一种软判决下的RS码识别算法

吴昭军[①] 张立民*[①] 钟兆根[②] 刘传辉[①]

[①](海军航空大学信息融合研究所 烟台 264001)

[②](海军航空大学航空基础学院 烟台 264001)

摘 要：针对现有RS码识别算法需要对码字符号在不同域之间进行转化，且容错性能较差的问题，该文提出一种直接利用软判决序列完成RS码识别算法。算法首先从RS码定义出发，给出了RS码校验关系从GF(2^m)到GF(2)上的等价转换方式，从而避免了不同域下复杂的符号转化；其次引入了能够衡量校验关系成立大小的平均校验符合度概念，然后基于其统计特性以及极大极小判决准则，遍历可能的码长以及对应的m级本原多项式，进行初始码根校验匹配，从而完成码长以及本原多项式识别；最后利用识别出的码长以及本原多项式，构建本原多项式下GF(2^m)，进行连续码根匹配判决，最终完成码生成多项式识别。仿真结果表明：推导的平均校验符合度统计特性与实际情况一致，算法能在低信噪比下有效完成参数识别；同时该算法具有较好的低信噪比适应能力，在信噪比为6 dB条件下，工程中常见的RS码识别率均能达到90%以上。与现有算法相比，该文算法性能明显好于硬判决算法，且比传统算法提升1 dB以上性能。

关键词：RS码；软判决；平均校验符合度；极大极小准则；码根匹配

中图分类号：TN911.7 **文献标识码**：A **文章编号**：1009-5896(2020)09-2150-08

DOI: 10.11999/JEIT190690

Blind Recognition of RS Codes Based on Soft Decision

WU Zhaojun[①] ZHANG Limin[①] ZHONG Zhaogen[②] LIU Chuanhui[①]

[①](*Department of Information Fusion*, *Naval Aviation University*, *Yantai* 264001, *China*)

[②](*School of Aviation Basis*, *Naval Aviation University*, *Yantai* 264001, *China*)

Abstract: To solve the problem that the existing algorithms for recognition of RS codes need to transform the code characters among different domains and poor performance, a new algorithm based on soft decision is proposed. Firstly, starting from the definition of RS codes, the equivalent conversion mode of the check relation of RS code from GF (2^m) to GF (2) is given, which avoids the complex symbol transformation in different domains. Secondly, the average check conformity which can measure the validity of the check relationship is introduced and based on its statistical characteristics and minimax decision criteria, the possible code length and corresponding m-level primitive polynomials are traversed to match the initial code root, as the results, the code length and primitive polynomial are recognized. Finally, under the identified code length and the primitive polynomial, the GF (2^m) is constructed, and the continuous code root matching decision is made, then the generation polynomial is recognized. The simulation results show that the derived statistical characteristics of the average check conformity are consistent with the actual situation, and the proposed algorithm can effectively recognize parameter under low Signal-to-Noise Ratio (SNR). At the same time, the proposed algorithm has good adaptability to low SNR. At SNR of 6 dB, the recognition rate of common RS codes in engineering can reach more than 90%. Compared with the existing methods, the performance of this algorithm is better than hard-decision algorithm, besides, it is improved by more than 1 dB compared by traditional algorithms.

Key words: RS code; Soft decision; Average check conformity; Minimax criterion; Code root matching

收稿日期：2019-09-05；改回日期：2020-04-16；网络出版：2020-04-23

*通信作者： 张立民 iamzlm@163.com

基金项目：国家自然科学基金(61179016)；泰山学者工程专项(ts201511020)

Foundation Items: The National Natural Science Foundation of China (61179016), The Taishan Scholar Special Foundation (ts201511020)

1　引言

在认知无线电、通信侦察等领域，信道编码盲识别技术日益成为关注的热点。RS码作为线性分组码中一个非常重要的子集，以其简单的编码译码结构和极强的纠正突发错误的能力，被广泛应用于如DVD存储、卫星通信和数字电视等领域。对于非合作方而言，实现在恶劣信道环境下RS码参数的有效识别，对于后续译码、信源协议分析以及密码的破译具有重要的现实意义[1–3]。

对于RS码的识别，绝大部分算法都是基于扩域中符号序列进行识别，主要的算法有：欧几里得辗转相除法[4]、有限域中高斯消元法[5]、基于GFFT识别算法[6]以及码根检测识别算法[7]。文献[4]利用辗转相除方法实现RS码码长与生成多项式识别，该方法虽然复杂度较低，但是不具有容错性；文献[5]提出了基于伽罗瓦域中高斯消元的识别方法，该方法在码长较短情况下具有一定的实用性，但是随着码长增加，算法复杂度会急剧增加，同时容错性能较差；文献[8–10]从减少复杂度出发，将RS码等效为二进制准循环码，其计算复杂度要小于文献[5]方法，但是仍然避免不了容错性差的缺点；文献[11,12]从提高容错性能出发，提出基于GFFT的识别算法，虽然算法具有一定的容错性能，但是运算量随着码长会急剧增加；为了兼顾计算复杂度以及容错性能两个方面，文献[13]提出基于部分码根校验匹配的识别方法，该算法在短码长下具有很好的识别性能，但是在长码条件下，实用性不好。由于实际工程中发送的RS码是二进制比特流，故以上算法都需要将码元映射到扩域GF(2^m)中，这无疑增加了算法的复杂度；针对该问题，文献[14]首次提出将RS码码根等价于二元域比特校验序列，将校验关系统一于二元域中。该算法减少了域中符号的转化，计算效率得到了提高，但是等效后的码长会成倍数增加，故算法性能会变差。从现有的RS码识别算法来看，其复杂度高，容错性差的缺点都还需要进一步优化改进。

