



基于 GFFT 的 LFSR 序列生成多项式估计方法

沈利华

(浙江工业大学之江学院, 浙江 绍兴 312030)

摘要: 针对线性反馈移位寄存器 (LFSR) 序列生成多项式的估计问题, 提出了一种基于 LFSR 序列有限域傅里叶变换 (GFFT) 的估计方法。首先证明了 LFSR 序列 GFFT 的非零点与 LFSR 序列生成多项式的零点之间的对应关系, 进而利用该性质实现 LFSR 序列生成多项式的快速估计, 并给出了算法在误码环境下的改进方法。仿真实验验证了算法的有效性, 并对算法的计算复杂度进行了理论分析。和已有算法相比较, 本文提出的算法具有更高的计算效率。

关键词: 信号处理; 线性反馈移位寄存器; 有限域傅里叶变换; 生成多项式

中图分类号: TN911.22

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018025

Generator polynomial estimation of LFSR sequence based on GFFT

SHEN Lihua

Zhijiang College of Zhejiang University of Technology, Shaoxing 312030, China

Abstract: The problem addressed here is generator polynomial estimation of linear feedback shift register (LFSR) sequence. An algorithm based on the Galois field Fourier transform (GFFT) was proposed. The relationship between non-zero points in GFFT of LFSR sequence and zero points in generator polynomial of LFSR sequence was illustrated firstly. Then the generator polynomial of LFSR sequence was fast estimated based on that property, and the improved method in noisy environment was proposed at last. Validity of the algorithm is verified by the simulation results, and the computational load is illustrated. The computational efficiency of the proposed algorithm is higher than that of the existing algorithms.

Key words: signal processing, linear feedback shift register, Galois field Fourier transform, generator polynomial

1 引言

线性反馈移位寄存器 (linear feedback shift register, LFSR) 序列因其构造方便, 理论成熟, 且具有良好的伪随机和自相关特性, 在扩频通信、

通信加扰/加密、航天测控等领域得到了广泛的应用^[1]。目前, 扩频通信中采用的扩频序列基本上都是基于 LFSR 生成的, 如 m 序列、Gold 序列等^[1-3]。同时, 为了避免通信过程中数字同步的失锁, 常对通信数据进行加扰处理以有效提高数据的概率

转换密度, 数据加扰使用的伪随机序列同样由 LFSR 生成^[4]。对于 LFSR 序列, 其生成多项式是一个非常重要的参数, 生成多项式和初始状态可以唯一确定 LFSR 序列, 因此在非合作信号处理领域, 完成 LFSR 序列生成多项式和初相的估计是对扩频信号进行相关干扰的基础, 也是实现数据解扰、解密的关键。

LFSR 序列生成多项式的估计问题已有较多研究成果^[5-21], 最直接的方法主要有组合枚举的方法^[5]与基于匹配搜索的方法^[6]两类, 根据 LFSR 输入与输出的关系, 列出齐次线性方程组, 通过搜索多项式系数, 找出方程组符合最多的解, 即生成多项式系数。该类方法思路简单直接, 但枚举组合时需要进行大量的试探并验证, 计算量较大。

参考文献[7]提出了基于 Walsh-Hadamard 变换的估计算法, 将 LFSR 序列排列成二元域上线性方程组的系数矩阵, 进而利用 Walsh-Hadamard 变换求解其生成多项式, 算法要求 LFSR 抽头系数较少。陈松等人^[8]利用序列软信息, 构建序列及多项式可信度集合, 通过可信度累积实现估计。参考文献[9]提出了基于高阶统计原理的 m 序列本原多项式的测定方法。算法寻找含错 m 序列的高阶统计峰值算得本原多项式的高阶倍式, 通过求解高阶倍式的最大公约式来估计序列的本原多项式。与基于 Walsh-Hadamard 变换的方法相比, 参考文献[8,9]不再受制于生成多项式的抽头数, 但不足之处在于计算复杂度相对较高。参考文献[10]提出的算法与之类似, 将 LFSR 序列转换为卷积码^[10]或分组码^[11,12], 利用译码的纠错实现 LFSR 序列的生成多项式估计, 这两种算法思路较新颖, 但算法过程都比较复杂, 步骤繁琐, 不易实现。

