基于平均余弦符合度下的本原 BCH 码盲识别

吴昭军[1]，张立民[1]，钟兆根[2]，龙玉峰[3]

（1. 海军航空大学信息融合研究所，山东 烟台 264001；2. 海军航空大学航空基础学院，山东 烟台 264001；
3. 海军航空大学 310 教研室，山东 烟台 264001）

摘 要：为克服现有 BCH 码识别算法在低信噪比下适应性差的缺点，提出了一种基于平均余弦符合度的识别算法。首先遍历可能的码长值以及 m 级本原多项式域，进行初始码根校验匹配，从而完成码长识别；然后在识别出码长前提下，遍历 m 级本原多项式下的 GF(2^m)域，其最强纠错能力的本原多项式即为 GF(2^m)域生成多项式；最后求取所有连续码根最小多项式对应的最小公倍式，完成编码生成多项式识别。在校验匹配过程中，引入了平均余弦符合度统计量，基于软判决下符合度的统计特性以及最小错误判决准则求解出最优门限，从而实现本原 BCH 码参数快速识别。仿真结果表明，推导的符合度统计特性与实际情况一致，所提算法能在低信噪比下有效完成参数识别，同时具有较好的低信噪比适应能力，在信噪比为 5 dB，码长为 511 的条件下，能够完成参数的可靠识别，与目前算法相比，所提算法性能优于现有的软判决算法，且比硬判决算法提升 1~3.5 dB。

关键词：本原 BCH 码；平均余弦符合度；软判决；最小错误判决准则；识别

中图分类号：TN911.7

文献标识码：A

doi:10.11959/j.issn.1000−436x.2020022

Blind recognition of primitive BCH code based on average cosine conformity

WU Zhaojun[1], ZHANG Limin[1], ZHONG Zhaogen[2], LONG Yufeng[3]

1. The Institute of Information Fusion, Naval Aviation University, Yantai 264001, China
2. The School of Basis Aviation, Naval Aviation University, Yantai 264001, China
3. 310 Department, Naval Aviation University, Yantai 264001, China

Abstract: In order to overcome the poor performance of existing algorithms for recognition of BCH code in low signal-to-noise ratio (SNR), a recognition algorithm based on average cosine conformity was proposed. Firstly, by traversing the possible values of code length and m-level primitive polynomial fields, the code length was identified by matching the initial code roots. Secondly, on the premise of recognizing the code length, the GF(2^m) domain was traversed under the m-level primitive polynomial and the primitive polynomial with the strongest error-correcting ability was the generator polynomial for the domain. Finally, the minimum common multiple corresponding to the minimum polynomial of code roots was obtained, and the BCH code generator polynomial was recognized. In checking matching, the statistic of average cosine conformity was introduced. The optimal threshold was solved based on the minimum error decision criterion and distribution of the statistic to realize the fast identification of the BCH. The simulation results show that the deduced statistical characteristics are consistent with the actual situation, and the proposed algorithm can achieve reliable recognition under SNR of 5 dB and code length of 511. Comparing with existing algorithms, the performance of the proposed algorithm is better than that of the existing soft-decision algorithm and 1~3.5 dB better than that of the hard-decision algorithms.

Key words: primitive BCH code, average cosine conformity, soft decision, minimum error decision criterion, recognition

收稿日期：2019–08–22；**修回日期**：2019–12–05

通信作者：钟兆根，zhongzhaogen@163.com

基金项目：国家自然科学基金资助项目（No.91538201）；泰山学者工程专项经费资助项目（No.ts201511020）

Foundation Items: The National Natural Science Foundation of China (No.91538201), Taishan Scholar Special Foundation (No.ts201511020)

1 引言

为了提高数字通信的可靠性，信道编码技术广泛应用于现代通信系统中。BCH码以其严格的代数结构而具有很强的纠错能力，从而成为循环码中一个重要的子类。BCH码在中短码长条件下，其性能接近于理论值，且编码译码计算复杂度低，这些优点使其广泛应用于卫星通信、微波通信以及与其他编码方式的级联过程中。在非合作通信领域，如果能够在恶劣信道环境下，利用截获的比特流完成BCH码的有效识别，则对于信源获取、密码协议分析具有重要的意义[1]。

目前，具有较强容错能力的编码识别算法主要集中于卷积码[2-3]、Turbo码[4]等，而针对BCH码的识别，大部分算法从BCH码的定义以及代数结构出发，利用比特流序列进行参数识别，其容错性能不足。文献[5-6]从BCH码定义出发，利用码字一定含有生成多项式因子这一性质，采用欧几里得算法，完成BCH码生成多项式识别，虽然这种算法具有较低的计算复杂度，但是该算法不具有容错性。文献[7-8]将BCH码等价于特殊的线性分组码，采用改进的高斯消元法识别BCH码码长以及校验矩阵，虽然具有一定的容错性能，但是当码长增加时，算法计算复杂度将急剧增加。由于BCH码生成多项式由扩域中某些元素的最小多项式构成，文献[9]直接对扩域中元素最小多项式进行校验匹配，从而完成码长以及生成多项式识别，但是当扩域中元素较多时，其虚警或是漏警概率会不可避免地增加，同时也不能完成本原多项式的识别。文献[10]利用码长为n的码字一定能够整除多项式x^n+1的特点，对多项式x^n+1进行因式分解，然后对因子进行校验匹配，同时完成码长以及生成多项式识别，该算法虽然具有较高的计算效率，但是随着码长的增加，因子的误判概率会急剧增加。为了提高算法的容错性能，文献[11]利用随机码字与BCH码码根概率分布不同，提出了基于码根信息差熵（RIDE, root information difference entropy）算法，该算法在短码情况下具有较好的识别性能，但是在中长码情况下还有待改进。文献[12-13]在RIDE算法的基础上，深入分析了随机码字与BCH码概率分布规律，通过设定判决门限完成码长以及具有最大连续码根数目的本原多项式，最终完成生成多项式的识别，该算法相比于RIDE方法容错性能得到了一定的提高。以上算法仅仅适用于二进制硬判决序列，这种硬判决序列不可避免地造成来自信道的信息损失。为了克服这一缺陷，文献[14]首次利用软判决信息建立起码字多项式的码根可靠性系数，同样利用码根分布概率分布识别出码长、本原多项式以及生成多项式，与以往算法相比，该方法识别性能得到较大的提高，但是在采用软判决度量过程中，算法采用了简单的近似处理，其性能在低信噪比条件下具有较大的性能损失。从现有的文献来看，目前BCH码识别的算法还需要进一步提高在恶劣信道环境下的容错能力。

