DOI：10.7652/xjtuxb201706010

一种软判决下的本原BCH码盲识别方法

刘杰，张立民，钟兆根，马超
（海军航空工程学院信息融合研究所，264001，山东烟台）

摘要：为解决现有BCH码识别方法容错性较差的问题，提出了一种软判决下的本原BCH码盲识别(SDBR)方法。首先，将截获数据进行解调软判决得到比特序列和对应可靠性信息，然后对比特序列进行码字划分，再由软判决可靠性信息建立码根可靠性系数，以此计算不同码根出现的概率，并引入Kullback-Leibler散度来确定码长；其次，定义公共码根可靠性统计量并建立二元假设检验，在不同本原多项式下对公共码根进行判定；最后，利用公共码根连续分布特点识别本原多项式，进而由所有公共码根计算生成多项式。仿真结果表明：SDBR方法在信噪比大于7 dB时能有效对常用本原BCH码进行识别；与基于码根信息差熵的方法相比，容错性提升了1.8 dB。

关键词：BCH码；盲识别；软判决；Kullback-Leibler散度；假设检验
中图分类号：TN911.22 **文献标志码**：A **文章编号**：0253-987X(2017)06-0059-07

A Blind Recognition Method for Primitive BCH Codes in Soft Decision Situations

LIU Jie, ZHANG Limin, ZHONG Zhaogen, MA Chao
(Institute of Information Fusion, Naval Aeronautical and Astronautical University, Yantai, Shandong 264001, China)

Abstract: A soft decision based blind recognition (SDBR) method for primitive BCH codes is proposed to solve the problem that existing recognition methods have low error-resilient capabilities. Firstly, bit sequences as well as the corresponding reliability information are obtained by soft demodulation of the intercepted data, then code words are divided and a reliability coefficient of code roots is established with the reliability information to calculate the occurrence probability of code roots, and code length is estimated by using Kullback-Leibler divergence. Secondly, reliability statistics of common code roots are defined and a binary hypothesis test is built, then common code roots are verified under different primitive polynomials. Finally, the right primitive polynomial is recognized by using the continuous distribution characteristics of common code roots, and a generator polynomial is calculated from all these code roots. Simulation results show that the SDBR method effectively recognizes the commonly used primitive BCH codes when the signal-to-noise ratio is above 7 dB. A comparison with the roots information dispersion entropy based method shows that the SDBR method improves the error-resilient performance by 1.8 dB.

Keywords: BCH codes; blind recognition; soft decision; Kullback-Leibler divergence; hypothesis test

---

收稿日期：2016-12-02。 作者简介：刘杰(1990—)，男，博士生；张立民(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金重大研究计划资助项目(91538201)；泰山学者工程专项经费资助项目(st201511020)。
网络出版时间：2017-04-11 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20170411.1043.002.html

数字通信中，为了抗击传输过程中的各种干扰，往往要人为地在信息序列中加入一些冗余位，使其具有自动检错或纠错能力，这就是信道编码技术[1]。信道编码盲识别是实现自适应调制编码、通信对抗的关键技术，其实际应用价值受到了国内外的广泛关注[2-4]。因此，对其进行研究具有非常重要的意义。

BCH 码是一种常见的线性分组码，具有纠错能力强、代数结构固定和编码构造简单等特点，在国际空间数据系统顾问委员会(CCSDS)标准和数字卫星广播(DVB-S2)标准中都采用了 BCH 码。针对 BCH 码的盲识别问题，目前国内外公开发表的文献较少，主要包括一些分组码通用识别算法、欧几里得法[5]、基于码根统计的方法[6-7]以及基于有限域傅里叶变换的方法[8]等。分组码通用识别算法包括基于码重分布距离的方法[9]、基于矩阵分析的方法[10-11]和基于 Walsh-Hadamard 变换的方法[12]等，其中前两种方法对误码率的要求较高，后一种方法性能较强，但计算复杂度较大，无法适用于码长较大时的情况。根据生成多项式是所有码字多项式的公约式这一特点，文献[5]采用欧几里得法计算最大公约式的阶数分布，完成对码长的识别，其容错性能较差。根据 BCH 码生成多项式码根连续分布特点，文献[6]首次提出基于码根信息差熵(RIDE)的方法对码长进行识别，通过将生成多项式的整数根转化为符号根以完成本原多项式的识别。该算法在高误码率下的识别性能有待进一步提升。文献[7]利用有限域傅里叶变换对码字多项式进行处理，计算复杂度较大。

目前的识别算法多基于解调器的硬判决输出，即匹配滤波器在每一个信号间隔内都量化为 0 和 1，因此当误码率较大时，不可避免地会对识别性能造成限制。如果采用软判决，则不仅能得到 0、1 比特数据，还能额外提供这些数据的可靠性信息。受此启发，本文首先利用软判决信息分析码根出现概率，并引入 Kullback-Leibler(KL)散度对码长进行识别，然后建立二元假设检验对码字连续公共码根进行判定，最终得到生成多项式。仿真结果表明，相比传统的基于硬判决的方法，本文方法容错性提升明显。

