

基于改进欧几里得算法的卷积码快速盲识别算法*

解 辉¹, 王丰华¹, 黄知涛¹, 张锡祥²

(1. 国防科技大学 电子科学与工程学院, 湖南 长沙 410073

2. 西南电子设备研究所, 四川 成都 610000)

摘要:卷积码盲识别技术在信号截获、智能移动通信、多点广播通信等领域具有广泛应用, 针对卷积码的快速盲识别问题, 对经典欧几里得算法进行了改进, 提出了一种基于改进欧几里得算法的卷积码的快速盲识别方法。算法对卷积码码率进行遍历, 通过欧几里得迭代算法求解卷积的校验多项式, 实现了任意码率卷积码的快速盲识别。对算法进行了仿真, 仿真结果验证了算法的有效性, 且算法的计算量小于文献中已有算法。

关键词:卷积码; 盲识别; 欧几里得

中图分类号: TN911.22 文献标志码: A 文章编号: 1001-2486(2012)06-0158-05

A fast method for blind recognition of convolutional codes based on improved Euclidean algorithm

XIE Hui¹, WANG Fenghua¹, HUANG Zhitao¹, ZHANG Xixiang²

(1. College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China;

2. Southwest China Research Institute of Electronic Equipment, Chengdu 610000, China)

Abstract: Blind recognition of convolutional codes is widely used in the fields of information interception, intelligent mobile communication and multicast communication. In order to solve the problem of fast recognition of convolutional codes, the classical Euclidean algorithm is improved, and a method for blind recognition of convolutional codes based on improved Euclidean algorithm is proposed. Code rate is searched first, the check polynomial of convolutional codes is solved through iterative process, and the convolutional codes can be identified quickly. Validity of the algorithm is verified by the simulation results, and computational load is less than the algorithms in the literature reviewed.

Key words: convolutional code; blind recognition; Euclidean

信道编码盲识别技术在信号截获、智能移动通信、多点广播通信等领域具有广泛应用^[1-4]。其中, 由于卷积码具有纠错能力强、编译码简单、应用广泛等特点^[5], 针对卷积码盲识别的研究成果尤为突出。B. Rice^[6]首次提出了 $1/n$ 码率卷积码的估计方法, 随后, E Filiol^[7]和 A. J. Han Vinck^[8]则将识别范围扩大到了 k/n 码率卷积码。目前, 国内外对各种条件下卷积码的盲识别进行了大量的研究工作^[8-21]。总体来说, 目前卷积码的盲识别主要有基于线性方程组求解^[13-16]、基于欧几里得算法^[17]、基于沃尔什变换^[18-19]和基于对偶码求解^[20-21]等主要算法以及这些方法的改进算法。但随着自适应编码调制等新技术的逐步使用, 对卷积码盲识别的实时性提出了更高的要求。目前已有算法中, 基于欧几里得算法的卷积码盲识别算法计算量最小, 实效性较强, 但该方法

只适用于 $1/2$ 码率卷积码, 适用范围受限。

对此, 本文针对卷积码的快速盲识别问题, 对经典的欧几里得算法进行了改进, 提出了一种基于改进欧几里得算法的卷积码盲识别算法, 使之可以求解多个多项式的最大公约式, 算法能够适用于所有码率卷积码, 且算法计算量小, 满足对数据的快速处理要求。

1 卷积码盲识别数学模型

由卷积码的编码原理可知, (n, k, m) 卷积码的编码过程可用下式表示^[3]

$$\mathbf{V}(X) = \mathbf{U}(X) \cdot \mathbf{G}(X) \quad (1)$$

其中, $\mathbf{V}(X)$ 表示编码输出序列, $\mathbf{U}(X)$ 表示待编码的信息序列, $\mathbf{G}(X)$ 为生成多项式矩阵。卷积码的生成多项式矩阵 $\mathbf{G}(X)$ 包含了 (n, k, m) 的信息以及卷积码的生成过程, 能唯一定义一种卷

* 收稿日期: 2012-04-16

基金项目: 国家自然科学基金资助项目(61072120); 教育部新世纪优秀人才支持计划项目

作者简介: 解辉(1983—), 男, 河北保定人, 博士研究生, E-mail: xiehui2005@gmail.com;

