

基于中国剩余定理分解的RS码快速盲识别算法

甘露* 周攀

(电子科技大学电子工程学院 成都 611731)

摘要: 该文提出一种新的RS (Reed Solomon)码盲识别方法。该方法利用RS码等效二进制准循环码的代数结构,将截获到的二进制码序列映射为环上的线性码,应用中国剩余定理(Chinese Remainder Theorem, CRT)将环上的线性码进行直和分解,计算不同码长下所有本原多项式对应分量码在相应码空间的归一化维数,通过寻找归一化维数的最小值,实现对RS码码长和本原多项式的识别;最后通过对码字进行因式分解识别RS码的生成多项式。该方法具有使用数据量少,运算量低等方面的特点。仿真结果表明,能完成在较高误码率的情况下对RS码的快速盲识别。

关键词: 无线通信; RS码; 非合作通信; 准循环码; 盲识别; 中国剩余定理

中图分类号: TN92

文献标识码: A

文章编号: 1009-5896(2012)12-2837-06

DOI: 10.3724/SP.J.1146.2012.00434

Fast Blind Recognition Method of RS Codes Based on Chinese Remainder Theorem Decomposition

Gan Lu Zhou Pan

(School of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: Based on the property that the equivalent binary block codes of Reed-Solomon (RS) codes are quasi-cyclic codes, a new blind recognition method of RS codes is proposed. The intercepted binary sequence is regarded as linear codes over a ring. Then, the decomposition into component codes of equivalent codes is conducted by using the Chinese Remainder Theorem (CRT). By computing the normalized dimensions of the component codes over different fields and finding the minimum of them, the length and the primitive polynomial of the RS code are estimated. Finally the generator polynomial can be obtained by factoring the RS code words. The proposed method has lower computational complexity and uses less intercepted data than existing methods. Simulation results show that it has good performance even if with high BER situation.

Key words: Wireless communication; Reed-Solomon (RS) codes; Non-cooperative communication; Quasi-cyclic codes; Blind recognition; Chinese Remainder Theorem (CRT)

1 引言

在无线通信中,由于信道传输特性与噪声的影响。传输信号不可避免地会发生错误。通常采用信道编码,即差错控制编码,将误码率降低,从而提高无线通信系统的可靠性。RS(Reed Solomon)码是一类具有很强纠错能力的多进制线性分组码,它首先由Reed和Solomon应用Mattson-Solomon多项式于1960年构造出来。因其构造方便,编解码简单,广泛应用于高密度磁盘、深空通讯、数字广播电视等多个方面^[1]。

在感知无线电通信系统中,若能仅根据接收到

的码流估计出系统所采用的编码参数,能大大提高系统的灵活性。在非合作通信中,若能仅从截获的码流中估计出编码参数,就能为实现对通信方信息的截获奠定重要的基础。因此,编码识别技术对合作与非合作通信领域都显得尤为重要。近几年来,编码盲识别技术发展迅速,逐渐成为了通信领域内新的研究热点。在交织盲识别技术方面,甘露等人^[2]提出的假设交织参数并对去交织后数据的结构特征进行分析,实现了对卷积交织参数的盲识别。对卷积码的盲识别,目前的研究较多,最近刘健等人^[3]提出了利用容错矩阵分解求解的方法,实现了对高误码卷积码的盲识别。对于线性分组码,目前的研究主要集中在二进制线性分组码的盲识别上,虽取得了较大的进展,但对于通信系统中常用的多进制线性分组码盲识别技术的研究还较少。由于多进制

2012-04-17 收到, 2012-09-21改回

中央高校基本科研业务费专项资金基础研究项目(ZYGX2010J027)