1 问题描述与分析

1.1 本原 BCH 码定义

定义 1[1] 给定任一有限域 $\boldsymbol{F}_{\mathrm{g}}(q)$及其扩域$\boldsymbol{F}_{\mathrm{g}}(q^m)$，其中 q 为素数或素数的幂，m 为某一正整数。若码元取自 $\boldsymbol{F}_{\mathrm{g}}(q)$上的一循环码，它的生成多项式 $g(x)$的根集合中包含以下 $\delta-1$ 个连续根 α^{m_0}，α^{m_0+1}，…，$\alpha^{m_0+\delta-2}$，则由 $g(x)$生成的循环码称为 q 进制 BCH 码。

如果 $q=2$、$m_0=1$、$\delta=2t+1$，且 α 为 $\boldsymbol{F}_{\mathrm{g}}(2^m)$中的本原元，则该码变为码长 $n=2^m-1$、纠 t 个错误的二进制本原 BCH 码，其生成多项式为 $x^{2^m-1}-1$ 的因式。实际应用中，本原 BCH 码多采用中短码，一般选取码长范围为 7～511 bit，对应 $3\leqslant m\leqslant 9$。

1.2 软判决下的识别模型

假设编码后使用二进制相移键控(BPSK)调制信号在加性高斯白噪声(AWGN)信道下传输，令发送比特序列 $\boldsymbol{s}=(s_0,s_1,\cdots,s_i,\cdots)$对应的接收软判决序列为 $\boldsymbol{c}=(c_0,c_1,\cdots,c_i,\cdots)$，则

$$c_i=(1-2s_i)+w_i \tag{1}$$

式中：s_i 取值为 0 或 1；w_i 表示均值为 0、功率为 σ^2 的加性高斯白噪声。对每个接收符号采用以下硬判决独立译码

$$v_i=\begin{cases}0, & c_i\geqslant 0\\ 1, & c_i<0\end{cases} \tag{2}$$

得到对应的 0、1 序列，则比特 v_i 的可靠度用对数似然比(Log Likelihood Ratio，LLR)定义为

$$L_{\mathrm{r}}(v_i\mid c_i)=\ln\frac{P_{\mathrm{r}}(v_i=0\mid c_i)}{P_{\mathrm{r}}(v_i=1\mid c_i)}=\frac{2c_i}{\sigma^2} \tag{3}$$

式中：$P_{\mathrm{r}}(\cdot)$表示概率。由式可以看出，$|c_i|$越大，对应 v_i 越可靠。

在帧同步的情况下，需识别的参数包括码长、本原多项式及生成多项式。接收软判决序列后，先根据式(2)得到对应比特序列，再由式(3)定义的可靠度信息进行参数识别。

2 码长识别

对 $m(3\leqslant m\leqslant 9)$进行遍历，在对应码长 n 下划分接收的比特序列，得到 N 组码字。称码字多项式的根为码根，用符号 α^j 表示，其中 j 为码根取值域内对应的整数，且 $1\leqslant j\leqslant n-1$。对所有码字的码根进行统计，当对应真实码长时，每一个码字的码根集合中必包含生成多项式 $g(x)$的根，因此整体的码根分布呈现一定的规律性。当码长估计不正确时，码根随机出现，可以将其近似为均匀分布。

假定 N 组码字中码根 $\alpha^j(1\leqslant j\leqslant n-1)$的数量为 S_j，令 $S=\sum_{j=1}^{n-1}S_j$，则每个码根出现的概率为

$$p_j=\frac{S_j}{S},\ 1\leqslant j\leqslant n-1 \tag{4}$$

引入 KL 散度[13]的系统形式来定义码根实际分布与均匀分布的距离

$$\Delta H=\sum_{j=1}^{n-1}\left[\left(p_j-\frac{1}{n-1}\right)\mathrm{lb}((n-1)p_j)\right] \tag{5}$$

则当 n 对应真实码长时，ΔH 达到最大值。由于同一码长下码根分布仅随本原多项式的不同发生位置改变，而数量不变。因此，本原多项式对码长识别无影响，在进行识别时采用对应 m 下任意一个本原多项式即可。下面利用软判决信息对 ΔH 进行计算。

码字 $\boldsymbol{v}_i=(v_{i,0},v_{i,1},\cdots,v_{i,n-1})$，$1\leqslant i\leqslant N$ 对应的码字多项式为

$$\boldsymbol{v}_i(x)=v_{i,0}+v_{i,1}x+v_{i,2}x^2+\cdots+v_{i,n-1}x^{n-1} \tag{6}$$

当 α^j 为其根时，有

$$v_{i,0}+v_{i,1}\alpha^j+v_{i,2}(\alpha^j)^2+\cdots+v_{i,n-1}(\alpha^j)^{n-1}=0 \tag{7}$$

