

一种适用于导航系统的维特比译码器电路设计与仿真

桂 琼, 李晓江

(中国科学院 微电子研究所, 浙江 杭州 310053)

摘 要: 设计了一种适用于导航系统的低功耗、串行维特比译码器电路. 介绍了设计的维特比译码器电路的整体结构和各部分硬件电路的设计与特点, 仿真结果显示设计的维特比译码器电路能够正常译码, 并能纠正传输过程中的错误比特; SMIC 0.18 μm 工艺下的综合结果表明译码器电路的面积只有 4 102 门, 功耗为 399.514 μW .

关键词: 维特比译码器; 分支度量单元; 加比选单元; 幸存路径管理单元; 回溯算法

中图分类号: TN492

文献标识码: A

文章编号: 1000-7180(2011)01-0054-04

Design and Simulation of Viterbi Decoder Used in Navigation Systems

GUI Qiong, LI Xiao-jiang

(Institute of Microelectronics of Chinese Academy of Science, Hangzhou 310053, China)

Abstract: We designed low power serial Viterbi decoder used in navigation systems. We introduce the whole architecture of the decoder and the design and features of each module in detail. The waveform shows that the designed Viterbi decoder can work in right condition and correct errors during transmission. The synthesize result under SMIC 0.18 μm technology shows that the area of the circuit is 4 102 gates, and the power is 399.514 μW .

Key words: Viterbi decoder; branch metric unit; add-compare-select unit; survivor path memory unit; trace-back algorithm

1 引言

在现代化的导航系统信号中, 采用 FEC 编码, 根据一些预定的方法在信道上传输冗余的比特, 使接收机能够监测和纠正可能由噪声、干扰或衰落等造成的错误, 避免重新接收电文, 从而可以提高接收机的工作速度. 因而这种编码被应用在 GPS 的 L2C^[1]、GALILEO^[2]、WAAS^[3] 中, 所采用的是如图 1 所示的 (2, 1, 7) 卷积码编码器.

此时需要相应的译码器对接收的导航卫星信号进行译码. 由于 FEC 编码的导航卫星信号速率是 50~500 sps^[1-3], 在速率不是很高的情况下, 本文采用串行结构, 复用加比选单元, 这样可以大大减小电路的面积和功耗.

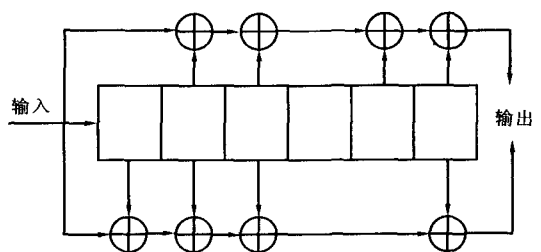


图 1 (2, 1, 7) 卷积码编码器

2 维特比译码算法原理

维特比译码算法是 1967 年由 Viterbi 提出. 译码的基本思路是按照最大似然译码准则寻找最有可能的译码路径.

假设一个二进制输入、 Q 进制输出、信道为无记忆的信道模型, 长度为 h 的信息序列 u 经码率为 $1/n$ 的卷积码编码器编码, 生成长度为 $N = n(h + m)$ 的

码字 v , 其中 m 为寄存器存储深度. 译码器根据接收序列 r 产生码字 v 的估计 $\hat{v}$, 无记忆信道上的最大似然译码就是选择最大化对数似然函数 $\log P(r|v)$ 的 $\hat{v}$ 作为码字. 对于无记忆信道, 有

$$\log P(r|v) = \sum_{l=0}^{h+m-1} \log P(r_l|v_l) = \sum_{i=0}^{N-1} \log P(r_i|v_i) \quad (1)$$

式中, $P(r_l|v_l)$ 是信道转移概率, 第一项为码字的路径度量, 第二项为分支度量, 第三项为比特度量^[4].

维特比算法是根据接收到的序列 r 通过网格图找到具有最大度量的路径, 根据上式, 这条路径即为所求的最大似然路径. 实现该算法主要有 3 个步骤:

(1) 从某一单位时间 $j = m$ 开始, 对进入每一状态的所有长为 j 段分支的部分路径, 计算部分路径度量. 对每一状态, 挑选并存储一条有最大度量的部分路径及其部分度量值, 称此部分为幸存路径;

(2) j 增加 1, 把此刻进入每一状态的所有分支度量, 和同这些分支相连的前一时刻的留选路径的度量相加, 得到了此刻进入每一状态的幸存路径, 加以储存删去其他所有路径, 因此留选路径延长了一个分支;

(3) 若 $j < L + m$ (L 为回溯深度), 则重复以上各步骤, 否则停止, 译码器得到了有最大路径度量的路径.

