

一种快速计算 Z_{p^k} 上码字的深度的算法

朱士信 童宏玺

(合肥工业大学应用数学系, 合肥, 230009)

摘要: 码字深度是研究码字复杂性的一个重要工具, 文献[1]和[2]分别给出了域 F_2 和域 F_q 上码字的深度的快速计算方法, 本文定义了环 Z_{p^k} 上码字的深度, 给出了一种快速计算环 Z_{p^k} 上码字的深度的算法。

关键词: 环 Z_{p^k} ; 码; 码字的深度; 码的深度分布。

中国分类号: TN911.22

A Fast Algorithm for Calculating the Depth of a Codeword on Ring Z_{p^k}

Zhu shixin, Tong Hongxi

(Department of Applied Mathematics, Hefei University of Technology, Hefei, 230009)

Abstract: The depth of a codeword is an important tool for studying complexity of a codeword. Fast algorithms for calculating the depth of a codeword over field F_2 and F_q are separately given in [1] and [2]. In this paper, we define the depth of a codeword over Ring Z_{p^k} , and give a fast algorithm for calculating the depth of a codeword over ring Z_{p^k} .

Key words: Ring Z_{p^k} ; Code; Depth of a codeword; Depth distribution of a code.

1 引言

由于有限域上的编码理论的发展日趋成熟, 因此近十几年来很多从事编码理论研究的学者将研究兴趣转移到模正整数 k 的剩余类环 Z_k 上的理论研究^[3-6]。研究码及码字的结构是编码理论的一个重要研究方向。码字的深度是刻画码字复杂性的一个重要特征^[1], 也是研究移位寄存器序列的线性复杂性的有力工具^[1]。Etzion在文献[1]中首先提出了域 F_2 上码字深度的概念, 研究了码字深度的一些基本性质, 给出了一个计算 2 元码字深度的递归算法; Lao等在文献[2]中给出了域 F_q 上码字深度的两种算法, 其中一种递归算法只有在 n 较小时适用, 另一种算法是快速有效算法; 文献[7]讨论了 2 元循环码的深度分布; 文献[8]将码的深度分布应用于码的周期分布研究中。这些研究都是有限域上的码的深度研究, 本文定义了

* 安徽省自然科学基金资助项目 (编号: 03042201)

环 Z_{p^k} 上码字的深度，并给出了深度的一个简单性质。由于环 Z_{p^k} 上码的结构比域 F_q 上码的结构复杂得多，因此要给出环 Z_{p^k} 上码字的深度的快速算法比给出域上码字的深度的快速算法困难得多，本文给出了能简化计算的关键性引理 2，从而给出了一种快速计算环 Z_{p^k} 上码字深度的算法。

2 基本概念

设 p 是素数， Z_{p^k} 是整数环模 p^k 的剩余类环，其中 k 是大于等于 2 的自然数（因 $k=1$ 时， Z_p 为域，文献[2]中已研究）。对 $\forall x=(x_1, x_2, \dots, x_n) \in Z_{p^k}^n$ ，定义 x 的微分为

$$Dx = (x_2 - x_1, x_3 - x_2, \dots, x_n - x_{n-1}).$$

容易验证，对 $\forall x, y \in Z_{p^k}^n$ ， $\forall a \in Z_{p^k}^n$ 有

$$D(x + y) = Dx + Dy, \quad D(ax) = aDx$$

既 D 是线性算子。

为了方便，下文中用 $[a^m]$ 表示连续 m 个分量都为 a 。

定义 1 设 $x \in Z_{p^k}^n$ ，称使得

$$D^i x = [0^{n-i}]$$

成立的最小非负整数 i 为向量 x 的深度，记为 $Depth(x)$ ；如果没有这样的 i 存在，则规定 $Depth(x) = n$ 。

显然，对 $\forall x \in Z_{p^k}^n$ ，恒有 $0 \leq Depth(x) \leq n$ ，且 $Depth(x) = i$ 的充要条件是存在 $a \in Z_{p^k}^*$ 使 $D^{i-1}(x) = [a^{n-i+1}]$ 。值得注意的是，在域上， $ax (a \neq 0)$ 与 x 有相同的深度，而在环 Z_{p^k} 上此结论不一定成立，如在 Z_4 中， $Depth(2^n) = 1$ 但 $Depth(2[2^n]) = depth[0^n] = 0$ 。因此，建立环 Z_{p^k} 上的深度理论是必要的，下面给出环 Z_{p^k} 上线性码的码字深度的一个简单性质。