基于此，本文提出一种直接利用软判决序列完成RS参数识别算法。算法首先给出了RS码校验约束关系从扩域GF(2^m)到GF(2)上的等价转化方式，其次引入了平均校验符合度概念，并详细分析了平均校验符合度统计特性，基于其统计特性以及极大极小判决门限，实现码根检测，最终完成RS码参数的快速识别。所提出的算法将RS码识别问题等效于二元域中校验关系检测问题，避免了以往算法需要在GF(2^m)与GF(2)进行符号转化问题，同时也克服了硬判决序列下，算法容错性能不足的缺点。

2　RS定义及其重要性质

RS码具有极强的纠正突发错误的能力，被广泛应用于数字电视、深空探测等领域，其定义为：

定义1[15]　设$q>2$，在GF(q)上码长为$n=q-1$的BCH码成为RS码。设计距离为$2t+1$的RS码，其生成多项式为

$$g(x)=(x-\alpha^{b})\cdot(x-\alpha^{b+1})\cdots(x-\alpha^{b+2t-1}) \tag{1}$$

其中，α为GF(q)中本原元；通常情况下，b=1，q=2^m。

设待编码的信息序列为$(u_0,u_1,\cdots,u_{k-1})$，则编码后的码字多项式为

$$\begin{aligned}C(x)&=(u_0+u_1\cdot x+\cdots+u_{k-1}\cdot x^{k-1})\cdot g(x)\\&=c_0+c_1\cdot x+\cdots+c_{n-1}\cdot x^{n-1}\end{aligned} \tag{2}$$

其中，$u_i,c_j\in \mathrm{GF}(2^m)\,(0\le i\le k-1,0\le j\le n-1)$，$k=n-2t-1$。

由式(2)可知，RS码码字多项式同样是以域GF(2^m)中元素$\alpha,\alpha^2,\cdots,\alpha^{2t}$作为码根。将元素代入式(2)中正好能够构成码字校验关系即

$$c_0+c_1\cdot\alpha^{i}+\cdots+c_{n-1}\cdot(\alpha^{i})^{n-1}=0 \tag{3}$$

其中，$1\le i\le 2t$。

设RS码码块数目为N，将式(3)变换为矩阵形式，得到

$$\begin{bmatrix}c_{1,0}&c_{1,1}&\cdots&c_{1,n-1}\\c_{2,0}&c_{2,1}&\cdots&c_{2,n-1}\\\vdots&\vdots&\ddots&\vdots\\c_{N,0}&c_{N,1}&\cdots&c_{N,n-1}\end{bmatrix}\cdot\begin{bmatrix}1&1&\cdots&1\\\alpha&\alpha^2&\cdots&\alpha^{2t}\\\alpha^2&\alpha^4&\cdots&(\alpha^{2t})^2\\\vdots&\vdots&\ddots&\vdots\\\alpha^{n-1}&(\alpha^2)^{n-1}&\cdots&(\alpha^{2t})^{n-1}\end{bmatrix}=\boldsymbol{0} \tag{4}$$

其中，$c_{i,j}\in \mathrm{GF}(2^m)(1\le i\le N,0\le j\le n-1)$；以后不再单独说明，默认编码之间的运算满足有限域中的规则。

式(4)给出了RS码在扩域GF(2^m)中的校验关系，而从域GF(2^m)到GF(2)上的等价转化关系由定理1给出。

定理1[14]　若RS码中码组在GF(2^m)中满足式(4)校验约束关系，则这种校验约束关系可以等价转化到GF(2)中的校验关系。设GF(2^m)域中的基为$1,\alpha,\alpha^2,\cdots,\alpha^{m-1}$，则转化方式为：式(4)中$c_{i,j}\,(1\le i\le N,0\le j\le n-1)$由其基下的坐标替换，$(\alpha^{l})^{j}\,(1\le l\le 2t,0\le j\le n-1)$由$m\times m$的方阵替换，

其中方阵中第k行由元素$\left(\alpha^l\right)^j\cdot\alpha^{k-1}\,(1\le k\le m)$在基下的坐标构成。

定理1直接给出了RS码校验关系从GF(2^m)到GF(2)的转化方法。由定理1，可以直接利用截获的序列，实现RS码的识别，而不需要将序列进行符号转换。

3 RS码参数识别模型建立

3.1 基于平均校验符合度的RS码识别

由定理1可知，RS码在GF(2^m)上的校验关系可以等价于二元域中的校验关系，不妨按照定理1方式将GF(2^m)上的校验关系进行转化，得到

$$\begin{bmatrix} \boldsymbol{c}_{1,0} & \boldsymbol{c}_{1,1} & \cdots & \boldsymbol{c}_{1,n-1} \\ \boldsymbol{c}_{2,0} & \boldsymbol{c}_{2,1} & \cdots & \boldsymbol{c}_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{c}_{N,0} & \boldsymbol{c}_{N,1} & \cdots & \boldsymbol{c}_{N,n-1} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{h}_{1,0} & \boldsymbol{h}_{2,0} & \cdots & \boldsymbol{h}_{2t,0} \\ \boldsymbol{h}_{1,1} & \boldsymbol{h}_{2,1} & \cdots & \boldsymbol{h}_{2t,1} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{h}_{1,n-1} & \boldsymbol{h}_{2,n-1} & \cdots & \boldsymbol{h}_{2t,n-1} \end{bmatrix} = \boldsymbol{0} \tag{5}$$

