

## 一种基于与 BCH 码等价原理的 $m$ 序列重构算法

柴先明<sup>\*①</sup> 魏跃敏<sup>①</sup> 师栋锋<sup>①</sup> 蔡凯<sup>①</sup> 黄知涛<sup>②</sup>

<sup>①</sup>(北京遥感信息研究所 北京 100192)

<sup>②</sup>(国防科技大学电子科学与工程学院 长沙 410073)

**摘要:** 该文针对现有  $m$  序列特征多项式估计方法在高阶高误码条件下的估计效率不高, 精度不够的问题展开研究, 通过分析  $m$  序列和 BCH 码的生成原理, 得出二者之间的等价关系, 进而提出了一种新的  $m$  序列特征多项式的估计算法。该算法通过构造与之等价的 BCH 码, 利用其良好的纠错性能, 实现高误码条件下的  $m$  序列特征多项式的估计, 仿真结果表明本算法能较好地解决误码条件下的  $m$  序列特征多项式估计问题, 运算速度主要适用于通信信号处理中常用 20 阶以内的  $m$  序列分析问题。

**关键词:** 信号处理;  $m$  序列; 特征多项式; BCH 码; 等价

中图分类号: TN911.2

文献标识码: A

文章编号: 1009-5896(2011)02-0304-05

DOI: 10.3724/SP.J.1146.2010.00028

## A Method for Reconstruction of $m$ Sequence Based on the Equivalence with BCH Codes

Chai Xian-ming<sup>①</sup> Wei Yue-min<sup>①</sup> Shi Dong-feng<sup>①</sup> Cai Kai<sup>①</sup> Huang Zhi-tao<sup>②</sup>

<sup>①</sup>(Beijing Institute of Remote Sensing Information, Beijing 100192, China)

<sup>②</sup>(Department of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

**Abstract:** The issue of insufficient efficiency and accuracy of current estimation methods for characteristic polynomial of  $m$  sequence under high error conditions is studied. A equivalent relationship between  $m$  sequence and BCH codes is derived by studying their generation principles, and then a new estimation algorithm for characteristic polynomial of  $m$  sequence is proposed in the paper. By constructing equivalent BCH codes, characteristic polynomial of  $m$  sequence is estimated using their good error-correction performance under high error conditions. Simulation results show that the algorithm can solve the estimation for characteristic polynomial of  $m$  sequence under error conditions, operation speed of the algorithm can mainly be accepted for analysis of  $m$  sequence lower than 20-order in signal processing.

**Key words:** Signal processing;  $m$  sequence; Characteristic polynomial; BCH codes; Equivalence

### 1 引言

伪随机噪声(PN)序列在扩频通信、伪码加扰、伪码测距以及密码学等领域<sup>[1]</sup>都有着广泛的应用。 $m$  序列即最大长度线性反馈移位寄存器序列, 是目前序列研究中理论最完备、应用最广泛的一种 PN 序列, 并且它是研究和构造其他 PN 序列的基础<sup>[2]</sup>。例如在扩频通信中的扩频码大多采用  $m$  序列, Gold 序列等 PN 序列。 $m$  序列的特征多项式是它的重要参数, 是完成扩频序列恢复、信息解密等工作的基础。 $m$  序列的特征多项式估计是序列分析中的重要研究问题<sup>[3]</sup>。

目前, 针对  $m$  序列的特征多项式估计问题的研究方法主要有 BM 算法<sup>[4]</sup>、欧几里德算法<sup>[5]</sup>、格基约化算法<sup>[6]</sup>、基于高阶累积量的方法<sup>[7]</sup>和有限域傅里叶变换方法<sup>[8]</sup>等, 其中, BM 算法、欧几里德算法和格

基约化算法效率很高, 算法执行所需时间的增长率与  $N^2$  的增长率成正比, 其中  $N$  表示  $m$  序列的阶数, 但是这类算法不能适应存在误码的情况; 当 PN 序列周期为  $2^l - 1$  时, 基于有限域傅里叶变换的方法比上述方法进一步降低了计算量, 但不足之处仍是缺乏误码适应能力<sup>[8]</sup>; 基于高阶累积量的方法利用了  $m$  序列尖锐的自相关特性, 尽管能够适应一定的误码, 但是算法计算量随着  $m$  序列阶数的增加急剧增大, 当误码率升高时, 估计精度较差。总的来说现有的  $m$  序列特征多项式估计方法在高阶高误码条件下的估计算法效率不高, 精度不够。

