RS码的盲识别方法

刘 健[1]，谢 锘[1,2]，周希元[1,2]

(1. 西安电子科技大学ISN国家重点实验室 西安 710071;

2. 中国电子科技集团公司第五十四研究所 石家庄 050081)

【摘要】针对信道编码的盲识别问题，首次提出了RS码的盲识别方法。先针对无误码的情况，通过基于矩阵行向量化简(RREF)的方法估计RS码的码长、本原多项式和生成多项式等参数；继而，针对有误码的情况，通过基于RREF、容错矩阵分解(FTMD)和伽罗华域的傅里叶变换(GFFT)方法估计码长、本原多项式和生成多项式等参数，这是一个全新的研究课题，在智能通信、信息截获、密码分析等领域有重要的应用。仿真实验表明文中提出的方法在误码率为10^{-3}的情况下，对于RS码的识别概率高于85%。

关 键 词 误码率； 容错矩阵； 信道编码； 伽罗华域傅里叶变换； RS码

中图分类号 TN97 **文献标识码** A doi.10.3969/j.issn.1001-0548.2009.03.011

Blind Recognition Method of RS Coding

LIU Jian[1], XIE Nuo[1,2], and ZHOU Xi-yuan[1,2]

(1. National Key Lab of Integrated Services Networks , Xidian University Xi' án 710071;

2. The 54th Research Institute of CETC Shijiazhuang 050081)

Abstract In order to solve the problem of the blind recognition of channel coding, some methods of blind recognition of Reed-Solomon (RS) coding are proposed. In the case of codes without errors, the coded length, primitive polynomial, and generator polynomial are obtained based on reduced row echelon form of the matrix (RREF). In the case of codes with errors, the coded length, primitive polynomial, and generator polynomial are obtained based on RREF, fault-tolerant matrix decomposing (FTMD) and Galois Field Fourier Transform (GFFT). The simulation experiments show that the recognition probability of the proposed methods is above 85% at a bit error rate (BER) of 10^{-3}.

Key words bit error rate blind recognition; channel coding; GFFT; RS code

信道编码的盲识别在信息截获、信息对抗以及智能通信等领域有重要的应用，但该方面的研究鲜见报道。

信道编码主要包括卷积码和分组码两大类。目前，信道编码的盲识别技术研究主要涉及卷积码的盲识别方面，如文献[1-2]提出的删除卷积码的盲识别方法；文献[3]提出的基于快速合冲算法的$(2,1,m)$类卷积码盲识别算法；文献[4]提出的基于欧几里德算法的$(2,1,m)$类卷积码盲识别算法等。

分组码是另一类重要的信道编码，现已广泛应用于通信系统，目前的研究主要集中在其编译码算法[5]上。由于其每个分组之间相互独立，并不存在卷积码的“相关性”，因此，盲识别的难度更大，至今未见文献报道。RS 码是分组码中较为重要的一类，主要应用于现代数字通信和数据存储系统中。本文根据 RS 编码性质，在给出无误码情况下的盲识别方法后，研究了有误码情况下的盲识别方法，并对识别性能进行了理论分析和仿真验证。

1 问题描述

设C_p是一个 RS 码序列，它的盲识别问题如下：由C_p确定源码C的分组码长、本原多项式和生成多项式。

下面给出本文需要引用的一些概念：

定义 1[6] 当$f(x)=p(x)$是m次不可约多项式时，同余类环$F_p[x]/(p(x))$是一个含有p^m个元素的有限域，称为$F_p[x] \bmod p(x)$的同余类域，简记为$\mathrm{GF}(p^m)$。

定义 2[6] 给定任一有限域$\mathrm{GF}(p)$(p是素数或素数的幂)、码长$n \geqslant 3$和$3 \leqslant \delta \leqslant n$，域$\mathrm{GF}(p)$上的

收稿日期：2008－12－21；修回日期：2009－03－28

基金项目：国家自然科学基金(60572147)

作者简介：刘 健(1983－)，男，博士生，主要从事信息截获、信息对抗方面的研究.