参考文献[14-17]利用大量数据的统计偏差, 估计生成多项式的倍式, 进而利用高阶倍式的最大公约式得到序列的生成多项式。参考文献[18-21]同样在信源不平衡的条件下, 以游程

距离和相关度等作为信源不平衡性的衡量准则, 通过比特抽取参照的多项式的不平衡性指标, 判定生成的多项式是否正确, 该类方法不用事先估计 LFSR 序列, 但主要问题是算法的计算量大, 实时性较差。

从目前的研究成果来看, LFSR 序列生成的多项式估计着重解决的是算法的容错能力, 而对算法的实时性要求不高。但在现代电子战的环境下, 要求能够实现对通信信号的实时干扰和信息截获, 因此需要研究 LFSR 序列生成多项式估计的快速方法。对此, 本文提出了一种基于 LFSR 序列有限域傅里叶变换 (Galois field Fourier transform, GFFT) 的估计方法, 利用 LFSR 序列 GFFT 的频谱中非零点与序列生成多项式零点的对应关系, 实现 LFSR 序列生成多项式的快速估计。

2 LFSR 序列生成多项式估计的数学模型

线性反馈移位寄存器的组成如图 1 所示。图 1 中各级移位寄存器的状态分别用 a_i 表示, $a_i = 0$ 或 1, i 是整数。反馈线的连接状态用 c_i 表示, $c_i = 1$ 表示此线接通 (参加反馈), $c_i = 0$ 表示此线断开。

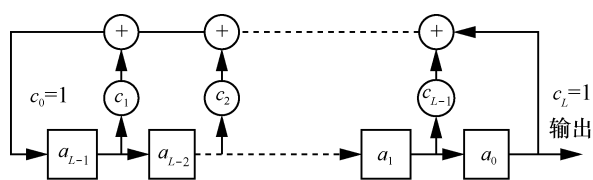


图 1 线性反馈移位寄存器

设 n 级移位寄存器的初始状态为 $a_{-1}a_{-2}\cdots a_{-n}$, 对于任意一状态 a_k , 有:

$$a_k = \sum_{i=1}^L c_i a_{k-i} \quad (1)$$

其中, 求和按模 2 运算, 式 (1) 为 LFSR 序列递推方程。 c_i 的取值决定了移位寄存器的反馈连接和序列的结构, 故 c_i 是 LFSR 序列一个很重要的参量, 现将它用式 (2) 表示:



$$f(x) = c_0 + c_1x + \cdots + c_{L-1}x^{L-1} + c_Lx^L \quad (2)$$

其中, $f(x)$ 为生成多项式, 也可称为特征方程或特征多项式。

同时, 可以将反馈移位寄存器的输出序列 $A = \{a_k\}$ 用多项式表示为:

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{2^L-2}x^{2^L-1} + \cdots \quad (3)$$

式 (3) 称为序列 A 的母函数。

LFSR 序列由移位寄存器生成, 即 LFSR 序列由移位寄存器的系数及初始状态唯一确定, 因此 LFSR 序列的参数估计就是估计移位寄存器系数及其初始状态。LFSR 序列的生成多项式估计可以转化为如下问题: 求解线性递归序列的阶数及递归关系。

设已知 LFSR 序列片段为 $a_i, i = 0, 1, \dots, n, \dots$, 则由式 (1) 可得如下线性方程组:

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{L-1} & a_L \\ a_1 & a_2 & \cdots & a_L & a_{L+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_L & a_{L+1} & \cdots & a_{2L} & a_{2L+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} c_L \\ c_{L-1} \\ \vdots \\ c_1 \\ 1 \end{pmatrix} = 0 \quad (4)$$

