

低信噪比下循环码识别

吴昭军¹, 张立民¹, 钟兆根², 金 堃²

(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)

摘 要: 针对硬判决分析方法存在计算复杂度高且容错性差的缺点, 本文提出了一种直接利用软判决序列完成循环码识别的新算法. 首先从编码代数结构出发, 推导出循环码生成多项式因子对应的对偶空间与码字能构成校验关系这一结论; 其次基于该结论, 遍历码长可能值, 在 $GF(2)$ 上, 将多项式 $x^n + 1$ 分解为不可约因子及其对应幂次的乘积, 当所遍历因子的对偶空间正好与码字序列构成校验关系时, 即可识别出循环码码长; 最后遍历构成校验关系因子的幂次, 最终完成生成多项式的识别. 为利用软判决序列完成校验关系检测, 引入了平均校验符合度概念, 基于其统计特性和最小错误判决准则, 实现了生成多项式不可约因子以及幂次的快速识别. 仿真结果表明, 推导的符合度统计特性与实际情况相吻合, 同时算法具有较好的低信噪比容错性能, 在 3dB 的噪声环境下, 码长以及生成多项式识别率能够达到 95% 以上, 与硬判决方法相比, 在增加较小的计算复杂度下, 识别性能提升将近 1dB. 在智能通信或是认知无线电领域具有较好的应用前景.

关键词: 循环码; 认知无线电; 智能通信; 平均校验符合度; 最小错误判决准则; 软判决

中图分类号: TN911.7 **文献标识码:** A **文章编号:** 0372-2112 (2020)03-0478-08

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.3969/j.issn.0372-2112.2020.03.009

Blind Recognition of Cyclic Codes at Low SNR

WU Zhao-jun¹, ZHANG Li-min¹, ZHONG Zhao-gen², JIN Kun²

(1. Department of Information Fusion, Naval Aviation University, Yantai, Shandong 264001, China;

2. The School of Aviation Basis, Naval Aviation University, Yantai, Shandong 264001, China)

Abstract: In order to overcome the shortcomings as high computational complexity and low fault tolerance in recognition of cyclic code by the hard-decision algorithms, a algorithm based on soft-decision is proposed. Firstly, based on the structure of coding algebra, it is deduced that the dual space corresponding to the polynomial factor are orthogonal to the codeword space. Secondly, based on the deduced conclusion, the possible length of code is traversed, then the polynomial $x^n + 1$ is decomposed into the product of irreducible factors and their powers, when the dual space of the traversing factor coincides with the parity-check of the code word sequence, the length can be recognized. Finally, by traversing the polynomial factors and the corresponding power, the generated polynomial can be identified. In addition, the concept of average checking conformity is introduced in parity-check matching. Based on its statistical property and minimum error decision criterion, the fast identification of generating polynomial factor and power is completed. The simulation results show that the derived statistical property are consistent with the actual situation, and at the same time, the proposed algorithm has better performance in low SNR, which can achieve over 95% of correct recognition rate in 3dB noise environment. Compared with the existing methods, although it increases the computational complexity slightly, its performance improved by nearly 1dB. It has a good application prospect in intelligent communication or cognitive radio.

Key words: cyclic code; cognitive radio; intelligent communication; average checking conformity; minimum error criterion; soft decision

1 引言

为改善通信质量, 数字通信中广泛采用差错控制

编码, 实现码元的自动检错与纠错. 在差错控制编码中, 循环码是一类非常重要的线性分组码, 因为其严格的代数结构, 能够以简单的电路实现编码与译码, 从而被

广泛应用于数字通信的各个方面. 对于非合作方而言, 在低信噪比下, 如果实现循环码参数的快速识别, 进而完成循环码的译码, 对于后续加扰分析、密码分析具有重要的现实意义^[1].

目前在有噪条件下适用的编码分析算法主要集中于卷积码^[2,3]以及循环码子集 RS 码^[4,5]和 BCH 码^[6,7]等, 而在恶劣信道环境下, 实用的循环码识别算法还比较少. 文献[8,9]提出了基于欧几里得辗转相除的识别算法, 该算法虽然计算效率较高, 但是容错性太差; 文献[10,11]提出了基于矩阵分析的识别算法, 这种方法在低误码率情况中具有一定的适用性, 但是一旦信道环境恶化, 算法将失效; 为提高算法的容错性能, 文献[12,13]利用循环码的码重分布不平衡特点, 实现码长、码字起点识别, 但该方法仅仅适用于短码长以及低码率的循环码; 文献[14]同样从提高算法的容错性为出发点, 利用 Walsh-Hardard 变换寻找循环码对偶空间码字, 虽然容错性能得到较大的提升, 但是计算复杂度会急剧增加; 文献[15,16]利用循环码生成多项式为 $x^n + 1$ 中因子这一特性, 将 $x^n + 1$ 进行因式分解, 进而完成循环码识别, 但是该算法仅适用于硬判决序列. 综合上述分析可知, 目前针对循环码识别的算法主要存在着容错性能不好以及计算复杂度太高的缺点.

为克服现有算法的缺点, 本文提出了一种低信噪比下的识别方法. 首先利用码长为 n 的循环码生成多项式一定能整除多项式 $x^n + 1$ 这一性质, 通过遍历循环码码长 n , 在 $\text{GF}(2)$ 上, 对多项式 $x^n + 1$ 进行因式分解, 然后遍历分解的因子进行校验匹配; 为了提高算法的容错性能, 本文将平均校验符合度作为优势统计量, 一旦因子对应的平均校验符合度大于设定的门限, 即可完成码长以及生成多项式因子的识别. 与以往算法相比, 本文所提出的算法具有较强的低信噪比适应能力, 同时其计算复杂度适中.