令 $\boldsymbol{h}_j=(1,(\alpha^j),(\alpha^j)^2,\cdots,(\alpha^j)^{n-1})$，$\boldsymbol{H}$ 为奇偶校验矩阵，则 $\boldsymbol{h}_j\in\boldsymbol{H}$。在本原多项式 $p(x)$ 下将 $\boldsymbol{h}_j$ 中每个元素转化为域 $\boldsymbol{F}_g$(2)中的 m 维列向量，得

$$\boldsymbol{H}_j=\begin{bmatrix}h_{0,0}&h_{0,1}&\cdots&h_{0,n-1}\\h_{1,0}&h_{1,1}&\cdots&h_{1,n-1}\\\vdots&\vdots&&\vdots\\h_{m-1,0}&h_{m-1,1}&\cdots&h_{m-1,n-1}\end{bmatrix} \tag{8}$$

因此式(7)等价于

$$\boldsymbol{H}_j\boldsymbol{v}_i^{\mathrm{T}}=\boldsymbol{0} \tag{9}$$

式中：$\boldsymbol{0}$表示全 0 向量。令 $\boldsymbol{H}_j$ 第 k 行为 $\boldsymbol{h}_{j,k}$，若 $\boldsymbol{h}_{j,k}$ 中有 M 个 1，$g_{k,l}$表示其第 l($1\leqslant l\leqslant M$)个 1 对应的位置，则式(9)在 $\boldsymbol{v}_i$ 对应软判决序列 $\boldsymbol{c}_i$ 下成立的条件概率表示为

$$\Gamma_{j,i}=\prod_{k=1}^{m}P_{\mathrm{r}}\left(\bigoplus_{l=1}^{M}v_{i,g_{k,l}}=0\,|\,\boldsymbol{c}_i\right) \tag{10}$$

式中：符号⊕表示二元域加法。令

$$\gamma_{j,i,k}=L_{\mathrm{r}}\left(P_{\mathrm{r}}\left(\bigoplus_{l=1}^{M}v_{i,g_{k,l}}=0\,|\,\boldsymbol{c}_i\right)\right)=\ln\left(\frac{P_{\mathrm{r}}\left(\bigoplus_{l=1}^{M}v_{i,g_{k,l}}=0\,|\,\boldsymbol{c}_i\right)}{1-P_{\mathrm{r}}\left(\bigoplus_{l=1}^{M}v_{i,g_{k,l}}=0\,|\,\boldsymbol{c}_i\right)}\right) \tag{11}$$

对式(11)进行变换，有

$$P_{\mathrm{r}}\left(\bigoplus_{l=1}^{M}v_{i,g_{k,l}}=0\,|\,\boldsymbol{c}_i\right)=\frac{\mathrm{e}^{\gamma_{j,i,k}}}{1+\mathrm{e}^{\gamma_{j,i,k}}} \tag{12}$$

将式(12)代入式(10)，得

$$\Gamma_{j,i}=\prod_{k=1}^{m}\frac{\mathrm{e}^{\gamma_{j,i,k}}}{1+\mathrm{e}^{\gamma_{j,i,k}}} \tag{13}$$

下面对 $\gamma_{j,i,k}$值计算过程进行说明。根据文献[14]，$\gamma_{j,i,k}=\bigotimes_{l=1}^{M}L_r(v_{i,g_{k,l}}\,|\,c_{i,g_{k,l}})$，其中运算符⊗表示该运算由双曲正切函数 tanh(·)定义

$$u_1\otimes u_2=\ln\left(\frac{1+\tanh(u_1/2)\tanh(u_2/2)}{1-\tanh(u_1/2)\tanh(u_2/2)}\right) \tag{14}$$

式(14)可以简化为

$$\bigotimes_{i=1}^{n}u_i\approx\left(\prod_{i=1}^{n}\mathrm{sign}(u_i)\right)\min_{i=1,2,\cdots,n}|\,u_i\,| \tag{15}$$

式中：sign(·)为符号函数；min(·)表示返回最小值。因此，有

$$\gamma_{j,i,k}\approx\left(\prod_{l=1}^{M}\mathrm{sign}(L_r(v_{i,g_{k,l}}\,|\,c_{i,g_{k,l}}))\right)\cdot\min_{l=1,2,\cdots,M}|\,L_{\mathrm{r}}(v_{i,g_{k,l}}\,|\,c_{i,g_{k,l}})\,| \tag{16}$$

将式(16)计算出的 $\gamma_{j,i,k}$代入式(13)，即可求得式(9)成立的条件概率。然而，上述过程涉及指数运算，仍然比较复杂。为了降低运算量，计算 $\Gamma_{j,i}$的对数似然比为

$$L_{\mathrm{r}}(\Gamma_{j,i})=\ln\left(\frac{\Gamma_{j,i}}{1-\Gamma_{j,i}}\right)=\sum_{k=1}^{m}\gamma_{j,i,k}-\ln\left(\prod_{k=1}^{m}(1+\mathrm{e}^{\gamma_{j,i,k}})-\exp\left(\sum_{k=1}^{m}\gamma_{j,i,k}\right)\right)\approx\sum_{k=1}^{m}\gamma_{j,i,k} \tag{17}$$

