0, 1, \dots, n - 1$) 按由小到大的顺序排列得到序对 $(0, 0), (j_1, 1), \dots, (j_{n-2}, n-2), (j_{n-1}, n-1)$, 其中 $s(j_i) = i, j_i = 1, \dots, n - 1$.

(c) 写出满足条件 $\forall k = 0, 1, \dots, n-1, s(l) = s(k)+1$ 的 (k, l) 对为 $(0, j_1), (j_1, j_2), \dots, (j_{n-2}, j_{n-1})$. 而足条件 $\forall k = 0, 1, \dots, n-1, s(l) = s(k)-1$ 的 (k, l) 对为 $(j_1, 0), (j_2, j_1), \dots, (j_{n-1}, j_{n-2})$, 其中 $s(j_i) = i, j_i = 1, \dots, n-1$.

(d) 求出 $j = 0, 1, \dots, n-2$, 使 $2^{j+1} \equiv \pm 3 \pmod{2n+1}$;

(e) 在乘法表 $T = (t_{i,j})$ 中, 有

$$\forall k = 1, \dots, n-2, t_{k,l} = 1; \quad t_{0,1} = 1; \quad t_{n-1,j} = 1.$$

若 $j = n-1$ 或 $2^{j+1} \equiv \pm 3 \pmod{2n+1}$. 而其余的 $t_{i,j}$ 取值为 0.

例 4 设 $n = 11$, 由于 $2n+1 = 23$ 是素数, 2 模 23 的次数为 11, 由 II 型最优正规基的构造定理可知, 如果 r 是一个 23 次本原单位根, 则 $\alpha = r + r^{-1}$ 生成 $F_{2^{11}}$ 到 F_2 上一组 II 型最优正规基, 即 $N = \{\alpha, \alpha^2, \dots, \alpha^{2^{10}}\}$.

首先, 我们不难算出满足 $2^i \equiv \pm(s(i) + 1) \pmod{23}$, $\forall i = 0, 1, \dots, n-1$ 的 $(i, s(i))$ 对为: $(0, 0), (1, 1), (2, 3), (3, 7), (4, 6), (5, 8), (6, 4), (7, 9), (8, 2), (9, 5), (10, 10)$. 易证, 满足 $s(l) = s(k) \pm 1$, $\forall k = 0, 1, \dots, n-1$ 的 (k, l) 对为: $(1, 0), (0, 1), (8, 1), (8, 2), (6, 2), (4, 3), (5, 3), (3, 4), (9, 4), (3, 5), (7, 5), (2, 6), (9, 6), (5, 7), (10, 7), (1, 8), (2, 8), (4, 9), (6, 9), (7, 10)$.

另一方面, 由 $2^{j+1} \equiv \pm 3 \pmod{2n+1} \implies j = 7$.

最后, 我们得到乘法表如下

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

注 2 当扩张次数 n 较大时, 用 (方法二) 计算最优正规基的乘法表非常方便.

参 考 文 献

- [1] Mullin R., Onyszchuk I., Vanstone S., Wilson R., Optimal normal bases in $GF(p^n)$, *Discrete Applied Math.*, 1988/1989, **22**: 149–161.
- [2] Blake I., Gao S., Mullin R., Vanstone S., Yaghoobian T., Applications of finite fields, Kluwer: Kluwer Academic Publishers, 1993.
- [3] Lidl R., Niederreiter H., Finite fields, Cambridge: Cambridge University Press, 1987.
- [4] Agnew G., Mullin R., Onyszchuk I., Vanstone S., An implementation for a fast public key cryptosystem, *J. of Cryptology*, 1991, **3**: 63–79.
- [5] Rosati T., A high speed data encryption processor for public key cryptography, San diego: Proc. of IEEE Custom Integrated Circuits Conference, 1989: 1231–1235.
- [6] Gao S., Lenstra H. W., Optimal normal bases, *Designs, Codes and Cryptology*, 1992, **2**: 315–323.
- [7] Sun Q., An algorithm on the multiplication table of the normal basis over finite fields, *J. Sichuan Univ. Nat. Sci. Ed.*, 2003, **40**(3): 447–452 (in Chinese).