文章编号:1671-6833(2012)03-0110-03

环 Z_M 上线性循环码的深度谱

常晓鹏[1], 郑喜英[2], 孔 波[3]

(1. 河南教育学院 信息技术系,河南 郑州 450046; 2. 黄河科技学院 信息工程学院,河南 郑州 450005; 3. 河南教育学院 数学系,河南 郑州 450046)

摘 要: 在整数剩余类环 $Z_{p_i^{q_i}}(i=1,2,\cdots,l)$ 上长为 n 的线性循环码的深度谱基础上,根据中国剩余定理,研究了整数剩余类环 $Z_M(M=p_1^{q_1}p_2^{q_2}\cdots p_l^{q_l},p_1,p_2,\cdots,p_l$ 为 M 的互不相同的素因子)上长为 $n(p_i$ 不整除 $n,i=1,2,\cdots,l)$ 的循环码的生成多项式,并以多重集的形式给出了 Z_M 上长为 n 的线性循环码的深度谱.

关键词: 生成多项式; 循环码; 深度谱; 深度分布

中图分类号: O157.4 **文献标志码**: A doi:10.3969/j.issn.1671-6833.2012.03.028

0 引言

Etzion T[1]给出了码字的深度、码的深度分布等概念,并定义了一些码的深度分布. Mitchell C J[2]给出了二元循环码的深度分布. Luo Y 等[3]给出了线性码深度分布的计算公式. 朱士信等[4]证明了 $4^{k_1}2^{k_2}$ 型的四元线性码至少含有 k_1+k_2 个非零深度值,并给出了 Z_4 环上循环码的深度谱. 石立叶等[5]证明了 4^k 和 2^k 型的四元循环码恰有 k 个非零深度值,$4^{k_1}2^{k_2}$ 型的四元循环码至少有 k_1+k_2 个非零深度值,并给出了它的深度谱. 郑喜英等[6]给出了整数剩余类环 Z_{p^m} 上的循环码的深度谱.

笔者首先介绍了整数剩余类环 Z_M 上循环码的基本概念及深度的概念和性质,然后由中国剩余定理给出了 Z_M 上长为 n(这里 n 不整除 $\bar{R}$ 的特征)循环码的深度谱.

1 基本概念和结论

设 $R=Z_M$ 的极大理想为 I,令 $\bar{R}=R/I$. R 上长度为 n 的线性码 C 叫做循环码,若满足性质:

$\forall c=(c_0,c_1,\cdots,c_{n-1})\in C\Rightarrow(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$.

我们把 R 上长度为 n 的循环码定义为 R 上的一个加法子模 R^n. 如果 $f(x)$ 整除 x^n-1(即 $x^n-1=f(x)g(x)$,就记 $g(x)=(x^n-1)/f(x)$ 为 $f(x)$. 因此,C 是循环码的充要条件是 C 是多项式环 $R[x]$ 模 x^n-1 的剩余类环 $R[x]/(x^n-1)$ 的理想.

笔者始终假设 n 不整除 $\bar{R}$ 的特征.

任取 $x=(x_1,x_2,\cdots,x_n)\in R$ 定义 x 的微分为 $D(x)=(x_2-x_1,x_3-x_2,\cdots x_n-x_{n-1})$. 这里约定 $n=1$ 时 $D(x)=0$. 对 $1<i\leqslant n$,定义 $D^i(x)=D(D^{i-1}(x))$. 显然 D 是从 R^n 到 R^{n-1} 的一个线性算子.

对任意多项式 $l(x)\in R[x]$,定义线性算子

$$L_{l(x)}:R[x]/(x^n-1)\to R[x]/(x^n-1)$$
$$f(x)\mapsto l(x)f(x)\pmod{x^n-1}.$$

定义 Γ

$$\Gamma:R^n\to R^{n-1}$$
$$(a_0,a_1,\cdots,a_{n-1})\mapsto(a_1,a_2,\cdots,a_{n-1}),$$

称为截取算子. 那么 Γ^i 就是截去前 i 位保留后 $n-i$ 位的算子.

合并算子 L_{x-1} 和 Γ,有 $\Gamma L_{x-1}(a_0,a_1,\cdots,a_{n-1})=(a_0-a_1,a_1-a_2,\cdots,a_{n-2}-a_{n-1})$,显然 $D=-\Gamma L_{x-1}$. 易证三个算子间的关系如下.

引理 1[5] 对 $0\leqslant i\leqslant n$,有 $D^i=-\Gamma^i L_{x-1}^i$.

定义 1 称使 $D^i(x)=0$ 成立的最小非负整

收稿日期:2012-01-08;修订日期:2012-03-22

基金项目:河南省科技攻关项目(112102310377);河南省教育厅自然科学基金(2009A110004);黄河科技学院自然科学基金(KYZR201022)

作者简介:常晓鹏(1977-),男,河南新乡人,河南教育学院讲师,主要从事计算数学方面的研究,E-mail:xpch316@126.com.

