ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 34,No. 6,Nov. 2019,pp. 1012－1018
DOI:10. 16337/j. 1004-9037. 2019. 06. 007

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

基于非零均值比的RS码盲识别方法

龙　浪[1,2]　杨俊安[1,2]　刘　辉[1,2]　梁宗伟[1,2]

(1. 国防科技大学电子对抗学院,合肥,230037;2. 安徽省电子制约技术重点实验室,合肥,230037)

摘　要: 针对现有的RS码盲识别方法抗误码性能不佳的问题,提出了一种基于非零均值比的盲识别算法。该算法通过将截获到的RS码序列转化为GF(2^m)码元来构建分析矩阵,利用有限域的高斯约当算法获得分析矩阵的非零均值比,并以此来识别码长、符号数和本原多项式,最后通过伽罗华域傅里叶变换来完成信息位长及生成多项式的识别。仿真结果表明,本文提出的算法可以有效识别出本原RS码及缩短RS码的所有编码参数,抗误码性能较好,并给出了识别性能与信息位长与码长的关系:随着码长和信息位长的增加,识别性能逐渐下降。

关键词: RS码;非零均值比;有限域;盲识别

中图分类号: TN919.3　　**文献标志码:** A

Blind Identification of RS Code Parameters Based on Non-Zero-Mean-Ratio

Long Lang[1,2], Yang Junan[1,2], Liu Hui[1,2], Liang Zongwei[1,2]

(1. School of Electronic Countermeasure, National University of Defense Technology, Hefei, 230037, China;2. Key Laboratory of Electronic Restricting Technique of Anhui Province, Hefei, 230037, China)

Abstract: Aiming at poor anti-error performance in the existing algorithms for RS codes, a blind recognition algorithm based on non-zero-mean-ratio is proposed. The algorithm constructs the analysis matrix by transforming the intercepted RS code sequence into GF (2^m) symbols. The finite-field Gauss-Jordan elimination algorithm is used to obtain the non-zero-mean-ratio of the analysis matrix and identify the code length, symbol number and the primitive polynomial. Finally, the Galois field Fourier transform is used to complete the information bit length and generator polynomial recognition. Simulation results show that the proposed algorithm can effectively identify all the coding parameters of the primitive RS code and shorten RS code. The anti-error performance is better, and the relationship among the recognition performance and the information bit length and the code length is given. As the code length and information bit length increase, the recognition performance gradually decreases.

Key words: RS code; non-zero-mean-ratio; finite field; blind recognition

引　　言

在数字通信中,信道编码可以提高通信的可靠性,目前信道编码主要包括线性分组码、RS(Reed-Solomon)码、卷积码和低密度校验码(Low-density parity-check, LDPC)码等[1-2],其中RS码是一

收稿日期:2018-06-14;**修订日期:**2018-09-01

种特殊的非二进制BCH(Bose-Chaudhuri-Hocquenghem)码,具有纠错能力强的特点,在数据存储、军事通信、卫星通信和数字视频广播(Digital video broadcasting,DVB)系统中起着至关重要的作用。因此,研究RS码的盲识别方法有重要意义。

现有文献表明,国内外已有大量学者对RS码盲识别算法展开研究。文献[3]对各种非二进制纠错码的码长进行了盲识别,并扩展到有噪环境下的研究,但未对RS码其他编码参数进行识别。文献[4]在文献[5]对偶码的识别基础上研究了有噪环境下的RS码盲识别,但算法抗误码性能不佳。文献[6]提出一种基于后验校验对数似然比[6-8]的方法来对RS码进行识别,但需要在发射端和接收端预定义RS编码集。以上方法并未对缩短RS码进行识别,识别分析不够全面。