性质 1 设 C 是环 Z_{p^k} 上的线性码， $c_1, c_2 \in C$ ，如果 $Depth(c_1) = i$ ， $Depth(c_2) = j$ ，且 $j < i$ ，则 $Depth(c_1 + c_2) = i$ 。

证明 由于 $Depth(c_1) = i$, 故 $\exists a \in Z_{p^k}^*$ 使 $D^{i-1}(c_1) = [a^{n-i+1}]$, 又 $Depth(c_2) = j < i$,

故 $D^{i-1}(c_2) = [0^{n-i+1}]$, 由于 D 是线性算子, 故

$D^{i-1}(c_1 + c_2) = D^{i-1}(c_1) + D^{i-1}(c_2) = [a^{n-i+1}] + [0^{n-i+1}] = [a^{n-i+1}]$, 故 $Depth(c_1 + c_2) = i$ 。

3 主要结论

令 $A_m = (a_{ij})_{m \times m-1}$ 为 Z_{p^k} 上的距阵, 其中 $a_{ij} = \begin{cases} -1 & i = j \\ 1 & i = j+1 \\ 0 & \text{其它} \end{cases}$, 直接验算可知, 对

$\forall x \in Z_{p^k}^n$, 有 $Dx = xA_n$ 。

令

$$Q_n(i) = A_n A_{n-1} \Lambda A_{n-i+1}, \quad i = 1, 2, \Lambda, n-1 \quad (3.1)$$

约定 $Q_n(0) = I_n$, $Q_n[n]$ 为 $n \times 0$ 的空距阵, 则

$$D^i(x) = xQ_n(i)$$

因此, $Depth(x)$ 是使得 $xQ_n(i) = [0^{n-i}]$ 成立的最小非负整数 i ; 如果这样的 i 不存在, 则

$Depth(x) = n$ 。

引理 1 约定 $a_{i0} = 1$, 则当 $i = 1, 2, \Lambda, n-1$ 时

$$Q_n(i) = \begin{pmatrix} a_{ii} & & & & \\ \mathbf{M} & a_{ii} & & & \\ a_{i1} & \mathbf{M} & \mathbf{O} & & \\ 1 & a_{i1} & \mathbf{O} & a_{ii} & \\ & 1 & a_{i1} & \mathbf{M} & \\ & & \mathbf{O} & a_{i1} & \\ & & & & 1 \end{pmatrix}_{n \times (n-i)} \quad (3.2)$$

其中 $a_{ij} = (-1)^j \binom{i}{j} \pmod{p^k}$, $j = 0, 1, \Lambda, i$, $\binom{i}{j}$ 为组合数。 (3.3)

证明 (1) 当 $i = 1$ 时, 由 (3.1) 式知:

$$Q_n(1) = A_n = \begin{pmatrix} -1 & & & & \\ 1 & -1 & & & \\ & 1 & 0 & & \\ & & 0 & -1 & \\ & & & & 1 \end{pmatrix}_{n \times (n-1)}$$

即 $i=1$ 时 (3.2) 式成立; 假设 $i=m$ 时 (3.2) 式成立, 由于 $Q_n(m+1) = Q_n(m)A_{n-m}$, 由 A_{n-m} 的定义直接验算, $i=m+1$ 时 (3.2) 式也成立。故 (3.2) 式得证。

