一种二进制伪随机序列盲识别方法

张天骐 赵 亮* 张 婷 杨 凯
(重庆邮电大学信号与信息处理重庆市重点实验室 重庆 400065)

摘 要：针对二进制伪随机序列生成多项式盲识别方法存在的需要预先知道生成多项式阶数、算法容错性能较差且复杂度较高的问题。该文提出首先将接收序列按照估计的生成多项式阶数建立分析矩阵，然后利用伽罗华域高斯列消元的方法识别出接收序列生成多项式的阶数，最后根据生成多项式的阶数构造关于生成多项式系数的方程组。为降低算法复杂度，在有限的多项式库中进行匹配搜索，能够满足该方程组的多项式就是接收序列的生成多项式。仿真结果表明，提出的方法能够区分接收序列是 m 序列、Gold 序列或者是其他二进制伪随机序列，并有效识别其各自的生成多项式，且具有较好的容错性能。

关键词：伪随机序列；高斯列消元；匹配搜索；生成多项式
中图分类号： TN911.2 **文献标识码**： A **文章编号**：1009-5896(2018)02-0394-06
DOI: 10.11999/JEIT170552

A Blind Recognition Method of Binary Pseudo-random Sequence

ZHANG Tianqi ZHAO Liang ZHANG Ting YANG Kai
(*Chongqing Key Laboratory of Signal and Imformation Processing*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: For the generator polynomial blind recognition method of binary pseudo-random sequences, it is necessary to know the polynomial's order in advance, the algorithm with poor fault tolerance and high complexity. In this paper, the analysis matrix is first constructed according to the estimated polynomial's order of the intercepted sequence. Then the method of Galoisian column Gaussian elimination is used to identify the order of the polynomial of the intercept sequence. Finally, the equation set is constructed according to the polynomial's order. In order to reduce the complexity of the algorithm, the polynomials that satisfy the equations in the finite polynomial library are the generator polynomials of the intercepted sequences. The simulation results show that the proposed method can distinguish the m sequence, the Gold sequence, or other binary pseudorandom sequences, and effectively identify their own generating polynomials, and has good fault tolerance.

Key words: Pseudo-random sequence; Column Gaussian elimination; Match search; Generator polynomial

1 引言

伪随机序列因具有良好的伪随机特性，而被广泛地的应用在扩频通信、雷达测距、码分多址系统以及密码学等领域。其中最常用的二进制伪随机序列包括 m 序列、Gold 序列和 Kasami 序列等。m 序列又叫做最长线性移位寄存器序列，Gold 序列和 Kasami 序列都是基于 m 序列优选对产生的。而二进制伪随机序列的生成多项式是其重要的参数，是完成扩频序列恢复和信息解密的基础。因此对二进制伪随机序列的参数识别具有比较重要的理论意义和价值[1−5]。

现有的国内外对二进制伪随机序列参数识别的文献中，梅西算法(BM)算法[6,7]、欧几里德算法[8]都能达到识别伪随机序列生成多项式的目的，但上述方法在误码存在的条件下不再能做到有效识别。因此，随着该研究的进一步深入，又出现了基于高阶统计分析的三阶相关函数法(TCF)[9−13]，根据 TCF 峰值出现的位置确定伪随机序列的本原多项式；文献[14]针对 Gold 序列的分类搜索算法，在识别高阶 Gold 序列时，算法复杂度过大；文献[15]将 m 序列和信道编码中的 BCH 码联系在一起，根据 BCH 码的性质进行识别，但只限于识别 20 阶以内的 m 序列；针对 Gold 序列生成多项式识别的方法还有匹配搜索算法[16]，根据伪随机序列位与位之间的线性约束关系构造关于生成多项式系数的方程组，并搜索匹配满足该方程组解的多项式。但是，基于高阶统计分析的方法容错性能较差，而搜索匹

收稿日期：2017-06-08；改回日期：2017-08-29；网络出版：2017-09-22
*通信作者：赵亮 535836848@qq.com
基金项目：国家自然科学基金(61671095, 61371164)，信号与信息处理重庆市市级重点实验室建设项目(CSTC2009CA2003)，重庆市教育委员会科研项目(KJ130524, KJ1600427, KJ1600429)
Foundation Items: The National Natural Science Foundation of China (61671095, 61371164), The Project of Key Laboratory of Signal and Information Processing of Chongqing (CSTC2009 CA2003), The Research Project of Chongqing Educational Commission (KJ130524, KJ1600427, KJ1600429)