2 循环码定义及其结构特性分析

首先给出循环码定义和定理 1.

定义 1^[17] 设 V_n 是包含有 $(a_0, a_1, \dots, a_{n-1})$ 的 n 维线性空间, 则其 k 维子空间 V_k 称为一个循环码空间, 如果对于任意的 $(a_0, a_1, \dots, a_{n-1}) \in V_n$, 只要 $(a_0, a_1, \dots, a_{n-1}) \in V_k$, 就必然有 $(a_{n-1}, a_0, \dots, a_{n-2}) \in V_k$.

定理 1^[17] 循环码空间 V_k 是多项式环 $\text{GF}_2(x)$ 中的主理想, 同时该主理想的生成多项式一定整除 $x^n + 1$.

由定理 1 可知, 在 $\text{GF}(2)$ 上, 多项式 $x^n + 1$ 可化为生成多项式 $g(x)$ 倍式, 即:

$$x^n + 1 = g(x) \cdot h(x) \quad (1)$$

其中, $\deg(g(x)) = n - k$, $\deg(h(x)) = k$, 符号 $\deg(\cdot)$

表示多项式最高幂次.

不妨设

$$g(x) = g_0 + g_1 \cdot x + \dots + g_{n-k} \cdot x^{n-k} \quad (2)$$

$$h(x) = h_0 + h_1 \cdot x + \dots + h_k \cdot x^k \quad (3)$$

其中, $g_i (0 \leq i \leq n - k), h_j (0 \leq j \leq k) \in \text{GF}(2)$.

将式(2)与式(3)带入式(1), 对比等式两边相同幂次项的系数, 得到:

$$g_0 h_i + g_1 h_{i-1} + \dots + g_{n-k} h_{i-n+k} = 0 \quad (4)$$

其中, $i = 1, 2, \dots, n - 1$, 当 h 下标为负时, $h = 0$.

由式(4)可以得到循环码空间 V_k 的校验矩阵为:

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{bmatrix} \quad (5)$$

定义 $x^{\deg(f(x))} \cdot f(1/x)$ 为多项式 $f(x)$ 的互反多项式^[17], 记为 $\tilde{f}(x)$, 则 $h(x)$ 的互反多项式 $\tilde{h}(x)$ 生成的循环码空间即为由 $g(x)$ 生成的循环码对偶空间.

循环码生成多项式决定了循环码空间的大小, 要比较不同循环码空间的大小, 仅仅需要对比生成多项式即可, 即定理 2.

定理 2^[17] 设 C_1 是由 $g_1(x)$ 生成的循环码空间, 记为: $C_1 = \langle g_1(x) \rangle$; C_2 是由 $g_2(x)$ 生成的循环码空间, 记为: $C_2 = \langle g_2(x) \rangle$; 当且仅当 $g_2(x) \mid g_1(x)$ 时 (“ $\mid$ ”表示前面多项式能够整除后面多项式), 有 $C_1 \subseteq C_2$.

由定理 2 可知, 对于由 $g(x)$ 生成的循环码空间 V_k , 其对偶空间 $V_k^\perp$ 生成多项式为 $h(x)$, 若 $h'(x)$ 为 $h(x)$ 的倍式, 则由 $h'(x)$ 生成的循环码空间 $V_k'^\perp$ 满足 $V_k'^\perp \subseteq V_k^\perp$, 所以对于 $V_k'^\perp$ 中的码字一定能够和 V_k 形成校验关系.

下面考虑多项式 $x^n + 1$ 的因式分解, 当 n 为奇数时, 因式分解的结果没有重因子; 当 n 为偶数时, 则 n 可以表示为 $n = 2^r \cdot t$, 其中 t 为奇数, 此时有:

$$x^n + 1 = (x^t + 1)^{2^r} \quad (6)$$

此时 $x^n + 1$ 可以分解为 2^r 重的不可约多项式乘积, 即:

$$x^n + 1 = \prod_{i=1}^m (g_i(x))^{2^r} \cdot \prod_{j=1}^l (h_j(x))^{2^r} \quad (7)$$

式(7)中, $g_i(x)$ 与 $h_j(x)$ 为不可约多项式, m 与 l 满足 $m + l = t$ 约束. 当 n 为奇数时, $r = 0$; 反之, r 满足 $n = 2^r \cdot t$, 其中 t 为奇数. 假定生成多项式 $g(x)$ 中的不可约因子多项式由 $g_i(x) (1 \leq i \leq m)$ 构成.

设循环码生成多项式中不可约因子多项式的幂次分别为 $s_1, s_2, \dots, s_m$, 即:

$$g(x) = \prod_{i=1}^m (g_i(x))^{s_i} \quad (8)$$

式(8)中, $1 \leq s_i \leq 2^r, (1 \leq i \leq m)$.