一个 (n,k) BCH 码是由下式生成的循环码：

$$g(x)=\mathrm{LCM}[m_{\beta^{m_0}}(x),m_{\beta^{m_0+1}}(x),\cdots,m_{\beta^{m_0+\delta-2}}(x)] \quad (1)$$

式中 β 是扩域 GF(p^m) 上的 n 级元素； $m_{\beta^i}(x)$ $(m_0\leqslant i\leqslant m_0+\delta-2)$ 是元素 β^i 的最小多项式；LCM 表示取最小公倍式。如果 β 是扩域 GF(p^m) 上的本原元素，这类 BCH 码称为本原 BCH 码。码长为 $n=q-1$ 的本原 BCH 码称为 RS 码。

2 无误码RS码的盲识别

当截获到的码序列无误码时，利用编码线性空间映射特性，通过矩阵行向量化简来识别分组码长 n；利用编码所在域的构成特性，通过引理 2 识别出本原多项式；根据本原多项式，将 RREF 的结果从 GF(2) 映射到 GF(2^m) 来识别生成多项式。

2.1 分组码长识别

引理 1[6] 设 $\boldsymbol{V}$ 是由 GF(2^m) 上的 $k\times n$ 阶生成矩阵 $\boldsymbol{G}$ 所生成的 RS 码，则 $\boldsymbol{V}$ 的向量表示 (mn,mk) 是 GF(2) 上的线性分组码。

由引理 1 可将 GF(2^m) 上的码字映射到GF(2)上。由定义 2 可知，在 GF(p) 上RS码的码长为n=q–1，将其映射到 GF(2) 域上，其 GF(2) 域上的码长为：

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

式中 $m\geqslant 2$。

定理 1 任一 (n,k) 线性分组码的码分组所构成的 $n\times l$ 矩阵 $\boldsymbol{A}$ ($l\geqslant k$)，其秩 gfrank($\boldsymbol{A}$) $\leqslant k$。

证明：由线性分组码的定义 $\boldsymbol{C}=m\boldsymbol{G}$，得 $\boldsymbol{C}$ 为信息序列 m 的一线性变换，由于其生成矩阵 $\boldsymbol{G}$ 的秩为 k。接收码序列 $\boldsymbol{C}$ 即为生成矩阵 $\boldsymbol{G}$ 映射的一个空间 R^n，而 $\boldsymbol{G}$ 即为 R^n 的 k 维的基。当 l 逐渐增大，gfrank($\boldsymbol{A}$) 将逐渐趋近于 k。

由定理1可知，对于任一 GF(2) 上的码字，当分组的起始位和分组长度判断正确之后，就可以将 $n\times l$ 矩阵 $\boldsymbol{A}$ 通过RREF化简成为 $n\times(k-a)$ 的矩阵 $\boldsymbol{A}'$。其中 n 即为分组长度，k 为信息长，a 为一整数变量且 $0\leqslant a\leqslant k-1$。随着 l 逐渐增大，a 将趋近于0。借助帧同步先验知识可以成功地找到分组的起始位，根据引理1，通过RREF将 m 的数值遍历便可以识别出其 GF(2) 域上的码长 n' 和信息长 k'。

2.2 域本原多项式识别

引理 2[6] GF(2^m) 上的 (n,k) RS 码对应于 GF(2) 上的 (mn,mk) 循环码，该二进制循环码的标准生成矩阵为：

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I} & 0 & \cdots & 0 & \boldsymbol{P}_{11} & \boldsymbol{P}_{12} & \cdots & \boldsymbol{P}_{1n-k}\\ 0 & \boldsymbol{I} & \cdots & 0 & \boldsymbol{P}_{21} & \boldsymbol{P}_{22} & \cdots & \boldsymbol{P}_{2n-k}\\ \vdots & \vdots & & \vdots & \vdots & \vdots & \cdots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{I} & \boldsymbol{P}_{k1} & \boldsymbol{P}_{k2} & \cdots & \boldsymbol{P}_{kn-k}\end{bmatrix} \quad (3)$$

式中 $\boldsymbol{I}$ 是 $m\times m$ 阶单位矩阵；每个 $\boldsymbol{P}_{ij}$ $(i=1,2,\cdots,k;\ j=1,2,\cdots,n-k)$ 是一个 $m\times m$ 阶矩阵块：

$$\boldsymbol{P}_{ij}=\begin{bmatrix}a_{11}^{(ij)} & a_{12}^{(ij)} & \cdots & a_{1m}^{(ij)}\\ a_{21}^{(ij)} & a_{22}^{(ij)} & \cdots & a_{2m}^{(ij)}\\ \vdots & \vdots & \cdots & \vdots\\ a_{m1}^{(ij)} & a_{m2}^{(ij)} & \cdots & a_{mm}^{(ij)}\end{bmatrix} \quad (4)$$

