

符合 CCSDS 标准的 RS(255, 223) 码译码器的 FPGA 实现及其性能测试^{*}

石俊峰^{1,3} 王 宇² 孙辉先¹

¹(中国科学院空间科学与应用研究中心 北京 100080)

²(中国科学院光电研究院)

³(中国科学院研究生院)

摘 要 RS(Reed-Solomon) 码是差错控制领域中一种性能优异的非二进制分组循环码, 由于它具有很强的随机错误和突发错误的纠错能力, 被 CCSDS, NASA, ESA 等空间组织接受, 广泛应用于深空探测中. 本文采用改进的 Berlekamp 算法, 用 FPGA 实现了符合 CCSDS 标准的 RS(255, 223) 码译码器; 介绍了该译码器的实现流程、性能测试方法和基于 PCI 总线接口的测试平台; 给出了测试结果, 并且对理论上 RS(255, 223) 译码器的误码性能与实际测试的误码率结果进行了比较和分析. 验证结果证明该译码器能工作在 400 Mbps 以上的码率, 使用 FPGA 资源 180 000 门, 译码效果与理论上译码效果一致.

关键词 CCSDS; Reed-Solomon 码; FPGA; 性能测试; PCI 总线

中图法分类号 V 557

The Implementation and Verification of RS(255, 223) Decoder According to CCSDS Specification

SHI Junfeng^{1,3} WANG Yu² SUN Huixian¹

¹(Center for Space Science and Applied Research, The Chinese Academy of Sciences, Beijing 100080)

²(Academy of Opto-Electronics, The Chinese Academy of Sciences)

³(Graduate School, The Chinese Academy of Sciences)

Abstract A RS(Reed-Solomon) code is an excellent linear cyclic block code in the error control field. It has found widespread use in deep space exploration and has been adopted by the spatial organizations such as CCSDS, NASA, ESA for its powerful random and burst error correcting ability. The research project adopts a new reformulated inversionless BM (Berlekamp-Massey) algorithm to fulfill a RS(255, 223) decoder according to CCSDS specification. In this paper, the algorithm, verification method and the verification platform based on PCI bus interface of the RS(255, 223) decoder have been introduced. The experiment result and the comparison of the theoretic and testing error probability of the decoder have been mentioned. The test result proves the complexity of the proposed decoder is only about 180 000 gates and has a throughput of 400 Mbps using FPGA. The error correcting ability of the decoder is normal.

Key words CCSDS, RS code, PCI bus, FPGA, Verification

^{*} 国家嫦娥工程有效载荷数管系统预研课题资助

2004-12-08 收到原稿, 2005-04-20 收到修定稿

1 引言

卫星通信系统传输数据的距离非常远, 受衰落、噪声和各种干扰的影响比较严重. 而卫星的体积和重量又约束了信号能量, 这种情况下, 为了保证远距离传输的误码率在允许范围之内, 必须采用纠错能力很强的差错控制方法来进行纠错. RS(Reed-Solomon) 码是差错控制领域中一类很重要的线性分组码. 由于它具有很强的纠正随机错误和突发错误能力以及具有极低的未探测差错率, 所以在深空卫星通信、军用通信、计算机通信、存储介质、数字视频广播和各种网络中得到广泛应用. RS 码中一个研究的热点是 RS(255, 223) 码. 1987 年开始, 空间数据系统咨询委员会 (CCSDS) 将 RS(255, 223) 码作为常规分包遥测信道编码和高级在轨 (AOS) 前向和反向链路纠错编码的标准^[1]. 它对实现信道纠错编码低差错率起着关键作用. 美国宇航局 (NASA) 和欧洲空间局 (ESA) 在深空卫星通信的级联码系统中把 RS(255, 223) 码作为标准的外码使用. 目前国内航天领域已经在卫星上使用了 RS(255, 223) 硬件编码器进行编码, 地面上应用 RS(255, 223) 软件译码器进行译码, 实时性要求得不到满足, 需要 RS(255, 223) 硬件译码器来解决这一问题. 同时我国深空探测的计划正在逐渐开展起来, 目前的差错控制系统很难满足这么远距离通信的要求. 另外, 虽然国外现在很多厂家都能生产 RS 译码器, 但是码率高的产品不仅很难购买而且价格昂贵. 这样, 按照 CCSDS 标准研制自主知识产权的 RS(255, 223) 硬件译码器就成为非常必要和有意义的工作.

