

一种高误码(n, k, m)非系统卷积码盲识别算法

张岱¹ 张玉¹ 杨晓静²

(1. 电子工程学院 504 教研室, 合肥, 230037; 2. 电子工程学院 402 教研室, 合肥, 230037)

摘要: 针对信息截获等领域中的卷积码盲识别问题, 提出一种高误码(n, k, m)非系统卷积码盲识别算法。首先建立可变的矩阵模型, 对接收到的数据进行相关预处理, 以减小误码对识别的影响, 提高算法的容错性能; 再对预处理后的数据矩阵进行统计分析, 识别出卷积码的各项参数, 并提取各个数据矩阵的校验序列; 进而利用校验序列构建线性方程组求解生成多项式矩阵组, 通过设定筛选生成多项式矩阵的条件, 筛选出非系统卷积码的生成多项式矩阵, 最终完成对非系统卷积码的识别。仿真实验表明, 该算法可以对高误码(n, k, m)非系统卷积码实现有效的盲识别。

关键词: 信息截获; 非系统卷积码; 盲识别; 预处理; 高误码率

中图分类号: TP309 **文献标志码:** A

Algorithm for Blind Recognition of (n, k, m) Non-systematic Convolutional Code With High BER

Zhang Dai¹, Zhang Yu¹, Yang Xiaojing²

(1. 504 Research Office, Electronic Engineering Institute, Hefei, 230037, China; 2. 402 Research Office, Electronic Engineering Institute, Hefei, 230037, China)

Abstract: An algorithm for blind recognition of (n, k, m) non-systematic convolutional code with high BER is proposed in information interception. Firstly, an alterable matrix model is constructed to deal with the received data in advance. Then, statistical analysis of the preprocessed data matrixes is carried out to recognize parameters of the convolutional code and extract check-sequences of the each data matrix. Linear equation set using check-sequences is built to figure out the generator polynomial matrix group. Through setting condition of selecting the generator polynomial matrix of the non-systematic convolutional code, the non-systematic convolutional code is recognized. Finally simulation results show that the algorithm can recognize (n, k, m) non-systematic convolutional code effectively in the high BER condition.

Key words: information interception; non-systematic convolutional code; blind recognition; preprocess; high BER

引 言

在数字通信中, 信道编码可以提高通信的可靠性, 目前信道编码主要包括线性分组码、卷积码、Tur-

bo 码和 LDPC 码等^[1-2]。其中, Viterbi 译码算法的提出和不断改进^[3], 降低了卷积码编译的复杂度, 使其广泛应用在卫星通信、深空探测等领域。因此卷积码盲识别研究在信息截获领域, 智能通信领域以及非合作信号处理领域有着重要的意义^[4-5]。

卷积码盲识别技术受到了国内外越来越多研究人员的关注^[5], 目前的识别方法主要有基于改进欧几里德算法^[6]、Walsh-Hadamard 分析法^[7]、基于 BM 的快速合冲法^[8]、基于对偶码代数特性的循环识别方法^[9-10]和基于矩阵分析的识别方法^[11]等。其中改进欧几里德算法只适用于 $1/n$ 码率卷积码, 具有使用数据量小的优点, 但不具有容错性; Walsh-Hadamard 分析法同样只适用于 $1/n$ 码率卷积码, 具有较好的容错性, 但该方法必须预估卷积码的码率和码字起点, 即需要一定的先验条件, 且使用的数据量巨大; 基于 BM 的快速合冲法使用较小数据量便能达到识别效果, 但该方法只适用于 $1/2$ 码率的卷积码; 基于对偶码代数特性的循环识别方法可对 (n, k, m) 卷积码进行识别, 该方法至少需使用数万比特码字数据进行识别, 在误码率为 0.02 时, 可达到 50% 以上的识别率, 具有一定的容错性, 但需要码字起点等先验条件; 基于矩阵分析求解校验序列的识别方法可利用少量的数据对 (n, k, m) 卷积码进行全盲识别, 但当误码率超过 0.01 时, 容错性能将急剧下降。同时, 以上两种识别方法均未对非系统卷积码的生成矩阵进行识别。

综上所述, 现有的卷积码识别方法主要针对 $(n, 1, m)$ 卷积码及 (n, k, m) 系统卷积码进行识别, 且需要一定的先验信息, 对性能更优的 (n, k, m) 非系统卷积码进行有效识别的方法尚未见诸报道。本文所提出的方法可在不需要任何先验条件及高误码环境下, 实现对 (n, k, m) 非系统卷积码的识别, 该识别方法创新性的工作主要表现为: (1) 通过建立一个可变的数据矩阵模型进行数据预处理, 筛除了线性约束关系较差的码字, 提高了数据利用率和识别的容错性能; (2) 改进了卷积码参数识别中编码记忆长度的识别方法, 通过统计筛选, 提高了卷积码参数的识别精度。同时, 提出了生成多项式矩阵组的概念, 为非系统卷积码生成多项式矩阵的识别创造条件; (3) 通过对非系统卷积码生成多项式矩阵的特性进行分析, 提出了基于阶次分析的非系统卷积码生成多项式矩阵识别步骤。

1 (n, k, m) 非系统卷积码识别问题描述

当前实际应用的卷积码均是二进制卷积码, 即建立在二元域 F_2 上。通常情况下, 卷积码的参数可表示为 (n, k, m) , 称 k 为信息位长度, n 为码字长度, m 为编码记忆长度。

