信道编码盲识别技术研究进展

解 辉,黄知涛,王丰华
(国防科学技术大学电子科学与工程学院,湖南长沙 410073)

摘 要: 信道编码盲识别是非合作信号处理领域的重要内容,将非合作信号处理技术从信号层扩展到了信息层,在智能通信、信息截获、信息对抗等领域具有重要作用.本文首先对广泛应用于现代数字通信系统中的卷积码、BCH码、RS码、Turbo码和扰码的盲识别算法进行了总结和归类,然后对算法原理进行了描述,并分别从计算量和误码适应能力两个方面对算法的性能进行了分析.最后,根据目前算法的不足和现实需求,指出了未来信道编码盲识别的研究方向.

关键词: 信道编码;卷积码;BCH码;Reed-Solomon码(RS码);Turbo码;扰码;盲识别
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2013)06-1166-11
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.06.019

Research Progress of Blind Recognition of Channel Coding

XIE Hui, HUANG Zhi-tao, WANG Feng-hua
(*College of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: Blind recognition of channel coding plays an important role in the field of non-cooperative signal processing, which has been extended from the signal level to the information level. Blind recognition of channel coding is widely used in the fields of intelligence communication, information interception and information countermeasure. Firstly, the recognition algorithms of convolution code, BCH code, RS code, Turbo code and scramble code which are commonly used in modern digital communication systems were summarized and classified. Then the theories of the algorithms were described, and the computational complexity and performances in noisy environment of the algorithms were analyzed. Finally, the future of blind recognition of channel coding was pointed out based on the shortcoming of current algorithms and practical need.

Key words: channel coding; convolution code; BCH code; Reed-Solomon code (RS code); Turbo code; scramble code; blind recognition

1 引言

近年来,信道编码盲识别已成为非合作信号处理领域一个新的研究方向,其在智能通信、信息截获和信息对抗领域具有广泛应用[1~6].

未来的智能移动通信、多点广播通信中,将广泛采用自适应调制编码技术,随着信道质量随时间的变化随时改变信道编码方式,以便获得最优的通信效率和服务质量[1].但在实际情况下,由于传输过程中的时延、干扰、中断等原因,使得相关控制信息有时不能准时或正确地传送到接收端,从而造成通信无法建立.这就需要接收方仅根据接收的未知数据快速识别出信道编码的体制、参数,以达到智能通信的目的.特别是随着认知无线电和认知通信的发展,信道编码的盲识别将成为未来智能通信系统的主要功能之一[2,3].

信息截获是第三方对通信双方的信息进行非常规获取的一种技术.对接收数据进行解调之后,要想获取通信的内容,则必须实现对数据信道编码的识别并译码,通过信道编码的盲识别技术可以进一步获取对方通信链路的通信数据,如无人机的传输图像、卫星广播服务的通信内容、多媒体通信服务的视频信息等[4~6],同时可对通信采用的协议进行分析,为实施基于通信协议的欺骗干扰和攻击提供先验信息[3].

信道编码盲识别技术的重要应用价值使其受到国外研究人员越来越多的关注和研究.目前常用的信道编码方式主要有卷积码、BCH(Bose Chaudhuri Hocquenghem,BCH)码、RS(Reed Solomon,RS)码、Turbo码和低密度单奇偶校验(Low-Density Parity-Check,LDPC)码,

收稿日期:2012-06-22;修回日期:2012-11-22
基金项目:国家自然科学基金(No.61072120);教育部新世纪人才支持计划

以及为消除数据中连续的0、1序列而加入的伪随机扰码等.本文主要是对近年来常用信道编码的盲识别算法进行归纳分类,分析与总结了各类算法的优缺点,并指出了信道编码的盲识别现在未解决的难点问题和现实需求,为信道编码盲识别的进一步研究提供广阔的视角.

2　卷积码盲识别算法

Elias在1953年时最早引入了不同于分组码的卷积码,并迅速得到发展,卷积码纠错能力强、译码简单,其中删除卷积码因为其具有高码率和译码简单等特点,应用尤为广泛[7].在国际空间数据系统顾问委员会(CCSDS)制定的帧同步与信道编码标准中,卷积码更是作为卫星通信中主要采用的信道编码方式之一[8].

B.Rice[9]首次提出了 $1/n$ 码率卷积码的估计方法,随后,E Filiol[10]和A.J.Han VinckPhillip[11]则将识别范围扩大到了 k/n 码率卷积码.L.Boyd[12]提出了合成脉冲响应序列算法解决了1/2码率卷积码的参数估计问题,Johann Barbier[13]则利用代数方法实现了卷积码的盲识别,但上述方法都不能很好的适应卷积码中存在误码的情况.为此,文献[14~29]针对误码条件下的卷积码盲识别进行了大量的研究工作,解决了 $1/n$、$(n-1)/n$ 等码率卷积码在误码环境下的盲识别问题.总体来说,目前卷积码的盲识别主要有基于线性方程组求解[5,16~23]、基于欧几里得算法[24]、基于Walsh-Hadamard变换[25~26]等算法以及这些方法的改进算法.

2.1　基于线性方程组的求解算法

卷积码序列 $\boldsymbol{V}$ 与校验矩阵 $\boldsymbol{H}$ 存在如下校验关系[7]

$$\boldsymbol{V}\boldsymbol{H}^{\mathrm{T}}=0 \tag{1}$$

校验矩阵多项式的最高阶数根据实际应用设定为 m,卷积码输出路数 n,容易得到校验矩阵多项式系数的齐次线性方程组

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_L \\ v_{n+1} & v_{n+2} & \cdots & v_{n+L} \\ v_{2n+1} & v_{2n+2} & \cdots & v_{2n+L} \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}\begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_L \end{pmatrix}=0 \tag{2}$$

其中 v_i 为接收序列中的第 i 位,L 为方程组未知个数 $n(m+1)$.文献[16~21]针对式中的模型给出了相应的求解算法,文献[22]将1/2码率卷积码校验矩阵的求解模型转化为关键模方程表示:在集合

$$\begin{aligned}\Phi^{(n)}=\{&(h^1(x),h^2(x),m)\in F[x]^2\times Z^+ \mid \\ &\exists\, d(x)\in F[x],\text{使得} \\ &h^1(x)v^1(x)+h^2(x)v^2(x)\equiv d(x)\bmod x^{N+1},\text{且} \\ &\deg d(x)<m,\max(\deg h^1(x),\deg h^2(x)))\leqslant m\}\end{aligned} \tag{3}$$

中寻找元素 $(h^1(x),h^2(x),m)$,使得 m 达到最小且 $(h^1(0),h^2(0))\neq(0,0)$.其中 $F[x]$ 为二元域上的多项式环.文献[5]、[22]和[23]针对该模型给出了基于快速合冲和 $F[x]$-格基约化算法的求解算法,将算法计算复杂度由 $O(N^3)$ 降低为 $O(N^2)$.

2.2　基于欧几里得算法的求解算法

欧几里得算法是一个递归算法[7],目的是寻找两个多项式 $a(x)$ 和 $b(x)$ 的最大公约数 $d(x)$,并寻找一个 $a(x)$ 和 $b(x)$ 的线性组合,使之等于 $d(x)$,即找到如下形式的等式

$$u(x)a(x)+v(x)b(x)=d(x) \tag{4}$$

初始条件为

$$u_{-1}(x)=1,v_{-1}(x)=0,r_{-1}(x)=a(x)$$

$$u_0(x)=0,v_0(x)=1,r_0(x)=b(x)$$

对于 $i\geqslant 1$,定义 $q_i(x)$ 和 $r_i(x)$ 分别为 $r_{i-2}(x)$ 除以 $r_{i-1}(x)$ 的商和余式

$$r_{i-2}(x)=q_i(x)r_{i-1}(x)+r_i(x) \tag{5}$$

而多项式 $u_i(x)$ 和 $v_i(x)$ 定义为

$$u_i(x)=u_{i-2}(x)-q_i(x)u_{i-1}(x) \tag{6}$$

$$v_i(x)=v_{i-2}(x)-q_i(x)v_{i-1}(x) \tag{7}$$

由于余式 $r_i(x)$ 的次数是严格递减的,最后将出现一个非零项,记为 $r_n(x)$.已经证实 $r_n(x)$ 就是 $a(x)$ 和 $b(x)$ 的最大公约数.