配算法存在需要遍历所有可能出现的情况因此导致计算复杂度较高的问题。同时搜索匹配算法需要预先知道接收序列的阶数，即构造该序列的线性移位寄存器的抽头数，并不能做到全盲识别。

针对上面提到的问题，本文提出首先利用伽罗华域高斯列消元的方法识别出接收序列的阶数，然后使用搜索匹配算法识别出生成多项式。之所以首先识别生成多项式阶数，是因为在实际应用中，接收一段序列，其先验知识是未知的，因此先识别出生成多项式阶数再识别生成多项式，以达到全盲识别的目的。在识别二进制伪随机序列的生成多项式时，首先构造生成多项式库，在有限的多项式库中进行搜索匹配，使搜索匹配算法的复杂度明显降低，并与传统搜索匹配算法相比在识别性能上也有一定的提高。本文方法适用于各阶数的二进制伪随机序列(m 序列、Gold 序列、Kasami 序列等)的生成多项式识别，能够在未知接收序列生成多项式阶数的情况下，有效识别接收序列的生成多项式的阶数和生成多项式，并根据搜索匹配成功的多项式所在的多项式库，可以有效区分 m 序列、Gold 序列或是其他二进制伪随机序列。

2　识别模型

二进制伪随机序列是按照确定的规律产生的二元序列，如式(1)所示。

$$a_i = c_l a_{i-l} + \cdots + c_v a_{i-v} + \cdots + c_1 a_{i-1} \tag{1}$$

即二进制伪随机序列的第 i 位，可以由其前 l 位线性表示，l 为序列生成多项式的阶数。集合 $\{a_i\} = a_0, a_1, a_2, \cdots$ 中的元素可以由递推公式计算得到

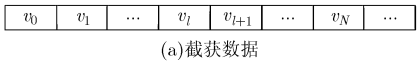
$$a_i = \sum_{v=1}^{l} c_v a_{i-v}, \quad i \geq 0 \tag{2}$$

则有

$$c_l a_{i-l} + c_{l-1} a_{i-l+1} + \cdots + c_v a_{i-v} + \cdots + a_i = 0 \tag{3}$$

本文研究对象为二进制伪随机序列，因此式中元素 $a_i, c_l \in \mathrm{GF}(2)$。伪随机序列的线性递推关系说明其具有严格的线性约束关系，这是本文识别方法的基础。

若接收序列为 $V = \{v_0, v_1, v_2, \cdots, v_l, \cdots\}$，按照估计的生成多项式阶数 $\hat{l}$ 建立分析矩阵如图 1 所示，依次累加 $\hat{l}$ 并迭代分析，直到完成阶数的识别。



(a)截获数据

v_0	v_1	…	$v_{\hat{l}}$
v_1	v_2	…	$v_{\hat{l}+1}$
⋮	⋮	⋮	⋮
v_M	v_{M+1}	…	$v_{\hat{l}+M}$

(b)分析矩阵

图 1　识别模型

接收序列的阶数识别成功以后，将接收序列按照生成多项式的真实阶数进行排列，以便于进行后续生成多项式的识别。

3　识别原理

实际中对于接收的伪随机序列，其任何先验知识都是未知的，包括生成多项式和其阶数。本文对二进制伪随机序列的识别方法就是在未知序列参数的情况下对其生成多项式识别进行识别。为了识别出二进制伪随机序列的生成多项式，首先利用伽罗华域高斯列消元法识别生成多项式的阶数，即生成该序列的线性反馈席位寄存器的抽头数，其次根据式(2)这一二进制伪随机序列固有的性质构造关于生成多项式的方程组，在生成多项式库中匹配搜索，进而识别出生成多项式。因此本文主要结构分为两部分：生成多项式阶数的识别和生成多项式的识别。

3.1　生成多项式阶数的识别

由伪随机序列的递推式(2)可知：伪随机序列的第 i 个元素 $a_i, (i \geq l)$ 必定是其前面 l 个元素 $a_{i-1}, a_{i-2}, \cdots, a_{i-l}$ 的线性组合。当接收序列构造的分析矩阵的列数大于 l 时，必定出现某些相关列可以被独立列线性表示，因此考虑使用高斯列消元法对分析矩阵进行化简。高斯列消元法在文献[17]中有详细的介绍。

