文章编号:1001 - 2486(2011)04 - 0123 - 05

一种 RS 码快速盲识别方法※

吕喜在,苏绍璟,黄芝平
(国防科技大学 机电工程与自动化学院,湖南 长沙 410073)

摘　要:为了获取数字通信中未知线路的纠错编码信息,提出了一种 RS 码快速盲识别方法。通过对 RS 码的二进制表示进行码根求解的方法来检测未知线路的 RS 码长、本原多项式阶数以及可能的本原多项式;进而遍历得到的本原多项式对 RS 序列进行伽罗华域的傅里叶变换(GFFT),通过连零位置和个数最终确定未知线路的真实本原多项式和生成多项式。实验验证和性能分析表明,该方法能实现绝大部分未知线路的 RS 码盲识别,并明显缩小以往算法中本原多项式的遍历范围。

关键词:RS 码;有限域;多项式根;本原多项式;盲识别
中图分类号:TN97　　**文献标识码:**A

A Fast Blind Recognition Method of RS Coding

LV Xi-zai, SU Shao-jing, HUANG Zhi-ping
(College of Mechatronics Engineering and Automation, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: In order to get the error-correcting coding information of the unknown lines in digital communication, a fast blind recognition method of Reed-Solomon(RS) coding is presented. RS coding length, the order of the primitive polynomial and the possible primitive polynomials were detected by seeking the roots of binary form of RS codes. The true primitive polynomial and generator polynomial of the unknown line were gained by the position and number of the connective zeros in the Galois Fields Fourier Transform (GFFT) of RS codes using the possible primitive polynomials. The results of experiments and performance analysis show that this method can blind recognize the RS coding of the great mass of unknown lines, and can obviously reduce the number of primitive polynomials searched in the recognition compared with the existing algorithms.

Key words: RS codes; finite fields; polynomial roots; primitive polynomial; blind recognition

RS 码是一类具有很强的可纠正随机错误和突发错误能力的多进制 BCH 码,在线性分组纠错码中占有非常重要的地位。自从 1960 年由 Reed 和 Solomon 构造出以来,RS 码已在密码学、数字通信以及数据存储领域中得到了广泛的应用[1-3]。

在通信对抗或智能通信领域中,纠错编码的盲识别至关重要。然而,当前国内外对这一领域的研究主要集中于卷积码的盲识别[4-7],针对线性分组纠错码盲识别的文献非常少见。文献[8]较早地提出了 BCH 码、RS 码的盲识别问题,但并没有给出具体的解决方法。文献[9]首次对有限域上 RS 码的二进制映射特性进行了深入研究,得出了很多有意义的结论。文献[10]分别讨论了长、短码长以及高、低误码率等不同情况下的 RS 码的盲识别问题,但就实际未知线路的全盲检测(即码长的长短和线路误码率的高低均未知)而言,其长码长高误码率情况下的基于伽罗华域的傅里叶变换(简称 GFFT)方法最有应用价值。其核心思想是通过对接收序列遍历本原多项式进行 GFFT 来识别本原多项式、码长及生成多项式。但文献[10]只验证了该方法的有效性及容错性,而没有考虑方法实现的计算复杂度。实际上,由于本原多项式的个数随着其阶数的增加会急剧增多[11],当未知线路 RS 码的本原多项式阶数较高时,因遍历本原多项式对 RS 序列进行 GFFT 而带来的计算量也会急剧增加。

在继承文献[9,10,13]所取得的部分成果的基础上,本文通过对 RS 码的二进制表示求公共码根的方法,先识别 RS 码的码长和可能的本原多项式,然后利用 GFFT 法遍历少数本原多项式求取生成多项式,最终实现 RS 码的快速盲识别。

1　RS 码盲识别问题描述

定义 1[12]　码元与其生成多项式的根均取自

※ **收稿日期:**2010 - 02 - 15
作者简介:吕喜在(1981—),男,博士生。

$GF(q)$(q 为素数或素数的幂)上,码长 $n=q-1$ 的本原 BCH 码称为 RS 码。

在数字通信领域,$q=2^m$,m 为生成 $GF(q)$的本原多项式 $p(x)$的阶数。由 BCH 码的定义和性质可知,(n,k)RS 码的生成多项式满足:

$$g(x)=(x+\alpha^{m_0})(x+\alpha^{m_0+1})\cdots(x+\alpha^{m_0+n-k-1}) \quad (1)$$

