文章编号：2095-4980(2021)01-0031-07

RS 码的校验和识别方法

王甲峰，蒋鸿宇，胡茂海，漆　钢

(中国工程物理研究院 电子工程研究所，四川 绵阳 621999)

摘　要：针对基于谱累积量的里德–所罗门(RS)码识别算法计算量大、识别速度慢的问题，提出一种基于校验和的快速识别方法。首先遍历所有可能的有限域，以每个有限域本原元为唯一码根构造循环码，利用该循环码的二进制校验矩阵计算校验和，通过与设定的阈值进行比较，实现编码域的识别；然后构造以编码域中每个元素为唯一码根的循环码，利用该循环码的二进制校验矩阵计算与该域中每个元素相对应的校验和，并利用 RS 码码根的连续性估计连续码根数及起点，从而实现生成多项式的识别。针对最常用的 8 阶 RS 码进行了仿真试验，仿真结果显示，所提方法相对于谱累积量方法，在数据量相同的前提下，识别速度提高了约一个数量级，识别性能改善了 0.1 dB；而在 0.001 误比特率条件下，获得相同识别性能所需的数据量约为原有方法的 1/3。仿真试验结果说明，无论是在识别速度方面，还是在数据量需求方面，所提识别方法都远优于谱累积量方法。

关键词：RS 码；校验矩阵；校验和；有限域；有限域傅里叶变换；谱累计量；生成多项式

中图分类号：TN791.1　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019388

Recognition of RS code based on check-sum

WANG Jiafeng，JIANG Hongyu，HU Maohai，QI Gang

(Institute of Electronic Engineering, China Academy of Engineering Physics，Mianyang Sichuan 621999，China)

Abstract：A fast recognition method of Reed–Solomon(RS) code based on check-sum is proposed to reduce the computation and improve the recognition speed. Firstly, the cyclic code with the primitive element of each possible finite field as the unique code root is constructed. The check-sum is calculated by using the binary check matrix of the cyclic code and is compared with the threshold so as to recognize the coding field. Then, the cyclic code with each element of the coding field as the unique code root is constructed. And the check-sum corresponding to each element is calculated. Finally, the generator polynomial is recognized based on the continuity of RS code roots. Compared with the spectral cumulant method, the proposed method improves the recognition speed by about one order of magnitude and the recognition performance by 0.1 dB; while at the error rate of 0.001, the amount of data required to achieve the same recognition performance is about 1/3 of the original method. Simulation results show that the proposed method is much better than the spectral cumulant method in terms of recognition speed and data requirement.

Keywords：RS code；check matrix；check-sum；finite field；Galois field Fourier transform；spectral cumulant；generator polynomial

在智能通信系统中，编码识别是解码的前提，编码参数的盲识别问题一直是盲信号处理领域研究的重点课题之一。RS码是一类纠错能力很强的前向纠错编码，广泛应用于各种无线通信系统中，因而成为编码识别领域的重要研究对象之一。目前RS码的主要识别方法有欧几里得分析法[1]、矩阵分析法[2-5]、码根统计分析法[6-8]、有限域傅里叶变换(Galois Field Fourier Transform，GFFT)分析法[9-12]等。GFFT分析法亦称为谱累积量(Spectrum

收稿日期：2019-10-11；**修回日期：**2019-11-06

基金项目：NSAF 联合基金—非合作信号信道编码分析课题(11176005)

作者简介：王甲峰(1974–)，男，副研究员，主要研究方向为通信信号及信息处理。email:wangjiafeng@caep.cn

Cumulant)分析法，由于完善的理论体系及较为理想的识别性能，已成为RS码的主流分析方法；但是，该方法需要遍历所有可能的有限域及有限域中的所有元素，导致计算量较大，识别速度慢。为此，文献[13]利用编码域本原元是RS码码根这一特性提出一种快速识别方法，把编码域的识别与生成多项式的识别分离，在一定程度上提高了识别速度，但该方法依然涉及大量高阶有限域运算，速度提高有限。为了进一步提高识别速度，本文提出一种基于校验和的识别方法，把谱累积量运算转换为校验矩阵的校验和运算，主要运算在 $GF(2)$ 内进行，识别速度显著提高，并且在一定程度上改善了识别性能。此外，本文还采取序列相关的方法识别生成多项式，解决了生成多项式识别性能随着RS码纠错能力增强而降低的问题。