求解式 (4) 所示的方程组就可以获得序列的生成多项式, 因此式 (4) 为 LFSR 序列生成多项式估计的线性方程组模型。

事实上, 对于所有的无限长 LFSR 序列, 有^[22]:

$$f(x)A(x) = h(x) \quad (5)$$

其中, $h(x)$ 为次数低于 $f(x)$ 的多项式。当 $f(x)$ 确定时, $h(x)$ 仅由初始状态决定, 因此 $h(x)$ 称为初始状态多项式。

3 LFSR 序列的有限域傅里叶变换及其性质

在信号处理中, 有限长序列 $x(n), n = 0, 1, \dots, N-1$ 的有限域傅里叶变换 (DFFT) 可以表示为^[22]:

$$X(k) = \sum_{n=0}^{N-1} x(n)e^{-j\frac{2\pi}{N}nk} \quad (6)$$

其中, $e^{-j\frac{2\pi}{N}}$ 为 1 在复数域的 N 次根。因此, GFFT 可以看作有限序列在 1 的 N 次根上的分解。

根据以上对傅里叶变换的理解, 在有限域 $GF(2^m)$ 中只要存在 1 的 N 次根, 就存在从 $x(n)$ 到 $X(k)$ 的变换, 等同于 GFFT。然而, 在有限域上这个条件是满足的, 而且对于长度为 2^{m-1} 的二进制向量在 $GF(2^m)$ 上变换可以写为如下变换形式^[22]:

$$\text{正变换: } X(k) = \sum_{n=0}^{N-1} x(n)\alpha^{nk} \quad (7)$$

$$\text{反变换: } x(n) = \sum_{k=0}^{N-1} X(k)\alpha^{-nk} \quad (8)$$

其中, α 为对应域上的本原元。

与复数域的傅里叶变换类似, 有限域的傅里叶变换具有线性性、正交性、相关特性、周期性、对称性、循环卷积特性、抽样性、位移特性等^[22]。

LFSR 序列是一种特殊的有限域序列, 本文还证明了其有限域的傅里叶变换还存在两条重要性质, 利用这些性质可实现 LFSR 序列生成多项式的快速估计。

性质 1 LFSR 序列 GFFT 的非零点对应序列生成多项式的零点。

证明: 对于线性反馈移位寄存器序列对应的母函数 $A(x)$ 、生成多项式 $f(x)$ 、初始状态多项式 $h(x)$, 存在如下关系:

$$A(x) = \frac{h(x)}{f(x)} \quad (9)$$

其中, $A(x)$ 为无穷序列对应的多项式, 而要分析的是移位寄存器序列的一个周期, 该周期对应的多项式用 $\bar{A}(x)$ 表示。下面就求 $\bar{A}(x)$ 的计算式。

式 (9) 可以写为:

$$A(x) = \frac{h(x)}{f(x)} = \frac{h(x)}{1+x^P} \cdot \frac{1+x^P}{f(x)} \quad (10)$$

令 $A'(x) = h(x) \cdot \frac{1+x^P}{f(x)}$, 则:

$$\begin{aligned} A(x) &= \frac{A'(x)}{1+x^l} \\ &= A'(x)(1+x^l+x^{2l}+\cdots) \\ &= A'(x) + x^l A'(x) + x^{2l} A'(x) + \cdots \end{aligned} \quad (11)$$

由此可见, $A'(x)$ 就是要求的移位寄存器序列的主周期对应的多项式, 即:

$$\bar{A}(x) = A'(x) = h(x) \cdot \frac{1+x^P}{f(x)} \quad (12)$$

令 $\bar{A}(x) = 0$, 得:

$$h(x) \cdot \frac{1+x^P}{f(x)} = 0 \quad (13)$$

其中, $1+x^P$ 有 P 个根, 且这些根对应域 $\text{GF}(2^m)$ 上 0 以外的所有元素。

对于 m 序列的生成多项式 $f(x)$, 有 n 个零点且与 $h(x)$ 无共同零点, 所以方程 $\bar{A}(x) = 0$ 有 $(2^n - 1 - n)$ 个根; 对于 Gold 序列生成多项式 $f(x)$, 有 $2n$ 个零点且与 $h(x)$ 无共同零点, 所以 $\bar{A}(x) = 0$ 有 $(2^n - 1 - 2n)$ 个根。

