

(19) 中华人民共和国国家知识产权局



(12) 发明专利申请

(10) 申请公布号 CN 104426555 A

(43) 申请公布日 2015. 03. 18

(21) 申请号 201310393476. 1

(22) 申请日 2013. 09. 03

(71) 申请人 电子科技大学

地址 611731 四川省成都市高新区西源大道 2006 号

(72) 发明人 卢欧欣 廖红舒 李立萍 魏平

(51) Int. Cl.

H03M 13/15(2006. 01)

H04L 1/00(2006. 01)

权利要求书1页 说明书4页 附图2页

(54) 发明名称

一种基于子模空间 Gröbner 基的准循环码盲识别方法

(57) 摘要

一种基于子模空间Gröbner基的准循环码盲识别方法。本方法应用于合作通信领域的智能通信以及非合作通信领域。本专利提出的基于子模空间Gröbner基的准循环码盲识别方法，是利用准循环码的代数结构特性，通过分组交织将其变换为一个商环上模空间的子模空间，根据该子模空间Gröbner基的性质对准循环码的编码参数进行盲识别和估计。本专利的方法，能够同时估计出准循环码码长和信息位长，具有运算复杂度低，识别速度快，性能稳定等特点，且能够抵抗高误码。

1. 基于子模空间**Gröbner**基的准循环码盲识别方法,其特征在于,包括以下步骤:
 - 1) 设需要遍历的码长范围以及当前二进制码长 n_{bt} ;
 - 2) 按照当前码长 n_{bt} 将截获的准循环码数据流进行分组,得到 N 组准循环码数据;
 - 3) 根据当前码长 n_{bt} 估计该码长下的 r 组准循环码移位因子 l_i 和分块个数 m_i , 满足 $n_0 = l_i \times m_i$, 且 $l_i > 1$; $\{(l_i, m_i) | i = 1, 2, \dots, r\}$;
 - 4) 根据不同组的准循环码移位因子 l_i 和分块个数 m_i 依次对 N 组码字进行一一对应的 $m_i \times l_i$ 维重排, 得到 N 个 R^1 上的 R -子模, 其中 $R = F[x]/\langle x^{m_i} + 1 \rangle$;
 - 5) 利用计算机代数系统求取 N 个 R^1 上 R -子模构成的子模空间的**Gröbner**基, 并记录其中单位基 e_i 的个数;
 - 6) 判断当前码长是否遍历完毕码长范围;如是,进入步骤 7), 如否, 更新当前码长 n_0 , 返回步骤 2);
 - 7) 选择**Gröbner**基中含单位基 e_i 个数最少的子模空间所对应的编码参数 (l_t, m_i) 为盲估计的编码参数。
 - 8) 利用行初等变换将估计出的编码参数 (l_i, m_i) 所对应的子模空间的**Gröbner**基化为上三角形式, 根据 $k_{bi} = \sum_{i=1}^l (m_i - \partial g_{ii})$ 得到二进制信息位长 k_{bi} , 其中 ∂g_{ii} 为对角线上元素的阶数, 则码率 $R = k_{bi} / (m_i \times l_i)$, RS 码信息位长 $k = n_i \times R$;
 - 9) 分为以下两种情况:

对于 RS 码, 由估计出的参数 n_0 和 k 确定生成多项式的根表达式 $g(x) = \prod_{i=1}^r (x + \alpha^i)$, 其中 $T = n - k$; 然后根据之前步骤中估计出的编码参数 (l_i, m_i, k) , 遍历编码维数 m_i 下的本原多项式得到本原多项式的估计值, 代入 $g(x) = \prod_{i=1}^r (x + \alpha^i)$ 记得到生成多项式估计值;

对于准循环 LDPC 码, 根据之前步骤中估计出的编码参数 (l_i, m_i, k) , 得到校验矩阵的维数 $H = (A_{ij})$, 其中 A_{ij} 为维数为 $m_i \times m_i$ 的循环移位单位阵或稀疏方阵, 且 H 的行重满足 $w_{Hamming}(H_{row}) \leq 0.25m_i$, 根据此限制条件对该码的对偶空间进行搜索得到校验矩阵 H 的估计值 H_{est} 。
2. 如权利要求 1 所述一种基于子模空间**Gröbner**基的准循环码盲识别方法,其特征在于,步骤 2) 中所述的码长为二元域 GF(2) 上的码长。
3. 如权利要求 1 所述一种基于子模空间**Gröbner**基的准循环码盲识别方法,其特征在于,步骤 2) 中所述的码字组数 N 大于循环移位因子 l_i , 为经验值;取值范围为 $l_i + 5 \leq N \leq l_i + 10$ 。
4. 如权利要求 1 所述一种基于子模空间**Gröbner**基的准循环码盲识别方法,其特征在于,步骤 5) 中所述的**Gröbner**基为约化的**Gröbner**基。