对于式(8)中因子 $(g_i(x))^{s'_i}$, $(1 \leq i \leq m, 1 \leq s'_i \leq s_i)$ 而言,令

$$h'(x) = \frac{x^n + 1}{(g_i(x))^{s'_i}} \quad (9)$$

则 $h'(x)$ 一定是式(3)中 $h(x)$ 的倍式,即:

$$h'(x) = v(x) \cdot h(x) \quad (10)$$

分别求取 $h'(x)$ 与 $h(x)$ 互反多项式得到:

$$\begin{aligned} \bar{h}'(x) &= x^{\deg(h'(x))} \cdot h'\left(\frac{1}{x}\right) \\ &= x^{\deg(h'(x))} \cdot v\left(\frac{1}{x}\right) \cdot h\left(\frac{1}{x}\right) \end{aligned} \quad (11)$$

$$\bar{h}(x) = x^{\deg(h(x))} h\left(\frac{1}{x}\right) \quad (12)$$

将式(11)与式(12)相除,得到:

$$\frac{\bar{h}'(x)}{\bar{h}(x)} = x^{\deg(h'(x)) - \deg(h(x))} v\left(\frac{1}{x}\right) = \tilde{v}(x) \quad (13)$$

由式(13)可知 $h'(x)$ 的反多项式同样也是 $h(x)$ 反多项式的倍式,由定理2可知, $h'(x)$ 生成的循环码空间 $V_k'^{\perp}$ 是 $\bar{h}(xx)$ 生成空间 $V_k^{\perp}$ 的子空间,故空间 $V_k'^{\perp}$ 中的向量与码字空间 V_k 同样也构成校验关系,即

$$\mathbf{C} \cdot \mathbf{H}'^T = \mathbf{0} \quad (14)$$

式(14)中 $\mathbf{0}$ 为全零向量, $\mathbf{C}$ 为码字矩阵, $\mathbf{H}'$ 为 $V_k'^{\perp}$ 的生成多项式矩阵,即:

$$\mathbf{C} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N,1} & c_{N,2} & \cdots & c_{N,n} \end{bmatrix} \quad (15)$$

$$\mathbf{H}' = \begin{bmatrix} h'_{k'} & h'_{k'-1} & \cdots & h'_0 & 0 & 0 & \cdots & 0 \\ 0 & h'_{k'} & h'_{k'-1} & \cdots & h'_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 0 & h'_{k'} & h'_{k'-1} & \cdots & h'_0 \end{bmatrix} \quad (16)$$

式(15)中 n 为循环码码长, N 为码块数目;式(16)中 $k' = \deg(\bar{h}'(x))$,系数 $h'_i \in \text{GF}(2)$ 对应于 $h'(x)$ 中 i 次项前的系数.

3 循环码参数识别模型

3.1 基于平均校验符合度下的循环码识别

由定理2可知,当多项式 $x^n + 1$ 中因子满足式(14)校验关系时,则该因子也一定为生成多项式 $g(x)$ 中的因子,此时将式(14)展开,去掉不参与校验的元素,得到:

$$\begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k'+1} \\ c_{1,2} & c_{1,3} & \cdots & c_{1,k'+2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,n-k'} & c_{1,n-k'+1} & \cdots & c_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N,1} & c_{N,2} & \cdots & c_{N,k'+1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N,n-k'} & c_{N,n-k'+1} & \cdots & c_{N,k'+1} \end{bmatrix} \cdot \begin{bmatrix} h'_{k'} \\ h'_{k'-1} \\ \vdots \\ h'_0 \end{bmatrix} = \mathbf{0} \quad (17)$$

式(17)中,将式(17)中某一编码约束方程单列出来研究,即:

$$c_{i,j} \cdot h'_{k'} + c_{i,j+1} \cdot h'_{k'-1} + \cdots + c_{i,j+k'} \cdot h'_0 = 0 \quad (18)$$

其中, $1 \leq i \leq N, 1 \leq j \leq n - k'$.

为提高算法的容错性能,从概率的角度来衡量式(18)成立可能性大小,本文引入校验符合度的概念^[18,19].设 $x_{i,j}, x_{i,j+1}, \cdots, x_{i,j+k'}$ 对应于码元 $c_{i,j}, c_{i,j+1}, \cdots, c_{i,j+k'}$ 软判决信息,则 $c_{i,j}, c_{i,j+1}, \cdots, c_{i,j+k'}$ 的后验概率可以表示为: $P(c_{i,j} | x_{i,j}), P(c_{i,j+1} | x_{i,j+1}), \cdots, P(c_{i,j+k'} | x_{i,j+k'})$,则校验符合度定义为:

$$F_{i,j} = \prod_{l=0}^{k'} (1 - 2P(c_{i,j+l} = 1 | x_{i,j+l}) \cdot h'_{k'-l}) \quad (19)$$

式(19)中,如果 $c_{i,j+l} \cdot h'_{k'-l} = 1$,则被映射为-1,反之则被映射为1,如果式(18)中的校验关系成立,则 $c_{i,j+l} \cdot h'_{k'-l} = 1$ 个数一定为偶数,所以对应于式(19)结果一定为正值,并且信道噪声越小,值越接近于1.

假定信道噪声为均值为0,方差为 σ^2 的高斯噪声,信号调制方式为2PSK调制,信号幅度为 A ,不妨以码元 $c_{i,j}$ 为例,对应的软判决信息为 $x_{i,j}$,则 $x_{i,j}$ 的概率密度函数为:

$$p(x_{i,j} | c_{i,j} = 1) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(x_{i,j}-A)^2/2\sigma^2} \quad (20)$$

$$p(x_{i,j} | c_{i,j} = 0) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(x_{i,j}+A)^2/2\sigma^2} \quad (21)$$

由贝叶斯公式与全概率公式,得到后验概率为:

$$P(c_{i,j} = 1 | x_{i,j}) = \frac{e^{2A \cdot x_{i,j}/\sigma^2}}{e^{2A \cdot x_{i,j}/\sigma^2} + 1} \quad (22)$$

在2PSK调制方式下,信噪比定义为:

$$\text{SNR} = 10 \lg \left(\frac{A^2}{2\sigma^2} \right) \quad (23)$$

在通信系统中,信号幅度取值一般为1,将式(22)带入式(19)中得到:

$$F_{i,j} = \prod_{l=0}^{k'} \left(1 - \frac{2e^{2x_{i,j+l}/\sigma^2}}{e^{2x_{i,j+l}/\sigma^2} + 1} h'_{k'-l} \right) \quad (24)$$

