基于可信度累积的伪随机序列多项式估计算法

陈松，黄开枝，赵华
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对高阶误码条件下伪随机序列多项式估计算法效率不高、容错性能差等问题进行研究，提出一种基于可信度累积的多项式估计算法。该算法结合了基于二元序列迭代的 BM 算法和改进型 Chase 算法，利用序列软信息，在 BM 算法外部构建序列及多项式可信度集合，通过可信度累积实现估计。然后，利用本原多项式的二元域性质，通过缩小累积多项式规模，提高估计精度。仿真结果表明，该算法性能不受制于多项式抽头个数，在误码率为 18%的条件下能够完成 17 阶 m 序列多项式估计。

关键词：m 序列；本原多项式；可信度；BM 算法；软信息
中图分类号：TN929.5 **文献标识码**：A **文章编号**：1000-436X(2012)09-0125-07

Polynomial estimation method for PN sequence based on reliability accumulation

CHEN Song, HUANG Kai-zhi, ZHAO Hua
(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: The issues of insufficient efficiency and poor error-tolerance of current high-order polynomial estimation methods under error conditions were studied. By combining the iterative berlekamp-massey(BM) algorithm in GF(2) and the improved Chase algorithm, a novel algorithm based on reliability accumulation was proposed. The sequence soft information was mapped to sequence reliability as the input information of BM algorithm, and the corresponding output reliability of estimated polynomial was accumulated as the rule of correct polynomial. In order to improve the estimation precision, the candidate reliability-accumulated polynomial set were reduced by the characteristics of primitive polynomial in GF(2). The simulation results show that the proposed method is irrelevant with the tapped number of ator polynomial, and has a good estimation performance to estimate 17-order polynomials when the sequence BER is 18%.

Key words: m sequence; primitive polynomial; reliability; BM algorithm; soft information

1 引言

伪随机（PN）序列具有抗干扰能力强、低截获、保密性能好等优点，在扩频通信（WCDMA、cdma2000 等）、测距导航、目标探测、密码学等领域都有广泛的应用[1]。伪随机序列分为线性和非线性序列，m 序列是目前序列研究中最为完备、使用最为广泛的一种线性序列。m 序列生成多项式是其重要参数，是完成序列恢复、扩频码捕获、信息解密、流密码攻击等后续课题的基础。因此，如何在接收序列有限和误码条件下，正确估计序列生成多项式具有重要意义，多项式估计已成为序列分析中的重要研究领域。

国内外相关文献对此问题进行了探讨。文献[2]提出了经典的 BM 算法，该算法是一种迭代算法，迭代多项式阶数的 2 倍次即能估计出多项式系数，

收稿日期：2011-11-28；修回日期：2012-06-13
基金项目：国家自然科学基金资助项目(61171108)
Foundation Item: The National Natural Science Foundation of China (6117 108)

算法效率高运算速度快，但容错性能差，不能适应误码情况。文献[3~5]提出了欧几里德算法、连分式算法和格基约化算法等高效算法，这类算法与 BM 算法为等价关系，均有运算速度快、容错性能差的特点。文献[6]提出了有限域变换的方法，通过寻找多项式有限域上根的分布进行多项式估计，但该方法仅适用于低阶多项式，且抗误码能力不足。文献[7]运用 Walsh 变换法估计多项式，是一类快速解方程算法，但该方法受制于多项式抽头的个数，容错能力有限。文献[8]提出高阶统计测定算法，并利用概率分析方法精确估计，该类方法利用了 m 序列良好的自相关性，具有一定的抗误码能力，但其运算复杂度较高，估计高阶多项式时精度较差。文献[9,10]运用 m 序列与 BCH 码、卷积码的内在关系，对接收序列译码后进行估计，具有较强的抗误码能力，但其运算复杂度很高，不适用于高阶多项式估计。综上所述，现有的 PN 序列估计算法仍然存在估计多项式抽头数受限、估计高阶多项式时复杂度较高、容错能力有限等问题。