式中 $\boldsymbol{P}_{ij}$ 的相邻两行移位相加如不为零向量，则和向量中的元素即为本原多项式的系数。

当已知码长 n' 之后，根据式(2)，可以准确判断出 m 的值，并由引理 2 求出本原多项式 $m(x)$。

2.3 生成多项式识别

根据本原多项式 $m(x)$ 将 RREF 化简后的矩阵 $\boldsymbol{A}'$ 由 GF(2) 恢复到 GF(2^m)，$\boldsymbol{A}'$ 的最后一行就是该 RS 码所对应生成的多项式系数。

3 有误码RS码盲识别

当截获的信号存在噪声时，可以根据信号的调制样式、信噪比及解调器的损耗大致估计数据解调后的误码率，再根据下述的识别方法选择最佳方法进行编码参数的盲识别。

由于随码长的不同，有误码 RS 码盲识别的性能和计算复杂度有较大的变化，因此，下面分短码长和长码长两种情况进行讨论。

3.1 短码长RS码识别

3.1.1 码长

短码长 RS 码的码长识别方法仍按照无误码的 RREF 算法进行矩阵化简，矩阵列数即为码长。

3.1.2 本原多项式

本原多项式的识别视误码率的高低采用不同的识别方法。

(1) 低误码率情况。

在低误码率情况下，采用基于容错矩阵分解的方法来求解本原多项式。

定理 2 一个 GF(2^m) 上的 (n,k) RS 码所对应的 GF(2) 上的标准校验矩阵为：

$$\boldsymbol{H}=[\boldsymbol{Q}\boldsymbol{I}_{nm-km}] \quad (5)$$

式中 $\boldsymbol{Q}$ 的相邻两行 m 位进行移位相加如不为零，即为所在有限域构成多项式的系数。

证明：因为该 RS 码在 GF(2) 上的标准生成矩阵

为$\boldsymbol{G}=[\boldsymbol{I}_{km}\boldsymbol{P}]$,由:

$$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=[\boldsymbol{I}_{km}\boldsymbol{P}]\begin{bmatrix}\boldsymbol{Q}\\ \boldsymbol{I}_{nm-km}\end{bmatrix}=0 \tag{6}$$

得$\boldsymbol{Q}=\boldsymbol{P}^{\mathrm{T}}$。又根据引理2，$\boldsymbol{P}$的相邻两行移位相加如不为零，则为所在有限域构成多项式的系数。定理得证。

由$\boldsymbol{C}=m\boldsymbol{G}$和$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=0$得$\boldsymbol{C}\boldsymbol{H}^{\mathrm{T}}=0$，可以对含错码序列$C_p$求解方程求得校验矩阵$\boldsymbol{H}$。

定义 3[7] 方程$f(\boldsymbol{H}\boldsymbol{C}')=b$被称作二元域含错方程，其中$\boldsymbol{C}'$为以码长为行数依次将含错码序列$C_p$进行排列的矩阵，$b$是$f(\boldsymbol{H}\boldsymbol{C}')$的汉明重量，$\boldsymbol{C}'$是一个$n\times m$的矩阵，$m>>n$，$b$是一个整数，且$0\leqslant b\leqslant m$。

矩阵$\boldsymbol{Q}$是一个行(或列)置换矩阵，对于任何置换矩阵$\boldsymbol{Q}$都有$w(y)=w(\boldsymbol{Q}y)$，其中$\boldsymbol{Q}^{-1}$也是一个置换矩阵。

引理 2[7] 对于给定的矩阵$\boldsymbol{C}'$，$l=0,1,2\cdots$,本文做了以下的变换:

$$\boldsymbol{C}_l'=\boldsymbol{P}_{l+1}\begin{pmatrix}\boldsymbol{I}_{r_{l+1}} & \boldsymbol{C}_{l+1}'\\ 0 & 0\end{pmatrix}\boldsymbol{Q}_{l+1}^{-1} \tag{7}$$