经分析可知，当 α^j 为码字 $\boldsymbol{v}_i$ 的码根时，$\gamma_{j,i,k}$取值以很大的概率大于 0，反之，则 $\gamma_{j,i,k}$可能为正，也可能为负。因此，$L_{\mathrm{r}}(\Gamma_{j,i})$越大，$\alpha^j$ 为 $\boldsymbol{v}_i$ 码根的可能性越大。为了避免负值对后续对数运算带来影响，仅取 $\gamma_{j,i,k}$中的正值。由于校验向量不可能为全 0 向量，因此若 $\boldsymbol{h}_{j,k}=\boldsymbol{0}$，则也应排除。最终，令 $\boldsymbol{\Theta}_{j,i}=\{k\,|\,1\leqslant k\leqslant m$，且 $\gamma_{j,i,k}>0,\boldsymbol{h}_{j,k}\neq\boldsymbol{0}\}$，则 α^j 为 $\boldsymbol{v}_i$ 码根的可靠性系数可表示为

$$\theta_{j,i}=\sum_{k\in\boldsymbol{\Theta}_{j,i}}\gamma_{j,i,k} \tag{18}$$

计算所有 α^j($1\leqslant j\leqslant n-1$)在 N 个码字下的 $\theta_{j,i}$，则式(4)可表示为

$$p_j=\frac{\sum_{i=1}^{N}\theta_{j,i}}{\sum_{j=1}^{n-1}\sum_{i=1}^{N}\theta_{j,i}},\quad 1\leqslant j\leqslant n-1 \tag{19}$$

然后将式(19)代入式(5)计算 ΔH，其最大值处即对应正确码长。

3　生成多项式识别

在真实的本原多项式下，从 α 开始对应的连续公共码根(也即生成多项式的根)的数量也最多，为 $2t$ 个。以此为依据，完成本原多项式和生成多项式的联合识别。为了提升容错性，基于软判决序列，给出公共码根的具体判决门限。

根据上节分析，若 α^j 为 N 个码字多项式的公共根，则其可靠性统计量可表示为

$$\lambda_j = \sum_{i=1}^{N}\sum_{k=1}^{m}\gamma_{j,i,k} = \sum_{k=1}^{m}\sum_{i=1}^{N}\gamma_{j,i,k} \tag{20}$$

建立二元假设 $H_0:\boldsymbol{h}_j \notin \boldsymbol{H}, H_1:\boldsymbol{h}_j \in \boldsymbol{H}$。对 H_0、H_1 进行检验，需要先知道 λ_j 在两种假设下的分布。根据式(16)，设 $X = \prod_{l=1}^{M}\mathrm{sign}(L_r(v_{i,g_{k,l}}|c_{i,g_{k,l}}))$，$Y = \min_{l=1,2,\cdots,M}|L_r(v_{i,g_{k,l}}|c_{i,g_{k,l}})|$，$\boldsymbol{V}_{i,k} = [v_{i,g_{k,1}}, v_{i,g_{k,2}}, \cdots, v_{i,g_{k,M}}]$，$\boldsymbol{C}_{i,k} = [c_{i,g_{k,1}}, c_{i,g_{k,2}}, \cdots, c_{i,g_{k,M}}]$。由文献[15]可知，在 H_0 假设下，x 等概率的取值为 1 和 -1，X、Y 相互独立，令符号 $E\{\cdot\}$ 表示期望，则此时 $\gamma_{j,i,k}$ 的均值和方差分别为

$$m_{k,0} = E\{\gamma_{j,i,k}|H_0\} = E\{XY|H_0\} = E\{X|H_0\}E\{Y|H_0\} = 0 \tag{21}$$

$$\sigma_{k,0}^2 = E\{\gamma_{j,i,k}^2|H_0\} = E\{Y^2\} = \frac{4}{\sigma^4}E\{\min_{l=1,2,\cdots,M}|c_{i,g_{k,l}}|^2\} \tag{22}$$

在 H_1 假设下，$\gamma_{j,i,k}$ 的均值为

$$m_{k,1} = E\{\gamma_{j,i,k}|H_1\} = E\{Y|H_1, X=1\}\cdot P_r(X=1|H_1) - E\{Y|H_1, X=-1\}\cdot P_r(X=-1|H_1) \tag{23}$$

式中：$\{X=1\}$ 表示 $X=1$ 时，$\boldsymbol{V}_{i,k}$ 中无错误比特或有偶数个错误比特；$\{X=-1\}$ 表示 $X=-1$ 时，$\boldsymbol{V}_{i,k}$ 中有奇数个错误比特。令 p_e 表示误码率，则

$$P_r(X=1|H_1) = \sum_{i=0}^{\lfloor M/2\rfloor} C_M^{2i} p_e^{2i}(1-p_e)^{M-2i} \tag{24}$$

$$P_r(X=-1|H_1) = 1 - P_r(X=1|H_1) \tag{25}$$

设 B_1 表示 $\boldsymbol{C}_{i,k}$ 中没有或有偶数个软判决值于小 0，B_2 表示 $\boldsymbol{C}_{i,k}$ 中有奇数个软判决值小于 0。根据 X 的定义，B_1 成立时，$X=1$；B_2 成立时，$X=-1$。因此，在 H_1 假设下，$X=1$ 和 $X=-1$ 两种情况对应 Y 的期望可分别表示为

$$E\{Y|H_1, X=1\} = \frac{2}{\sigma^2}E\{\min_{l=1,2,\cdots,M}|c_{i,g_{k,l}}||B_1\} \tag{26}$$

$$E\{Y|H_1, X=-1\} = \frac{2}{\sigma^2}E\{\min_{l=1,2,\cdots,M}|c_{i,g_{k,l}}||B_2\} \tag{27}$$