针对上述问题，本文针对误码条件下的高阶多项式估计问题进行研究，提出了一种基于可信度累积的序列本原多项式估计算法。首先分析了 BM 算法的本质，其利用 m 序列线性约束关系进行迭代，算法内部均在 GF(2)上进行，估计效率高；但是，其不能适应误码。为提高容错性能，本文算法利用序列软信息进行估计。本文结合 Chase 算法思想，以 BM 算法为基础算法，将序列软信息映射成序列可信度，在 BM 算法外部构造序列可信度集合和对应的估计多项式可信度集合，通过可信度累积的方式得到最大可信度估计多项式集合。为提高可信度累积速度，利用 GF(2)上本原多项式约束准则，剔除错误多项式，缩小多项式累积规模。算法不受多项式抽头数制约，估计效率高，可以完成一定误码条件下高阶多项式估计。仿真结果表明，本算法性能不受制于多项式抽头个数，在误码率为 18%的条件下仍能够较好地完成 17 阶 m 序列多项式估计。

2 问题描述

2.1 多项式估计难点

m 序列由多个移位寄存器移位相加产生，其生成原理如图 1 所示。系数为 $c=(c_1,c_2,\mathrm{L},c_l)$ 的 l 阶移位寄存器生成多项式为 $g(x)=c_lx^l+c_{l-1}x^{l-1}+\cdots+c_1x+1$。$g(x)$ 为 GF(2)上本原多项式，与移存器初态共同决定 PN 序列 a。序列 a 经过二元对称信道 BSC，以错误转移概率 p 得到含错序列 r，数学模型如图 2 所示。序列多项式估计问题即根据 r 估计出生成多项式 $g(x)$ 的系数 c。

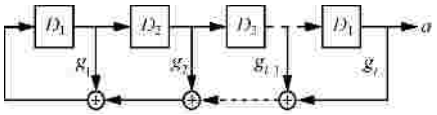

图 1 伪随机序列产生原理

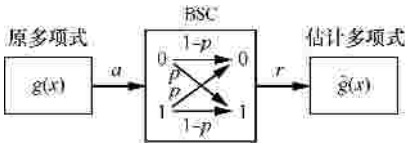

图 2 多项式估计模型

由 m 序列产生原理可知，序列 a_i，$i=1,2,\cdots,n$ 满足关系：$a_n=\sum_{i=1}^{l}c_ia_{n-i}$ 写成线性方程组的形式为

$$\begin{pmatrix} a_0 & a_1 & \mathrm{L} & a_{l-1} & a_l \\ a_1 & a_2 & \mathrm{L} & a_l & a_{l+1} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} & \mathrm{M} \\ a_l & a_{l+1} & \mathrm{L} & a_{2l-1} & a_{2l} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} & \mathrm{M} \end{pmatrix}\cdot\begin{pmatrix} c_l \\ c_{l-1} \\ \mathrm{M} \\ c_1 \\ 1 \end{pmatrix}=0 \tag{1}$$

将序列 r 代入式（1），可得到接收序列与系数之间的线性方程组表达式为

$$\begin{pmatrix} r_0 & r_1 & \mathrm{L} & r_{l-1} & r_l \\ r_1 & r_2 & \mathrm{L} & r_l & r_{l+1} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} & \mathrm{M} \\ r_l & r_{l+1} & \mathrm{L} & r_{2l-1} & r_{2l} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} & \mathrm{M} \end{pmatrix}\cdot\begin{pmatrix} c_l \\ c_{l-1} \\ \mathrm{M} \\ c_1 \\ 1 \end{pmatrix}=\begin{pmatrix} d_0 \\ d_1 \\ \mathrm{M} \\ d_l \\ \mathrm{M} \end{pmatrix} \tag{2}$$

其中，接收序列矩阵用 $\boldsymbol{R}$ 表示，误码引起的误差向量表示为 d。

因此，多项式估计问题可描述为：已知含错序列矩阵 $\boldsymbol{R}$，求 GF(2)上最优向量 c，使得 d 与 0 之间的欧式距离最小。

显然，向量 d 与 0 向量距离越远，多项式系数估计难度越大。由式(2)可知，d 与 2 个因素有关：错误转移概率 p 和多项式阶数 l。p 越大，接收序列误码率越高，累积错误越多，d 越大；l 越大，序列约束关系越强，d 随接收序列错误抖动程度越大，d 与 0 的距离也越远。因此，在高阶高误码条件下，多项式估计难度较大。