和国家自然科学基金(11176005)资助课题

*通信作者: 甘露 ganlu@uestc.edu.cn

线性分组码是在高阶伽罗华域上构造,并且在实际应用中具有码长较长的特点。如果直接将二进制线性分组码的识别技术应用于对其的盲识别上,一方面会因为所需接收数据量大,导致识别算法的计算量大,抗误码性能下降等问题;另外一方面不能给出多进制线性分组码中特有的本原多项式的估计,因而需要对多进制线性分组码的盲识别技术进一步开展研究。RS码是一类非常重要的多进制线性分组码,文献[4-6]均提出可利用二进制线性分组码的性质完成码长的识别,再利用RS码在伽罗华域上的快速傅里叶变换(GFFT)具有连零的性质来识别本原多项式以及生成多项式。其中文献[4]和文献[5]提出利用矩阵化简秩特性识别RS码码长,但是该方法只对短码长RS码的识别有较好效果;文献[6]利用RS码码字的二进制形式进行码根求解,缩小了本原多项式的搜索范围,但该方法存在对短码长RS码适用率不高等缺点;文献[7]中提出的仅用GFFT来识别码长、本原多项式和生成多项式的方法,虽具有较好性能,但所需运算量和计算量均很大;文献[8]提出利用RS码等效二进制码的循环移位特性,通过欧几里得算法计算循环移位前后码字的最大公因子来完成RS码码长的识别,该方法适用于长码长RS码,相较于文献[7]的方法,该方法的运算量较低,但依旧需要大量的数据。

上述几种RS码识别算法,利用RS码等效二进制码的性质来估计码长,并缩小算法中估计本原多项式与生成多项式的搜索范围,却没有减少估计码长时所需的数据量,因而算法总体所需数据量并没有减少,性能也得不到实质提升。本文提出的RS码盲识别方法,就是利用RS码在二元域上的映射为准循环码的性质^[9],并利用中国剩余定理(Chinese Remainder Theorem, CRT)分解构造出与原码一一对应的线性码^[10],将码长估计与本原多项式估计结合起来。通过计算该线性码在不同本原多项式下分量码空间的归一化维数,进而寻找归一化维数的最小值,完成对RS码参数的盲估计。理论分析表明,相较于现有算法,本文提出的算法所需的数据量大幅降低。计算机仿真结果表明,在误码率为 10^{-3} 的情况下,识别概率在90%以上。

2 RS码的定义与准循环码

2.1 RS码的定义

RS码是多进制线性分组码,在一个可纠正 t 个符号错误的 (n, k) RS码中,输入符号分为 km bit一组,每组包括 k 个符号,每个符号由 m bit组成,即RS码的码元和生成多项式的根都取自 $\text{GF}(2^m)$ 上

$(m \neq 1)$ ^[9]。由于在 $\text{GF}(2^m)$ 域中以 α^i 为根的最小多项式的形式为 $m_i(x) = (x - \alpha^i), 0 \leq i < 2^m - 1$,故生成多项式 $g(x)$ 为

$$g(x) = \prod_{i=j}^{j+2t-1} (x - \alpha^i) \quad (1)$$

以一个码长 $n = 63$,可纠正3个错误的RS码为例,该码的生成多项式为

$$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4) \cdot (x + \alpha^5)(x + \alpha^6)$$

2.2 RS码在二元域上的映射与准循环码

引理1^[9] 设 \mathbf{V} 是由 $\text{GF}(2^m)$ 上的 $k \times n$ 阶生成矩阵 \mathbf{G} 所生成的RS码,则 \mathbf{V} 的二进制向量表示 (mn, mk) 是 $\text{GF}(2)$ 上的线性分组码。

显然可见,将 $\text{GF}(2^m)$ 上码长为 $n = (2^m - 1)$ 的RS码码字映射到 $\text{GF}(2)$ 上,其码长为

$$n' = (2^m - 1)m \quad (2)$$

记 \mathbf{C} 为 \mathbf{V} 映射到 $\text{GF}(2)$ 上的二进制码。由RS码的循环移位特性可知, \mathbf{C} 为 $\text{GF}(2)$ 上长度为 n' ,指数为 m 的准循环码^[10]。