为了衡量 $h' = [h'_{k'}, h'_{k'-1}, \cdots, h'_0]^T$ 对全体码字校验关系成立可能性的大小,将 $F_{i,j}$ 进行统计平均,得到平均校验符合度为:

$$\bar{F} = \frac{1}{N(n-k')} \sum_{i=1}^N \sum_{j=1}^{n-k'} F_{i,j} \quad (25)$$

3.2 平均校验符合度统计特性

首先考虑 $\mathbf{h}' = [h'_{k'}, h'_{k'-1}, \dots, h'_0]^T$ 为真实的校验向量情况. 记 $w(\mathbf{h}')$ 为向量 $\mathbf{h}'$ 码重, 记集合 $\Phi = \{l = k' - i | h'_i = 1, 0 \leq i \leq k'\}$, 式(24)进一步变为:

$$F_{i,j} = \prod_{l \in \Phi} \left(\frac{e^{-2x_{i,j+l}/\sigma^2} - 1}{e^{-2x_{i,j+l}/\sigma^2} + 1} \right) \quad (26)$$

当 $\mathbf{h}'$ 满足校验关系时, 设向量中等于 1 的元素分别为: $[h'_{l_1}, h'_{l_2}, \dots, h'_{l_m}]$, 其对应参与校验的码元分别为: $[c_{i,n-l_1}, c_{i,n-l_2}, \dots, c_{i,n-l_m}]$. 由于校验约束关系成立, 参与校验的码元等于 1 的个数必须为偶数, 这样的情况总共有:

$$\sum_{k=0}^{\lfloor w(\mathbf{h}')/2 \rfloor} C_{w(\mathbf{h}')}^{2k} = 2^{w(\mathbf{h}')-1} \quad (27)$$

式(27)中 $\lfloor \cdot \rfloor$ 表示向下取整, 符号 C_n^m 表示组合数运算, 即 $C_n^m = \frac{n \cdot (n-1) \cdots (n-m+1)}{m \cdot (m-1) \cdots 1}$.

此时分别计算每一种情况下的均值, 然后再对每一种情况加权, 即在 $\mathbf{h}'$ 满足校验关系时, $F_{i,j}$ 的均值和方差分别为:

$$u'_1 = \sum_{i=0}^{\lfloor w(\mathbf{h}')/2 \rfloor} \frac{C_{w(\mathbf{h}')}^{2i}}{2^{w(\mathbf{h}')-1}} \left(\int_{-\infty}^{\infty} \frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} p(x | c = 1) dx \right)^{2i} \cdot \left(\int_{-\infty}^{\infty} \frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} p(x | c = 0) dx \right)^{w(\mathbf{h}')-2i} \quad (28)$$

$$\sigma_1'^2 = \sum_{i=0}^{\lfloor w(\mathbf{h}')/2 \rfloor} \frac{C_{w(\mathbf{h}')}^{2i}}{2^{w(\mathbf{h}')-1}} \left(\int_{-\infty}^{\infty} \left(\frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} \right)^2 p(x | c = 1) dx \right)^{2i} \cdot \left(\int_{-\infty}^{\infty} \left(\frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} \right)^2 p(x | c = 0) dx \right)^{w(\mathbf{h}')-2i} - u_1'^2 \quad (29)$$

其次当 $\mathbf{h}'$ 不为校验向量时, 此时参与校验的码元, 其码重没有偶数的限制, 此时参与校验的码元分布共有:

$$\sum_{k=0}^{w(\mathbf{h}')} C_{w(\mathbf{h}')}^k = 2^{w(\mathbf{h}')} \quad (30)$$

同样针对每一种情况都求取其均值与方差, 然后再加权平均, 得到在 $\mathbf{h}'$ 不满足校验关系时, $F_{i,j}$ 的均值和方差分别为:

$$u'_0 = \sum_{i=0}^{w(\mathbf{h}')} \frac{C_{w(\mathbf{h}')}^i}{2^{w(\mathbf{h}')}} \left(\int_{-\infty}^{\infty} \frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} p(x | c = 1) dx \right)^i \cdot \left(\int_{-\infty}^{\infty} \frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} p(x | c = 0) dx \right)^{w(\mathbf{h}')-i} \quad (31)$$

$$\sigma_0'^2 = \sum_{i=0}^{w(\mathbf{h}')} \frac{C_{w(\mathbf{h}')}^i}{2^{w(\mathbf{h}')}} \left(\int_{-\infty}^{\infty} \left(\frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} \right)^2 p(x | c = 1) dx \right)^i$$

$$\cdot \left(\int_{-\infty}^{\infty} \left(\frac{e^{-2x/\sigma^2} - 1}{e^{-2x/\sigma^2} + 1} \right)^2 p(x | c = 0) dx \right)^{w(\mathbf{h}')-i} - u_0'^2 \quad (32)$$

在得到上述两种情况下 $F_{i,j}$ 的均值和方差后, 可以进一步得到 $\bar{F}$ 的均值与方差为: $u_1 = u'_1, u_0 = u'_0, \sigma_1^2 = \frac{\sigma_1'^2}{N(n-k')}, \sigma_0^2 = \frac{\sigma_0'^2}{N(n-k')}.$

下面进一步推导因子判决门限, 首先设定两类假设检验为:

H_0 : 遍历的因子不是生成多项式中的因子.

H_1 : 遍历的因子为生成多项式中的因子.