将式(24)～(27)代入式(23)，可计算 $\gamma_{j,i,k}$ 的均值 $m_{k,1}$，从而 $\gamma_{j,i,k}$ 的方差为

$$\sigma_{k,1}^2 = E\{\gamma_{j,i,k}^2|H_1\} - m_{k,1}^2 = \frac{4}{\sigma^4}E\{\min_{l=1,2,\cdots,M}|c_{i,g_{k,l}}|^2\} - m_{k,1}^2 \tag{28}$$

当 N 足够大时，$\sum_{i=1}^{N}\gamma_{j,i,k}$ 在两种假设下均趋于高斯分布，此时 λ_j 等价于 m 个独立高斯分布的线性组合。令 $\sigma_{j,0}^2 = N\sum_{k=1}^{m}\sigma_{k,0}^2$，$m_{j,1} = N\sum_{k=1}^{m}m_{k,1}$，$\sigma_{j,1}^2 = N\sum_{k=1}^{m}\sigma_{k,1}^2$，易知 λ_j 在两种假设下的概率密度分别为

$$p(\lambda_j|H_0) = \frac{(2\pi)^{-1/2}}{\sigma_{j,0}}\exp\left(-\frac{\lambda_j^2}{2\sigma_{j,0}^2}\right) \tag{29}$$

$$p(\lambda_j|H_1) = \frac{(2\pi)^{-1/2}}{\sigma_{j,1}}\exp\left(-\frac{(\lambda_j - m_{j,1})^2}{2\sigma_{j,1}^2}\right) \tag{30}$$

定义 T_j 为该统计检测下的判决门限，则其对应的虚警概率为 $P_{fa} = \int_{T_j}^{\infty}p(\lambda_j|H_0)\mathrm{d}\lambda_j$。因此，令 $\Phi^{-1}(\cdot)$ 表示标准高斯分布的累积分布函数的反函数，则在规定的虚警概率 P_{fa} 下，判决门限为

$$T_j = \sigma_{j,0}\Phi^{-1}(1-P_{fa}) \tag{31}$$

此时，若计算得到的 $\lambda_j > T_j$，则 α^j 为公共码根。

根据文献[16]，$\boldsymbol{F}_g(2^m)$ 上首系数为 1 的 m 次本原多项式个数为 $\phi(2^m-1)/m$，其中 $\phi(\cdot)$ 称为欧拉函数。在每个本原多项式下，从 α 开始依次对 α^j 计算 λ_j 值，并按判决门限进行判定。每判定通过一个元素后，就根据如下定理减少后续计算量。

定理 1[17] 设 $f(x)$ 是一个以 $\boldsymbol{F}_g(2)$ 中的元素为系数的多项式，β 是 $\boldsymbol{F}_g(2)$ 的扩域 $\boldsymbol{F}_g(2^m)$ 中的一个元素，若 β 是 $f(x)$ 的一个根，则对任意 $d \geqslant 0$，β^{2^d} 也是 $f(x)$ 的根。

元素 β^{2^d} 称为 β 的共轭，具有相同的最小多项式。因此，在判定公共码根时，可以进行共轭分组，避免重复判定。例如，如果 α 通过判定，则共轭分组 $\boldsymbol{\Omega}_1 = \{\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{i-1}} \bmod \alpha^{2^m-1}\}$ 均通过判定。然后，从上一个分组中未出现的 α 最小次幂开始，重复上述判定步骤。以此类推，直到找到最多的连续公共码根个数，此时即对应正确的本原多项式。

