一个面积优化的高速 RS(255,239)译码器 VLSI 设计

张静波[1]，戴显英[2]，张鹤鸣[2]，胡辉勇[1]，贾大中[1]
(1. 西安电子科技大学 微电子学院，陕西 西安 710071；
2. 西安电子科技大学 宽禁带半导体材料与器件教育部重点实验室，陕西 西安 710071)

摘要：基于改进的 Euclid 算法，提出了一种仅含两个折叠计算单元的结构，并用三级流水线结构整体实现以提高吞吐率. 将常规有限域乘法器转化到复合域中实现，降低了芯片的复杂性和关键路径延迟. 以 RS(255,239)为例，基于 TSMC 0.18 标准单元库的译码器电路规模约为20 614门，在相同纠错能力下，该结构相比较于传统的并行脉动阵列结构，其硬件复杂度可减少 60%左右.

关键词：RS 码；流水线结构；Euclid 算法；Verilog HDL；超大规模集成电路
中图分类号：TN47 **文献标识码**：A **文章编号**：1001-2400(2008)01-0116-05

Area-efficient high-speed VLSI design of the RS(255,239) decoder

ZHANG Jing-bo[1], *DAI Xian-ying*[2], *ZHANG He-ming*[2], *HU Hui-yong*[1], *JIA Da-zhong*[1]
(1. School of Microelectronic, Xidian Univ., Xi′an 710071, China; 2. Ministry of Education Key Lab. of Wide Band-Gap Semiconductor Materials and Devices, Xidian Univ., Xi′an 710071, China)

Abstract: Based on the modified Euclid's algorithm, a VLSI architecture is proposed, which only uses two folding calculating cells and three-stage pipeline processing architectures to improve its throughput. Also, a way is introduced to reduce the complexity and critical path delay of general finite multipliers by the transferring of field from the time domain to the composite domain. Based on the TSMC 0.18 standard cell library, the proposed RS decoder consists of about 20 614 gates for widely used RS(255, 239) code, which reduces complexity by about 60% compared with an existing architecture with systolic arrays when having the same error correction ability.

Key Words: Reed-Solomon codes; pipeline architecture; Euclid algorithm; verilog HDL; VLSI

RS 码(Reed-Solomon Code)是非二元 BCH 码的一个重要子类，是 GF(2^m)上的一类极大最小距离可分码. RS(n,k) 码的码长为 n 个符号($n \leqslant 2^m-1$)，由 k 个信息符号和 $n-k$ 个校验符号组成，每个符号由 m 个比特表示，其最大纠错能力为 t ($t=(n-k)/2$). RS 码因其具有优良的纠突发错误和随机错误的能力而被广泛应用于网络通信系统、计算机系统、存储媒介、扩频通信以及数字多媒体等多种领域，是一种循环字符错误校正码. 与其他非二元码类相比，在相同冗余度下，RS 码有较大的纠错能力，目前已成为美国航天局(NASA)和欧洲空间站(ESA)在深空卫星通信的级联码系统中采用的标准外码[1,2].

对 RS 码译码方法的研究一直是学术界和工程界所热衷讨论的课题，随之各种 RS 译码方法被提出来，以减少面积，提高实时性[1~5]. RS(255,239)码是国际电信联盟(ITU)规定的用于水下光纤通信的一类码. 笔者基于修正的 Euclid(ME)算法，在不改变整体译码速度的前提下，改变其初始迭代条件，针对 RS(255,239)提出了一种适用于光纤通信的新的硬件实现结构，实现了多项式计算单元的分时复用.

1 RS 译码器总体架构

基于伴随式的 RS 译码包括 5 步[4]. 第 1 步是计算伴随式 $S(x)$，用于产生伴随式多项式以计算关键方

收稿日期：2007-08-03
基金项目：模拟集成电路国家重点实验室基金资助(9140C0905040706)
作者简介：张静波(1980-)，男，西安电子科技大学硕士研究生，E-mail：zhangjingbo@neusoft.com.