3 维特比译码器电路设计

3.1 整体电路结构

维特比译码器的整体电路结构如图 2 所示. 在电路工作过程中, 输入的编码数据首先经过分支度量单元计算出分支度量值, 随后加比选单元根据当前时刻的分支度量值分别计算出进入各个状态所的路径度量值, 并选择出每个状态的最大度量值, 以及路径信息, 并将这些信息存入 RAM 中. 当接收完一段编码数据后, 选出最大度量值对应的状态, 最后幸存路径管理单元根据该状态以及 RAM 中存储的幸存路径信息进行回溯, 最后得到译码结果.

3.2 分支度量单元设计

分支度量的计算有硬判决和软判决两种算法. 在输出端, 根据接收信号波形输出的 Q 个不同的值, 与 M 个值比较, 直接将接收信号判决为 M 个可能信号之一. 当 $Q = M$ 时用硬判决译码, 此时分支度量采用的是最小汉明距离; 当 $Q > M$ 时, 需要采用软

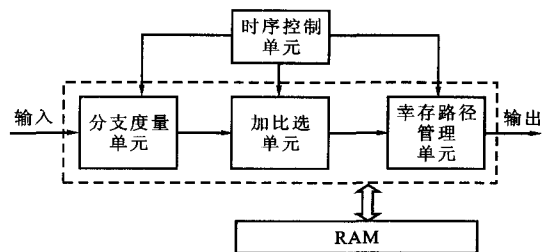


图2 维特比译码器的结构框图

判决, 使用最小欧氏距离^[5]. 在对图 1 所示的卷积码编码器的译码的过程中, 由于 $Q = M$, 因而采用硬判决. 图 3 所示为分支度量单元电路的结构示意图, 其中加法表示汉明距离的计算. $\{a, b\}$ 表示接收的 2 位宽的编码数据, 则它与 00, 01, 10, 11 的汉明距离可以通过简单的组合逻辑运算实现: $d_0 = a + b$; $d_1 = a + (\sim b)$; $d_2 = (\sim a) + b$; $d_3 = (\sim a) + (\sim b)$.

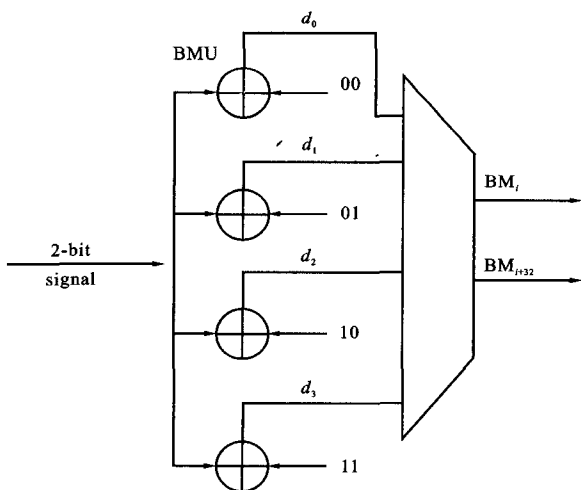


图3 分支度量单元电路结构示意图

3.3 加比选单元设计

加比选单元是维特比译码器中一个重要单元, 主要完成路径度量的计算, 幸存路径的选择也与它有关.

路径度量计算的最小单元为图 4 所示的 radix-2 运算. 为了减小延迟, 产生了将网格图中多个时刻的运算合成一步完成的 radix-4 算法^[6]. 虽然这种算法能够减小延迟时间, 从而提高译码速度, 适用于并行、高速的译码电路, 但是会增加电路的复杂度和面积. 在导航系统中码速率不是很高的情况下, 采用 radix-2 算法, 可以使加比选单元电路结构更简单, 面积更小.

