基于求解校验序列的$(n,1,m)$卷积码盲识别

刘建成* 杨晓静
(解放军电子工程学院 合肥 230037)

摘 要：伴随信息对抗和智能通信的快速发展，信道编码识别已成为信息恢复领域一个重要的课题。针对$(n,1,m)$卷积码盲识别问题，该文提出一种新的识别方法，该方法首先提出了校验序列的概念，通过改进后的矩阵模型求解出校验序列，进而由校验序列构造方程求解出生成多项式矩阵，完成识别。最后，通过实例仿真验证了该方法能够在参数n和码字起始位置都未知情况下有效识别出$(n,1,m)$卷积码。

关键词：信息对抗；卷积码盲识别；校验序列；生成多项式矩阵
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2012)10-2363-06
DOI: 10.3724/SP.J.1146.2012.00497

Blind Recognition of $(n,1,m)$ Convolutional Code Based on Solving Check-sequence

Liu Jian-cheng Yang Xiao-jing
(*Electronic Engineering Institute of PLA*, *Hefei* 230037, *China*)

Abstract: In view of the fast development of information countermeasure and intelligent communication, recognition of channel coding has been a vital issue in information interception. This paper proposes a new method of recognition in order to recognize the $(n,1,m)$ convolutional codes. Firstly, this method defines the notion of check-sequence, and solves it by an advanced model of matrix, then deduces the matrix of generator polynomial, having recognized the convolutional code, by check-sequence. Finally, examples of simulation show that this method is able to recognize, neither knowing the parameter of code n nor the begin location of coding, all $(n,1,m)$ convolutional codes effectively.

Key words: Information countermeasure; Blind recognition of convolutional code; Check-sequence; Matrix of generator polynomial

1 引言

在数字通信中，信道编码可以提高信息传输的可靠性，保证通信质量。目前信道编码主要包括线性分组码、卷积码、LDPC 码和 Turbo 码等。卷积码具有纠错能力强和编译简单等优点已广泛应用于卫星系统测控链路、深空探测系统和第 3 代移动通信系统等，这也使得卷积码识别成为了信息对抗和智能移动通信 AMC(自适应调制编码)技术中实现信息恢复所亟需解决的问题。目前，国外针对信道编码识别研究的公开文献资料相对较少，国内对线性分组码的研究方法主要有文献[1,2]中的秩函数求解、码根统计等；对卷积码识别主要有文献[3]中的基于快速双合冲算法、文献[4]中的欧几里德算法、文献[5,6]中的构建分析矩阵法和文献[7]中的 Walsh-Hadamard 变换法。欧几里德算法和基于快速合冲算法计算复杂度低、所需数据量小，但只适于无记忆的$(2,1,m)$卷积码码字序列识别；构建分析矩阵法只对$(n,1,m)$卷积码和系统卷积码进行了相关的识别分析，且所需数据量非常巨大，在不知子码长度n的情况下一般需要几万比特；Walsh-Hadamard 变换法具有较好的容错性能，同时需要参数n、码字起始位置等先验条件和巨大的数据存储空间。可见，现有的卷积码识别方法一般具有应用范围受限、数据利用率低和所需先验条件较多等不足。

$(n,1,m)$卷积码具有良好的纠错性能，是卫星通信、深空探测等常用的低码率信道编码方式[8]。本文针对该类卷积码提出了一种新的盲识别方法，该方法计算复杂度较低，能够在参数n和码字起始位置均未知的情况下有效完成识别。

2 $(n,1,m)$卷积码识别问题的描述

本文讨论卷积码是建立在二元域F_2上，卷积码是把信源输出的信息序列，以k个码元分为一组，通过编码器输出长为$n(n>k)$的一组码字，该码组的$n-k$个校验元不仅与本组的信息元相关，而且还与先前的m组信息元有关。因此，卷积码一般表示为：(n,k,m)，称k为信息子组长度，n为子码长度，

2012-05-02 收到，2012-06-18 改回
*通信作者：刘建成 liujiancheng1987@126.com

m 为编码记忆长度， $n(m+1)$ 为卷积码的约束长度[9]。现只讨论 $k=1$ 的卷积码。

2.1 $(n,1,m)$ 卷积码

设 $\boldsymbol{I}$ 和 $\boldsymbol{C}$ 分别为 $(n,1,m)$ 卷积码的信息序列和码字序列，在环 $F_2[x]$ 上二者可以表示为

$$\boldsymbol{I}(x)=i(x)=i_0+i_1x+\cdots+i_jx^j+\cdots=\sum_{j=0}^{+\infty}i_jx^j \quad (1)$$

$$\boldsymbol{C}(x)=[c_1(x)\ \ c_2(x)\ \cdots\ c_n(x)],$$

$$c_i(x)=c_{i,0}+c_{i,1}x+\cdots+c_{i,j}x^j+\cdots=\sum_{j=0}^{+\infty}c_{i,j}x^j,\ \ 1\le i\le n \quad (2)$$