文献[24]利用欧几里得算法的实现了式(3)的快速求解,相比于求解线性方程组算法,该算法大大减少了计算量,增强了盲识别的实时性,但算法只使用于1/2码率卷积码.通过对欧几里得算法进行改进,能够实现高码率卷积码校验矩阵的快速求解.

2.3　基于 Walsh-Hadamard 变换的求解算法

利用Walsh-Hadamard变换可以求解式(2)中的数学模型[27],$\boldsymbol{V}$ 中每一行的码字是长度为 L 的二进制向量 $\boldsymbol{v}_L$,将 $\boldsymbol{v}_L$ 转化为十进制数 v,在 $2^L\times 2^L$ 的 Hadamard 矩阵 $\boldsymbol{H}^L$ 中找出第 $v+1$ 行,该行为1元素的位置 c 的二进制向量 $\boldsymbol{c}_L$ 就是方程的解.上述求解过程可以用下面的公式表示

$$\mathscr{H}(\boldsymbol{v})=[\underbrace{0,0,\cdots,0}_{v},1,0,\cdots,0]\boldsymbol{H}^L=[x_1\ x_2\cdots\ x_{2^L}] \tag{8}$$

其中 $x_i=\pm 1$,$\boldsymbol{v}=[\underbrace{0,0,\cdots,0}_{v},1,0,\cdots,0]$ 称为方程对应的向量,$\mathscr{H}(\boldsymbol{v})$ 称为 $\boldsymbol{v}$ 的沃尔什谱.设其中的 x_j,$j=[0,1,\cdots,2^L-1]$ 为1,则 j 转化为 L 维二进制向量就是方程的解,显然这样的解有 2^{L-1} 个.对 $\boldsymbol{V}$ 中的每行码字进行求解,其解的公共部分就是方程组的解.因为Walsh-Hadamard变换为线性运算,可先将每个码字转化为十进制数,并统计每个数出现的次数,转化为方程组对应的向量,进行一次Walsh-Hadamard变换,最后峰值

所在位置的二进制向量就是方程组的解.

当方程组中包含有错误方程时,假设第 k 个方程出错,则得到的 $\boldsymbol{v}^k$ 和 $\mathscr{H}(\boldsymbol{v})^k$ 是错误的,使得方程组公共解所在位置的值可能为 -1,导致 Walsh 谱峰值达不到方程总个数 N,而是 $N-2$. 当错误方程个数不多时,满足正确解的方程仍占大多数,虽然峰值幅度下降,但 Walsh 谱的均值为 0,使得仍能对峰值有效地进行检测,因此基于 Walsh-Hadamard 变换的识别算法具有很强的误码适应能力.

但随着方程组中未知数个数的增加,Walsh-Hadamard 变换的计算量也成指数增加. 对于高码率卷积码,求解校验矩阵方程组的未知数个数超过 50 个,Walsh-Hadamard 变换的计算量则超过 50×2^{50},计算量和计算机所需内存都难以接受,在实际中无法应用.

文献[25]将 $1/n$ 码率卷积码拆分为多个 1/2 码率卷积码,利用 Walsh-Hadamard 变换解决了 $1/n$ 码率卷积码的盲识别问题,文献[26]则对 Walsh-Hadamard 变换进行了改进,将高码率卷积码进行分段的 Walsh-Hadamard 变换,并对分段部分进行循环,直至计算出全部的分段 Walsh-Hadamard 变换,算法解决了内存空间不足的问题,但计算量并未减少.

2.4 卷积码生成矩阵求解算法

前文所介绍的算法可实现对卷积码校验矩阵 $\boldsymbol{H}$ 的求解,但对卷积码进行译码,还需要对卷积码的生成矩阵 $\boldsymbol{G}$ 进行估计,$\boldsymbol{H}$ 与 $\boldsymbol{G}$ 存在如下校验关系[7]

$$\boldsymbol{G}\cdot\boldsymbol{H}^{\mathrm{T}}=0 \tag{9}$$

因为 $\boldsymbol{H}$ 与 $\boldsymbol{G}$ 的校验关系为一对多的不定方程组,主要的方法有求出全部解,并选取次数最低解的组合进行译码验证[3];或者求解出其中一个解,对该解进行矩阵变换使其次数降到最低,并通过译码验证得到最终的生成矩阵[17].

2.5 算法性能分性

在算法性能分析时,计算量是一个重要的指标,本文中一次有限域加法和乘法的计算量定义为 1 次运算,实数域中加法的计算量为 1 次运算,乘法的运算时间约为加法的 4 倍,因此一次乘法运算定义为 4 次运算,下面对各卷积码识别算法的计算量进行分析.

假设卷积码校验矩阵多项式的最高阶数为 m,卷积码输出路数 n,则列方程组所需要的码元长度 $N>=(n+1)\times(m+1)$,求解线性方程组所需的计算量为 $O(N^3)$,文献[22]对算法进行优化,使得算法的计算量减少为 $O(N^2)$. 基于欧几里得算法的求解算法最多需要 $N^2/2$ 次多项式乘法和加法运算,而基于 Walsh-Hadamard 变换的求解算法的计算量则为 $(m+1)n\cdot 2^{(m+1)n}$. 三种算法在求解 CCSDS 标准卷积码校验矩阵的计算量如所图 1 所示,不难看出,基于欧几里得算法的计算量最小,而 Walsh-Hadamard 变换算法的计算量远大于其他两种算法.

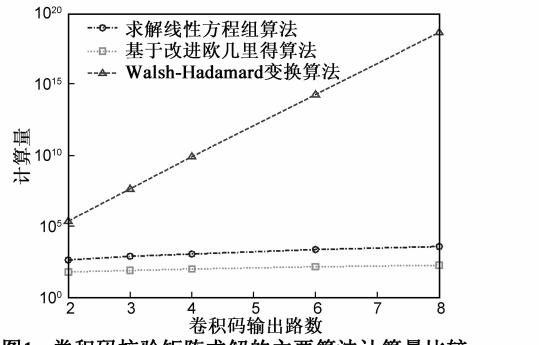


图1 卷积码校验矩阵求解的主要算法计算量比较

利用上述三种算法对 CCSDS 中的卷积码校验矩阵进行求解,算法的误码适应能力如图 2 所示. 图中的误码适应能力以正确识别率在 90% 以上为准. 从图中可以看出,求解线性方程组算法与基于欧几里得算法的误码适应能力相差不大,而基于 Walsh-Hadamard 变换算法的误码适应能力则明显优于上述两种算法,性能提高了一个数量级以上.

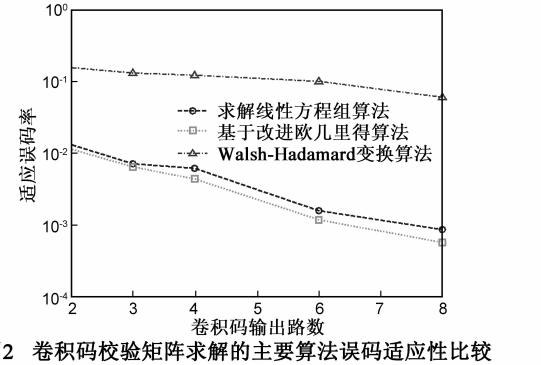


图2 卷积码校验矩阵求解的主要算法误码适应性比较

综上所述,在信号解调良好,误码率低于 10^{-3} 时,宜采用基于欧几里得算法以实现快速求解;在信号解调误码率较高时,则采用 Walsh-Hadamard 变换算法,实现在高误码环境下的正确求解.