针对以上不足,本文提出一种基于非零均值比的盲识别算法来完成RS码和缩短RS码的识别。利用截获到的RS码序列建立分析矩阵,通过有限域的高斯约当算法[9]获得分析矩阵的非零均值比,以此来识别码长、符号数和本原多项式,然后通过伽罗华域傅里叶变换(Galois field Fourier transform,GFFT)来完成信息位长及生成多项式的识别,最后针对典型的RS码和缩短RS码编码方式,设计了仿真分析实验,对不同识别算法在不同误码率下的识别性能进行了分析比较。

1　RS码识别基础

RS码属于一个特殊的非二进制BCH码,码符号来源于伽罗华域(Galois field,GF),GF(2^m),其中m表示每个符号的位数且$m\geqslant 3$。假设α为GF(2^m)的本原元,则$\alpha^{2^m-1}=1$。在纠错能力为t的(n,k)RS码中,$\alpha,\alpha^2,\cdots\alpha^{2t}$是$n-k$次生成多项式$g(x)$的根,则$g(x)$为

$$g(x)=lcm(\phi_1(x),\phi_2(x),\cdots,\phi_{2t}(x)) \tag{1}$$

式中:$\phi_i(x)$是α^i的最小多项式,由于α^i是GF(2^m)中的元素,$\phi_i(x)=x-\alpha^i$,则$g(x)$可以表示为[10]

$$\begin{aligned} g(x)&=(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t})=\\ &g_0+g_1x+g_2x^2+\cdots+g_{2t-1}x^{2t-1}+x^{2t}\end{aligned} \tag{2}$$

式中:$g(x)$有$2t+1$非零项,而$g(x)$是$n-k$次多项式,所以$n-k=2t$。

综上所述,需要识别的GF(2^m)上的RS码参数分别为:

(1) 码字长度n。其中本原RS码$n=2^m-1$,而缩短RS码[11]是原(n,k)本原RS码删除前i位信息位为0的码字后所构造的新码,由于仍可构成一个$(k-i)$维的线性子空间,所以能得到一个$(n-i,k-i)(1\leqslant i\leqslant k)$的缩短RS码,其码长$n\neq 2^m-1$,其他参数均与原RS码相同,识别方法基本与本原RS码一致。

(2) 信息位长$k=n-2t$。

(3) 校验位长$2t=n-k$。

(4) 生成多项式$g(x)$。

(5) 符号数m,一般m取3~8。

(6) 本原多项式$p(x)$,一般采用十进制表示,如$p=41$表示$p(x)=x^5+x^3+1$,因为$41_{10}=101001_2$。符号数m及其本原多项式如表1所示[12]。

表1　m值及其对应的本原多项式十进制表示

Tab. 1　m and decimal primitive polynomial

m	本原多项式十进制表示
3	11 13
4	19 25
5	37 41 47 55 59 61
6	67 91 97 103 109 115
7	131 137 143 145 157 167 171 185 191 193 203 211 213 229 239 241 247 253
8	285 299 301 333 351 355 357 361 369 391 397 425 451 463 487 501

2　基于非零均值比的盲识别算法

在实际通信系统中,(n,k,m,p)RS码是以二进制等价码流进行传输的[13],所以需先将截获得到的

RS码序列转化为GF(2^m)码元，并构建分析矩阵，通过有限域的高斯约当算法[9]获得分析矩阵的非零均值比，以此来识别码长、符号数和本原多项式，最后通过GFFT来完成信息位长及生成多项式的识别。