定义 1[9] $(n,1,m)$ 卷积码的生成多项式矩阵 $\boldsymbol{G}(x)$ 定义为

$$\boldsymbol{G}(x)=[g_1(x)\ \ g_2(x)\ \cdots\ g_n(x)],$$

$$g_i(x)=g_{i,0}+g_{i,1}x+g_{i,2}x^2+\cdots+g_{i,m}x^m,$$

m 为记忆长度 (3)

则 $\boldsymbol{I}(x)$ 和 $\boldsymbol{C}(x)$ 之间满足如下关系：

$$\boldsymbol{C}(x)=\boldsymbol{I}(x)\cdot\boldsymbol{G}(x) \quad (4)$$

定义 2[9] 与线性分组码相似，对于卷积码定义校验多项式矩阵，设 $\boldsymbol{G}(x)$ 是 $(n,1,m)$ 卷积码的生成多项式矩阵， $\boldsymbol{H}(x)$ 为 $(n-1)\times n$ 的多项式矩阵，若满足

$$\boldsymbol{G}(x)\cdot\boldsymbol{H}^{\mathrm{T}}(x)=\boldsymbol{0} \quad (5)$$

称 $\boldsymbol{H}(x)$ 为 $(n,1,m)$ 卷积码的校验多项式矩阵(满足式(5)的 $\boldsymbol{H}(x)$ 不唯一， T 表示矩阵转置)。

由式(3)和式(5)可知

$$\boldsymbol{C}(x)\cdot\boldsymbol{H}^{\mathrm{T}}(x)=\boldsymbol{0} \quad (6)$$

现 $(n,1,m)$ 卷积码的盲识别问题可转化为求解式(5)和式(6)，本文将通过构建数据利用率高的矩阵识别模型，引入校验序列解决该识别问题。

2.2 识别问题的描述

现将卷积码的编码过程由 $F_2[x]$ 引申至 F_2 上，即由标量矩阵表示，以便由截获或接收到的 0, 1 序列建立识别模型。

定义 3[9] $(n,1,m)$ 卷积码码字序列 $\boldsymbol{C}$ 定义为

$$\boldsymbol{C}=[c_{1,0}\ \ c_{2,0}\cdots c_{n,0}\ \ c_{1,1}\ \ c_{2,1}\cdots\ c_{n,1}\ \ c_{1,2}\ \ c_{2,2}\cdots\ c_{n,2}\ \cdots],\ \ c_{i,j}=0,1 \quad (7)$$

定义 4[9] 校验矩阵 $\boldsymbol{H}$ 定义为

$$\boldsymbol{H}=\begin{pmatrix}\boldsymbol{h}_0 & 0 & 0 & \cdots & 0 & 0\cdots\\ \boldsymbol{h}_1 & \boldsymbol{h}_0 & 0 & \cdots & 0 & 0\cdots\\ \boldsymbol{h}_2 & \boldsymbol{h}_1 & \boldsymbol{h}_0 & \cdots & 0 & 0\cdots\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ \boldsymbol{h}_M & \boldsymbol{h}_{M-1} & \boldsymbol{h}_{M-2} & \cdots & \boldsymbol{h}_0 & 0\cdots\\ 0 & \boldsymbol{h}_M & \boldsymbol{h}_{M-1} & \cdots & \boldsymbol{h}_1 & \boldsymbol{h}_0\cdots\\ 0 & 0 & \boldsymbol{h}_M & \cdots & \boldsymbol{h}_2 & \boldsymbol{h}_1\cdots\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\end{pmatrix} \quad (8)$$

其中 $\boldsymbol{h}_t$ 为 $(n-1)\times n$ 的矩阵($0\le t\le M$ ， M 等于 $\boldsymbol{H}(x)$ 中元素的最高幂次的值)，可表示为

$$\boldsymbol{h}_t=\begin{pmatrix}h_{1,1}^t & h_{1,2}^t & \cdots & h_{1,n}^t\\ h_{2,1}^t & h_{2,2}^t & \cdots & h_{2,n}^t\\ \vdots & \vdots & \ddots & \vdots\\ h_{n-1,1}^t & h_{n-1,2}^t & \cdots & h_{n-1,n}^t\end{pmatrix},\quad h_{i,j}^t=0,1 \quad (9)$$