在设计的维特比译码器电路中, 串行结构是通过复用图 5 所示的加比选单元实现. 用该单元串行地完成所有状态、所有时刻的加、比、选操作. 相比于采用多个加比选单元同时工作的并行结构, 在能达

到速度要求的前提下,串行结构能够节省面积。

加比选单元中路径度量的计算可以通过加法器和比较器完成,如图4所示, $n+1$ 时刻的状态 $PM_{2^{i+1}}$ 由 n 时刻的 PM_i 与 BM_i 之和,和 n 时刻的状态 PM_{i+32} 和与 BM_{i+32} 之和中的较小值决定。 $PM_{2^{i+1}}$ 由 n 时刻的 PM_i 与 BM_{i+32} 之和,和 n 时刻的状态 PM_{i+32} 和与 BM_i 之和中的较小值决定。选择一个状态的 $n+1$ 时刻的度量值后,在时序逻辑控制单元的控制下,用该度量值替换掉 RAM 中存储的 n 时刻的该状态的路径度量值。

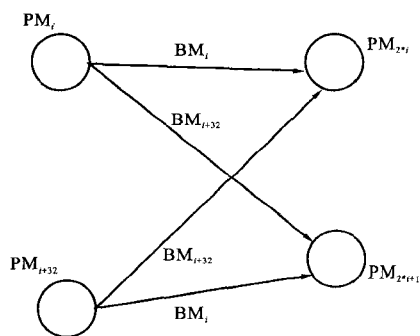


图4 radix-2 运算图

幸存路径在路径度量计算过程中比较大小的时候就决定,较小值对应的 n 时刻的状态转移信息就是幸存路径的信息,为了减小存储空间,用 0,1 来表示。这些幸存路径信息也存储到 RAM 中,供译码的时候使用。

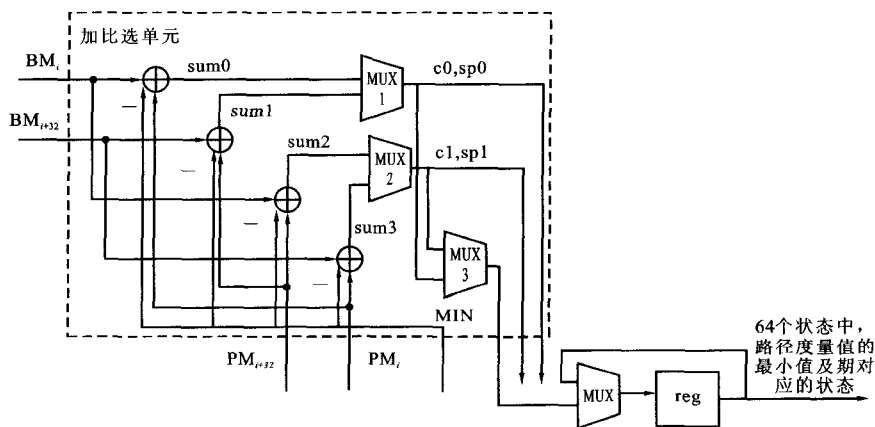


图5 加比选单元电路结构示意图

3.4 幸存路径管理单元设计

通常幸存路径的管理方法有回溯法和寄存器交换法。寄存器交换法是最直接的一种方法,能够实现全并行的高速译码^[7]。需要二维的寄存器阵列来存储可能的译码结果,译码延迟小,但是每一时刻都要进行寄存器之间值的交换,并且当需要译码大的约束长度($K \geq 7$)的卷积码时,由于大的功耗和面积,

设计的加比选单元电路除了完成上述的两个重要的基本功能外,还有具有以下功能:

(1) 溢出问题的解决。随着时间增加,路径度量值也会不断增大,由于寄存器位宽的限制,可能会出现溢出的情况。针对溢出问题,设计的译码器电路支持两种模式,一种是采用最简单的清零模式,在要开始一段数据的译码时,所有的路径度量值先全部清零,这种模式通过设置时序控制逻辑单元中相应的寄存器来实现;另一种模式是每开始一段数据译码时,减去这些度量值中的最小值,由图5中所示的加减运算完成。

(2) 最小值比较器。在接收完一段编码数据后,需要比较 64 个状态的路径度量值,选取其中的最小值及其对应的状态,再根据这个状态进行译码。如图5所示,在加比选单元中增加一个选择器 MUX3,可以方便电路快速实现最小值的比较。具体实现为:寄存器 reg 首先置成最大值,在接收一段编码数据的最后 2bit 数据时,每进行一次加比选操作的时候,时序控制单元就将 MUX3 选出的较小值 MIN 与 reg 中的值比较,将较小者保存在 reg 中。这样在加比选单元串行地依次完成 64 个状态的路径度量值计算时,所有状态的路径度量值的大小也比较完成,从而可以立即进行译码。并且,该最小值还要作为下次译码时为防止溢出而要减去的值。