针对现有算法的不足，本文提出了一种新的识别算法。该算法首先遍历BCH码可能的码长以及构成扩域的本原多项式，当扩域中的本原元满足校验关系时，遍历的码长即为本原BCH码码长；然后在该码长下，遍历域上所有的本原多项式，具有最大连续码根数目的本原多项式即为域生成多项式，同时连续码根最小多项式对应的最小公倍式即为本原BCH码生成多项式。为了直接利用截获码元的软判决序列，在校验匹配过程中，引入平均余弦符合度概念，利用随机码字与本原BCH码字在平均余弦符合度下的统计特性差异，设定判决门限，能够在低信噪比下快速完成码长以及码根的判决。仿真结果表明，与以往方法相比，本文提出的算法在低信噪比环境下的适应能力具有较大的提升。

2 本原BCH码原理及其性质

本原BCH码是实际工程中应用较多的一种编码，凭借较强的纠错能力被广泛应用于数字通信系统中，其定义如下。

定义 1[15] 给定任一有限域GF(q)以及扩域GF(q^m)，其中q为素数，则称GF(q)上码长为n的循环码设计距离是δ的BCH码，其生成多项式是

$$g(x)=\mathrm{lcm}\left(\phi_m(x),\phi_{m+1}(x),\cdots,\phi_{m+\delta-2}(x)\right) \quad (1)$$

其中，$m\geqslant 1$，$\mathrm{lcm}(\cdot)$表示取多项式的最小公倍式，$\phi_k(x)\ (m\leqslant k\leqslant m+\delta-2)$表示GF($q^m$)中元素$\alpha^k$的最小多项式。

当定义1中$q=2$，δ=$2t-1$时，BCH码变为码长为2^m-1、能够纠正t个错误的本原BCH码。在实际工程中，本原BCH码是中短码，其码长范围为$7\sim 511$（即$3\leqslant m\leqslant 9$）。

由本原 BCH 码定义可知，其生成多项式 $g(x)$ 以 GF(q^m)域中连续幂次 $\alpha,\alpha^2,\cdots,\alpha^{2t}$ 为根，故其码字生成多项式也一定以这些元素为根。设截获的本原 BCH 码码字数目为 N，第 k 个 BCH 码码字多项式为

$$c_k(x)=c_{k,0}+c_{k,1}x+\cdots+c_{k,n-1}x^{n-1} \tag{2}$$

其中，n 为 BCH 码码长。

将第 i 个码根代入式(2)中得到

$$c_k(\alpha^i)=c_{k,0}+c_{k,1}\alpha^i+c_{k,2}\alpha^{2i}+\cdots+c_{k,n-1}\alpha^{(n-1)i}=0 \tag{3}$$

其中，$1\leqslant i\leqslant 2t$，$1\leqslant k\leqslant N$。

将式(3)展开，进一步得到

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

式(4)中涉及的加法与乘法都是在 GF(2^m)域中的加法与乘法，后面不再单独说明，涉及码元之间的运算都是在其有限域中进行。在有限域中存在定理 1。

定理 1[15]　设 $f(x)$ 是 GF(q)上的一个多项式，β 是 GF(q)的扩域 GF(q^m)中的一个元素。如果 β 是 $f(x)$ 的一个根，那么对于任意非负正整数 t，β^{q^t} 是 $f(x)$ 的一个根。

由式(4)以及定理 1 可得本原 BCH 码校验矩阵 $\boldsymbol{H}$ 为

$$\boldsymbol{H}=\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t-1} & \alpha^{4t-2} & \cdots & \alpha^{(2t-1)(n-1)} \end{bmatrix} \tag{5}$$

对于本原 BCH 码的识别，需要澄清的参数包括 BCH 码码长、域本原多项式以及生成多项式三部分。需要注意的是，在实际通信系统中，为了便于数据帧同步，在每一数据帧头会添加 8 位或是 16 位的同步码，所以本文并未将码字同步作为研究重点，重点解决的则是如何直接利用来源信道的软判决信息，完成上述参数的识别。

3　本原 BCH 码识别模型建立

3.1　基于平均余弦符合度下的 BCH 码识别

由式(4)可知，本原 BCH 码码字与 GF(2^m)上元素满足校验关系，不妨取式(4)中校验矩阵第 i 列单独进行研究，即

$$\begin{bmatrix} c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ c_{2,0} & c_{2,1} & \cdots & c_{2,n-1} \\ \vdots & \vdots & \cdots & \vdots \\ c_{N,0} & c_{N,1} & \cdots & c_{N,n-1} \end{bmatrix}\begin{bmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(n-1)i} \end{bmatrix}=\mathbf{0} \tag{6}$$

其中，$1\leqslant i\leqslant 2t$。

由于式(6)中存在 GF(2^m)中的元素，而参与校验的序列存在于 GF(2)域中，在 2 种不同的域中，元素之间的运算并不方便，此时考虑将校验关系等价于二元域 GF(2) 中，由于元素 α^{ki} $(1\leqslant i\leqslant 2t,0\leqslant k\leqslant n-1)$，在 GF($2^m$)中可以表示为 m 维向量的形式，即

$$\boldsymbol{\alpha}^{ki}=\left[h_1^{ki},h_2^{ki},\cdots,h_m^{ki}\right] \tag{7}$$

其中，向量中元素 $h_j^{ki}\in$GF(2)，$1\leqslant j\leqslant m$。

联立式(6)与式(7)可知

$$\begin{bmatrix} c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ c_{2,0} & c_{2,1} & \cdots & c_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N,0} & c_{N,1} & \cdots & c_{N,n-1} \end{bmatrix}\begin{bmatrix} h_1^0 & h_2^0 & \cdots & h_m^0 \\ h_1^i & h_2^i & \cdots & h_m^i \\ h_1^{2i} & h_2^{2i} & \cdots & h_m^{2i} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{(n-1)i} & h_2^{(n-1)i} & \cdots & h_m^{(n-1)i} \end{bmatrix}=\mathbf{0} \tag{8}$$

其中，$1\leqslant i\leqslant 2t$。

这样式(8)就将扩域中的校验关系统一于二元域中的校验关系。当遍历的 BCH 码码长、域本原多项式正确时，BCH 码字与生成多项式根一定满足式(9)的校验约束关系。传统方法主要利用硬判决序列，通过遍历码长、本原多项式以及码根，在扩域中进行校验匹配，这种算法计算复杂度高，同时在恶劣信道环境下实用性不好。本文直接利用截获的软判决序列，最大可能地保留来自信道环境的信息，实现参数的识别。