在确定正确的本原多项式和最多的连续公共码根后，令已通过判定的所有共轭分组组成的集合为 $\boldsymbol{\Omega}$，则生成多项式为

$$g(x) = \prod_{\alpha^i \in \boldsymbol{\Omega}}(x + \alpha^i) \tag{32}$$

综合以上分析，软判决下本原 BCH 码盲识别(SDBR)方法流程如图 1 所示。

4 仿真结果与分析

仿真分为 3 部分，首先分别对码长和生成多项

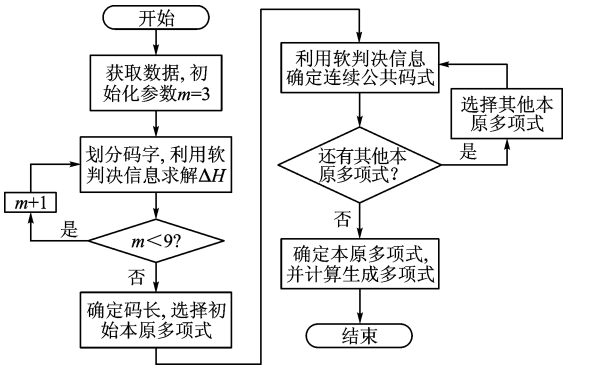


图 1　软判决下本原 BCH 码盲识别方法流程图

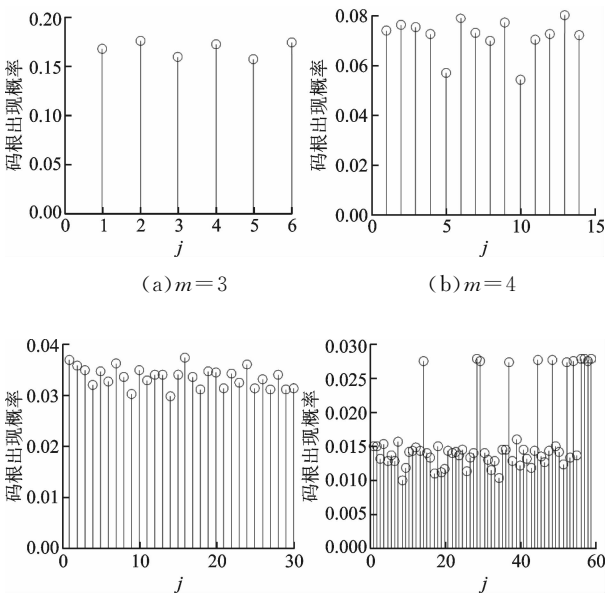
式识别方法进行验证，确定其可行性，然后研究了所提 SDBR 方法的识别性能，并与传统方法进行了对比。

4.1　码长识别

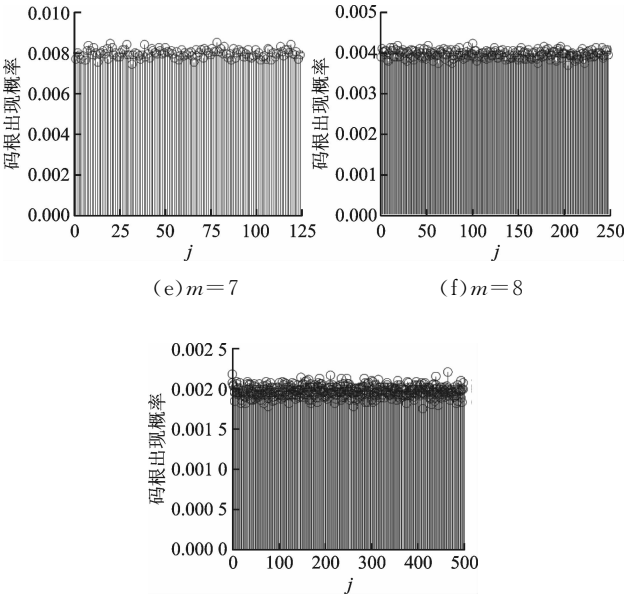
选取(63，51)BCH 码进行研究，生成多项式取 $g(x)=1+x^2+x^4+x^7+x^8+x^9+x^{12}$，对应本原多项式为 $p(x)=1+x^5+x^6$。采用 AWGN 信道和 BPSK 调制方式，信噪比取 7 dB，码字个数 $N=200$。按本文方法依次对 $m(3\leqslant m\leqslant 9)$进行遍历和验证，本原多项式分别取 $p(x)=1+x+x^3$、$p(x)=1+x+x^4$、$p(x)=1+x^2+x^5$、$p(x)=1+x+x^6$、$p(x)=1+x+x^7$、$p(x)=1+x+x^2+x^3+x^4+x^8$ 和 $p(x)=1+x^4+x^9$。不同 m 值下码根出现概率如图 2 所示，最终识别结果如图 3 所示。可以看出，$m=6$，即码长 $n=63$ 时，ΔH 值最大，识别结果正确。

4.2　生成多项式识别

根据欧拉函数，$m=6$ 时对应 6 个本原多项式 $p_1(x)=1+x+x^6$、$p_2(x)=1+x+x^3+x^4+x^6$、$p_3(x)=1+x^5+x^6$、$p_4(x)=1+x+x^2+x^5+x^6$、$p_5(x)=1+x^2+x^3+x^5+x^6$、$p_6(x)=1+x+x^4+x^5+x^6$。首先从本原元 α 开始，对不同本原多项式进行公共码根判定，虚警概率取为 10^{-4}，λ_1 和其判决门限 T_1 如表 1 所示(因式(3)中的常数项 $2/\sigma^2$ 仅影响 λ_j 和 T_j 的绝对数值，并不影响判决，因此为了计算简便，忽略该项)。



(a)$m=3$　(b)$m=4$　(c)$m=5$　(d)$m=6$



(e)$m=7$　(f)$m=8$

(g)$m=9$

图 2　不同 m 值下码根出现概率

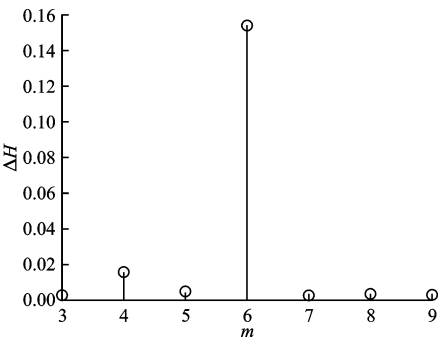


图 3　码长识别结果

表 1　公共码根 α 判定结果

本原多项式	可靠性统计量 λ_1	判决门限 T_1
$p_1(x)$	−43.4	80.5
$p_2(x)$	13.9	82.3
$p_3(x)$	705.7	78.4
$p_4(x)$	3.9	76.3
$p_5(x)$	−5.9	82.5
$p_6(x)$	−49.4	78.2