至此, 性质 1 证毕。

性质 2 对一个周期的 LFSR 序列进行循环移位, 其 GFFT 的非零点不变。

证明: 一个周期的 LFSR 序列平移序列仍然为 LFSR 序列, 而且生成多项式相同。根据性质 1 及其证明可知, 生成多项式相同的序列具有相同的 GFFT 非零点位置, 因此 LFSR 序列的 GFFT 对原序列具有平移保持性。

至此, 性质 2 证毕。

4 基于 GFFT 的 LFSR 序列生成多项式估计

根据性质 1 的证明可知, 序列 GFFT 的非零点对应生成多项式的零点。设周期为 P 的 LFSR 序列 $\bar{A}$ 的 GFFT 有 m 个零点, 其位置分别为 $p_i, i=1, 2, \cdots, m$, 则生成多项式在域 $\text{GF}(2^m)$ 中可写为如下形式:

$$f(x) = \prod_{i=1}^m (x - \alpha^{p_i}) \quad (14)$$

其中, α 为域 $\text{GF}(2^m)$ 的本原元。

若令 $c_i, i=0, 1, \cdots, m$ 为 LFSR 序列生成多项式系数, 则有:

$$f(x) = \sum_{i=0}^m c_i x^i = \prod_{i=1}^m (x - \alpha^{p_i}) \quad (15)$$

由此可得:

$$\begin{aligned} c_0 &= \prod_{i=1}^m \alpha^{p_i} \\ &\cdots \\ c_{m-1} &= \sum_{i=1}^m \alpha^{p_i} \\ c_m &= 1 \end{aligned} \quad (16)$$

即 c_i 为式 (15) 展开后 x^i 的系数。

根据式 (15) 求得的 $f(x)$, 且已知 $\bar{A}(x) = h(x) \cdot \frac{1+x^P}{f(x)}$, 则有:

$$h(x) = \bar{A}(x) \cdot \frac{f(x)}{1+x^P} \quad (17)$$

由此可得, 利用 GFFT 求 LFSR 序列生成多项式的算法如下 (简称算法 1)。

输入: LFSR 序列的一个周期 $\bar{A}$ 。

输出: 序列生成多项式 $f(x)$ 和初始相位 $h(x)$ 。

步骤 1 计算序列 $\bar{A}$ 的有限域 GFFT, 记为 G 。

步骤 2 获取 G 的非零点位置, 记为 $\alpha_i, i=1, 2, \cdots, m$, m 为非零点个数。

步骤 3 根据式 (15) 和式 (16) 求生成多项式 $f(x)$ 。

步骤 4 根据式 (17) 求序列初始状态多项式。

当 LFSR 序列中存在有限个误码时, 序列的 GFFT 同时包含了 LFSR 序列与误码的信息, 因此可以通过序列 GFFT 求得误码, 然后再求生成多项式。

设序列中含有 Q 个误码, 其位置对应为 $q_i, i=1, \cdots, Q$ 。对于无误码 LFSR 序列 GFFT 为零的点, 设为 X_k , 则有:



$$X_k = \sum_{i=1}^Q \alpha^{kq_i} \quad (18)$$

估计误码的问题可以转化为已知 X_k , 求误码数 Q 及其位置 q_i 。

当仅有一个误码时, 有:

$$X_k = \alpha^{kq} \quad (19)$$

对式 (19) 两边取对数有:

$$\lg(X_k) = kq \quad (20)$$

则:

$$q = \frac{\lg(X_k)}{k} \quad (21)$$

当存在多个误码时, 可得如下方程组:

$$X_{k_j} = \sum_{i=1}^Q \alpha^{k_j q_i}, j=1, \dots, Q, \dots \quad (22)$$

上述方程组能够做如下转换:

$$X_{k_j} = \sum_{i=1}^Q \alpha^{k_j q_i} = \sum_{i=1}^Q \sigma_i X_{k_j - i}, j=1, \dots, Q, \dots \quad (23)$$