(2) 由 (1) 的证明知, 在 $Q_n(1)$ 中 $a_{11} = -1 = (-1)^1 \binom{1}{1} (\text{mod } p^k)$, 即 (3.3) 式在 $i=1$ 时成立; 假设 $i=m$ 时 (3.3) 式成立, 即 $a_{mj} = (-1)^j \binom{m}{j} (\text{mod } p^k)$, 由 $Q_n(m+1) = Q_n(m)A_{n-m}$ 可得:

$$a_{m+1,m+1} = -a_{mm}, \quad a_{m+1,j} = a_{mj} - a_{m,j-1}$$

$$\text{则 } a_{m+1,m+1} = -a_{mm} = -(-1)^m \binom{m}{m} (\text{mod } p^k) = (-1)^{m+1} \binom{m+1}{m+1} (\text{mod } p^k)$$

$$\begin{aligned} a_{m+1,j} &= a_{mj} - a_{m,j-1} = (-1)^j \binom{m}{j} (\text{mod } p^k) - (-1)^{j-1} \binom{m}{j-1} (\text{mod } p^k) \\ &= (-1)^j \left[\binom{m}{j} + \binom{m}{j-1} \right] (\text{mod } p^k) \\ &= (-1)^j \binom{m+1}{j} (\text{mod } p^k), \quad j = 0, 1, \Lambda, m. \end{aligned}$$

故 $i=m+1$ 时 (3.3) 式也成立, 因而 (3.3) 式得证。

为了使建立的算法快速有效, 需要先证明下面能简化计算的关键性的引理 2。

引理 2 设 m 为自然数, 则 $\binom{p^{km}}{ip^{km-k+1}} \equiv \binom{p^k}{ip} (\text{mod } p^k)$, $i = 0, 1, \Lambda, p^{k-1}$ 。

证明 由于此引理证明很困难, 为了简单明了, 下面证明过程中出现的等式都是模 p^k 情况的。又 $i=0$ 时引理显然成立, 故在下面证明过程中设 $i > 0$ 。

由于 $j \binom{p^k}{j} = p^k \binom{p^k-1}{j-1}$, 故当 $(j, p) = 1$ 时, $p^k \mid \binom{p^k}{j}$, 从而同余式

$$(1+x)^{p^k} = 1 + \binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \quad (3.4)$$

成立；又由于 $j \binom{p^{km}}{j} = p^{km} \binom{p^{km}-1}{j-1}$ ，故当 $p^{km-k+1} \nmid j$ 时， $p^k \mid \binom{p^{km}}{j}$ ，从而同余式

$$(1+x)^{p^{km}} = 1 + \binom{p^{km}}{p^{km-k+1}} X^{p^{km-k+1}} + \binom{p^{km}}{2p^{km-k+1}} X^{2p^{km-k+1}} + \Lambda + x^{p^{km}} \quad (3.5)$$

成立，利用这两个同余式，对 m 使用归纳法，证明引理如下：

- (1) 当 $m=1$ 时，引理显然成立；
- (2) 当 $m=2$ 时（注，为了证明简单，此种情况必须证明），由 (3.5) 式得：

$$(1+x)^{p^{2k}} = 1 + \binom{p^{2k}}{p^{k+1}} x^{p^{k+1}} + \binom{p^{2k}}{2p^{k+1}} x^{2p^{k+1}} + \Lambda + x^{p^{2k}} \quad (3.6)$$

又连续两次利用 (3.4) 式得：

$$\begin{aligned} (1+x)^{p^{2k}} &= \left[(1+x)^{p^k} \right]^{p^k} = \left(1 + \binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \right)^{p^k} \\ &= 1 + \binom{p^k}{p} \left[\binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \right]^p + \binom{p^k}{2p} \left[\binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \right]^{2p} \\ &\quad + \Lambda + \binom{p^k}{p \cdot p^{k-1}} \left[\binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \right]^{p^k} \end{aligned} \quad (3.7)$$

令 $\alpha_i = \binom{p^k}{ip} \left[\binom{p^k}{p} x^p + \binom{p^k}{2p} x^{2p} + \Lambda + x^{p^k} \right]^{ip}$ ， $1 \leq i \leq p^{k-1}$ ，下面计算 (3.6) 式与 (3.7)