本文主要对  $m$  序列在高误码率条件下的特征多项式估计问题进行研究。 $m$  序列是由线性递归关系式为本原多项式的线性移位寄存器产生的最大周期序列。根据  $m$  序列的生成原理可知,  $m$  序列的产生过程和二进制 BCH 码<sup>[9]</sup>的编码过程相似, 两者均是基于本原多项式在二元域上作乘法运算得到的。经分析得出两者之间的等价关系, 又因为 BCH 码具有

2010-01-12 收到, 2010-10-27 改回

\*通信作者: 柴先明 clewant110@163.com

很强的纠错能力,所以利用该等价原理,可以完成对高误码条件下 m 序列的特征多项式估计。

## 2 BCH 码和 m 序列的构造特征

m 序列是最大长度的线性反馈移存器序列,线性反馈移存器的组成如图 1 所示。

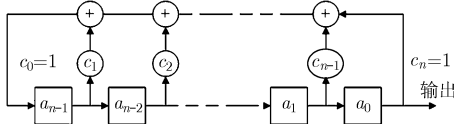


图 1 线性反馈移存器序列的生成原理图

其中  $a_n, n = 0, 1, 2, \dots$  为产生的序列,移位寄存器左端新得到的输入  $a_n$ ,按图中线路连接关系,可以写为

$$a_n = c_1 a_{n-1} \oplus c_2 a_{n-2} \oplus \dots \oplus c_{n-1} a_1 \oplus c_n a_0 = \sum_{i=1}^n c_i a_{n-i} \quad (1)$$

其中  $c_i$  的取值决定了移位寄存器的反馈连接和序列的结构,用式(2)表示。

$$p(X) = c_0 + c_1 X + \dots + c_{L-1} X^{L-1} + c_L X^L \quad (2)$$

式(2)称为特征多项式。特征多项式的结构就决定了所产生的线性移存器的特性,当其为本原多项式时能够产生最大周期的序列即 m 序列。

BCH 码是由分组码发展而来,是循环码的一个重要子类,在短码编码时具有良好的纠错性能。 $(n, k)$  BCH 码的编码过程可简要表示为<sup>[9]</sup>

$$v(X) = u(X)g(X) \quad (3)$$

其中  $v(X)$  是码字多项式,  $u(X) = (u_0 + u_1 X + L + u_{k-1} X^{k-1})$  为信息序列多项式,其系数  $u_0, u_1, \dots, u_{k-1}$  为  $k$  个待编码的信息位,  $g(X) = g_0 + g_1 X + L + g_{n-k-1} X^{n-k-1} + X^{n-k}$  是生成多项式。

BCH 码的生成多项式  $g(X)$  由它在伽罗华域<sup>[9]</sup>  $GF(2^m)$  上的根确定,而伽罗华域  $GF(2^m)$  由生成该域的本原多项式  $p'(X)$  确定。若令  $\alpha$  为  $GF(2^m)$  上的本原元,则码长为  $n = 2^m - 1$ 、纠正  $t$  个错误的 BCH 码的生成多项式  $g(X)$  就是二元域  $GF(2)$  上以

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t} \quad (4)$$

为根的最低次数多项式<sup>[10]</sup>。

令  $\phi_i(X)$  为  $\alpha^i$  的最小多项式,根据伽罗华域的构造过程和性质,有  $p(X) = \phi_1(X)$ 。同时  $g(X)$  必为  $\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)$  的最小公倍式<sup>[11]</sup>,即

$$g(X) = \text{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)\} \quad (5)$$

## 3 基于 m 序列与 BCH 码等价变换的特征多项式估计算法

### 3.1 m 序列与 BCH 码等价关系分析

假设  $L$  阶 m 序列的特征多项式为  $p(X) = c_0 +$

$c_1 X + \dots + c_{L-1} X^{L-1} + c_L X^L$ , 生成的 m 序列为  $\mathbf{A}_\infty(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_{2^L-2} X^{2^L-2} + \dots$ , 则满足定理<sup>[2]</sup>:

$$p(X)\mathbf{A}_\infty(X) = h(X) \quad (6)$$

$$\mathbf{A}_n(X) = \frac{h(X)(1 + X^P)}{p(X)} \quad (7)$$

其中  $h(X) = \sum_{i=1}^n c_i X^i (a_{-i} X^{-i} + a_{-(i-1)} X^{-(i-1)} + \dots + a_{-1} X^{-1})$ ,  $P = 2^L - 1$ ,  $h(X)$  仅取决于移存器的初始状态  $(a_{-i} \dots a_{-1})$ ,  $\mathbf{A}_n(X)$  为一个完整周期的 m 序列。