其中, σ_i 为位置多项式系数, 即:

$$\sigma(x) = \prod_{i \in I} (1 - \alpha^i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \dots \quad (24)$$

其中, I 表示原序列中不为零元素的位置集合。

由此可见, 只要在频域求得了 σ_i 就可实现误码位置的估计, 因此误码估计可以等效为在频域上的序列综合。在频域上可以将生成多项式的根视为误码, 当误码数小于生成多项式阶数时, 首先在频域上完成序列综合, 估计误码位置, 然后估计原序列的生成多项式。当频域存在误码 (原序列生成多项式根的位置) 时, 其序列综合仍较困难, 此处考虑通过有限域方程组的求解完成频域的序列综合。

频域方程组表示为:

$$\begin{pmatrix} X_0 & X_1 & \cdots & X_{K-1} & X_K \\ X_1 & X_2 & \cdots & X_K & X_{K+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ X_K & X_{K+1} & \cdots & X_{K+2} & X_{2K} \\ \vdots & \vdots & \ddots & \vdots & \vdots \end{pmatrix} \cdot \begin{pmatrix} \sigma_K \\ \sigma_{K-1} \\ \vdots \\ \sigma_1 \\ 1 \end{pmatrix} = 0 \quad (25)$$

其中, K 为大于误码数的一个整数, 因为误码数

事先未知, 因此 K 可以预设一个较大的值。需要注意的是, 频域方程组对应的域与原序列对应的域有所不同。

总结以上分析可得, 误码环境下基于 GFFT 求解 LFSR 序列生成多项式的算法如下 (简称算法 2)。

输入: 含有误码的一个完整周期 LFSR 序列 $\bar{A}$ 。

输出: 误码位置 Q , 序列的生成多项式系数 F 。

步骤 1 计算序列 $\bar{A}$ 的 GFFT, 记为 G 。

步骤 2 将 G 排列为式 (25) 所示方程组。

步骤 3 依次求方程组系数矩阵的秩。

步骤 4 获得秩的最小值, 求解一个对应的方程组, 其解记为 σ_i 。

步骤 5 根据式 (23) 求得误码位置为 Q 。

步骤 6 改变 $\bar{A}$ 中对应误码位置的值, 得到序列 A' 。

步骤 7 计算 A' 的 GFFT, 并根据算法 1 估计生成多项式和初始相位。

5 算法仿真实验

以生成多项式阶数为 8 的 m 序列为对象进行仿真分析, 其生成多项式为 $f(x) = 1 + x^2 + x^3 + x^4 + x^8$, 当序列中不存在误码时, 其 GFFT 如图 2 所示。由图 2 可以看出, 序列 GFFT 中共有 8 个非零点, 获取其位置并利用式 (15) 和式 (16) 求解其生成多项式, 可得 $f(x) = 1 + x^2 + x^3 + x^4 + x^8$, 算法估计正确。