为了利用软判决序列度量式(8)编码约束关系成立的可能性大小，首先引入余弦符合度[16]的概念，为了方便说明，将式(8)中校验矩阵第 i 列单独列出来讨论，即

$$\sum_{l=0}^{n-1} c_{k,l} h_j^{li} = 0 \tag{9}$$

其中，$1 \leqslant k \leqslant N, 1 \leqslant i \leqslant 2t, 1 \leqslant j \leqslant m$。

设截获到的软判决序列为 $x_{k,0}, x_{k,1}, \cdots, x_{k,n-1}$，对应于发送的信息码元序列为 $c_{k,0}, c_{k,1}, \cdots, c_{k,n-1}$。记在截获软判决信息为 $x_{k,l}$ 条件下，码元 $c_{k,l}$ 取值为 1 的概率为 $P\left(c_{k,l} \mid x_{k,l}\right)$，则余弦符合度的定义为

$$F_k^{i,j} = \prod_{l=0}^{n-1} \cos\left(\pi P\left(c_{k,l} \mid x_{k,l}\right) h_j^{li}\right) \tag{10}$$

由余弦符合度的定义可知，当 $P\left(c_{k,l} \mid x_{k,l}\right) h_j^{li}$<0.5 时，对应于 $c_{k,l} h_j^{li}$ 取 0 的可能性更大，余弦函数将其映射为正值；反之，当 $P\left(c_{k,l} \mid x_{k,l}\right) h_j^{li}$>0.5 时，对应于 $c_{k,l} h_j^{li}$ 取 1 的可能性更大，余弦函数将其映射为负值。当校验关系成立时，式(9)中参与模 2 加元素等于 1 的个数为偶数个，此时对应于式(10)乘积结果 $F_k^{i,j}$ 一定为正；当校验关系不成立时，$F_k^{i,j}$ 为负。下面，进一步推导后验概率 $P\left(c_{k,l} \mid x_{k,l}\right)$ 的计算方法。

假设信号调制方式为 BPSK，信号幅度为 A，噪声环境为方差为 σ^2、均值为 0 的高斯白噪声，此时定义信噪比为

$$\mathrm{SNR} = 10\lg\left(\frac{A^2}{2\sigma^2}\right) \tag{11}$$

当发送的码元为 $c_{k,l}$，对应于截获软判决为 $x_{k,l}$，则 $x_{k,l}$ 的条件概率密度函数为

$$p\left(x_{k,l} \mid c_{k,l} = 1\right) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{\frac{-\left(x_{k,l} - A\right)^2}{\left(2\sigma^2\right)}} \tag{12}$$

$$p\left(x_{k,l} \mid c_{k,l} = 0\right) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{\frac{-\left(x_{k,l} + A\right)^2}{\left(2\sigma^2\right)}} \tag{13}$$

由贝叶斯公式可知

$$P\left(c_{k,l} \mid x_{k,l}\right) = \frac{p\left(x_{k,l} \mid c_{k,l} = 1\right) P\left(c_{k,l} = 1\right)}{p\left(x_{k,l}\right)} \tag{14}$$

将分母用全概率公式展开，得到

$$P\left(c_{k,l} \mid x_{k,l}\right) = \frac{p\left(x_{k,l} \mid c_{k,l} = 1\right) P\left(c_{k,l} = 1\right)}{p\left(x_{k,l} \mid c_{k,l} = 0\right) P\left(c_{k,l} = 0\right) + p\left(x_{k,l} \mid c_{k,l} = 1\right) P\left(c_{k,l} = 1\right)} \tag{15}$$

在没有先验信息的条件下，$P\left(c_{k,l} = 0\right) = P\left(c_{k,l}\right) = 0.5$，联立式(12)~式(15)得到

$$P\left(c_{k,l} \mid x_{k,l}\right) = \frac{\mathrm{e}^{\frac{2Ax_{k,l}}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax_{k,l}}{\sigma^2}} + 1} \tag{16}$$

将式(16)代入式(10)中，得到余弦符合度的计算方法为

$$F_k^{i,j} = \prod_{l=0}^{n-1} \cos\left(\pi \frac{\mathrm{e}^{\frac{2Ax_{k,l}}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax_{k,l}}{\sigma^2}} + 1} h_j^{li}\right) \tag{17}$$

由式(17)可知，当校验关系成立时，信噪比越大，$F_k^{i,j}$ 越趋近 1；反之，$F_k^{i,j}$ 越接近–1。综合考虑所有的编码约束关系，将 $F_k^{i,j}$ 取统计平均，得到平均余弦符合度为

$$\overline{F}_i = \frac{1}{mN} \sum_{k=1}^{N} \sum_{j=1}^{m} F_k^{i,j} \tag{18}$$

其中，$1 \leqslant i \leqslant 2t$。

当参数估计正确时，所有的码字都满足式(8)，此时平均余弦符合度 $\overline{F}_i$ 一定大于 0，且信噪比越大，越接近 1；当参数估计不正确时，码字为随机序列，编码方程成立概率为 0.5，$\overline{F}_i$ 值一定在 0 附近徘徊。此时利用二者的统计特性不同，设置最优的判决门限，即可完成本原 BCH 码参数的可靠识别。下一步重点研究 $\overline{F}_i$ 的统计特性，为门限计算准备条件。

3.2 最小错误判决准则的门限推导

由 3.1 节可知，利用平均余弦符合度的统计特性，合理设定判决门限是完成本原 BCH 码参数识别的前提条件，首先针对 $F_k^{i,j}$ 的统计特性进行研究。

记式(8)中矩阵第 j 列为 $\boldsymbol{h}_{i,l} = \left[h_l^0, h_l^i, \cdots, h_l^{(n-1)i}\right]^{\mathrm{T}}$，设其中元素等于 1 的个数为 $w_{i,l}$，元素等于 1 的集合为 $\boldsymbol{h}'_{i,l} = \left[h_l^{l_1 i}, h_l^{l_2 i}, \cdots, h_l^{l_{w_{i,l}} i}\right]^{\mathrm{T}}$，对应于参与校验的码元为 $\left[c_{k,m_1}, c_{k,m_2}, \cdots, c_{k,m_{w_l}}\right]$。

首先，讨论当参数正确时，校验关系成立，此时参与校验的码元等于 1 的元素个数一定为偶数，所有的可能情况为

$$S_{1,i,l}=\sum_{j=0}^{\left\lfloor\frac{w_{i,l}}{2}\right\rfloor}\mathrm{C}_{w_{i,l}}^{2j} \tag{19}$$