式中 $x^{jp^{k+1+l}}$ 的系数，其中 l 为非负整数， $(j, p) = 1$ ， $i = jp^l \leq p^{k-1}$ 。

在 (3.6) 式中 $x^{jp^{k+1+l}}$ 的系数为 $\binom{p^{2k}}{jp^{k+1+l}}$ ；在 (3.7) 式中，当 $i < jp^l$ 时， α_i 中不含 $x^{jp^{k+1+l}}$

项，当 $i = jp^l$ 时， α_{jp^l} 中出现唯一一项 $\binom{p^{2k}}{jp^{l+1}} x^{jp^{k+1+l}}$ ，当 $i > jp^l$ 时，可以证明 p^k 整

除 $x^{jp^{k+1+l}}$ 项的系数，即 α_i 中也不含 $x^{jp^{k+1+l}}$ 项，因此 (3.7) 式中， $x^{jp^{k+1+l}}$ 的系数为 $\binom{p^k}{jp^{l+1}}$ ，

故

$$\binom{p^{2k}}{j p^{k+1+l}} \equiv \binom{p^k}{j p^{l+1}} \pmod{p^k}$$

成立，由于 $i = j p^l$ ，代入上式即得 $m = 2$ 时，引理成立；

(3) 假设 $m = t - 1$ ($t \geq 3$) 时引理成立，即

$$\binom{p^{k(t-1)}}{i p^{k(t-2)+1}} \equiv \binom{p^k}{i p} \pmod{p^k}, \quad i = 0, 1, \Lambda, p^{k-1}$$

下证 $m = t$ 时引理成立。

记 $y = x^{p^{kt-2k}}$ ，由 (3.5) 式知

$$\begin{aligned} (1+x)^{p^{ik}} &= 1 + \binom{p^{kt}}{p^{k(t-1)+1}} x^{p^{kt-k+1}} + \binom{p^{kt}}{2p^{k(t-1)+1}} x^{2p^{kt-k+1}} + \Lambda + x^{p^{kt}} \\ &= 1 + \binom{p^{kt}}{p^{kt-k+1}} y^{p^{k+1}} + \binom{p^{kt}}{2p^{kt-k+1}} y^{2p^{k+1}} + \Lambda + y^{p^{2k}} \end{aligned}$$

再由 (3.5) 式知

$$(1+x)^{p^i} = \left[(1+x)^{p^{k(t-1)}} \right]^{p^k} = \left[1 + \binom{p^{k(t-1)}}{p^{k(t-2)+1}} x^{p^{k(t-2)+1}} + \binom{p^{k(t-1)}}{2p^{k(t-2)+1}} x^{2p^{k(t-2)+1}} + \Lambda + x^{p^{k(t-1)}} \right]^{p^k}$$

由归纳假设及 $y = X^{p^{k(t-2)}}$ 得

$$(1+x)^{p^{ik}} = \left[1 + \binom{p^k}{p} y^p + \binom{p^k}{2p} y^{2p} + \Lambda + y^{p^k} \right]^{p^k}$$

再由 (3.4) 式得：

$$\begin{aligned} (1+x)^{p^{ik}} &= 1 + \binom{p^k}{p} \left[\binom{p^k}{p} y^p + \binom{p^k}{2p} y^{2p} + \Lambda + y^{p^k} \right]^p \\ &\quad + \binom{p^k}{2p} \left[\binom{p^k}{p} y^p + \binom{p^k}{2p} y^{2p} + \Lambda + y^{p^k} \right]^{2p} \\ &\quad + \Lambda + \binom{p^k}{p \cdot p^{k-1}} \left[\binom{p^k}{p} y^p + \binom{p^k}{2p} y^{2p} + \Lambda + y^{p^k} \right]^{p^k} \end{aligned} \quad (3.9)$$

类似于 $m = 2$ 的情况，比较(3.8)式与(3.9)式中 $y^{jp^{k+1+l}}$ 的系数即可得：

$$\binom{p^{kt}}{i p^{kt-k+1}} \equiv \binom{p^k}{i p} \pmod{p^k}$$

即引理对 $m = t$ 式也成立，由归纳法知，引理成立。

引理 3 设 $x = (x_1, x_2, \Lambda, x_n) \in Z_{p^k}^n$ ，若 $p^{km} < n$ ，则

$$D^{p^{km}} x = \left(\sum_{i=0}^{p^{k-1}} c_i x_{p^{km+1}-p^{km-k+1}i}, \sum_{i=0}^{p^{k-1}} c_i x_{p^{km+2}-p^{km-k+1}i}, \Lambda, \sum_{i=0}^{p^{k-1}} c_i x_{n-p^{km-k+1}i} \right)$$