多项式  $1 + X^P$  在伽罗华域  $GF(2^L)$  的所有根对应了该域的所有非零元素  $\alpha^i, i = 0, 1, \dots, 2^L - 2$ 。若对  $1 + X^P$  在  $GF(2)$  上进行因式分解,由伽罗华域的性质可知道,  $1 + X^P$  的因式中包含了  $L$  阶所有本原多项式,由于特征多项式  $p(X)$  是一个  $L$  阶的本原多项式,所以它必定是  $1 + X^P$  的一个多项式因子。

由伽罗华域的性质<sup>[9]</sup>可知多项式  $1 + X^P$  可以表示为

$$1 + X^P = \text{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2^L-2}(X)\} \quad (8)$$

其中  $\phi_i(X)$  为  $\alpha^i$  的最小多项式。

不妨将  $1 + X^P$  表示为

$$1 + X^P = \text{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)\} \cdot \text{LCM}\{\phi_{2t+1}(X), \phi_{2t+2}(X), \dots, \phi_{2^L-2}(X)\} = g(X)a(X) \quad (9)$$

其中  $g(X) = \text{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)\}$ ,  $a(X) = \text{LCM}\{\phi_{2t+1}(X), \phi_{2t+2}(X), \dots, \phi_{2^L-2}(X)\}$ 。

假若  $p(X) \in \{\phi_{2t+1}(X), \phi_{2t+2}(X), \dots, \phi_{2^L-2}(X)\}$ , 则可对式(7)作如下变换:

$$\begin{aligned} \mathbf{A}_n(X) &= \frac{h(X)(1 + X^P)}{p(X)} = \left[ h(X) \frac{a(X)}{p(X)} \right] g(X) \\ &= [h(X)a'(X)]g(X) = b(X)g(X) \end{aligned} \quad (10)$$

此时 m 序列  $\mathbf{A}_n(X)$  可以看作是分组长度  $n = 2^L - 1$ , 生成多项式为  $g(X)$ , 纠正  $t$  个错误的二进制 BCH 码。利用 BCH 码的译码原理<sup>[12]</sup>, 在可纠正的错误范围内,可以完成对 m 序列的纠错,从而得到无误码的 m 序列,进而可利用 BM 等方法完成对该序列特征多项式的估计。

通过上述分析,可以发现, m 序列  $p_n(X)$  能否与二进制 BCH 码等价,关键在于

$$p(X) \in \{\phi_{2t+1}(X), \phi_{2t+2}(X), \dots, \phi_{2^L-2}(X)\} \quad (11)$$

是否成立。式(11)是否成立又取决于生成二进制 BCH 码的本原多项式  $p'(X)$  与 m 序列的特征多项式  $p(X)$  在伽罗华域  $GF(2^L)$  上的根元素对应关系。经过分析总结得到如下结论。

(1)当  $p'(X) = p(X)$  时, 则  $p(X) = \phi_1(X)$ , 式(11)中的  $t$  为 0, 因此不能构造出由  $p'(X)$  生成的伽罗华域  $GF(2^L)$  上的生成多项式形如  $g(X) = \text{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2^t}(X)\}$  的二进制 BCH 码, 从而  $m$  序列  $A_n(X)$  不能等价于二进制 BCH 码。

(2)当  $p'(X) \neq p(X)$  时, 即  $p(X) \neq \phi_1(X)$ , 总存在  $1 \leq t < 2^{L-1}$ , 使得式(11)成立, 从而  $m$  序列  $p_n(X)$  等价于以  $p'(X)$  生成的伽罗华域  $GF(2^L)$  上的纠  $t$  个错误的  $(2^L - 1, k)$  二进制 BCH 码。

(3)纠错位数  $t$  的大小则取决于  $p(X)$  在以  $p'(X)$  为本原多项式生成的伽罗华域  $GF(2^L)$  中的最低次数根元素  $\alpha^i$ , 它们之间的关系可表示为  $t = (i - 1)/2$ 。