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

此时，利用均值与方差的定义，对于每一种情况计算均值与方差，并进行统计平均，得到在校验关系成立下的均值与方差分别为

$$u_{1,i,k,l}=\sum_{j=0}^{\left\lfloor\frac{w_{i,l}}{2}\right\rfloor}\frac{\mathrm{C}_{w_{i,l}}^{2j}}{S_{1,i,l}}\left(\int_{-\infty}^{\infty}\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)p\left(x\mid c=1\right)\mathrm{d}x\right)^{2j}\cdot$$

$$\left(\int_{-\infty}^{\infty}\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)p\left(x\mid c=0\right)\mathrm{d}x\right)^{w_{i,l}-2j} \tag{20}$$

$$\sigma_{1,i,k,l}^2=\sum_{j=0}^{\left\lfloor\frac{w_{i,l}}{2}\right\rfloor}\frac{\mathrm{C}_{w_{i,l}}^{2j}}{S_{1,i,l}}\left(\int_{-\infty}^{\infty}\left(\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)\right)^2p\left(x\mid c=1\right)\mathrm{d}x\right)^{2j}\cdot$$

$$\left(\int_{-\infty}^{\infty}\left(\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)\right)^2p\left(x\mid c=0\right)\mathrm{d}x\right)^{w_{i,l}-2j}-u_{1,i,k,l}^2 \tag{21}$$

由于式(8)中校验列码重 $w_{i,l}(1\leqslant i\leqslant 2t,\ 1\leqslant l\leqslant m)$ 可能不一定相等，此时同样需要将 $u_{1,i,k,l}$ 与 $\sigma_{1,i,k,l}^2$ 进行平均加权，得到 $u_{1,i,k}=\dfrac{1}{m}\sum_{l=1}^{m}u_{1,i,k,l}$，$\sigma_{1,i,k}^2=\dfrac{1}{m}\sum_{l=1}^{m}\sigma_{1,i,k,l}^2$。

下面进一步考虑参数不正确的情况，此时参与校验的码元等于 1 的元素个数不需要满足为偶数的约束，奇偶随机出现，所有可能的情况为

$$S_{0,i,l}=\sum_{j=0}^{w_{i,l}}\mathrm{C}_{w_{i,l}}^{j}=2^{w_{i,l}} \tag{22}$$

同样，计算每一种情况的均值与方差，然后进行统计平均加权，得到参数不正确情况下的均值与方差分别为

$$u_{0,i,k,l}=\sum_{j=0}^{w_{i,l}}\frac{\mathrm{C}_{w_{i,l}}^{j}}{S_{0,i,l}}\left(\int_{-\infty}^{\infty}\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)p\left(x\mid c=1\right)\mathrm{d}x\right)^{j}\cdot$$

$$\left(\int_{-\infty}^{\infty}\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)p\left(x\mid c=0\right)\mathrm{d}x\right)^{w_{i,l}-j} \tag{23}$$

$$\sigma_{0,i,k,l}^2=\sum_{j=0}^{w_{i,l}}\frac{\mathrm{C}_{w_{i,l}}^{j}}{S_{0,i,l}}\left(\int_{-\infty}^{\infty}\left(\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)\right)^2p\left(x\mid c=1\right)\mathrm{d}x\right)^{j}\cdot$$

$$\left(\int_{-\infty}^{\infty}\left(\cos\left(\frac{\pi\mathrm{e}^{\frac{2Ax}{\sigma^2}}}{\mathrm{e}^{\frac{2Ax}{\sigma^2}}+1}\right)\right)^2p\left(x\mid c=0\right)\mathrm{d}x\right)^{w_{i,l}-j}-u_{0,i,k,l}^2 \tag{24}$$

考虑到校验列码重不等的情况，将 $u_{0,i,k,l}$ 与 $\sigma_{0,i,k,l}^2$ 进行平均处理，得到 $u_{0,i,k}=\dfrac{1}{m}\sum_{l=1}^{m}u_{0,i,k,l}$，$\sigma_{0,i,k}^2=\dfrac{1}{m}\sum_{l=1}^{m}\sigma_{0,i,k,l}^2$。

由于式(20)~式(24)的积分表达式不存在解析解，此时可直接采用数值积分方式求解，不仅能够快速完成计算，还能达到很高的数值精度。

在明确 $F_k^{i,j}$ 的统计特性后，可以很容易地求出平均余弦符合度 $\overline{F}_i$ 的统计特性。首先列出以下 2 种检验假设。

H_0：遍历的域中元素 α^i 不是本原 BCH 码码根。

H_1：遍历的域中元素 α^i 是本原 BCH 码码根。

设截获的码块数目为 N，当 N 较大时，由大数定律可知，在假设条件 H_0 下，$\overline{F}_i$ 服从均值为 $u_{0,i,k}$、方差为 $\dfrac{\sigma_{0,i,k}^2}{N}$ 的高斯分布，记 $u_{0,i}=u_{0,i,k}$，$\sigma_{0,i}^2=\dfrac{\sigma_{0,i,k}^2}{N}$，则有

$$H_0:\overline{F}_i\sim\mathcal{N}\left(\mu_{0,i},\sigma_{0,i}^2\right) \tag{25}$$

同理，在假设条件 H_1 下，$\overline{F}_i$ 服从均值为 $u_{1,i,k}$、方差为 $\dfrac{\sigma_{1,i,k}^2}{N}$ 的高斯分布，记 $u_{1,i}=u_{1,i,k}$，$\sigma_{1,i}^2=\dfrac{\sigma_{1,i,k}^2}{N}$，则

$$H_1:\overline{F}_i\sim\mathcal{N}\left(\mu_{1,i},\sigma_{1,i}^2\right) \tag{26}$$

设判决门限为 Λ，则虚警概率 P_f 与漏警概率 P_a 分别为

$$P_\mathrm{f}=\int_{\Lambda_i}^{\infty}\frac{1}{\sqrt{2\pi}\sigma_{0,i}}\mathrm{e}^{\frac{-\left(x-\mu_{0,i}\right)^2}{\sigma_{0,i}^2}}\mathrm{d}x \tag{27}$$

$$P_\mathrm{a}=\int_{-\infty}^{\Lambda_i}\frac{1}{\sqrt{2\pi}\sigma_{1,i}}\mathrm{e}^{\frac{-\left(x-\mu_{1,i}\right)^2}{\sigma_{1,i}^2}}\mathrm{d}x \tag{28}$$