其中,α 是 $GF(q)$中的 n 级元素,m_0 通常为 1,即

$$g(x)=(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{n-k}) \quad (2)$$

当获取到某未知线路传输的信息后,通过帧同步信息的检测,很容易确定 RS 码分组的正确起点。因此,本文所研究的 RS 码的盲识别问题与文献[10]描述的一样,即在分组起点已知的条件下,通过对码字序列的分析处理,最终识别 RS 码的本原多项式 $p(x)$、码长 n 和生成多项式 $g(x)$。

2 RS 码的 GFFT

定义 2[12] 设 $GF(q)$上的多项式

$$a(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \quad a_i\in GF(q) \quad (3)$$

则它在 $GF(q)$上的谱多项式(也称为 Mattson-Solomon(MS)多项式):

$$A(z)=A_{n-1}z^{n-1}+\cdots+A_1z+A_0=\sum_{j=0}^{n-1}A_jz^j \quad (4)$$

其中 $A_j=\sum_{i=0}^{n-1}a_i\alpha^{ij}$,$j=n-1,\cdots,1,0$,$\alpha$ 是$GF(q)$中的 n 级单位本原根,$\alpha^n=1$。$A=(A_{n-1},\cdots A_1,A_0)$称为 $a=(a_{n-1},\cdots,a_1,a_0)$在 $GF(q)$上的离散傅里叶变换。

定理 1[12] 多项式 $a(x)$以 α^j 为根的充要条件是其谱多项式的第j 个分量A_j 等于零。

定理 2[10] 对(n,k)RS 码作 $GF(q)$上的 GFFT,A 中至少有 $n-k$ 个连零。

文献[10]针对长码长高误码条件下的 RS 码的盲识别方法正是依据定理 2 展开的。先选定较小的本原多项式阶数 m',然后按照长度 $n'=2^{m'}-1$ 将 RS 码序列分成 N 组,遍历 m'阶本原多项式进行 GFFT。考虑到误码影响,当发现 $r(r\leqslant N)$组码字变换后具有相同的连零位置且个数相同时,则判断此时选取的本原多项式为未知线路 RS 码的本原多项式 $p(x)$,由 $p(x)$的阶数也就同时得到了 RS 码的长度为 $n'=2^{m'}-1$,最后根据定理 1 和式(1)即可得到 $g(x)$。如果没有发现连零现象,则 m'递增 1,重复以上步骤,直到识别成功。为便于描述,简称该方法为 GFFT 法。

该方法成功地解决了 RS 码盲识别的容错性问题,但是由于需要遍历本原多项式进行 GFFT,所以如果未知线路 RS 码的 $p(x)$阶数较高,整个识别过程涉及的计算量会很大。

3 RS 码的二进制表示及其特性

定理 3[9] 设 $\boldsymbol{V}$ 是由$GF(2^m)$上的 $k\times n$ 阶生成矩阵 $\boldsymbol{G}$ 生成的(n,k)RS 系统码,则 V 的二进制向量表示(mn,mk)是 $GF(2)$上由 $\boldsymbol{G}'$生成的线性分组码。

(n,k)RS 系统码的 $k\times n$ 阶生成矩阵$\boldsymbol{G}$ 的第 i 行的多项式可表示为

$$g(i)=x^{n-i}+\sum_{j=1}^{n-k}a(i,j)x^{j-1},i=1,2,\cdots,k \quad (5)$$

其中 $a(i,j)\in GF(2^m)$为 $\boldsymbol{G}$ 中第i 行,倒数第j 列元素。不妨设 $a(i,j)=\alpha^{f(i,j)}$,$f(i,j)=0,1,\cdots,2^m-1$,α 是 $GF(2^m)$中的 2^m-1 级单位本原根。另外,由循环码的性质可知,$g(i)$还满足:

$$g(i)=x^{n-i}+x^{n-i}\bmod g(x),i=1,2,\cdots,k \quad (6)$$

显然 $g(i)$可以被 $g(x)$整除,特别当 $i=k$ 时,由于 $g(x)$的阶数为 $n-k$,所以有

$$g(k)=x^{n-k}+x^{n-k}\bmod g(x)=g(x) \quad (7)$$

$\boldsymbol{G}'$可由 $\boldsymbol{G}$ 映射而成,具体的映射规则是[9]:$\boldsymbol{G}$ 中的第 i 行映射为 $\boldsymbol{G}'$中的第 $mi-m-1\sim mi$ 行,且 $\boldsymbol{G}'$的第 $mi-l$ 行的多项式表示满足

$$g'(i,l)$$
$$=x^{m(n-i)+l}+\sum_{j=1}^{n-k}[x^{f(i,j)+l}\bmod p(x)]\cdot x^{m(j-1)} \quad (8)$$

其中 $l=0,1,\cdots,m-1$。

定理 4 如果(n,k)RS 系统码的生成多项式 $g(x)$的 $n-k$ 个根中包含α^m,则(n,k)RS 码的二进制向量表示(mn,mk)对应的多项式 $c'(x)$一定能被 $p(x)$整除。

证明 设与 $c'(x)$对应的二进制信息码为 $d'=(d_1,d_2,\cdots,d_{mk})$,则由线性分组码定义可知

$$c'(x)=\sum_{i=1}^{k}\sum_{l=0}^{m-1}d_{mi-l}g'(i,l) \quad (9)$$

显然,只要能证明 $\boldsymbol{G}'$的每一行的多项式表示均能被$p(x)$整除,也就证明了定理 4。

$g(i)$可以被 $g(x)$整除,而 $g(x)$的根又包含 α^m。所以 $g(i)$肯定可以被 $x+\alpha^m$ 整除,于是,不妨设

$$g(i)=(x+\alpha^m)(x^{n-i-1}+\sum_{j=1}^{n-i-1}b(i,j)x^{j-1}) \quad (10)$$

其中 $b(i,j)\in GF(2^m)$,不妨设 $b(i,j)=\alpha^{s(i,j)}$,$s(i,j)=0,1,\cdots,2^m-1$,α 是 $GF(2^m)$中的 2^m-1 级单位本原根。将式(10)整理,得

$$
\begin{aligned}
& g(i) \\
&= x^{n-i}+b(i,1)\alpha^m+\sum_{j=1}^{n-i-2}[b(i,j+1)\alpha^m+ \\
&\quad b(i,j)]x^j+[\alpha^m+b(i,n-i-1)]x^{n-i-1}
\end{aligned}
\tag{11}
$$

根据式(8),将式(11)映射到 $GF(2)$中,得

$$
\begin{aligned}
& g'(i,l) \\
&= x^{m(n-i)+l}+x^{s(i,1)+m+l}\bmod p(x) \\
&\quad +\sum_{j=1}^{n-i-2}[(x^{s(i,j+1)+m+l}+x^{s(i,j)+l})\bmod p(x)]\cdot x^{mj} \\
&\quad +[(x^{m+l}+x^{s(i,n-i-1)+l})\bmod p(x)]x^{m(n-i-1)}
\end{aligned}
\tag{12}
$$

将上式各项分解、重新组合得

$$
\begin{aligned}
g'(i,l) &= [x^{m+l}+x^{m+l}\bmod p(x)]x^{m(n-i-1)+l} \\
&\quad +\sum_{j=1}^{n-i-1}\{[x^{s(i,j)+l}\bmod p(x)]\cdot x^{mj} \\
&\quad +[x^{s(i,j)+m+l}\bmod p(x)]x^{m(j-1)}\}
\end{aligned}
\tag{13}
$$

上式中第一项显然可以被 $p(x)$整除,而在二元域中,第二项求和公式的每一项等价于

$$
\begin{aligned}
& [x^{s(i,j)+l}+x^{s(i,j)+l}\bmod p(x)]x^{mj}+x^{s(i,j)+l+mj} \\
&\quad +[x^{s(i,j)+m+l}+x^{s(i,j)+m+l}\bmod p(x)]x^{m(j-1)} \\
&\quad +x^{s(i,j)+m+l+m(j-1)} \\
&=[x^{s(i,j)+l}+x^{s(i,j)+l}\bmod p(x)]x^{mj} \\
&\quad +[x^{s(i,j)+m+l}+x^{s(i,j)+m+l}\bmod p(x)]x^{m(j-1)}
\end{aligned}
\tag{14}
$$