2 基本原理和算法选择

RS 码是一种多进制 BCH(Bose-Chaudhuri-Hocquenghem) 码, 也是一类典型的代数几何线性循环码, 同时又是极大最小距离可分码 (MDS 码). 它的重量分布可以预知. 它与一般 BCH 码的主要区别在于它的符号域与计算域一致, 而一般 BCH 码的计算域大于符号域. 这在实际应用上表现为 RS 码按信息字处理数据, 而一般 BCH 码按信息位处理数据.

根据空间数据系统咨询委员会发布的《空间数据系统标准建议书》(CCSDS 蓝皮书)^[1], RS(255,

223) 码的参数如下.

(1) $m = 8$, 为 RS(255, 223) 码一个符号数表示的信息位数.

(2) $t = 16$, 为 RS(255, 223) 码一个码字内的所能纠正的最大错误符号数, m 和 t 为独立参数.

(3) $n = 2^m - 1 = 255$, 为 RS(255, 223) 码一个码字所包含的符号数.

(4) $2t$ 是 RS(255, 223) 码一个码字校验位的符号个数.

(5) $GF(2^8)$ 域上的生成多项式为

$$F(x) = x^8 + x^7 + x^2 + x + 1.$$

(6) 码生成多项式为

$$G(x) = \prod_{j=112}^{143} (x - \alpha^{11j}) = \sum_{i=0}^{32} G_i x^i.$$

在 $GF(2^8)$ 上定义, 其中 $F(\alpha) = 0$, α^{11} 为 $GF(2^8)$ 中的一个本原元素.

RS 译码器主要由校验子计算, 错误位置和错误值多项式计算, 错误位置计算和错误值计算, 以及错误模式与原来的输入向量进行模 4 部分组成 (见图 1). 其中错误位置和错误值多项式计算最为关键, 也称为关键方程的计算. Berlekamp-Massey (BM) 算法和 Euclid 算法译长码的性能较好, 有规则的结构且易于 VLSI 实现, 这些优点使其成为错误位置和错误值多项式计算的典型算法. BM 算法又可分为时域算法和频域算法. 频域算法由于能够在有限域中进行快速傅里叶变换, 因此译码速度高. BM 算法与 Euclid 算法的主要区别在于迭代过程, BM 迭代基于自回归滤波器综合原理, 求最短反馈连接多项式的代数迭代; Euclid 迭代则基于多项式分解原理, 求两多项式的最大公因式的迭代^[2]. BM 算法和 Euclid 算法一直在被不断地改进, 以提

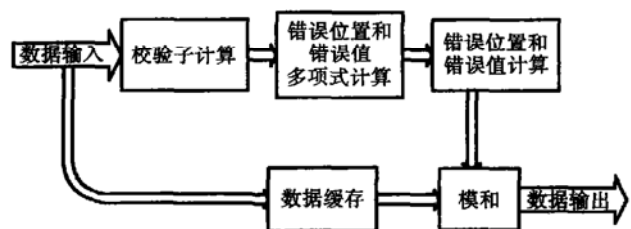


图 1 RS 译码器结构框图

Fig.1 Frame of RS decoder

高 RS 译码器的性能. 文献 [3] 提出的新改进的 RiBM 算法在关键路径延时和资源使用两方面与传统的 BM 和 Euclid 算法及其改进算法相比做到了更好的折中. 本文即采用该算法实现 RS 译码器, 其算法原理简述如下.