2.2　BM 算法的问题

针对高阶误码情况下的多项式估计问题，目前算法均从解方程或者相关运算的角度来提高抗误码性能和估计多项式的阶数，但算法的计算复杂度均较高，且估计高阶多项式时精度较差。本文拟利用 BM 迭代算法[2]高效、运算速度快和存储空间小的优点，进行高误码条件下的高阶多项式估计。但是，BM 算法的容错性较差，该算法均在 GF(2)上进行，依赖于迭代差值 d_n 的正确性

$$d_n = c_0^{(n)} a_n + c_1^{(n)} a_{n-1} + \cdots + c_{l_n}^{(n)} a_{n-l_n} \tag{3}$$

当每一步差值完全正确时，迭代至 l_N 即可正确估计多项式系数。若其中第 n 步差值 d_n 发生错误，则后续迭代多项式均错误。定理 1 给出了接收序列长度 N 与 l_N 的关系。

定理 1[2]　对于给定的 N 长二元序列 r，假定产生 r 的最短移位寄存器的级数为 l_N，则产生 r 的最短移位寄存器唯一，其充分必要条件是 $l_N \le N/2$。

根据定理 1，估计一个 N 级多项式，仅需要 $2N$ 长度的序列。为保证迭代差值 d 完全正确，需要 $2N$ 长度的连续无错序列。即 BM 算法正确估计一个 $2N$ 级多项式，最少需要 $2N$ 长度的连续无错二元序列。

由以上分析可知，BM 算法的高效估计性能依赖于连续 $2N$ 长度个二元序列无错，这是其容错性能较差的本质问题。为了提高其容错性能，本文利用序列软信息构建估计系数的可信度，通过可信度累积完成多项式估计。

3　基于可信度累积的多项式估计算法及算法优化

序列可信度可描述为接收序列与发送序列的欧式距离，可信度较低的序列发生错误的可能性较大。Chase 算法[11,12]是基于可信度进行容错处理的一种有效算法，其性能接近最大似然译码算法。算法基本思想是对可信度低的序列段进行翻转处理，遍历可信度低序列位置。根据不同试探序列集合可分为 Chase1、Chase2、Chase3 等 3 种方案，最多可以纠正 $(d_{\min}-1)/2$ 个错误[11]。下面应用一种改进型 Chase 算法，在 BM 算法外部建立序列可信度和多项式可信度信息，通过可信度累积完成估计。

3.1　基于可信度累积的多项式估计算法

设发送二元序列 $a_0, a_1, \cdots, a_{n-1}$，$a_i \in (0,1)$，接收端解调器输出序列 $r_0, r_1, \cdots, r_{n-1}$。软判决区间为 $[e_1, e_2]$。给定单个接收序列 r_i，设其初判值 $\hat{r}_i$，可信度为 $p(r_i)$。运用一次试探判决序列估计多项式系数为 $\vec{c}$，系数可信度为 $f(\vec{c})$。

定义 1　序列初判值 $\hat{r}_i$。根据欧氏距离准则，若 $d(r_i,0) > d(r_i,1)$，则 $\hat{r}_i$ 为 0，反之成立。判决表达式如式(4)所示。

$$\hat{r}_i = \begin{cases} 1, & r_i \ge \dfrac{e_2 - e_1}{2} \\ 0, & r_i < \dfrac{e_2 - e_1}{2} \end{cases} \tag{4}$$

定义 2　序列可信度函数 $p(r_i)$。给定任意接收序列 r_i，当其在判决区间外时，表明其离 1 或者 0 的距离比较近，可信度较高；当在判决区间内时，根据欧氏准则确定其可信度。表达式如式(5)所示。

$$p(r_i) = \begin{cases} 1, r_i \notin [e_1, e_2] \\ \max\left(\dfrac{r_i - e_1}{2(e_2 - e_1)}, 1 - \dfrac{r_i - e_1}{2(e_2 - e_1)} \right), r_i \in [e_1, e_2] \end{cases} \tag{5}$$