在无误码条件下某些列经过高斯列消元变换将被化为全零列。如图 2 所示，对不含误码的 7 阶 m 序列构造的分析矩阵化简后的结果，阴影部分的 7 列表示独立列，后面的 3 列为相关列将被化为全零列。

接下来考虑含误码情况下对序列生成多项式阶数的识别，在含误码条件下，分析矩阵经过化简后的相关列不再能化简为全零列，但相关列中非零元素的比例远小于零元素的个数，即相关列的列重(元素 1 的个数)要远小于独立列的列重。考虑伪随机序列中 0 和 1 的概率趋近于 1/2，因此对 M 行的分析矩阵进行高斯列消元操作之后，独立列的列重将趋近于 $M/2$，而相关列的列重将远小于 $M/2$，随着误码率的提高，相关列和独立列之间的线性约束关系被破坏，相关列的列重也将趋近于 $M/2$，但只要设

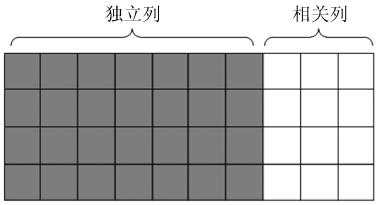


图 2　分析矩阵化简结果

置合适的阈值依然可以区分相关列和独立列。令 $w_j, j=1,2,\cdots,M$，为经过高斯列消元操作后的各列的列重，T_1 为设置的阈值，则有

$$\left.\begin{aligned} w_j \le T_1,\ \text{相关列} \\ w_j > T_1,\ \text{独立列} \end{aligned}\right\} \tag{4}$$

列重 w_j 大于阈值的列被认为是独立列，否则被认为是相关列，得到的独立列的个数就是序列生成多项式的阶数。

完成序列生成多项式阶数 l 的识别之后，下一步将进行生成多项式的识别。

3.2 生成多项式的识别

考虑根据序列的线性递推关系可以表示为齐次线性方程：

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{l-1} & a_l \\ a_1 & a_2 & \cdots & a_l & a_{l+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_l & a_{l+1} & \cdots & a_{2l-1} & a_{2l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_M & a_{M+1} & \cdots & a_{M+l-1} & a_{M+l} \end{pmatrix} \cdot \begin{pmatrix} c_l \\ c_{l-1} \\ \vdots \\ c_1 \\ 1 \end{pmatrix} = 0 \tag{5}$$

理论上只要找到符合上述齐次线性方程组的 $(1,c_1,c_2,\cdots,c_{l-1},c_l)$ 的解，即为序列的生成多项式。

由于序列在传输过程中不可避免将受到信道中噪声的影响，在接收序列中不可避免地会出现误码，不能保证在正确生成多项式的情况下式(6)中的方程组全部都能成立，因此对 l 阶序列建立方程组如式(7)：

$$g(x) = \hat{c}_l x^l + \hat{c}_{l-1} x^{l-1} + \cdots + \hat{c}_1 x + 1 \tag{6}$$

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{l-1} & a_l \\ a_1 & a_2 & \cdots & a_l & a_{l+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_l & a_{l+1} & \cdots & a_{2l-1} & a_{2l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_M & a_{M+1} & \cdots & a_{M+l-1} & a_{M+l} \end{pmatrix} \cdot \begin{pmatrix} \hat{c}_l \\ \hat{c}_{l-1} \\ \vdots \\ \hat{c}_1 \\ 1 \end{pmatrix} = R = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_l \\ \vdots \\ r_M \end{pmatrix} \tag{7}$$

在无误码情况下，若 $(\hat{c}_l,\hat{c}_{l-1},\cdots,\hat{c}_2,\hat{c}_1,1)$ 是序列真实生成多项式的系数，则有 $r_j\,(j=0,1,2,\cdots,M)$ 恒等于 0，即 R 中等于 0 的个数一定等于 M。因为实际情况下接收的序列可能含有误码，所以 $r_j(j=0,1,2,\cdots,M)$ 不恒等于 0，即 R 中等于 0 的个数一定小于等于 M。可知若接收数据为随机序列则 R 中元素等于 0 的概率 $P_1\left(r_j=0\right)=1/2$，而伪随机序列构造的数据的 R 中元素等于 0 的概率 $P_2\left(r_j=0\right)\ll 1/2$。因此取