假设经过编码后的码字记为

$$C(x) = C_{254}x^{254} + C_{253}x^{253} + \cdots + C_1x + C_0,$$

译码器接译码后的码字记为

$$R(x) = R_{254}x^{254} + R_{253}x^{253} + \cdots + R_1x + R_0,$$

经过译码后获得的错误图样记为

$$E(x) = E_{254}x^{254} + E_{253}x^{253} + \cdots + E_1x + E_0.$$

$C(x)$, $R(x)$ 和 $E(x)$ 满足关系

$$C(x) = R(x) + E(x).$$

译码器的实现主要包括下面 4 个流程.

(1) 校验子 S_i 的计算.

$$S_i = (\cdots (((R_{n-1}\alpha^i + R_{n-2})\alpha^i + R_{n-3})\alpha^i + \cdots)\alpha^i + R_0).$$

其中, $n = 255$, $i = 1, 2, \cdots, 32$, α 为 $x^8 + x^7 + x^2 + x + 1 = 0$ 所生成的 $GF(2^8)$ 中的本原元^[4]. 其实现结构如图 2 所示.

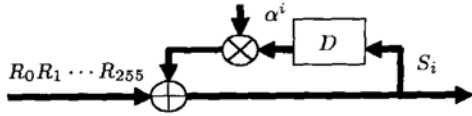


图 2 校验子计算模块

Fig.2 Computational module of syndrome values

(2) 采用 RiBM(Reformulated inversionless BM) 算法求取关键方程, 算法流程如下.

初始化 $\bar{\sigma}_{3t}(0) = 1$; $\bar{\sigma}_i(0) = 0$ for $i = 2t, 2t + 1, 2t + 2, \cdots, 3t - 1$ $k(0) = 1$; $\gamma(0) = 0$.

输入: S_i , $i = 0, 1, 2, \cdots, 2t - 1$;

$$\bar{\sigma}_i(0) = \bar{\theta}_i(0) = S_i, \quad i = 0, 1, 2, \cdots, 2t - 1.$$

for $r = 0$ step 1 until $2t - 1$ do

begin

Step RiBM.1 $\bar{\sigma}_i(r+1) = \gamma(r)$; $\bar{\sigma}_{i+1}(r) = \bar{\sigma}_0(r)$;

$$\bar{\theta}_i(r), \quad i = 0, 1, 2, \cdots, 3t.$$

Step RiBM.2 if $\bar{\sigma}_0(r) \neq 0$ and $k(r) \geq 0$ then

begin

$$\bar{\theta}_i(r+1) = \bar{\sigma}_{i+1}(r), \quad i = 0, 1, 2, \cdots, 3t;$$

$$\gamma(r+1) = \bar{\sigma}_0(r); \quad k(r+1) = -k(r) - 1$$

end

else

begin

$$\bar{\theta}_i(r+1) = \bar{\theta}_i(r), \quad i = 0, 1, 2, \cdots, 3t;$$

$$\gamma(r+1) = \bar{\gamma}(r); \quad k(r+1) = k(r) + 1$$

end

end

输出:

$$\lambda_i(2t) = \bar{\sigma}_{t+i}(2t), \quad i = 0, 1, 2, \cdots, t;$$

$$\omega_i^{(h)}(2t) = \bar{\sigma}_i(2t), \quad i = 0, 1, 2, \cdots, t-1.$$

(3) 使用钱搜索来求取错误位置多项式的根以及使用 Forney 算法求取错误位置上的错误值. 若是码字错误个数小于等于 16, 上一步可求出错误位置多项式

$$\Lambda(z) = \sum_{i=0}^e \lambda_i z^i,$$

其中, $e \leq 16$. 将 a^{-j} ($0 \leq j \leq 254$) 带入 $\Lambda(z)$, 若 $\Lambda(a^{-j}) = 0$, 则 a^{-j} 是一个错误位置. 同时, 令

$$z\Lambda'(z) = \sum_{i=1}^{e/2} \lambda_{2i-1} z^{2i-1},$$

$$\Omega(z) = \sum_{i=0}^{e-1} \omega_i z^i,$$

错误值 Y_i 为

$$Y_i = \frac{z^{m_0} \Omega(z)}{z\Lambda'(z)} \Big|_{z=a^{-j}}.$$

(4) 错误图样与原来缓存的码字进行模和得到正确码字, 即 $C(x) = R(x) + E(x)$.