其中，行向量$\boldsymbol{c}_{i,j}=\left[c_0^{i,j},c_2^{i,j},\cdots,c_{m-1}^{i,j}\right]\,(1\le i\le N,\,0\le j\le n-1)$，由基下坐标决定；方阵$\boldsymbol{h}_{l,j}\,(1\le l\le 2t,0\le j\le n-1)$的构建方式由定理1给出，即

$$\boldsymbol{h}_{l,j}=\begin{bmatrix} h_{0,0}^{l,j} & h_{0,1}^{l,j} & \cdots & h_{0,m-1}^{l,j} \\ h_{1,0}^{l,j} & h_{1,1}^{l,j} & \cdots & h_{1,m-1}^{l,j} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m-1,0}^{l,j} & h_{m-1,1}^{l,j} & \cdots & h_{m-1,m-1}^{l,j} \end{bmatrix} \tag{6}$$

此时原始编码序列矩阵由$N\times n$大小转化为$N\times n\cdot m$的二进制序列矩阵，校验矩阵由$n\times 2t$转化为$n\cdot m\times 2t\cdot m$。为了直接利用软判决序列完成参数的识别，首先引入校验符合度概念[16,17]，用以衡量编码约束关系成立可能性大小，为了方便说明，考虑将式(5)中某一二元域中的校验关系单列出来研究，即

$$\sum_{j=0}^{n-1}\sum_{k=0}^{m-1}c_k^{i,j}\cdot h_{k,r}^{l,j}=0 \tag{7}$$

其中，$1\le i\le N,0\le r\le m-1,1\le l\le 2t$。

设来源于信道的软判决码元为$y_k^{i,j}$对应于编码码元为$c_k^{i,j}$，定义在截获软判决$y_k^{i,j}$条件下，码元$c_k^{i,j}$取值为1的条件概率为$P\left(c_k^{i,j}|y_k^{i,j}\right)$，则校验符合度定义为

$$F_r^{i,l}=\prod_{j=0}^{n-1}\prod_{k=1}^{m}\left(1-2P\left(c_k^{i,j}|y_k^{i,j}\right)\cdot h_{k,r}^{l,j}\right) \tag{8}$$

从式(8)定义来看，当校验关系成立时，$F_r^{i,l}$一定为正值；而不成立时$F_r^{i,l}$一定为负值，上面仅仅考虑了在一个码子校验关系的情况，如果将所有的校验关系考虑进来，便得到平均校验符合度的定义为

$$\bar{F}_l=\frac{1}{N\cdot m}\sum_{i=1}^{N}\sum_{r=0}^{m-1}F_r^{i,l} \tag{9}$$

当扩域中的元素α^l为码根时，由于校验关系成立，此时$\bar{F}_l$将远远大于0；而非码根时，由于校验约束关系成立随机，经过平均后$\bar{F}_l$将趋近于0，这样就可判断α^l是否为码根。在式(8)中还需要解决条件概率$P\left(c_k^{i,j}|y_k^{i,j}\right)$计算问题，下面推导其计算方法。

假定信号的调制方式为二进制相移键控(Binary Phase Shift Key, BPSK)，信号幅度为A(通常取值为1)，此时码元0被映射为-A，而1被映射为A；设信道噪声是方差为σ^2，均值为0的高斯白噪声，此时信噪比定义为

$$\mathrm{SNR}=10\lg\left(\frac{A^2}{2\sigma^2}\right) \tag{10}$$

在码元$c=0$与$c=1$条件下的概率密度函数为

$$p\left(y|c=0\right)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{\frac{-(y+A)}{2\sigma^2}} \tag{11}$$

$$p\left(y|c=1\right)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{\frac{-(y-A)}{2\sigma^2}} \tag{12}$$

由贝叶斯公式可知

$$P\left(c_k^{i,j}|y_k^{i,j}\right)=\frac{p\left(y_k^{i,j}|c_k^{i,j}=1\right)\cdot P\left(c_k^{i,j}=1\right)}{p\left(y_k^{i,j}\right)} \tag{13}$$

由于信源在编码之前会经过扰码处理，其0, 1序列平衡，故$P\left(c_k^{i,j}=1\right)$=$P\left(c_k^{i,j}=0\right)$，利用全概率公式将分母展开，化简后得到

$$P\left(c_k^{i,j}|y_k^{i,j}\right)=\frac{\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}}{\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}+1} \tag{14}$$

将式(14)代入式(9)得到

$$\bar{F}_l=\frac{1}{N\cdot m}\sum_{i=1}^{N}\sum_{r=0}^{m-1}\prod_{j=0}^{n-1}\prod_{k=0}^{m}\left(1-2\frac{\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}}{\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}+1}h_{k,r}^{l,j}\right) \tag{15}$$

记集合$\phi_{l,r}=\left\{(j,k)\,|h_{k,r}^{l,j}=1\right\}$，此时$\bar{F}_l$进一步转化为

$$\bar{F}_l=\frac{1}{N\cdot m}\sum_{i=1}^{N}\sum_{r=0}^{m-1}\prod_{(j,k)\in\phi_{l,r}}\frac{1-\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}}{1+\mathrm{e}^{2A\cdot y_k^{i,j}/\sigma^2}} \tag{16}$$

3.2 码根判决门限的求解

首先考察$F_r^{i,l}$的统计特性。对于集合$\phi_{l,r}$，其下

标所对应的校验矩阵中元素集合设为$\varphi_{l,r}=\left\{h_{k,r}^{l,j}|\,(j,k)\in\phi_{l.r}\right\}$，此时对应于第$i$个码组，真正参与校验的码元集合为$\psi_i=\left\{c_k^{i,j}|\,(j,k)\in\phi_{l,r}\right\}$，记$W_{l,r}$为集合$\varphi_{l,r}$中1的个数，当遍历的元素$\alpha^l$为码字多项式码根时，由于在GF(2)中模2加校验关系成立，集合ψ_i中元素为1的个数一定为偶数，此时集合ψ_i中码元0,1分布情况总共有

$$V_{l,r,1}=\sum_{i=0}^{\lfloor w_{l,r}/2\rfloor}\mathrm{C}_{w_{l,r}}^{2i}=2^{w_{l,r}-1}\tag{17}$$