其中 $j=1,2,\cdots,n-i-1$,显然式(14)也可以被 $p(x)$整除,因此,式(13)可以被 $p(x)$整除。结合式(9),定理得证。

4　RS 码快速盲识别方法

定理 4 为 RS 码的本原多项式 $p(x)$的盲识别提供了一种新的途径,即对满足定理 4 条件的多组 RS 码的二进制表示进行码根求解,其公共根中必然含有 $p(x)$的 m 个共轭根,再由共轭根即可得出本原多项式。另外,根据有限域同构的原理,设由不同的 m 阶本原多项式 $p_1(x)$和 $p_2(x)$产生的有限域分别为 $GF_1(2^m)$和 $GF_2(2^m)$,则 $c'(x)$(或 $p(x)$)在 $GF_1(2^m)$中的根与在 $GF_2(2^m)$中的根虽然不一定相同,但必然存在一一对应的关系,即根数是相等的。这也正是文献[13]在码长识别过程中可以简化的理论依据。

进一步,设 $p(x)$在 $GF_1(2^m)$中求得的根为 $\beta=\{\beta_1,\beta_2,\cdots,\beta_{n-k}\}$,而在 $GF_2(2^m)$中求得的根为 $\gamma=\{\gamma_1,\gamma_2,\cdots,\gamma_{n-k}\}$。则根据有限域根的定义,在 $GF_1(2^m)$中根据 $p_1(x)$化简$(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{n-k})$必然得 $p(x)$;而在 $GF_2(2^m)$中根据 $p_2(x)$化简$(x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_{n-k})$必然也得 $p(x)$。所以,针对 RS 码的二进制,可任意选择一个 m 阶本原多项式$p_i(x)$,在由 $p_i(x)$所生成的有限域 $GF_i(2^m)$中求取公共码根并进行随后的乘积与化简,均会得到系数属于 $GF(2)$的 m 阶多项式$p(x)$。

基于以上考虑,给出满足定理 4 条件的 RS 码的盲识别方法(简称 RS 码快速盲识别方法):

(1)先选定较小的本原多项式的阶数 m',然后按照长度 $n'=2^{m'}-1$ 将 RS 码序列分成 N 组并转换为二进制表示,任选 m'阶本原多项式$p'(x)$在由 $p'(x)$生成的有限域 $GF(2^{m'})$中进行码根求解,如果存在明显的公共根,即可确定 RS 码的码长和本原多项式的阶数,同时由公共根中的 m'个共轭根在$GF(2^{m'})$中通过有限域乘法即可得到 m'阶本原多项式。如果没有明显的公共根,将 m'递加 1,重复以上步骤。

(2)遍历(1)中得到的本原多项式对 N 组长为$n'=2^{m'}-1$ 的 RS 码进行 GFFT,通过观察连零现象,即可最终确定未知线路 RS 码的本原多项式,并求出生成多项式。

步骤(1)中判断 RS 码二进制表示是否存在公共根以及码根的求解采用文献[13]中的码根信息差熵方法完成。对于不满足定理 4 条件的 RS 码的盲识别仍然采用文献[10]中的 GFFT 法。

在实际的数字通信中,绝大部分 RS 编码是满足定理 4 条件的,尤其当本原多项式阶数较高时。对于(n,k)RS 码而言,由步骤(2)可知,要想满足定理 4 条件,需有

$$n-k\geqslant m \tag{15}$$

将 $n=2^m-1$ 代入上式,整理得

$$k\leqslant 2^m-m-1 \tag{16}$$

表 1　RS 码快速盲识别方法的适用范围

Tab.1　Applicability of the fast blind recognition method of RS coding

m	3	4	5	6	7	8	9	10
n	7	15	31	63	127	255	511	1023
$k\leqslant$	4	11	26	57	120	247	502	1013
η/%	57.1	73.3	83.9	90.5	94.5	96.9	98.2	99.0