王丰华(通信作者), 男, 讲师, 博士, E-mail: wfh.abc@163.com

积码。

又因为卷积码的校验矩阵 $\mathbf{H}(X)$ 与生成矩阵 $\mathbf{G}(X)$ 满足

$$\mathbf{G}(X) \cdot \mathbf{H}(X)^T = 0 \quad (2)$$

由式(1)和式(2)可以得到

$$\mathbf{V}(X) \cdot \mathbf{H}(X)^T = \mathbf{U}(X) \cdot \mathbf{G}(X) \cdot \mathbf{H}(X)^T = 0 \quad (3)$$

其多项式表示为

$$\sum_{i=1}^n v^i(x) h^i(x) = 0 \quad (4)$$

在通信过程中,接收方或侦收方通过对接收数据进行解调等系列处理能恢复出 $\mathbf{V}(X)$ 。卷积码的生成多项式矩阵盲估计就是在 $\mathbf{U}(X)$ 和 $\mathbf{G}(X)$ 都是未知的情况下根据 $\mathbf{V}(X)$ 求出生成多项式矩阵 $\mathbf{G}(X)$, 进而解码恢复出信息序列 $\mathbf{U}(X)$ 。

在实际应用中,很难从卷积码编码的起始位置获取数据,造成(4)式结果不等于0,文献[17]对此进行了分析,并给出了1/2码率卷积码盲识别的数学模型

$$v^1(x) h^1(x) + v^2(x) h^2(x) \equiv d(x) \pmod{x^N} \quad (5)$$

对于 $(n-1)/n$ 码率的卷积码,则有

$$v^1(x) h^1(x) + v^2(x) h^2(x) + \dots + v^n(x) h^n(x) \equiv d(x) \pmod{x^N} \quad (6)$$

上式与关键方程形式相似,称为 n 阶关键方程。

$(n-1)/n$ 码率卷积码校验矩阵的求解可以用 n 阶关键方程描述为: 在集合 $\Phi^{(n)} = \{(h^1(x), \dots, h^n(x), L) \in F[x]^{n+1} \mid \exists d(x) \in F[x], \text{使得 } h^1(x)v^1(x) + \dots + h^n(x)v^n(x) \equiv d(x) \pmod{x^{N+1}}, \text{且 } \deg d(x) < L, \max(\deg h^1(x), \dots, \deg h^n(x)) \leq L\}$

中寻找元素 $(h^1(x), \dots, h^n(x), L)$, 使得 $(h^1(0), \dots, h^n(0)) \neq (0, \dots, 0)$ 且 L 达到最小。其中 $F[x]$ 为二元域上的多项式环。

2 改进欧几里得算法的推导

经典欧几里得算法是一个递归算法,能够快速求解式(5)中的关键方程,但无法适应式(6),本节对经典欧几里得算法进行扩展,使之能够快速求解 n 阶关键方程。

首先以 $n=3$ 时的多项式为例进行分析。设有限域的三个多项式 $v^1(x)$ 、 $v^2(x)$ 和 $v^3(x)$, 求阶数最小的 $h^1(x)$ 、 $h^2(x)$ 和 $h^3(x)$ 使得

$$v^1(x) h^1(x) + v^2(x) h^2(x) + v^3(x) h^3(x) = 0 \quad (8)$$

为不失一般性,设 $v^1(x)$ 的阶数低于 $v^2(x)$ 和 $v^3(x)$ 的阶数(可能并列最低), 则式(8)可转换为

$$\begin{aligned} h^1(x) &= \frac{v^2(x) h^2(x) + v^3(x) h^3(x)}{v^1(x)} \\ &= k_1 h^2(x) + \beta_1 h^3(x) + \frac{v_1^2(x) h^2(x)}{v^1(x)} \\ &\quad + \frac{v_1^3(x) h^3(x)}{v^1(x)} \end{aligned} \quad (9)$$

其中 k_1, β_1 为商, $v_1^2(x), v_1^3(x)$ 为余数, 即 $v^2(x) = k_1 v^1(x) + v_1^2(x)$, $v^3(x) = \beta_1 v^1(x) + v_1^3(x)$ 。因为 $v^1(x)$ 为最小, 则商是非零的, 但余数可能为零。