3 BCH 码、RS 码盲识别算法

BCH 码和 RS 码同属循环线性分组码,BCH 码是构造成熟、应用广泛的一类二进制线性分组码[7],在 CCSDS 标准[30]及 DVB-S2 标准[31]中都采用了 BCH 编码. RS 码是能够纠正多个随机错误的多进制循环线性分组码[7],具有较强的纠错能力和严格的代数结构,且具有构造方便、编码简单的优点,已经广泛应用于数字通信系统中,卫星通信中广泛采用 CCSDS 标准推荐的(255,223)和(255,239)RS 码[8]以及在 DVB-S 链路中采用(204,188)截短 RS 码[32]等.

在线性分组码的盲检测与识别方法上,Antoine Val-

embois[33]率先提出了基于求解对偶码的二进制线性码检测方法,随后文献[35]、[36]和[37]~[40]分别研究了基于 BM 迭代算法和基于码重分布的二进制线性码的检测方法.而对于 BCH 码和 RS 码,则主要有基于欧几里得算法[41,42]、基于码根信息差熵和码根统计算法[43~47]和基于有限域傅立叶变换的检测识别方法[48~50].

3.1　基于欧几里得算法的识别算法

上文已对欧几里得算法进行了描述,BCH 码字序列$[v_0, v_1, \cdots, v_{n-1}]$可表示为多项式

$$v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1} \tag{10}$$

由 BCH 码的编码过程可知

$$v(x) = u(x) \cdot g(x) \tag{11}$$

其中,$u(x)$为信息序列多项式,$g(x)$为生成多项式.若已知 q 个码字,利用欧几里得算法便能得到生成多项式 $g(x)$,即

$$g(x) = \gcd\{v_1(x), v_2(x), \cdots, v_q(x)\} \tag{12}$$

其中"gcd"表示最大公约式.

根据二进制 BCH 码的原理有

$$g(x) = \mathrm{lcm}\{\phi_1(x), \phi_2(x), \cdots, \phi_{2t}(x)\} \tag{13}$$

其中,"lcm"表示最小公倍式,构造伽罗华域 $GF(2^m)$的本原多项式 $p(x) = \phi_1(x)$,由 $\phi_1(x)$则可以计算出 $\phi_2(x), \cdots, \phi_{2t}(x)$,从而既可以确定本原多项式 $p(x)$,还可以验证 $g(x)$是否是二进制 BCH 码的生成多项式,同时完成了检测与参数估计.

文献[41]假定码长已知或码长未知而帧长度已知,对码字进行分组,采用欧几里得算法,实现了二进制 BCH 码的盲识别.文献[42]则将 RS 码等效为二进制码,同样利用欧几里得算法,实现了 RS 码的盲识别,但从上文分析可知,欧几里得算法虽然计算量小,但对码字的误码率要求比较高,一般需要在 10^{-3}以下.

3.2　基于码根信息差熵和码根统计的识别算法

文献[43]提出了基于码根信息差熵和码根统计的 BCH 码识别方法,对于码长为 n 的循环码码字,其码根个数为 $n-1$,范围为 $0 \sim n-1$,并且其分布具有一定的规律,即生成多项式 $g(x)$的根在每个码字中均会出现,而每个码字中其他的码根是随机出现的,对于错误的码字,其所有的根都是随机出现的,设每个码根出现的概率为 p,则

$$p = 1/n \tag{14}$$

对多个码字的根进行求解,其所有解的公共部分即为 $g(x)$的解.文献给出了码根信息差熵函数,即实际测得的码根分布信息熵与均匀分布的码根分布信息熵的差值

$$\Delta H = \frac{1}{n} \sum_{i=1}^{n} \lg p_i + \lg \frac{1}{n} \tag{15}$$

利用码根信息差熵函数识别 BCH 码的码长,进而利用码根统计获取生成多项式的整数根,通过遍历该域中的本原多项式以寻求满足 BCH 码生成多项式根性质的码根和本原多项式,从而实现 BCH 码的盲识别.

文献[47]将该算法进行了改进,利用有限域同构的原理,由统计得到的码根经过有限域乘法并化简直接求出 BCH 码的生成多项式,避免了原算法遍历本原多项式带来的计算量.文献[45]、[46]则将 RS 码转换为等价二进制码,求解其根值,并利用上述方法实现了 RS 码的盲识别.

3.3　基于有限域傅立叶变换的识别算法

RS 编码过程与 BCH 一致,令 $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$为 $GF(2^m)$上的 RS 码字多项式,其中 n 能够整除 $2^m - 1$ 并且 $n \neq 1$.令 α 为 $GF(2^m)$中阶数为 n 的元素.于是,$\alpha^n = 1$ 并且 α 是 $x^n - 1$ 的根.$v(x)$的有限域傅立叶变换定义为 $GF(2^m)$上的多项式

$$V(X) = V_0 + V_1 X + \cdots + V_{n-1} X^{n-1} \tag{16}$$

其中对于 $0 \leqslant j < n$,

$$V_j = v(\alpha^j) = \sum_{i=0}^{n-1} v_i \alpha^{ij} \tag{17}$$

系数 V_j 被称为 $V(X)$的第 j 个谱分量,且第 j 个谱分量 V_j 为 0,当且仅当 α^j 是 $v(x)$的一个根.

多项式 $v(x)$和 $V(X)$构成一组变换对,考虑长度 $n = 2^m - 1$、纠 t 个错误的 RS 码,其生成多项式 $g(x)$以 $\alpha, \alpha^2, \cdots, \alpha^{2t}$为根.则 $V(X)$从位置 X 到位置 X^{2t}的 $2t$ 个连续的谱分量均为 0,即 $V_1 = V_2 = \cdots = V_{2t} = 0$,这就是 RS 码的频域特征[7].

文献[48]利用 RS 码的频域特征进行 RS 码的盲检测,首先利用矩阵化简的方法识别 RS 码码长,再对码字进行有限域的傅立叶变换,从而根据频谱的连零性质进行 RS 码检测.针对有误码的情况,文献将连续的零频分量权重定义为 0.99,将非零的频谱权重定义为 0.01,利用统计的方法对 RS 码进行识别.文献[49]、[50]则分别将 RS 码进行等价二进制变换,分别利用码根统计和欧几里得算法来估计 RS 码的码长,最后采用有限域傅立叶算法对 RS 码的生成多项式和本原多项式进行估计.

3.4　算法性能分析

对于码长为 $m \times n = m \times (2^m - 1)$的一个码字,采用欧几里得算法得到码字的最大公约式需要进行$(m^2 \times n^2)/2$ 次模 2 和运算,而一次有限域傅立叶变换算法需要进行 $n^2 - n$ 次 $GF(2^m)$上的加法和 n^2 次 $GF(2^m)$上的乘法,则总共等效为模 2 和运算量为:$3m^2n^2 - 2mn^2 - mn$ 次[49].基于码根信息差熵和码根统计的算法中,求解多项式根的计算复杂度为 $O(m^2n^2)$,假设统计码

字个数为 N,设单个码字的根个数平均为 l,则码根统计需要的计算量约为$(N-1)\cdot l\cdot O(m^2n^2)$.若全部对 N 个码字进行上述算法求解,则各算法主要计算量如图 3 所示,不难看出,欧几里得算法算法的计算量最小,其余两种算法计算量相差不多.