1　RS 码基础

定义在 $GF(2^m)$ ($m\geqslant 3$)上，能够纠正 t 个错误的 RS 码具有如下特征：a) 码长 $n=2^m-1$；b) 校验符号数 $k=n-2t$；c) 生成多项式可表示为：

$$g(x)=(x-\alpha^{t_0})(x-\alpha^{t_0+1})\cdots(x-\alpha^{t_0+2t-1}) \tag{1}$$

式中：m 为该 RS 码的阶数；α 为 $GF(2^m)$ 的本原元；$t_0=0$ 或 1，$1\leqslant t\leqslant\dfrac{(n-1)}{2}$。因为编码域 $GF(2^m)$ 取决于阶数 m 及 m 阶本原多项式 $p(x)$，所以一个 RS 码由阶数 m、本原多项式 $p(x)$ 及生成多项式 $g(x)$ 唯一确定。

假设 $c_1,c_2,\cdots,c_N$ 为发送端发送的已转换为二进制的 RS 码比特数据，$r_1,r_2,\cdots,r_N$ 为接收端解调输出的含有误码的比特数据，并且假定已通过帧同步等方法实现了码同步，那么 RS 码识别问题，就是利用 $r_1,r_2,\cdots,r_N$ 识别出目标 RS 码的编码域 $GF(2^m)$ 和生成多项式 $g(x)$。

2　识别算法

2.1 识别原理

定义：记 $c(x)$ 为该 RS 码的任一码多项式，β 是 $GF(2^m)$ 上的一个元素，如果 $c(\beta)=0$ 则称 β 为该 RS 码的一个码根。

命题 1：定义在 $GF(2^m)$ 上以 $g(x)=(x-\alpha^{t_0})(x-\alpha^{t_0+1})\cdots(x-\alpha^{t_0+2t-1})$ 为生成多项式的 RS 码，一定存在且只存在 $2t$ 个连续码根，并且这 $2t$ 个连续码根为 $\alpha^{t_0},\alpha^{t_0+1},\cdots,\alpha^{t_0+2t-1}$。

证明：由码根的定义及 RS 码的生成多项式表示形式可知，$\alpha^{t_0},\alpha^{t_0+1},\cdots,\alpha^{t_0+2t-1}$ 为该 RS 码的 $2t$ 个连续码根。如果假设还存在另一个公共码根 α^l，则由于 RS 码为循环码，其生成多项式为所有码多项式的最大公因式，则生成多项式为 $g(x)=(x-\alpha^{t_0})(x-\alpha^{t_0+1})\cdots(x-\alpha^{t_0+2t-1})(x-\alpha^l)$，这与该 RS 码的定义不一致，从而证明了 $2t$ 个连续公共码根的唯一性。

命题 2：对于定义在 $GF(2^m)$ 上的 RS 码，$GF(2^m)$ 的本原元 α 一定是该 RS 码的一个码根。

证明：由于 $t_0=0$ 或 1，根据命题 1 可知 $2t$ 个连续码根为 $1,\alpha,\cdots,\alpha^{2t-1}$ 或 $\alpha,\alpha^2,\cdots,\alpha^{2t}$；且 $1\leqslant t\leqslant\dfrac{(n-1)}{2}$，则该 RS 码至少存在 2 个码根为 $1,\alpha$ 或 α,α^2，因此 α 一定是该 RS 码的一个码根。

根据命题 1 和命题 2 可知，可以把 RS 码的识别分为 2 步：a)编码域的识别，即阶数 m 及本原多项式 $p(x)$ 的识别；b)生成多项式 $g(x)$ 的识别。

2.1.1 编码域识别

根据命题 2，对于定义在 $GF(2^m)$ 上的(n,k)RS 码，本原元 α 一定为其一个码根。令 $\boldsymbol{C}$ 为该 RS 码的一个码字，对应的码多项式为 $c(x)$，则必有 $c(\alpha)=0$，亦即 $x-\alpha$ 必然整除 $c(x)$。因此如果以 $x-\alpha$ 为生成多项式定义一个 m 进制$(n,n-1)$循环码，$\boldsymbol{H}$ 为该循环码的校验矩阵，则必有

$$\boldsymbol{C}\cdot\boldsymbol{H}^{\mathrm{T}}=0 \tag{2}$$

对于任一 m 阶(n,k)RS 码，都存在一个等价的(mn,mk)二进制线性分组码，设与 RS 码字 $\boldsymbol{C}$ 对应的二进制线性分组码的码字为 $\boldsymbol{C}_b$；同理，以 $x-\alpha$ 为生成多项式的 m 进制$(n,n-1)$循环码也对应一个$(nm,nm-m)$二进制线性分组码，设其校验矩阵为 $\boldsymbol{H}_b$，则有

$$\boldsymbol{C}_b\cdot\boldsymbol{H}_b^{\mathrm{T}}=0 \tag{3}$$

式中 $\boldsymbol{H}_b$ 为 $nm\times m$ 维二进制矩阵。实际识别过程中，能够获取的是接收到的二进制码字 $\boldsymbol{R}_b$，在含噪的情况下一般