当码块数目足够多时, 由中心极限定理可知, 在 H_0 假设条件下, $\bar{F}$ 服从均值为 u_0 , 方差为 σ_0^2 的高斯分布; 在 H_1 假设条件下, $\bar{F}$ 服从均值为 u_1 , 方差为 σ_1^2 的高斯分布. 假定判决门限为 Λ , 虚警概率为 P_f , 漏警概率为 P_a , 则两类错误概率为:

$$P_f = \int_{\Lambda}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_0} e^{-(x-u_0)^2/\sigma_0^2} dx \quad (33)$$

$$P_a = \int_{-\infty}^{\Lambda} \frac{1}{\sqrt{2\pi}\sigma_1} e^{-(x-u_1)^2/\sigma_1^2} dx \quad (34)$$

平均错误概率为:

$$P_e = \frac{1}{2} (P_a + P_f) \quad (35)$$

将 P_e 对 Λ 求导数得到:

$$\frac{dP_e}{d\Lambda} = -\frac{1}{2\sqrt{2\pi}} \left(\frac{e^{-(\Lambda-u_0)^2/2\sigma_0^2}}{\sigma_0} - \frac{e^{-(\Lambda-u_1)^2/2\sigma_1^2}}{\sigma_1} \right) \quad (36)$$

令式(36)等于 0, 得到最小错误判决门限为:

$$\Lambda = \frac{u_1\sigma_0^2 - u_0\sigma_1^2 - \sigma_0\sigma_1 \sqrt{\left((u_1 - u_0)^2 + 2(\sigma_1^2 - \sigma_0^2) \ln\left(\frac{\sigma_1}{\sigma_0}\right) \right)}}{\sigma_0^2 - \sigma_1^2} \quad (37)$$

当 N 足够大时, $\sigma_1 \approx \sigma_0$, 此时 $\Lambda \approx \frac{u_0\sigma_1 + u_1\sigma_0}{\sigma_1 + \sigma_0}.$

3.3 算法流程及计算复杂度分析

由前面的分析可知, 循环码识别的关键在于对多项式 $x^n + 1$ 中因子的正确判定, 具体的算法流程步骤, 如算法 1 所示.

算法 1 循环码识别流程

输入: $n_{\min}, n_{\max}$

输出: 码长 $\hat{n}$, 生成多项式 $\hat{g}(x)$

步骤 1: 将软判决序列转化为条件概率, 初始化码长 $n = n_{\min}$.

步骤 2: 分解 $x^n + 1$, 保存不可约因子与幂次.

步骤 3: 遍历步骤 2 中不可约因子, 计算门限 Λ .

步骤4:计算步骤3中因子对应的 $\bar{F}$,若 $\bar{F} > \Lambda$,保存该不可约因子,输出 $\hat{n} = n$,然后跳转步骤5;否则跳转步骤3,遍历下一个不可约因子;若未出现通过门限的情况,则 $n = n + 1$,跳转步骤2,直到 $n > n_{\max}$.

步骤5:设定幂次 $k = 2$,计算步骤4中通过门限的因子 k 次幂对应的 Λ 和 $\bar{F}$,若 $\bar{F} > \Lambda$,则 $k = k + 1$,重复步骤5,直到 $\bar{F} < \Lambda$ 或 $k > 2'$,确定出该因子幂次为 $k - 1$,然后跳转步骤3,遍历下一个不变因子,直到遍历结束.

步骤6:步骤4与步骤5中所有不可约因子以及幂次乘积,结果为 $\hat{g}(x)$,算法终止.

从上述算法步骤来看,算法的计算复杂度主要集中在对 $x^n + 1$ 的分解以及 $\bar{F}$ 计算上,按照文献[20]的方法, $x^n + 1$ 的分解需要对 $n \times n$ 的矩阵进行高斯消元,故完成一次分解的计算复杂度近似为 $O(n^3)$,设码块数目为 N ,遍历的因子数目为 S_i ,则需要进行 $O(N \cdot S_i)$ 量级的加法以及乘法.在极极端条件下,当遍历到最后一个码长才完成识别,故算法的最大计算复杂度近似为 $O\left(n_{\max}^4 + N \sum_{i=n_{\min}}^{n_{\max}} S_i\right)$.

4 仿真实验

4.1 校验符合度统计特性验证

本节中主要验证校验符合度的统计特性.仿真实验中,设定截获的码块数目为2000,采用三种循环码,码率分别为:11/15,26/31以及57/63;对应的生成多项式为 $x^4 + x + 1$, $x^5 + x^3 + x^2 + x + 1$ 以及 $x^6 + x^5 + x^4 + x^2 + 1$;设定遍历的错误多项式因子分别为 $x^4 + x^3 + 1$, $x^5 + x^4 + x^3 + x^2 + 1$ 以及 $x^6 + x^4 + x^2 + x + 1$,其对应的 $w(\mathbf{h}')$ 分别为:7,15以及23.分别得到在假设条件 H_0 以及 H_1 下, $F_{i,j}$ 均值和方差的理论值与仿真值,结果如图1所示.