寄存器交换法就不太适用^[8]。而回溯算法只根据存储的路径信息,串行的选择出一条最可能的译码结果,虽然速度不如寄存器交换法,但是可以大大的减小电路的面积和功耗。一般,回溯深度取(5~7)倍的约束长度^[9]。

完成路径度量值的比较后,回溯译码过程主要分两个步骤:

- (1) 译码:若状态为偶数时,译码输出 0,为奇数时,译码输出 1;
- (2) 读取上一时刻到该时刻的幸存路径信息,计算上一时刻的状态.如果幸存路径信息为 1,则上一时刻的状态=当前状态/2+32;如果为 0,则上一时刻的状态=当前状态/2;
- 重复进行(1)和(2)的操作,直到完成译码.

3.5 时序控制单元

时序控制单元是控制整个译码器电路的工作时序,在相应的时刻给分支度量单元、加比选单元、幸存路径管理单元提供正确的数据和控制信号.由于维特比译码算法中有大量的数据需要存储到 RAM 中,因而时序控制单元另一个重要的作用是控制对 RAM 的读写操作.时序控制单元主要由状态机实现.

4 仿真结果

图 6 是电路的仿真波形,图中 m_initial 为初始的信号源,m_fec_raw 为经过(2,1,7)卷积码编码器后的编码数据,m_fec_noise 为加了信噪比为 5 的高斯白噪声后的编码数据.电路对 m_fec_noise 数据进行译码,done 为译码完成标志信号,code 为译码后的输出结果.由图中数据可知虽然加入噪声后,m_fec_noise 与 m_fec_raw 相比,出现了一些误码,但是译码后的结果 code 的值和初始信号源 m_initial 的值一致.可见,维特比译码器电路正常工作,并能够对接收数据中的一些错误进行纠正.

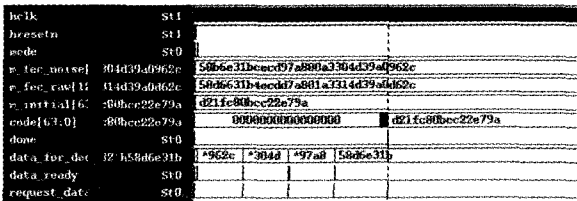


图 6 维特比译码器电路功能验证的仿真波形图

用 Synopsys 的 Design Ware 工具在中芯国际 (SMIC)0.18 μm 的工艺下对以上维特比译码电路进行综合,综合结果如表 1 所示.

5 结束语

本文针对导航系统中使用的(2,1,7)卷积码编码器,设计了一个串行的维特比译码器.充分复用了加比选模块,采用回溯算法进行译码,很大程度上减小了电路的面积和功耗.电路通过 Synopsys 的 Design Ware 工具在中芯国际(smic)0.18 μm 的工艺

表 1 维特比译码器电路综合结果

面积		
组成部分	门电路数	百分比/%
分支度量单元	14	0.34
加比选单元	406	9.90
幸存路径管理单元	3 403	82.96
时序控制单元	279	6.80
Total	4 102	100
功耗		
399.514 1 μW		
最高工作频率		
100 MHz		

下综合得到的芯片面积为 4 102 门,功耗为 399.514 1 μW .仿真结果表明,该电路在噪声的信噪比不是太低的情况下,能够很好地纠正传输过程中的错误.

参考文献:

[1] Navstar global positioning system interface specification [EB/OL]. (2004-12-07) [2010-02-01]. <http://www.navcen.uscg.gov/gps/geninfo/IS-GPS-200D.pdf>.

[2] Galileo open service signal in space interface control document [EB/OL]. (2006-05-23) [2010-02-01]. <http://www.galileoic.org/la/files/Galileo%20OS%20SIS%20ICD%20230506.pdf>.

[3] U S Department of Transportation Federal Aviation Administration, Specification for the Wide Area Augmentation System (WAAS) [EB/OL]. (2001-08-13) [2010-02-01]. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/documents/media/waas/2892b_C2a.pdf.