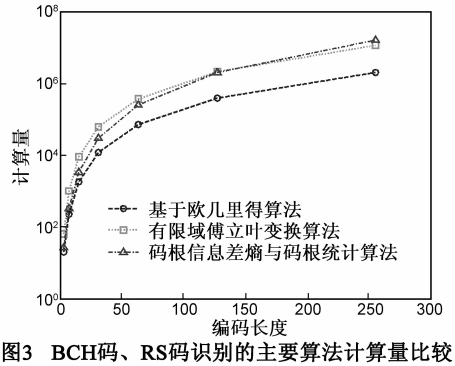


图3 BCH码、RS码识别的主要算法计算量比较

分别取 200 组各种长度的 BCH 码,对上述三种算法的误码适应能力进行比较,结果如图 4 所示,图中的误码适应能力以正确识别率在 90% 以上为准,从图中可以看出,欧几里得算法误码适应能力较弱,其余两种算法误码适应能力相差不多,有限域傅立叶变换算法略好一些.

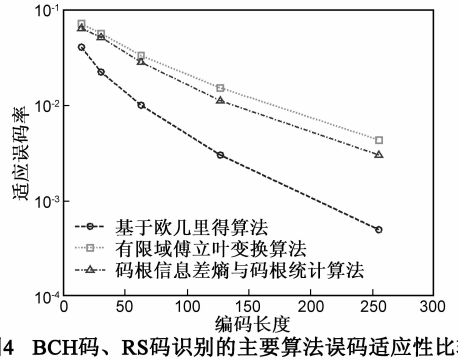


图4 BCH码、RS码识别的主要算法误码适应性比较

4 Turbo 码盲识别算法

1993 年 Berrou 等提出 Turbo 码,通过并行编码,引入随机交织器和带有反馈的迭代译码结构,首次获得了接近 Shannon 理论极限的性能,成为信道编码史上的一个重大突破[51].Turbo 码已被美国空间数据系统顾问委员会作为深空通信的标准,同时它也被确定为第三代移动通信系统(IMT-2000)的信道编码方案之一,Turbo 码已经成为下一代卫星通信系统的核心技术之一.

Turbo 码由两个递归循环卷积码通过交织器以并行级联的方式结合而成,因此又称为并行级联卷积码,所以 Turbo 码的盲检测与识别可以分为卷积码的检测识别与交织器的检测识别两部分,卷积码的检测识别技术已经比较成熟,针对交织器的检测识别研究较少,文献[52]、[53]给出了矩形交织器的参数估计方法;文献[54]、[55]则对卷积交织器的盲识别进行了研究.但 Turbo 码一般进行伪随机交织来获得更高的编码增益,针对 Turbo 码的盲识别算法,目前相关文献主要有[56]~[59].

4.1 Turbo 码盲识别算法描述

Mathieu Cluzeau 在文献[56]中对编码序列进行分路,得到信息序列 A、原始编码序列 B 和交织后的编码序列 C,并选取多个样本数据,利用 A 和 C 对交织器进行逐位恢复,对每一位交织图案列出多个候选,并计算出由每位候选带给卷积分量码编码器状态的平均信息熵,通过设定检测门限对候选进行排除,最终经过 N 步排除,最终得到整个交织器的交织图案.

Maxime Côte 在文献[57]中分两种情况对 Turbo 码交织器进行了识别,一是第二个分量编码器参数已知且信息序列无差错;二是第二个分量编码器参数未知且信息序列无差错.在分量编码器参数已知时,利用多项式为最低项总为 1,所以 C 输出的第一位 c_0 即为信息序列通过交织置换到第一位的值 $a_{\pi(0)}$,可以根据 M 个样本数据恢复出 $\pi(0)$,并逐位恢复 $\pi(1),\cdots,\pi(N-1)$.在恢复 $\pi(i)$时,利用前面恢复出的 $\pi(j)(j<i)$和分量码编码器参数,计算

$$u_i = c_i - \sum_{j=0}^{i-1} a_{\pi(j)} g_{i-j} \tag{18}$$

g_j 为编码器多项式系数.利用 M 个样本数据在 A 中找出与 u_i 相关最大的值,该值对应的位置即为 $\pi(i)$.在分量编码器参数未知时,算法在恢复 $\pi(i)$时,计算变量

$$v_i = c_i - \sum_{j=1}^{i-1} a_{\pi(j)} g_{i-j} = u_i + a_{\pi(0)} g_i \tag{19}$$

由于 g_i 非 0 即 1,根据 $a_{\pi(0)}$的值为 0 或 1,得到两个不同的变量 α_i 和 β_i,并利用 M 个样本数据在 A 中找出与 α_i 和 β_i 相关最大的值,该值位置即为 $\pi(i)$,且如果 $\alpha_i>\beta_i$,$g_i=0$;否则 $g_i=1$.

Ali Naseri 在文献[58]中提出了一种基于矩阵高斯三角化的 Turbo 码参数识别方法,简称为 Naseri 算法.Naseri 算法按不同的分段长度将码序列转换为一个 N_r 行和 N_c 列的矩阵 $\boldsymbol{H}$,N_c 初始化为 1,则 N_r 等于码长 L/N_c,对矩阵进行高斯三角化,得到矩阵 $\boldsymbol{H}_G$,N_c 递增加 1,直至 $N_r<N_c$.计算

$$R_n = \frac{N_c - \boldsymbol{Z}}{N_c} = \begin{cases} 1, & N_c \neq pn \\ <1, & N_c = pn \end{cases} \tag{20}$$

其中,$\boldsymbol{Z}$ 为 $\boldsymbol{H}_G$ 中全部为 0 的列,n 为 Turbo 码的输出路数,p 为一个正整数.通过多个 R_n 幅度的变化情况,Naseri 算法可以识别 Turbo 码的码率、交织器大小、分量码生成多项式阶数等参数,但无法识别分量码生成多项式及交织器图案等参数,且由于采用了矩阵变换算

法,因此算法对于误码的适应能力较差.

文献[59]通过对 Turbo 码中的卷积分量码的识别,可以确定交织器大小 N、交织起点、交织前信息序列和交织后的编码序列.如要确定交织前 $i(1\leqslant i\leqslant N)$处所对应的交织后置换位置 j,可以从从交织帧起始点开始,不断连续比对交织前后对应交织长度内位置的数据,当连续多帧都是惟一对应并且没有其他点重合对应时,即可确定该点的对应关系,从而继续进行下一个交织关系的确定,从识别原理上与 Côte 算法相似,都属于多样本数据的一阶相关统计算法.

4.2　Turbo 码盲识别算法性能分析

Turbo 码盲识别算法的主要计算量在交织器图案的估计上面,Naseri 算法不能识别交织器图案,因此本文只对其余三种算法的计算量进行分析.

假设交织器大小为 N,选取的样本数为 M,分量编码器多项式阶数为 m,Cluzeau 算法需要进行 N 步计算,每一步的计算复杂度为 $O(NM^2\cdot 2^m)$,则算法总共计算复杂度为 $O(N^2M^2\cdot 2^m)$[56].Côte 算法提出的算法同样需要 N 步完成,在计算第 i 步时,需要计算需要计算 $N-i$ 次 u_i,且每次的计算量为 i,因此总的计算量为 $\sum_{i=1}^{N}M\cdot i\cdot(N-i)\approx MN^3/6$,如果在每一步后对 $\sum_{j=0}^{i-1}a_{\pi(j)}g_{i-j}$进行存储,则可以将计算 u_i 的计算量减少到 1 次,因此总的计算量约为 $MN^2/2$.文献[59]提出的算法与 Côte 算法相似,其总的计算量也约为 $MN^2/2$.下面给出分量码生成多项式阶数为 2 时,在 50 个样本数据下,不同长度交织器识别所需要的计算量,如图 5 所示.