所以，校验矩阵 $\boldsymbol{H}$ 可看作是 $(n-1)\times n(M+1)$ 维矩阵 $(\boldsymbol{h}_M\ \ \boldsymbol{h}_{M-1}\ \cdots\ \boldsymbol{h}_0)$ 的移位，可以表示为

$$\boldsymbol{H}=\begin{pmatrix}\boldsymbol{H}_{0,1}\\ \boldsymbol{H}_{0,2}\\ \vdots\\ \boldsymbol{H}_{0,n-1}\\ \boldsymbol{H}_{1,1}\\ \vdots\\ \boldsymbol{H}_{1,n-1}\\ \vdots\end{pmatrix} \quad (10)$$

$$\boldsymbol{H}_{f,i}=\begin{cases}(h_{i,1}^f\cdots h_{i,n}^f\ \ h_{i,1}^{f-1}\cdots h_{i,n}^{f-1}\ \cdots\ h_{i,1}^0\cdots h_{i,n}^0\\ \quad 0\ \ 0\ \cdots),\ 0\le f\le M,\ 1\le i<n-1\\ \Big(\underbrace{0\ \cdots\ 0}_{n\cdot(f-M)}\ \ h_{i,1}^M\cdots h_{i,n}^M\ \ h_{i,1}^{M-1}\cdots h_{i,n}^{M-1}\ \cdots\\ \quad h_{i,1}^0\cdots h_{i,n}^0\ \ 0\ \ 0\ \cdots\Big),\\ \qquad f>M,\ \ 1\le i\le n-1\end{cases} \quad (11)$$

码字序列 $\boldsymbol{C}$ 和校验矩阵 $\boldsymbol{H}$ 满足关系式[9]

$$\boldsymbol{C}\cdot\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0} \quad (12)$$

由于校验矩阵 $\boldsymbol{H}$ 的不唯一性，故对其求解较为困难。现引入校验序列 $\boldsymbol{H}'$，能容易地由后续内容中建立的矩阵模型求解得出，进而由多个 $\boldsymbol{H}'$ 构造出校验多项式矩阵 $\boldsymbol{H}(x)$，并由式(5)推导出生成多项式矩阵 $\boldsymbol{G}(x)$。

定义 5 $(n,1,m)$ 卷积码校验序列 $\boldsymbol{H}'$ 定义为：$\boldsymbol{H}'$ 为 F_2 上半无限长行向量

$$\boldsymbol{H}'=[h_1\ \ h_2\ \ h_3\ \cdots\ h_i\ \cdots] \quad (13)$$

对于 $(n,1,m)$ 卷积码任意输出的编码序列 $\boldsymbol{C}$，若满足

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

则称 $\boldsymbol{H}'$ 为 $(n,1,m)$ 卷积码的校验序列。

可见，校验矩阵 $\boldsymbol{H}$ 的各行 $\boldsymbol{H}_{f,i}$ 均为校验序列，式(12)可表示为

$$\boldsymbol{C}\cdot\boldsymbol{H}^{\mathrm{T}}=\left[\boldsymbol{C}\cdot\boldsymbol{H}_{0,1}^{\mathrm{T}}\ \cdots\ \boldsymbol{C}\cdot\boldsymbol{H}_{f,i}^{\mathrm{T}}\ \cdots\right]=\boldsymbol{0} \quad (15)$$

表示成二元齐次线性方程组的形式为

$$\left(\underbrace{\sum_{j=1}^{n}\sum_{t=0}^{f}c_{j,f-t}h_{i,j}^{t}}_{\text{第}f(n-1)+i\text{列},0\le f\le M}\quad\cdots\quad\underbrace{\sum_{j=1}^{n}\sum_{t=0}^{M}c_{j,f-t}h_{i,j}^{t}}_{\text{第}f(n-1)+i\text{列},\ f>M}\quad\cdots\right)$$
$$=(0\ \cdots\ 0\ \cdots),\quad 1\le i\le n-1 \tag{16}$$

这里$c_{j,f-t}$表示第$f-t$个子码的第j个码元；i和j作为下标，$h_{f,i}^{t}$为式(9)中$\boldsymbol{h}_t$的元素。

实际中的码字序列$\boldsymbol{C}$不可能半无限长，由式(15)和式(16)可知当码字序列长度大于卷积码的约束长度，利用多组码字序列作为方程的系数可求解出一

$$\boldsymbol{N}=\begin{pmatrix} c_{1,0} & \cdots & c_{n,0} & c_{1,1} & \cdots & c_{n,1} & \cdots & c_{1,M} & \cdots & c_{n,M} \\ c_{1,1} & \cdots & c_{n,1} & c_{1,2} & \cdots & c_{n,2} & \cdots & c_{1,M+1} & \cdots & c_{n,M+1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{1,n\cdot(M+1)} & \cdots & c_{n,n\cdot(M+1)} & c_{1,n\cdot(M+1)+1} & \cdots & c_{n,n\cdot(M+1)+1} & \cdots & c_{1,n\cdot(M+1)+M} & \cdots & c_{n,n\cdot(M+1)+M} \end{pmatrix} \tag{17}$$