表 1 给出了 RS 码快速盲识别方法的适用范围,$\eta=(2^m-m-1)/(2^m-1)\times100\%$ 表示 RS 码快速盲识别方法的适用率。

5 有效性验证与性能分析

5.1 RS 码快速盲识别方法实验验证

模拟产生足够长的(31,17)RS 编码的未知线路数据,本原多项式设定为 $p(x)=x^5+x^2+1$,误码率为 $p_e=1\times10^{-2}$。当 m' 取 4,本原多项式 $p'(x)$取 x^4+x+1 时,对模拟数据截取 100 组长为 15×4 比特的数据,在由 x^4+x+1 生成的 $GF(2^4)$中进行二进制表示的码根求解,结果如图 1 所示,显然无明显共轭根,表明当前本原多项式的阶数和 RS 码码长估计不正确。

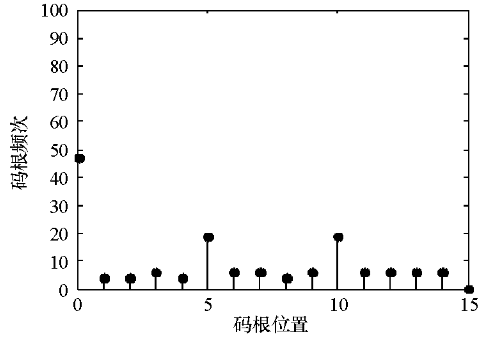

图 1 二进制码根求解($m'=4$)

Fig.1 Roots of binary form of RS codes($m'=4$)

m'取 5,本原多项式分别取如下六种情况:$p_1(x)=x^5+x^2+1$、$p_2(x)=x^5+x^4+x^2+x+1$、$p_3(x)=x^5+x^4+x^3+x^2+1$、$p_4(x)=x^5+x^3+1$、$p_5(x)=x^5+x^4+x^3+x+1$、$p_6(x)=x^5+x^3+x^2+x+1$。对模拟数据截取 100 组长为 31×5 比特的数据,分别在由各本原多项式生成的 $GF(2^5)$中进行二进制表示的码根求解,结果如图 2 所示。

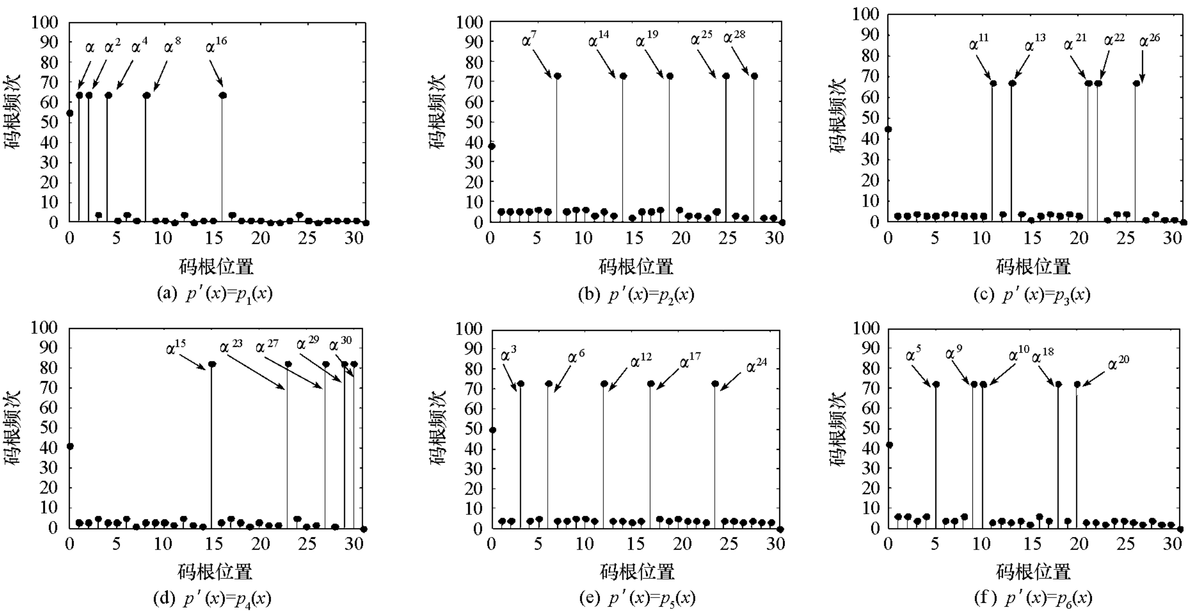

图 2 二进制码根求解($m'=5$)