定义 3　估计多项式可信度函数 $f(\vec{c})$。设一次试探判决序列为 $r_0', r_1', \cdots, r_{n-1}'$，其对应可信度分别为 $p(r_0'), p(r_1'), \cdots, p(r_{n-1}')$，定义其多项式估计系数可信度

$$f(\vec{c}) = \prod_{i=0}^{n-1} p(r_i') \tag{6}$$

设 k 次试探得到系数可信度集合 $\{f(\vec{c}_0), f(\vec{c}_2), \cdots, f(\vec{c}_{k-1})\}$，对其中一种估计多项式系数 $\vec{c}$，其可信度累积表达式为

$$j(\vec{c}) = \sum_{i=0}^{k-1} f(\vec{c} = \vec{c}_i) \tag{7}$$

算法步骤如下。

1) 接收序列分组。根据 2.2 节分析，通过接收序列游程粗估计序列多项式级数为 N，通常 N 值大于实际多项式级数。将接收序列 $\vec{r}$ 按照连续 $2N$ 长度分组，每组间隔长度 $l \le 2N$，间隔越短分组越多，估计越精确，运算量随之增大。设分成 m 组 $2N$ 长度序列 $\{\vec{r}_0, \vec{r}_1, \cdots, \vec{r}_{m-1}\}$，分别对每组数据进行估计。

2) 对一组 $2N$ 长度序列 $r_0, r_1, \cdots, r_{2N-1}$，设定判决区间，确定序列可信度 $\vec{p}$。设判决区间为 $[e_1, e_2]$，根据式(4)、式(5)确定初判序列 $r'_0, r'_1, \cdots, r'_{2N-1}$，计

算对应的可信度 $p(r'_0), p(r'_1), \cdots, p(r'_{2N-1})$。

3) 确定序列试探集合 R' 及对应的可信度集合 P。对 $r'_0, r'_1, \cdots, r'_{2N-1}$ 中可信度小于 1 位置进行排序，取其中可信度最小的前 d 个序列进行遍历翻转，即 $0 \to 1$，$1 \to 0$，对应的可信度修改为 $1-p(r'_i)$。试探序列集合和可信度集合大小为 $k = 2^d$。

4) 遍历 k 个长度为 $2N$ 的试探序列，进入 BM 算法迭代运算，得到 k 组多项式估计系数，根据式(6)计算对应的 k 个系数可信度。

5) 计算 m 组序列的多项式估计系数和对应可信度，共 mk 组多项式估计系数和 mk 个系数可信度。根据式(7)进行可信度累加，按可信度由大到小排序得到累加可信度系数向量集合 $\{c_0, c_1, \cdots\}$。

6) 估计多项式校验。取累加可信度集合中前 L 项多项式系数向量集合：$C = \{c_0, c_1, \cdots, c_{L-1}\}$，分别代入到原接收序列 r 中，按照多项式系数约束关系进行逐比特校验，错误率最少的 c_i 即估计多项式系数。

算法的本质是对进入 BM 算法的二元序列建立对应的可信度，利用序列可信度得到 BM 算法估计多项式系数的可信度，从而在 BM 算法外部建立可信度的软信息。通过对可信度较低序列的遍历修正，利用 BM 算法高效估计的同时，提高其容错性能。通过多项式可信度累积，最大可能地估计出准确的多项式系数。

3.2 算法优化

算法完成可信度累积进行了 mk 次 BM 迭代运算，mk 分别由累积次数和试探集合大小决定。mk 越大，迭代出的多项式越多，进行分类累积规模越大。由于算法基于可信度累积大小进行判断，理想情况是可信度累积个数 mk 较多，同时出现的多项式系数种类较少，即多项式可信度累积较集中，这样估计多项式正确率更高。因此，在 mk 一定的条件下，需要缩小多项式累积规模，提升累积速度。

当序列出现错误时，估计的多项式为错误的本原多项式或非本原多项式。因此，可以利用 GF(2) 上不可约多项式和本原多项式系数特性[13~15]将非本原多项式剔除。这里给出几项可约多项式判定方法，快速将可约多项式去除。

引理 1[14] 设 $g(x) = \sum_{i=0}^{l} c_i x^i$ 是 GF(2)上 l 次多项式，其中，$c_i \in (0,1)$，$c_0 = c_l = 1$，若满足下述任意条件，则该多项式为可约多项式。

① $\sum_{i=0}^{l} c_i \bmod 2 = 0$；

② $\forall c_i$，$c_i = 1$ 时 $i \bmod 2 = 0$；

③ 令 $Z_0 = \{i; c_i = 1, i \bmod 3 = 0\}$，$Z_1 = \{i;\ c_i = 1, i \bmod 3 = 1\}$，$Z_2 = \{i; c_i = 1, i \bmod 3 = 2\}$，$Q_0 = \sum_{i \in Z_0} c_i$，$Q_1 = \sum_{i \in Z_1} c_i$，$Q_2 = \sum_{i \in Z_2} c_i$，则有 $Q_0 \bmod 2 = 0$，$Q_1 \bmod 2 = 1$，$Q_1 = Q_2$；