$$S = \frac{M}{2} - \sum_{i=1}^{M} r_i \tag{8}$$

且 S 越大，估计多项式是生成多项式的可能越大。设置阈值 T_2，若 $S \ge T_2$ 就认为此时的估计多项式是真实生成多项式。

综上所述，识别生成多项式的关键是能否找到符合方程组的解，传统搜索匹配符合方程组解的经典思想是遍历所有可能的系数取值，但是随着待识别伪随机序列的阶数提高，需要遍历的可能情况呈指数级急剧增加，例如识别 7 阶时有 2^7 种可能，13 阶时就提高到有 2^{13} 种可能。因此当需要识别高阶的伪随机序列时这种方法局限于算法复杂度的问题并不适用。

因此可以考虑缩小搜索匹配的多项式库的范围。以 m 序列和 Gold 序列为例。已知构造 m 序列的本原多项式是有限的，各阶本原多项式在文献[2]中已详细列出。而 l 阶 Gold 序列的生成多项式是两个 l 阶 m 序列优选对的本原多项式的乘积。设 $\{a\}$ 是 l 阶本原多项式 $m_a(x)$ 生成的 m 序列，$\{b\}$ 是 l 阶本原多项式 $m_b(x)$ 生成的 m 序列，若这两个序列的互相关函数 $Z_{ab}(\tau)$ 满足：

$$\left|Z_{ab}(\tau)\right| = \left|\sum_{i=0}^{2^l-2} \eta\left(a_i\right)\eta\left(b_{i+\tau}\right)\right| \le \begin{cases} 2^{\frac{l+1}{2}}, & l\text{为奇数} \\ 2^{\frac{l+2}{2}}, & l\text{为偶数} \end{cases} \tag{9}$$

那么序列 $\{a\}$ 和 $\{b\}$ 构成优选对，其中 $\eta(\ )$ 表示 $1\leftrightarrow -1$，$0\leftrightarrow 1$ 映射操作。且序列 $\{a\}$ 和 $\{b\}$ 构造的 Gold 序列的生成多项式为 $m_a(x)m_b(x)$。依此可以构造出所有的 l 阶 Gold 序列生成多项式库。从尽量减小搜索范围、压缩算法复杂度的角度考虑，可以构建 m 序列本原多项式库和 Gold 序列生成多项式库。识别 m 序列时在本原多项式库中搜索，同样识别 Gold 序列时在其生成多项式库中搜索，大大减小了搜索量，同时在算法复杂度上有大幅度的降低。同理，在识别其他二进制伪随机序列时，可以构造其生成多项式库，在生成多项式库中进行搜索匹配，已期望达到降低算法搜索量的目的。

对比改进前后的搜索量，对 l 阶的序列进行识别时，文献[16]中的传统匹配搜索算法要进行 $(l+1)\cdot 2^l$ 次乘法和 $l\cdot 2^l$ 次加法，而本文算法秩序进行 $(l+1)\cdot k_l$ 次乘法和 $l\cdot k_l$ 次加法，其中 k_l 是 l 阶序列生成多项式库中多项式的个数。和传统搜索匹配算法相比，改进后算法性能提升体现在需要搜索的多项式的个数明显减少，即搜索量明显下降。以 m 序列和 Gold 序列为例，识别 l 阶序列时传统匹配搜索算法和改进后算法的搜索量对比，如表 1 和表 2 所示。

在识别序列生成多项式时，在生成多项式库中搜索匹配，若第 j 个多项式对应的 $S_j \ge T_2$，$j=1,2,\cdots$，则该多项式就是接收序列的生成多项式。