其校验和满足一定的分布，可根据该分布确定阈值 T，如果校验和小于 T，则认为由当前阶数 m 及本原多项式 $p(x)$ 确定的有限域即为RS码的编码域。由此得到编码域的识别过程为：a) 遍历所有可能的阶数 m 及本原多项式 $p(x)$；b) 在每个 m 及 $p(x)$ 下构造有限域 $GF(2^m)$；c) 求出以 $x-\alpha$ 为生成多项式的 m 进制$(n,n-m)$循环码对应的$(nm,nm-m)$二进制线性分组码的校验矩阵 $\boldsymbol{H}_b$；d) 把接收到比特数据 $r_1,r_2,\cdots,r_N$ 分割为 M 个长度为 nm 的二进制向量，$n=2^m-1$；计算校验和 $CH(m,p)=\dfrac{1}{Mm}\sum_{i=1}^{M}\sum_{j=1}^{m}\boldsymbol{R}_{b,i}\boldsymbol{h}_{b,j}^{\mathrm{T}}$，其中：$p$ 为 $p(x)$，$\boldsymbol{R}_{b,i}$ 为第 i 个二进制向量，$\boldsymbol{h}_{b,i}$ 为 $\boldsymbol{H}_b$ 中的第 j 个行向量；e) 把校验和 $CH(m,p)$ 与设定的阈值 T 进行比较，如果 $CH(m,p)<T$，则认为当前 $GF(2^m)$ 即为目标 RS 码的编码域，识别结束，否则继续。

2.1.2 生成多项式识别

由定义可知，$GF(2^m)$ 上的 RS 码，其生成多项式 $g(x)$ 是由 t_0 及 t 唯一确定的，所以识别 $g(x)$ 就等价于识别 t_0 及 t；根据命题 1，RS 码存在 $2t$ 个连续码根，所以可据此识别 t_0 及 t。

识别出编码域 $GF(2^m)$ 后，设其中的第 l 个元素为 α^l ($0\leqslant l\leqslant(n-1)$)，求出以 $x-\alpha^l$ 为生成多项式的 m 进制$(n,n-1)$循环码对应的$(nm,nm-m)$二进制线性分组码的校验矩阵 $\boldsymbol{H}_{b,l}$(显然，$\boldsymbol{H}_b$=$\boldsymbol{H}_{b,1}$)，并计算校验和

$$CH(l)=\frac{1}{Mm}\sum_{i=1}^{M}\sum_{j=1}^{m}\boldsymbol{R}_{b,i}\boldsymbol{h}_{b,l,j}^{\mathrm{T}},\quad 0\leqslant l\leqslant(n-1) \tag{4}$$

式中 $\boldsymbol{h}_{b,l,j}$ 为 $\boldsymbol{H}_{b,l}$ 中的第 j 个行向量。如果 $CH(l)<T$，则 α^l 为 RS 码的码根，所以可采用直接法识别 t_0 及 t，步骤如下：a) 初始化 l=1；b) 计算 $CH(l)$；c) 如果 $CH(l)<T$，取 l=l+1，转到 b)，否则转到 d)；d) 如果 l 为偶数，则 $\hat{t}_0=1$，$\hat{t}=\dfrac{l}{2}$；否则，$\hat{t}_0=0$，$\hat{t}=\dfrac{(l+1)}{2}$。

直接法直接利用 BCH 码的连续码根特性识别 t_0 和 t，需要进行多个二元假设检验，随着 t 的增大必然会降低正确识别率，为此需要对识别算法进行改进。

首先，计算除 l=0 外的所有校验和 $CH(l)$ ($0\leqslant l\leqslant(n-1)$)，并把每个校验和与阈值 T 进行对比，得到校验和序列 $B_{\mathrm{ch}}=\{b_1,b_2,\cdots,b_{n-1}\}$，其中

$$b_l=\begin{cases}-1, & CH(l)<T\\ 1, & CH(l)\geqslant T\end{cases},\quad 0\leqslant l\leqslant(n-1) \tag{5}$$