④ 如果 $g(x+1)$ 可约，那么 $g(x)$ 也可约；

⑤ 如果 $x^l g(\frac{1}{x})$ 可约，则 $g(x)$ 也可约。

利用准则①，即可将估计多项式规模减少一半，准则②~⑤均可剔除一定数量错误多项式。

另外，本算法对区间 $[e_1, e_2]$ 以内可信度最低的 d 个序列进行翻转修正，实际上是对错误可能性较大的序列进行 0，1 遍历，$[e_1, e_2]$ 外的 $2N-d$ 个序列，则认为其完全正确。在实际中，$2N-d$ 个序列可能出现个别错误。因此，可对 $2N-d$ 个序列进行 C_{2N-d}^{1} 次翻转，提高准确性。同时，可根据信道环境，灵活选择修正序列长度，信道环境差时修正序列长度增大，信道环境好时修正序列长度缩小，以运算量来换取容错性能的提升。

综上所述，本算法流程如图 3 所示。

4 算法仿真及性能分析

使用 Matlab 软件，以 m 序列为例，分析本算法多项式估计性能。仿真环境如下，在 AWGN 条件下，采用序列生成多项式。

多项式 1：

$$g_1(x) = 1 + x^3 + x^5 + x^7 + x^8 \tag{8}$$

多项式 2：

$$g_2(x) = 1 + x^3 + x^{10} \tag{9}$$

多项式 3：

$$g_3(x) = 1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^9 + x^{10} \tag{10}$$

多项式 4：

$$g_4(x) = 1 + x + x^3 + x^7 + x^{12} + x^{16} + x^{17} \tag{11}$$

按照‘0’→‘1’,‘1’→‘-1’映射，发送序列取值 $a_i \in \{-1, 1\}$，接收序列 $r(i) = a(i) + n_i$，其中，n_i 表示加性高斯噪声。接收序列为截短序列。

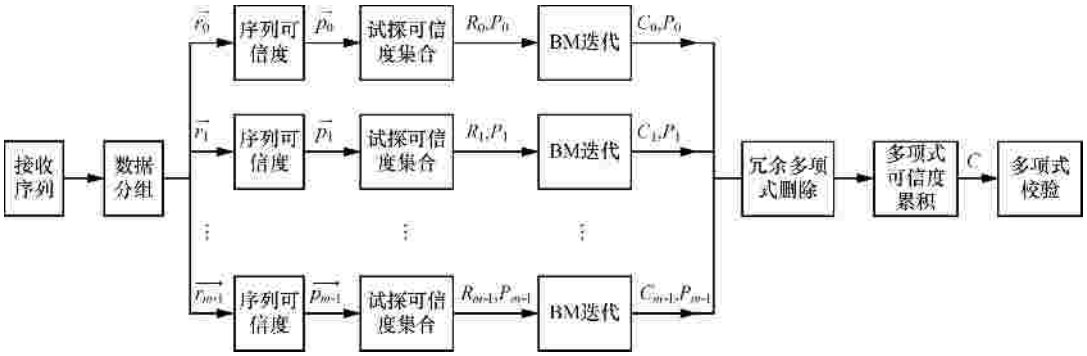

图 3　可信度累积估计算法流程

4.1　实例计算

以多项式一为本原多项式，误码率为 0.2，产生含错 m 序列。该序列多项式阶数为 8，在观察接收序列游程基础上，估计本原多项式阶数为 10。将接收序列进行分组，每组长度为 20，取 200 组这样的数据进行估计。判决区间设为[0.2,0.8]，试探集合大小为 4，用 BM 算法进行估计，得到估计多项式结合和对应可信度，按照相应准则剔除错误多项式。将 200 组数据全部估计完后，进行可信度累加，按可信度大小取前 10 项多项式系数。如表 1 所示，多项式系数 651 对应的累积可信度大大超过其他错误多项式。