其中，符号$\lfloor\cdot\rfloor$表示向下取整，C_n^m表示组合数运算。

按照均值与方差的定义，将每一种情况进行计算，然后再将每一种情况下的均值与方差求取平均即可，从而得到

$$\begin{aligned}u_{l,r,1}=&\sum_{j=0}^{\lfloor w_{l,r}/2\rfloor}\frac{\mathrm{C}_{w,l}^{2\cdot j}}{2^{w_{l,r}-1}}\\&\cdot\left(\int_{-\infty}^{\infty}\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\cdot p\left(x|c=1\right)\mathrm{d}x\right)^{2j}\\&\cdot\left(\int_{-\infty}^{\infty}\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\cdot p\left(x|c=0\right)\mathrm{d}x\right)^{w_{l,r}-2j}\end{aligned}\tag{18}$$

$$\begin{aligned}\sigma_{l,r,1}^2=&\sum_{j=0}^{\lfloor w_{l,r}/2\rfloor}\frac{\mathrm{C}_{w_{l,r}}^{2j}}{2^{w_{l,r}-1}}\\&\cdot\left(\int_{-\infty}^{\infty}\left(\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\right)^2\cdot p\left(x|c=1\right)\mathrm{d}x\right)^{2j}\\&\cdot\left(\int_{-\infty}^{\infty}\left(\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\right)^2\cdot p\left(x|c=0\right)\mathrm{d}x\right)^{w_{l,r}-2j}\\&-u_{l,r,1}^2\end{aligned}\tag{19}$$

其中，$1\le l\le 2t,0\le r\le m-1$。

对于校验关系不成立的情况，此时集合ψ_i中元素为1的个数奇偶随机，此时集合中0, 1元素分布情况为

$$V_{l,r,0}=\sum_{i=0}^{w_{l,r}}\mathrm{C}_{w_{l,r}}^{i}=2^{w_{l,r}}\tag{20}$$

同样由均值与方差的定义，求取每一种情况下的均值与方差，然后进行统计平均，得到

$$\begin{aligned}u_{l,r,0}=&\sum_{j=0}^{w_{l,r}}\frac{\mathrm{C}_{w,l}^{j}}{2^{w_{l,r}}}\cdot\left(\int_{-\infty}^{\infty}\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\cdot p\left(x|c=1\right)\mathrm{d}x\right)^{j}\\&\cdot\left(\int_{-\infty}^{\infty}\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\cdot p\left(x|c=0\right)\mathrm{d}x\right)^{w_{l,r}}\end{aligned}\tag{21}$$

$$\begin{aligned}\sigma_{l,r,0}^2=&\sum_{j=0}^{w_{l,r}}\frac{\mathrm{C}_{w_{l,r}}^{j}}{2^{w_{l,r}}}\\&\cdot\left(\int_{-\infty}^{\infty}\left(\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\right)^2\cdot p\left(x|c=1\right)\mathrm{d}x\right)^{j}\\&\cdot\left(\int_{-\infty}^{\infty}\left(\frac{1-\mathrm{e}^{-2A\cdot x/\sigma^2}}{1+\mathrm{e}^{-2A\cdot x/\sigma^2}}\right)^2\cdot p\left(x|c=0\right)\mathrm{d}x\right)^{w_{l,r}-j}\\&-u_{l,r,0}^2\end{aligned}\tag{22}$$

由于在不同的r下，$w_{l,r}$值可能不同，此时将r的因素考虑进来，进一步得到：$u_{l,0}=\dfrac{1}{m}\sum_{r=0}^{m-1}u_{l,r,0}$, $\sigma_{l,0}^2=\dfrac{1}{m}\sum_{r=0}^{m-1}\sigma_{l,r,0}^2$, $u_{l,1}=\dfrac{1}{m}\sum_{r=0}^{m-1}u_{l,r,1}$以及$\sigma_{l,1}^2=\dfrac{1}{m}\sum_{r=0}^{m-1}\sigma_{l,r,1}^2$。

对于式(18)、式(19)、式(21)以及式(22)中出现的积分，可能不会出现解析解，此时采用数值积分，除了能够快速完成解算之外，还能够达到很高的精度。

在求得$u_{l,1}$, $u_{l,0}$, $\sigma_{l,1}^2$以及$\sigma_{l,0}^2$之后，会很容易得到平均校验符合$\bar{F}_l$的统计特性，考虑以下两种假设检验。

H_0：元素α^l不是码字多项式中的码根；

H_1：元素α^l是码字多项式中的码根。

设截获的码块数目为N，当N较大时，由中心极限定理可知：$\bar{F}_l$服从高斯分布，令$\bar{\sigma}_{l,0}^2=\sigma_{l,0}^2/N$, $\bar{\sigma}_{l,1}^2=\sigma_{l,1}^2/N$，则在假设条件$\mathrm{H}_0$下，$\bar{F}_l$服从

$$\mathrm{H}_0:\bar{F}_l\sim\mathcal{N}\left(u_{l,0},\bar{\sigma}_{l,0}^2\right)\tag{23}$$

$$\mathrm{H}_1:\bar{F}_l\sim\mathcal{N}\left(u_{l,1},\bar{\sigma}_{l,1}^2\right)\tag{24}$$