该系数矩阵$\boldsymbol{N}$即为识别所需的矩阵模型，由其可估计出某一校验序列$\boldsymbol{H}'$，进而推导出生成多项式矩阵。为方便表示，令$L=n(M+1)$，$L+1=n(M+1)+1$。

3　识别方法

根据以上建立的识别模型，本节提出了校验序列$\boldsymbol{H}'$的识别算法和基于$\boldsymbol{H}'$的生成多项式矩阵$\boldsymbol{G}(x)$求解方法。针对$(n,1,m)$卷积码的该识别方法同文献[5]中的方法相比，有效地降低了所需数据量和计算复杂度。

3.1 校验序列$\boldsymbol{H}'$的识别方法

识别模型的建立和求解中要解决两个问题，如何预知参数(子码长度)n和确定码字起始位置即$c_{i,j}$中j的数值。通过系数矩阵$\boldsymbol{N}$的秩可判断估计的n是否正确，进而可以通过化简后的矩阵$\boldsymbol{N}'$确定码字起始位置，具体算法步骤如下：

(1)设系数矩阵维数$(L+1)\times L$，$L=48$。

(2)假设参数n依次取5,6,7和8(实际应用中n不会超过8[5])。因为6是3的倍数，8是2和4的倍数，当估值不准确时只是码字序列多移位整数个子码长，故构建的矩阵$\boldsymbol{N}$每一行仍满足式(16)。

(3)根据步骤(2)中n的值由已知码字序列$\boldsymbol{C}$构造系数矩阵$\boldsymbol{N}$，所需数据量为：$(n\cdot 49+48)$ bit，当$n=8$时所需数据量最多，为440 bit小于500 bit。

(4)把$\boldsymbol{N}$化成行最简形$\boldsymbol{N}'$，计算出$\boldsymbol{N}$的秩K，判断K是否等于列数L，若等于则表明式(16)只有全0解，$\boldsymbol{N}'$除最后一行外为单位阵，此时返回步骤(2)改变n的取值；若小于L则表明具有非0解，化简后的矩阵即为要分析的结果，执行步骤(5)。

(5)秩K不等于列数L时，矩阵化简结果如下[5,6]：

$$\boldsymbol{N}'=\begin{pmatrix} \boldsymbol{I}_a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \boldsymbol{I}_v & & & & & \\ 0 & 0 & \boldsymbol{I}_1\boldsymbol{P}_{n-1}^{1} & & & & \\ 0 & 0 & 0 & \boldsymbol{I}_1\boldsymbol{P}_{n-1}^{2} & & & \\ 0 & 0 & 0 & 0 & \cdots & & \\ 0 & 0 & 0 & 0 & 0 & \boldsymbol{I}_1\boldsymbol{P}_{n-1}^{b} & \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{I}_w \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{18}$$

其中$\boldsymbol{I}_a$，$\boldsymbol{I}_v$，$\boldsymbol{I}_1$和$\boldsymbol{I}_w$是单位阵(下标表示维数)，$\boldsymbol{P}_{n-1}^{i}$是$(v+i\cdot n)\times(n-1)$维的矩阵。由矩阵式(18)可以很容易识别出参数n。出现$\boldsymbol{I}_a$是由于构造的系数矩阵$\boldsymbol{N}$中的第1个元素$c_{i,j}$不是码字序列起始位置，a，j和n满足：$a=n-j$；a，v，n，b和w满足：$a+v+n\cdot b+w=L$。矩阵$\boldsymbol{P}_{n-1}^{i}$的各列即为所要识别的校验序列$\boldsymbol{H}'$的部分序列，一般取前若干个$\boldsymbol{P}_{n-1}^{i}$即可。

3.2 生成多项式的求解

由上一节可识别出卷积码的参数n和若干个(记为r个)校验序列$\boldsymbol{H}'$的部分序列，现介绍由识别出的r个部分序列推导出生成多项式矩阵方法的具体步骤：