程;第 2 步,也是整个译码器的核心部分,即解关键方程$S(x)\sigma(x)\equiv\omega(x) \bmod x^{2t}$,以得到错误位置多项式$\sigma(x)$和错误值多项式$\omega(x)$;第 3 步是钱搜索(Chien Search)部分,用于计算错误位置多项式和错误值多项式;第 4 步是错误图样计算,即用 Forney 算法求得错误值;第 5 步,纠错. 该译码器的架构如图 1 所示. 为了达到高吞吐率的目的,笔者采用了文献[4]提出的三级流水线结构,如图 2 所示.

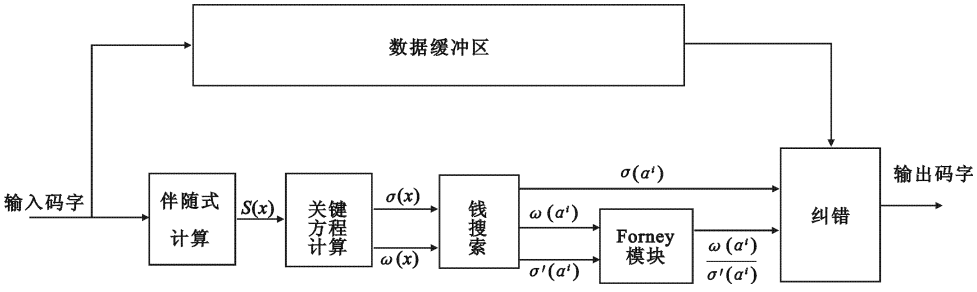

图 1　RS 译码器结构

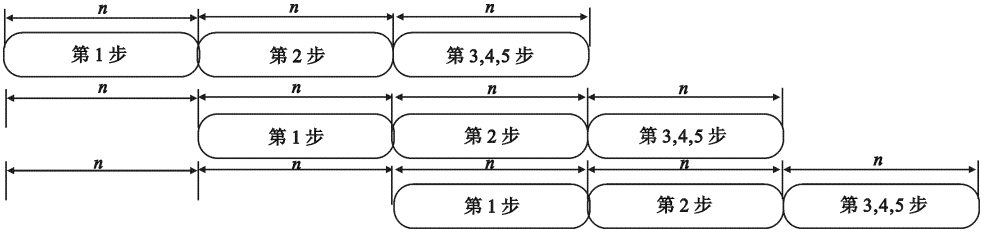

图 2　RS 译码器三级流水线结构

2　RS(255,239)译码器的 VLSI 设计

2.1　有限域乘法器设计

在各种有限域计算操作中,乘法是结构较复杂、时延较大的运算. 在 RS 编译码的 VLSI 实现电路中,有限域乘法器是其主要的运算单元,对编译码性能有重要影响,因此迫切需要设计一种面积小、性能高的乘法器. 一般说来,有限域乘法器有比特并行和比特串行两种,而笔者采用的复合域乘法原理最初由 Mastrovito 建议,它利用 GF($(2^n)^m$)来表示 GF(2^k)($k=n\cdot m$). 这种方法在次域 GF(2^n)上采用比特并行算法,且串行处理其扩展域,这种串并混合的方法致使乘法结果可以快速实现. Paar 等人证明了标准基在二元扩展域($m=2$)中乘法和乘方及求逆的正确性[6].