设在事件H_0下的判决空间为D_0，事件H_1下的判决空间为D_1。在二元通信系统中，判定正确不付出代价，而判定错误代价为1，为了使极大可能的代价极小化，本文采用极大极小准则来求解判决门限。在极大极小准则条件下，两类错误判决概率必须满足条件为

$$P\left(D_1|\mathrm{H}_0\right)=P\left(D_0|\mathrm{H}_1\right)\tag{25}$$

设判决门限为Λ_l，式(25)变为

$$\int_{\Lambda_l}^{\infty}\frac{1}{\sqrt{2\pi}\bar{\sigma}_{l,0}}\mathrm{e}^{\frac{-\left(x-u_{l,0}\right)^2}{2\bar{\sigma}_{l,0}^2}}\mathrm{d}x=\int_{-\infty}^{\Lambda_l}\frac{1}{\sqrt{2\pi}\bar{\sigma}_{l,1}}\mathrm{e}^{\frac{-\left(x-u_{l,1}\right)^2}{2\bar{\sigma}_{l,1}^2}}\mathrm{d}x\tag{26}$$

求解式(26)，得到码根判决门限为$\Lambda_l=\dfrac{u_{l,1}\cdot\bar{\sigma}_{l,0}+u_{l,0}\cdot\bar{\sigma}_{l,1}}{\bar{\sigma}_{l,0}+\bar{\sigma}_{l,1}}$。

3.3 算法步骤以及复杂度分析

对于RS码的识别，首先要将截获的软判决序列转化为条件概率形式，然后遍历可能的码长，本原多项式以及连续码根数目。由RS码定义可知，RS码具有连续$2t$个码根，若α^{2l-1}是码根，则α^{2l}一定也是码根，所以在码长与多项式识别过程中，可以将元素α^{2l-1}与α^{2l}进行校验匹配，具体的识别步骤如下：

步骤 1　将截获的序列转化为码元的条件概率序列；

步骤 2　设定m初值为3，构造二元等效码字矩阵，同时存储m级内本原多项式；

步骤 3　遍历步骤2中多项式，构造$\mathrm{GF}(2^m)$，构造关于元素α,α^2的二元校验矩阵；

步骤 4　计算判决门限Λ_1以及$\bar{F}_1$，若$\bar{F}_1 \geq \Lambda_1$，则识别出码长为2^m-1以及本原多项式，否则遍历下一个本原多项式，直到出现$\bar{F}_1 \geq \Lambda_1$，若遍历结束未出现，则m=m+1，跳转步骤3，直到$m>8$；

步骤 5　完成码长以及本原多项式识别后，构建$\mathrm{GF}(2^m)$，赋初值$l=2$，构造关于元素α^{2l-1}，α^{2l}的二元校验矩阵，同时计算门限Λ_l以及$\bar{F}_l$，若$\bar{F}_l \geq \Lambda_l$，则$l=l+1$，重复步骤5，直到出现$\bar{F}_l < \Lambda_l$，识别出RS码纠错能力为$l-1$，完成生成多项式识别。

从上述参数识别步骤来看，算法的计算量主要来源于平均校验符合度的计算上。在某一本原多项式下，设由元素α构建二进制校验矩阵中第r列的码重为$w_{l,r}(1 \leq r \leq m)$，则对于一个码组而言，在计算过程中，需要进行$w_{l,r}$次指数运算，$2w_{l,r}$次加减法运算，$w_{l,r}$次乘法运算以及$w_{l,r}$次的除法运算，为了方便量化，将1次指数运算等价于2次乘法运算，将一次门限计算等价于8次乘法运算。当截获的码组数目为N，m级下的所有本原多项式数目为$\gamma(2^m-1)/m$(其中，$\gamma(\cdot)$为欧拉函数)，在最不利情况下，将3～8级本原多项式遍历完，则码长识别最大计算量为：$(4N+8)\cdot\sum_{m=3}^{8}\sum_{r=1}^{m}\gamma(2^m-1)/m\cdot w_{1,r}$次乘法以及$2N\cdot\sum_{m=3}^{8}\sum_{r=1}^{m}\gamma(2^m-1)/m\cdot w_{1,r}$次乘法；设RS码纠错能力为$t$，则生成多项式识别最大计算复杂度为：$(4N+8)\cdot\sum_{l=2}^{2t}\sum_{r=1}^{m}w_{l,r}$次乘法以及$2N\cdot\sum_{l=2}^{2t}\sum_{r=1}^{m}w_{l,r}$加法。

4 仿真验证

4.1 校验符合度统计特性验证

本节主要验证在H_0与H_1条件下，推导的校验符合度统计特性是否与实际情况相符。仿真设定码块数目为10000，设定RS码编码器种类为3种，具体参数如表1所示。

其中，H_1条件下测试元素为生成多项式码根，而H_0条件下的测试元素为非码根。在两种假设条件下，就校验符合度的均值与方差进行验证，结果如图1所示。

从图1的结果来看，在两种假设条件下，推导结果与实际情况几乎重合，这说明理论推导是正确的。从图1(a)可知，当元素不是码根时，其均值一定为0；同时随着码长的增加，两种假设条件下均值曲线交点向右移动；从图1(b)来看，两种假设条件下曲线重合点同样随着码长的增加而右移，由此可见，码长对算法的性能会有较大的影响。

4.2 算法容错性能验证

仿真1：码长对算法性能影响。

仿真设定RS码编码类型有5种，对应码长分别为15, 31, 63, 127以及255，每一种RS码编码类型对应的纠错能力为2，具体参数如表2所示。

仿真中设定截获的码块数目为1000，统计在不同信噪比以及码长情况下，RS码正确识别率，结果如图2所示。

从图2结果来看，码长对于算法识别性能具有较大的影响，随着码长的增加，算法性能逐渐变差，主要原因在于码长增加后，需要遍历的本原多项式会增加，这时会出现较大的虚警与漏警概率。