其中 $c_i = (-1)^{ip} \binom{p^k}{ip} \pmod{p^k}$,

证明 由 $D^i x = xQ_n(i)$ 与引理 1 得

$$D^{p^{km}} x = xQ_n(p^{km}) = \left(\sum_{j=0}^{p^{km}} b_j x_{p^{km+1}-j}, \sum_{j=0}^{p^{km}} b_j x_{p^{km+2}-j}, \Lambda, \sum_{j=0}^{p^{km}} b_j x_{n-j} \right)$$

其中 $b_j = (-1)^j \binom{p^{km}}{j} \pmod{p^k}$

由于 $j \binom{p^{km}}{j} = p^{km} \binom{p^{km}-1}{j-1}$, 故当 $p^{km-k+1} \nmid j$ 时, 即 $j \neq p^{km-k+1}i$ 时, $p^k \mid \binom{p^{km}}{j}$, 则

$b_j = 0 \pmod{p^k}$, 当 $j = p^{km-k+1}i$, $0 \leq i \leq p^{k-1}$ 时, 由引理 2 得:

$$b_j \equiv (-1)^{p^{km-k+1}i} \binom{p^{km}}{p^{km-k+1}i} \equiv (-1)^{ip} \binom{p^k}{ip} \pmod{p^k} = c_i$$

从而

$$D^{p^{km}} x = \left(\sum_{i=0}^{p^{k-1}} c_i x_{p^{km+1}-p^{km-k+1}i}, \sum_{i=0}^{p^{k-1}} c_i x_{p^{km+2}-p^{km-k+1}i}, \Lambda, \sum_{i=0}^{p^{k-1}} c_i x_{n-p^{km-k+1}i} \right)$$

其中 $c_i = (-1)^{pi} \binom{p^k}{ip} \pmod{p^k}$, 即引理 3 得证。

引理 4 设 $x = (x_1, x_2, \Lambda, x_n) \in Z_{p^k}^n$, 且 $\text{depth}(x) = m$,

(1) 令 $\bar{x} = (x_1, \Lambda, x_n, x_{n+1}) \in Z_{p^k}^{n+1}$, 则 $\text{depth}(\bar{x}) = m$ 当且仅当 $x_{n+1} + a_{m1}x_n +$

$a_{m2}x_{n-1} + \Lambda + a_{mm}x_{n-m+1} = 0$, 否则 $\text{depth}(\bar{x}) = n+1$, 其中 a_{mj} 由 (3.2) 式确定;

(2) 令 $x^* = (x_1, \Lambda, x_n, x_{n+1}, x_{n+s}) \in Z_{p^k}^{n+s}$, 如果 $\text{depth}(x^*) \leq n$, 则

$\text{depth}(x^*) = \text{depth}(x)$ 。

证明 (1) 由于 $D^i(\bar{x}) = \bar{x}Q_{n+1}(i) = (D^i(x), x_{n+1} + a_{i1}x_n + a_{i2}x_{n-1} + \Lambda + a_{ii}x_{n-i+1})$,

$$\begin{aligned} D^m(\bar{x}) &= (D^m(x), x_{n+1} + a_{m1}x_n + a_{m2}x_{n-1} + \Lambda + a_{mm}x_{n-m+1}) \\ &= (0^{n-m}, x_{n+1} + a_{m1}x_n + a_{m2}x_{n-1} + \Lambda + a_{mm}x_{n-m+1}) \end{aligned}$$