当 k 可分解为两个整数 n,m 时,有限域 GF(2^k)上的任一元素均可用标准基表示为$a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,$a_i$ 为 GF(2^m)上的元素. 这里 GF(2^k)为 GF(2^m)的扩展域,扩展度为 n. 同理,GF(2^8)可看作其次域 GF(2^4)的二元扩展域. 在译码器的输入端,将 GF(2^8)上的一个符号的高低四位转化为两个 GF(2^4)上的符号,每四位采用比特并行的方法来实现乘法,其本原多项式为$Q(z)=\varphi^{14}+z+z^2$,其中 φ 为$t(y)=y^4+y+1$ 的根[6],然后将高低四位组合成 8 位,最后在译码器的输出端再转化为 GF(2^8)上的符号. 不考虑译码器中的乘法器共用一对转换和逆转换电路,复合域乘法器仅需 48 个与非门和 62 个或非门便可实现,不仅规模比 Mastrovito 乘法器和文献[7]中乘法器的规模小 25%,而且乘法器关键路径的延迟也小.

2.2　译码器设计

在时域 RS 译码算法中,使用 Euclid 算法解关键方程 $S(x)\sigma(x)\equiv\omega(x) \bmod x^{2t}$,求出错误位置多项式和错误值多项式,需要做多项式的除法运算,每一步都要用到有限域元素的倒数. 在用超大规模集成电路(VLSI)实现时,连续计算这些倒数是相当耗费面积的,并且降低了运算速度. 因此,需要进一步改进算法. 文献[8]给出了改进的 Euclid 算法,可避免计算元素倒数.

在解关键方程中,考虑如下两个多项式:

$$A(x)=\sum_{i=0}^{n-1}a_ix^i \quad , \quad B(x)=\sum_{j=0}^{m-1}b_jx^j \quad . \tag{1}$$

一般的 Euclid 算法利用式(1)和它们除法运算之后的余式做连续的除法,而这样的除法可以用连续的减法代替.通过将单次的多项式减法运算单元连接起来,就能用流水线的方式实现解关键方程.为了避免除法(算出一个商式,其实这个商式每次都作为中间结果,并不参与迭代运算),可利用交叉相乘两个多项式的首项系数的方法算出余式:

$$\sum_{k=0}^{n-2}c_kx^k=b_{m-1}A(x)-a_{n-1}x^{n-m}B(x) \quad . \tag{2}$$

因此,ME 算法描述如下:

初始化条件为 $R_0(x)=x^{2t}$, $Q_0(x)=S(x)$, $L_0(x)=0$, $U_0(x)=1$.

迭代过程:

$$R_i(x)=[\sigma_{i-1}b_{i-1}R_{i-1}(x)+\bar{\sigma}_{i-1}a_{i-1}Q_{i-1}(x)]-x^{|l_{i-1}|}[\sigma_{i-1}a_{i-1}Q_{i-1}(x)+\bar{\sigma}_{i-1}b_{i-1}R_{i-1}(x)] \quad ,$$

$$Q_i(x)=\sigma_{i-1}Q_{i-1}(x)+\bar{\sigma}_{i-1}R_{i-1}(x) \quad ,$$

$$L_i(x)=[\sigma_{i-1}b_{i-1}L_{i-1}(x)+\bar{\sigma}_{i-1}a_{i-1}U_{i-1}(x)]-x^{|l_{i-1}|}[\sigma_{i-1}a_{i-1}U_{i-1}(x)+\bar{\sigma}_{i-1}b_{i-1}L_{i-1}(x)] \quad ,$$

$$U_i(x)=\sigma_{i-1}U_{i-1}(x)+\bar{\sigma}_{i-1}L_{i-1}(x) \quad .$$

其中 a_{i-1} 和 b_{i-1} 分别是 $R_{i-1}(x)$ 和 $Q_{i-1}(x)$ 的首项系数,且

$$l_{i-1}=\deg[R_{i-1}(x)]-\deg[Q_{i-1}(x)] \quad , \tag{3}$$

$$\sigma_{i-1}\begin{cases}1 \quad , & l_{i-1}\geqslant 0 \quad ,\\ 0 \quad , & l_{i-1}<0 \quad .\end{cases} \tag{4}$$

终止条件:$\deg[R_i(x)]<t$,此时有 $\omega(x)=R_i(x)$,$\sigma(x)=L_i(x)$.式中 $\deg[\cdot]$ 表示多项式的次数.