式中　$\boldsymbol{C}_0'=\boldsymbol{C}'$，$r_0=n$，$m_0=m$；$\boldsymbol{C}_l'$是一个$r_l\times m_l$的矩阵；$\boldsymbol{P}_{l+1}$是一个$r_l\times r_l$的可逆矩阵；$\boldsymbol{Q}_{l+1}$是一个$m_l\times m_l$的置换矩阵；$\boldsymbol{I}_{r_{l+1}}$是一个$r_{l+1}$的单位矩阵；$\boldsymbol{C}_{l+1}'$是一个$r_{l+1}\times m_{l+1}$的矩阵；$r_{l+1}$是矩阵$\boldsymbol{C}_l'$的秩，并且$r_{l+1}\leqslant r_l, m_l$且$m_l=m_{l+1}+r_{l+1}$。这样可以将$r_l$维的行向量$\boldsymbol{x}_l$分解为:

$$(\boldsymbol{x}_l\boldsymbol{C}_l')\boldsymbol{Q}_{l+1}=(\boldsymbol{x}_{l+1},\boldsymbol{x}_{l+1}\boldsymbol{C}_{l+1}')\quad l=0,1,2\cdots \tag{8}$$

其中$\boldsymbol{x}_{l+1}$是一个r_{l+1}维的行向量。即有:

$$f(\boldsymbol{x}_l\boldsymbol{C}_{l+1}')=f(\boldsymbol{x}_{l+1})+f(\boldsymbol{x}_{l+1}\boldsymbol{C}_{l+1}') \tag{9}$$

显然

$$f(x\boldsymbol{C}')=f(x_1)+f(x_2)+\cdots+f(x_k)=f_1+f_2+\cdots+f_k \tag{10}$$

设$x_{k-1}P_k=(y_k,z_k)$，可得:

$$f(x_{k-1})f((y_k,z_k)P_k^{-1})=f_{k-1} \tag{11}$$

由式(10)和式(11)解出校验矩阵$\boldsymbol{H}$。

将$\boldsymbol{H}$化简成标准校验矩阵，然后根据定理 2 即可求出本原多项式$m(x)$。

(2) 高误码率情况。

在高误码率情况下，采用基于伽罗华域傅里叶变换的方法来求解域的本原多项式。

定义 4[6] 设GF(p)上的多项式为:

$$a(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0\qquad a_i\in \mathrm{GF}(p) \tag{12}$$

则它在GF(p^m)上的谱多项式(或者称为Mattson-Solomon (MS)多项式):

$$A(z)=A_{n-1}z^{n-1}+\cdots+A_1z+A_0=\sum_{j=0}^{n-1}A_jz^j \tag{13}$$

式中　$A_i=\sum_{i=1}^{n-1}a_i\alpha^{ji}$，$j=n-1,\cdots,1,0$，$\alpha$是GF($p^m$)中的$n$级单位本原元，$\alpha^n=1$；$A(z)=(A_{n-1},\cdots,A_1,A_0)$是$a=(a_{n-1},\cdots,a_1,a_0)$的GF($p^m$)上离散傅里叶变换。

引理 4[6] 多项式$a(x)$以α^j为根的充要条件是其MS多项式$A(z)$的系数$A_j=a(\alpha^j)=0$。

定理 3 对任一距离为δ的RS码字做GFFT变换，$A(z)$中至少有$\delta-1$个连零。

证明：由式(1)知，β是扩域GF(p^m)上的n级元素，$m_{\beta^i}(x)$($m_0\leqslant i\leqslant m_0+\delta-2$)是元素$\beta^i$的最小多项式($\delta-1$为校验元的个数)，又由引理 4 可知：多项式$a(x)$是以$\alpha^j$为根的充分必要条件是其MS多项式$A(z)$的系数$A_j=a(\alpha^j)=0$。因而$A(z)$中至少有$\delta-1$个连零。又因为RS码是极大最小距离可分码，所以$\delta$为该RS码的距离。

根据定理 3,将收到的码序列按照识别出来的m对N组码字做GFFT变换，当发现对r组码字做同一GFFT变换时具有相同的连零位置且个数相同时，则判断此时选取的本原多项式$m(x)$即为该码字的本原多项式。