记 u 和 c 分别为 (n, k, m) 卷积码的信息序列和码字序列, 在环 $F_2[x]$ 上, 二者满足关系如下

$$c(x) = u(x) \cdot G(x) \quad (1)$$

式中: $G(x)$ 为 (n, k, m) 卷积码的生成多项式矩阵。卷积码是线性的, 因此也像分组码一样存在校验多项式矩阵, 并满足以下关系

$$G(x) \cdot H^T(x) = 0 \quad (2)$$

式中: $G(x)$ 为 $k \times n$ 阶多项式矩阵; $H(x)$ 为 $(n-k) \times n$ 阶多项式矩阵。则由式(1)和式(2)可得

$$c(x) \cdot H^T(x) = 0 \quad (3)$$

通过式(3), 可以完成对卷积码校验矩阵的识别^[4]。然而与系统卷积码不同, 对于 (n, k, m) 非系统卷积码的校验多项式矩阵 $H(x)$, 存在多个 $G(x)$ 与之满足式(2)中关系, 且非系统卷积码的生成多项式矩阵与校验多项式矩阵之间并无严格的相似转换关系, 因此当通过式(2)求解得到一系列生成多项式矩阵时, 需要对其进行筛选以得到原卷积码的生成多项式矩阵, 以完成最终识别。经过上述分析, (n, k, m) 非系统卷积码的识别可分为以下两个部分: (1) 卷积码参数(码长 n , 码率 k/n , 记忆长度 m)的识别。(2) 求解卷积码生成多项式矩阵组, 并最终识别出原卷积码的生成多项式矩阵。

根据以上内容, 本文解决 (n, k, m) 非系统卷积码的盲识别问题主要分为以下 3 步:

(1) 建立可变的数据矩阵模型, 利用卷积码码字间的线性相关性, 对侦收到的卷积码数据进行预处理;

(2) 选取预处理后的卷积码数据矩阵, 对其进行综合统计分析, 识别出码率 k/n 、估计记忆长度 \hat{m} , 并利用校验序列求解生成多项式矩阵组;

(3) 设定卷积码生成多项式矩阵筛选规则, 利用阶次分析对生成多项式矩阵组进行筛选, 并作初等变换处理, 最终识别出原卷积码的生成多项式矩阵 $G(x)$ 。

2 对高误码 (n, k, m) 非系统卷积码的盲识别算法

2.1 卷积码数据预处理

针对目前卷积码识别容错性不高的问题, 本文提出了一种基于卷积码码字间线性相关性的方法, 对侦收的卷积码码字进行预处理, 筛选具有较好线性相关性的码字, 大大减小了误码对识别算法的影响。同时, 由于在不同环境下, 所侦收的码字数据量差异很大, 为提高在不同应用背景下的侦收数据利用率, 本文提出建立一个可变数据矩阵模型的方法, 提高了侦收数据利用率, 使对所侦收编码数据的利用更为灵活。

设 c 为 (n, k, m) 卷积码的码字序列, 在 F_2 上表示如下

$$c = (c_{0,1} \quad c_{0,2} \quad \cdots \quad c_{0,n} \quad c_{1,1} \quad c_{1,2} \quad \cdots \quad c_{1,n} \quad c_{2,1} \quad c_{2,2} \quad \cdots \quad c_{2,n} \quad \cdots) \quad (4)$$

将该 (n, k, m) 卷积码的校验矩阵表示为

$$H = \begin{bmatrix} h_0 & 0 & \cdots & & & & \\ h_1 & h_0 & 0 & \cdots & & & \\ h_2 & h_1 & h_0 & 0 & \cdots & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ h_m & h_{m-1} & \cdots & h_1 & h_0 & \cdots & \\ 0 & h_m & h_{m-1} & \cdots & h_1 & h_0 & \cdots \\ 0 & 0 & h_m & \cdots & & & \end{bmatrix} \quad (5)$$

$$h_i = \begin{bmatrix} h'_{i,1} & h'_{i,2} & \cdots & h'_{i,n} \\ h'_{2,1} & h'_{2,2} & \cdots & h'_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ h'_{n-k,1} & h'_{n-k,2} & \cdots & h'_{n-k,n} \end{bmatrix} \quad (h'_{i,j} = 0, 1) \quad (6)$$

由 $c \cdot H^T = 0$, 可知编码输出的码元必然满足一定的约束关系。从 H 的结构可知, 每次 c 都有最多 $N = n(m+1)$ 个元素与 H^T 相乘。也就是说从码字分组起点开始取 N 个 c 中的子码, 那么这 N 个相邻子码都符合方程 $x_1 c_1 + x_2 c_2 + \cdots + x_N c_N = 0$, 其中 x_i 由 H 决定。 $x \cdot c = 0$ 称为编码约束方程, N 为编码约束长度。

定义 1^[11] 设 h' 为 F_2 上半无限长行向量, 对于卷积码码字序列 c , 若满足 $C \cdot h'^T = 0$, 则称 h' 为 (n, k, m) 卷积码的校验序列。

由定义 1, 校验矩阵 H 的各行 H_i 均为校验序列, 其与码字间的线性关系可表示为

$$c \cdot H^T = (c \cdot H_1^T \quad \cdots \quad c \cdot H_{n-k}^T \quad c \cdot H_{1+(n-k)}^T \quad \cdots \quad c \cdot H_{2(n-k)}^T \quad \cdots) = 0 \quad (7)$$

由以上分析, 相邻的 N 个卷积码码字间具有固定的线性约束关系。对此, 将侦收的大量待识别比特流数据 $B = (b_0, b_1, b_2, \cdots)$ 逐行注入到 x 行 y 列的多个数据矩阵模型 D 中, 其中 y 要大于编码约束长度 N , 设定 $x = y + 1$ 。实际应用中, 卷积码的复杂度决定了记忆长度 m 和码长 n 不会太大, 一般有 $m \leq 7, 2 \leq n \leq 6$, 所以 y 取 48 即可。当侦收数据量较大时, 可将卷积码数据不重复地注入到矩阵模型中, 当侦收数据量有限时, 对数据矩阵模型进行如下设置:

第 1 个数据矩阵 D_1 : 第 1 行以 b_a 为起点, 取连续长为 L 比特的数据; 第 2 行以 b_{a+d} 为起点, 取连续

长为 L 比特的数据;其他行的设置依此类推,最终将数据注满该数据矩阵。其中 d 设置为码长的整数倍,以保留各列数据间的线性关系(一般取 4, 5, 6 进行逐个循环)。

第 2 个数据矩阵 \mathbf{D}_2 : 码字起点可设为 b_{a+p} , 其中 $p \geq 1$ 为一自由整数变量, 这样根据总体数据量大小调整 p 的值, 可完成对侦收数据的灵活利用, 以达到更好的识别效果。其他数据矩阵模型设置依此类推, 最终完成所有数据的注入。

按上述规则, 第 q 个数据矩阵模型 \mathbf{D}_q 表示如下

$$\mathbf{D}_q = \begin{bmatrix} b_{a+(q-1)p} & b_{a+1+(q-1)p} & \cdots & b_{a+L-1+(q-1)p} \\ b_{a+d+(q-1)p} & b_{a+d+1+(q-1)p} & \cdots & b_{a+d+L-1+(q-1)p} \\ \vdots & \vdots & & \vdots \\ b_{a+Ld+(q-1)p} & b_{a+Ld+1+(q-1)p} & \cdots & b_{a+(L+1)d-1+(q-1)p} \end{bmatrix}_{(L+1) \times L} \quad (8)$$

当将待识别卷积码比特流注入到数据矩阵模型之后, 矩阵秩的大小表征了该数据矩阵内数据的线性约束关系, 矩阵秩越小, 码字间的线性约束关系越强。对此, 计算各个数据矩阵模型的秩 $\text{rank}(\mathbf{D}_i)$, 根据各个矩阵秩的大小对所有数据矩阵按秩由小到大的顺序进行排序。

由于数据矩阵的起始码字与卷积码码组的起始码字并不严格对应, 因此, 即使是线性关系完备的数据矩阵, 其秩的值也并不一定达到最小^[12]。针对以上情况, 对数据矩阵的秩设判决门限 λ , 由于一般 (n, k, m) 卷积码的码长范围为 $2 \leq n \leq 6$, 对 λ 设置如下

$$\lambda = \min_{i=1,2,\dots} (\text{rank}(\mathbf{D}_i)) + 5 \quad (9)$$

根据矩阵秩判决门限, 设置卷积码数据矩阵的筛选准则如下

$$\mathbf{D} = \{\mathbf{D}_i \mid \text{rank}(\mathbf{D}_i) \leq \lambda\} \quad i = 1, 2, \dots \quad (10)$$

将卷积码数据矩阵组按式(10)进行筛选后, 选择符合线性约束关系的前 r 个数据矩阵(r 的大小视信道干扰情况而定), 并分别赋值给 $(L+1) \times L$ 阶矩阵 $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_r$, 最终得到一个 \mathbf{F}_2 上的二维矩阵序列 $\mathbf{S} = (\mathbf{S}_1 \ \mathbf{S}_2 \ \cdots \ \mathbf{S}_r)$, 将预处理后数据保存, 以待下一步处理。

2.2 卷积码参数识别及生成多项式矩阵组的求解

逐个选取 2.1 节中得到的矩阵序列 \mathbf{S} 中的矩阵 $\mathbf{S}_i (1 \leq i \leq r)$, 并进行初等行变换处理, 可化简为下面矩阵^[4]

$$\mathbf{S}'_i = \begin{bmatrix} \mathbf{I}_a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{I}_v & & & & & \\ 0 & 0 & \mathbf{I}_k \mathbf{P}_{n-k}^1 & & & & \\ 0 & 0 & 0 & \mathbf{I}_k \mathbf{P}_{n-k}^2 & & & \\ 0 & 0 & 0 & 0 & \cdots & & \\ 0 & 0 & 0 & 0 & 0 & \mathbf{I}_k \mathbf{P}_{n-k}^l & \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{I}_w \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (11)$$

式中: $\mathbf{I}_a, \mathbf{I}_v, \mathbf{I}_k$ 和 \mathbf{I}_w 是单位阵(下标表示维数), \mathbf{P}_{n-k}^i 是 $(v+i \cdot n) \times (n-k)$ 的矩阵。由式(11)可以识别出码长 n_i 和信息位数 k_i , 存在 \mathbf{I}_a 是由于数据矩阵 \mathbf{S}_i 中的第一个元素不是码字序列起始位置, a, v, n, l 和 w 满足: $a+v+n \cdot l+w=L$ 。取前若干个 \mathbf{P}_{n-k}^i , 由式(6)知 \mathbf{P}_{n-k}^i 的列即为该 (n, k, m) 卷积码的校验序列^[11]。抽取时, \mathbf{P}_{n-k}^i 所在列的对角线上 0 改 1(保留完整的线性约束关系)。

侦收码字序列中存在的码字错误往往为突发错误, 在经预处理后, 得到的码字数据矩阵中误码较少, 进行初等变换之后将仅造成校验位发生错误, 而不会改变码字整体的线性约束关系。通过对一系列数据矩阵 $\mathbf{S}_i (1 \leq i \leq r)$ 逐个进行上述分析, 统计不同数据矩阵识别后的参数 n_i, k_i , 若 n_i 共有 b 种取值, 记