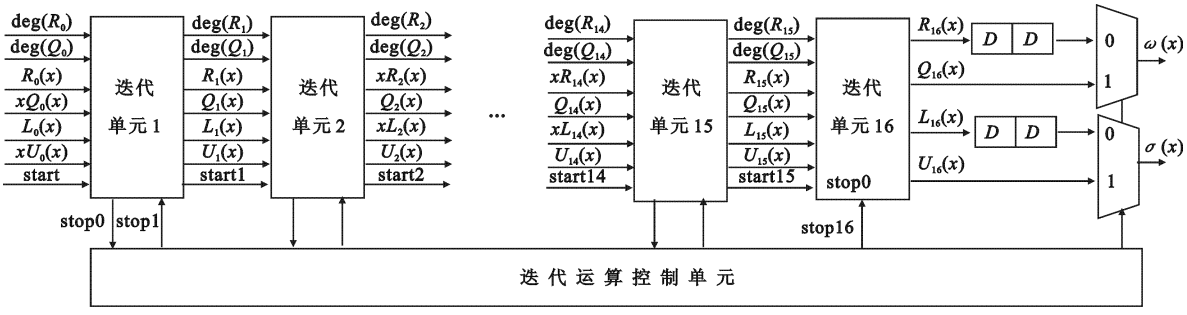

图 3 一般译码方法结构

为了减小译码延迟,许多 RS 译码器使用了脉动阵列结构[8~10],这就需要有更多的寄存器以控制时序和存储中间结果,因此大大增加了芯片面积,使得该算法的硬件消耗占整个译码器面积的 60%~70%,其结构如图 3 所示.从图 3 中可以发现,以上用于计算 ME 算法的文献中其速度"太快",仅需 $4t$ ~$6t$ 个时钟,实际上,在三级流水线结构译码中,限制译码器吞吐率提高的瓶颈是需要 n 个时钟才能完成的伴随式和钱搜索的计算,因此,增加 ME 算法的时钟个数不会降低译码速度.正是基于以上结构的不足,笔者提出了以下改进方案,以第一次迭代后的结果作为初始化条件:

$$R_0(x)=\sum_{i=0}^{2t-2}s_ix^{i+1}, \quad Q_0(x)=S(x), \quad L_0(x)=1, \quad U_0(x)=x \quad , \tag{5}$$

并用两个折叠的串行运算单元代替传统的 $2t$ 个并行迭代单元,如图 4 所示.

利用新的初始化条件,可有如下规律:经过奇次迭代后 $\deg[R_i(x)]<\deg[Q_i(x)]$,而经过偶次迭代后 $\deg[R_i(x)]=\deg[Q_i(x)]$. 这样,在奇次迭代后,乘法器输出端直接交换,而在偶次迭代后不交换,计算式(3)和式(4)的电路可以省去,简化了控制电路.整个算法的迭代过程可简化为

$$\begin{aligned}&R_i(x)=b_{i-1}R_{i-1}(x)-x^{l_{i-1}}a_{i-1}Q_{i-1}(x), \quad Q_i(x)=Q_{i-1}(x) \quad ,\\ &L_i(x)=b_{i-1}L_{i-1}(x)-x^{l_{i-1}}a_{i-1}U_{i-1}(x), \quad U_i(x)=U_{i-1}(x) \quad .\end{aligned} \tag{6}$$