在译码器具体实现过程中, 为了减少乘法器在 FPGA 中的使用资源, 在数据输入端进行了二元域到复合域的域变换, 数据输出时又进行了复合域到二元域的域变换.

3 理论性能

这里所提到的误码率分析均是在 BPSK 条件下提出的.

根据文献 [5], 在没有编码的 BPSK 调制下, 在高斯白噪声 (AGWN) 信道中的译码器输入之前的

数据比特错误率 P_x 为

$$P_x = \frac{1}{2} \left(1 - \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \right).$$

其中, $x = \sqrt{E_b/N_0}$, 即

$$P_b = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{N_0}} \right).$$

RS 译码器译码时以符号为单位, 一个符号等于 8 位数据, 则译码器输入前的数据符号错误率 P_s 为

$$P_s = 1 - (1 - P_b)^8.$$

以上都是输入 RS 译码器之前数据的比特错误率和符号错误率。

RS 译码器主要工作在下面 3 种输入情况。

(1) 码块中符号错误个数小于等于 16 时, 所有错误能够纠正, 输出信息无误码。

(2) 码块中符号错误个数大于 16 个, 且出错后的码块没有错成其他可纠的码块, 这种输入比特错误率记为 P_{b-f} 。

(3) 码块中符号错误个数大于 16, 但是出错后的码块正好变成另外一个错误个数小于等于 16 的可纠码块, 被译码器纠成了其他码块, 造成了误纠情况, 这种情况下的输入比特错误率记为 P_{b-e} 。

根据文献 [6], 由于 P_{s-e} 小于 10^{-13} , $P_{s-e} \ll P_{s-f}$, $P_{b-e} \ll P_{b-f}$, 所以在实际的误码率分析中只考虑第一种和第二种情况。如果 P_{b-RS} 记为总的译码位错误率, 则有

$$P_{b-RS} = P_{b-e} + P_{b-f} \approx P_{b-f}.$$

因为 RS(255, 223) 码译码器的纠错能力为 16, 所以输出码块的出错概率 P_c 为

$$P_c = \sum_{k=17}^{255} \binom{255}{k} P_s^k (1 - P_s)^{255-k}.$$

如果出现上述的第二种译码情况, 译码器输出的信息位将保持和输入不变, 这样假设输出的某一位出现了错误, 它所在的符号在输入时肯定也是错误的, 那么剩下的 254 个符号中至少有 17 个错误, 所以

$$P_{b-RS} \approx P_{b-f} = P_b \cdot \sum_{k=16}^{254} \binom{254}{k} P_s^k (1 - P_s)^{254-k},$$

即译码输出的信息位比特错误率 P_{b-RS_m} 为

$$P_{b-RS_m} = \frac{223}{255} P_b \cdot \sum_{k=16}^{254} \binom{254}{k} P_s^k (1 - P_s)^{254-k}.$$

4 性能测试

以前很多国内关于 RS 译码器的文章几乎都是介绍译码器算法和 FPGA 实现流程, 而关于译码器性能测试方面几乎没有详细介绍, 鉴于这个原因, 本文较为详细地介绍了测试方法和测试平台, 给出了试验结果。对于 RS(255, 223) 译码器的测试主要采取下面两种方法。

(1) 利用 FPGA 的块 RAM 把典型的测试用例循环输入译码器, 用逻辑分析仪观测译码器输出确定译码器各项性能, 包括纠错能力、速度、译码输入/输出延时、连续工作时间等。

(2) 把软件编码的海量随机数据经过软件加噪, 然后使用这些数据作为数据源在调试好且完全没有误码的基于 PCI 总线接口的测试平台 (见图 3) 上对 RS 译码器进行全面验证。