为 n'_1, \dots, n'_b , 则分别计算其出现概率 $p(n'_j) (1 \leq j \leq b)$ 。最终识别出 (n, k, m) 卷积码的码长 n 为

$$n = \{n'_i \mid p(n=n'_i) = \max(p(n=n'_j)) \quad 1 \leq i \leq b, 1 \leq j \leq b\} \quad (12)$$

与码长 n 的计算过程类似, 可同样统计计算取得信息位数 k 的值, 并从矩阵序列 \mathbf{S} 中选取与参数 n, k 对应的数据矩阵, 组成矩阵序列 \mathbf{S}' 并保存, 完成进一步的数据筛选。对符合参数 n, k 的数据矩阵, 如式(11)的形式, 记录其中单位阵 \mathbf{I}_a 的起点 a 以及 \mathbf{P}_{n-k}^1 首列所在列数 p_1 , 对于第 i 个数据矩阵的参数 a 和 p_1 , 记为 a_i, p_1^i 。根据大量仿真测试, 对 (n, k, m) 卷积码的记忆长度 m_i 估计为

$$\hat{m}_i = \text{ceil}\left(\frac{n-k}{k} \cdot \left(\frac{p_1^i - a_i}{n} - 1\right)\right) \quad (13)$$

式中: $\text{ceil}()$ 表示向上取整。由于码字中出现误码将会破坏码字间的线性约束关系, 使其约束长度增大或不再存在线性约束关系, 对得到的不同估计值 \hat{m}_i , 筛选出所有估计记忆长度中的最小值, 最终得到该 (n, k, m) 卷积码的估计记忆长度 \hat{m} 。从矩阵序列 \mathbf{S}' 中选取与参数 \hat{m} 对应的数据矩阵, 组成矩阵序列 \mathbf{S}'' 并保存, 即完成了卷积码参数的识别, 并进一步进行了卷积码码字数据筛选。 \mathbf{S}'' 记为

$$\mathbf{S}'' = (\mathbf{S}''_1 \quad \mathbf{S}''_2 \quad \dots \quad \mathbf{S}''_l) \quad (14)$$

在得到经进一步筛选的卷积码码字数据之后, 根据文献[11]中基于校验序列的 (n, k, m) 卷积码识别方法, 对原卷积码的生成多项式矩阵组进行识别。对于式(14)中的 l 个数据矩阵, 分别抽取其前 r 个校验序列, 记为

$$\mathbf{H}' = (\mathbf{H}'_1 \quad \mathbf{H}'_2 \quad \dots \quad \mathbf{H}'_l) \quad (15)$$

$$\mathbf{H}'_i = (\mathbf{P}_i^1 \quad \dots \quad \mathbf{P}_i^r) \quad 1 \leq i \leq l \quad (16)$$

式中: \mathbf{P}_i^j 代表矩阵 \mathbf{S}''_i 中 \mathbf{P}_{n-k}^1 的首列, $\mathbf{P}_i^1 \dots \mathbf{P}_i^r$ 的设置依此类推。

定义 2 如果两个生成多项式矩阵 $\mathbf{G}(x)$ 和 $\mathbf{G}'(x)$ 可编码生成同一个卷积码, 那么它们就是等价的, 等价生成多项式矩阵的集合称为生成多项式矩阵组。

不考虑恶性码及编码器缺失等情况, 对于 (n, k, m) 非系统卷积码的校验矩阵 \mathbf{H} , 存在多个非零矩阵 \mathbf{G}_i 满足 $\mathbf{G}_i \cdot \mathbf{H}^T = 0 (i=1, 2, \dots)$, 则 \mathbf{G}_i 均可为该卷积码的生成矩阵^[1]。由定义 1 中校验序列的概念可得, 对于式(16)中多个校验序列构造的多项式矩阵 $\mathbf{H}'_j(x)$, 必有

$$\mathbf{G}_i(x) \cdot \mathbf{H}'_j^T(x) = 0 \quad 1 \leq j \leq l \quad (17)$$

则由 \mathbf{H}' 求解出生成多项式矩阵组的具体步骤如下:

(1) 取 \mathbf{H}'_1 , 对其中的 r 个校验序列分别按码长 n 抽取, 由此将 $\mathbf{P}^i (1 \leq i \leq r)$ 构造成 $\mathbf{F}_2(x)$ 上的 n 个多项式: $h_1^i(x), \dots, h_n^i(x)$, 等效于校验多项式矩阵 $\mathbf{H}(x)$ 的某一行, 记作 $\mathbf{h}^i(x)$ 。

(2) 由识别出的参数码长 n 、信息位数 k 和估计记忆长度 \hat{m} 假设生成多项式矩阵 $\mathbf{G}(x)$, $\mathbf{G}(x)$ 的 k 行分别记为 $\mathbf{g}^j(x), 1 \leq j \leq k$ 。由式(2)建立 k 个 $\mathbf{g}^j(x)$ 与 r 个 $\mathbf{h}^i(x)$ 的线性方程组, $\mathbf{g}^j(x) \cdot [\mathbf{h}^i(x)]^T = 0$, 当 $j=1$ 时, 有

$$\begin{cases} g_{1,1}(x) \cdot h_1^1(x) + \dots + g_{1,n}(x) \cdot h_n^1(x) = 0 \\ g_{1,1}(x) \cdot h_1^2(x) + \dots + g_{1,n}(x) \cdot h_n^2(x) = 0 \\ \vdots \\ g_{1,1}(x) \cdot h_1^r(x) + \dots + g_{1,n}(x) \cdot h_n^r(x) = 0 \end{cases} \quad (18)$$