仿真2：码块数目对算法性能影响。

仿真设定RS码码长为127，本原多项式为x^7+x+1，其生成多项式为$\alpha^6x^4+\alpha^{23}x^3+\alpha^{69}x^2+\alpha^{18}x+\alpha^{123}$，对应于纠错能力为2；设定截获的码块数目$N$为500, 1000, 1500, 2000以及2500，统计在不同信噪比下参数识别率如图3所示。

从图3来看，随着截获码块数目的增加，算法性能在不断提高，故增加码块数目可以有效改善算法性能。当码长比较长时，可以通过增加码块数目可以提高算法的容错性。

表 1　RS码编码器参数设定

m	码长	本原多项式	生成多项式	H_1下测试元素	H_0下测试元素
4	15	x^4+x+1	$\alpha^3x^4+\alpha^{11}x^3+\alpha^{14}x^2+\alpha^6x+\alpha^8$	α^2	α^5
5	31	x^5+x^2+1	$\alpha^4x^2+\alpha^{20}x+\alpha$	α	α^3
6	63	x^6+x+1	$\alpha^5x^4+\alpha^{19}x^3+\alpha^{36}x^2+\alpha^{14}x+\alpha^{58}$	α^3	α^6

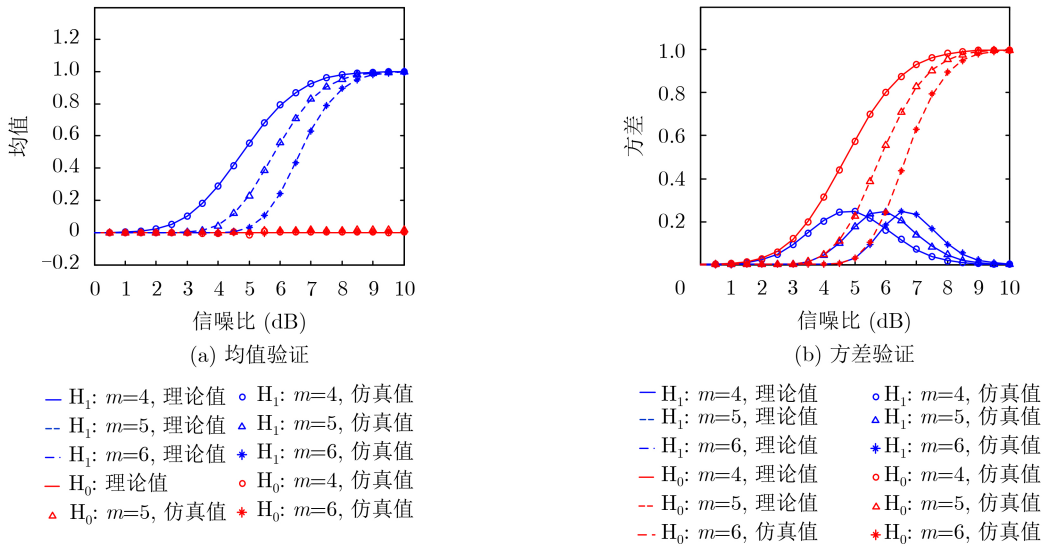

图 1 校验符合度统计特性对比

表 2　不同码长的RS码编码器参数

m	码长	本原多项式	生成多项式	纠错能力
4	15	x^4+x+1	$\alpha^3x^4+\alpha^{11}x^3+\alpha^{14}x^2+\alpha^6x+\alpha^8$	2
5	31	x^5+x^2+1	$\alpha^4x^4+\alpha^{23}x^3+\alpha^{13}x^2+\alpha^{18}x+\alpha^{25}$	2
6	63	x^6+x+1	$\alpha^5x^4+\alpha^{19}x^3+\alpha^{36}x^2+\alpha^{14}x+\alpha^{58}$	2
7	127	x^7+x+1	$\alpha^6x^4+\alpha^{23}x^3+\alpha^{69}x^2+\alpha^{18}x+\alpha^{123}$	2
8	255	$x^8+x^4+x^3+x^2+1$	$\alpha^7x^4+\alpha^{78}x^3+\alpha^{248}x^2+\alpha^{73}x+\alpha^{252}$	2