利用式(27)与式(28)计算最小错误判决概率为

$$P_{\mathrm{e}} = 0.5P_{\mathrm{f}} + 0.5P_{\mathrm{a}} \tag{29}$$

将 P_{e} 对门限 Λ_i 求导数，并令其等于 0，将方程化为一元二次方程形式

$$a\Lambda_i^2 + b\Lambda_i + c = 0 \tag{30}$$

其中，有

$$a = \left(\sigma_{0,i}^2 - \sigma_{1,i}^2\right) \tag{31}$$

$$b = -2\left(\sigma_{0,i}^2 u_{1,i} - \sigma_{1,i}^2 u_{0,i}\right) \tag{32}$$

$$c = \sigma_{0,i}^2 \mu_{1,i}^2 - \sigma_{1,i}^2 \mu_{0,i}^2 + \sigma_{0,i}^2 \sigma_{1,i}^2 \left(\ln\left(\sigma_{1,i}\right) - \ln\left(\sigma_{0,i}\right)\right) \tag{33}$$

求解得到最小错误判决门限为

$$\Lambda_i = \frac{\sigma_{0,i}^2 \mu_{1,i} - \sigma_{1,i}^2 \mu_{0,i} - \sigma_{0,i}\sigma_{1,i}\sqrt{\left(\mu_0 - \mu_1\right)^2 + \left(\sigma_{1,i}^2 - \sigma_{0,i}^2\right)\ln\dfrac{\sigma_{1,i}}{\sigma_{0,i}}}}{\left(\sigma_{0,i}^2 - \sigma_{1,i}^2\right)} \tag{34}$$

当求解出判决门限后，通过遍历本原 BCH 码码长、域本原生成多项式，然后判断域中元素 α^i 是否为码字的码根，从而确定出本原 BCH 码码长、域生成多项式以及 BCH 码生成多项式。

3.3 本原 BCH 码参数识别步骤

在实际工程中，BCH 码码长满足 $2^m - 1$（$3 \leqslant m \leqslant 9$），此时可以遍历 m 值以及 m 级本原多项式构成的扩域 GF(2^m)，判断域中元素 α 是否为码字的码根，从而确定出本原 BCH 码码长；然后再次遍历 m 级本原多项式构成的扩域，确定出从 α 开始具有最大连续码根的本原多项式，从而确定出域生成多项式以及码字生成多项式，算法具体步骤如下。

步骤 1 将截获的软判决序列按照式(16)转化为码元的条件概率序列。

步骤 2 设定 m 初值为 3，构造码长为 $2^m - 1$ 的 BCH 码码字，同时存储 m 级的所有本原多项式。

步骤 3 遍历步骤 2 中本原多项式，利用本原多项式构建扩域 GF(2^m)，利用域元素 α 按照式(8)构造校验矩阵。

步骤 4 计算判决门限 Λ_1，同时利用式(17)与式(18)计算平均余弦符合度 $\overline{F}_1$，若 $\overline{F}_1 \geqslant \Lambda_1$，则识别出本原 BCH 码码长；否则跳转至步骤 3，遍历下一个本原多项式，直到出现 $\overline{F}_1 \geqslant \Lambda_1$，否则 m=m+1，跳转至步骤 2，直到 $m > 9$。

步骤 5 再次遍历 m 级本原多项式，同时构建扩域 GF(2^m)，赋初值 t=1，利用域中元素 α^{2t-1}，按照式(8)构造校验矩阵，同时计算判决门限 Λ_{2t-1}。

步骤 6 计算元素 α^{2t-1} 下的平均余弦符合度值 $\overline{F}_{2t-1}$，若 $\overline{F}_{2t-1} \geqslant \Lambda_{2t-1}$，则 $t = t + 1$，跳转至步骤 5，直到 $\overline{F}_{2t-1} < \Lambda_{2t-1}$ 出现，此时保存该本原多项式下的最大纠错能力为 $t - 1$，同时跳转至步骤 5，遍历下一个本原多项式，直到遍历完成。

步骤 7 输出最大纠错能力下的本原多项式，即为生成多项式，同时计算连续码根的最小多项式对应的最小公倍式，完成本原 BCH 码生成多项式识别。

从以上步骤来看，本文算法的计算复杂度主要来源于平均余弦符合度的计算。设截获的码块数目为 N，BCH 码最大纠错能力为 t，则在第一次遍历本原多项式过程中，需要进行 $N\left(2^m - 1\right)$ 次乘法，$N\left(2^m - 1\right)$ 次余弦运算以及 N 次加法运算，为方便分析，这里将一次余弦运算等价为 3 次乘法运算，故一次本原多项式遍历需要进行 $4N\left(2^m - 1\right)$ 次乘法以及 N 次加法。考虑最不利的情况，遍历到最后一个本原多项式，则码长识别所需要的最大计算量为 $\sum_{m=3}^{9} 4N\left(2^m - 1\right)\dfrac{\varphi\left(2^m - 1\right)}{m}$ 次乘法以及 $\sum_{m=3}^{9} N\dfrac{\varphi\left(2^m - 1\right)}{m}$ 次加法（其中 $\varphi(\cdot)$ 表示欧拉函数，$\dfrac{\varphi\left(2^m - 1\right)}{m}$ 表示 m 级本原多项式个数）；对于 BCH 码生成多项式以及域生成多项式而言，在确定了码长后，需要 $4N\left(2^m - 1\right)\dfrac{\varphi\left(2^m - 1\right)}{m}t$ 次乘法以及 $N\dfrac{\varphi\left(2^m - 1\right)}{m}t$ 次加法。

4 仿真验证

4.1 平均余弦符合度统计特性验证

在算法识别过程中，需要设定最小错误判决门限，在门限的求解过程中，需要利用 2 种假设条件下的平均余弦符合度的统计特性，所以验证推导的统计特性是否正确至关重要。仿真设定 3 种 BCH 码，具体的参数如表 1 所示。

表 1　　**统计特性验证参数设定**

m	码长	GF(2^m)域本原多项式	BCH 码生成多项式	正确码根验证	错误码根验证
5	31	x^5+x^2+1	$x^{10}+x^9+x^8+x^6+x^5+x^3+1$	α	α^5
7	127	x^7+x+1	$x^{14}+x^{12}+x^{10}+x^6+x^5+x^4+x^3+x^2+1$	α^3	α^7
9	511	x^9+x^4+1	$x^{18}+x^{15}+x^{12}+x^{10}+x^8+x^7+x^6+x^3+1$	α^2	α^9

设定信噪比范围为–2~10 dB，步长为 0.5 dB。为了尽可能地反映实际统计特性，仿真中生成的样本数目为 10 000 个。在假设条件 H_0 与 H_1 下，仿真求得的平均余弦符合度均值与方差以及理论计算得到的均值与方差如图 1 所示。