由于 $depth(\bar{x}) \geq depth(x)$, 故 $depth(\bar{x}) = depth(x)$, 当且仅当

$$x_{n+1} + a_{m1}x_n + a_{m2}x_{n-1} + \Lambda + a_{mm}x_{n-m+1} = 0; \text{ 当}$$

$$x_{n+1} + a_{m1}x_n + a_{m2}x_{n-1} + \Lambda + a_{mm}x_{n-m+1} = a \neq 0 \text{ 时, } D^m(\bar{x}) = [0^{n-m} a], \text{ 则}$$

$depth(\bar{x}) = n + 1$; 反之亦然。

(2) 由于 $depth(\bar{x}) \leq depth(x^*) \leq n$, 由 (1) 得, $depth(x^*) = depth(\bar{x}) = depth(x)$

算法 1 设 $x = (x_1, x_2, \Lambda, x_n)$ 是环 Z_{p^k} 上码 c 中的码字, m 是使 $p^{km} < n$ 成立的最大自然数, 令 $y = (x_1, x_2, \Lambda, x_{p^{km}})$,

$$z = D^{p^{km}} x = \left(\sum_{i=0}^{p^k-1} c_i x_{p^{km+1-p^{km-k+1}i}}, \sum_{i=0}^{p^k-1} c_i x_{p^{km+2-p^{km-k+1}i}}, \Lambda, \sum_{i=0}^{p^k-1} c_i x_{n-p^{km-k+1}i} \right), \text{ 其中}$$

$$c_i = (-1)^{ip} \binom{p^k}{ip} \pmod{p^k}, \text{ 则}$$

- (1) 如果 $x = [0^n]$, 则 $depth(x) = 0$;
- (2) 如果 $x = [a^n]$, $a(\neq 0) \in Z_{p^k}$, 则 $depth(x) = 1$;
- (3) 如果 $x = [0^{n-p^{km}}]$, 则 $depth(x) = depth(y)$;
- (4) 如果 $x \neq [0^{n-p^{km}}]$, 则 $depth(x) = p^{km} + depth(z)$ 。

定理 1 算法 1 是正确的。

证明 (1), (2) 由定义即得证。

(3) 如果 $z = D^{p^{km}}(x) = [0^{n-p^{km}}]$, 则 $depth(x) < p^{km} < n$, 由引理 4 知,

$$depth(x) = depth(y);$$

(4) 由于 $z = D^{p^{km}}(x) \neq [0^{n-p^{km}}]$, 则 $depth(x) > p^{km}$, 由深度定义即得:

$$depth(x) = p^{km} + depth(z)。$$

4 总结

显然, 本文给出计算环 Z_{p^k} 上码字深度的算法在计算机上很容易实现, 因此此算法对研究环 Z_{p^k} 上码的深度分布是有参考价值的。环 Z_{p^k} 上码的深度有关性质, 特别是一些特殊类

型码（如线性码，循环码等）的深度分布仍有待进一步研究。

参考文献

- [1] T.Etzion. The depth distribution—A new characterization for linear codes[J]. IEEE Trans.Inform.Th., 1997, 43(4), 1361-1363.
- [2] Y.Luo, F.W.Fu, K.W.Wei. On the depth distribution of linear codes[J]. IEEE Trans.Inform.Th., 2000, 46(6), 2197-2203.
- [3] C.Carlet. Z_{z^k} -linear codes[J]. IEEE Trans.Inform.Th., 1998, 44(4), 1543-1547.
- [4] S.Ling, T.T.Blackford. $Z_{p^{k+1}}$ -linear codes[J]. IEEE Trans.Inform.Th., 2002, 48(9),2592-2605.
- [5] 朱士信, Z_k 线性码的对称形式的 Macwillians 恒等式[J]. 电子与信息学报, 2003, 25(7), 901-906.
- [6] 朱士信, k 元 de Bruijn 序列的升元算法[J]. 电子科学学刊, 2000, 23(1), 68-72.
- [7] C.J.Mithcell. On integer-Valued rational polynomials and depth distributions of binary codes[J]. IEEE Trans. Inform.Th., 1998, 44(7), 3146-3510.
- [8] 岳殿武, E.Shwedyk. 纠错码的深度分布在其周期分布研究中的应用[J]. 应用科学学报, 2001, 19(3), 189-192.