表 1　　估计多项式可信度

序号	估计多项式 $g'(x)$	累积可信度
1	651	6.868 4
2	515	1.469 0
3	435	1.316 9
4	711	1.185 9
5	433	1.105 2
6	551	1.077 5
7	675	0.985 3
8	777	0.938 7
9	543	0.937 9
10	643	0.925 1

(表中多项式用八进制表示)

4.2　计算复杂度

多项式估计常用 Walsh 转换法，其计算复杂度为 $O((l+1)\times 2^{(l+1)})$，BM 算法的计算复杂度为 $O(l^2)$。本算法运用基本的 BM 算法，结合 Chase 改进型算法实现可信度叠加，进行了多次 BM 迭代运算。设一组数据试探集合大小为 k，进行了 m 组数据估计，则计算复杂度为 $O(m\times k\times l^2)$。因此，本算法计算复杂度与试探集合大小、累积次数、多项式阶数的平方等 3 个参数呈线性递增关系。当 m 和 k 不是足够大时，本算法计算复杂度将明显小于 Walsh 变换法。

4.3　算法成功率

Walsh 变换法估计成功率与多项式抽头系数有关，抽头系数越多，估计成功率越低。为考察本算法性能，分别以多项式 2(2 抽头)和多项式 2(8 抽头)为生成多项式，在不同误码率的条件下进行仿真。图 4 给出了本算法与 Walsh 算法不同抽头数条件下容错性能对比曲线。接收序列长度为 200，试探集合大小为 4，累积次数为 30，算法成功率为随机实验 1000 次得到的估计值。此时，Walsh 算法计算复杂度为 $O(11\times 2^{11})$，本算法计算复杂度为 $O(30\times 4\times 10^2)$，本算法计算复杂度较 Walsh 算法降低一半。从图 4 可以看出，生成多项式抽头数为 2 时，Walsh 算法和本算法容错性能相当，当生成多项式抽头数为 8 时，Walsh 算法容错性能急剧降低，而本算法容错性能基本不变。即在相同误码条件下，抽头系数较小时，本算法与 Walsh 算法估计成功率相当，抽头数较大时，本算法较 Walsh 算法估计成功率有较大提高。