以上方程组建立在 $\mathbf{F}_2(x)$ 上, 成立条件是 x 所有幂次的系数均为 0, 故方程组(18)中共有 $n(\hat{m}+1)$ 个未知数, 方程组中的每个方程由于 x 幂次的不同在 $\mathbf{F}_2(x)$ 上可等同于多个方程^[11], 所以抽取校验序列的个数 r 不必取太大, 一般取 3 即可。

(3) 将方程组(18)转化成 $\mathbf{F}_2(x)$ 上的方程组, 易知其解空间的维数为 k , 通过行阶梯法求解得到一系列以生成多项式矩阵行向量为基的解向量, 取前 k 个解序列, 记为

$$\mathbf{G}_1(x) = [\mathbf{g}_1^1(x) \quad \dots \quad \mathbf{g}_1^k(x)]^T \quad (19)$$

(4) 依照步骤(1), (2), (3)对 \mathbf{H}' 中的其他校验序列矩阵进行处理, 最终得到生成多项式矩阵组

$$\mathbf{G}\mathbf{G}(x) = [\mathbf{G}_1(x) \quad \mathbf{G}_2(x) \quad \cdots \quad \mathbf{G}_l(x)] \quad (20)$$

2.3 生成多项式矩阵的识别

由定义 2 可知, 对于非系统卷积码, 可存在多个生成矩阵与其校验矩阵相对应, 然而, 不同的卷积码生成矩阵在性能上存在着巨大差异。

定义 3 对于卷积码的生成多项式矩阵 $\mathbf{G}(x)$, 定义其逆为 $\mathbf{G}^{-1}(x)$, 满足

$$\mathbf{G}(x) \cdot \mathbf{G}^{-1}(x) = \mathbf{I} \quad (21)$$

如果 $\mathbf{G}^{-1}(x)$ 可实现, 从传输函数的角度来考虑, 则它相当于卷积码的译码器, 在接收端应有

$$c(x) \cdot \mathbf{G}^{-1}(x) = u(x) \quad (22)$$

假设有一个卷积码的 $\mathbf{G}(x) = [1+x, 1+x+x^2]$, 可求得 $\mathbf{G}^{-1}(x) = [x, 1]^T$, 可以看出此译码器中仅有一级延时存储单元, 故在译码过程中码字中的错误只要经一个单位时间即被遗忘掉, 称这种 $\mathbf{G}^{-1}(x)$ 为前馈逆。假设另一个 $\mathbf{G}(x) = [1+x, 1+x^2]$, 则有

$$\mathbf{G}^{-1}(x) = \begin{bmatrix} \frac{x}{1+x} & \frac{1}{1+x} \end{bmatrix}^T \quad (23)$$

式中: $\mathbf{G}^{-1}(x)$ 分母为 $1+x$, 在电路上相当于作除法, 称为反馈逆。这种电路的记忆是无限的, 因为 $1/(1+x) = 1+x+x^2+\cdots$, 所以错误无法消除。这个例子里误码会无限传播, 称之为 I 类无限误差传播, 这个码便称为恶性码^[13]。只要 $\mathbf{G}^{-1}(x)$ 是无时延的有限多项式, 其所代表的码就不会是恶性的。

定理 1 如果一个卷积码的 $\mathbf{G}(x)$ 和 $\mathbf{G}^{-1}(x)$ 都是有限多项式矩阵, 则 $\mathbf{G}(x)$ 就是该卷积码的一个基本编码矩阵^[13]。

而对于有限域上的多项式矩阵 $\mathbf{G}(x)$, 计算 $\mathbf{G}^{-1}(x)$ 的过程较为复杂, 因此将定理 1 作为筛选卷积码生成多项式矩阵的依据会造成巨大的计算量, 不易实现。做出如下改进。

推论 1 对于 (n, k, m) 卷积码, 其生成多项式矩阵 $\mathbf{G}(x)$ 表示如下

$$\mathbf{G}(x) = \begin{bmatrix} g_{1,1}(x) & g_{1,2}(x) & \cdots & g_{1,n}(x) \\ g_{2,1}(x) & g_{2,2}(x) & \cdots & g_{2,n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1}(x) & g_{k,2}(x) & \cdots & g_{k,n}(x) \end{bmatrix} \quad (24)$$

则 $\mathbf{G}(x)$ 为基本编码矩阵的必要条件是

$$\gcd(g_{i,1}(x), g_{i,2}(x), \cdots, g_{i,n}(x)) = 1 \quad i = 1, \cdots, k \quad (25)$$

证明:

若 $\gcd(g_{i,1}(x), g_{i,2}(x), \cdots, g_{i,n}(x)) = g_i(x) \quad i = 1, 2, \cdots, k$, 并满足

$$\max(\deg(g_1(x)), \deg(g_2(x)), \cdots, \deg(g_k(x))) > 1 \quad (26)$$

则有

$$\gcd(g_{i,1}(x)/g_i(x), g_{i,2}(x)/g_i(x), \cdots, g_{i,n}(x)/g_i(x)) = 1 \quad (27)$$

由有限域上多项式的性质可知, 必存在 $h_{i,1}(x), h_{i,2}(x), \cdots, h_{i,n}(x)$ 使得^[14]

$$h_{i,1}(x) \cdot g_{i,1}(x)/g_i(x) + h_{i,2}(x) \cdot g_{i,2}(x)/g_i(x) + \cdots + h_{i,n}(x) \cdot g_{i,n}(x)/g_i(x) = 1 \quad (28)$$