然后，构造如下序列

$$w(d)=1-2\,pulse(1,d,n-1),\quad 1\leqslant d\leqslant(n-2) \tag{6}$$

式中 $pulse(1,d,n-1)$ 表示一个长度为 $n-1$ 的序列，其中 1~d 项为 1，其余为 0。令 $w(t,l)$ 为 $w(d)$ 中第 l 项，则 $w(t,1)=w(t,2)=\cdots=w(t,d)=-1$，其他为 1；计算下式，

$$prod(d)=\prod_{l=1}^{n-1}w(d,l)\cdot b_l \tag{7}$$

显然，当 $prod(t)$ 取最大时所取的 d 与 t_0 和 t 相关，

$$\hat{d}=\arg\max_{d}\,prod(d) \tag{8}$$

$$\begin{cases}\hat{t}_0=1,\hat{t}=\dfrac{\hat{d}}{2} & rem(\hat{d},2)=0\\ \hat{t}_0=0,\hat{t}=\dfrac{(\hat{d}+1)}{2} & rem(\hat{d},2)=1\end{cases} \tag{9}$$

式(8)实际上是 2 个序列的相关，所以称此方法为相关法。得到 $\hat{t}_0$ 及 $\hat{t}$ 之后，则可进一步得到生成多项式 $g(x)$。

2.1.3 校验矩阵的求取方法

由 2.1.1 和 2.1.2 可知，上述算法的关键是求取 $\boldsymbol{H}_{b,l}$，而分析等价二进制线性分组码与 m 进制原循环码之间的关系是比较复杂的。为此，本文采用高斯约旦消元法直接利用二进制线性分组码数据求取对应的校验矩阵[14]。

对于阶数 m、本原多项式 $p(x)$ 构造的有限域 $GF(2^m)$，生成 P 组长度为 $n-1$ ($n=2^m-1$, $P\geqslant 2mn$)的 m 进制随机消息分组 $\boldsymbol{U}_i$($1\leqslant i\leqslant(n-P)$)，$u_i(x)$ 为 $GF(2^m)$ 上对应的消息多项式，则以 $x-\alpha^l$ 为生成多项式的 m 进制 $(n,n-1)$ 循环码的编码过程可表示为：

$$v_i(x)=u_i(x)(x-\alpha^l) \tag{10}$$

式中 $v_i(x)$ 为码多项式，对应的码字为 $\boldsymbol{V}_i$，由 n 个 m 进制整数构成。将 $\boldsymbol{V}_i$ 中的每个元素用二进制表示，则可得到

长度为 mn 二进制码字 $\boldsymbol{V}_{b,i}$。以 $\boldsymbol{V}_{b,i}$ 为行向量构成 $P\times mn$ 维数组 $\boldsymbol{A}$。然后，利用高斯消元法，将码矩阵 $\boldsymbol{A}$ 转换为一个下三角矩阵 $\boldsymbol{B}$，即

$$\boldsymbol{B}=\boldsymbol{A}\boldsymbol{\Phi} \tag{11}$$

式中：$\boldsymbol{B}$ 是 $P\times mn$ 维二进制矩阵；$\boldsymbol{\Phi}$ 是 $mn\times mn$ 维二进制矩阵，且 $\boldsymbol{\Phi}=[\boldsymbol{\phi}_1\quad\boldsymbol{\phi}_2\quad\cdots\quad\boldsymbol{\phi}_{mn}]^{\mathrm{T}}$，$\boldsymbol{\phi}_j(1\leqslant j\leqslant mn)$为矩阵 $\boldsymbol{\Phi}$ 的列向量。统计矩阵 $\boldsymbol{B}$ 中的列重 $w_{B,j}(1\leqslant j\leqslant mn)$，如果当 $j=\lambda_1,\lambda_2,\cdots,\lambda_m$ 时 $w_{B,\lambda_1}=w_{B,\lambda_2}=\cdots=w_{B,\lambda_m}=0$，则 $\boldsymbol{H}_{b,l}$ 由 $\boldsymbol{\Phi}$ 中对应的列向量构成：

$$\boldsymbol{H}_{b,l}=[\boldsymbol{\phi}_{\lambda_1}\quad\boldsymbol{\phi}_{\lambda_2}\quad\cdots\quad\boldsymbol{\phi}_{\lambda_m}]^{\mathrm{T}} \tag{12}$$

上述求取方法随着阶数的增大，计算量会显著增加，所以在识别前需要离线求出待识别阶数范围内所有的校验矩阵，并保存起来，识别时直接读取，即以存储空间换取识别速度；不过，由于存储的都是二进制数据，所需要的存储空间不大；以 8 阶 RS 码为例，所需的存储空间为 2 040×2 040×16≈6.5 MB。