(1)设$\boldsymbol{P}_{n-1}^{1}$在$\boldsymbol{N}'$的第p_1至p_1+n-1列，由p_1，$\boldsymbol{I}_a$的维数a和识别出的n估计记忆长度m，m估计值为：$\left\lfloor 2\cdot\left(\frac{p_1-a}{n}\right)\right\rfloor$。将识别出的第$i$个校验序列$\boldsymbol{H}'$的部分序列按参数$n$抽取，构造$F_2[x]$上的$n$个多项式$h_j^i(x)\,(1\le i\le r,1\le j\le n)$:$h_1^i(x),\cdots,h_n^i(x)$，作为$\boldsymbol{H}(x)$的某一行：$\boldsymbol{h}^i(x)$。其中$\lfloor\ \rfloor$表示下取整，抽取时$\boldsymbol{P}_{n-1}^{i}$所在的列对应的对角线上0改为1。

(2)由识别出的参数n和估计出的记忆长度m假设式(3)所示的生成多项式矩阵$\boldsymbol{G}(x)$,$\boldsymbol{G}(x)$的n个元素分别记为$g_j(x),1\le j\le n$。若识别出$n=2$，则有：$g_1(x)=h_2^1(x)$，$g_2(x)=h_1^1(x)$，可直接识别出

个或多个校验序列$\boldsymbol{H}'$的部分序列，且这些序列能够体现出码字序列$\boldsymbol{C}$的完整约束关系，在末尾加上无限多个0既可以构成校验序列。

由已知的码字序列$\boldsymbol{C}$根据式(16)构造求解校验序列$\boldsymbol{H}'$的方程系数，如式(17)所示，$\boldsymbol{N}$为$[n(M+1)+1]\times n(M+1)$维的矩阵，系数矩阵的列数$n(M+1)$要大于$(n,1,m)$卷积码的约束长度。由于译码复杂度的限制，卷积码约束长度通常情况下不大于48[10]，构建矩阵$\boldsymbol{N}$时$n(M+1)$取值为48即可。

$\boldsymbol{G}(x)$[7]。若 $n \neq 2$，则由关系式(5)建立 $\boldsymbol{G}(x)$ 与 r 个 $\boldsymbol{h}^i(x)$ 的方程，$[g_1(x)\ \ g_2(x)\ \cdots\ g_n(x)]\cdot[\boldsymbol{h}^i(x)]^{\mathrm{T}}=0$ $(1\le j\le n,\ 1\le i\le r)$，即

$$\left.\begin{aligned} &g_1(x)\cdot h_1^1(x)+g_2(x)\cdot h_2^1(x)+\cdots+g_n(x)\cdot h_n^1(x)=0\\ &g_1(x)\cdot h_1^2(x)+g_2(x)\cdot h_2^2(x)+\cdots+g_n(x)\cdot h_n^2(x)=0\\ &\qquad\qquad\vdots\\ &g_1(x)\cdot h_1^r(x)+g_2(x)\cdot h_2^r(x)+\cdots+g_n(x)\cdot h_n^r(x)=0 \end{aligned}\right\} \tag{19}$$

因识别出参数子码长度为 n、记忆长度为 m，故方程组式(19)中共有 $n(m+1)$ 个未知数。在 $F_2[x]$ 上，方程组成立条件为 x 所有幂次的系数均等于 0，故方程组式(19)中每个方程在 F_2 上可等效于多个。设 $\boldsymbol{h}^i(x)$ 中元素的最高幂次为 M^i，则方程组式(19)可等价于 F_2 上的 $\sum_{i=1}^{r}(m+M^i+1)$ 个方程，可见 $\sum_{i=1}^{r}(m+M^i+1)$ 大于 $n(m+1)$ 即可确定 $g_j(x)$ 的系数，进而求解出生成多项式矩阵 $\boldsymbol{G}(x)$，所以 r 的取值只需满足 $\sum_{i=1}^{r}(m+M^i+1)$ 大于 $n(m+1)$。

(3)将方程组式(19)转化为 F_2 上的方程组，利用高斯消元法求解。方程组求解过程中可能存在 $q(q\ge 1)$ 组解，由 q 组解中幂次最小的一组构成生成多项式矩阵 $\boldsymbol{G}(x)$，完成识别。

3.3 计算复杂度分析

文献[5]中的方法要求等间隔选取码字序列，间隔长度为可能码长的最小公倍数(840 bit)，若构建系数矩阵 $\boldsymbol{N}$ 则需 $840\cdot L+L=840\cdot 48+48=40368$ bit，而本文仅需不到 500 bit 数据。文献[5]中的方法经过 1 次矩阵化简运算识别出参数 n 和码字起始位置后，需再进行 $n-1$ 次 $(2,1,m)$ 卷积码分析矩阵的构建和化简运算，复杂度为：$O(L^3/2)+O((n-1)\cdot L^3/2)$，即 $O(n\cdot L^3/2)$；假设 $(n,1,m)$ 卷积码码长 n 从 2 到 8 等概率出现，则本文方法识别出码长 n 和校验序列 $\boldsymbol{H}'$，所需构建和化简系数矩阵的平均次数为：$\frac{1}{7}\times 1+\frac{3}{7}\times 2+\frac{1}{7}\times 3+\frac{2}{7}\times 4=\frac{18}{7}$，由 $\boldsymbol{H}'$ 推导出生成多项式矩阵 $\boldsymbol{G}(x)$ 需要进行 1 次方程系数矩阵的构建和化简，且该矩阵列数不会大于 L，所以本文识别方法复杂度最高为：$O(25\cdot L^3/14)$。