结合式(21)可得

$$\mathbf{G}^{-1}(x) = \begin{bmatrix} h_{1,1}(x)/g_1(x) & h_{1,2}(x)/g_1(x) & \cdots & h_{1,n}(x)/g_1(x) \\ h_{2,1}(x)/g_2(x) & h_{2,2}(x)/g_2(x) & \cdots & h_{2,n}(x)/g_2(x) \\ \vdots & \vdots & \ddots & \vdots \\ h_{k,1}(x)/g_k(x) & h_{k,2}(x)/g_k(x) & \cdots & h_{k,n}(x)/g_k(x) \end{bmatrix}^T \quad (29)$$

由式(29)可知, $\mathbf{G}^{-1}(x)$ 存在反馈逆, 则由 $\mathbf{G}(x)$ 生成的卷积码为恶性码。由以上步骤反证得到若 \mathbf{G}

(x)生成的卷积码为非恶性码,则必有式(25)成立,从而推论1得证。根据上述定义和推论,对(n, k, m)非系统卷积码生成多项式矩阵的识别步骤如下:

(1)对2.2节中所得到的生成多项式矩阵组 $\mathbf{GG}(x)$,设置累积量记录其中不同的元素多项式矩阵出现次数,将不同的多项式矩阵按其累积量由大到小的顺序重新排序如下

$$\mathbf{GG}'(x) = [\mathbf{G}'_1(x) \quad \mathbf{G}'_2(x) \quad \cdots \quad \mathbf{G}'_t(x)] \quad 1 \leq t \leq l \quad (30)$$

(2)对 $\mathbf{G}'_p(x)$ 的各行求其最大公因式,若阶次不为1,则将该生成多项式矩阵舍弃。

(3)将 $\mathbf{G}'_p(x)$ 按列表示如下

$$\mathbf{G}'_p(x) = [g_1^p(x) \quad g_2^p(x) \quad \cdots \quad g_n^p(x)] \quad (31)$$

若有 $g_j^p(x) = 0, 1 \leq j \leq n$,即输出码字中某一路存在缺失,则将该生成多项式矩阵舍弃,取 $\mathbf{G}'_{p+1}(x)$ 返回步骤(2)继续执行。

(4)对于满足步骤(2),(3)中条件的生成多项式矩阵 $\mathbf{G}'_p(x)$,将其按行表示如下

$$\mathbf{G}'_p(x) = [g_1^p(x) \quad g_2^p(x) \quad \cdots \quad g_k^p(x)]^T \quad (32)$$

记 $\mathbf{G}'_p(x)$ 的阶次如下

$$\deg(\mathbf{G}'_p(x)) = \sum_{i=1}^k \deg(g_i^p(x)) \quad (33)$$

若对 $\mathbf{G}'_p(x)$ 进行初等行变换后,使得 $\deg(\mathbf{G}'_p(x))$ 降低,则保留其初等行变换后的形式并替代原 $\mathbf{G}'_p(x)$,否则仍保存原 $\mathbf{G}'_p(x)$ 。则 $\mathbf{G}'_p(x)$ 即为最终识别得到的原(n, k, m)非系统卷积码的生成多项式矩阵,由 $\mathbf{G}'_p(x)$ 的行阶次最终确认记忆长度 m 为

$$m = \max_{i=1, \dots, k} (\deg(g_i^p(x))) \quad (34)$$

3 实例仿真分析

首先对所提出识别算法进行仿真验证,随后使用蒙特卡罗法,将本文算法与其他算法在卷积码参数识别性能上作对比,最后对采用不同数据量时对非系统卷积码的识别效果进行比较。

3.1 算法验证

以常用的(3,2,4)非系统卷积码为例验证本文算法的可行性。(3,2,4)非系统卷积码的生成矩阵用八进制表示为 $\mathbf{G} = (23 \ 35 \ 0; 0 \ 5 \ 13)$,则其生成多项式矩阵为

$$\mathbf{G}(x) = \begin{bmatrix} x^4 + x^3 + 1 & x^4 + x^2 + x + 1 \\ 0 & x^3 + x \end{bmatrix} \quad (35)$$

选取5 000 bit 误码率为2%的(3,2,4)卷积码数据进行仿真如下。首先,将得到的卷积码数据逐行注入2.1节中建立的数据矩阵模型中,由于所侦收的数据量有限,设置可变矩阵参数 $p=5$,通过数据预处理,从预处理后的数据矩阵组中选取一个数据矩阵,使用2.2节中的方法对其进行卷积码参数识别,得到式(11)形式的分析矩阵如图1所示。

对图中矩阵分析可得, $n=3, k=2, p=24, a=1$,由记忆长度估计式(13)计算得

$$\hat{m}_i = \text{ceil}\left(\frac{n-k}{k} \cdot \left(\frac{p_i - a_i}{n} - 1\right)\right) = 4 \quad (36)$$

使用2.2节中方法进行统计,最终得到该卷积码的参数为码长 $n=3$,信息位长度 $k=2$,估计记忆长度 $\hat{m}=4$ 。接下来求解该卷积码的生成多项式矩阵组,使用2.3节中的步骤(1),按累积量进行排序后,得到生成多项式矩阵组如下

$$\mathbf{G}'_1 = \begin{bmatrix} x^4 + x^3 + 1 & x^4 + x^2 + x + 1 & 0 \\ 0 & x^3 + x & x^3 + x^2 + 1 \end{bmatrix}$$

$$\mathbf{G}'_2 = \begin{bmatrix} x^3 + x^2 + 1 & 0 \\ x^4 + x^3 + x & 0 \end{bmatrix}$$

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

图1 数据矩阵模型化简结果

Fig. 1 Results of simplifying data matrix model

$$\mathbf{G}'_3 = \begin{bmatrix} x^3 + x & x^3 + x^2 + 1 \\ x^4 + x^3 + x^2 + x & x^4 + x^2 + x + 1 \end{bmatrix}$$

$$\mathbf{G}'_4 = \begin{bmatrix} x^3 + x^2 & 0 \\ x^4 + x^3 + x^2 + x & x^3 + x \end{bmatrix} \quad (37)$$