数 i 为 x 的深度，记为 $depth(x)$；若没有这样的 i 存在，则令 x 的深度为 n.

定义 2　设 C 是环 R 上长为 n 的码，用 D_i 表示 C 中深度为 i 的码字个数，则称集合 $\{D_0, D_1, \cdots, D_n\}$ 为码 C 的深度分布，称 $\{i \mid D_i \neq 0, 1 \leqslant i \leqslant n\}$ 为码 C 的深度谱，记作 $Dept(C)$. 约定 $Dept(\{0\}) = \phi$.

引理 2　(1)微分算子 D 是从 R^n 到 R^{n-1} 的满线性同态；(2)如果 $depth(x) = d > t > 0$，则 $depth(D^t(x)) = d - t$；(3) $Dept(R^n) = \{1, 2, \cdots, n\}$.

定理 1　设 C 是环 R 上长为 n 的码，即 $C \subset R^n$；设 $1 \leqslant i \leqslant n$，记 $C' = D^i(C)$ 是码 C 通过算子 D^i 在 R^{n-i} 中的像，记 $C'' = \{c \in C \mid D^i(C) = 0\}$，则 $Dept(C) = Dept(C'') \cup (i + Dept(C'))$.

证明　可参看文献[5]中定理 2.6 的证明.

2　主要结论及其证明

定理 2[6]　设 C 是有限链环 Z_{p^a} 上长度为 n 的循环码，则 $R[x]$ 中存在两两互素的多项式 $f_0, f_1, \cdots, f_t$，$f_0 f_1 \cdots f_t = x^n - 1$，使得 $C = (\hat{f}_1, a\hat{f}_2, \cdots, a^{t-1}\hat{f}_t)$，这里 $\deg \hat{f}_i = n - k_i$，$i = 1, 2, \cdots, t$. 若 $(x-1)^{s_i} \| \hat{f}_i$（$\|$ 表示 $(x-1)^{s_i} \mid \hat{f}_i$，但 $(x-1)^{s_i+1}$ 不整除 $\hat{f}_i$）. 则 C 至少有 $k_1 + k_2 + \cdots + k_t$ 个深度值，其深度谱为多重集

$\{1, 2, \cdots, s_1, n - (k_1 - s_1) + 1, n - (k_1 - s_1) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_t, n - (k_t - s_t) + 1, n - (k_t - s_t) + 2, \cdots, n\}$. 只要对数大小比较，去掉重复的值即可.

定理 3　Z_M 为任意的模 M 剩余类环，C 是 Z_M 上长度为 n 的循环码，Z_M 上长度为 n 的循环码 C 至少有 $k_{1_1} + k_{1_2} + \cdots + k_{1_{l_1}} + \cdots + k_{l_1} + k_{l_2} + \cdots + k_{l_{l_l}}$ 个深度值，其深度谱为多重集：

$\{1, 2, \cdots, s_{1_1}, n - (k_{1_1} - s_{1_1}) + 1, n - (k_{1_1} - s_{1_1}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{1_t}, n - (k_{1_t} - s_{1_t}) + 1, n - (k_{1_t} - s_{1_t}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{l_1}, n - (k_{l_1} - s_{l_1}) + 1, n - (k_{l_1} - s_{l_1}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{l_t}, n - (k_{l_t} - s_{l_t}) + 1, n - (k_{l_t} - s_{l_t}) + 2, \cdots, n\}$.

只要对数大小比较，去掉重复的值即可.

证明　令 $M = p_1^{a_1} \cdots p_l^{a_l}$，$p_1, \cdots, p_l$ 为 M 的互不相同的素因子，则在 $Z_M[x]$ 中元素 $p_1^{a_1}, \cdots, p_l^{a_l}$ 是彼此互素的. 由中国剩余定理，

$$Z_M[x]/\langle x^n - 1\rangle \cong Z_{p_1^{a_1}}[x]/\langle x^n - 1\rangle \oplus \cdots \oplus Z_{p_l^{a_l}}[x]/\langle x^n - 1\rangle,$$

设 C 是 Z_M 上长度为 n 的循环码，则 $C \cong C_1 \oplus C_2 \oplus \cdots \oplus C_l$，其中 C_i 为 $Z_{p_i^{a_i}}$ 上长度为 n 的循环码，由定理 2 $Z_{p_i^{a_i}}$ $(i = 1, 2, \cdots, l)$ 上长度为 n 的循环码 C_i 至少有 $k_{i_1} + k_{i_2} + \cdots + k_{i_{l_i}}$ 个深度值，其深度谱为多重集

$\{1, 2, \cdots, s_{i_1}, n - (k_{i_1} - s_{i_1}) + 1, n - (k_{i_1} - s_{i_1}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{i_{l_i}}, n - (k_{i_{l_i}} - s_{i_{l_i}}) + 1, n - (k_{i_{l_i}} - s_{i_{l_i}}) + 2, \cdots, n\}$. 只要对数大小比较，去掉重复的值即可.