2.2 阈值的选取

由文献[15]可知，假设 $R_i(1\leqslant i\leqslant M)$是 M 个二进制线性分组码码字，$\boldsymbol{h}$ 为该码的一个校验向量，则当 M 足够大时，校验和 $CH=\dfrac{1}{M}\sum_{i=1}^{M}\boldsymbol{R}_i\boldsymbol{h}^{\mathrm{T}}$ 近似服从均值为 $e_1=\dfrac{1}{2}-\dfrac{(1-2\tau)^w}{2GF(2)}$，方差为 $d_1=\dfrac{1}{4M}-\dfrac{(1-2\tau)^{2w}}{4M}$ 的高斯分布，其中 τ 为误比特率，w 为 $\boldsymbol{h}$ 的汉明重量，即其中 1 的个数；当 $\boldsymbol{R}_i$ 不是与 $\boldsymbol{h}$ 对应的码字或 $\boldsymbol{h}$ 不是与 $\boldsymbol{R}_i$ 对应的校验向量时，当 M 足够大时，校验和近似服从均值为 $e_0=1/2$，方差为 $d_0=1/4M$ 的高斯分布。

由此可以得到，当 M 足够大时校验和 $CH(l)$ 的分布满足：

1) 当 $\boldsymbol{R}_{b,i}(1\leqslant i\leqslant M)$与 $\boldsymbol{H}_{b,l}$ 是对应的码字的校验矩阵时 $CH(l)$ 近似服从高斯分布，

$$CH(l)\sim N(E_1,D_1) \tag{13}$$

式中：$E_1=\dfrac{1}{2}-\dfrac{1}{2m}\sum_{j=1}^{m}(1-2\tau)^{w_j}$；$D_1=\dfrac{1}{4Mm}-\dfrac{1}{4Mm^2}\sum_{j=1}^{m}(1-2\tau)^{2w_j}$；$w_j$ 为 $\boldsymbol{h}_{b,l,j}$ 的汉明重量。为了简化，一般可取 $w_j=\dfrac{nm}{2}$，则 $E_1\approx\dfrac{1}{2}-\dfrac{1}{2}(1-2\tau)^{mn/2}$，$D_1\approx\dfrac{1}{4Mm}-\dfrac{1}{4Mm}(1-2\tau)^{mn}$，下面讨论中 E_1 和 D_1 取近似值。

2) 其他情况下，$CH(l)$ 也近似服从高斯分布

$$CH(l)\sim N(E_0,D_0) \tag{14}$$

式中：$E_0=\dfrac{1}{2}$；$D_0=\dfrac{1}{4Mm}$。

因为 $E_1<E_0$，所以判断 $GF(2^m)$ 中某一元素 α^l $(0\leqslant l\leqslant(n-1))$是否为码根的问题就转换为一个二元假设检验问题：

$$H=\begin{cases}H_1 & CH(l)<T\\ H_0 & CH(l)\geqslant T\end{cases}\qquad E_1<T<E_0 \tag{15}$$

式中：H_0 表示 α^l 不是码根的假设；H_1 表示 α^l 是码根的假设。另外由于 $CH(m,p)=CH(1)$，因此也符合同样的概率分布。

得到 $CH(l)$ 所符合的概率分布后，即可据此选取最优判决阈值。为了兼顾检测概率和虚警概率，本文根据最大后验概率准则确定阈值。由最大后验概率准则可知，当 $\dfrac{CH(l)-E_1}{\sqrt{D_1}}>\dfrac{CH(l)-E_0}{\sqrt{D_0}}$ 时应取 H_1 假设，否则取 H_0 假设，取两边相等时的 $CH(l)$ 为阈值 T，则可得到：

$$T=\frac{E_1\sqrt{D_0}+E_0\sqrt{D_1}}{\sqrt{D_0}+\sqrt{D_1}} \tag{16}$$

分析可知，按式(17)确定的阈值与 M 无关。

2.3 数据量需求分析

令

$$\alpha=\frac{E_0-T}{\sqrt{D_0}}=\frac{T-E_1}{\sqrt{D_1}}=\frac{E_0-E_1}{\sqrt{D_0}+\sqrt{D_1}} \tag{17}$$

为了保证足够高的正确识别率和足够低的虚警概率，根据 3σ 准则，α 应满足 $\alpha \geqslant 3$，由此得到：

$$M \geqslant 9\left(\frac{\sqrt{d_1}+\sqrt{d_0}}{E_0-E_1}\right)^2 \tag{18}$$

式中：$d_0=\frac{1}{4m}$；$d_1=\frac{1}{4m}-\frac{1}{4m}(1-2\tau)^{mn}$。因此，在 3σ 准则下，所需的最少码字数 $M_{\min}$ 为：

$$M_{\min}=\left\lceil 9\left(\frac{\sqrt{d_1}+\sqrt{d_0}}{E_0-E_1}\right)^2\right\rceil \tag{19}$$