4 仿真实验与容错性分析

本节以常用的 (3,1,5) 卷积码和 (4,1,5) 卷积码为例，对该识别方法的有效性进行了验证，同时在蒙特卡洛仿真实验的基础上分析了该识别方法的容错性能，即在码字序列含有误码情况下能够正确识别的能力。

4.1 实例仿真

例 1 (3,1,5) 卷积码的生成多项式矩阵用八进制数分别表示为[11]：$\boldsymbol{G}(47\ \ 53\ \ 75)$，即

$$\boldsymbol{G}(x)=[1+x^3+x^4+\ x^5\quad 1+x^2+x^4+x^5\quad 1+x+x^2+x^3+x^5] \tag{20}$$

下面是该卷积码非码字同步的 500 bit 编码数据：1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 1 1 0 1 0 1 … 0 0 1 1 0 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1。按照 2.1 节和 2.2 节的方法建立校验序列识别模型 $\boldsymbol{N}$，估计参数 $n=6$ 时，矩阵模型化简后的 $\boldsymbol{N}'$ 形式如图 1 所示。

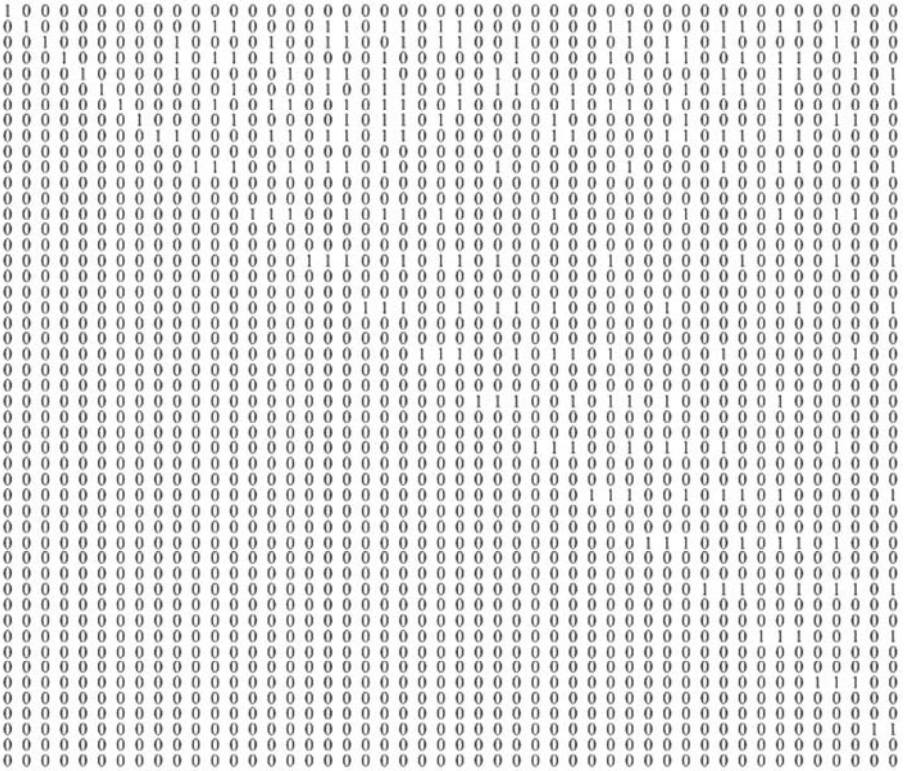

图 1 矩阵模型化简结果

由图中矩阵化简的结果可以很容易识别出$n=3$，$k=1$，码字起始位为2。由于码字起始位不是0，第1个有效的校验序列$\boldsymbol{P}_{n-1}^{1}$出现在第12和13列：1 0 1 0 0 1 0 0 0 1 1 0; 1 0 1 0 1 0 1 0 0 1 0 1。抽取后可得：$h_1^1(x)=x^3+1$，$h_2^1(x)=1$，$h_3^1(x)=x^3+x^2$；$h_1^2(x)=x^3+1$，$h_2^2(x)=x^2$，$h_3^2(x)=x^3+1$，依此抽取$\boldsymbol{P}_{n-1}^{2}$和$\boldsymbol{P}_{n-1}^{3}$。同时，按3.1节步骤(1)估计记忆长度为6，假设生成多项式矩阵：

$$\boldsymbol{G}(x)=[g_{1,0}+g_{1,1}x+\cdots+g_{1,6}x^6 \quad g_{2,0}+g_{2,1}x+\cdots+g_{2,6}x^6 \quad g_{3,0}+g_{3,1}x+\cdots+g_{3,6}x^6] \tag{21}$$