表 1　l 阶 m 序列搜索量对比

	改进前	改进后	减少(%)
7 阶	2^7	18	85.93
10 阶	2^{10}	60	94.14
13 阶	2^{13}	630	92.30

表 2　l 阶 Gold 序列搜索量对比

	改进前	改进后	减少(%)
7 阶	2^{14}	90	99.45
10 阶	2^{20}	330	99.97
13 阶	2^{26}	8190	99.99

综上所述，算法流程如图 3。

算法步骤：

步骤 1　将接收序列按照估计生成多项式阶数 $\hat{l}$ 构造分析矩阵，利用高斯列消元法进行化简；

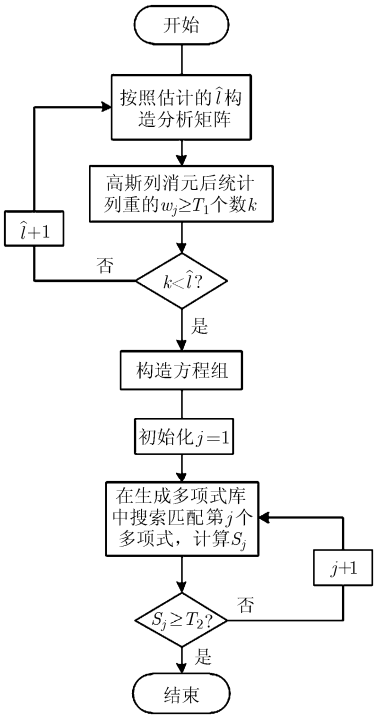


图 3 算法流程图

步骤 2　统计各列的列重 w_j，若满足 $w_j \geq T_1$ 的列数即独立列的个数等于 $\hat{l}$，则 $\hat{l}+1$，并重复步骤 1；

步骤 3　若满足 $w_j \geq T_1$ 的列数即独立列的个数小于 $\hat{l}$，则独立列的个数就是生成多项式的阶数 l；

步骤 4　按照生成多项式阶数 l 构造关于生成多项式系数的方程组，在生成多项式库中进行搜索匹配，直到出现满足 $S_j \geq T_2$ 的第 j 个多项式即为接收序列的生成多项式。

4　仿真验证

由于实际情况下，接收序列不一定为完整周期的长度，属于截断序列，因此在下面的仿真过程中，考虑选取数据长度都小于一个完整周期的长度。例如识别 l 阶序列时，选取序列长度小于 2^l-1。

首先进行生成多项式阶数的识别。以 7 阶 m 序列为例，分别在误码率为 0 以及误码率为 0.02 的条件下，将序列长度为 112 的 m 序列排列为 $M=100$ 行 13 列矩阵，进行高斯列消元后，统计各列的列重，结果如图 4。

从图 4 可以看出，从第 7 列以后的列的列重明显小于前面 7 列的列重。设置阈值 $T_1=30$，w_j 大于阈值 T_1 的只有前 7 列，可得该 m 序列的生成多项式阶数为 7。

再以 7 阶 Gold 序列为例，在误码率为 0 和误码率为 0.02 的条件下，将序列长度为 127 的 Gold 序列排列为 $M=100$ 行 28 列矩阵，进行高斯列消元后，统计各列的列重，结果如图 5。

设置阈值为 $T_1=30$，从图 5 可以看出列重 w_j 大于阈值 T_1 的只有前 14 列，因此可得序列生成多项式的阶数为 14。

选取 7 阶 m 序列、11 阶 m 序列、7 阶 Gold 序列和 11 阶 Gold 序列，数据长度都为 127 位，分别在不同误码率下做 200 次蒙特卡洛仿真，设置阈值为 $T_1=30$，正确识别率如图 6。

从图 6 中可以看出，7 阶 m 序列的识别效果要

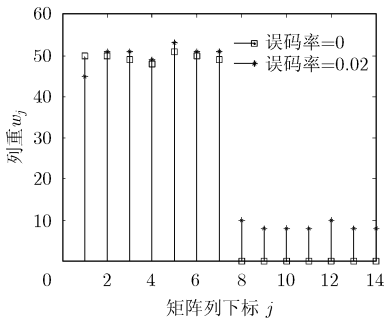


图 4　m 序列生成多项式阶数的识别

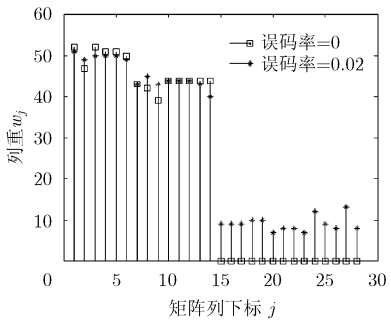


图 5　Gold 序列生成多项式阶数的识别

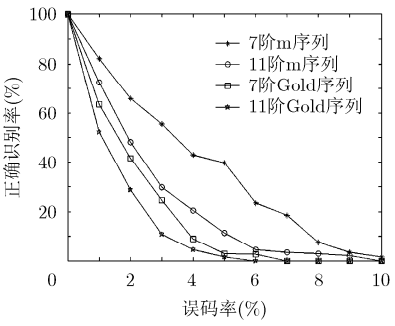


图 6 生成多项式阶数的识别性能

比 11 阶 m 序列识别效果好，7 阶 Gold 序列的识别效果要比 11 阶 Gold 序列识别效果好，7 阶 m 序列的识别效果要比 7 阶 Gold 序列识别效果好，11 阶 m 序列的识别效果要比 11 阶 Gold 序列识别效果好。因此可以得出结论，序列生成多项式阶数的阶数越高，识别率越低。