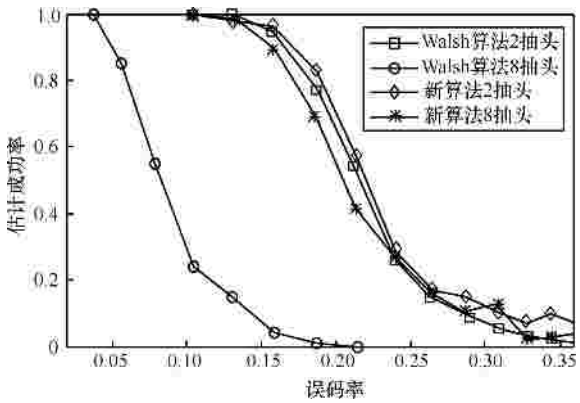

图 4　不同抽头数多项式算法容错性能对比

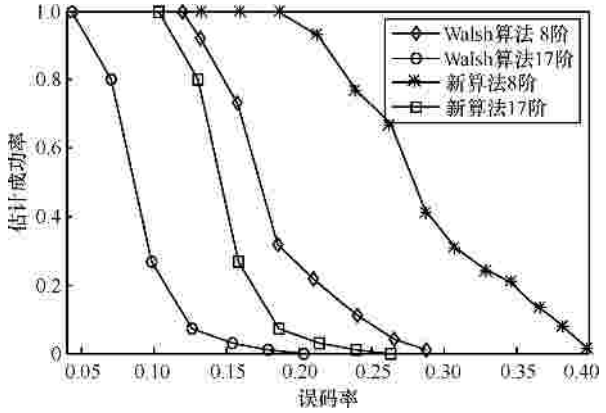

图 5 不同阶多项式算法容错性能对比

多项式估计算法性能与多项式阶数密切相关，阶数越高，估计越困难。为考察本算法针对不同阶多项式估计性能，分别以多项式 1(8 阶)、多项式 4(17 阶)作为序列生成多项式进行仿真，图 4 给出了本算法和 Walsh 算法不同阶多项式条件下容错性能对比曲线。算法成功率为随机实验 1 000 次得到的估计值。8 阶条件下，接收列长度为 100，试探集合大小为 4，累积次数为 20。此时，Walsh 算法计算复杂度为 $O(9\times 2^9)$，本算法计算复杂度为 $O(20\times 4\times 8^2)$，2 个算法计算复杂度相当。17 阶条件下，接收列长度为 3 500，试探集合大小为 8，累积次数为 200。Walsh 算法计算复杂度为 $O(18\times 2^{18})$，本算法计算复杂度为 $O(200\times 8\times 17^2)$，本算法计算复杂度约为 Walsh 算法的 10%。从图 5 中可以看出，在计算复杂度小于 Walsh 算法情况下，由于抽头数原因，对不同阶多项式，本算法容错性能较 Walsh 算法均有提高。另外，本算法计算复杂度随多项式阶数的提高而增大，而容错性能却随着多项式阶数的提高而降低，8 阶多项式能适应 20%的误码率，17 阶多项式能适应 12%的误码率，原因是多项式阶数越高，估计时需要连续正确的序列个数越多，提升容错性能所付出的计算量代价也越大。

本算法建立在可信度累积之上，可信度累积规模与试探空间大小和累积次数相关。为分析这 2 个因素对容错性能影响，以多项式 4 为生成多项式进行仿真。图 6 给出了不同试探空间大小条件下算法容错性能对比曲线，算法成功率为随机实验 1000 次得到的估计值。试探空间大小分别为 4、8 和 16，累积次数为 200 次，对应计算法复杂度分别为 $O(200\times 4\times 17^2)$、$O(200\times 8\times 17^2)$ 和 $O(200\times 16\times 17^2)$。图 7 给出了不同累积次数条件下算法容错性能对比曲线，算法成功率为随机实验 1 000 次得到的估计值。累积次数分别为 100、500、1 000，试探空间大小为 16，对应计算法复杂度分别为 $O(100\times 16\times 17^2)$、$O(500\times 16\times 17^2)$ 和 $O(1\ 000\times 16\times 17^2)$。从图 6、图 7 可以看出，试探空间越大，累积次数越多，计算复杂度越高，算法容错性能越好。累积次数的提高对算法成功率提高显著，原因是累积次数越多，正确多项式可信度优势越明显，累积 1 000 次时能适应约 18%的误码率。

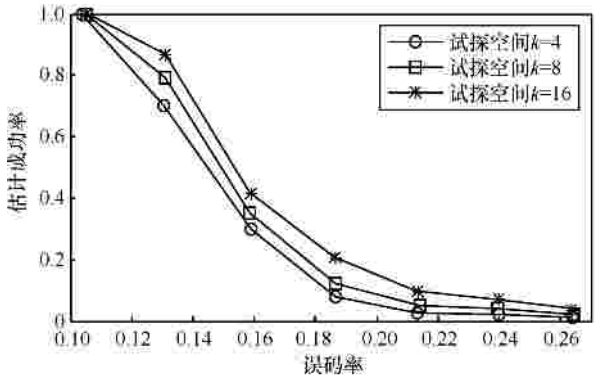

图 6 不同试探空间容错性能对比

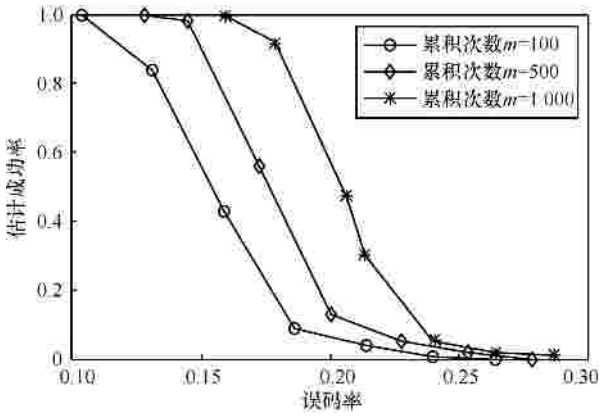

图 7 不同累积次数容错性能对比

5 结束语

本文通过分析 BM 算法缺陷，利用序列软信息，将 BM 算法和 Chase 改进型算法有效结合，在 BM 算法外部建立序列可信度及其对应的估计多项式可信度，通过多项式可信度累积实现估计。为加快可信度累积速度，利用本原多项式判决准则减小多项式累积规模。通过分析和仿真，本算法能够较好解决误码条件下高阶多项式估计问题。相比实际中常用的 Walsh 变换法，算法性能不受多项式抽头数影响，估计效率较高且具有一定的容错能力，能够

适应 18%误码率条件下 17 阶多项式估计。算法不足之处是随着估计多项式阶数的增大，计算复杂度增大较快且容错性能提高有限。

参考文献：

[1] **田日才**. **扩频通信**[M]. **北京:清华大学出版社**, 2007.1-29,67-73.
TIAN R C. Spread Spectrum Communication[M]. Beijing: Tsinghua University Press, 2007. 1-29, 67-73.