任取 $c \in C$，存在 $l_i(x) \in Z_M[x]$，使得 $c(x) = \sum_{i=1}^{l} f_i l_i$. 令 $f_i(x) = f_i(x)$ 模 p^{a_i}，$c_i = f_i(x) l_i(x)$，$i = 1, 2, \cdots, l$，所以 $c_i \in C_i$，又 $depth(c) = \max(depth(c_i))$，所以 $Dept(C) \subseteq Dept(C_1) \cup Dept(C_2) \cup \cdots \cup Dept(C_l)$.

显然反包含也成立，即 $Dept(C) = Dept(C_1) \cup Dept(C_2) \cup \cdots \cup Dept(C_l)$.

Z_M 上长度为 n 的循环码 C 至少有 $k_{1_1} + k_{1_2} + \cdots + k_{1_{l_1}} + \cdots + k_{l_1} + k_{l_2} + \cdots + k_{l_{l_l}}$ 个深度值个深度值，其深度谱为多重集

$\{1, 2, \cdots, s_{1_1}, n - (k_{1_1} - s_{1_1}) + 1, n - (k_{1_1} - s_{1_1}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{1_t}, n - (k_{1_t} - s_{1_t}) + 1, n - (k_{1_t} - s_{1_t}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{l_1}, n - (k_{l_1} - s_{l_1}) + 1, n - (k_{l_1} - s_{l_1}) + 2, \cdots, n; \cdots;$

$1, 2, \cdots, s_{l_t}, n - (k_{l_t} - s_{l_t}) + 1, n - (k_{l_t} - s_{l_t}) + 2, \cdots, n\}$. 只要对数大小比较，去掉重复的值即可.

参考文献：

[1] ETZION E T. The depth distribution: a new characterization for linear codes [J]. IEEE Trans on IT, 1997, 43(4): 1361 - 1363.

[2] MITCHELL C J. On integer-valued rational polynomials and depth distributions of binary codes [J]. IEEE Trans on IT, 1998, 44(7): 1346 - 1350.

[3] YUAN Luo, FU Fang-wei, WEI V K-W. On the depth distribution of linear codes [J]. IEEE Trans Inform Theory, 2000, 46(2): 2197 - 2203.

[4] 朱士信，杨善林，童宏玺. 环 Z4 上线性循环码的深度谱[J]. 电子与信息学报，2005，27(10)：1597 - 1599.

[5] 石立叶，樊恽. 四元循环码的深度分布[J]. 华中

师范大学学报:自然科学版,2009, 43(3):355 - 358.

[6] ZHENG Xi-ying, KONG Bo. The depth spectrums of linear cyclic Codes on Ring Z_{p^m} [C]//IEEE Youth Conference on Information. Beijing: Computing and Telecommunication, 2010: 162 - 165.

Depth Spectrums of Linear Cyclic Codes over Ring Z_M

CHANG Xiao-peng[1], ZHENG Xi-ying[2], KONG Bo[3]

(1. Department of Information Technology, Henan Institute of Education, Zhengzhou 450046, China; 2. Institute of Information Engineering, Huanghe Science and Technology College, Zhengzhou 450005, China; 3. Department of Mathematics, Henan Institute of Education, Zhengzhou 450046, China)

Abstract: Based on the depth spectrum of linear cyclic code of length n over the integer residue class ring $Z_{p_i^{\alpha_i}}$ $(i=1,2,\cdots,l)$, according to the Chinese remainder theorem, the generator polynomial of cyclic code of length n (p_i is not exactly divisible by $n, i=1,2,\cdots,l$) over the integer residue class ring Z_M ($M=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}$ and $p_1,p_2,\cdots,p_l$ are different prime factors of M) is studied. And the depth spectrum of linear cyclic code of length n over Z_M is given in the form of multiset.

Key words: generate polynomial; cyclic code; depth spectrum; depth distribution

---

(上接第109页)

[11] 杨绿溪,李克,周长春,等.一种用于超高斯信号和亚高斯混合信号盲分离的新算法[J].东南大学学报,1999,29(1):1 - 7.

[12] 翁乐明.独立分量分析若干问题的研究[D].上海:上海交通大学理学院数学系,2009.

Research of Image Blind Separation Method Based on QPSO and ICA

FAN Wen-bing, XING Jun-yang, LI Hai-tao, DAI Lin-na

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: In this paper, we introduce the Independent Component Analysis (ICA) and Quantum Particle Swarm Optimization (PSO) briefly. As the ordinary gradient algorithm of ICA technology is easy to fall into local optimum, we proposed quantum-behavior based particle swarm optimization and independent component analysis for blind source separation combining new algorithms. This algorithm takes negative entropy as the objective function of independent component analysis, replaces the ordinary gradient algorithm with QPSO algorithm and separates the instantaneous mixed signals, All the steps of this algorithm are given in this paper. Experiment is show that the proposed algorithm can effectively achieve the image of the blind source separation. Compared with other algorithms, this algorithm shows better performance.

Key words: independent component analysis; quantum particle swarm optimization; blind source separation; negentropy