设 $\mathbf{c} = (c_{0,0}, c_{0,1}, \dots, c_{0,m-1}, c_{1,0}, \dots, c_{1,m-1}, \dots, c_{n-1,0}, \dots, c_{n-1,m-1})$ 为 \mathbf{C} 中一个码字,其中 $c_{i,j}$ 表示第 i 个循环块中第 j bit。记 $\mathbf{F}[x]$ 表示 $\text{GF}(2)$ 上关于变量 x 的所有多项式的集合,则 $\mathbf{R}(\mathbf{F}, n) = \mathbf{F}[x]/(x^n - 1)$ 为 $\mathbf{F}[x]$ 关于理想 $(x^n - 1)$ 的商环。将 $\mathbf{R}(\mathbf{F}, n)$ 简记为 \mathbf{R} ,记 \mathbf{F}^{nm} 为 $\text{GF}(2)$ 上 nm 维向量张成的子空间, \mathbf{R}^m 为 \mathbf{R} 上 m 维向量张成的子空间,则下面的定理1成立。

定理1^[10] 定义 $\mathbf{F}^{nm} \rightarrow \mathbf{R}^m$ 的映射 ϕ :

$$\phi(\mathbf{c}) = (c'_0(x), c'_1(x), \dots, c'_{m-1}(x)) \in \mathbf{R}^m \quad (3)$$

其中

$$c'_j(x) = \sum_{i=0}^{n-1} c_{i,j} x^i \in \mathbf{R}$$

显然,由映射 ϕ 得到的线性码 \mathbf{C}' 与原准循环码 \mathbf{C} 一一映射。以 \mathbf{c} 为例,在映射 ϕ 下,与 \mathbf{c} 相对应的 \mathbf{c}' 的构造可表示为

$$\begin{array}{ccc} c_{0,0} & c_{0,1} & c_{0,m-1} \\ +c_{1,0}x & +c_{1,1}x & +c_{1,m-1}x \\ +c_{2,0}x^2 & +c_{2,1}x^2 & +c_{2,m-1}x^2 \\ +c_{3,0}x^3 & +c_{3,1}x^3 & \dots & +c_{3,m-1}x^3 \\ \vdots & \vdots & & \vdots \\ +c_{n-1,0}x^{n-1} & +c_{n-1,1}x^{n-1} & & +c_{n-1,m-1}x^{n-1} \\ \downarrow & \downarrow & & \downarrow \\ c'_0(x) & c'_1(x) & \dots & c'_{m-1}(x) \end{array}$$

$\mathbf{c}' = (c'_0(x), c'_1(x), \dots, c'_{m-1}(x))$ 是由映射 ϕ 得到的线性码 \mathbf{C}' 中的一个码字。

2.3 环与环上码的分解

考虑RS码在二元域上的映射, $n = (2^m - 1)$ 与域 $GF(2)$ 的特征2互质, 由CRT可知, 环 R 可拆分为一些有限域的直和。由唯一因式分解定理^[11]可知, 多项式 $x^n - 1 = x^{2^m-1} - 1$ 可完全分解为 $F[x]$ 上不可约多项式的乘积, 即

$$x^{2^m-1} - 1 = \prod_{i=1}^r f_i \quad (4)$$

其中 f_i 为互不相同的不可约多项式。

定理 2^[11] 当 $f(x) = p(x)$ 是 m 次不可约多项式时, 则同余类环 $F[x]/p(x)$ 是一个含有 p^m 个元素的有限域(p 为域 F 的特征), 可称为 $F[x] \bmod p(x)$ 的同余类域。因此有

$$R = \frac{F[x]}{x^{2^m-1} - 1} = \bigoplus_{i=1}^r \frac{F[x]}{f_i} \quad (5)$$

其中 \bigoplus 表示直和。用 F_i 代表 $F[x]/f_i$, 则 R 的 m 维子空间 R^m 满足

$$R^m = \bigoplus_{i=1}^r F_i^m \quad (6)$$

相应地, 每一个环 R 上长度为 m 的线性码 C' 可以写成

$$C' = \bigoplus_{i=1}^r C'_i \quad (7)$$

其中 C'_i 为 F_i 上的线性码。设 C' 中一码字 $c' = (c'_0(x), c'_1(x), \dots, c'_{m-1}(x))$, $\alpha_i \in F_i$ 为 f_i 的根。则

$$c'_i = (c'_0(\alpha_i), c'_1(\alpha_i), \dots, c'_{m-1}(\alpha_i)) \quad (8)$$

为 C'_i 中的码字。

若准循环码在 $R = F[x]/(x^n - 1)$ 上的生成矩阵包含 ρ 行, 则称该准循环码为 ρ -生成元准循环码。设 k_i 为 C'_i 的维数, 则有定理3成立。