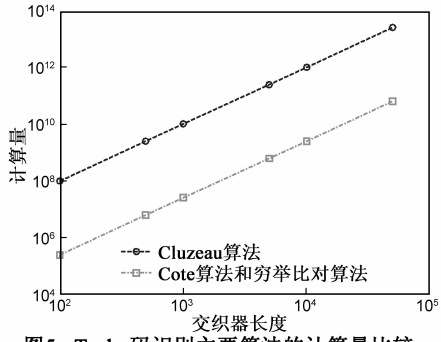


图5　Turbo码识别主要算法的计算量比较

从图中可以看出,Cluzeau 算法计算量较大,但该算法的优势是可以适应一定的误码;Côte 算法与穷举比对算法计算量较小,但前提条件是信息序列中不含误码.因此在实际应用中,可以根据信道环境选择合适的算法.

5　扰码盲识别算法

通常所采用的伪随机扰码都是由移位寄存器生成的 m 序列,通过对数据进行模 2 和可实现数据的伪随机化,能够有效降低数据中出现的突发错误,在通信和密码中有着广泛的应用.目前对伪随机扰码的盲识别方法主要有基于组合枚举方法[60,61]、基于匹配搜索方法[62]、基于沃尔什变换算法[63]、基于高阶统计量算法[64]、基于与 BCH 码等价原理[65]和基于输入序列统计偏差算法[66]的扰码识别方法.

5.1　扰码盲识别算法描述

文献[60]提出了基于组合枚举求解优势值的扰码多项式估计算法,算法定义了优势值函数

$$T=(N_0-N_1)/\sqrt{N} \tag{21}$$

其中,N 为输出序列位数,N_0、N_1 分别为输出序列中 0、1 的个数,通过对移位寄存器抽头系数进行枚举组合,找出其中最大的优势值,则该优势值对应的抽头系数即为扰码生成多项式,进而采用基于卷积码的快速相关攻击算法对扰码的初态进行盲恢复.算法对抽头数大于 5 的扰码进行生成多项式估计时,其枚举组合数会迅速增加,导致算法的计算量较大.

基于匹配搜索的方法[62]与组合枚举的方法类似,根据移位寄存器输入与输出的关系,列出齐次线性方程组通过搜索多项式系数,找出方程组符合最多的解,即为多项式系数.

文献[63]则采用沃尔什变换法对扰码序列的生成多项式进行了测定.对式(22)中的线性方程组按 2.3 节方法进行求解,该方法较之组合枚举和匹配搜索法,计算复杂度大为降低.

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{L-1} & a_L \\ a_1 & a_2 & \cdots & a_L & a_{L+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_L & a_{L+1} & \cdots & a_{2L-1} & a_{2L} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}\cdot\begin{bmatrix} c_L \\ c_{L-1} \\ \vdots \\ c_1 \\ 1 \end{bmatrix}=0 \tag{22}$$

文献[64]提出了基于高阶统计原理的 m 序列本原多项式的测定方法.通过寻找含错 m 序列的高阶统计峰值求得本原多项式的高阶倍式,再通过求高阶倍式的最大公约式推导出该序列的本原多项式.

文献[65]则将 m 序列扰码的生成过程与 BCH 码等价,将 m 序列构造与之等价的 BCH 码,利用 BCH 码良好的纠错性能,实现高误码条件下的 m 序列生成多项式的估计,但该算法遍历次数多,计算量大.

上述几种算法都是基于扰码已知,或者扰码中带有误码的情况下,求解扰码的生成多项式,而实际情况中,则需要先从加扰数据中将扰码分离出来,再进行扰码的多项式估计.对此,文献[66]利用大量加扰前数据的统计偏差,估计生成多项式的倍式,进而利用高阶倍式的最大公约式得到扰码的生成多项式.文献[67]对上

述算法进行了改进,提高了算法的检测和抗误码的能力.

5.2 扰码盲识别算法性能分析

假设接收的扰码数据长度为 L,抽头数为 m,生成多项式阶数为 l,则枚举组合算法的组合次数为 $\sum_{i=3}^{l_{\max}} C_{i-2}^{m-2}$,$l_{\max}$为算法搜索多项式的最大阶数.每次需要计算数据经过该抽头系数组合时的输出序列 B 以及优势值 T,计算量约为$(m-1)L$.因此算法总的计算量为 $\sum_{i=3}^{l_{\max}} C_{i-2}^{m-2}(m\text{-}1)L$.基于匹配搜索算法则需要 $2^{l+2}l$ 次乘法和 $2^{l+2}(l-1)$加法运算,经过优化后,算法的总计算量减少为 $3\cdot 2^{l+1}l - 3\cdot 2^{l/2-1}l$[62].基于 Walsh 变换算法的计算量已经分析过为 $l\cdot 2^{l+1}$,而高阶统计测定算法的计算量为 $N\cdot 2^l$,N 为统计次数,一般为几百至上千次,否则无法将峰值与非峰值的概率分布区分开来.文献[65]提出的算法需要遍历 l 阶的本原多项式,且需要构造不同的错误位数来进行 BCH 码的译码,最后利用 BM 算法进行扰码多项式的求解.其中构造错误位数次数最大为 2^{l-2},每次进行译码的计算量约为 2^{2l},因此算法的计算量约为 2^{3l-2}.而文献[66]提出的算法计算量约为 $m2^lN_p$,其中 N_p 为算法平均所需的统计位数,在文献中 N_p 约为 $4e^4$.在抽头数为 3,数据长度为 $4e^4$ 时,不同扰码多项式阶数情况下,各算法的计算量如图 6 所示.

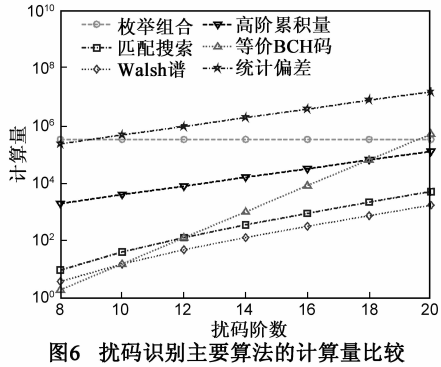


图6 扰码识别主要算法的计算量比较

从图中可以看出,基于 Walsh 谱算法的计算量最小,基于输入信息序列统计偏差算法的计算量最大,而基于等价 BCH 码算法的计算量增长最快,因此该算法一般适用于扰码阶数较低的情况.

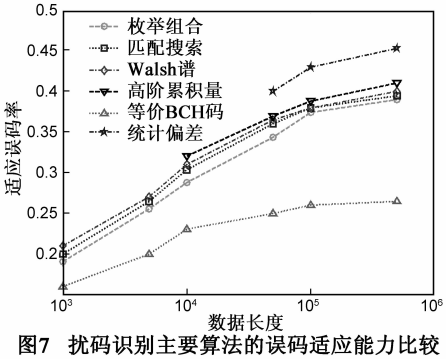


图7 扰码识别主要算法的误码适应能力比较

取不同数据长度对各算法的误码适应能力进行分析,扰码阶数为 11,抽头数为 3,误码适应能力以正确识别率在 90% 以上为准,结果如图 7 所示.

从图中可以看出,各算法的误码适应能力较强,基于输入统计偏差的扰码识别算法误码适应能力最好,但该算法只适合在大数据量下处理.基于等价 BCH 码的算法误码适应能力较弱,原因是 BCH 码纠错能力有限,超出 BCH 码纠错能力的误码则无法识别.其余算法的误码适应能力则相差不多.