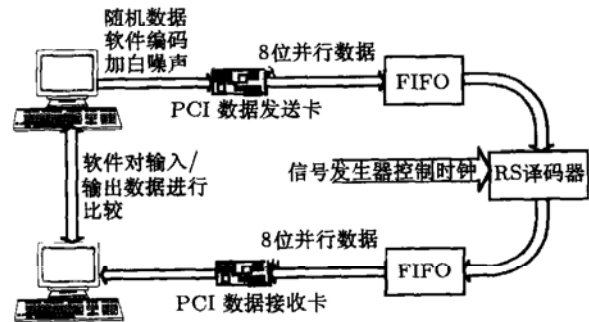


图3 基于PCI总线接口的RS(255, 223)译码器测试平台

Fig.3 Test platform of RS(255, 223) decoder based on PCI bus interface

第一种测试方法较为简单, 测得译码器的译码数据通过率为 400 Mbps 左右, 能够纠正错误个数不大于 16 个符号的码块, 译码输入/输出延时为 554 个时钟周期, 译码器经过连续工作 120 小时的测试, 随机观察的测试结果均表明译码器工作正常。下面主要介绍一下第二种测试方法。

第二种测试方法的测试步骤如下。

(1) 用 MATLAB 软件产生大量随机数据, 然后对随机数据进行编码, 也就是加校验位。

(2) 针对 BPSK 调制情况的误码率 (BER) 与信噪比 (SNR) 的曲线图, 选取不同 SNR 对应的不同误码率模仿高斯白噪声给编码后的数据加噪。

(3) 把编码加噪后的随机数据通过基于 PCI 总线接口的数据发送卡发送到译码器中, 译码后的数据再通过 PCI 数据接收卡接收, 把试验数据 (见表

1) 和原来编码后没有加噪的随机数利用软件进行比较, 得到 RS(255, 223) 译码器的试验译码效果曲线。

表 1 给定 SNR 加噪数据进行的译码试验结果
Table 1 Test result of decoder based on the data disturbed according to the SNR coefficients

SNR (E_b/N_0) /dB	验证码 块总数	有符号错误 的码块个数	译码后不可 纠错码块数	译码前信息 位比特误码率	译码后信息 位比特误码率
0.5	195 840	195 840	195 840	$5.864\,76 \times 10^{-2}$	$5.864\,76 \times 10^{-2}$
3	48 960	48 960	48 958	$1.999\,91 \times 10^{-2}$	$1.999\,89 \times 10^{-2}$
3.3	48 960	48 960	48 950	$1.693\,59 \times 10^{-2}$	$1.693\,44 \times 10^{-2}$
3.5	48 960	48 960	48 920	$1.505\,49 \times 10^{-2}$	$1.504\,92 \times 10^{-2}$
3.8	24 480	24 480	24 340	$1.241\,71 \times 10^{-2}$	$1.237\,77 \times 10^{-2}$
4	48 960	48 960	47 032	$1.093\,13 \times 10^{-2}$	$1.067\,06 \times 10^{-2}$
4.25	48 960	48 960	40 774	$9.201\,45 \times 10^{-3}$	$8.128\,78 \times 10^{-3}$
4.5	48 960	48 960	28 138	$7.686\,05 \times 10^{-3}$	$5.108\,18 \times 10^{-3}$
4.75	45 450	45 040	124 95	$6.347\,35 \times 10^{-3}$	$2.318\,52 \times 10^{-3}$
5	97 920	97 917	8853	$5.214\,11 \times 10^{-3}$	$7.259\,03 \times 10^{-4}$
5.5	106 908	106 876	272	$3.369\,98 \times 10^{-3}$	$1.763\,29 \times 10^{-5}$
5.75	602 465	601 288	114	$2.673\,83 \times 10^{-3}$	$1.440\,97 \times 10^{-6}$
6	979 200	971 787	9	$2.089\,49 \times 10^{-3}$	$7.158\,70 \times 10^{-8}$