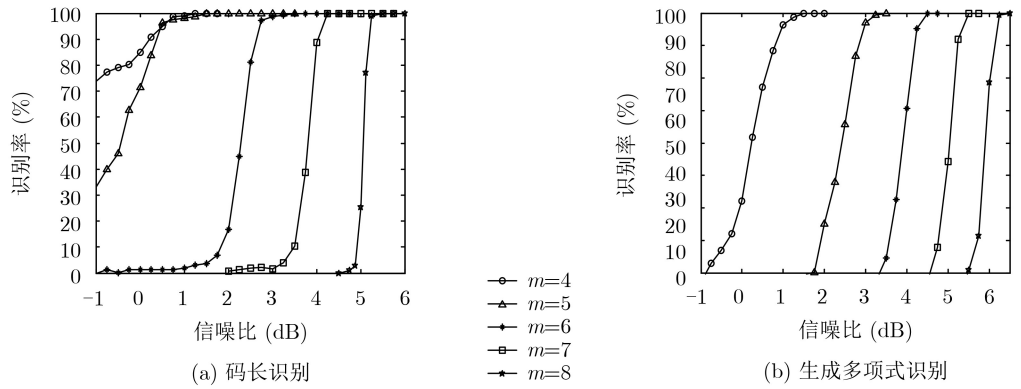

图 2 码长对算法识别性能影响

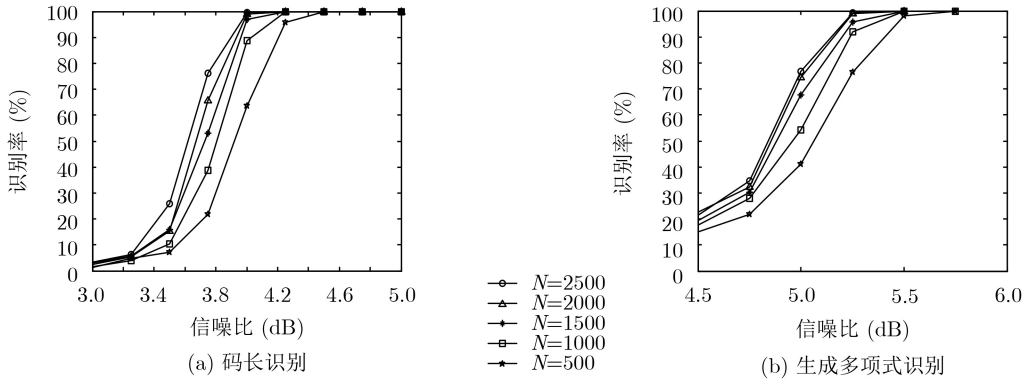

图 3 码块数目对算法影响

5 与其它算法对比

与本文算法进行性能比较的分别是：基于二元域等效的硬判决识别算法[14]、基于GFFT识别算法[11]、文献[12]算法以及矩阵分析识别算法[5]。对比中采用的RS码编码器为码长为255，能够纠正8个符号错误的RS(255, 239)，设定截获的码块数目为2000，统计每一种算法在不同信噪比下参数的正确识别率，结果如图4所示。

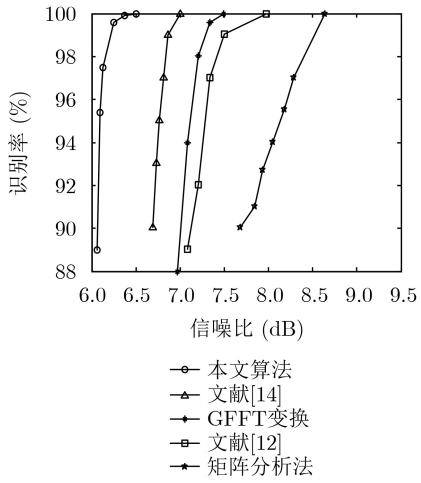

图 4 5种算法对比

从图4来看，本文算法的容错性能要好于其它4种算法。由于在识别参数过程中，矩阵分析方法会造成误码的扩散，所以在5种算法中性能最差；其次文献[12]通过采用GrÖber基方法在一定程度上减小了GFFT算法的运算量，但是其识别性能却在一定的程度上减弱了；文献[14]将RS码等价于二元域中，利用硬判决序列完成码根校验匹配，虽然在现有的硬判决分析方法中性能是最好的，但是却无法利用到信道的特性，而本文算法直接利用截获于信道的软判决序列，采用平均校验符合度对码根进行校验匹配，相比较于硬判决方法，其低信噪比适应能力将会更强。从结果来看，本文提出的算法相比较于文献[14]硬判决方法，性能提升0.5 dB以上，与基于GFFT识别算法相比，提升将近1 dB，与矩阵分析相比，提升性能将近2 dB，故本文算法具有更好的容错性。

6 结束语

本文首先从RS码定义出发，给出了符号校验关系从GF(2^m)到GF(2)的等价转化方法；其次在校验匹配中，引入了平均校验符合度概念，基于其统计特性以及极大极小错误判决准则，完成了在低信噪比下生成多项式码根的检测，从而实现RS码的识别。与以往算法相比，本文算法避免了码元符号在不同域之间的转化，其计算效率更高；同时由于直接采用了软判决序列，其低信噪比适应能力更强。综合来看本文算法的更具工程实用性。

参 考 文 献

[1] 解辉, 黄知涛, 王丰华. 信道编码盲识别技术研究进展[J]. 电子学报, 2013, 41(6): 1166–1176. doi: 10.3969/j.issn.0372-2112.2013.06.019.
XIE Hui, HUANG Zhitao, and WANG Fenghua. Research progress of blind recognition of channel coding[J]. *Acta Electronica Sinica*, 2013, 41(6): 1166–1176. doi: 10.3969/j.issn.0372-2112.2013.06.019.

[2] HUANG Li, CHEN Wengu, CHEN Enhong, *et al*. Blind recognition of k/n rate convolutional encoders from noisy observation[J]. *Journal of Systems Engineering and Electronics*, 2017, 28(2): 235–243. doi: 10.21629/JSEE.2017.02.04.

[3] 于沛东, 彭华, 巩克现, 等. 基于最小二乘代价函数的卷积码盲识别方法[J]. 电子学报, 2018, 46(7): 1545–1552. doi: 10.3969/j.issn.0372-2112.2018.07.002.
YU Peidong, PENG Hua, GONG Kexian, *et al*. Blind recognition of convolutional codes based on least-Square cost-function[J]. *Acta Electronica Sinica*, 2018, 46(7): 1545–1552. doi: 10.3969/j.issn.0372-2112.2018.07.002.

[4] 戚林, 郝士琦, 李今山. 基于有限域欧几里德算法的RS码识别[J]. 探测与控制学报, 2011, 33(2): 63–67. doi: 10.3969/j.issn.1008-1194.2011.02.015.
QI Lin, HAO Shiqi, and LI Jinshan. Recognition method of RS codes based on euclidean algorithm in Galois field[J]. *Journal of Detection & Control*, 2011, 33(2): 63–67. doi: 10.3969/j.issn.1008-1194.2011.02.015.