(4)根据本原多项式在伽罗华的根元素分布特点, 若  $\alpha^i$  为  $p(X)$  在以  $p'(X)$  为本原多项式生成的伽罗华域  $GF(2^L)$  中的最低次数根元素, 则通过选取不同的  $p'(X)$ , 总能使得  $i = 2^{L-1} - 1$  最大可能纠错位数  $t$  达到  $2^{L-2} - 2$ , 此时可适应约 25% 以下的误码率。

### 3.2 基于与 BCH 码等价变换的 $m$ 序列特征多项式估计算法

在对扩频序列盲分析的实际处理中, 假设通过处理已经获取扩频码的周期  $2^L - 1$  以及一个完整周期的扩频码序列  $p_n(X)$ , 该序列中可能存在误码。

总结起来, 利用上述等价原理, 根据周期估计得到多项式阶数  $L$ , 然后选择  $L$  阶本原多项式  $p'(X)$ , 构造 BCH 码 ( $p'(X)$  的选择决定了最大可纠错个数  $t$ ), 并对其进行译码, 当  $m$  序列中误码个数低于构造出 BCH 码的可纠错个数时, 才能正确译码。BCH 码的译码算法可判断译码过程是否正确, 如果正确, 说明构造出了合理的 BCH 码, 整个估计过程符合  $m$  序列与 BCH 码的等价原理的, 从而完成估计。

综上所述, 本文提出基于 BCH 码等价变换的  $m$  序列特征多项式估计算法, 具体步骤如下:

(1)在  $L$  阶本原多项式中, 选择一个  $p_1(X)$ , 利用  $m$  序列构造过程中的线性关系, 通过代入验证可判定  $p_1(X)$  是否就是  $m$  序列的特征多项式  $p(X)$ 。在有误码的情况下主要采取: 一是以  $L$  为间隔选取接收码序列和选择合适验证门限的方法来适应一定误码, 二是根据误码粗估情况, 选择合适的验证门限, 可适应一定的误码。通过对周期为 2048 的  $m$  序列进行 10000 次蒙特卡洛仿真验证得出, 在无粗估误码率的情况下, 0.6-0.7 的验证门限既能适应一定的误码, 又能抑制虚警, 该方法大约能适应 20% 以下的误码率。

(2)若  $p(X) = p_1(X)$ , 则已经完成  $m$  序列特征多项式的识别, 结束算法。

(3)若  $p(X) \neq p_1(X)$ , 则按上述原理, 构造二进制 BCH 码。

(4)选择纠错位数  $t$  (初始为  $t=1$ ), 利用 BCH 码译码算法进行译码。

(5)若译码成功, 则能够得到无误码的  $m$  序列, 进而利用 BM 算法快速地估计出  $m$  序列的特征多项式, 结束算法。

(6)若译码失败, 则递增纠错位数  $t$  ( $t \leq 2^{L-2}$ ), 返回步骤(4)。

(7)直到遍历完所有  $L$  阶本原多项式, 若未能完成估计, 则说明序列误码率超过算法适应范围。

## 4 算法仿真性能与分析

### 4.1 实例分析

不妨以特征多项式为  $p(X) = 1 + X + X^4 + X^5 + X^6$  的  $m$  序列为例, 假设已知一个完整周期的  $m$  序列  $p_n(X)$ , 且周期  $p$  为 63。根据  $p = 2^L - 1$ , 可知该序列特征多项式的阶数  $L$  为 6, 选择以本原多项式  $p'(X) = 1 + X + X^6$  生成的伽罗华域  $GF(2^6)$  上构造二进制 BCH 码。该伽罗华域  $GF(2^6)$  如表 1 所示。

从表 1 中可以看到, 在该域中  $1 + X + X^4 + X^5 + X^6$  的首个根元素为  $\alpha^{23}$ , 即  $p(X) = \phi_{23}(X)$ , 因此该  $m$  序列可表示为

$$\begin{aligned} A_n(X) &= \frac{h(X)(1 + X^p)}{p(X)} \\ &= \frac{h(X)\text{LCM}\{\phi_1(X), \phi_2(X), \phi_3(X), \dots, \phi_{31}(X)\}}{p(X)} \\ &= \text{LCM}\{\phi_1(X), \phi_3(X), \dots, \phi_{21}(X)\} \times [h(X) \\ &\quad \cdot \text{LCM}\{\phi_{27}(X), \phi_{31}(X)\}] = g(X)b(X) \end{aligned} \quad (12)$$