对矩阵组(37)执行 2.3 节中的非系统卷积码生成多项式矩阵识别步骤,最终识别出原卷积码的生成多项式矩阵为

$$\mathbf{G} = \begin{bmatrix} x^4 + x^3 + 1 & x^4 + x^2 + x + 1 \\ 0 & x^3 + x \end{bmatrix} \quad (38)$$

与式(35)相同,同时确认记忆长度 $m=4$,达到了识别目的。对以上例子中得到的生成多项式矩阵组进行分析可得,即使误码率变化,导致按累积量排序后生成多项式矩阵组中元素的顺序发生改变,利用 2.3 节中的非系统卷积码生成多项式矩阵的识别步骤仍可准确识别,这表明了本文所提出算法的可行性。

3.2 识别性能对比

由于 (n, k, m) 非系统卷积码的参数识别和 (n, k, m) 系统卷积码的参数识别具有通用性,现将本文识别算法与文献[10-11]中卷积码识别算法在参数识别上的性能进行比较,采用 20 000 bit(3, 2, 4)非系统卷积码数据进行参数识别时,其识别性能对比如图 2 所示。

由图 2 可以看出,当误码率达到 0.02 时,文献[11]所提出的矩阵分析方法识别率下降到 50% 以下,文献[10]中基于对偶码代数特性识别方法的识别率在 65% 左右,而本文算法的识别率仍高于 80%。综上可知,本文所提出的 (n, k, m) 非系统卷积码盲识别算法在卷积码参数识别上与矩阵分析法和基于对偶码代数特性识别方法相比,在误码适应能力上具有优势。同时,由于本文算法在识别过程中进行了预处理和逐层数据筛选的过程,将线性关系缺失的码字不断剔除,减少了矩阵分析的数据量,从而在计算量上也低于另外两种 (n, k, m) 卷积码识别方法。

此外,本文所提出的 (n, k, m) 非系统卷积码盲识别算法在应用上还具有较强的灵活性,这集中体现在 2.1 节中可变量数据矩阵模型的建立上,可根据侦收数据量的不同进行模型上的调整。现以(3, 2, 4)卷积码和(5, 1, 6)卷积码为例,分别选取 500, 2 000, 5 000, 10 000 bit 侦收编码数据,设置不同误码率进行全盲识别,通过蒙特卡洛仿真实验统计对应的识别成功概率(包括非系统卷积码参数和其生成多项式矩阵),如图 3 所示。

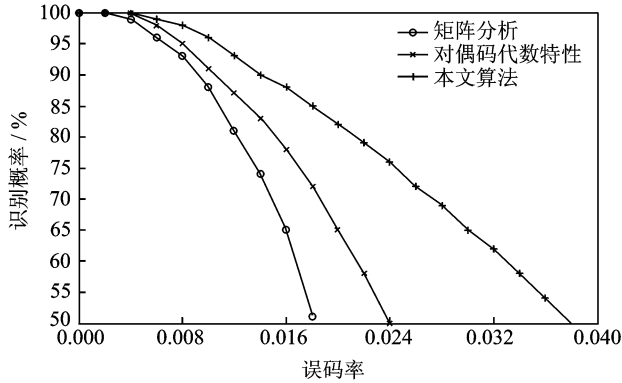
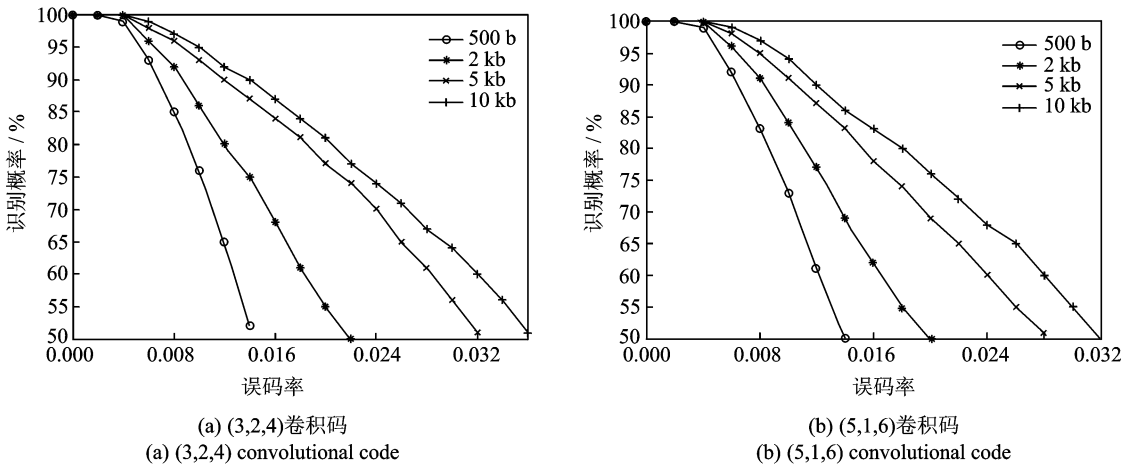


图2 不同误码环境下识别概率对比

Fig. 2 Recognition probability in different bit error rates

由图3的统计结果可知,本文算法可对不同量级数据量的非系统卷积码进行全盲识别,且随着侦收数据量的提高,算法容错性能逐渐增强,其中,在取得10 000 bit 侦收数据的情况下,当误码率达到0.03时,对(3,2,4)卷积码仍具有接近70%的成功识别率,对(5,1,6)卷积码具有接近60%的识别率。从理论上来看,由于本文算法采用了逐层筛选的方法,不断提取侦收数据中线性约束关系完备的码字,当侦收数据量非常巨大时,该方法对高误码的卷积码数据将取得十分理想的识别效果。