3.1.3 生成多项式识别

在低误码率的情况下，根据求解出来的$\boldsymbol{H}$可以得出式(3)，将式(3)从GF(2)映射到GF(2^m)，其最后一行就是生成多项式。

在高误码率的情况下，根据识别出的本原多项式$m(x)$及通过GFFT后的连零个数，按照式(1)即可求出该RS码的生成多项式。

3.2 长码长RS码识别

对长码长RS码采用基于伽罗华域傅里叶变换的方法进行识别：(1) 通过对接收码序列遍历进行GFFT变换，识别本原多项式$m(x)$；(2) 根据$n=2^m-1$识别码长n；(3) 其生成多项式$g(x)$按照短码长高误码方法进行识别。

4 仿真实验与结果分析

本文针对不同误码率，给出了判决门限，通过蒙特卡罗仿真实验统计了识别概率。

4.1 数据来源

针对不同码长，随机选取其他编码参数，在不同误码率下，用Matlab各生成1 000组仿真数据。码长与误码率的选择如表 1 所示。

表 1 仿真数据参数选择表

码长($n=2^m-1$)	误码率(P_e)
$m=2,3,4$	$1\times10^{-2}, 7\times10^{-3}, 5\times10^{-3}, 3\times10^{-3}, 1\times10^{-3}, 9\times10^{-4}, 8\times10^{-4}, 7\times10^{-4}, 1\times10^{-5}$
$m=5$	$1\times10^{-2}, 7\times10^{-3}, 5\times10^{-3}, 3\times10^{-3}, 1\times10^{-3}, 7\times10^{-4}, 5\times10^{-4}, 2\times10^{-4}$
$m=6$	$5\times10^{-3}, 4\times10^{-3}, 3\times10^{-3}, 2\times10^{-3}, 1\times10^{-3}, 7\times10^{-4}, 5\times10^{-4}$
$m=7$	$2\times10^{-3}, 1.5\times10^{-3}, 1\times10^{-3}, 7\times10^{-4}, 5\times10^{-4}, 3\times10^{-4}, 2\times10^{-4}$
$m=8$	$1\times10^{-3}, 7\times10^{-4}, 5\times10^{-4}, 2\times10^{-4}, 1\times10^{-4}$

4.2 仿真参数设定

当采用容错矩阵分解法时，因接收RS码序列有误码，故要从概率角度讨论解向量的置信度。

求校验矩阵时，设某解向量代入方程组成立方程个数为 m_1，不成立方程个数为 m_2，则 $m_1+m_2=m$，$m_1-m_2=f(a_1,a_2,\cdots,a_n)$。则符合率 FHL $=1/2+f(a_1,a_2,\cdots,a_n)/2m$，其中 m 为方程个数。

假设 $c=(c_1,c_2,\cdots,c_n)$ 是 n 元含错方程组的解向量，方程成立的概率为 p。当 c 满足第 i 个方程时，令 $\xi_i=1$；当 c 不满足第 i 个方程时，令 $\xi_i=-1$。则 $E\left(\sum_{i=1}^{m}\xi_i\right)=m(p-q)$，$D\left(\sum_{i=1}^{m}\xi_i\right)=4mpq$。其中 m 为方程个数。当 m 足够大时，由中心极限定理有：$\sum\xi_i-m(p-q)/\sqrt{4mpq}\propto N(0,1)$。

令 $z=m_1-m_2$，计算统计量为：

$$T=z-m(p-q)/\sqrt{4mpq} \tag{14}$$

如果显著性水平为 α，则：

$$\alpha/2=1-F(t) \tag{15}$$

式中 $F(t)$ 是 t 的概率分布函数。由式(15)可以给出一个标准 t，在解方程过程中应保证 $T\geqslant t$。

取 $p=q=0.5$，则 $T=z/\sqrt{m}$。可根据该式来判别解向量的置信度。当 $t\geqslant3$ 时，错误概率为 0.001 35，此时将门限值 t 设为 3。

当采用伽罗华域的傅里叶变换法时，必须给出合适的判决门限。

根据信号检测理论[8]，H_0 表示多个样本经 GFFT 运算后产生位置、个数均相同的连零；H_1 表示经 GFFT 运算后不产生连零事件；D_0 和 D_1 分别表示判断产生连零和不产生连零，则可用下式计算 RS 码正确识别概率：

$$P_r=P(D_0\mid H_0)P(H_0)+P(D_1\mid H_1)P(H_1)=\frac{r}{N_0}\frac{N_0}{N}+\frac{l}{N_1}\frac{N_1}{N}=\frac{r+l}{N} \tag{16}$$