完成对生成多项式阶数的识别之后，继续进行对生成多项式的识别。

假设已经识别出接收序列的阶数为 13 阶，取 1025 位接收序列。若接收序列是 m 序列，序列误码率为 0.03，将序列构造规模为 1000 的方程组后，设置阈值 $T_2=200$，在阶数为 13 的 m 序列本原多项式中进行搜索匹配结果如图 7。

从图 7 可以看出，只有在多项式下标为 133 时的本原多项式对应的 S 大于阈值 T_2，该本原多项式为 $g(x)=x^{13}+x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+1$。该本原多项式就是序列的生成多项式，识别正确。

若已经识别出接收序列生成多项式阶数为 12，但此时并不知道该序列是 m 序列还是 Gold 序列。在误码率为 0.03 条件下，构造规模为 50 的方程组，所需数据长度为 61 位，设置阈值 $T_2=15$，首先在阶数为 12 的 m 序列本原多项式库中搜索匹配，结果如图 8。

从图 8 中可以看出，明显没有多项式对应的 S 大于阈值 T_2，考虑接收序列是否有可能是 6 阶 Gold 序列，因此在 6 阶 Gold 序列的生成多项式库中进行搜索匹配，结果如图 9。

从图 9 中看出，第 6 个多项式对应的 S 大于阈值 T_2，该多项式为 $x^{12}+x^{10}+x^9+x^5+x^3+x^2+1$，认为该接收序列是 Gold 序列。识别结果正确，且说明在较少数据量的情况下，依然可以有效识别接收序列的生成多项式。

再以 Kasami 序列为例，假设接收数据长度为 925、误码率为 0.03 的 6 阶 Kasami 序列，设置阈值 $T_2=200$，在 6 阶 Kasami 序列对应的生成多项式中进行搜索匹配，结果如图 10。

从图 10 中可以看出，只有下标为 3 的多项式大于阈值 T_2，该多项式为 $x^9+x^5+x^4+x^2+1$，该多项式就是接收序列的生成多项式。

对数据长度都为 925 的 6 阶 Kasami 序列，10 阶、13 阶 m 序列和 10 阶、13 阶 Gold 序列，分别划分后构造规模为 900 的方程组，对生成多项式进行识别，做 200 次蒙特卡洛仿真，识别结果如图 11。

采用本文算法和文献[16]中全搜索算法进行生成多项式的识别性能对比，分别对接收序列长度为 925 的 7 阶 m 序列和 7 阶 Gold 序列进行 200 次蒙特卡罗仿真，在不同误码率下的识别结果如图 12 所示。