一种基于子模空间**Gröbner**基的准循环码盲识别方法

技术领域

[0001] 本发明应用于合作通信领域的智能通信以及非合作通信领域,涉及一种容误码的包含 RS 码在内的准循环码编码参数的盲估计。

背景技术

[0002] 为保证信息传输的可靠性,信道编码常用于通信领域中。当接收端对通信信号解调、解交织后,还需要进行解码,若能在接收端进行数据盲处理获得编码参数,则可提高系统效率,况且在一些特殊的领域并不能得到编码参数。如在非合作通信中要在非授权接入的情况下正确提取有用信息则必须正确估计编码参数,才能恢复更多的信息数据,为信号探测提供可靠信息,具有重要的实际应用价值。近年来,信道编码盲识别技术发展迅速,逐渐成为了通信领域内新的研究热点。

[0003] 准循环码是线性分组码的一类非常重要的子类,由于其特殊的代数结构可以简化编译码电路及存储空间,准循环码被广泛应用于差错控制编码中。例如,RS 码作为一类经典线性分组码,在二元域上为一个循环移位因子等于其编码域维数的准循环码;咬尾卷积码在一个分组长度内可等效于一个准循环码,被应用于 LTE 协议中;而准循环 LDPC 码是 LDPC 码的一大重要子类,广泛应用于包括 IEEE802.16e 在内的协议中。

[0004] 目前对于信道编码方式的盲识别研究主要集中在卷积码上,对于线性分组码的研究较少,专门针对具有准循环特性的线性分组码的参数盲识别的研究更少。若直接将传统二进制线性分组码的估计方法应用于 RS 码或具有准循环特性的线性分组码参数盲估计上,不能充分利用码字的代数结构性质,估计效率低。

[0005] 目前关于 RS 码参数盲识别的相关文献主要有刘健等人发表于《电子科技大学学报》(2009,38(3) : 363-367) 的“RS 码的盲识别方法”,闻年成等人发表于《计算机工程与应用》(2011,47(19) : 136-139) 的“RS 码的参数识别”以及吕喜等人在发表在《国防科技大学学报》(2011,33(4) : 123-127) 中的“一种 RS 码快速盲识别方法”,这些方法的共同点是利用 RS 码在二元域上的等效码字性质来估计码长,并缩小本原多项式和生成多项式的搜索范围,但估计码长时所使用的数据量没有减小,因而整个算法所需数据量并没有减少,性能也没有得到实质提升,且算法仅适用于 RS 码,没有利用准循环代数结构特性。甘露等人在《电子与信息学报》(第 34 卷第 12 期,2012 年 12 月) 发表的“基于中国剩余定理分解的 RS 码快速盲识别算法”中利用了循环码的代数特性,根据中国剩余定理,将原码字分解为一系列低阶分量码,通过对分量码字的识别与估计得到原码的码长和本原多项式,进一步对生成多项式进行估计,但缺点在于求取分量码时需遍历本原多项式,运算量较大,且无法直接估计出原码的信息位长。

[0006] 本发明提供了一种容误码的准循环码编码参数盲识别方法,充分利用准循环码的代数结构特性,通过分组交织将其变换为一商环上模空间的子模空间,根据该子模空间**Gröbner**基的性质对准循环码的编码参数进行盲识别和估计,可同时获得码长和信息位长参数,所需数据量和运算量均较少。

发明内容

[0007] 本发明所要解决的技术问题是，在数据量有限的情况下，充分利用准循环码的代数结构特性，高效地对准循环码的编码参数进行盲估计。

[0008] 为达到本发明的目的所采用的技术方案是，一种基于码字变换子模空间**Gröbner**基的准循环码参数盲估计方法，包括以下步骤：

[0009] 1) 设需要遍历的码长范围以及当前二进制码长 n_{bi} ；

[0010] 2) 按照当前码长 n_{bi} 将截获的准循环码数据流进行分组，得到 N 组准循环码数据；

[0011] 3) 根据当前码长 n_{bi} 估计该码长下可能的 r 组准循环码移位因子 l_i 和分块个数 m_i ，满足 $n_0 = l_i \times m_i$ ，且 $l_i > 1$ ； $\{(l_i, m_i) | i = 1, 2, \dots, r\}$ ；