从表 1 中可以发现，对本原元 α 进行判定时，只

有 $p_3(x)$对应的 λ_1 大于门限值 T_1，其他 5 个本原多项式均不符合，故 $p_3(x)$为正确的本原多项式，与设定的仿真条件符合。确定共轭分组 $\boldsymbol{\Omega}_1=\{\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16},\alpha^{32}\}$为公共码根后，从 $\boldsymbol{\Omega}_1$ 中未出现的 α 最小次幂，即 α^3 开始继续判定。经计算，可靠性统计量 $\lambda_3=686.0$，判决门限 $T_3=81.5$，因此 α^3 为公共码根，对应共轭分组为 $\boldsymbol{\Omega}_2=\{\alpha^3,\alpha^6,\alpha^{12},\alpha^{24},\alpha^{48},\alpha^{33}\}$。继续上述步骤，求得 $\lambda_5=2.6$，$T_5=80.9$，α^5 无法通过判决。因此，连续公共码根为$\{\alpha,\alpha^2,\alpha^3,\alpha^4\}$，对应生成多项式为

$$g(x)=\prod_{\alpha^i\in\Omega}(x+\alpha^i)=1+x^2+x^4+x^7+x^8+x^9+x^{12} \tag{33}$$

至此，识别完成。

4.3 识别性能仿真

根据 BCH 码编码结构可知，码长越大，码率越高，对识别方法的容错性要求也越高。因此，选取(63,51)、(127,113)、(255,247)和(511,502) bit 这 4 种高码率的 BCH 码进行研究，在不同信噪比下进行 200 次蒙特卡洛仿真，不同码长下 BCH 码的识别率如图 4 所示。可以看出，在信噪比大于 7 dB 时，4 种 BCH 码的识别率均能达到 100%。因此，当码长更短、码率更低时，也同样能在相同条件下有效完成识别。

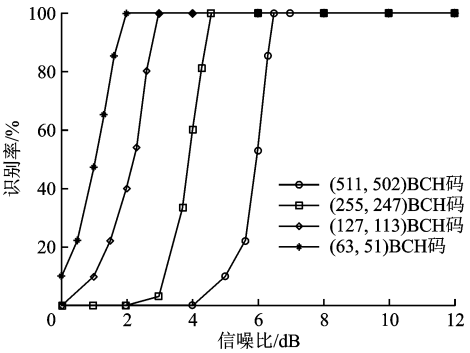


图 4 不同码长下本文方法的识别性能

将本文 SDBR 方法与文献[6]中的 RIDE 方法进行性能对比，在相同仿真条件下对(63,51)BCH 码进行识别。由于文献[6]中采用的是硬判决序列，因此为了统一，将其在不同误码率下识别结果转化到对应信噪比上。根据文献[13]，当 BPSK 调制用于 AWGN 信道，采用最优相干检测和二进制输出量化时，硬判决的误码率 $p_e=Q((2E_s/N_0)^{1/2})$，其中 E_s/N_0 表示信噪比，$Q(x)=(2\pi)^{-1/2}\int_x^{\infty}e^{-y^2/2}dy$ 是高斯统计的互补误差函数。最终，在不同信噪比下两种方法的对比结果如图 5 所示。可以看出，SDBR 方法在信噪比为 2 dB 时仍能有效完成识别，而 RIDE 方法在信噪比大于 3.8 dB 时才能达到 100%识别率，因此本文方法的容错性明显优于对比方法。

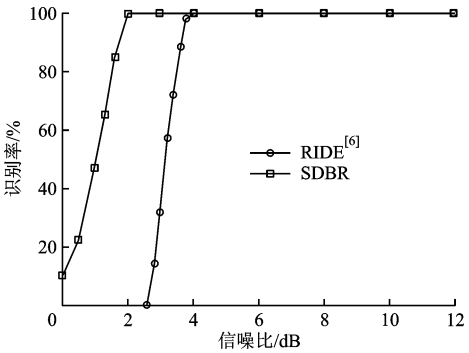


图 5 本文方法与文献[6]方法的识别性能对比

5 结束语

为了提升识别容错性能，本文提出了一种软判决下的二进制本原 BCH 码盲识别方法。首先根据待定码长对比特序列进行码字划分，并利用软判决信息计算其码根出现概率；然后引入 KL 散度来度量码根分布与均匀分布的距离，距离最大处即对应正确的码长；最后建立公共码根可靠性统计量，在不同本原多项式下对公共码根进行判定，利用连续公共码根的分布特性完成对本原多项式的识别，进而计算生成多项式。仿真结果表明，相比传统方法，本文方法的容错性能有了很大的提升。

参考文献：

[1] 王新梅，肖国镇. 纠错码：原理与方法 [M]. 修订版. 西安：西安电子科技大学出版社，2011：243.