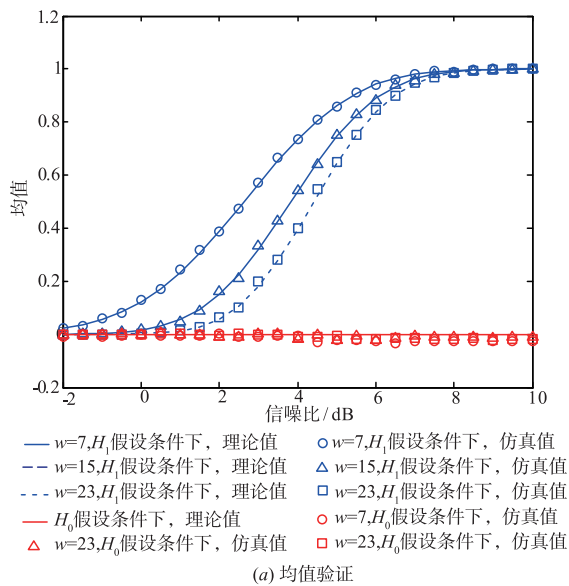
从图1结果来看,在不同的信噪比下,理论与仿真能够很好的吻合,这说明在3.2节中平均校验符合度统计特性推导过程是完全正确的.随着信噪比的减小,无论遍历的因子是否是生成多项式的因子,其方差以及均值都将趋近于0;其次随着 $w(\mathbf{h}')$ 值增加,对于均值来说, H_1 假设条件下曲线逐渐减小,而 H_0 下均值始终在0附近徘徊;对于方差而言, H_1 假设条件下的曲线峰值逐渐向由右移动,且最终趋于0,而在 H_0 条件下,方差逐渐减小,最终趋于1.这反映出在信噪比越大, $w(\mathbf{h}')$ 越小,二者统计特性差异越明显.

4.2 算法的容错性分析

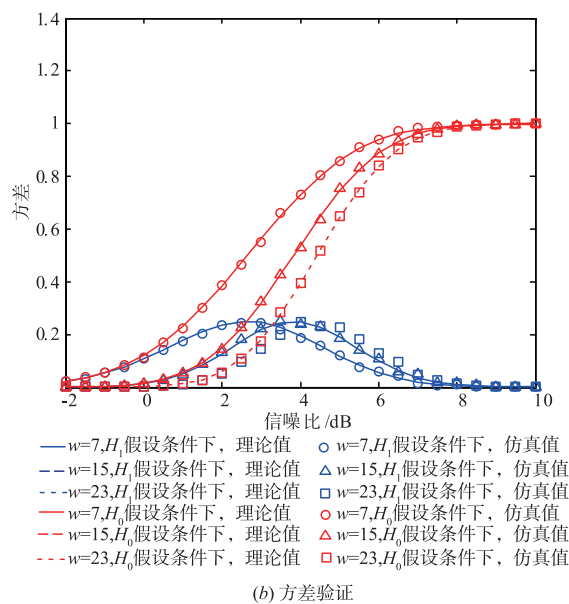
仿真1 循环码码长对算法影响

仿真设定5种不同的循环码码长,具体如表1所示,表格中数字代表多项式各项幂次,如 $x + 1$,可写为(1,0).

从图2的结果来看,随着码长的增加,参数的识别率会有较大幅度的下降,主要原因在于码长越大,需要遍历的因子就越多,此时虚警概率就会增加.



(a) 均值验证



(b) 方差验证

图1 统计特性验证

表1 仿真的循环码参数

n	k	生成多项式
23	11	(1,0)(11,9,7,6,5,1,0)
33	22	(1,0)(10,9,8,7,6,5,4,3,2,1,0)
43	15	(14,12,10,7,4,2,0)(14,11,10,9,8,7,6,5,4,3,0)
51	35	(8,4,3,1,0)(8,7,6,4,2,1,0)
63	51	(6,3,0)(6,1,0)

仿真2 码块数目对算法影响

仿真设定循环码码长为31,码率为21/31,其生成多项式为 $(5,3,2,1,0) \cdot (5,4,3,2,0)$,设定截获的码块数目 N 分别为500,1000,1500,2000,2500.得到在不同信噪比下码长以及生成多项式正确识别率曲线,如图3所示.