[0012] 4) 根据不同组的准循环码移位因子 l_i 和分块个数 m_i 依次对 N 组码字进行 $m_i \times l_i$ 维重排，即按行写入 $m_i \times l_i$ 维矩阵。得到 N 个数据矩阵 c_i , $i=1, 2, \dots, N$ ；然后分别将 N 个数据矩阵按列读出并按照由低到高的阶数顺序转化为多项式形式，见附图 2，得到 N 个 R^1 上的 R^- 子模，其中 $R = F[x]/\langle x^{m_i} + 1 \rangle$ ；

[0013] 5) 利用计算机代数系统求取 N 个 R^1 上 R^- 子模构成的子模空间的**Gröbner**基，并记录其中单位基 e_i （即除第 i 位为单位元外其余位为零的基）的个数；

[0014] 6) 判断当前码长是否遍历完毕码长范围；如是，进入步骤 8)，如否，更新当前码长 n_0 ，返回步骤 2)；

[0015] 7) 选择**Gröbner**基中含单位基 e_i 个数最少的子模空间所对应的编码参数 (l_i, m_i) 为盲估计的编码参数。

[0016] 8) 利用行初等变换将估计出的编码参数 (l_i, m_i) 所对应的子模空间的**Gröbner**基化为上三角形式，根据 $k_{bi} = \sum_{i=1}^l (m_i - \partial g_u)$ 得到二进制信息位长 k_{bi} ，其中 ∂g_u 为对角线上元素的阶数，则码率 $R = k_{bi} / (m_i \times l_i)$ ，RS 码信息位长 $k = n_i \times R$ ；

[0017] 9) 分为以下两种情况：

[0018] I. 对于 RS 码，由估计出的参数 n_0 和 k 可确定生成多项式的根表达式

$$g(x) = \prod_{i=1}^T (x + \alpha'),$$
 其中 $T = n - k$ ；然后根据之前步骤 8) 中估计出的编码参数 (l_i, m_i, k) ，遍历编码维数 m_i 下的本原多项式得到本原多项式的估计值，代入 $g(x) = \prod_{i=1}^T (x + \alpha')$ 得到生成多项式估计值；

[0019] II. 对于准循环 LDPC 码，根据之前步骤中估计出的编码参数 (l_i, m_i, k) ，得到校验矩阵的维数 $H = (A_{ij})$ ，其中 A_{ij} 为维数为 $m_i \times m_i$ 的循环移位单位阵或稀疏方阵，且 H 的行重满足 $w_{Hamming}(H_{row}) \leqslant 0.25m_i$ ，（稀疏性），根据此限制条件对该码的对偶空间进行搜索得到校验矩阵 H 的估计值 H_{est} 。

[0020] 本发明的有益效果是，在同等误码率条件下运算复杂度低，在识别码长的同时可以识别出信息位长，且所需数据量低，特别适用于智能通信、无线电检测以及非合作通信领域的信道编码识别。

附图说明

- [0021] 图 1 :准循环码编码参数盲识别方法流程图
 [0022] 图 2 :准循环码变换子模空间的构造

具体实施方式

[0023] 本发明的原理是利用准循环码的代数结构特性对其编码参数进行盲识别与估计。下面结合附图和具体实施例,进一步阐述本发明。这些实施例应理解为仅用于说明本发明而不同于限制本发明的保护范围。在阅读了本发明记载的内容之后,本领域技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明权利要求所限定的范围。

[0024] 实施例 :

[0025] 以本原多项式为 $\text{prim_poly}=x^4+x+1$ 的 $(15, 11)$ RS 码为例。其编码域维数 $\dim=4$ 且对应的二进制码长为 60, 生成多项式为 $\text{gen_poly}=x^4+13x^3+12^2+8x+7$ 。比特误码率 (BER) $P_e=0.001$; 截获数据流长度 $L=20500\text{bits}$ 。

[0026] 识别步骤如下 :