Fig.2 Roots of binary form of RS codes($m'=5$)

从图 2 可见明显有共轭根存在,由此可判断出未知线路本原多项式的阶数 $m=5$,码长 $n=31$。接着,对图 2 中得到的共轭根分别在由$p_1(x)\sim p_6(x)$生成的 $GF(2^5)$中进行有限域乘法并化简,均有$(x+\beta_{i1})(x+\beta_{i2})\cdots(x+\beta_{i5})=x^5+x^2+1, i=1,2,\cdots,6$。其中 $\beta_{ij}\in GF(2^5)$,表示利用$p_i(x)$对 RS 码二进制表示进行码根求解得到的共轭根。

该实验结果表明,采用任意一种 5 阶本原多项式对(31,17)RS 码的二进制表示进行码根求解,均能得到真实的本原多项式 $p(x)$。当然对于低码率的 RS 码通过码根求解可能会得到多个本原多项式,但其中必然包括 $p(x)$,而且其个数不会超过所有 m 阶本原多项式的数目。

在检测出未知线路可能的本原多项式后,遍历这些多项式对 RS 码进行 GFFT,通过连零个数和位置即可得到未知线路的生成多项式,这一点文献[10]已做验证,这里不再重复。

5.2 RS 码快速盲识别方法性能分析

本文提出的 RS 码快速盲识别方法,与文献[10]中的 GFFT 法相比,不同之处主要体现在两个方面:首先,当遍历的本原多项式阶数 m'小于真实的阶数 m 时,新方法针对每个阶数只需任意选取一个 m'阶的本原多项式进行码根求解,而 GFFT 法需要遍历所有的 m'阶本原多项式进行 GFFT;其次,当 $m'=m$ 时,新方法只需遍历前面步骤求得的数个(实验发现,对于满足 $k\geqslant n/2$ 的 RS 码,只有一个)m 阶本原多项式,而 GFFT 仍需

遍历所有 m 阶本原多项式。

通过以上分析,不难发现:新方法与 GFFT 法的计算复杂度和时间复杂度主要由本原多项式的遍历次数和每次遍历所进行的核心运算(二进制码根求解或 GFFT)决定。

表 2 给出了遍历不同阶本原多项式所进行的二进制码根求解与 GFFT 的耗时对比(实验平台为 Inter 双核计算机,主频 1.8GHz,内存 2G 字节),参与运算的数据都为 100 组。结果表明,两种核心运算的耗时相差不明显,处于同一数量级。

表 2　不同阶本原多项式下的核心运算耗时比对(ms)

Tab.2　Comparisons of time-consumed in core-operation with different order of primitive polynomial (ms)

m	3	4	5	6	7	8	9	10
求码根	10	20	40	110	319	883	3392	12 006
GFFT	10	20	40	100	251	802	2992	10 965

表 3 和表 4 分别给出了低码率($k < n/2$)和高码率($k \geqslant n/2$)下新方法与 GFFT 法识别 RS 码所需核心运算的次数,假设均从 $m' = 3$ 开始遍历。

表 3　低码率情况下识别 RS 码所需核心运算次数比对

Tab.3　Comparisons of core-operation times in RS recognition with low code rate

m		3	4	5	6	7	8	9	10
n		7	15	31	63	127	255	511	1023
k		3	7	15	31	63	121	151	121
遍历次数	GFFT 法	–	2	4	10	16	34	50	98
$m' < m$	新方法	–	1	2	3	4	5	6	7
遍历次数	GFFT 法	2	2	6	6	18	16	48	60
$m' = m$	新方法	2	1	2	1	2	1	8	48

表 4　高码率情况下识别 RS 码所需核心运算次数比对

Tab.4　Comparisons of core-operation times in RS recognition with high code rate

m		3	4	5	6	7	8	9	10
n		7	15	31	63	127	255	511	1023
k		5	9	17	33	65	129	257	513
遍历次数	GFFT 法	–	2	4	10	16	34	50	98
$m' < m$	新方法	–	1	2	3	4	5	6	7
遍历次数	GFFT 法	2	2	6	6	18	16	48	60
$m' = m$	新方法	*	1	1	1	1	1	1	1