2.1 基于非零均值比的码长、符号数和本原多项式的识别

利用假定的符号数m'及本原多项式p'将截获到的RS码流转化为GF(2^m)上的$0\sim 2^m$元素，按行放入一个$a\times b$的矩阵$\boldsymbol{A}$中，其中a表示矩阵的行数，b表示矩阵的列数，且$a\gg b$。如果矩阵$\boldsymbol{A}$的矩阵列数为真实码长且符号数及本原多项式估计正确时，则每行的信息位和校验位对齐，由于校验码元与信息码元线性相关，每行均存在着相同的线性关系，当对矩阵$\boldsymbol{A}$进行高斯消元变换后，$n-k$列相关列（校验位所在的列）将会被消去，只会留下k列非零列即独立列（信息位所在的列），如图1(a)所示，分析矩阵将会出现秩的缺失；反之，当列数不是真实码长或符号数及本原多项式估计错误时，同一码字的信息位和奇偶校验位在不同的行中被隔离，在同一列中没有正确对齐，校验位不能被表示为信息位的线性组合，在特定的行中线性关系将受到影响，而这将导致列之间的线性关系消失，因此，矩阵$\boldsymbol{A}$会表现得像一个随机矩阵。当矩阵$\boldsymbol{A}$进行高斯消元变换后，由于不存在相关列，所以秩被完全获得，如图1(b)所示，则分析矩阵为满秩矩阵。

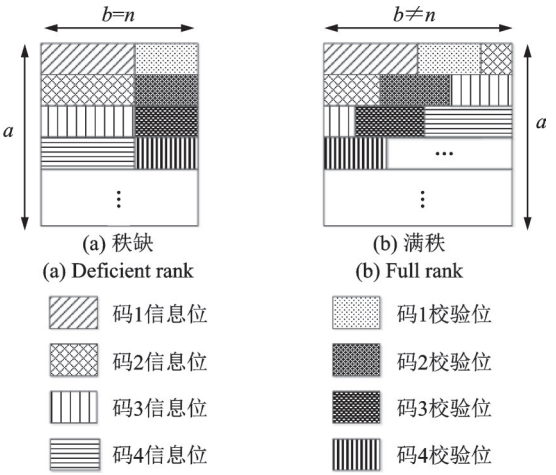

图1 分析矩阵结构图

Fig. 1 Structure of analysis matrix

简而言之，当且仅当$m'=m^{\text{est}}$，$p'=p^{\text{est}}$，$b=n^{\text{est}}$时，矩阵$\boldsymbol{A}$为秩缺矩阵，在无误码的情况下计算矩阵秩ρ如式(3)所示，归一化秩ρ'如式(4)所示，此时，秩ρ等于信息位长，归一化秩ρ'为码率r。

$$\rho=k \tag{3}$$

$$\rho'=\frac{k}{b}=\frac{k}{n}=r \tag{4}$$

其他情况下，矩阵$\boldsymbol{A}$为满秩矩阵，此时矩阵秩ρ如式(5)所示，归一化秩ρ'如式(6)所示，此时，秩ρ等于列数，归一化秩ρ'为1。

$$\rho=b \tag{5}$$

$$\rho'=\frac{b}{b}=1 \tag{6}$$

在无误码的情况下，可利用有限域的高斯约当法对矩阵$\boldsymbol{A}$求秩来识别码长、符号数及本原多项式，当且仅当归一化秩ρ'最小时完成识别。然而在有误码的情况下，直接求秩法并不适用[5,9,14]。如前所述，当一个矩阵所有行和列都是线性无关的，此时称为满秩矩阵；如果一个矩阵至少有一列/行依赖于其他列/行，那么此时会出现秩缺。在实际通信系统中，传输错误或白噪声的存在增加了行/列之间的线性无关性[15]，并且这种线性无关随着噪声强度的增大而增大，当噪声水平超过阈值时，使分析矩阵$\boldsymbol{A}$不会有任何相关列/行，就像一个随机矩阵。此时，不管列数b是否等于真实码长，矩阵$\boldsymbol{A}$均会是一个满秩矩阵。

但在有误码的情况下，利用有限域的高斯约当算法将矩阵$\boldsymbol{A}$转换成为三角矩阵$\boldsymbol{Q}$，通过对下三角阵$\boldsymbol{Q}$的观察可以发现，与独立列相比，相关列的非零元素较少，因此，存在秩缺失的矩阵比满秩矩阵含有的零元素要少，因此，在有误码的情况下，可以根据矩阵$\boldsymbol{Q}$中每列的非零元素所占的比例来确定矩阵的秩