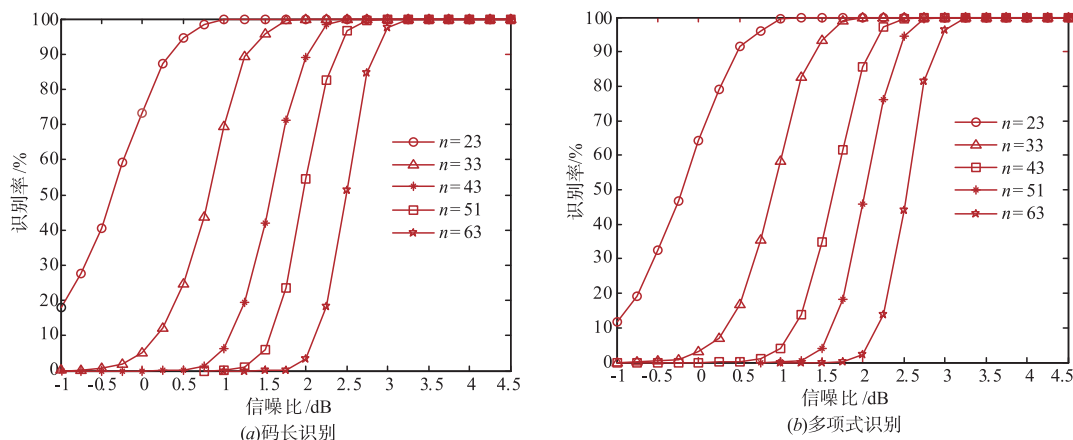


图2 循环码码长对算法性能的影响

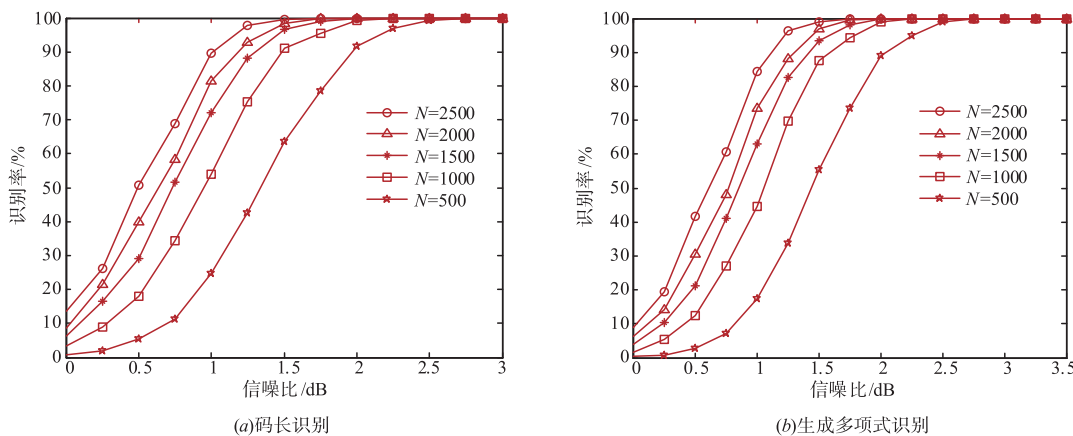


图3 不同截获码块数目对算法影响

从图 3 来看,截获的码块数目越多,参数识别的正确率就越高,原因在于,随着 N 的增加,实际计算所得的平均校验符合值统计特性就越接近于理论推导,在参数识别过程中的虚警与漏警概率就在一定程度上减少。

4.3 与它算法比较

与本文算法进行比较的是目前性能较好的文献[16]算法,该算法通过分解 $x^n + 1$ 多项式,获取循环码校验矩阵,采用硬判决序列进行校验匹配。二者对比主要从识别性能以及实时性上对比。

首先是识别性能对比,选择 4 种码长的循环码,其参数与表 1 中前 4 种一致,设定截获的码块数目为 2000,在相同的信道环境下分别统计本文算法与文献[16]算法的码长与生成多项式正确识别率如图 4 所示。

从图 4 结果来看,本文算法性能提升将近 1dB,其原因在于本文直接利用信道截获的软判决序列,能够最大化的利用上能够反映信道特性的软判决信息;相反,文献[16]算法利用的是解调后的硬判决序列,这使

得反映信道特性的信息丢失。

其次,进一步考察两种算法的运行复杂度。在 i3-6006U 处理器,运行内存为 4GB 的个人笔记本下,记录在不同码长下,完成一次识别所需要的平均时间,结果如表 2 所示。

表 2 不同码长下,两种算法识别时间对比

n	本文算法耗时(s)	文献[16]耗时(s)
23	0.158 6	0.059 5
33	0.281 4	0.112 8
43	0.430 7	0.212 4
51	0.599 0	0.302 5
63	0.984 0	0.422 7

从表 2 可知,文献[16]算法的实时性能是本文算法实时性的 2 到 3 倍,其原因在于文献[16]参与运算的是硬判决比特流,同时在求取判决门限时,不需要进行数值积分;相反本文算法为了提高低信噪比的适应能力,采用软判决序列,整个运算在实数域中进行,在求解判决门限时,需要进行数值积分,故本文是以计算复杂度换取了参数识别性能的提高。

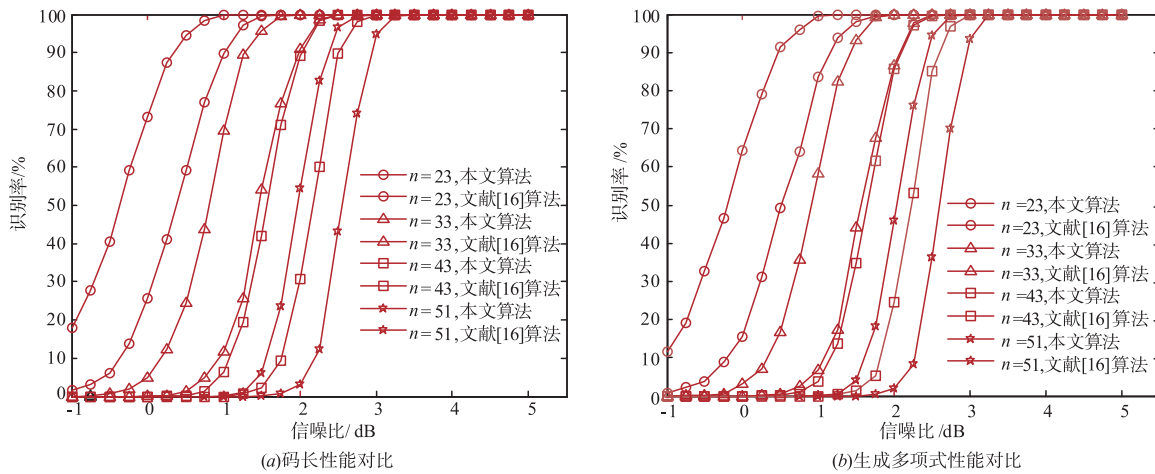


图4 算法性能对比

5 结论

本文首先从循环码代数结构出发,推导出生成多项式因子对应的对偶空间同样与码字保持校验关系结论,然后基于该结论,遍历码长 n 并分解 $x^n + 1$,对其不可约多项式因子及其幂次进行校验关系匹配,匹配过程中,提出了基于平均校验符合度以及最小错误判决准则的匹配方法,可实现在实数域中快速完成参数识别.与硬判决方法相比,本算法在牺牲较小的计算复杂度下,识别性能提升将近 1 dB.