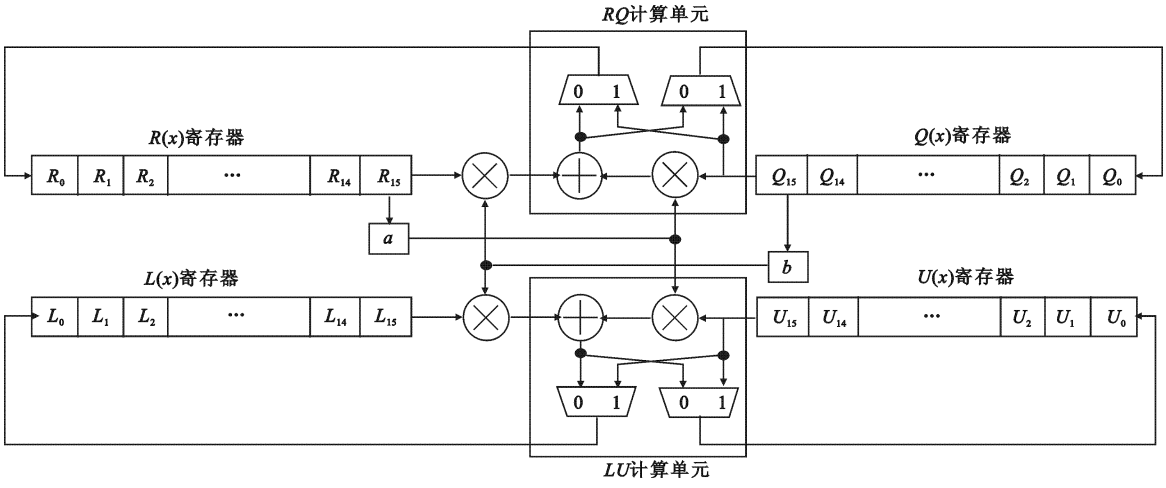

图 4　改进的折叠结构

式(6)中,如果 i 为奇数,l_{i-1} 为 0;否则,l_{i-1} 为 1. 这样相应的迭代停止条件也可简化为判断 $R_{i-1}(x)$ 和 $Q_{i-1}(x)$ 的最高项系数是否都为零,如果均为零,则可将数据直接送到下一级中,而无需进行乘法运算. 该方法的优点是既可通过时钟关断技术降低功耗,又不会损害流水性. 在每次迭代完毕后,存储 $R_i(x)$ 和 $Q_i(x)$ 的首项系数 a_i 和 b_i,这样,每次运算需要 $2t+1$ 个时钟,最多需要运算的次数是 $2t-1$ 次. 所以,终止条件满足时,最多需要时钟个数为 $(2t+1)(2t-1)=255$ $(t=8)$,与伴随式计算电路和钱搜索电路所用时钟相等. 相比较于文献[8~10],该结构充分利用了 ME 算法本身的特点,实现了电路的复用. 观察此电路不难发现,其关键路径延迟为 $T_{\mathrm{MUL}}+T_{\mathrm{MUX}}+T_{\mathrm{ADD}}$.

3　RS 译码器实现结果及性能比较

应用上面介绍的电路结构,笔者设计并实现了 RS(255,239)译码器. 整个译码器模型由 Verilog 语言描述,并用 Modelsim 仿真器进行了功能性验证. 在 SYNOPSYS 编译器下基于 TSMC 0.18 标准单元库的译码器电路规模约为20 614门.

表 1 为笔者与文献[8~11]在解关键方程模块上所用主要运算部件的对比;表 2 为笔者提出的结构与文献[9,11,12]结构在主要性能指标上的比较. 由表可以看出,笔者提出的结构相比较于文献[9]的全并行结构在面积上节省了 60%左右,且时钟频率提高了 30%.