谱累计量具有类似的性质，可以得到类似的结论，

$$M'_{\min}=\left\lceil 9\left(\frac{\sqrt{d'_1}+\sqrt{d'_0}}{e'_0-e'_1}\right)^2\right\rceil \tag{20}$$

式中：$e'_0=\frac{1}{2}$；$d'_0=\frac{1}{12}$；$e'_1=\frac{1}{2}-\frac{1}{2}(1-\tau)^{mn}$；$d'_1=\frac{1}{3}\left[1-(1-\tau)^{mn}\right]-\frac{1}{4}\left[1-(1-\tau)^{mn}\right]^2$。图 1 给出了 m=8 时，$M_{\min}$ 和 $M'_{\min}$ 随误比特率的变化。可以看出 $M'_{\min}>M_{\min}$，并且随着误比特率的增加，二者的差值越大。这表明，在同等识别性能下，本文识别方法要比累计量识别方法所需的码字数要少得多；换言之，利用等量数据，本文方法可以获得更优的识别性能。后面的仿真试验也验证了这一点。

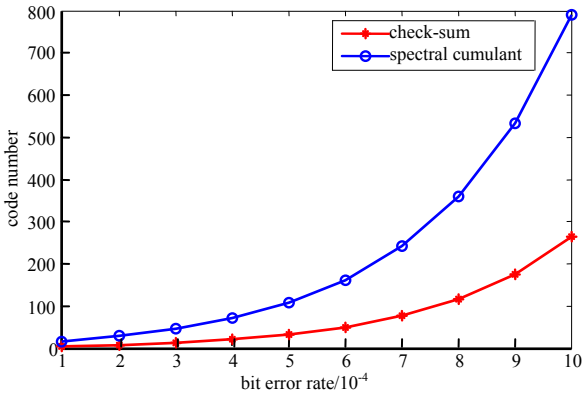

Fig.1 Code number for different bit error rates
图 1 码字数随误比特率变化曲线

3 仿真试验

实际应用中 8 阶 RS 码应用最广，所以这里以 8 阶 RS 码为例进行仿真。待识别 RS 码的本原多项式在所有 8 阶本原多项式集合中随机选取；识别时，阶数搜索范围为 3~8，采用 BPSK 调制方式，噪声为高斯白噪声，每次试验重复测试 1 000 次，统计正确识别率。

3.1 编码域的识别

t_0 在0和1之间随机选取，$t=1$，在误比特率0.000 1~0.002(步进0.000 1)条件下，分别取 $M=300$ 和 $M=500$，本文方法及谱累积量识别方法识别性能对比见图2，为了便于对比，绘图时横轴为BPSK调制模式下误比特对应的信噪比。由图2可知，在相同数据量条件下，本文方法优于谱累积量方法，性能改进约0.1dB，但在同一平台上的运行速度相对于谱累积量法提高了1个数量级(运行用时比约为20)。

图3给出了误比特率0.001，码字数取50~1 000(步进50)时，正确识别率随码字数的变化，由图可知，当 $t>250$，本文方法的正确识别率接近于1，而当 $t>750$，谱累积量方法的正确识别率才接近于1，与理论分析一致。