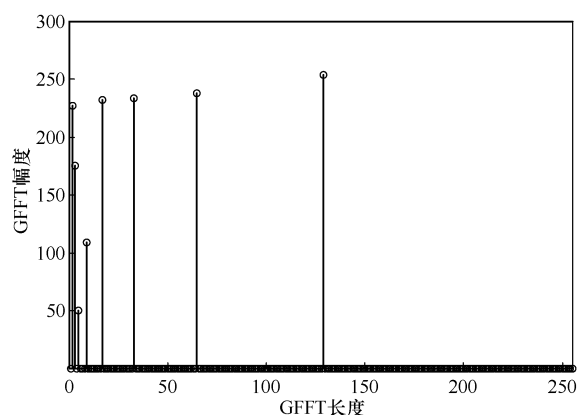


图 2 无误码时 255 长度 LFSR 序列的 GFFT

当序列中存在误码时, 设误码率为 2%, 此时序列的 GFFT 如图 3 所示, 利用算法 2 构建频域上的线性方程组, 其方程组秩的分布情况如图 4 所示。从图 4 中可以看出, 方程组秩的最小值稳定为 4, 可知序列中含有 4 个误码。选择其中一个秩为 4 的方程组并求解, 可得误码位置分别为 32、93、189、242。将序列中的误码进行纠正, 并利用算法 1 估计序列的生成多项式即可。

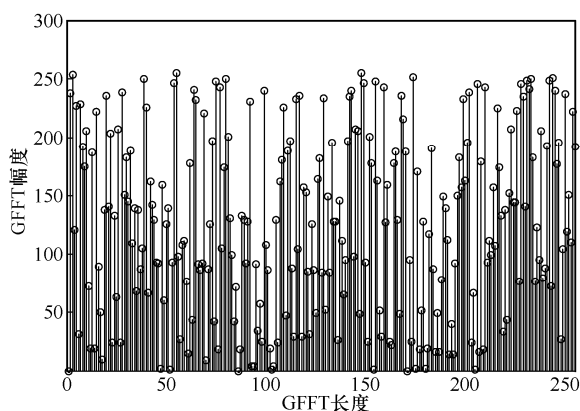


图3 含误码时 255 长度 LFSR 序列的 GFFT

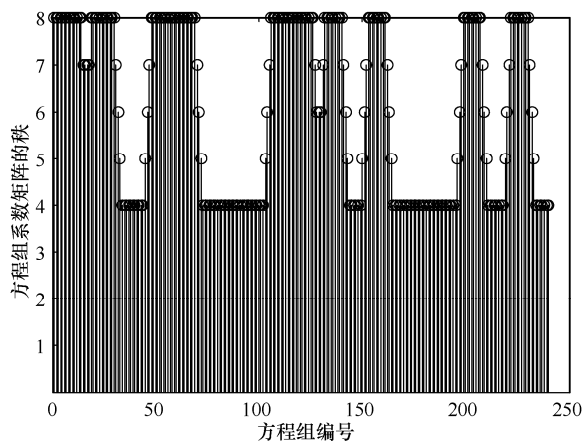


图4 频域线性方程组秩的分布

LFSR 序列生成多项式估计问题的研究成果较多, 最著名的是 Berlekamp-Massey 算法 (BM 算法) [23], 而计算效率较高的是基于 Walsh-Hadamard 变换算法 [7], 下面分别分析本文算法与上述两种算法的计算复杂度。设生成多项式的最高次数为 L , LFSR 序列长度为 N , BM 算法估计生成多项式的计算量为 $O(N^2)$, 利用沃尔什

变换求解生成多项式的计算量主要集中在两部分: 一是将方程组系数矩阵中的行向量用十进制数表示; 二是计算沃尔什谱, 总的计算量为 $N \lg N + (N-L)(L+1)$ 。而本文算法的计算量主要集中在 GFFT 的计算上, 其计算量为 $N \lg N$, 由非零点计算生成多项式的计算量为 L^2 , 所以算法的计算量为 $N \lg N + L^2$ 。

3 种算法在估计不同长度序列生成多项式时所需的计算量如图 5 所示。从图 5 中可以看出, 本文算法计算量低于 BM 算法和 Walsh-Hadamard 变换算法, 算法计算效率得到进一步提高。