[0027] 1) 设需要遍历的码长 n 范围为 $\{n=2^m - 1, 3 \leq m \leq 8\}$ 以及当前码长 $n_0=7$;

[0028] 2) 按照当前码长 n_0 对应的二进制码长 $n_{b0}=21$ 将截获的准循环码数据流进行分组, 得到 $N=10$ 组准循环码数据;

[0029] 3) 由于是 RS 码, 该码长下可能的准循环码移位因子 l_i 和分块个数 m_i 只有 1 组, 即 $l_i=3, m_i=7$;

[0030] 4) 根据 $l_i=3, m_i=7$ 对 $N=10$ 组码字进行 $m_i \times l_i$ 维重排, 即按行写入 $m_i \times l_i$ 维矩阵。得到 10 个数据矩阵 $c_i, i=1, 2, \dots, 10$; 然后分别将 10 个数据矩阵按列读出并按照由低到高的阶数顺序转化为多项式形式, 得到 10 个 R^3 上的 R - 子模, 其中 $R=F[x]/\langle x^7+1 \rangle$, 如下所示: $\{x^3+x^4+x^5+1, x^2+x^3+1, x+x^5+1\} \{x+x^2+x^6, x^2+x^3+x^4+x^6, x^1+x^3+x^4\} \dots \dots \{x^3+x^3+x^3+1, x^3+x^3+1, x^3+x^3+1\}$;

[0031] 5) 利用计算机代数系统求取步骤 3) 中 10 个 R^1 上 R - 子模构成的子模空间的 Gröbner 基, 记录其中单位基 e_i 的个数为 3;

[0032] 6) 判断当前码长是否遍历完毕码长范围; 如否, 更新当前码长 n_0 , 返回步骤 2), 如是, 进入步骤 8); ,

[0033] 7) 当达到搜索上限时, 根据之前步骤的记录, 可得当 $n_i=15$ 即 $l_i=4, m_i=15$ 时, 对应子模空间的 Groebner 基中含单位基 e_i 个数最少, 为 0:

$$[0034] \begin{bmatrix} x^2 + 1 & x^4 + x^3 + x^2 + x & x^3 + x^1 + 1 & x^3 + x^2 + 1 \\ x^3 + x^2 + 1 & x^2 + 1 & x^4 + x^3 + x^2 + x & x^2 + x \\ x^4 + x^3 & x^2 + x & x^3 + x^2 + 1 & x^4 + x^3 + x^2 + 1 \\ x^5 + x^3 + x & x^2 + x & x^3 + x^2 + 1 & x^2 \end{bmatrix}$$

[0035] 因而将该子模空间所对应的编码参数 ($l_i=4, m_i=15$) 作为盲估计的编码参数。

[0036] 8) 利用行初等变换将估计出的编码参数 (l_i, m_i) 所对应的子模空间的 Gröbner 基化为上三角形式:

$$[0037] \quad \begin{bmatrix} x^8 + x^4 + x^2 + x + 1 & x^7 + x^4 + x^3 + x^2 + x & x^7 + x^6 + x^4 + 1 & x^5 + x^4 + x^2 \\ 0 & x^4 + x^3 + 1 & 0 & x^3 + x^2 + 1 \\ 0 & 0 & x^4 + x^3 + 1 & x^2 + 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

[0038] 根据 $k_{bi} = \sum_{i=1}^l (m_i - \partial g_u) = (15-7)+(15-4)+(15-4)+(15-0) = 44$, 得到码率为

$R=44 / 60=11 / 15$, 则 RS 码的信息位长 $k=n_i \times R=11$;

[0039] 9) 遍历估计出的 RS 码编码域维数 $\dim=4$ 下所有本原多项式, 得到估计本原多项式为 $\text{prim_poly}_i=x^4+x+1$; 根据估计出的码长和信息位长 ($n_i=15$, $k_i=11$) 可知生成多项式的形式为: $g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$, 代入本原多项式后即得到生成多项式的估计值 $\text{gen_poly}_i=x^4+13x^3+12^2+8x+7$;