[2] MASSEY J L. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15:122-127.

[3] HEYDTMANN A E, 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): 2614-2622.

[4] YIN Q, YUAN Z Y, GUO P. Further studies on the distribution of the shortest linear recurring sequences for the stream cipher over the ring[A]. Proceedings of 2007 International Conference on Intelligent Computing[C]. Berlin Heidelberg, German, 2007.680-688.

[5] WANG L P, ZHU Y F, PEI D Y. On the lattice basis reduction multi-sequence synthesis algorithm[J]. IEEE Transactions on Information Theory, 2004, 50(11): 2905-2910.

[6] WANG F H, HUANG Z T, ZHOU Y Y. A new method for m-sequence and gold-sequence generator polynomial estimation[A]. Proceedings of IEEE International Symposium on Microwave Antenna, Propagation and EMC Technologies for Wireless Communication[C]. Hangzhou, China, 2007.1039-1044.

[7] YOU L, ZHU Z L. The application of Walsh function in resolving of F(2) equations[J]. Signal Processing(Chinese), 2000, 16: 27-30.

[8] **苏绍璟**, **伍文君**. **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 S J, WU W J. Blind identification of the primitive polynomial m-sequence with error using high-order statistic[J]. Acta Armamentarii, 2010, 31(12):1593-1598.

[9] **柴先明**, **魏跃敏**. **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): 305-308.
CHAI X M, WEI Y M. A method for reconstruction of m sequence based on the equivalence with BCH codes[J]. Journal of Electronics & Information Technology, 2011, 33(2): 305-308.

[10] **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 S Q, QI L, WANG Y. A new blind recognition method of pesudo-randomizer code sequence[J]. Journal of Circuits and Systems, 2011, 16(4): 6-12.

[11] **张卫**, **陈亦卉**. **基于 MSF 的低复杂度 Chase 型 RS 码软判决译码算法**[J].**重庆大学学报(自然科学版)**, 2011, 23(2): 172-177.
ZHANG W, CHEN Y H. A new blind recognition method of pesudo-randomizer code sequence[J]. Journal of Chongqing University of Posts and Telecommunications, 2011, 23(2): 172-177.

[12] **齐佩汉**. RS **码软判决译码算法研究及其** SOPC **技术实现**[D]. **西安：西安电子科技大学**, 2011.
QI P H. Research on Soft-decision Decoding Algorithms of RS Codes and Its Implementation in SOPC Technology[D]. Xi'an: Xidian University, 2011.

[13] NINA D, LI C. LDPC Encoding based on the primitive polynomial[A]. Proceedings of 2007 International Conference on Wireless Communication Networking and Mobile Computing(WiCOM)[C]. Chongqing, China, 2010.1-2.

[14] **王鑫**, **王新梅**, **韦宝典**.**判定有限域上不可约多项式及本原多项式的一种高效算法**[J]. **中山大学学报**, 2009, 48(1): 6-9.
WANG X, WANG X M, WEI B D. An efficient and deterministic algorithm to determine irreducible and primitive polynomials over finite fields[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2009, 48(1): 6-9.

[15] CAO H, CHEN G L. Test of irreducible polynomials based on primality-test[J]. Information Security and Communications Privacy, 2006, 3:73-74.

作者简介：

陈松（1983-），男，湖北武汉人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为无线移动通信、通信信号处理等。

黄开枝（1973-），女，安徽滁州人，博士，国家数字交换系统工程技术研究中心副教授、硕士生导师，主要研究方向为无线移动通信、通信信号处理、物理层安全等。

赵华（1978-），女，陕西西安人，硕士，国家数字交换系统工程技术研究中心讲师，主要研究方向为无线移动通信、物理层安全等。