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 Hui, HUANG Zhi-tao, WANG Feng-hua. Research progress of blind recognition of channel coding[J]. Acta Electronica Sinica, 2013, 41(6): 1166-1176. (in Chinese)
- [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 Pei-dong, PENG Hua, GONG Ke-xian, et al. Blind recognition of convolutional codes based on least-square cost-function[J]. Acta Electronica Sinica, 2018, 7(46): 1545-1552. (in Chinese)
- [4] 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.
LIU Jie, ZHANG Li-min, ZHONG Zhao-gen. Blind parameter identification of RS code based on binary field equivalence[J]. Acta Electronica Sinica, 2018, 46(12): 2888-2895. (in Chinese)
- [5] 龙浪,杨俊安,刘辉,等.基于信息位与校验位分离的 RS 码盲识别[J].探测与控制学报,2018,40(6):94-98.
LONG Lang, YANG Jun'an, LIU Hui, et al. Blind identification of RS codes based on separation of message bits and parity bits[J]. Journal of Detection & Control, 2018, 40(6): 94-98. (in Chinese)
- [6] 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 Jie, ZHANG Limin, ZHONG Zhaogen. A blind recognition method for primitive BCH codes in soft decision situations[J]. Journal of Xi'an Jiao Tong University, 2017, 51(6): 59-65. (in Chinese)
- [7] 阔永红,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 Yonghong, ZENG Weitao, CHEN Jian. Blind identification of primitive BCH codes parameters based on probability approximation[J]. Journal of Electronics & Information Technology, 2014, 36(2): 332-339. (in Chinese)
- [8] 杨晓静,闻年成.基于秩函数和 Euclidean 算法的循环码盲识别[J].电路与系统学报,2012,17(5):120-129.
YANG Xiaojing, WEN Niancheng. A blind method of cyclic codes based on rank function and euclidean arithmetic[J]. Journal of Circuits and Systems, 2012, 17(5): 120-129. (in Chinese)
- [9] WANG J, YUE Y, YAO J. A method of blind recognition of cyclic code generator polynomial[A]. 6th International Conference on Wireless Communications Networking and Mobile Computing[C]. Chengdu: IEEE Press, 2010. 1-4.
- [10] 郑瑞瑞,汪立新.基于码重分布概率方差的循环码识别

- 方法[J]. 太赫兹科学与电子与信息学报, 2013, 11(5): 792 - 796.
ZHENG Ruirui, WANG Lixin. Recognition method of cyclic codes based on code weight distribution probability variance[J]. Journal of Terahertz Science and Electronic Information Technology, 2013, 11(5): 792 - 796. (in Chinese)
- [11] 王兰勋, 贾层娟, 熊政达. 一种循环码参数的全盲识别方法[J]. 计算机科学, 2017, 44(3): 283 - 287.
WANG Lanxun, JIA Cengjuan, XIONG Zhengda. Blind recognition method of cyclic codes parameters[J]. Computer Science, 2017, 44(3): 283 - 287. (in Chinese)
- [12] 张天骐, 易琛, 张刚. 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 Tianqi, YI Chen, ZHANG Gang. Blind identification of parameters of linear block codes based on columns Gaussian elimination[J]. Systems Engineering and Electronics, 2013, 35(7): 1514 - 1519. (in Chinese)
- [13] 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 Jie, ZHANG Limin, ZHAN Chao. Blind recognition of linear block codes based on matrix analysis[J]. Systems Engineering and Electronics, 2017, 39(2): 404 - 409. (in Chinese)
- [14] 杨晓伟, 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 Lou. Blind estimation algorithm of the linear block codes parameters based on WHT[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1642 - 1646. (in Chinese)
- [15] 张天骐, 王军霞, 江晓磊, 等. 基于校验矩阵匹配的循环码参数盲识别[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. (in Chinese)
- [16] 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.
- [17] 肖国镇, 卿斯汉. 编码理论[M]. 北京: 国防工业出版社, 1993. 120 - 153.
XIAO Guozhen, QING Shihan. Coding Theory[M]. Beijing: National Defence Industry Press, 1993. 120 - 153. (in Chinese)
- [18] 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.
ZHANG Limin, WU Zhaojun, 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. (in Chinese)
- [19] 刘俊, 李静, 彭华. 基于校验方程平均符合度的 Turbo 码交织器估计[J]. 电子学报, 2016, 44(5): 1213 - 1217.
Liu Jun, Li Jing, Peng Hua. Estimation of turbo-code interleaver based on average conformity of parity-check equation[J]. Acta Electronica Sinica, 2016, 44(5): 1213 - 1217. (in Chinese)
- [20] 林东岱. 代数学基础与有限域[M]. 北京: 高等教育出版社, 2006. 70 - 82.
LIN Dongdai. Introduction to Algebra and Finite Fields[M]. Beijing: Higher Education Press, 2006. 70 - 82. (in Chinese)

作者简介



吴昭军 男, 1992 年 9 月出生于四川蓬溪县. 现为海军航空大学博士研究生. 主要研究方向为信道编码盲识别.
E-mail: wuzhaojun1992@qq.com



张立民 (通信作者) 男, 1966 年出生于辽宁开原. 现为海军航空大学教授、博士生导师. 主要研究方向为卫星信号处理及应用.
E-mail: iamzlm@163.com



钟兆根 男, 1984 年出生于江西南昌, 博士. 现为海军航空大学讲师, 主要研究方向为通信信号盲分离与统计信号处理.
E-mail: zhongzhaogen@163.com

金堃 女, 1993 年出生于河南郑州, 硕士, 现为海军航空大学助教, 主要研究方向为通信信号处理及仿真技术.
E-mail: jinkunhg@163.com