表 1　主要运算部件的对比

	笔者提出的方案	文献[8]	文献[9]	文献[10]	文献[11]
乘法器	4	$8t$	$3t+1$	$6t+2$	$6t+2$
加法器	2	$8t$	$4t+1$	$3t+1$	$3t+1$
D 触发器	66	$78t+4$	$14t+6$	$6t+2$	$6t+4$
多路选择器	4	$40t+2$	$11t+4$	$3t+1$	$3t+2$

表 2　主要性能指标的对比

	笔者采用的结构	文[9]中结构	文[11]中结构	文[12] 中结构
工艺/μm	0.18	0.18	0.16	0.25
译码时延	512	287	168	288
频率/MHz	400	300	312	200
门数	20 614	55 600	38 500	21 000
吞吐率	3.2	2.4	2.5	1.6

4 结 束 语

基于改进的 Euclid 算法,笔者提出了一种面积优化的 RS(255,239)译码器结构,并对译码器中用到的主要运算部件——乘法器作了改进.在求解关键方程时采用了新的初始条件,并在流水线基础上使用折叠结构来实现关键方程的求解电路,提高了译码器主要运算部件的复用率,精简了电路结构,缩减了电路面积,使其复杂性约为常规并行脉动阵列结构的 60%左右.基于此算法,只需 4 路并行的折叠结构即可满足光纤通信系统 10GBase-LX4 的要求.

参考文献:

[1] Lee M H. A High Speed Reed-Solomon Decoder[J]. IEEE Trans on Consumer Electron, 1995, 41(4): 1142-1149.

[2] Shayan Y R. A Cellular Structure for a Versatile Reed-Solomon Decoder[J]. IEEE Trans on Computer, 1997, 46(1): 80-85.

[3] Blahut R E. A Universal Reed-Solomon Decoder[J]. IBM J Res Develop, 1984, 28(3): 150-158.

[4] Kavian Y S, Falahati A, Khayatzadeh A, et al. High Speed Reed-Solomon Decoder with Pipeline Architecture[C]//2005 International Conference on Wireless and Optical Communications Networks. New York: IEEE, 2005: 415-419.

[5] Baek J H, Kang J Y, Sunwoo M H. Design of a High-Speed Reed-Solomon Decoder[J]. IEEE ISCAS, 2002, 5(18): 793-796.

[6] Paar C. A New Architecture for a Parallel Finite field Multiplier with Low Complexity Based on Composite Field[J]. IEEE Trans on Computer, 1996, 45(7): 856-861.

[7] Jeng J H, Kuo J M, Truong T K. A High Efficient Multiplier for RS Decoder[C]//International Symposium on 1999 VLSI Technology, Systems and Applications. Taibei: IEEE, 1999: 116-118.

[8] Lee H. High-speed VLSI Architecture for Reed-Solomon Decoder[J]. IEEE Trans on Very Large Scale(VLSI) Integer Syst, 2003, 11(2): 288-294.

[9] Truong T K. An Area-efficient Euclidean Architecture for Parallel Reed-Solomon Decoder[C]//IEEE Computer Society Annu Symp VLSI. New York: IEEE, 2003: 209-210.

[10]Sarwate D V, Shanbhag N R. High-speed Architecture for Reed-Solomon Decoder[J]. IEEE Trans on Very Large Scale (VLSI) Integr Syst, 2003, 17(3): 288-294.

[11]Song L, Yu M L, Shaffer M S. 10 and 40-Gb/s Forward Error Correction Devices for Optical Communications[J]. IEEE Journal Solid-State Circuits, 2002, 37(11): 1565-1573.

[12]Strollo A G M, Petra N, De Caro D, et al. An Area-Efficient High-Speed Reed-Solomon Decoder in 0.25μm CMOS[J]. IEEE Trans on Circuit and Systems, 2004, 36(8): 479-482.

(编辑: 郭 华)

简 讯

❖ 2007 年 11 月 15 日~16 日,美国威斯康辛-麦迪逊大学空间科学和工程中心(SSEC)教授、首席研究员 Bormin Huang 来校讲学访问. Bormin Huang 教授于 1991 年获美国密西根大学博士,是 2007 年 SPIE 卫星数据压缩和通信会议主席,美国国家海洋和气象局(NOAA)和美国宇航局(NASA)多个超光谱图像压缩科研项目负责人.

摘自《西电情况》2007.12.10