缺情况,故定义非零均值比$u'(b)$来表示矩阵的秩缺失情况为

$$u'(b)=\frac{\sum_{c=1}^{b}\phi'(c)}{b} \tag{7}$$

$$\phi'(c)=\frac{\varphi'(c)}{a} \tag{8}$$

式中:$\varphi'(c)$表示第c列中非零的数目,$\phi'(c)$表示下三角矩阵$\boldsymbol{Q}$中第c列含非零数目所占比重。

利用有限域的高斯约当消元法将分析矩阵$\boldsymbol{A}$转化为下三角阵$\boldsymbol{Q}$后,通过计算矩阵$\boldsymbol{Q}$的非零均值比$u'(b)$来完成RS码参数的盲识别,当且仅当$m'=m^{\text{est}},p'=p^{\text{est}},b=n^{\text{est}}$时,$u'(b)$最小。

2.2　信息位、校验位及生成多项式的识别

设GF(2^m)上的多项式[16]

$$a(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0\quad a_i\in GF(q) \tag{9}$$

则它在GF(q)的谱多项式为

$$A(z)=A_{n-1}z^{n-1}+\cdots+A_1z+A_0=\sum_{j=0}^{n-1}A_jz^j \tag{10}$$

式中:$A_j=a(a^j)=\sum_{i=1}^{n-1}a_ia^{ji}(j=0,1,\cdots,n-1)$,　$a^n=1$;　$A(z)=(A_{n-1},\cdots,A_1,A_0)$　是　$a=(a_{n-1},\cdots,a_1,a_0)$的GF($2^m$)上的离散傅里叶变换,记为GFFT,$a(x)$和$A(z)$是一对傅里叶变换对。

在RS码中,码多项式与生成多项式具有相同的码根,因此,在码长,符号数及本原多项式正确识别后,将接受序列按正确码长分组对其进行GFFT变换,并采用最大似然法来评估根数,当多组码字经GFFT后具有相同的连零位置且个数相同时,由此可以估计出码根数即校验位长$2t$,通过计算$n-2t=k$即可求取信息位长,最后通过式(2)得到生成多项式$g(x)$。

2.3　算法流程

(1)设RS码的估计码长为n',遍历对应的符号数m'及本原多项式p',并利用p'将截获的RS码序列由GF(2)转化为GF(2^m)中的元素。

(2)将转化后的RS码序列按行放入$a\times b$的矩阵$\boldsymbol{A}$中,其中a为矩阵的行数,b为矩阵的列数,$b=n'$且满足$a\gg b$,构建分析矩阵。

(3)利用有限域的高斯消元法将$\boldsymbol{A}$转化为下三角阵$\boldsymbol{Q}$。

(4)计算每列列中非零的数目$\varphi'(c)$,并计算出每列非零数目所占比重$\phi'(c)$。

(5)计算整个下三角阵$\boldsymbol{Q}$的非零均值比$u'(b)$。

(6)改变RS的估计码长n',重复步骤(1)—(5),当且仅当非零均值比$u'(b)$最小时完成识别,即$[n^{\text{est}},m^{\text{est}},p^{\text{est}}]=\underset{n',m',p'}{\operatorname{argmin}}\,u'(b)$。

(7)计算码字多项式的根,记录根的数目来估计$n-k$,从而计算出信息位长k。

(8)根据式(2)计算生成多项式$g(x)$。

3　仿真实验与性能分析

3.1　实验仿真

为了验证本文所提方法的有效性,分别针对本原RS码以及缩短RS码设计仿真分析实验,编码参数设置如表2所示。利用MATLAB随机生成0、1随机序列,然后以表2中编码参数进行编码,并叠加

高斯随机噪声，信噪比SNR=10 dB，产生误码率为$p_e=0.01$的码序列，并用本文所提出的算法对其进行识别。

表2 参数设置

Tab. 2 Parameter setting

码型	编码	符号数	本原多项式	生成多项式
本原RS码	(63,58)	6	103	$g(x)=x^5+62x^4+32x^3+53x^2+3x+31$
缩短RS码	(204,199)	8	285	$g(x)=x^5+62x^4+63x^3+229x^2+197x+38$