由3.1节推导生成多项式矩阵方法的步骤(2)建立F_2上的齐次线性方程组$\boldsymbol{A}\cdot\boldsymbol{G}^{\mathrm{T}}=\boldsymbol{0}$，其中$\boldsymbol{G}=[g_{1,0}\ g_{1,1}\cdots g_{1,6}\ g_{2,0}\ g_{2,1}\cdots g_{2,6}\ g_{3,0}\ g_{3,1}\cdots g_{3,6}]$，$\boldsymbol{A}$为$F_2$上$22\times21$维矩阵，方程组如式(22)所示。

$$\boldsymbol{A}\cdot\boldsymbol{G}^{\mathrm{T}}=\begin{bmatrix}
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&0&0\\
0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&0\\
0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&0&1&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&1&0&1&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&1&0&0&1&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}\cdot\begin{pmatrix}
\boldsymbol{g}_{1,0}\\ \vdots\\ \boldsymbol{g}_{1,6}\\ \boldsymbol{g}_{2,0}\\ \vdots\\ \boldsymbol{g}_{2,6}\\ \boldsymbol{g}_{3,0}\\ \vdots\\ \boldsymbol{g}_{3,6}
\end{pmatrix}=0 \tag{22}$$

利用消元法求解方程组$\boldsymbol{A}\cdot\boldsymbol{G}^{\mathrm{T}}=\boldsymbol{0}$得解为：$\boldsymbol{G}_1=[1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1\,1\,1\,1\,0\,1\,0]$，$\boldsymbol{G}_2=[0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1\,1\,1\,1\,0\,1]$。可见$\boldsymbol{G}_2$只是$\boldsymbol{G}_1$的移位，所以识别出该码字序列为(3,1,5)卷积码编码序列，生成多项式矩阵为：$[1+x^3+x^4+x^5 \quad 1+x^2+x^4+x^5 \quad 1+x+x^2+x^3+x^5]$，与式(20)相同，识别准确有效。

例 2　(4,1,5)卷积码的生成多项式矩阵用八进制数分别表示为[11]：$\boldsymbol{G}$(53　67　71　75)，即

$$\boldsymbol{G}(x)=[1+x^2+x^4+x^5 \quad 1+x+x^3+x^4+x^5 \quad 1+x+x^2+x^5 \quad 1+x+x^2+x^3+x^5] \tag{23}$$

下面是该卷积码输出的500 bit编码数据：1 1 1 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 0 1 …… 1 1 0 0 0 1 0 0 0 0 1 0 1 1 1 0 1 0 0。同例1的方法步骤，可识别出参数$n=4$，$k=1$，码字起始位为0。第1个有效的校验序列$\boldsymbol{P}_{n-1}^{1}$出现在第10,11和12列：1 0 0 1 1 1 0 1 1 1 0 0; 0 0 1 1 0 0 0 1 1 0 1 0; 0 1 1 0 1 0 0 0　1　0　0　1，抽取后可得：$h_1^1(x)=1+x+x^2$，$h_2^1(x)=1+x$，$h_3^1(x)=0$，$h_4^1(x)=x+x^2$；$h_1^2(x)=1$，$h_2^2(x)=0$，$h_3^2(x)=1+x^2$，$h_4^2(x)=x+x^2$；$h_1^3(x)=1+x$，$h_2^3(x)=x^2$，$h_3^3(x)=x^2$，$h_4^3(x)=1$。依此抽取$\boldsymbol{P}_{n-1}^{2}$，同时估计记忆长度为5，建立齐次线性方程组$\boldsymbol{A}\cdot\boldsymbol{G}^{\mathrm{T}}=\boldsymbol{0}$，求得生成多项式矩阵：$[1+x^2+x^4+x^5 \quad 1+x+x^3+x^4+x^5 \quad 1+x+x^2+x^5 \quad 1+x+x^2+x^3+x^5]$，可见识别结果正确。