定理 3^[12] 若 C 为 $GF(2)$ 上码长为 mn 的 ρ -生成元准循环码, 有 $\rho = \max k_i$ 。即 C' 在CRT下可分解为

$$C' = \bigoplus_{i=1}^r C'_i$$

其中 C'_i 为 F_i 上的 (m, k_i) 线性码, 且 $\rho = \max k_i$ 。相反地, 任一准循环码的分量码 C'_i , 满足 $\rho = \max k_i$, 为 ρ -生成元准循环码。

3 RS码盲识别模型

在实际的通信应用中, RS码都是以二进制的形式进行传输。截获的RS码序列实为RS码在 $GF(2)$ 上的映射, 即二进制准循环码。通过分析截获数据中的帧结构, 可以找到帧头, 便能找到RS码的起始位置。本文同文献[7]和文献[8]一样暂不考虑RS码的码组同步问题, 因此RS码盲识别就是要估计出其码长 n , 本原多项式 $p(x)$, 生成多项式 $g(x)$ 。

当 (n, k) RS码码长选取正确时, 通过定理1中的映射 ϕ 得到的 C' , 在CRT下可将其分解为分量码的组合。由定理3可知, 其分量码 C'_i 的码空间维数 k_i 必然满足

$$k_i \leq m \quad (9)$$

若码长选取不正确, 分组后的序列类似于随机序列^[13]。通过映射 ϕ 得到的 C' , 其分量码 C'_i 的码空间维数 $k_i = m$ 。

定义分量码 C'_i 的码空间的归一化维数为

$$\sigma_i = \dim(C'_i) / m \quad (10)$$

其中 $\dim(C'_i)$ 表示分量码 C'_i 码空间的维数。

由于多项式 $x^n - 1 = x^{2^m-1} - 1$ 的因式分解 $x^{2^m-1} - 1 = \prod_{i=1}^r f_i$, $f_i (i = 1, \dots, r)$ 中包括 m 下所有的本原多项式, 其中设RS码编码域的本原多项式 $p(x)$ 对应的分量码 C'_p 码空间归一化维数为 σ_p , 则有

$$\sigma_p = \min_i \sigma_i \quad (11)$$

通过计算分别得到 m 个 f_i 下的分量码码字, 将其排列成 $GF(2^m)$ 上的 $m \times m$ 的数据矩阵 A_i , $\text{rank}(A_i)$ 表示矩阵 A_i 的秩。在无误码的情况下, 矩阵 A_i 的归一化秩 $\text{rank}(A_i) / m$ 小于等于码空间的归一化维数; 在一定误码率下, 仍可认为数据矩阵的归一化秩为分量码码空间归一化维数较好的估计。

通过前面的分析可知, 选取适当的码长对截获的二进制RS数据进行分组。通常情况下编码域维数的取值 $m = 3 \sim 8$, 对应的符号码长的取值范围为 $n = 2^m - 1$, 各种码长对应的所有本原多项式可事先计算出并存储下来^[1]。当码长选取错误, 该码长下所有本原多项式对应的分量码码空间归一化维数都取得最大值; 当码长选取正确, 码长下所有本原多项式对应的分量码满足定理3, 且归一化维数最小的分量码所对应的本原多项式即为RS码编码域的本原多项式。最后对RS码码字进行因式分解, 其中连续根对应最小多项式的乘积即为RS码的生成多项式。综上所述, 本文提出的RS码盲识别算法的流程如图1所示。

4 算法有效性仿真验证及性能分析

4.1 仿真验证

以 $(63, 55)$ RS码为例, 本原多项式为 $p(x) = 1 + x^5 + x^6$ 。用matlab模拟产生出16320 bit数据。设 $c = (c_{0,0}, c_{0,1}, \dots, c_{0,5}, c_{1,0}, \dots, c_{1,5}, \dots, c_{63,0}, \dots, c_{63,5})$ 为其中一个码字, $c' = (c'_0(x), c'_1(x), \dots, c'_5(x))$ 为在映射 ϕ 下, 与 c 相对应的码字。