从图2可以看出，与其他可能的组合相比，当$[n, m, p]=[63,6,103]$时，$u'(b)$达到最小值，因此，可以识别出码长，符号数及本原多项式。当正确识别码长、符号数及本原多项式后，利用GFFT可以计算出在码根$\alpha^5,\alpha^4,\alpha^3,\alpha^2,\alpha$处码谱为0，码根数为5，即校验位长$2t=5$，则$k=n-2t=58$，即信息位长58，将码根代入式(2)，可以得到生成多项式$g(x)=x^5+62x^4+32x^3+53x^2+3x+31$。至此，完成了对本原RS码的识别。

同样地，在图3中，当$[n, m, p]=[204,8,285]$，$u'(b)$达到最小值，因此，可以识别出码长、符号数及本原多项式。当正确识别码长、符号数及本原多项式后，利用GFFT可以计算出在码根$\alpha^5,\alpha^4,\alpha^3,\alpha^2,\alpha$处码谱为0，码根数为5，即校验位长$2t=5$，则$k=n-2t=199$，即信息位长199，将码根代入式(2)，可以得到生成多项式$g(x)=x^5+62x^4+63x^3+229x^2+197x+38$。至此，完成了对缩短RS码的识别。

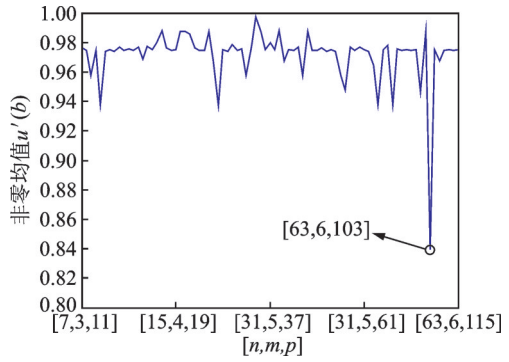

图2 本原RS码识别时$u'(b)$随估计参数的变化

Fig.2 Values of assuming primitive RS code

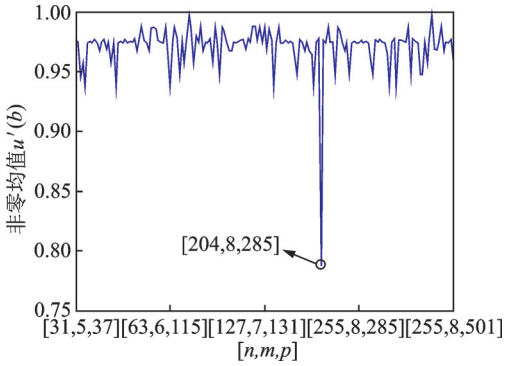

图3 缩短RS码识别时$u'(b)$随估计参数的变化

Fig.3 Values of assuming short RS code

3.2 识别性能分析

在图4中，对$n=15, m=4, p=19$的RS码，选取$k=7, k=9, k=11$不同的信息位长在不同误码率的情况下进行识别性能分析，从图4中可以看出，RS码参数识别性能随着信息位长k或码率r的增大而减小。随着r的增大，$n-k$减小即相关列会随之减少，利用$u'(b)$区分满秩矩阵和秩缺矩阵难度加大，因此，识别难度加大，准确度下降。

在图5中，对码率$r\approx0.6$的(63,38,6,67)RS码，(127,76,7,131)RS码和(255,153,8,285)RS码在不同误码率的情况下进行识别性能分析，从图5中可以看出，RS码参数识别性能随着码长n的增大而减小，在误码率不超过0.02时，对所有RS码都能达到90%的识别率，具有较好的识别性能。