4.2 容错性能分析

在假设子码长度 n 估值准确情况下，分析该识别方法的容错性能，即能够正确识别不同误码率的码字序列的概率。以 4.1 节中的 $(3,1,5)$ 和 $(4,1,5)$ 卷积码为例，通过蒙特卡洛仿真实验统计正确识别的次数。每次仿真实验从 10000 bit 的码字序列中随机选取连续的 500 bit 进行识别，识别概率如图 2 所示。由图可见，随着子码长度 n 的增大识别概率有明显的下降，这是因为 n 的增大增加了约束长度，使长度为 $n(m+1)$ 的序列含有错误码元的可能性增加；但在误码率高达 10^{-2} 时，对以上两种卷积码的成功识别率仍可以达到 90%以上，所以该方法具有较好的容错性能和较高的实际应用价值。

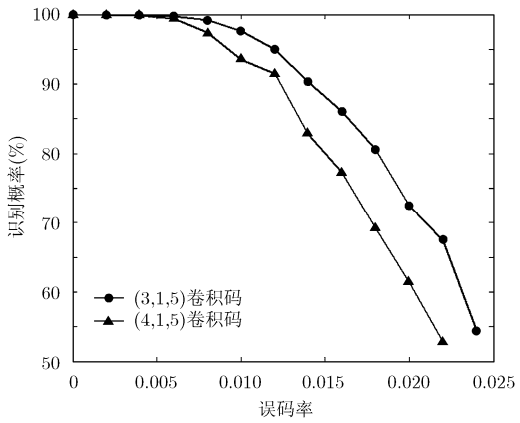

图 2 两种卷积码的识别概率

5 结论

本文通过改进的分析矩阵构造方法，在仅需不到 500 bit 数据量的情况下能够识别出所有 $(n,1,m)$ 卷积码的子码长度 n 、码字起始位置和校验序列 $\boldsymbol{H}'$，在对记忆长度进行估计的基础上由校验序列 $\boldsymbol{H}'$ 的部分序列构造了生成多项式矩阵 $\boldsymbol{G}(x)$ 的识别方程组，进而利用高斯消元法求解该方程组，准确有效地完成了 $(n,1,m)$ 卷积码的识别。该识别方法不需任何先验条件，数据利用率高，克服了卷积码现有识别方法的不足，同时具有较好的容错性能，在卫星通信、深空探测及航天控制的通信体制识别、智能通信及信息恢复等领域都有重要应用意义。

参 考 文 献

[1] 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, and Bai Yu. A new recognition method of RS codes[J]. *Electronic Information Warfare Technology*, 2011, 26(2): 36–40.

[2] 闻年成, 杨晓静. 采用秩统计和码根特征的二进制循环码盲识别方法[J]. 电子信息对抗技术, 2010, 25(6): 26–29.
Wen Nian-cheng and Yang Xiao-jing. Blind recognition of cyclic codes based on rank statistic and codes roots characteristic [J]. *Electronic Information Warfare Technology*, 2010, 25(6): 26–29.

[3] 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 and Lu Pei-zhong. A new generalization of key equation[J]. *Journal of Computers*, 2006, 29(5): 711–718.

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

[5] 薛国庆, 常逢佳, 柳卫平, 等. $1/n$ 卷积码盲识别[J]. 无线通信技术, 2009, 38(3): 38–42.
Xue Guo-qing, Chang Feng-jia, Liu Wei-ping, *et al.*. Blind identification of $1/n$ convolutional codes[J]. *Wireless Communication Technology*, 2009, 38(3): 38–42.

[6] 薛国庆, 李易, 柳卫平. 系统卷积码盲识别[J]. 信息安全与通信保密, 2009, 54(2): 57–60.
Xue Guo-qing, Li Yi, and Liu Wei-ping. Blind identification of system convolutional codes[J]. *Information Security and Communications Privacy*, 2009, 54(2): 57–60.

[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 Xiao-jun, and Zhou Xi-yuan. Blind recognition of convolutional coding based on Walsh-Hadamard transform[J]. *Journal of Electronics & Information Technology*, 2010, 32(4): 884–888.

[8] CCSDS/131. 0-B-1-2003, CCSDS Recommendation for TM Synchronization and Channel Coding[S]. Washington: CCSDS Secretariat, 2003.

[9] 赵晓群. 现代编码理论[M]. 武汉: 华中科技大学出版社, 2008: 154–189.

[10] 陈占计. (2,1,4)卷积码的逻辑代数译码方法研究[D]. [硕士论文], 四川大学, 2006.

[11] Katsiotis A, Rizomiliotis P, and Kalouptsidis N. New constructions of high-performance low-complexity convolutional codes[J]. *IEEE Transactions on Communications*, 2010, 58(7): 1950–1961.

刘建成： 男，1987 年生，硕士生，研究方向为信道编码识别分析.
杨晓静： 女，1963 年生，硕士，副教授，研究方向为编码理论、通信系统.