令 $v_1^1(x) = v^1(x)$ 及 $h_1^1(x) = \frac{v_1^2(x) h^2(x)}{v^1(x)} + \frac{v_1^3(x) h^3(x)}{v^1(x)}$, $h_1^2(x) = h^2(x)$, $h_1^3(x) = h^3(x)$, 则有

$$v_1^1(x) h_1^1(x) + v_1^2(x) h_1^2(x) + v_1^3(x) h_1^3(x) = 0 \quad (10)$$

再选择 $v_1^1(x), v_1^2(x), v_1^3(x)$ 的阶数最低者, 例如设 $v_1^3(x)$ 阶数最低(也可以并列最低), 则有

$$\begin{aligned} h_1^3(x) &= \frac{v_1^1(x) h_1^1(x) + v_1^2(x) h_1^2(x)}{v_1^3(x)} \\ &= k_2 h_1^1(x) + \beta_2 h_1^2(x) + \frac{v_2^1(x) h_1^1(x)}{v_1^3(x)} \\ &\quad + \frac{v_2^2(x) h_1^2(x)}{v_1^3(x)} \end{aligned} \quad (11)$$

其中 $v_1^1(x) = k_2 v_1^3(x) + v_2^1(x)$, $v_1^2(x) = \beta_2 v_1^3(x) + v_2^2(x)$ 。

令 $v_2^3(x) = v_1^3(x)$ 及 $h_2^3(x) = \frac{v_2^1(x) h_1^1(x)}{v_1^3(x)} + \frac{v_2^2(x) h_1^2(x)}{v_1^3(x)}$, $h_2^1(x) = h_1^1(x)$, $h_2^2(x) = h_1^2(x)$, 则

式(11)可化为

$$v_2^1(x) h_2^1(x) + v_2^2(x) h_2^2(x) + v_2^3(x) h_2^3(x) = 0 \quad (12)$$

因为上述过程中 $v_i^1(x), v_i^2(x), v_i^3(x)$ 是严格递减的, 则一定可以达到 $v_i^1(x), v_i^2(x), v_i^3(x)$ 中出现0或1。设最后一步递推形式为

$$\begin{aligned} Z_m(x) &= \frac{v_m^1(x) h_m^1(x) + v_m^2(x) h_m^2(x)}{v_m^3(x)} \\ &= k_{m+1} h_m^1(x) + \beta_{m+1} h_m^2(x) + \frac{v_{m+1}^1(x) h_m^1(x)}{v_m^3(x)} \end{aligned}$$

递推过程如表2所示。算法输出的 $h^1(x)$ 、 $h^2(x)$ 和 $h^3(x)$ 就是该码的校验多项式。

表1 前向迭代过程

Tab.1 Process of forward iteration

递推次数	v^1 次数	v^2 次数	v^3 次数	v^4 次数	除数
1	75	70	75	75	v^2
2	69	70	68	68	v^3
3	65	64	68	66	v^2
4	63	64	63	63	v^1
5	63	62	61	62	v^3
6	59	59	61	59	v^1
7	59	58	57	55	v^4
8	54	54	53	55	v^3
9	51	52	53	50	v^4
10	49	5	49	50	

表2 反向迭代估计过程

Tab.2 Process of reverse iteration

递推次数	$h^1(x)$	$h^2(x)$	$h^3(x)$	$d(x)$
1	0	1	0	0
2	0	x^2	0	$1+x$
3	0	x^4	$1+x^2+x^3$	x^2+x^3
4	0	x^6	$x^2+x^4+x^5$	$1+x+x^3$
5	$1+x^4+x^5$	x^6	$x^2+x^4+x^5$	$1+x+x^3$
6	$1+x^4+x^5$	x^6	$x^2+x^4+x^5$	$1+x+x^3$
7	$1+x^2+x^3+x^5+x^6$	x^6	$x^2+x^4+x^5$	$1+x+x^3$
8	$1+x^2+x^3+x^5+x^6$	$xx^2+x^5+x^6$	$x^2+x^4+x^5$	$1+x+x^3$
9	$1+x^2+x^3+x^5+x^6$	$xx^2+x^5+x^6$	$xx^2+x^3+x^6$	$1+x+x^3$
10	$1+x^2+x^3+x^5+x^6$	$1+x^4+x^6$	$xx^2+x^3+x^6$	$1+x+x^3$

通过逆向迭代,得 $h^1(x) = 1 + x^2 + x^3 + x^5 + x^6$, $h^2(x) = 1 + x^4 + x^6$, $h^3(x) = x + x^2 + x^3 + x^6$ 。算法正确估计出了该卷积码的校验多项式,从而验证了算法的有效性。对卷积码的校验矩阵进行求解后,根据文献[13]的方法可以求出卷积码的生成矩阵,进而实现对卷积码的译码。