图6给出了在采用(15,7,4,19)RS码时，本文算法，文献[6]中基于后验校验对数似然比算法与文献

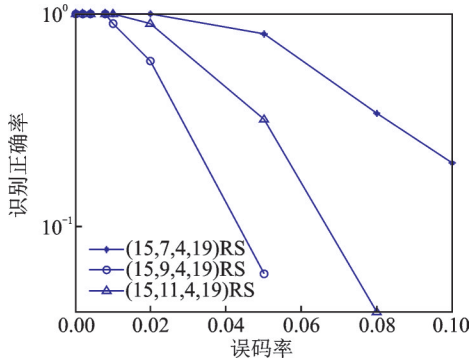

图4　不同信息位长识别性能比较

Fig.4　Comparison of recognition performance among different information bit lengths

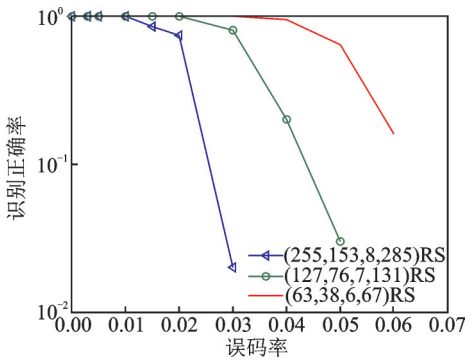

图5　不同码长识别性能比较

Fig.5　Comparison of recognition performance among different code lengths

[4]中基于Barbier方法的参数估计法的比较。随着误码率的增加,3种算法识别性能也随之下降,但本文算法下降较慢,优于其他两种算法,并给出了正确识别一次3种算法所需时间,如表3所示,本文算法运算时间由于经过多次行列变换,稍逊于基于后验校验对数似然比算法,但抗误码性能较优。

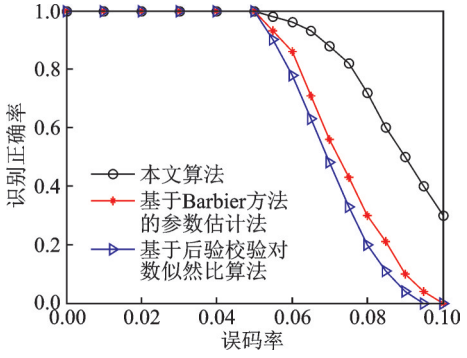

图6　3种算法识别性能比较

Fig.6　Comparison of recognition performance among three algorithms

表3　不同算法的运行时间对比

Tab. 3　Comparison of run time among different algorithms

算法	运行时间/s
基于后验校验对数似然比算法[6]	72.896
基于Barbier方法的参数估计法[4]	105.630
本文算法	100.161

4　结束语

根据RS码的编码结构及特点,提出了一种基于非零均值比的RS码盲识别方法,利用有限域的高斯消元法计算出分析矩阵的非零均值比来确定码长、符号数及本原多项式,然后利用GFFT变换求解出其他参数,完成了对本原RS码缩短RS码的识别,并且分析了信息位长和码长与识别的准确性之间的关系,随着信息位长和码长度的减少,识别更加准确。并与文献[4,6]方法进行比较,本文算法抗误码性能优于其他两种算法,并且计算复杂度低,更适合有噪环境下的RS码识别。

参考文献:

[1]　张岱, 张玉, 杨晓静. 一种高误码(n,k,m)非系统卷积码盲识别算法[J]. 数据采集与处理, 2015, 30(3): 636-645.
Zhang Dai, Zhang Yu, Yang Xiaojing. Algorithm for blind recognition of (n,k,m) non-systematic convolutional code with high BER[J]. Journal of Data Acquisition and Processing, 2015, 30(3): 636-645.

[2]　曾辉, 黄鲁, 杨灿美. 基于IR-UWB系统的高速准循环LDPC编解码器设计[J]. 数据采集与处理, 2015, 30(3): 599-605.
Zeng Hui, Huang Lu, Yang Canmei. High-rate quasi-cyclic LDPC design for IR-UWB system[J]. Journal of Data Acquisition and Processing, 2015, 30(3): 599-605.