此时的  $m$  序列可以看作是信息序列为  $b(X)$ , 生成多项式为  $g(X)$  的二进制 BCH 码。

根据伽罗华域的性质, 可计算出  $g(X)$  是一个次数为 47 的多项式, 即  $n - k = 47$ , 则  $k = 16$ , 纠错位数  $t = (23 - 1)/2 = 11$ 。所以通过构造以本原多项式  $p'(X) = 1 + X + X^6$  生成的伽罗华域  $GF(2^6)$  上的 (63,16) 二进制 BCH 码, 该码能纠正 11 位误码。利用 BCH 码的译码算法, 可以完成对含有误码的  $m$  序列  $A_n(X)$  的纠错处理, 得到没有误码的  $m$  序列, 进而可利用 BM 算法, 完成  $m$  序列特征多项式的估计。此时最大纠错个数可适应到 11 位, 在噪声分布比较均匀的情况下大约能适应 17.46% 的误码率。

根据前文分析, 误码适应性跟构造 BCH 码的本原多项式选择有关, 通过选择不同的  $p_1(X)$  进一步仿真, 发现若  $p_1(X)$  未完成估计, 则选择  $p_1(X)$  的逆序多项式作为本原多项式, 至少能适应 9.52% 以上的误码, 结果如表 2 所示。

表 1 以本原多项式  $p'(X) = 1 + X + X^6$  生成的伽罗华域  $GF(2^6)$

序号	最小多项式	根元素	是否本原多项式
1	$1 + X + X^6$	$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	是
2	$1 + X + X^2 + X^4 + X^6$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	否
3	$1 + X + X^2 + X^5 + X^6$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	是
4	$1 + X^3 + X^6$	$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	否
5	$1 + X^2 + X^3$	$\alpha^9, \alpha^{18}, \alpha^{36}$	否
6	$1 + X^2 + X^3 + X^5 + X^6$	$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}$	是
7	$1 + X + X^3 + X^4 + X^6$	$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}$	是
8	$1 + X^2 + X^4 + X^5 + X^6$	$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}$	否
9	$1 + X + X^2$	$\alpha^{21}, \alpha^{42}$	否
10	$1 + X + X^4 + X^5 + X^6$	$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$	是
11	$1 + X + X^3$	$\alpha^{27}, \alpha^{54}, \alpha^{45}$	否
12	$1 + X^5 + X^6$	$\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}$	是

表 2 选择不同的  $p_1(X)$  及其逆序多项式的误码适应能力

分组	本原多项式 $p_1(X)$	可适应误码率	$p_1(X)$ 的逆序多项式	可适应误码率	算法误码适应率
1	$1 + X + X^6$	17.46%	$1 + X^5 + X^6$	3.17%	17.46%
2	$1 + X + X^2 + X^5 + X^6$	23.81%	$1 + X + X^4 + X^5 + X^6$	步骤(1)即可判定	> 23.81%
3	$1 + X^2 + X^3 + X^5 + X^6$	7.94%	$1 + X + X^3 + X^4 + X^6$	9.52%	9.52%

4.2 误码适应性能仿真分析

仿真以特征多项式为  $p(X) = 1 + X^7 + X^{10}$  的 10 阶 m 序列为识别对象。现有估计算法中基于高阶累积量的方法具有较好的误码适应性能，因此仿真仅将该算法与本文算法在误码适应性能方面进行比较。假设已到完整周期的含误码 m 序列，在本文算法的步骤(1)中不妨选择  $p_1(X) = 1 + X^3 + X^{10}$  来构造二进制 BCH 码。两种算法在不同误码率条件下的估计正确率的仿真结果如图 2 所示。

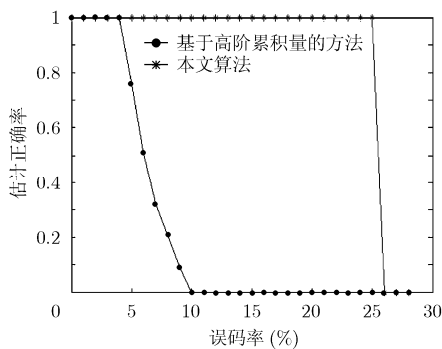


图 2 两种估计算法的误码适应性能比较

从图 2 中可以看出，基于 m 序列与 BCH 码等价变换的特征多项式估计算法在误码适应性能上比基于高阶累积量的方法要好，算法中选择构造 BCH 的本原多项式  $p_1(X)$  刚好实现最大纠错位数，达到算法的最优性能，大约能适应 24.93% 的误码率。