$x^{63} - 1$ 在 $GF(2)$ 上因式分解所得的最小多项式中包括 $m' = 6$ 下所有的本原多项式, 即 $p_1(x) = 1$

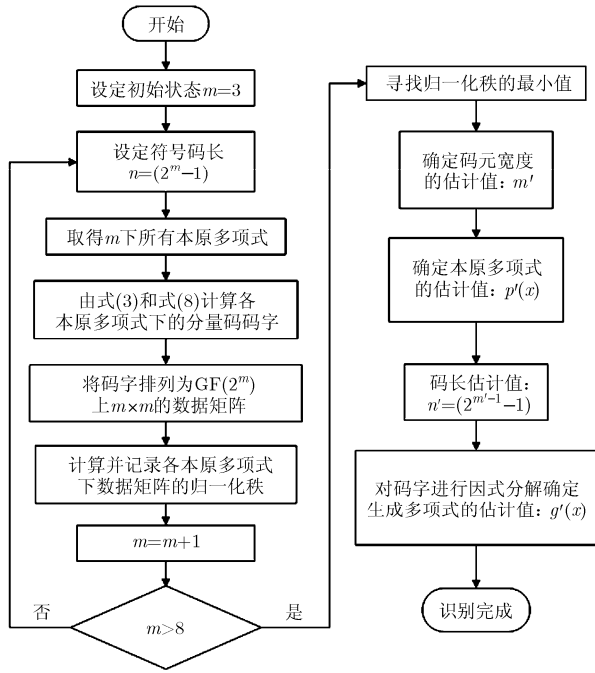


图1 RS码盲识别算法流程

$+x+x^6$, $p_2(x) = 1+x+x^3+x^4+x^6$, $p_3(x) = 1+x^5+x^6$, $p_4(x) = 1+x+x^2+x^5+x^6$, $p_5(x) = 1+x^2+x^3+x^5+x^6$ 和 $p_6(x) = 1+x+x^4+x^5+x^6$, 其余因式分解所得的最小多项式非 $m'=6$ 下的本原多项式, 与识别过程无关, 故不再对这些最小多项式进行讨论和运算。设 α_1 为 $p_1(x) = 0$ 的根, 则 $c'_{\alpha_1} = (c'_0(\alpha_1), c'_1(\alpha_1), \dots, c'_5(\alpha_1))$ 为 $p_1(x)$ 下的一个分量码码字, 计算得到 $m'=6$ 个 $p_1(x)$ 下的分量码码字, 排列成 $GF(2^{m'})$ 上的 $m' \times m'$ 的数据矩阵 A_1 , $\text{rank}(A_1)/m'$ 即为 $p_1(x)$ 下对应的分量码码空间的归一化维数。利

用截获数据分别在 $m = 3 \sim 8$ 下做上述计算, 依次构造各本原多项式下的分量码, 计算并记录下所有分量码码空间的归一化维数, 结果如图2所示。

由图2可见, 仅当 $m'=6$ 出现了码空间归一化维数小于1的情况, 而在遍历到第3个本原多项式, 即 $p_3(x) = 1+x^5+x^6$ 时, 分量码码空间归一化维数取到了最小。成功完成了对码长和本原多项式的识别。最后对码字进行因式分解, 其中连续根对应的一次因式的乘积为其生成多项式^[9], 即 $g(x) = \prod_{i=1}^8 (x + \alpha^i)$ 。

4.2 算法复杂度分析

对本文的方法和文献[7]中提出的仅使用GFFT的识别算法、文献[8]中提出的综合运用欧几里得算法和GFFT的方法进行算法复杂度的比较。本文提出的方法, 需要的数据量最少为 $8 \times 8 \times 255 = 16320$ bit。实际上, 如表1所示, 对 m 进行遍历时, 在具体 m' 下, 最少仅需 $m' \times m' \times (2^{m'} - 1)$ bit 的数据量参与运算。文献[7]和文献[8]的方法至少需约50组RS码, 以 $m = 3, n = 7$ 的情况为例, 也需1050 bit, 若需对 $m = 8, n = 255$ 的RS码进行识别, 则需 1.02×10^5 bit。识别所需数据量大是目前RS码识别算法研究所遇到的困难之一, 由表1可见, 本文所提算法对数据量的要求相较于以往的算法已降低了很多, 因而具备一定的先进性。