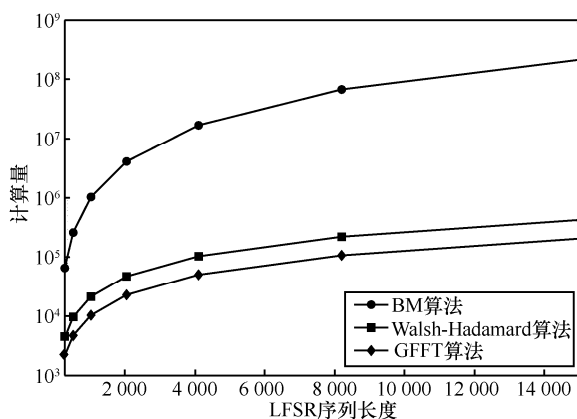


图5 本文算法与 BM 算法和 Walsh-Hadamard 算法计算量的比较

6 结束语

本文针对 LFSR 序列的生成多项式估计问题, 提出了一种基于 LFSR 序列 GFFT 的估计方法。本文首先证明了 LFSR 序列 GFFT 中的非零点对应着序列生成多项式的零点, 利用这一性质从 GFFT 中获取序列生成多项式的零点, 进而得到 LFSR 序列的生成多项式, 实现 LFSR 序列生成多项式的快速估计, 并给出了算法在误码环境下的改进方法。仿真结果表明算法有效可行, 且计算效率优于文献中已有算法。

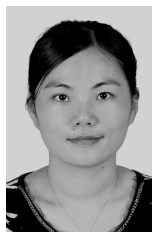
参考文献:

- [1] 刘洋. TD-SCDMA 同频组网中扰码性能分析及同频干扰的解决方法[J]. 电信科学, 2007, 23(12): 48-53.