式中 N 表示进行 GFFT 运算的码分组数；N_0 表示产生连零的分组数；N_1 表示不产生连零的分组数；r 表示给定的门限条件下判别为连零分组数；l 为在给定门限条件下判断为非连零分组数。

式(16)给予两个事件相同的权重。如果对于不同事件的重视程度不同，应对不同的事件给予不同的权重。实际上本文的目的是检测出连零，因此判断为产生连零的事件应给以较大的权重：$c_{00}=0.99$，对判断为不产生连零的事件给予较小的权重：$c_{11}=0.01$。由此得：

$$P_r=c_{00}P(D_0\mid H_0)P(H_0)+c_{11}P(D_1\mid H_1)P(H_1)=c_{00}\frac{r}{N_0}\frac{N_0}{N}+c_{11}\frac{l}{N_1}\frac{N_1}{N}=\frac{c_{00}r+c_{11}l}{N} \tag{17}$$

对式(17)进行归一化，归一化的标准是：假设产生连零时，完全正确地判断为此RS码编码形式；不产生连零时，也完全判断为不是此类RS码编码形式。归一化的概率表达式为：

$$P_r=\frac{c_{00}r+c_{11}l}{c_{00}N_0+c_{11}N_1} \tag{18}$$

根据概率论，当误码率为 P_e 时，对于码长为 n' 的 RS 码，无误码分组存在的概率为 $P_t=(1-P_e)^{n'}$。在 GF(2^m) 下，假设信息均匀分布，信息位末位为零的概率 $P_z=1/2^m$。

假定对 N 个分组进行判定，则产生连零的分组数 $N_0=P_t(1-P_z)N$，不产生连零的分组数 $N_1=N-N_0$。分别将 N_0 和 N_1 代入式(18)得：

$$P_r=\frac{0.99r+0.01l}{0.99P_t(1-P_z)N+0.01[1-P_t(1-P_k)]N}=\frac{0.99r+0.01l}{0.98P_t(1-P_z)N+0.01N}=\frac{0.99r+0.01l}{[0.98(1-P_e)^{(2^m-1)m}(1-(1/2)^m)+0.01]N} \tag{19}$$

令 $l=r-1$，此时要达到90%的识别概率，得出近似门限：

$$r=\lfloor0.88(1-P_e)^{(2^m-1)m}N\rfloor \tag{20}$$

由式(20)可知，门限 r 依赖于误码率和码长的变化，为了保证很低的虚警概率，一般需保证 $r>0.1N$，且 $N_{\min}=50$。当门限 r 取 $\lceil0.51N\rceil$ 时，可以保证 0 虚警概率，当由式(20)计算的门限大于 $\lceil0.51N\rceil$ 时，将门限定义为 $\lceil0.51N\rceil$。

4.3　结果分析

图 1 为短码长(本文认为 $m \leqslant 4$)RS 码的识别概率与误码率的曲线图。当误码率 $P_e \leqslant 10^{-3}$ 时，按照低误码率的识别方法进行识别；当误码率 $P_e > 10^{-3}$ 时，以式(20)为门限，按照高误码率识别方法进行识别。由于容错矩阵分解法的实质是求解出满足方程个数最多的解向量，由 P_t 表达式可知，随着误码率和码长的增加，错误分组数量将增加。此时需要求解的方程个数和计算复杂度都将增加，因此当误码率较高或码长较长时采用伽罗华域傅里叶法。