本文提出的方法主要的运算量集中在分量码的计算上, 以一个 (n, k) RS码码字为例, 某一本原多项式下其分量码的计算需要 mn 次 $GF(2^m)$ 上的加法, 不需要 $GF(2^m)$ 上的乘法, 总共等效的模2加运算量

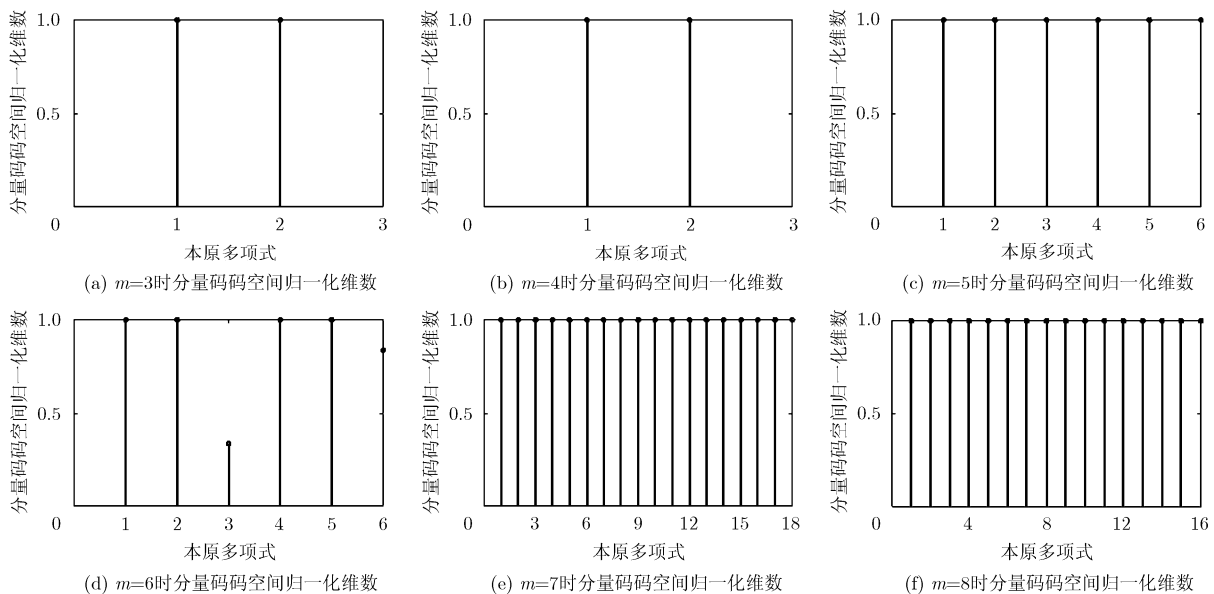


图2 各码长下分量码空间归一化维数

表1 3种算法所需数据量比较(bit)

m	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$
本文算法	63	240	775	2268	6223	1.63×10^4
文献[7]算法	1050	3000	7750	1.89×10^4	4.45×10^4	1.02×10^5
文献[8]算法	1050	3000	7750	1.89×10^4	4.45×10^4	1.02×10^5