5 总结

本文通过分析 m 序列和二进制 BCH 码在生成原理上的相似性，构造出 PN 序列与 BCH 码的等价模型，提出了基于 m 序列与 BCH 码等价变换的特征多项式估计算法。该算法可以利用 BCH 码的纠错性能适应较大的误码率，通过实例分析和仿真，表明本算法能较好地解决误码条件下的 m 序列特征多项式估计问题，相比以往算法，本文算法在误码适应性能上具有较大优越性。同时，BCH 码常采用时域的迭代法译码，算法的译码速度与纠错位数成线性关系，对于二进制码，需要进行(可纠错个数+错误个数)/2 次迭代运算，当错误位数较多时，迭代次数相应增多。本文估计算法的耗时主要在于 BCH 码的纠错译码过程，现有的 BCH 码译码算法在生成多

项式阶数低于 20 时效率较高,但是估计算法需要尝试多种生成多项式,随着阶数的增加,算法计算量会增大较快。本文算法的运算速度主要适用于通信信号处理中常用 20 阶以内的  $m$  序列分析问题,具有一定的军事意义和经济价值。

### 参 考 文 献

- [1] Trappe W and Washington L C 著. 王全龙, 王鹏, 林昌露译. 密码学与编码理论. 北京: 人民邮电出版社, 2008, 第3章第3节.
- [2] 刘焯淋, 向劲松, 代少升. 扩展频谱通信. 北京: 北京邮电大学出版社, 2008, 第4章第3节.
- [3] 吴迪. 直扩信号的快速同步技术研究[D]. [硕士学位论文, 南京理工大学, 2009.
- [4] Berlekamp E R. Algebraic Coding Theory. McGraw-Hill Book Company[M]. New York: USA, 1968: 313-325.
- [5] 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.
- [6] 王丽萍, 祝跃飞. F[x]-格基约化算法和多条序列综合[J]. 中国科学E辑, 2003, 33(2): 168-173.
- [7] El-Khamy S E. Efficient detection of truncated  $m$ -sequence using higher order statistics[C]. 20th National Radio Science Conference[C]. Cairo Egypt. 2003, C8 1-9.
- [8] Wang Feng-hua, Huang Zhi-tao, and Zhou Yi-yu. A new method for  $m$ -sequence and gold-sequence generator polynomial estimation[C]. IEEE International Symposium on Microwave Antenna, Propagation and EMC Technologies for Wireless Communications, Hangzhou China, 2007: 1039-1044.
- [9] Pless V. Introduction to the Theory of Error Correcting Codes [M]. Second Edition. New York: Wiley, 1989: 109-117.
- [10] Cho Jun-ho and Sung Won-yong. Strength-reduced parallel chien search architecture for strong BCH codes[J]. *IEEE Transactions on Circuits and Systems*, 2008, 55(5): 427-431.
- [11] Zheng Jun-ru and Takayasu Kaida. Equivalence between the BCH bound and the schaub bound for cyclic codes[C]. Proceedings of IEEE Information Theory Workshop, Chengdu China, 2006: 29-32.
- [12] Shi Zhi-ping, Zhou Liang, Wen Hong, and Li Shao-qian. Iterative decoding for the concatenation of LDPC codes and BCH codes based on bphase algorithm[C]. International Conference on ITS Telecommunications Proceedings, Chengdu China, 2006: 12-15.
- 柴先明: 男, 1984年生, 助理工程师, 研究方向为电子侦察信号处理、信道编码盲识别和伪随机序列盲估计.
- 魏跃敏: 男, 1978年生, 工程师, 研究方向为电子侦察信号处理和空间信息对抗.
- 师栋锋: 男, 1980年生, 工程师, 研究方向为电子侦察信号处理和空间信息对抗.
- 蔡 凯: 男, 1973年生, 高级工程师, 研究方向为电子侦察信号处理和空间信息对抗.
- 黄知涛: 男, 1976年生, 教授, 研究方向为循环平稳信号处理、电子侦察信号处理、无源目标探测与定位、空间信息对抗.