对于系统递归卷积码,其校验多项式存在分母多项式,但输出码字为系统码,例如一个2/3码率的非递归卷积码校验多项式和递归卷积码校验多项式如下所示

$$H(x) = [1 \quad 1+x^2 \quad 1+x+x^2] \quad (22)$$

$$H(x) = [1/(1+x+x^2) \quad (1+x^2)/(1+x+x^2) \quad 1] \quad (23)$$

可以看出,两种多项式之间为一个线性变换,并不影响码字之间的线性关系,因此,本文提出的算法对于系统递归卷积码同样适用。

5 算法性能分析

假设卷积码校验多项式的最高阶数为 m ,卷积码输出路数 n ,则列方程组所需要的码元长度 $N \geq (n+1) \times (m+1)$,求解线性方程组所需的计算量为 $O(N^3)$,文献[14-15]对求解算法进行优化,使得算法的计算量减少为 $O(N^2)$ 。而基于Walsh-Hadamard变换的求解算法的计算量则为 $(m+1)n2^{(m+1)n}$ [18]。本文中所给出的基于改进欧几里得算法求解校验矩阵的最大递推次数为 $2n(m+1)-1$ 。每次递推中进行的多项式乘法次数为 $n-1$,则每次多项式乘法的计算量为 N 次二元域乘法 and 加法。因此基于改进欧几里得算法求解的二元域乘法和加法的计算量最大为

$$M = 2N(n-1)(n(m+1)-1) = 2N((m+1)n^2 - (m+2)n + 1) \quad (24)$$

算法的计算复杂度为 $O(N)$ 。

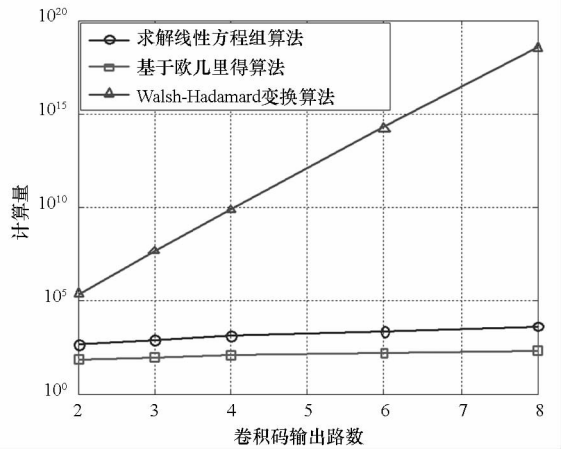


图1 各主要算法计算量比较

Fig.1 The computational load of algorithms

图1给出了本文算法与高斯消元法和Walsh-Hadamard变换算法在求解CCSDS标准卷积码校验矩阵时计算量的比较,仿真中改进欧几里得算法中假定接收的每路码长度为100,仿真次数为1000。从图中可以看出,基于欧几里得算法的计算量最小,且在实际应用中迭代算法会提前终止跳出,所以实际的计算量小于理论上的最大计算量。

在实际应用中,由于接收码序列中存在误码,导致算法产生错误的结果,对于长度为 N 的码字,其正确的校验多项式是固定的,而由于随机误码导致的错误校验多项式则是随机分布的。因此在一定码字正确率条件下,可通过对多组码字进行求解,并对结果进行直方图统计来提高算法的误码适应能力。

6 结束语

本文针对任意码率卷积码的快速盲识别问题,对经典欧几里得算法进行了改进推导,提出了一种基于改进欧几里得算法的卷积码的快速盲识别方法,并对该算法进行了仿真,仿真结果验证了算法的有效性。对算法计算量的分析表明,本文提出的算法计算量小于目前文献已有算法,可以较好地适应系统对算法实时性的要求,同时算法简单,易于工程实现。

参考文献 (References)