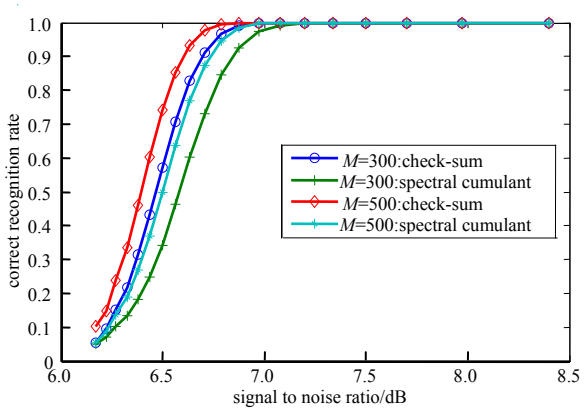

Fig.2 CRR of the code field for different SNRs
图 2 编码域识别性能随信噪比变化曲线

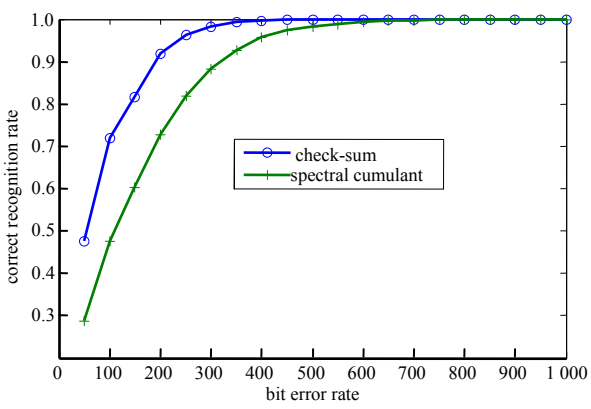

Fig.3 CRR of the code field for different code numbers when τ=0.001
图 3 τ=0.001 时编码域识别性能随码字数变化曲线

3.2 生成多项式的识别

由 2.1.2 可知，生成多项式 $g(x)$ 的识别可转换为 t_0 和 t 的识别，但这是以正确识别编码域 $GF(2^m)$ 为前提的，所以 $g(x)$ 的正确识别等价于同时正确识别编码域 $GF(2^m)$、t_0 及 t。在与 3.1 相同的条件下进行仿真，识别 t_0 和 t 时采用直接法，图 4 给出了仿真结果。由图 4 可得到与 3.1 类似的结论，即在同等条件下，本文方法优于谱累积量方法，性能改进约 0.1dB。由于皆采用直接法估计 t_0 和 t，所以性能改善主要是由编码域识别性能的改善带来的。

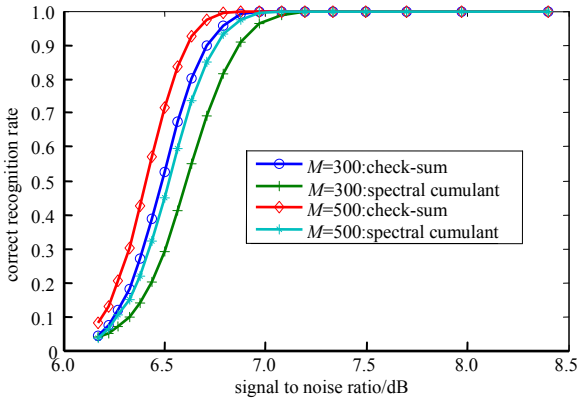

Fig.4 CRR of the generator polynomial when t=1
图 4 t=1 时生成多项式识别性能随信噪比变化曲线

为了对比直接法和相关法识别 t_0 和 t 的性能，取 $t=1,2,4,8,16$，$M=500$，其他条件与 3.1 同，采用本文方法进行识别，仿真结果见图 5 和图 6。由图可知，直接法的识别性能随 t 取值增大而恶化，而相关法中，当 $t\geqslant 2$ 时，识别性能已基本保持不变。限于篇幅没有给出 t 取相同值时，两种方法的性能曲线，但对比图 4 和图 5，大致可以看出，相关法的性能优于直接法，并且随着 t 取值增大，其性能改善程度越大，体现了相关法的优越性。

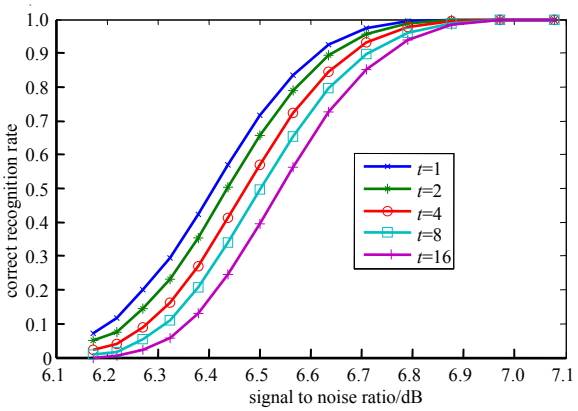

Fig.5 CRR of the generator polynomial using direct method
图 5 t 取不同值时直接法生成多项式识别性能

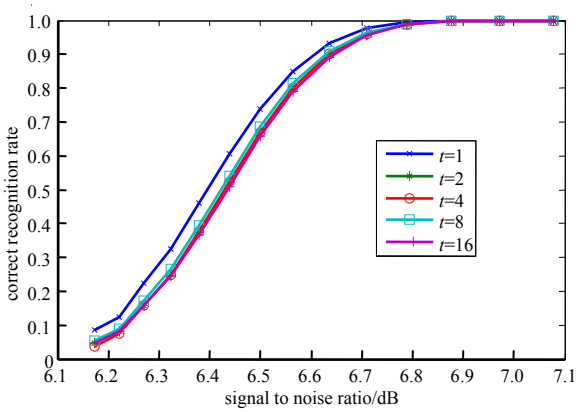

Fig.6 CRR of the generator polynomial using correlation method
图 6 t 取不同值时相关法生成多项式识别性能