6 总结与展望

本文对现有信道编码盲识别技术的主要算法进行了描述,并对算法的计算量与误码适应能力进行了分析.通过对目前信道编码盲识别算法的分析与总结,可以预测未来信道编码盲识别技术的主要研究方向:

(1)高码率卷积码盲识别及生成多项式估计.在卷积码盲识别和生成多项式估计方面,目前比较成熟的算法都是针对 1/2 码率提出的,对于高码率卷积码,现有算法存在计算量大、误码适应能力低的问题.

针对高码率卷积码的盲识别,可以考虑采取基于最大似然的估计方法,由于误码的影响,使得卷积码与其校验多项式的乘积不全为 0,通过最大似然的方法找到与卷积码乘积的重量最低的向量,则该向量即为卷积码的校验多项式,通过设置合理的检测门限,可以实现在高误码率环境下较高的检测概率.

(2)高误码率条件下的信道编码盲识别.对信道编码的盲识别是基于非合作信号处理和数字盲解调的条件下进行的,由于信号本身的信噪比较低和参数估计带来的误差,使得解调数据中存在较多的误码,误码率可能达到 10^{-2}量级.目前现有算法的误码适应能力尚达不到这一需求,不具备较好的实际应用能力.

针对高误码条件下的信道编码识别问题,Walsh-Hadamard 变换是一个有效的方法,但对于长码的识别,计算量和内存的需求使其难以应用,可以考虑基于 Walsh 谱上峰值的稀疏性,或者分段的 Walsh 谱来解决计算量大和内存不足的问题.

(3)Turbo 码及交织器的盲识别.目前 Turbo 码盲识别的关键问题在于编码时所采用的伪随机交织器的识别,已有的一些算法都是针对分组交织器、卷积交织器等确定性交织器的,对于伪随机交织器的识别只有逐步恢复的一阶相关统计方法,过程较为复杂,同时,多重 Turbo 码和删除 Turbo 码也得到了越来越多的应用,需要进一步研究其识别的数学模型,探索 Turbo 码识别的新思路.

(4)LDPC 码的盲识别.LDPC 码是一类逼近香农限的编码,其码编解码简单、时延小等特点非常适合高速信息传输系统,是未来卫星通信系统的首选信道编码方案[68].LDPC 码的优异性能也使它成功击败 Turbo 码,成为 ETSI 的第二代卫星数字广播标准 DVB-S2 中的标准编码.虽然目前尚未有 LDPC 码识别的文献报道,但随着 LDPC 编码在通信系统中越来越多的使用,对 LDPC 码的识别研究已成为信道编码识别技术中的一个迫切需求.

对于 LDPC 码,由于其码元长度较大,一般几千至上万比特,因此常规的矩阵分析、求解线性方程组、Walsh-Hadamard 变换等在大长度编码前很难得到应用,因此可从特定的 LDPC 码入手.如 DVB-S2 中包含 21 种 LDPC 码,其校验矩阵已知,且稀疏性良好,可以考虑利用校验矩阵的稀疏性,对接收的码序列进行稀疏校验,并对校验结果进行统计,可以实现特定 LDPC 码的识别,对于缺乏先验信息的大长度 LDPC 码的识别,仍是信道编码盲识别中的难点问题.

(5)数据盲解扰.目前对于扰码的盲识别主要体现在扰码的多项式和初相的估计上,而盲解扰的关键问题是如何从加扰数据中提取扰码,这是扰码多项式估计的前提条件,也是数据盲解扰的关键环节.因此需要进一步研究从加扰数据中提取扰码的有效方法.

总体来说,目前国内外对信道编码的盲识别问题已经做了大量的研究,取得了一系列丰硕的成果,但同时也存在着许多难点问题有待解决,新的数学模型和方法有待探索.

参考文献

[1] 张平,王卫东,陈月华.WCDMA 移动通信系统的信道编码技术的研究[J].电子学报,1999,27(11):16 – 20.
Zhang Ping, Wang Wei-dong, Chen Yue-hua. Study of channel coding technology in WCDMA mobile communications systems [J]. Acta Electronica Sinica, 1999, 27(11): 16 – 20. (in Chinese)

[2] Reza Moosavi, Erik G. Larsson. A fast scheme for blind identification of channel codes[A]. Global Telecommunications Conference 2011[C]. Linkoping, Sweden: IEEE Press, 2011. 1 – 5.

[3] 张永光,楼才义.信道编码及其识别分析[M].北京:电子工业出版社,2010.
Zhang Yong-guang, Lou Cai-yi. Channel Coding Recognition and Analysis[M]. Beijng: Publishing House of Electronics Industry, 2010. (in Chinese)

[4] Julien Bringer, Hervé Chabanne. Code reverse engineering problem for identification codes[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2406 – 2412.

[5] 邹艳.信息截获与处理的容错技术研究[D].上海:复旦大学,2006.
Zou Yan. Research on Error-resilient Techniques of Information Intercepting and Processing[D]. Shanghai: Fudan University, 2006. (in Chinese)

[6] 宋镜业.信道编码识别技术研究[D].西安:西安电子科技大学,2009.
Song Jing-ye. Research on Technique of Channel Coding Recognition[D]. Xi′an: Xidian University, 2009. (in Chinese)

[7] J H van Lint. Introduction to Coding Theory[M]. Beijing: World Publishing Corporation, 2003.

[8] CCSDS 131. 0-B-1-2003, TM Synchronization and Channel Coding[S].

[9] B Rice. Determining the parameters of a rate $1/n$ convolutional encoder over GF(q)[A]. Proceedings of the 3rd International Conference on Finite Fields and Applications[C]. Glasgow, USA: IEEE Press, 1995.

[10] Eric Filiol. Reconstruction of convolutional encoders over GF(q)[J]. Lecture Notes in Computer Science, 1997, 1355: 101 – 109.

[11] A J Han Vinck, Petr Dolezal, Young-Gil Kim. Convolutional encoder state estimation[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1604 – 1608.

[12] Phillip L Boyd. Recovery of Unknown Constraint Length and Encoder Polynomials for Rate 1/2 Linear Convolutional Encoders[D]. California: Naval Graduate School, 1999.

[13] Johann Barbier, Guillaume Sicot, Sebastien Houcke. Algebraic approach for the reconstruct-tion of linear and convolutional error correcting codes[J]. International Journal of Applied Mathematics and Computer Science, 2006, 2(3): 113 – 118.

[14] Maxime Cote, Nicolas Sendrier. Reconstruction of convolutional codes from noisy observation[A]. International Symposium on Information Theory 2009[C]. Seoul, Korea: IEEE Press, 2009. 546 – 550.

[15] Janis Dingel, Joachim Hagenauer. Parameter estimation of a convolutional encoder from noisy observations[A]. International Symposium on Information Theory 2007[C]. Nice, France: IEEE Press, 2007. 1776 – 1780.

[16] 周亚建,刘健.(n, $n-1$, m)卷积码的盲识别[J].北京邮电大学学报,2010,33(3):135 – 138.
Zhou Ya-jian, Liu Jian. A blind recognition of the(n, $n-1$, m)convolution code[J]. Journal of Beijing University of Posts and Telecommica-tions, 2010, 33(3): 135 – 138. (in Chinese)

[17] Lu Pei-zhong, Shen Li, Zou Yan, Luo Xiang-yang. Blind recognition of punctured convolutional codes[J]. Science in China Ser. F Information Sciences, 2005, 48(4): 484 – 498.

[18] Mathieu Cluzeau, Matthieu Finiasz. Reconstruction of punctured convolutional codes[A]. Information Theory Workshop 2009[C]. Taormina: IEEE Press, 2009. 75 – 79.