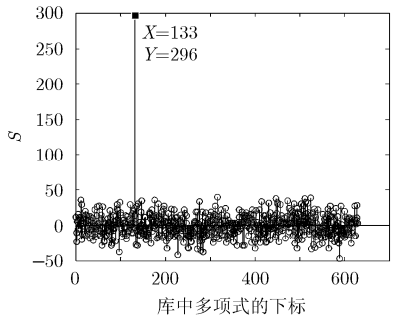


图 7 在 13 阶 m 多项式库中识别结果

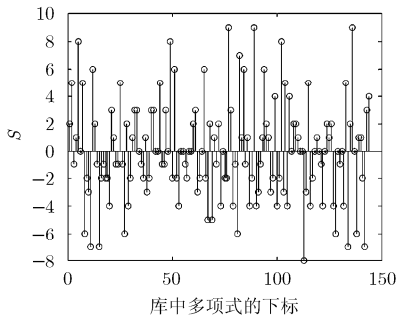


图 8 在 12 阶 m 多项式库中识别结果

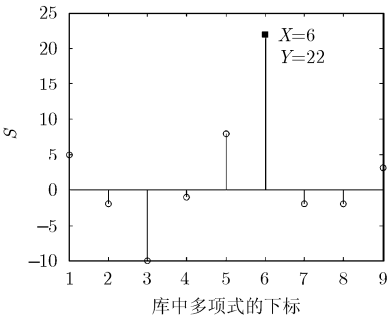


图 9 在 6 阶 Gold 多项式库中识别结果

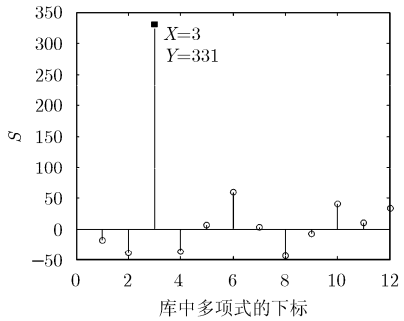


图 10 在 6 阶 Kasami 多项式库中识别结果

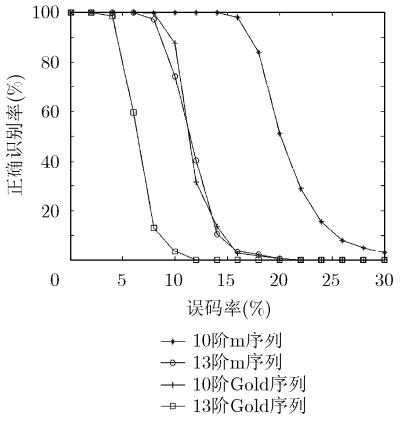


图 11 不同序列的识别性能

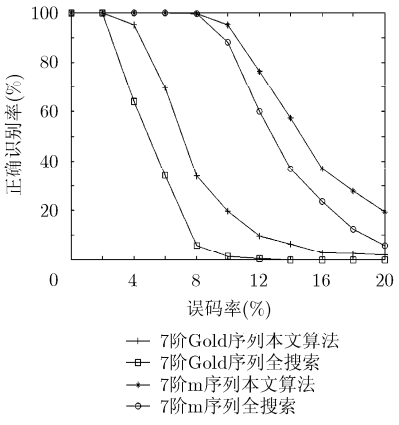


图 12 算法性能对比

5 总结

本文根据传统匹配搜索算法需要已知生成多项式阶数、搜索量大、算法复杂度高的不足，提出了新的伪随机序列生成多项式识别方法。基于伪随机序列的位之间具有严格的线性约束关系，利用高斯列消元的方法找到独立列的个数，完成对序列生成多项式阶数的识别，又构造各种二进制伪随机序列的生成多项式个数是有限的，分别对各种序列构造包含所有生成多项式的库，在多项式库中进行搜索匹配，与传统的全搜索匹配算法相比，计算量和复杂度都得到了明显的降低，正确识别性能也得到了一定的提高，并且可以有效区分接收序列是 m 序列、Gold 序列或者是其他二进制伪随机序列。

参 考 文 献

[1] 肖国镇, 梁传甲, 王育民. 伪随机序列及其应用[M]. 北京: 国防工业出版社, 1985: 123–210.

[2] 林可祥, 汪一飞. 伪随机码的应用[M]. 北京: 人民邮电出版社, 1978: 228–304.

[3] 王统昕. 扩频通信系统中伪随机序列研究与生成算法仿真[D]. [硕士论文], 河北师范大学, 2016.

[4] 徐立平. m 序列及其采样序列互相关特性研究[D]. [硕士论文], 解放军信息工程大学, 2015.

[5] 孙全玲, 吕虹, 陈万里, 等. m 子序列的密码学性质研究[J]. 计算机应用研究, 2018, 35(1): 1–6.
SUN Quanling, LÜ Hong, CHEN Wanli, *et al*. Research on cryptographic properties of m subsequences[J]. *Application Research of Computers*, 2018, 35(1): 1–6.

[6] 万哲先. 代数和编码[M]. 北京: 高等教育出版社, 2007: 257–260.

[7] BERLEKAMP E R. Algebraic Coding Theory. McGraw-Hill Book Company[M]. New York: USA, 1968: 313–325.

[8] HEYDTMANN A E and JENSEN J M. On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for decoding[J]. *IEEE Transactions on Information Theory*, 2000, 46(7): 2614–2624. doi: 10.1109/18.887869.