注:"–"表示从 $m' = 3$ 开始遍历,"*"表示不满足定理 4 条件

可见,GFFT 法的运算次数与码率高低无关,在 $m' < m$ 时,运算次数为 $\sum_{m'=3}^{m-1} \varphi(2^{m'} - 1)/m'$,$\varphi()$ 为欧拉函数;在 $m' = m$ 时,运算次数为 $\varphi(2^m - 1)/m$。新方法在 $m' < m$ 时,遍历的次数与码率高低也无关,均为 $m - 1$;而在 $m' = m$ 时,高码率条件下只需遍历 1 次,在低码率情况下,运算次数通常少于 GFFT 法,最坏情况下等于 GFFT 法。

综上所述,在定理 4 条件下,本文提出的 RS 码快速盲识别方法在计算复杂度和识别时间等性能方面明显优于 GFFT 法。当然,如果未知线路不满足定理 4 条件,本文提出的 RS 码快速盲识别方法将失效,此时只能借助于 GFFT 法进行识别。但这种情况毕竟属于少数,由表 1 可知,如果 k 太接近于 n,也就意味着该 RS 编码的检错和纠错能力很弱,其应用范围必然很窄。

6　结束语

根据 RS 码的二进制表示所具有的结构和性质,本文提出了一种 RS 码快速盲识别方法。相比于已有的 GFFT 法,新方法在识别过程中所需遍历的本原多项式数目大大减少,从而可以明显减少计算量和识别时间。虽然新方法的应用需要满足一定的条件,但分析表明:该方法能适应大多数 RS 码的盲识别,特别当 RS 码的码长不小于 63 时,其适用率可达 90%以上。

参 考 文 献:

[1] Albanese M, Spalvieri A. Two Algorithms for Soft-decision Decoding of Reed-solomon Codes, with Application to Multilevel Coded Modulations[J]. IEEE transactions on Communications, 2008, 56(10): 1569 – 1574.

[2] Yuan B, Sha J, Li L, et al. High-speed Reed-solomon Errors-and-erasures Decoder Design with Burst Error Correcting[C]//2009 IEEE 8th International Conference on ASIC, Changsha, 2009: 485 – 488.

[3] Claus B, Jiang W Y. Optimal Choice of Reed-solomon Codes to Protect Against Queuing Losses in Wireless Networks [J]. The Journal of China Universities of Posts and Telecommunications, 2009, 16(3): 71 – 83.

[4] Lu P Z, Shen L, Luo X Y, et al. Blind Recognition of Punctured Convolutional Codes [C]//IEEE International Symposium on Information Theory, Shanghai: IEEE Press, 2004: 457.

[5] Lu P Z, Shen L, Zou Y. Blind Recognition of Punctured Convolutional Codes[J]. Science in China Ser F Information Sciences, 2005, 48(4): 484 – 498.

[6] Wang F H, Huang Z T, Zhou Y Y. A Method for Blind Recognition of Convolution Code based Euclidean Algorithm [C]//IEEE International Conference on Wireless Communications, Shanghai: IEEE Press, 2007: 1414 – 1417.

[7] 刘健,王晓君,周希元. 基于 Walsh-Hadamard 变换的卷积码盲识别[J].电子与信息学报,2010: 32(4): 884 – 888.

[8] 柴先明,黄知涛,王丰华,等.信道编码盲识别问题研究[J].通信对抗,2008,(2): 33 – 36.

[9] 刘玉君,严玉平.有限域上 RS 码特征的研究[J]. 信息工程大学学报,2007,8(1): 64 – 67.

[10] 刘健,谢锘,周希元. RS 码的盲识别方法[J]. 电子科技大学学报,2009,38(3): 363 – 367.

[11] 郭鑫,陈克非.求解本原多项式的快速算法[J].计算机工程,2008,34(15): 146 – 147.

[12] 王新梅,肖国镇. 纠错码 – 原理与方法[M]. 修订版. 西安:西安电子科技大学出版社,2001: 178 – 260.

[13] 杨晓静,闻年成.基于码根信息差熵和码根统计的 BCH 码识别方法[J].探测与控制学报,2010,32(3): 69 – 73.