[0040] 至此完成容错码的 RS 码编码参数盲估计。

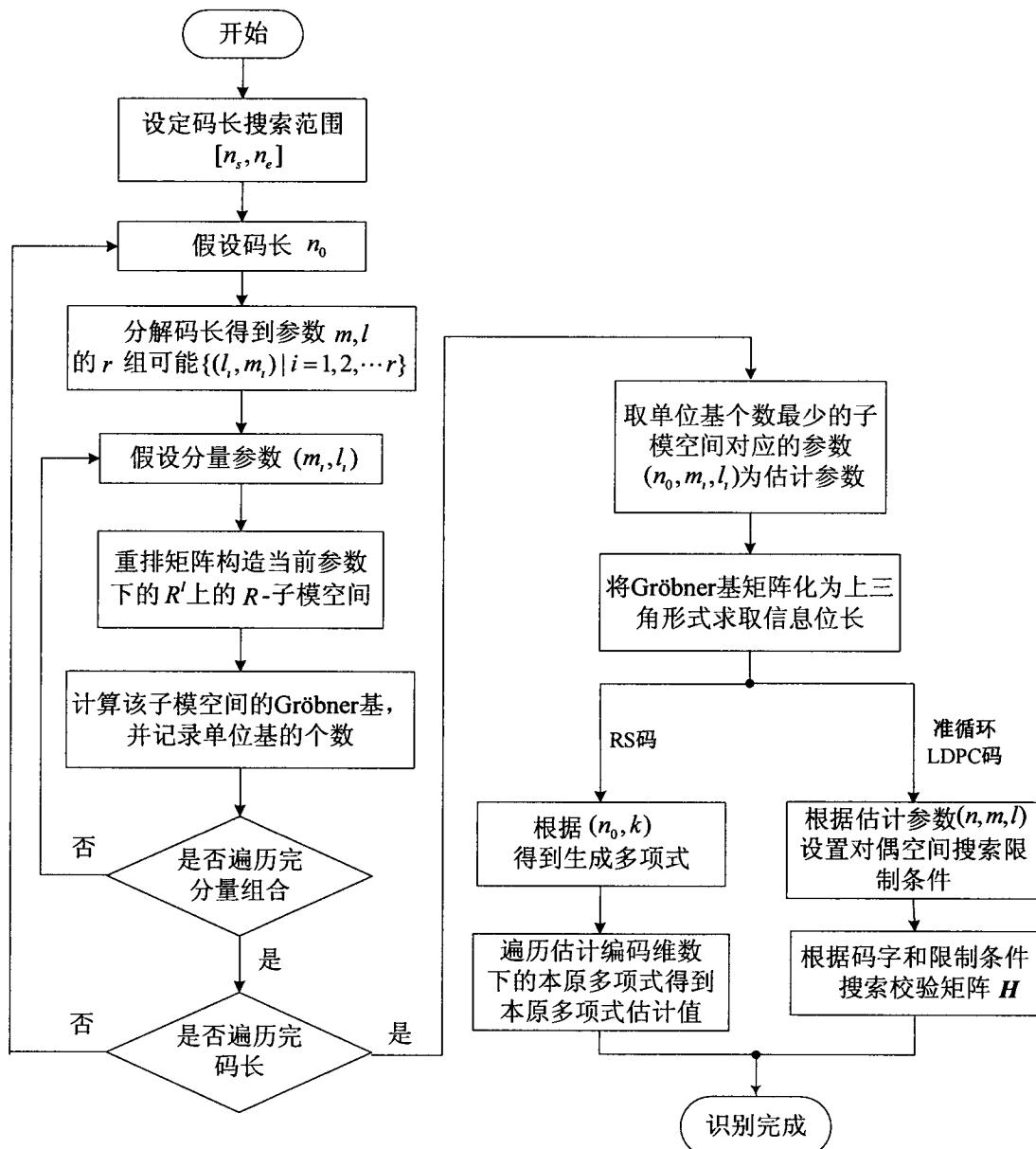


图 1

$$\mathbf{c} = (c_{0,0}, c_{0,1}, \dots, c_{0,l_i-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l_i-1}, \dots, c_{m_i-1,0}, c_{m_i-1,1}, \dots, c_{m_i-1,l_i-1})$$

↓ 按行写入

$$\mathbf{c}_{m_i \times l_i} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,l_i-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,l_i-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m_i-1,0} & c_{m_i-1,1} & \cdots & c_{m_i-1,l_i-1} \end{bmatrix}$$

↓ 按列取出

$$\mathbf{c}_{new} = (c_1(x), c_2(x), \dots, c_{l_i}(x)) \quad \text{其中 } c_i(x) = \sum_{k=0}^{m_i-1} c_{k,i} x^{k-1}$$

图 2