[2] XIA T, WU H C. Joint blind frame synchronization and encoder identification for low-density parity-check codes [J]. IEEE Communication Letters, 2014, 18(2): 352-355.

[3] CHEN W G, WU G Q. Blind recognition of $(n-1)/n$ rate punctured convolutional encoders in a noisy environment [J]. Journal of Communications, 2015, 10(4): 260-267.

[4] BRINGER J, CHABANNE H. Code reverse engineering problem for identification codes [J]. IEEE Transactions on Information Theory, 2012, 58(4): 2406-2412.

[5] 王兰勋，李丹芳，汪洋. 二进制本原 BCH 码的参数盲识别 [J]. 河北大学学报(自然科学版)，2012，32(4)：416-420.

WANG Lanxun, LI Danfang, WANG Yang. Blind recognition of binary primitive BCH codes parameters [J]. Journal of Hebei University (Natural Science Edition), 2012, 41(6): 1166-1175.

[6] 杨晓静，闻年成. 基于码根信息差熵和码根统计的 BCH 码识别方法 [J]. 探测与控制学报，2010，32(3)：69-73.
YANG Xiaojing, WEN Niancheng. Recognition method of BCH codes based on roots information dispersion entropy and roots statistic [J]. Journal of Detection & Control, 2010, 32(3): 69-73.

[7] ZHOU J, HUANG Z P, SU S J, et al. Blind recognition of binary cyclic codes [J]. EURASIP Journal on Wireless Communication and Networking, 2013, 218: 1-17.

[8] 李歆昊，张旻. 基于码重分布与汉明距离的线性码盲识别方法 [J]. 探测与控制学报，2013，35(4)：68-73.
LI Xinhao, ZHANG Min. Linear code blind identification method based on code weight distribution and hamming distance [J]. Journal of Detection & Control, 2013, 35(4): 68-73.

[9] WU G, ZHANG B N, GUO D X, et al. Blind recognition of BCH codes in faster than-Nyquist signaling system [J]. Electronics Letters, 2016, 52(9): 716-718.

[10] 陈金杰，杨俊安. 一种对线性分组码编码参数的盲识别方法 [J]. 电路与系统学报，2013，18(2)：249-254.
CHEN Jinjie, YANG Junan. A method of blind recognition to coding parameters of linear block codes [J]. Journal of Circuits and Systems, 2013, 18(2): 249-254.

[11] ZRELLI G, MARAZIN M, RANNON E, et al. Blind identification of code word length for non-binary error-correcting codes in noisy transmission [J]. EURASIP Journal on Wireless Communication and Networking, 2015, 43: 1-16.

[12] 杨晓炜，甘露. 基于 Walsh-Hadamard 变换的线性分组码参数盲估计算法 [J]. 电子与信息学报，2012，34(7)：1642-1646.
YANG Xiaowei, GAN Lu. Blind estimation algorithm of the linear block codes parameters based on WHT [J]. Journal of Electronics & Information Technology, 2012, 34(7): 1642-1646.

[13] CHA S H. Comprehensive survey on distance/similarity measures between probability density functions [J]. International Journal of Mathematical and Methods in Applied Sciences, 2007, 4(1): 300-307.

[14] MOOSAVI R, LARSSON E G. A fast scheme for blind identification of channel codes [C]// 54th Annual IEEE Global Telecommunications Conference. Piscataway, NJ, USA: IEEE, 2011: 6133507.

[15] MOOSAVI R, LARSSON E G. Fast blind recognition of channel codes [J]. IEEE Transactions on Communications, 2013, 62(5): 1393-1405.

[16] 陈鲁生，沈世镒. 编码理论基础 [M]. 北京：高等教育出版社，2005：37-58.

[17] LIN S, COSTELLO D J. Error control coding [M]. 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2005: 130-136.

（编辑　刘杨）

（上接第 34 页）

[17] GAO Haiyan, CAI Yuanli. Nonlinear disturbance observer-based model predictive control for a generic hypersonic vehicle [J]. Proceedings of the Institution of Mechanical Engineers: Part I Journal of Systems and Control Engineering, 2016, 230(1): 3-12.

[18] BUMROONGSRI P, KHEAWHOM S. An off-line robust MPC algorithm for uncertain polytopic discrete-time systems using polyhedral invariant sets [J]. Journal of Process Control, 2012, 22(6): 975-983.

[19] 王明昊，刘刚，赵鹏涛，等. 多胞约束 LPV 系统多面体不变集 RMPC 算法 [J]. 控制与决策，2013，28(11)：1661-1666.
WANG Minghao, LIU Gang, ZHAO Pengtao, et al. RMPC algorithm for polytopic constrained LPV systems using polyhedral invariant sets [J]. Control and Decision, 2013, 28(11): 1661-1666.

[20] WU Huaining, LIU Zhiyong, GUO Lei. Robust-gain fuzzy disturbance observer-based control design with adaptive bounding for a hypersonic vehicle [J]. IEEE Transactions on Fuzzy Systems, 2014, 22(6): 1401-1412.

（编辑　刘杨）