同时,通过两种卷积码的识别结果对比,可以看出,随着编码约束长度的增加,识别难度逐渐增大。这是由于编码约束长度较大时,编码数据线性相关性更容易被错误码字破坏的缘故。



(a) (3,2,4)卷积码

(a) (3,2,4) convolutional code

(b) (5,1,6)卷积码

(b) (5,1,6) convolutional code

图3 不同侦收编码数据量对应的识别概率

Fig. 3 Recognition probability of different received coded data sizes

4 结束语

本文提出了一种高误码(n, k, m)非系统卷积码盲识别算法,通过建立可变的数据矩阵模型对侦收数据进行预处理,较以往卷积码识别方法具有数据利用灵活、利用率高的特点。同时改进了矩阵分析法中对卷积码参数的识别方法,通过统计分析,提高了卷积码参数的识别精度,在求解出生成多项式矩阵组之后,通过对非系统卷积码的生成多项式矩阵特性进行分析,提出了非系统卷积码生成多项式矩阵的

筛选条件,最终完成了对 (n, k, m) 非系统卷积码的识别。本文识别方法不需要任何先验条件,数据利用率高并具有较好的容错性,在误码率为0.02的条件下,对 $(3, 2, 4)$ 非系统卷积码的正确识别率达到80%以上,弥补了当前卷积码识别研究上的不足,在智能通信及信息截获等领域具有重要应用意义。

参考文献:

- [1] 刘玉君. 信道编码[M]. 郑州:河南科学技术出版社,2001:45-47,190-216.
Liu Yujun. Channel coding[M]. Zhengzhou:Henan Publishing House of Science&Technology,2001:45-47,190-216.
- [2] 张艳,仰帆帆. 基于非规则 LDPC 码的协作 MIMO 系统性能分析[J]. 数据采集与处理,2013,28(6):714-718.
Zhang Yan, Yang Fanfeng. Based on irregular LDPC cooperative MIMO system performance analysis[J]. Journal of Data Acquisition and Processing, 2013,28(6):714-718.
- [3] Zhou Ting, Xu Ming, Chen Dongxia, et al. Constrained Viterbi algorithm and its application to error resilient transmission of spirit coded images[J]. Transactions of Nanjing University of Aeronautics&Astronautics, 2008,25(2):155-159.
- [4] 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,2010:9-94.
Zhang Yongguang, Lou Caiyi. Channel coding recognition and analysis[M]. Beijing:Publishing House of Electronics Industry, 2010:9-94.
- [5] 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 Zhitao, Wang Fenghua. Research progress of blind recognition of channel coding[J]. Acta Electronic Sinica, 2013,41(6):1166-1176.
- [6] 刘建成,杨晓静,张玉. 基于改进欧几里德算法的 $(n, 1, m)$ 卷积码识别[J]. 探测与控制学报,2012,34(1):64-68.
Liu Jiancheng, Yang Xiaojing, Zhang Yu. Recognition of $(n, 1, m)$ convolutional code based on improved Euclidean algorithm [J]. Journal of Detection&Control, 2012,34(1):64-68.
- [7] 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 Xiaojun, Zhou Xiyuan. Blind recognition of convolutional coding based on Walsh-Hadamard transform[J]. Journal of Electronic&Information Technology, 2010,32(4):884-888.
- [8] 邹艳,陆佩忠. 关键方程的新推广[J]. 计算机学报,2006,29(5):712-718.
Zou Yan, Lu Peizhong. A new generalization of key equation[J]. Chinese Journal of Computers, 2006,29(5):712-718.
- [9] Marazin M, Gautier R, Burel G. Dual code method for blind identification of convolutional encoder for cognitive radio receiver design[C]//GLOBECOM Workshops 2009. Rennes, France:IEEE Press,2009:1-6.
- [10] Marazin M, Gautier R, Burel G. Blind recovery of k/n rate convolutional encoders in a noisy environment[J]. Wireless Communications and Networking, 2011,2011(1):1186-1687.
- [11] 杨晓静,刘建成,张玉. 基于求解校验序列的 (n, k, m) 卷积码盲识别[J]. 宇航学报,2013,34(04):568-573.
Yang Xiaojing, Liu Jiancheng, Zhang Yu. Blind recognition of (n, k, m) convolutional codes based on solving check-sequence [J]. Journal of Astronautics, 2013,34(04):568-573.
- [12] 田同旺. 卷积码识别技术研究[D]. 西安:西安电子科技大学,2012.
Tian Tongwang. Research on technology of identification of convolutional codes[D]. Xi'an:Xidian University,2012.
- [13] 王琳,徐位凯. 高效信道编码译码技术及其应用[M]. 北京:人民邮电出版社,2007:35-61.
Wang Lin, Xu Weikai. High effective channel coding&decoding technology and its application[M]. Beijing:Posts & Telecom Press,2007:35-61.
- [14] 万哲先. 代数和编码[M]. 北京:高等教育出版社,2007:406-437.
Wan Zhexian. Algebra and coding[M]. Beijing:Higher Education Press,2007:406-437.

作者简介:



张岱(1993-),男,硕士研究生,研究方向:信道编码识别分析, E-mail: zhang-dai1208@gmail.com.



张玉(1962-),男,教授,硕士生导师,研究方向:信号处理及信息对抗。



杨晓静(1963-),女,副教授,硕士生导师,研究方向:通信及信息对抗。