- LIU Y. An improved coverage solution for TD-SCDMA multi-frequency cellular network [J]. Telecommunications Science, 2007, 23(12): 48-53.
- [2] 任啸天, 徐晖, 王翔, 等. 一种针对短码、周期长码直扩信号扩频序列盲估计方法[J]. 宇航学报, 2011, 32(12): 2596-2600.
- REN X T, XU H, WANG X, et al. A method for blind estimation of PN sequence of short-code and periodic long-code DSSS signal[J]. Journal of Astronautics, 2011, 32(12): 2596-2600.
- [3] 张志成, 黄小娜, 熊丽. 一种适合多载波码分多址系统的扩频序列[J]. 电信科学, 2015, 31(11): 47-51.
- ZHANG Z C, HUANG X N, XIONG L. A spread spectrum sequence for MC-CDMA system [J]. Telecommunications Science, 2015, 31(11): 47-51.
- [4] YUAN C, ZHONG Y Z, YANG S Q. Composite chaotic pseudo-random sequence encryption algorithm for compressed video[J]. Tsinghua Science and Technology, 2004, 9(2): 234-241.
- [5] HE W J. Reconstructing the feedback polynomial of a linear scrambler with the method of hypothesis testing[J]. IET Communications, 2015, 9(8): 1044-1047.
- [6] 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.
- CHAI X M, PENG G, SHI D F, et al. Generator polynomial estimation of pseudo-random sequence based on match-searching[J]. Optics and Precision Engineering, 2011, 19(9): 2222-2227.
- [7] 黄开枝, 陈松. 基于加权 WHT 的软判决序列快速估计算法[J]. 电子与信息学报, 2013, 35(1): 74-79.
- HUANG K Z, CHEN S. A soft fast estimation method of PN sequence based on weighting Walsh Hadamard Transform (WHT)[J]. Journal of Electronics & Information Technology, 2013, 35(1): 74-79.
- [8] 陈松, 黄开枝, 赵华. 基于可信度累积的伪随机序列多项式估计算法[J]. 通信学报, 2012, 33(9): 125-131.
- CHEN S, HUANG K Z, ZHAO H. Polynomial estimation method for PN sequence based on reliability accumulation[J]. Journal on Communications, 2012, 33(9): 125-131.
- [9] 陈松, 黄开枝. 基于正反向联合 TCF 的序列多项式估计算法[J]. 电路与系统学报, 2013, 18(2): 145-151.
- CHEN S, HUANG K Z. A method for generator polynomial estimation of PN sequence based on forward and backward combined TCF[J]. Journal of Circuits and Systems, 2013, 18(2): 145-151.
- [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): 6-11.
- HAO S Q, QI L, WANG Y. A new blind recognition method of pseudo-randomizer code sequence[J]. Journal of circuits and systems, 2011, 16(4): 6-11.
- [11] 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.
- CHAI X M, WEI Y M, SHI D F, 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.
- [12] 张昊, 吕全通, 朱宇轩. 基于线性分组码的自同步扰码盲识别[J]. 应用科学学报, 2015, 33(2): 178-186.
- ZHANG W, LV Q T, ZHU Y X. Blind recognition of self-synchronized scrambler based on linear block code[J]. Journal of Applied Sciences, 2015, 33(2): 178-186.
- [13] 陈泽亮, 彭华, 巩克现, 等. 基于软信息的扰码盲识别方法[J]. 通信学报, 2017, 38(3): 174-182.
- CHEN Z L, PENG H, GONG K X, et al. Scrambler blind recognition method based on soft information[J]. Journal on Communications, 2017, 38(3): 174-182.
- [14] MATHIEU C. Reconstruction of a linear scrambler[J]. IEEE Transactions on Computers, 2007, 56(9): 1283-1291.
- [15] LIU X B, SOO N K, WU X W. Reconstructing a linear scrambler with improved detection capability and in the presence of noise[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 208-218.
- [16] LIU X B, KOH S N, CHUI C C, et al. A study on reconstruction of linear scrambler using dual words of channel encoder[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 542-552.
- [17] XIE H, WANG F H, HUANG Z T. Blind reconstruction of linear scrambler[J]. Journal of Systems Engineering and Electronics, 2014, 25(4): 560-565.
- [18] 廖红舒, 袁叶, 甘露. 自同步扰码的盲识别方法[J]. 通信学报, 2013, 34(1): 136-143.
- LIAO H S, YUAN Y, GAN L. Novel blind recognition method for self-synchronized scrambler[J]. Journal on Communications, 2013, 34(1): 136-143.
- [19] 虞红芳, 吴曼, 刘曼, 等. 一种快速准确适用性广的伪随机扰码识别方法[J]. 电子科技大学学报, 2015, 44(4): 500-504.
- YU H F, WU M, LIU M, et al. Fast and correct recognition method for pseudo-randomizer code[J]. Journal of University of Electronic Science and Technology of China, 2015, 44(4): 500-504.
- [20] 黄芝平, 周靖, 苏绍璟, 等. 基于游程统计的自同步扰码多项式阶数估计[J]. 电子科技大学学报, 2013, 42(4): 541-545.
- HUANG Z P, ZHOU J, SU S J, et al. Order estimation of self-synchronizing scrambling polynomial based on run statistic[J]. Journal of University of Electronic Science and Technology of China, 2013, 42(4): 541-545.
- [21] 吕全通, 张昊, 朱宇轩. 基于相关度统计的同步扰码盲识别方法[J]. 数据采集与处理, 2016, 31(3): 570-576.
- LV Q T, ZHANG M, ZHU Y X. Blind recognition method for synchronous scrambler based on statistical correlation [J]. Journal of Data Acquisition and Processing, 2016, 31(3): 570-576.
- [22] ROBERT J M. 信息论与编码理论[M]. 李斗, 殷悦, 罗燕, 译. 北京: 电子工业出版社, 2007.
- ROBERT J M. The theory of information and coding[M]. Translated by LI D, YIN Y, LUO Y. Beijing: Publishing House of Electronics Industry, 2007.
- [23] IMAMURA K, YOSHIDA W. A simple derivation of the Berlekamp-Massey algorithm and some applications [J]. IEEE Transactions on Information Theory, 1987, 33(1): 146-150.

[作者简介]



沈利华 (1978-), 女, 浙江工业大学之江学院副教授, 主要研究方向为电子商务技术、网络安全、算法设计等。