为 m^2n 次。而对同一码字进行GFFT运算得到该码字频谱,需要约 $n^2 - n$ 次 $GF(2^m)$ 上的加法,和 n^2 次 $GF(2^m)$ 上的乘法,总共等效的模2加运算量为 $3m(m-1)n^2 + mn(n-1)$ 次;采用欧几里得算法得到码字的最大公因式需要进行 $(mn+1)mn/2$ 次模2加运算^[8]。本文算法和文献[7]算法都需要遍历各码长下所有的本原多项式,而文献[8]的方法在使用欧几里得算法估计码长时不需要遍历本原多项式,为了便于比较,将其运算所需的模2加的次数分摊到每个本原多项式下,即 $(mn+1)mn/(2P)$,其中 P 为 m 下本原多项式的个数^[11]。如表2所示,在 $m=8$ 的情况下对同一码字进行分量码计算、GFFT运算和欧几里得算法,本文算法的是文献[7]算法的约千分之一,是文献[8]算法的十分之一,且文献[8]在应用欧几里得算法时,仅完成了对码长的识别,还没有完成对本原多项式的识别。要达到相同的性能,本文提出的算法需要的数据量远小于文献[7]和文献[8]的方法。由此可见,本文提出的算法运算量明显小于文献[7]和文献[8]的方法,随着码长的增加,这一优势越发明显。模2加运算可利用数字信号处理芯片与现场可编程门阵列中的位操作就能实现,并且所提算法具有结构清晰简单的特点,因此可在硬件设备中高速实现。

4.3 仿真结果分析

产生 $m=3 \sim 8$ 的二进制RS码各16320 bit。在

各误码率下,对各码长的RS码分别进行1000次识别实验,得到识别概率曲线如图3和图4所示。可以看出,在 $m \leq 5$ 的情况下,在误码率低于 10^{-2} 时识别概率达到了95%以上;在 $m > 5$ 时,本文所提算法对RS码参数的检测性能明显优于文献[7]和文献[8]的方法,在误码率低于 10^{-3} 时识别概率也到了90%以上。在更高的误码率下可增加使用数据量来提高识别概率。

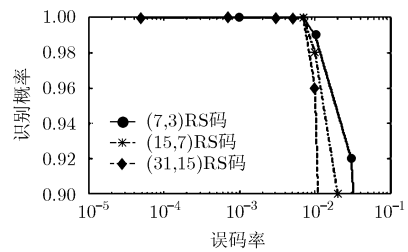


图3 $m=3-5$ 识别概率图

5 结束语

本文利用RS码在二元域上的映射为准循环码的性质,提出了一种基于准循环码代数结构的RS码盲识别方法。将接收到的二进制码序列映射为环上的线性码,运用CRT将环上的线性码分解为一些分量码的直和,计算各码长下所有本原多项式对应的

表2 3种算法所需模2加次数比较

m	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$
本文算法	63	240	775	2268	6223	1.6×10^4
文献[7]算法	1008	8940	6.2×10^4	3.8×10^5	2.1×10^6	1.1×10^7
文献[8]算法	116	915	2015	1.4×10^4	2.2×10^4	1.3×10^5

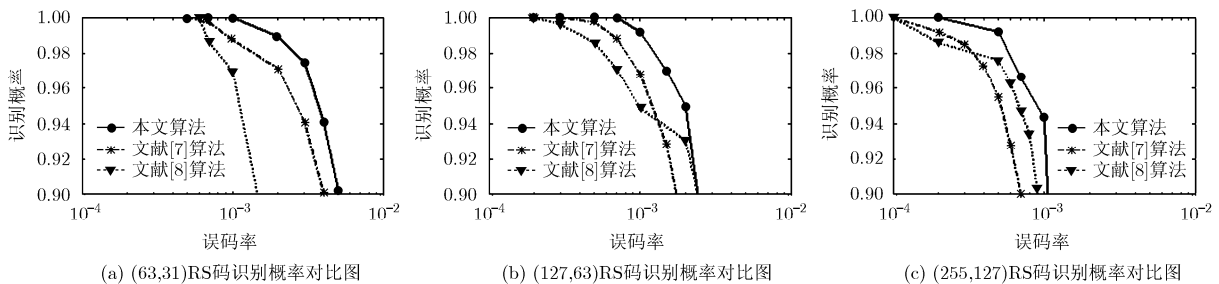


图4 $m=6-8$ 识别概率对比图

分量码空间归一化维数, 通过寻找归一化维数的最小值, 同时完成对码长和本原多项式的识别; 最后通过对码字进行因式分解识别生成多项式。因具有使用数据量少, 计算速度快等优点, 与基于GFFT的方法相比, 本文提出的算法运算量大大降低。仿真结果表明, 该方法能实现在较高误码率的情况下对RS码参数的快速盲估计, 在误码率为 10^{-3} 的情况下, 识别概率在90%以上。