[19] 薛国庆.卷积码的盲识别研究[D].合肥:中国科学技术

大学,2009.
Xue Guo-qing. Research on Technique of Convolution Coding Recognition[D]. Hefei: University of Science and Technology of China, 2009. (in Chinese)

[20] 韩国宾.删除卷积码的识别技术[D].成都:电子科技大学,2009.
Han Guo-bin. Blind Recognition of Punctured Convolutional Codes[D]. Chengdu: University of Electronic Science and Technology of China, 2009. (in Chinese)

[21] 柴先明,蔡凯,吕守业,等.卷积码盲识别方法研究[J].电路与系统学报,2010,15(4):38 – 44.
Chai Xian-ming, Cai Kai, Lv Shou-ye, et al. Study on blind recognition of convolutional codes[J]. Journal of Circuits and Systems, 2010, 15(4): 38 – 44. (in Chinese)

[22] 邹艳,陆佩忠.关键方程的新推广[J].计算机学报,2006,29(5):711 – 718.
Zou Yan, Lu Pei-zhong. A new generalization of key equation [J]. Chinese Journal of Computers, 2006, 29(5): 711 – 718. (in Chinese)

[23] Pei-zhong Lu, Yan Zou. Fast computations of gröbner bases and blind recognitions of convolutional codes[J]. Lecture Notes in Computer Science, 2007, (4547): 303 – 317.

[24] Wang Feng-hua, Huang Zhi-tao, Zhou Yi-yu. A method for blind recognition of convolution code based on Euclidean algorithm[A]. IEEE International Conference on Wireless Communications[C]. Shanghai: IEEE Press, 2007. 1414 – 1417.

[25] 刘健,王晓君,周希元.基于 Walsh-Hadamard 变换的卷积码盲识别[J].电子与信息学报,2010,32(4):884 – 888.
Liu Jian, Wang Xiao-jun, Zhou Xi-yuan. Blind recognition of convolutional coding based on Walsh-Hadamard transform [J]. Journal of Electronics&Information Technology, 2010, 32 (4): 884 – 888. (in Chinese)

[26] 戚林,郝士琦,王磊.基于改进 Walsh-Hadamard 变换的删除卷积码盲解码算法[J].计算机应用研究,2011,28(4):1457 – 1459.
Qi Lin, Hao Shi-qi, Wang Lei. Blind decoding algorithm of punctured convolutional codes based on improved WHT[J]. Application Research of Computers, 2011, 28(4): 1457 – 1459. (in Chinese)

[27] 游凌,朱中梁.Walsh 函数在解二元域方程组上的应用[J].信号处理,2000,16(12):27 – 32.
You Ling, Zhu Zhong-liang. The application of Walsh function in resolving of F(2) equations[J]. Signal Processing, 2000, 16 (12): 27 – 32. (in Chinese)

[28] Melanie Marazin, Roland Gautier, Gilles Burel. Blind recovery of k/n rate convolutional encoders in a noisy environment[J]. Wireless Communications and Networking, 2011, 2011(1): 1186 – 1687.

[29] M Marazin, R Gautier, G Burel. Dual code method for blind identification of convolutional encoder for cognitive radio receiver design [A]. GLOBECOM Workshops 2009 [C]. Rennes, France: IEEE Press, 2009. 1 – 6.

[30] CCSDS 231.0-B-1-2003, TC Synchronization and Channel Coding[S].

[31] ETSI EN 302 307 – 2009, Second Generation Framing Structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and other Broadband Satellite Applications[S].

[32] EN 300 421 – 1997, Framing Structure, Channel Coding and Modulation for 11/12GHz Satellite Services[S].

[33] Antoine Valembois. Detection and recognition of a binary linear code[J]. Discrete Applied Mathematics, 2001, 111: 199 – 218.

[34] 肖芳英,陈汉武,刘志昊,等.有限域上非本原 BCH 码的对偶包含判定[J].电子学报,2010,38(8):1858 – 1861.
Xiao Fang-ying, Chen Han-wu, Liu Zhi-hao, et al. Dual-containing determination method for non-primitive BCH codes over finete field[J]. Acta Electronica Sinica, 2010, 38(8): 1858 – 1861. (in Chinese)

[35] Mathieu Cluzeau. Block code reconstruction using iterative decoding techniques[A]. International Symposium on Information Theory 2006[C]. Seattle, USA: IEEE Press, 2006. 2269 – 2273.

[36] 刘菁.卷积码和循环码识别技术研究[D].西安:西安电子科技大学,2010.
Liu Jing. Research on Technique of Convolution Code and Cyclic Code Recognition[D]. Xi'an: Xidian University, 2010. (in Chinese)

[37] Christophe Chabot. Recognition of a code in a noisy environment[A]. International Symposium on Information Theory 2007[C]. Nice, France: IEEE Press, 2007. 2211 – 2215.

[38] 咎俊军,李艳斌.低码率二进制线性分组码的盲识别[J].无线电工程,2009,39(1):19 – 24.
Zan Jun-jun, Li Yan-bin. Blind recognition of low code-rate binary linear block codes[J]. Radio Engineering of China, 2009, 39(1): 19 – 24. (in Chinese)

[39] 陈金杰,杨俊安.基于码重信息熵低码率线性分组码的盲识别[J].电路与系统学报,2012,17(1):41 – 46.
Chen Jin-jie, Yang Jun-an. A method of blind recognition to low code-rate linear block codes based on weight information entropy[J]. Journal of Circuits and Systems, 2012, 17(1): 41 – 46. (in Chinese)

[40] Wang Lei, Hu Yihua, Hao Shiqi, Qi Lin. The method of estimating the length of linear cyclic code based on the distribution of code weight[A]. 2010 2nd International Conference on Information Science and Engineering[C]. Hefei: IEEE Press, 2010. 2459 – 2462.

[41] Jia-feng Wang, Yang Yue, Jun Yao. A method of blind recog-

nition of cyclic code generator polynomial[A]. Wireless Communications Networking and Mobile Computing 2010 6th International Conference[C]. Chengdu: IEEE Press, 2010. 23 – 25.

[42] 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 Shi-qi, Li Jin-shan. Recognition method of RS codes based on Euclidean algorithm in Galois field[J]. Journal of Detection&Control, 2011, 33(2): 63 – 67. (in Chinese)

[43] 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):70 – 73.
Yang Xiao-jing, Wen Nian-cheng. Recognition method of BCH codes based on roots information dispersion entropy and roots statistic[J]. Journal of Detection&Control, 2010, 32(3): 70 – 73. (in Chinese)

[44] Jia-feng Wang, Yang Yue, Jun Yao. Statistical recognition method of binary BCH code[J]. Communications and Network, 2011, 3: 17 – 22.