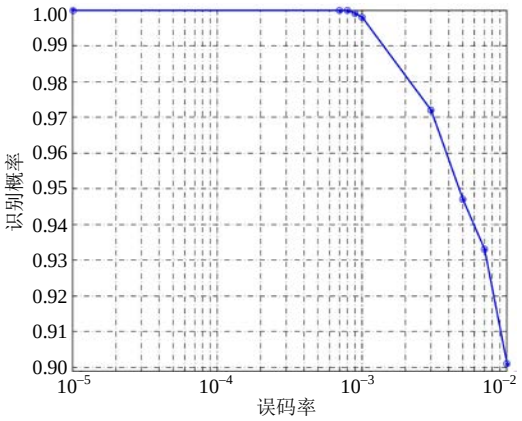

图1　短码长RS码识别概率曲线图

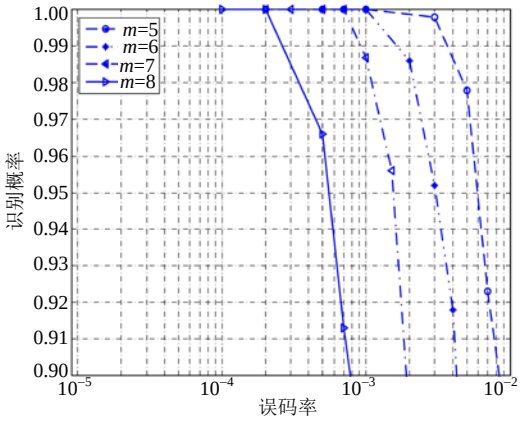

图2　长码长RS码识别概率曲线图

图 2 为长码长(本文认为 $m \geqslant 5$)RS 码识别概率与误码率曲线图(门限根据式(20)得到)。图中的 4 条曲线分别代表了当 $m=5$ 、$m=6$ 、$m=7$ 、$m=8$ 时，4 种不同码长的识别概率曲线。

由图 1 和图 2 可以看出，当误码率 P_e 低于 10^{-3} 时，除 $m=8$ 的 RS 码外，其他编码类型的 RS 码识别概率均接近 100%；当 $P_e = 5\times10^{-4}$ 时，$m=8$ 的 RS 码的识别概率为 96.9%；当误码率 $P_e \leqslant 2\times10^{-4}$ ，4 种不同码长的识别概率达到 100%。

根据 P_z 和 P_t 表达式可以得知，当码长增长，虽然漏报概率降低，但要求的无误码长度以指数增长，故而随着码长的增长要达到同样的识别概率，对误码率的要求会更高。仿真曲线验证了文中的分析结果。

5　结　论

根据RS码的结构和性质，本文建立了RS码盲识别的数学模型；通过RREF识别出短码码长后，根据误码率的高低，应用FTMD和GFFT成功地识别其他编码参数；通过对长码长进行遍历GFFT变换获得长码长的编码参数。实验表明该方法能够有效地实现RS码的盲识别，并已应用在某无线通信侦察课题。

参　考　文　献

[1] LU Pei-zhong, SHEN Li, LUO Xiang-yang, et al. Blind recognition of punctured convolutional codes[C]//IEEE International Symposium on Information Theory. Shanghai: IEEE Press, 2004: 457-457.

[2] SHEN Li, LU Pei-zhong, LUO Xiang-yang, et al. Equivalence of punctured convolutional codes from shift equivalent puncturing patterns[C]//IEEE International Conference on Information Technology: Coding and Computing. Las Vegas: IEEE Press, 2004, 1: 786-790.

[3] 邹　艳, 陆佩忠. 关键方程的新推广[J]. 计算机学报, 2006, 29(5): 712-718.
ZOU Yan, LU Pei-zhong. A new generalization of key equation[J]. Chinese Journal of Computers, 2006, 29(5): 712-718.

[4] WANG Feng-hua, HUANG Zhi-tao, ZHOU Yi-yu. A method for blind recognition of convolution code based Euclidean algorithm[C]//IEEE International Conference on Wireless Communications. Shanghai: IEEE Press, 2007: 1414-1417.

[5] WANG Zhong-feng, ZHANG Xin-miao, ZHU Jiang-li. Novel interpolation architecture for low-complexity chase soft-decision decoding of Reed-Solomon codes[C]//IEEE International Symposium on Circuits and Systems. Washington: IEEE Press, 2008: 3078-3081.

[6]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.

[7] XIA Jian-guo. Linear error equation on filed F2[J]. Chinese Quarterly Journal of Mathematics, 2007, 22(4): 518-522.

[8] 赵树杰, 赵建勋, 信号检测与估计理论[M]. 北京: 清华大学出版社, 2005: 260-348.
ZHAO Shu-jie, ZHAO Jian-xun. Signal detection and estimation theory[M]. Beijing: Tsinghua University Press, 2005: 260-348.

[9] KOETTER R, VARDY A. Algebraic soft-decision decoding of Reed-Solomon codes[J]. IEEE Transactions on Information Theory, 2003, 49(11): 2809-2825.

编　辑　张　俊