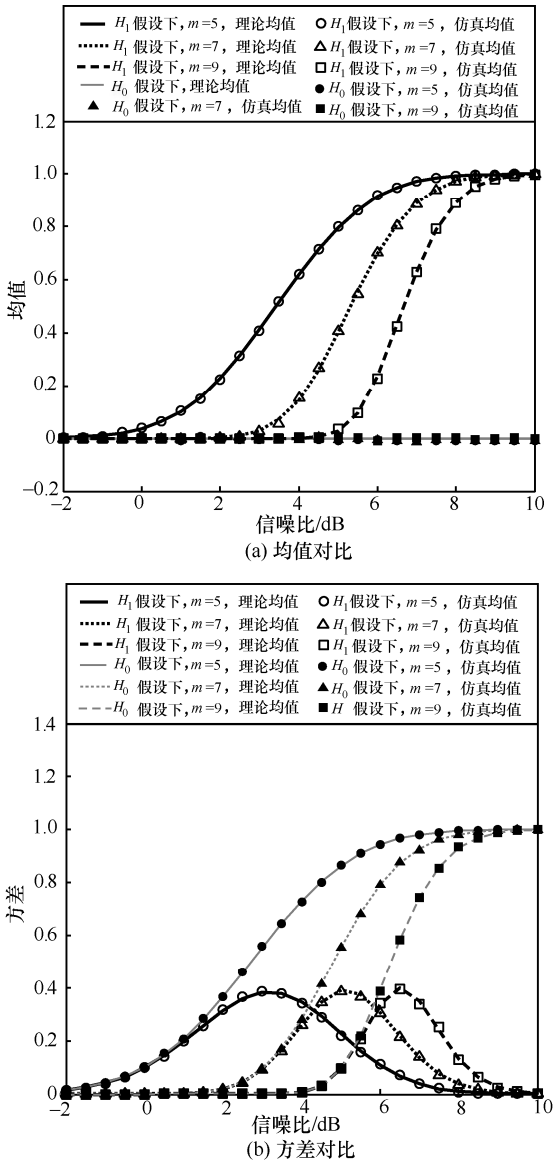


图 1　2 种假设条件下理论与仿真统计特性对比

从图 1 的结果来看，首先，理论值与仿真值几乎重合，这说明在 2 种假设条件下推导的平均余弦符合度的统计特性能够反映实际的情况；其次，当码长增加时，均值与方差曲线逐渐前移，在同一信噪比下，码长越长，统计特性区分越难。本文算法在低信噪比下的统计特性区分度较好，在 6 dB 信道环境、码长为 511 的情况下，2 种假设条件的均值仍存在明显差异。

4.2　算法容错性验证

仿真 1　码长对 BCH 码识别性能影响

仿真设定本原 BCH 码类型为 5 种，m 值分别为 5、6、7、8、9，每种编码的纠错能力都为 2，具体的编码参数如表 2 所示。

表 2　　**码长对容错性影响仿真参数设定**

m	码长	GF(2^m)域本原多项式	BCH 码生成多项式
5	31	x^5+x^2+1	$x^{10}+x^9+x^8+x^6+x^5+x^3+1$
6	63	x^6+x+1	$x^{12}+x^{10}+x^8+x^5+x^4+x^3+1$
7	127	x^7+x+1	$x^{14}+x^{12}+x^{10}+x^6+x^5+x^4+x^3+x^2+1$
8	255	$x^8+x^4+x^3+x^2+1$	$x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^8+x^6+x^5+x+1$
9	511	x^9+x^4+1	$x^{18}+x^{15}+x^{12}+x^{10}+x^8+x^7+x^6+x^3+1$

仿真中设定的信噪比范围为–2~7 dB，步长为 0.25 dB，蒙特卡洛仿真次数为 1 000 次，记录不同信噪比下本原 BCH 码码长以及生成多项式正确识别率，如图 2 所示，其中 L 表示码长。

从图 2 结果来看，码长对于本原 BCH 码识别具有较大的影响，随着码长的增加，算法识别性能会变差，主要原因在于随着码长的增加，在 2 种假设条件下平均余弦符合度统计特性差距会缩小，此时会造成较大的虚警概率，使算法性能恶化；从识别的效果来看，算法对于码长的识别性能要远远好于生成多项式的识别。从 1 000 次的蒙特卡洛统计结果来看，在信噪比不小于 5 dB 条件下，目前常用的本原 BCH 码正确识别率能够达到 95%以上，故能满足绝大多数实际情况下的性能需求。

仿真 2　码块数目对于算法影响

仿真设定本原 BCH 码为码长为 127，域 GF(2^7)

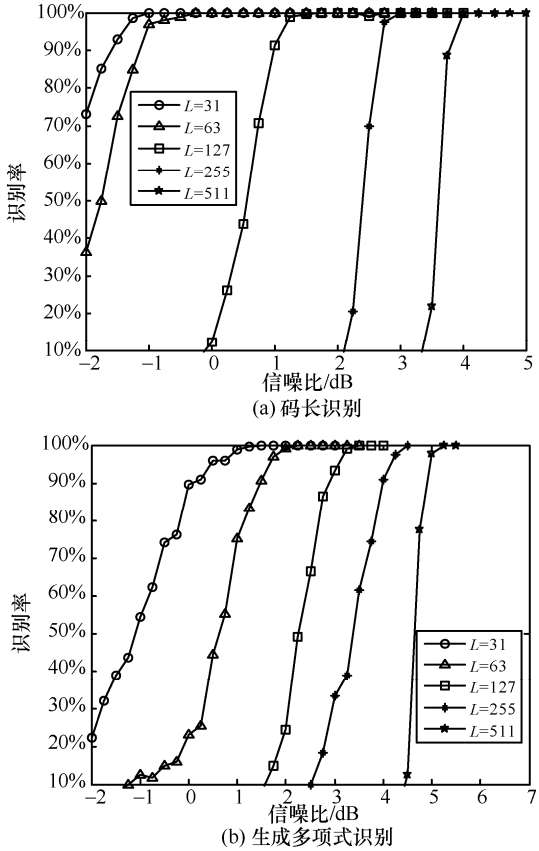


图 2　不同码长对 BCH 码识别的影响

本原多项式为 x^7+x+1，BCH 码生成多项式为 $x^{14}+x^{12}+x^{10}+x^6+x^5+x^4+x^3+x^2+1$，其纠错能力为 2，设定截获的码块数目为 500、1 000、1 500、2 000、2 500，设定的信噪比范围为–1~4 dB，步长为 0.25 dB，蒙特卡洛仿真次数为 1 000，统计在不同信噪比环境下，码长与生成多项式正确识别率，结果如图 3 所示。