[9] SHEN Lei and ZHAO Zhijin. Blind estimation of the pseudo-random sequences of direct sequence spread spectrum signals in multi-Path using fast ICA[C]. Pacific-Asia Conference on Circuits, Communications and Systems, IEEE Computer Society, Chengdu, 2009: 531–535.

[10] 俎云霄. 基于高阶统计处理技术的 m-序列检测及识别[J]. 电子与信息学报, 2007, 29(7): 1576–1579.
ZU Yunxiao. The detection and recognition of m-sequence using higher-order statistical processing[J]. *Journal of Electronics & Information Technology*, 2007, 29(7): 1576–1579.

[11] 赵知劲, 顾骁炜, 沈雷, 等. 宽带码分多址信号的戈尔德序列盲识别[J]. 电波科学学报, 2015, 30(3): 603–608. doi: 10.13443/j.cjors.2014060801.
ZHAO Zhijin, GU Xiaowei, SHEN Lei, *et al*. Blind identification of Gold sequences in wideband code division multipie access signal[J]. *Chinese Journal of Randio Science*, 2015, 30(3): 603–608. doi: 10.13443/j.cjors.2014060801.

[12] 赵知劲, 强芳芳, 李淼, 等. 利用拟合优度检验的 NPLSC-DSSS 信号伪码盲估计[J]. 电子与信息学报, 2017, 39(3): 749–753. doi: 10.11999/JEIT160541.
ZHAO Zhijin, QIANG Fangfang, LI Miao, *et al*. Blind estimation of pseudo-random noise codes in NPLSC-DSSS signals based on goodness of fit test[J]. *Journal of Electronics & Information Technology*, 2017, 39(3): 749–753. doi: 10.11999/JEIT160541.

[13] 赵知劲, 强芳芳, 顾骁炜, 等. 利用三阶相关特征信息的周期长码扩频信号伪码盲估计[J]. 信号处理, 2016, 32(6): 739–745. doi: 10.16798/j.issn.1003-0530.2016.06.014.
ZHAO Zhijin, QIANG Fangfang, GU Xiaowei, *et al*. Blind estimation of pseudo-random codes in period long code spread spectrum signals by using triple correlation feature information[J]. *Journal of Signal Processing*, 2016, 32(6): 739–745. doi: 10.16798/j.issn.1003-0530.2016.06.014.

[14] 张希会. 一种基于分类搜索的 Gold 误码修正算法[J]. 电讯技术, 2017, 57(4): 402–406. doi: 10.3969/j.issn.1001-893x.2017.04.006.
ZHANG Xihui. An error correction algorithm for Gold codes based on classification search[J]. *Telecommunication Engineering*, 2017, 57(4): 402–406. doi: 10.3969/j.issn.1001-893x.2017.04.006.

[15] 柴先明, 魏跃敏, 师栋锋, 等. 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. doi: 10.3724/SP.J.1146.2010.00028.
CHAI Xianming, WEI Yuemin, SHI Dongfeng, *et al*. 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. doi: 10.3724/SP.J.1146.2010.00028.

[16] 柴先明, 彭耿, 师栋锋, 等. 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): 2222–2227. doi: 10.3788/OPE.20111909.2222.
CHAI Xianming, PENG Geng, SHI Dongfeng, *et al*. Generator polynomial estimation of pseudo-random sequence based on match-searching[J]. *Optices and Precision Engineering*, 2011, 19(9): 2222–2227. doi: 10.3788/OPE.20111909.2222.

[17] 张天骐, 易琛, 张刚, 等. 基于高斯列消元法的线性分组码参数盲识别[J]. 系统工程与电子技术, 2013, 35(7): 1514–1519. doi: 10.3969/j.issn.1001-506X.2013.07.27.
ZHANG Tianqi, YI Chen, ZHANG Gang, *et al*. Blind identification of parameters of linear block codes based on columns Gaussian elimination[J]. *Systems Engineering and Electronics*, 2013, 35(7): 1514–1519. doi: 10.3969/j.issn.1001-506X.2013.07.27.

张天骐：男，1971 年生，博士后，教授，主要研究方向为扩频信号的盲处理、神经网络实现以及信号的同步处理.

赵　亮：男，1991 年生，硕士生，研究方向为信道编码参数盲识别.

张　婷：男，1991 年生，硕士生，研究方向为通信信号处理.

杨　凯：男，1990 年生，硕士生，研究方向为通信信号处理.