5 理论 RS(255, 223) 译码器译码功能与实际测试功能的比较

第 3 部分推论的结果可以用 Matlab 软件仿真出理论上 RS 译码器在 BPSK 调制下的误码率与信噪比的关系曲线, 结合前面试验部分测得的试验数据, RS(255, 223) 码译码器信噪比变化条件下的理论误码率曲线和试验误码率曲线图如图 4 所示。作图时, 考虑了 255 个符号的整个码字和 223 个符号的信息位数据在信噪比上的转换, 即总能量不变的条件下, 255 个符号所包含的能量要转化到 223 个信息符号上, 记 SNR_{w-c} 为整个码块的信噪比, SNR_m 为信息部分的信噪比, 那么有

$$SNR_{w-c} + 10 \lg \frac{255}{223} = SNR_m.$$

从图 4 中可以看到, 试验给出的数据在加噪后与 BPSK 条件下的误码率一致, 证明了试验数据的可靠性。从 0.5 dB 到 6 dB 选出十余个较为典型的测试点, 译码输出的效果与理论上推出的结果一致, 较全面地验证了译码器的译码功能。

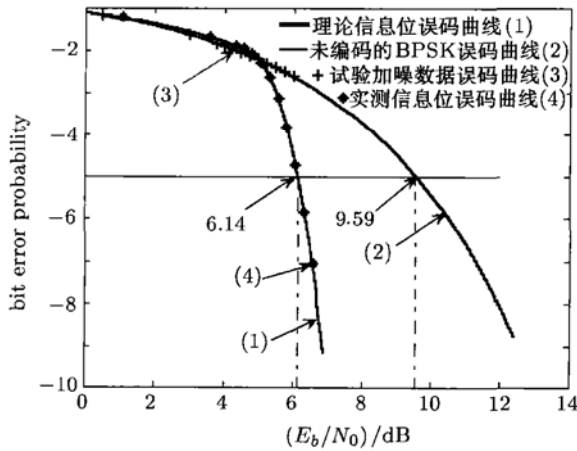


图 4 RS(255, 223) 码理论误码率曲线与试验误码曲线的比较

Fig.4 Comparison of theoretic and testing error probability curves of the RS(255, 223) decoder

6 结论

本文介绍了一种符合 CCSDS 标准的 RS(255, 223) 码硬件译码器的实现流程及其误码率分析与性能测试。译码过程采用改进的 BM 算法求取关键方

程, 达到了 Eculid 算法的速度, 使用面积得到很大的减少.

文中提到的译码器已经用 Xilinx 公司的 Virtex600E 芯片实现, 最高译码通过率达到 400 Mbps, 使用面积为 180 000 门, 不仅通过计算机仿真进行了验证, 而且通过基于 PCI 总线的测试平台用大量经过编码且误码率可控的随机数据对译码器进行全面验证, 通过理论分析与实际试验结果的比较推定该译码器译码效果与理论上译码效果一致, 符合使用要求. 下一步设计工作将在更大的 FPGA 芯片内实现 2 个或者多个 RS(255, 223) 码译码器的级联译码, 以达到更好的译码效果.

参考文献

- [1] Recommendation for Space Data System Standards Telemetry Channel Coding. CCSDS 101.0-B-5 Blue Book, 2001. 3-1—3-7
- [2] Wang Jinxing *et al.* RS decoder summary. *Microelectronics*, 1997, **27**(2):115—120. in Chinese (王进祥等. RS 译码器综述. 微电子学, 1997, **27**(2):115—120)
- [3] Sarwate D V, Shanbhag N R. High-speed architecture for reed-solomon decoders. *IEEE Trans. VLSI Sys.*, 2001, **9**(5):641—655
- [4] Cai Minqi *et al.* Pipeline design of RS(255, 239) decoder. *Appl. IC*, 2003, (10):34—37. in Chinese (蔡珉琦等. RS(255, 239) 译码器的流水线设计. 集成电路应用, 2003, (10):34—37)
- [5] Yuen J H. Deep Space Telecommunications System Engineering. New York and London: Plenum Press, 1992. 248—265, 275—279
- [6] McEliec R J, Swanson L. On the Decoder Error Probability for Reed-Solomn Codes. TDA Progress Report 42-71, 1985. 66—72
- [7] Divsalar D, Yuen J H. Performance of Concatenated Reed-Solomn/Viterbi Channel Coding. TDA Progress Report 42-84, 1982. 81—94