[5] 李灿, 张天骐, 刘瑜. 基于伽罗华域高斯列消元法的RS码盲识别[J]. 电讯技术, 2014, 54(7): 926–931.
LI Can, ZHANG Tianqi, and LIU Yu. Blind recognition of RS codes based on Galois field columns Gaussian elimination[J]. *Telecommunication Engineering*, 2014, 54(7): 926–931.

[6] 包昕, 陆佩忠, 游凌. 基于伽罗华域傅里叶变换的RS码识别方法[J]. 电子科技大学学报, 2016, 45(1): 30–35. doi: 10.3969/j.issn.1001-0548.2016.01.004.
BAO Xin, LU Peizhong, and YOU Ling. Recognition of RS coding based on Galois field Fourier transform[J]. *Journal of University of Electronic Science and Technology of China*, 2016, 45(1): 30–35. doi: 10.3969/j.issn.1001-0548.2016.01.004.

[7] 张立民, 刘杰, 孙永威, 等. RS码编码参数的盲识别[J]. 电讯技术, 2017, 57(6): 650–655. doi: 10.3969/j.issn.1001-893x.2017.06.006.
ZHANG Limin, LIU Jie, SUN Yongwei, *et al*. Blind parameter recognition of RS codes[J]. *Telecommunication*

Engineering, 2017, 57(6): 650–655. doi: 10.3969/j.issn.1001-893x.2017.06.006.

[8] 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. doi: 10.3724/SP.J.1146.2012.00434.
GAN Lu and ZHOU Pan. Fast blind recognition method of RS codes based on Chinese remainder theorem decomposition[J]. *Journal of Electronics & Information Technology*, 2012, 34(12): 2837–2842. doi: 10.3724/SP.J.1146.2012.00434.

[9] LI Tong, MIAO Chenglin, and LÜ Jun. An improved algorithm of RS codes blind recognition[J]. *Applied Mechanics and Materials*, 2014, 603-605: 2308–2312.

[10] 杨烁. CPM信号非相干解调与RS码盲识别技术研究[D]. [硕士论文], 哈尔滨工程大学, 2018: 23–54.
YANG Shuo. Research on non-coherent demodulation of continuous phase modulation signal and Reed-Solomon code blind recognition[D]. [Master dissertation], Harbin Engineering University, 2018: 23–54.

[11] LIU Pengtao, PAN Zhipeng, and LEI Jing. Parameter identification of Reed-Solomon codes based on probability statistics and Galois field Fourier transform[J]. *IEEE Access*, 2019, 7: 33619–33630. doi: 10.1109/ACCESS.2019.2904718.

[12] LU Ouxin, GAN Lu, and LIAO Hongshu. Blind reconstruction of RS codes[J]. *Asian Journal of Applied Sciences*, 2015, 8(1): 37–45. doi: 10.3923/ajaps.2015.37.45.

[13] 王平, 曾伟涛, 陈健, 等. 一种利用本原元的快速RS码盲识别算法[J]. 西安电子科技大学学报: 自然科学版, 2013, 40(1): 105–110, 168.
WANG Ping, ZENG Weitao, CHEN Jian, *et al*. Fast blind recognition algorithm for RS codes by primitive element[J]. *Journal of Xidian University*: *Natural Science*, 2013, 40(1): 105–110, 168.

[14] 刘杰, 张立民, 钟兆根. 基于二元域等效的RS码编码参数盲识别[J]. 电子学报, 2018, 46(12): 2888–2895. doi: 10.3969/j.issn.0372-2112.2018.12.010.
LIU Jie, ZHANG Limin, and ZHONG Zhaogen. Blind parameter identification of RS code based on binary field equivalence[J]. *Acta Electronica Sinica*, 2018, 46(12): 2888–2895. doi: 10.3969/j.issn.0372-2112.2018.12.010.

[15] 王新梅, 肖国镇. 纠错码-原理与方法[M]. 西安: 西安电子科技大学出版社, 2001: 145–240.
WANG Xinmei and XIAO Guozhen. Error Correcting Code Theory and Method[M]. Xi'an: Xidian University Press, 2001: 145–240.

[16] 张立民, 吴昭军, 钟兆根. 基于校验方程符合度下的Turbo码编码器盲识别[J]. 电子与信息学报, 2017, 39(9): 2155–2161. doi: 10.11999/JEIT161391.
ZHANG Limin, WU Zhaojun, and ZHONG Zhaogen. Blind recognition of turbo code encoder based on conformity of parity-check equation[J]. *Journal of Electronics & Information Technology*, 2017, 39(9): 2155–2161. doi: 10.11999/JEIT161391.

[17] 陈泽亮, 李静, 彭华, 等. 利用Gibbs采样进行优化的Turbo码交织器识别[J]. 电子学报, 2018, 46(1): 15–23. doi: 10.3969/j.issn.0372-2112.2018.01.003.
CHEN Zeliang, LI Jing, PENG Hua, *et al*. An optimization method using Gibbs sampler for turbo-code Interleaver identification[J]. *Acta Electronica Sinica*, 2018, 46(1): 15–23. doi: 10.3969/j.issn.0372-2112.2018.01.003.

吴昭军：男，1992年生，博士生，研究方向为信道编码识别.
张立民：男，1966年生，教授，博士生导师，研究方向为卫星信号处理及应用.
钟兆根：男，1984年生，博士，讲师，研究方向为扩频信号处理.
刘传辉：男，1984年生，博士，讲师，研究方向为航空通信系统与网络.

责任编辑：马秀强