参考文献

- [1] Lin Shu and Costello D J. Error Control Coding [M]. Second Edition, New Jersey: USA, Prentice Hall, 2005: 67-95.
 - [2] 甘露, 刘宗辉, 廖红舒, 等. 卷积交织参数的盲估计[J]. 电子学报, 2011, 39(9): 2173-2177.
Gan Lu, Liu Zong-hui, Liao Hong-shu, et al.. Blind estimation of the parameters of convolutional interleave[J]. *Acta Electronica Sinica*, 2011, 39(9): 2173-2177.
 - [3] 刘健, 林宇生, 周希元. 高误码(2,1,m)卷积码盲识别[J]. 北京工业大学学报, 2011, 37(1): 60-65.
Liu Jian, Lin Yu-sheng, and Zhou Xi-yuan. Blind recognition of (2,1,m) convolution coding in the high error rate condition[J]. *Journal of Beijing University of Technology*, 2011, 37(1): 60-65.
 - [4] 刘健, 谢锴, 周希元. RS码的盲识别方法[J]. 电子科技大学学报, 2009, 38(3): 363-367.
Liu Jian, Xie Nuo, and Zhou Xi-yuan. Blind recognition method of RS coding[J]. *Journal of University of Electronic Science and Technology of China*, 2009, 38(3): 363-367.
 - [5] 闻年成, 杨晓静. RS码的参数识别[J]. 计算机工程与应用, 2011, 47(19): 136-139.
Wen Nian-cheng and Yang Xiao-jing. Blind recognition of RS codes parameters[J]. *Computer Engineering and Applications*, 2011, 47(19): 136-139.
 - [6] 吕喜在, 苏绍璟, 黄芝平. 一种RS码快速盲识别方法[J]. 国防科技大学学报, 2011, 33(4): 123-127.
Lü Xi-zai, Su Shao-jing, and Huang Zhi-ping. A fast blind recognition method of RS coding[J]. *Journal of National University of Defense Technology*, 2011, 33(4): 123-127.
 - [7] 刘健. 信道编码的盲识别技术研究[D]. [博士学位论文], 西安电子科技大学, 2010.
Liu Jian. Research on blind recognition technology for channel coding[D]. [Ph.D. dissertation], Xidian University, 2010.
 - [8] 戚林, 郝士琦, 王磊, 等. 一种RS码快速盲识别方法[J]. 电路与系统学报, 2011, 16(2): 71-76.
Qi Lin, Hao Shi-qi, Wang Lei, et al.. A fast blind recognition method of RS codes[J]. *Journal of Circuits and Systems*, 2011, 16(2): 71-76.
 - [9] 刘玉君. 信道编码[M]. 郑州: 河南科学技术出版社, 2007: 129-180.
Liu Yu-jun. Channel Coding[M]. Zhengzhou: Henan Science and Technology Press, 2007: 129-180.
 - [10] Ling S and Sole P. On the algebraic structure of quasi-cyclic codes I: finite fields[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 2751-2760.
 - [11] 万哲先. 代数和编码[M]. 北京: 高等教育出版社, 2007: 39-111.
Wan Zhe-xian. Algebra and Coding[M]. Beijing: Higher Education Press, 2007: 39-111.
 - [12] Ling S and Sole P. On the algebraic structure of quasi-cyclic codes III: generator theory[J]. *IEEE Transactions on Information Theory*, 2005, 51(7): 2692-2700.
 - [13] Lally K and Fitzpatrick P. Algebraic structure of quasi-cyclic codes[J]. *Discrete Applied Mathematics*, 2001, 111(1): 157-175.
- 甘露: 男, 1974年生, 副教授, 硕士生导师, 从事通信信号分析、阵列信号处理方面的研究工作。
周攀: 男, 1987年生, 硕士生, 从事信道编码识别与参数估计方面的研究工作。