[3] Zrelli Y, Gautier R, Rannou E, et al. Blind identification of code word length for non-binary error-correcting codes in noisy transmission[J]. Eurasip Journal on Wireless Communications & Networking, 2015, 2015(1): 1-16.

[4] Zahedi A, Gholam-Reza M K. Reconstruction of a non-binary block code from an intercepted sequence with application to Reed-Solomon Codes[J]. Ieice Trans Fundamentals, 2012, 95(11): 1873-1880.

[5] Sicot G, Houcke S, Barbier J. Blind detection of interleaver parameters[J]. Signal Processing, 2009, 89(4): 450-462.

[6] Zhang H, Wu H C, Jiang H. Novel blind encoder identification of Reed-Solomon codes with low computational complexity [C]// Global Communications Conference. Atlanta, GA, USA: IEEE Communications Press, 2013: 3294-3299.

[7] Moosavi R, Larsson E G. Fast blind recognition of channel codes[J]. IEEE Transactions on Communications, 2014, 62(5): 1393-1405.

[8] Xia T, Wu H C. Novel blind identification of LDPC codes using average LLR of syndrome a posteriori probability[J]. IEEE Transactions on Signal Processing, 2014, 62(3): 632-640.

[9] Lu L, Li K H, Guan Y L. Blind detection of interleaver parameters for non-binary coded data streams[C]// IEEE International Conference on Communications. Dresden, Germany: IEEE Communications Press, 2009: 1-4.

[10] 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: 109-112.
Zhang Yongguang, Lou Caiyi. Channel coding and recognition analysis[M]. Beijing: Publishing House of Electronics Industry, 2010: 109-112.

[11] 赵旸, 耿相铭. RS(16,12)缩短码编译码原理及性能分析[J]. 通信技术, 2012, 45(2): 49-52.
Zhao Yang, Geng Xiangming. Encoding and decoding algorithm for RS(16,12)shortened codes and its performance analysis[J]. Communications Technology, 2012, 45(2): 49-52.

[12] 朱联祥, 李荔. RS码的盲识别方法研究[J]. 电子测量与仪器学报, 2013, 27(8): 781-787.
Zhu Lianxiang, Li Li. Research on blind recognition for RS code[J]. Journal of Electronic Measurement and Instrument, 2013, 27(8): 781-787.

[13] 甘露, 周攀. 基于中国剩余定理分解的RS码快速盲识别算法[J]. 电子与信息学报, 2012, 34(12): 2837-2842.
Gan Lu, Zhou Pan. Fast blind recognition method of RS codes based on Chinese remainder theorem decomposition[J]. Journal of Electronics and Information Technology , 2012, 34(12): 2837-2842.

[14] Swaminathan R, Madhukumar A S. Classification of error correcting codes and estimation of interleaver parameters in a noisy transmission environment[J]. IEEE Transactions on Broadcasting, 2017,63(3): 463-478.

[15] Zrelli Y, Gautier R, Rannou E, et al. Blind identification of code word length for non-binary error-correcting codes in noisy transmission[J]. Eurasip Journal on Wireless Communications & Networking, 2015, 2015(1): 1-16.

[16] 解辉, 王丰华, 黄知涛,等. 基于频谱预处理的RS码盲检测识别方法[J]. 宇航学报, 2013, 34(1): 128-132.
Xie Hui, Wang Fenghua, Huang Zhitao, et al. Blind detection and recognition of RS code based on spectral preprocessing[J]. Journal of Astronautics, 2013, 34(1): 128-132.

作者简介:

龙浪(1994-),女,硕士研究生,研究方向:信道编码识别分析、通信对抗,E-mail:1244102522@qq.com。

杨俊安(1965-),男,教授,博士,研究方向:信号处理、智能计算等。

刘辉(1983-),男,讲师,博士,研究方向:通信对抗、智能信息处理等。

梁宗伟(1994-),男,硕士研究生,研究方向:卫星信号处理、通信对抗。

(编辑:陈珺)