从图 3 的结果来看，通过增加截获的码块数目，可以显著提高算法对于参数的正确识别率，当实际码长较长时，可以通过增加码块数目来克服由于码长造成的算法下降的缺陷。同时，从蒙特卡洛统计结果来看，本文算法具有较好的低信噪比适应性，在截获码块为 500、信噪比为 3 dB 的情况下，码长与生成多项式的正确识别率达到 90%以上，能够满足实际工程需要。

仿真 3　码率对算法影响

仿真参数设定本原 BCH 码码长为 127，域 GF(2^7)本原多项式为 x^7+x+1，码率类型总共 5 种，具体为 BCH(127,120)、BCH(127,113)、BCH(127,106)、BCH(127,99)、BCH(127,92)，对应于纠错能力分别为 1、2、3、4、5，连续码根起点

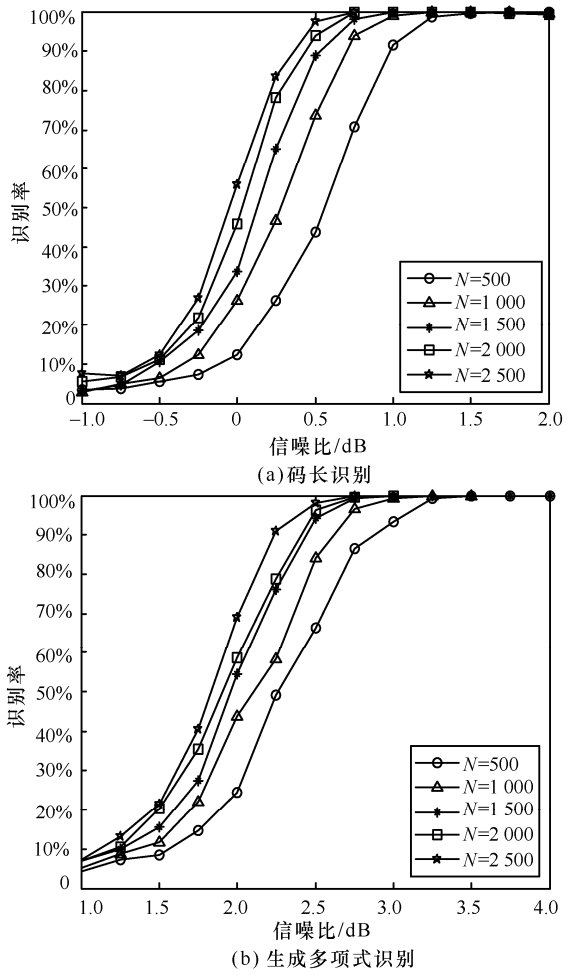


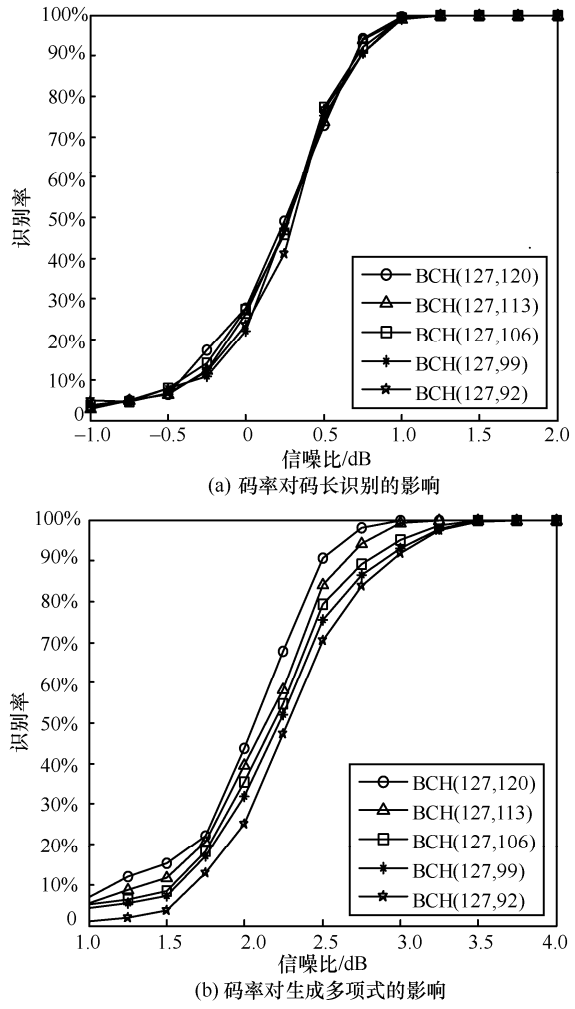
图 3　码块数目对 BCH 码识别的影响

从 α 开始，设定截获码块数目为 1 000，仿真中设定信噪比范围–1~4 dB，步长为 0.25 dB，蒙特卡洛仿真次数为 1 000，得到在设定的信噪比范围内的码长与生成多项式正确识别率曲线如图 4 所示。

从图 4 结果来看，码率对于码长识别的影响几乎可以忽略不计，因为在码长识别过程中，主要考察的是域中元素 α 的校验关系是否成立；而对于生成多项式的识别而言，算法性能随着码率的减小而逐渐变差，原因在于码率越小，纠错能力越强，此时需要遍历的连续码根数目必然增加，相应的误判概率也会增加。从识别率来看，当码率下降后，算法的正确识别率变化缓慢，说明算法对于码率具有较强的稳健性。

4.3　与其他算法对比

与本文算法进行对比的是目前具有一定容错性的 4 种方法，分别是软判决与硬判决相结合（SDBR, soft decision BCH recognition）的识别算法[14]（以下简称 SDBR 算法）、基于 BCH 码码根分布的



(a) 码率对码长识别的影响

(b) 码率对生成多项式的影响

图 4　码率对算法性能的影响

RIDE 识别算法[11]（以下简称 RIDE 算法）、改进 RIDE 算法[12]以及文献[10]基于多项式因子匹配识别算法（以下简称文献[10]算法）。设定本原 BCH 码为 BCH(63,51)，截获码块数目为 300，统计各个算法在不同信噪比下 BCH 码生成多项式识别概率，结果如图 5 所示。

从图 5 中 5 种算法的识别性能对比来看，本文算法性能要明显好于其他 4 种算法。与 SDBR 算法相比，性能提升约 0.5 dB；与改进 RIDE 算法、RIDE 算法以及文献[10]算法相比，性能分别提升约 1 dB、2.5 dB 以及 3.5 dB。本文算法能够取得性能的提升，主要原因在于采用了平均余弦符合度来衡量校验关系成立可靠性大小，没有造成码元信息的丢失；相反，其他 4 种算法在进行参数识别过程中采用了硬判决序列或是在进行运算过程中进行了简单的近似替代，不可避免地造成码元可靠性信息损失。