4　结论

本文从 RS 码的码根特性出发，提出一种基于校验和的识别方法。仿真试验结果表明，无论是在识别速度方面还是在数据量需求方面，本文所提方法都远优于谱累积量方法。而且，由于校验和计算仅涉及二进制运算和十进制运算，容易用硬件描述语言实现，所以更有利于应用于实时系统中。

此外，由于需要利用二进制校验矩阵，所以本文方法可以很方便地转换为基于软信息的识别方法。软信息中包含了每个比特的可靠性信息，因此利用软信息进行识别有望进一步提高识别性能，值得深入研究。

参考文献：

[1] 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. (QI Lin,HAO Shiqi,LI Jinshan. Recognition method of RS codes based on Euclidean algorithm in Galois field[J]. Journal of Detection & Control, 2011,33(2):63-67.)

[2] 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 & Information Technology, 2012,34(12):2837-2842.)

[3] LI Wenwen,LEI Jing,WEN Lei,et al. An improved method of blind recognition of RS code based on matrix transformation[C]// Proceedings of International Conference on Communication Technology(ICCT). Guilin,Guangxi,China: [s.n.], 2013:196-200.

[4] SWAMINATHAN R,MADHUKUMAR A S,WANG Guohua,et al. Parameter identification of Reed-Solomon codes over

noisy environment[C]// Proceedings of IEEE 86th Vehicular Technology Conference. Toronto,Canada:IEEE, 2017:1-5.

[5] SWAMINATHAN R,MADHUKUMAR A S,WANG Guohua,et al. Blind reconstruction of Reed-Solomon encoder and interleavers over noisy environment[J]. IEEE Transactions on Broadcasting, 2018,64(4):830-845.

[6] 闻年成,杨晓静. 基于码根统计的 RS 码盲识别[J]. 通信对抗, 2010(4):18-21. (WEN Niancheng,YANG Xiaojing. Blind recognition of RS code based on code roots statistic[J]. Communication Countermeasures, 2010(4):18-21.)

[7] 闻年成,杨晓静. RS 码的盲参数识别[J]. 计算机工程与应用, 2011,47(19):136-139. (WEN Niancheng,YANG Xiaojing. Blind recognition of RS codes parameters[J]. Computer Engineering and Applications, 2011,47(19):136-139.)

[8] 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. (ZHANG Limin,LIU Jie,SUN Yongwei,et al. Blind parameter recognition of RS codes[J]. Telecommunication Engineering, 2017,57(6):650-655.)

[9] 戚林,郝士琦,王勇. 基于 GFFT 的 CCSDS 标准 RS 码交织识别算法[J]. 电光与控制, 2011,18(12):93-97. (QI Lin,HAO Shiqi,WANG Yong. Recognition algorithm of interlace depth of CCSDS RS coding based on GFFT[J]. Electronics Optics & Control, 2011,18(12):93-97.)

[10] 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. (BAO Xin,LU Peizhong,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.)

[11] ZHANG Xiaokai,WU Gang,ZHANG Bangning,et al. Blind recognition of RS codes based on Galois field Fourier transform[C]// Proceedings of 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Dalian,China:[s.n.], 2016:429-433.

[12] LIU Pengtao,PAN Zhipeng,LEI Jing. Parameter identification of Reed-Solomon codes based on probability statistics and Galois field Fourier transform[J]. IEEE Access, 2019,7(1):33619-33630.

[13] 王平,曾伟涛,陈健. 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. (WANG Ping,ZENG Weitao,CHEN Jian. Fast blind recognition algorithm for RS codes by primitive element[J]. Journal of Xidian University, 2013,40(1):105-110.)

[14] XU Yiyao,ZHONG Yang,HUANG Zhiping. An improved blind recognition method of the convolutional interleaver parameters in a noisy channel[J]. IEEE Access, 2019,7(1):101775-101784.

[15] 张天骐,王俊霞,江晓磊.等. 基于校验矩阵匹配的循环码参数盲识别算法[J]. 电子与信息学报, 2017,39(4):901-907. (ZHANG Tianqi,WANG Junxia,JIANG Xiaolei,et al. Blind recognition of cyclic code based on check matrix match algorithm[J]. Journal of Electronics & Information Technology, 2017,39(4):901-907.)