[45] 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 Nian-cheng, Yang Xiao-jing. Blind recognition of RS codes parameters[J]. Computer Engineering and Applications, 2011, 47(19): 136 – 139. (in Chinese)

[46] 闻年成,杨晓静,白或.一种新的 RS 码识别方法[J].电子信息对抗技术,2011,26(2):36 – 40.
Wen Nian-cheng, Yang Xiao-jing, Bai Yu. A new recognition method of RS codes[J]. Electronic Warfare Technology, 2011, 26(2): 36 – 40. (in Chinese)

[47] 吕喜在,黄芝平,苏绍▮.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 – 162.
Lv Xi-zai, Huang Zhi-ping, Su Shao-jing. Fast recognition method for generator polynomial of BCH codes[J]. Journal of Xidian University(Natural Science), 2011, 38(6): 159 – 162. (in Chinese)

[48] 刘健,谢锘,周希元.RS 码的盲识别方法[J].电子科技大学学报,2009,38(3):363 – 367.
Liu Jian, Xie Nuo, Zhou Xi-yuan. Blind recognition method of RS coding[J]. Journal of University of Electronic Science and Technology of China, 2009, 38(3): 363 – 367. (in Chinese)

[49] 戚林,郝士琦,王磊,王勇.一种 RS 码快速盲识别方法[J].电路与系统学报,2011,16(2):71 – 76.
Qi Lin, Hao Shi-qi, Wang Lei, Wang Yong. A fast recognition method of RS codes[J]. Journal of Circuits and Systems, 2011, 16(2): 71 – 76. (in Chinese)

[50] 吕喜在,苏绍▮,黄芝平.一种 RS 码快速盲识别方法[J].国防科技大学学报,2011,33(4):123 – 127.
Lv Xi-zai, Su Shao-jing, Huang Zhi-ping. A fast blind recognition method of RS coding[J]. Journal of National University of Defense Technology, 2011, 33(4): 123 – 127. (in Chinese)

[51] 吴伟陵.通向信道编码定理的 Turbo 码及其性能分析[J].电子学报,1998,26(7):35 – 40.
Wu Wei-ling. Turbo codes to channel coding theory and their performance analyses[J]. Acta Electronica Sinica, 1998, 26(7): 35 – 40. (in Chinese)

[52] Guillaume Sicot, Sbastien Houcke. Blind detection of interleaver parameters[J]. Signal processing, 2009, 89(4): 450 – 462.

[53] Liru Lu, Kwok Hung Li, Yong Liang Guan. Blind detection of interleaver parameters for non-binary coded data streams[A]. IEEE International Conference on Computing[C]. Dresden: IEEE Press, 2009. 1 – 4.

[54] Liru Lu, Kwok Hung Li, Yong Liang Guan. Blind identification of convolutional interleaver parameters[A]. International Conference on Information and Communications Security 2009[C]. Beijing, China: Springer Press, 2009. 1 – 5.

[55] 甘露,刘宗辉,廖红舒,李立萍.卷积交织参数的盲估计[J].电子学报,2011,39(9):2173 – 2177.
Gan Lu, Liu Zong-hui, Liao Hong-shu, Li Li-ping. Blind estimation of the parameters of convolutional interleave[J]. Acta Electronica Sinica, 2011, 39(9): 2173 – 2177. (in Chinese)

[56] Mathieu Cluzeau, Matthieu Finiasz, Jean-Pierre Tillich. Methods for the reconstruction of parallel Turbo codes[A]. International Symposium on Information Theory 2010[C]. Austin, Texas, USA: IEEE Press, 2010. 2008 – 2012.

[57] Maxime Côote, Nicolas Sendrier. Reconstruction of a Turbo-code interleaver from noisy observation[A]. International Symposium on Information Theory 2010[C]. Austin, Texas, USA: IEEE Press, 2010. 2003 – 2007.

[58] Ali Naseri, Omid Azmoon, Samad Fazeli. Blind recognition algorithm of Turbo codes for communication intelligence systems[J]. International Journal of Computer Science Issues, 2011, 8(6): 68 – 72.

[59] 张永光.一种 Turbo 码编码参数的盲识别方法[J].西安电子科技大学学报,2011,38(4):167 – 172.
Zhang Yong-guang. Blind recognition method for the Turbo coding parameter[J]. Journal of Xidian University, 2011, 38(4): 167 – 172. (in Chinese)

[60] 罗向阳,沈利,陆佩忠,刘粉林.高容错伪随机扰码的快速盲恢复[J].信号处理,2004,20(6):552 – 558.
Luo Xiang-yang, Shen Li, Lu Pei-zhong, Liu Fen-lin. Fast blind restore of LFSR sequences with high error tolerance[J]. Signal Processing, 2004, 20(6): 552 – 558. (in Chinese)

[61] 郝士琦,戚林,王勇.一种新的伪随机扰码盲识别方法[J].电路与系统学报,2011,16(4):6 – 12.
Hao Shi-qi, Qi Lin, Wang Yong. A new blind recognition method of pesudo-randomizer code sequence[J]. Journal of Circuits and Systems, 2011, 16(4): 6 – 12. (in Chinese)

[62] 柴先明,彭耿,师栋锋.基于匹配搜索的伪随机序列生成多项式估计[J].光学精密工程,2011,19(9):2222 – 2226.
Chai Xian-ming, Peng Geng, Sshi Dong-feng. Generator polynomial estimation of pseudo-random sequence based on match-searching[J]. Optics and Precision Engineering, 2011, 19(9): 2222 – 2226. (in Chinese)

[63] 伍文君,黄芝平,唐贵林,刘纯武.含错扰码序列的快速恢复[J].兵工学报,2009,30(8):1134 – 1138.
Wu Wen-jun, Huang Zhi-ping, Tang Gui-lin, Liu Chun-Wu. Fast recovery of interfered scrambling code sequence[J]. Acta Armamentarit, 2009, 30(8): 1134 – 1138. (in Chinese)

[64] 苏绍碌,伍文君,黄芝平,刘纯武.含错 m 序列本原多项式的高阶统计测定算法[J].兵工学报,2010,31(12):1593 – 1598.
Su Shao-jing, Wu Wen-jun, Huang Zhi-ping, Liu Chun-Wu. Blind identification of the primitive polynomial of m-sequence with error using high-order statistic[J]. Acta Armamentarit, 2010, 31(12): 1593 – 1598. (in Chinese)

[65] 柴先明,魏跃敏,师栋锋.一种基于与 BCH 码等价原理的 m 序列重构算法[J].电子与信息学报,2011,33(2):304 – 308.
Chai Xian-ming, Wei Yue-min, Shi Dong-feng. A method for reconstruction of m sequence based on the equivalence with BCH codes[J]. Journal of Electronics & Information Technology, 2011, 33(2): 304 – 308. (in Chinese)

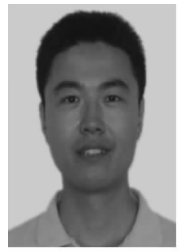
[66] Mathieu Cluzeau. Reconstruction of a linear scrambler[J]. IEEE Transactions on Computers, 2007, 56(9): 1283 – 1291.

[67] Xiao-bei Liu, Soo Ngee Koh, Xin-wen Wu. Reconstructing a linear scrambler with improved detection capability and in the presence of noise[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 208 – 218.

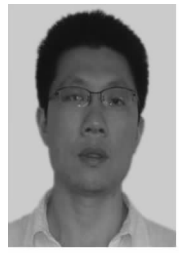
[68] 朱琦,叶芳,刘钧雷,酆广赠.LDPC 码在 802.16a OFDM 系统衰落信道中的性能分析[J].电子学报,2005,33(4):624 – 627.
Zhu Oi, Ye Fang, Liu Jun-iei, Feng Guang-zhen. Performance analysis of LDPC codes for IEEE 802.16a OFDM system in multipath fading channel[J]. Acta Electronica Sinica, 2005, 33(4): 624 – 627. (in Chinese)

作者简介

解 辉 男,1983 年出生于河北省易县,现为国防科技大学电子科学与工程学院博士研究生,研究方向为信道编码盲识别、通信侦察与对抗技术.
E-mail: xiehui2005@gmail.com



王丰华 男,1981 年出生于山东安丘,国防科技大学电子科学与工程学院讲师,研究方向为电子战仿真、通信侦察与对抗、综合电子战技术.



黄知涛 男,1976 年出生于湖北荆州,国防科技大学电子科学与工程学院教授,博士生导师.入选教育部新世纪优秀人才支持计划,博士论文获全国优秀博士论文提名.出版专著 2 部,在 IEEE、IEE 等国内外期刊发表论文 80 余篇.主要研究方向为航天侦察信息处理、雷达/通信信号处理、综合电子战技术等.