- [1] Moosavi R, Larsson E. A fast scheme for blind identification of channel codes [C]//Proceedings of Global Telecommunications Conference, Linköping, Sweden, IEEE press, 2011: 1-5.
- [2] Bringer J, Chabanne H. Code reverse engineering problem for identification codes [J]. IEEE Transactions on Information Theory, 2012, 58(4): 2406-2412.
- [3] 张永光, 楼才义. 信道编码及其识别分析 [M]. 北京: 电子工业出版社, 2010.
ZHANG Yongguang, LOU Caiyi. Channel coding recognition and analysis [M]. Beijing: Publishing House of Electronics Industry, 2010. (in Chinese)
- [4] 邹艳. 信息截获与处理的容错技术研究 [D]. 上海: 复旦大学, 2006.
ZOU yan. Research on error-resilient techniques of information intercepting and processing [D]. Shanghai: Fudan University, 2006. (in Chinese)
- [5] Lint J. Introduction to coding theory [M]. Third Edition. Springer-Verlag Press, 2003.
- [6] Rice B. Determining the parameters of a rate $1/n$ convolutional encoder over $GF(q)$ [C]//Proceedings of the 3rd International Conference on Finite Fields and Applications, Glasgow, USA, IEEE press, 1995.
- [7] Filiol E. Reconstruction of convolutional encoders over $GF(q)$ [J]. Lecture Notes in Computer Science, 1997(1355): 101-109.
- [8] Vinck A, Dolezal P, Kim Y. Convolutional encoder state estimation [J]. IEEE Transactions on Information Theory, 1998, 44(4): 1604-1608.
- [9] Barbier J, Sicot G, Houcke S. Algebraic approach for the reconstruction of linear and convolutional error correcting codes [C]//Proceedings of World Academy of Science, Engineering and Technology. 2006, 11(16): 1307-6884.
- [10] Dingel J, Hagenauer J. Parameter estimation of a convolutional encoder from noisy observations [C]//ISIT 2007, France: IEEE Press, 2007: 1776-1780.
- [11] Cote M, Sendrier N. Reconstruction of convolutional codes from noisy observation [C]//ISIT 2009, Seoul, Korea; IEEE Press, 2009: 546-550.
- [12] Cluzeau M, Finiasz M. Reconstruction of punctured convolutional codes [C]//Information Theory Workshop 2009, IEEE press, 2009: 75-79.
- [13] LU P Z, SHEN L, ZOU Y, et al. Blind recognition of punctured convolutional codes [J]. Science in China Ser. F Information Sciences, 2005, 48(4): 484-498.
- [14] 邹艳, 陆佩忠. 关键方程的新推广 [J]. 计算机学报, 2006, 29(5): 711-718.
ZOU Yan, LU Peizhong. A new generalization of key equation [J]. Chinese Journal of Computers, 2006, 29(5): 711-718. (in Chinese)
- [15] Lu P Z, Zou Y. Fast computations of gröbner bases and blind recognitions of convolutional codes [J]. Lecture Notes in Computer Science, 2007(4547): 303-317.
- [16] 周亚建, 刘健. $(n, n-1, m)$ 卷积码的盲识别 [J]. 北京邮电大学学报, 2010, 33(3): 135-138.
ZHOU Yajian, LIU Jian. A blind recognition of the $(n, n-1, m)$ convolution code [J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3): 135-138. (in Chinese)
- [17] Wang F H, Huang Z T, Zhou Y Y. A method for blind recognition of convolution code based on Euclidean algorithm [C]//IEEE International Conference on Wireless Communications. Shanghai: IEEE Press. 2007: 1414-1417.
- [18] 刘健, 王晓君, 周希元. 基于 Walsh-Hadamard 变换的卷积码盲识别 [J]. 电子与信息学报, 2010, 32(4): 884-888.
LIU Jian, WANG Xiaojun, ZHOU Xiyuan. Blind recognition of convolutional coding based on walsh-hadamard transform [J]. Journal of Electronics & Information Technology, 2010, 32(4): 884-888. (in Chinese)
- [19] 戚林, 郝士琦, 王磊. 基于改进 Walsh-Hadamard 变换的删除卷积码盲解码算法 [J]. 计算机应用研究, 2011, 28(4): 1457-1459.
QI Lin, HAO Shiqi, WANG Lei. Blind decoding algorithm of punctured convolutional codes based on improved WHT [J]. Application Research of Computers, 2011, 28(4): 1457-1459. (in Chinese)
- [20] Marazin M, Gautier R, Burel G. Dual code method for blind identification of convolutional encoder for cognitive radio receiver design [C]//GLOBECOM Workshops 2009, Univ. Europeenne de Bretagne, Rennes, France, IEEE press, 2009: 1-6.
- [21] Marazin M, Gautier R, Burel G. Blind recovery of k/n rate convolutional encoders in a noisy environment [J]. Wireless Communications and Networking, 2011, 2011(1): 1186-1687.