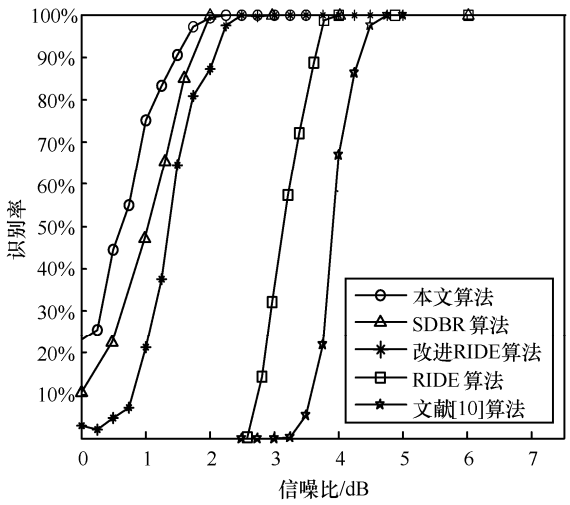


图 5　5 种算法性能对比

5　结束语

本文从本原 BCH 码定义出发，将域 GF(2^m)中的校验关系等价转化为二元域中的校验关系；然后引入了能够很好地度量校验约束关系的平均余弦符合度的概念，基于平均余弦符合度以及最小错误判决准则，实现在低信噪比下 BCH 码码根的快速检测，从而完成 BCH 码参数的识别。从仿真结果来看，在 2 种假设条件下推导的平均余弦符合度统计特性与实际情况相符。与其他算法相比，本文算法识别性能提升比较明显，其工程实用性更强。

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.
XIE H, HUANG Z T, WANG F H. Research progress of blind recognition of channel coding[J]. ACTA Electronica Sinica, 2013, 41(6): 1166-1176.

[2] HUANG L, CHEN W G, CHEN E H, et al. Blind recognition of *k*/*n* rate convolutional encoders from noisy observation[J]. Journal of Systems Engineering and Electronics, 2017, 2(28): 235-243.

[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, 7(46): 1545-1552.
YU P D, PENG H, GONG K X, et al. Blind recognition of convolutional codes based on least-square cost-function[J]. ACTA Electronica Sinica, 2018, 7(46): 1545-1552.

[4] 钟兆根, 吴昭军, 张立民, 等. 基于对数符合度下的RSC码识别[J]. 通信学报, 2018, 39(10): 79-86.
ZHONG Z G, WU Z J, ZHANG L M, et al. Blind recognition of RSC based on logarithmic conformity[J]. Journal on Communications, 2018, 39(10): 79-86.

[5] 杨晓静, 闻年成. 基于秩函数和 Euclide 算法的循环码盲识别[J]. 电路与系统学报, 2012, 17(5): 120-129.
YANG X J, WEN N C. A blind method of cyclic codes based on rank

function and Euclide arithmetic[J]. Journal of Circuits and Systems, 2012, 17(5): 120-129.

[6] WANG J, YUE Y, YAO J. A method of blind recognition of cyclic code generator polynomial[C]//2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM). 2010: 1-4.

[7] 张天骐, 易琛, 张刚, 等. 基于高斯列消元法的线性分组码参数盲识别[J]. 系统工程与电子技术, 2013, 35(7): 1514-1519.
ZHANG T Q, YI C, ZHANG G, et al. Blind identification of parameters of linear block codes based on columns Gaussian elimination[J]. Systems Engineering and Electronics, 2013, 35(7): 1514-1519.

[8] 刘杰, 张立民, 占超. 基于矩阵分析的线性分组码盲识别[J]. 系统工程与电子技术, 2017, 39(2): 404-409.
LIU J, ZHANG L M, ZHAN C. Blind recognition of linear block codes based on matrix analysis[J]. Systems Engineering and Electronics, 2017, 39(2): 404-409.

[9] 吕喜在, 黄芝平, 苏绍璟. BCH 码生成多项式快速识别方法[J]. 西安电子科技大学学报 (自然科学版), 2011, 38(6): 159-172.
LYU X Z, HUANG Z P, SU S J. Fast recognition method for generator polynomial of BCH codes[J]. Journal of Xidian University (Natural Scierce), 2011, 38(6): 159-172.

[10] ARTI D Y, SARAVANAN V, ANIMESH K. Blind recognition of binary cyclic codes from unsynchronized bitstream[J]. IEEE Transactions on Communications, 2016, 64(7): 2693-2706.

[11] 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 X J, WEN N C. Recognition method of BCH codes based on roots information dispersion entropy and roots statistic[J]. Journal of Detection & Control, 2010, 32(3): 69-73.

[12] 阚永红, 曾伟涛, 陈健. 基于概率逼近的本原 BCH 码编码参数的盲识别方法[J]. 电子与信息学报, 2014, 36(2): 332-339.
KONG Y H, ZENG W T, CHEN J. Blind identification of primitive BCH codes parameters based on probability approximation[J]. Journal of Electronics & Information Technology, 2014, 36(2): 332-339.

[13] 吴刚, 张邦宁, 郭道省. 非理想同步下 BCH 码盲识别的改进算法[J]. 信号处理, 2016, 32(6): 746-754.
WU G, ZHANG B N, GUO D X. Improved algorithm for blind recognition of BCH codes under imperfect synchronization[J]. Journal of Signal Processing, 2016, 32(6): 746-754.

[14] 刘杰, 张立民, 钟兆根, 等. 一种软判决下的本原 BCH 码盲识别方法[J]. 西安交通大学学报, 2017, 51(6): 59-65.
LIU J, ZHANG L M, ZHONG Z G. A blind recognition method forprimitive BCH codes in soft decision situations[J]. Journal of Xi'an Jiaotong University, 2017, 51(6): 59-65.

[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 X M, XIAO G Z. Error correcting code theory and method[M]. Xi'an: Xidian University Publishing Company, 2001: 145-240.

[16] WU Z J, ZHANG L M, ZHONG Z G. A maximum cosinoidal cost function method for parameter estimation of RSC Turbo codes[J]. IEEE Communications Letters, 23(3): 390-393.

[作者简介]

吴昭军（1992– ），男，四川遂宁人，海军航空大学博士生，主要研究方向为信道编码盲识别。

张立民（1966– ），男，辽宁开原人，博士，海军航空大学教授，主要研究方向为卫星信号处理及应用。

钟兆根（1984– ），男，江西南昌人，博士，海军航空大学讲师，主要研究方向为通信信号盲分离与统计信号处理。

龙玉峰（1982– ），男，山东烟台人，海军航空大学博士生，主要研究方向为飞行器故障检测与诊断。