[4] Shu Lin, Daniel J Costello, Jr. 差错控制编码[M]. 晏坚,何元智,潘亚汉,等译. 北京:机械工业出版社,2007.

[5] 黄载禄,殷蔚华,黄本雄. 通信原理[M]. 北京:科学出版社,2007.

[6] Chao Cheng, Parhi K K. Hardware efficient low-latency architecture for high throughput rate viterbi decoders [J]. IEEE Trans Circuits and Systems II: Express Briefs,2008,55(12):1254-1258.

[7] 黄君凯,王鑫. 一种高速 Viterbi 译码器的优化设计及 Verilog 实现[J]. 微电子学与计算机,2005,22(2):178-182.

其他用户能从密文 σ 中恢复出消息 m . B 在多接收者代理签密阶段给出 $\omega_j = e(P_j + P_{SA}, Q_j)^k$, 则攻击者由 $R = kP$ 求出 k , 进而伪造 (ω_j, c_j) 以通过 $c_j = H_2(\omega_j) \oplus m$ 恢复消息明文是不可行的, 因为这相当于解决 ECDL 难题.

另一方面, 如果某个攻击者能够计算出 $\omega_j = e(R, S_j) = e(kP, (r_j + s)Q_j) = e(P, P)^{kab}$, 这就相当于已知 $R = kP, Q_j = aP, (r_j + s)P = bP$, 求出了 $e(P, P)^{kab}$, 这和 BDH 困难问题相矛盾. 则攻击者从 (m_w, R, c, S) 提取出消息 m 是不可行的. 由此可见, 本文方案满足保密性.

5.3 不可否认性

虽然只有代理签密人 B 才能声称有效的多接收者代理签密, 但是仅仅只有指定的多个接收者利用其私钥才能正确恢复出消息 m , 并在这个基础上验证 (m_w, R, S) 的有效性, 因此, 代理签密人 B 无法否认曾经向多个接收者发送过关于消息 m 的有效密文.

5.4 强可识别性

完整有效的密文中有原始签密人所建立的授权许可证 m_w , 而 m_w 中有代理签密人的身份信息, 任何第三方都可以从 m_w 中确定相应代理签密人的身份.

5.5 抗滥用性

由于授权许可证 m_w 出现在验证阶段的验证式中, 而且代理密钥中包含有原始签密人的授权信息, 因此, 代理签密人不能签署未经授权的信息, 只能用于产生有效密文, 当然他也不能把代理签密权力转给其他人.

6 结束语

本文构造的基于 pairings 的自认证多接收者代理签密方案, 实现了在特定情形下代理签密人代替

原始签密人行使签密权力, 并将密文发送给多个指定的接收者, 在整个多接收者代理签密阶段和验证阶段仅使用了 $2n+1$ 次双线性对运算, 计算效率很高, 因而适合应用于代理签密中具有多个密文接收者的电子政务和电子商务活动中.

参考文献:

- [1] Wang Q, SAo Z F. Two proxy signcryption schemes from bilinear pairings[C]// Proceedings of SANS 2005. Berlin: Springer-Verlag, 2005:161-171.
- [2] Wang Meng, Li Hui, Liu Zhijing. Efficient identity-based proxy signcryption schemes with forward security and public verifiability[C]// The Third International Conference on Networking and Mobile Computing (ICCNMC 2005). Berlin: Springer-Verlag, 2005:982-991.
- [3] Li Xiangxue, Chen Kefei. Identity-based proxy signcryption scheme from pairings[C]// Proceedings of the IEEE International Conference on Service Computing (SCC). Los Alamitos, California: IEEE Computer Society Press, 2004: 494-497.
- [4] 宋文敏, 杨广林. 一个扩展的基于身份的签密方案. 微电子学与计算机, 2006, 23(10):138-140.
- [5] 张学军, 王育民. 高效的基于身份的代理签密[J]. 计算机工程与应用, 2007, 43(3):109-111.
- [6] 胡振鹏, 钱海峰, 李志斌. 基于身份的多接收者的代理签密方案[J]. 华东师范大学学报: 自然科学版, 2008(1): 83-88.
- [7] 俞惠芳, 王彩芬. 一个高效的自认证签密方案[J]. 计算机工程, 2009, 35(16):138-139, 142.

作者简介:

俞惠芳 女, (1972-), 副教授, 工学硕士. 研究方向为信息安全、现代密码学.

王之仓 男, (1974-), 副教授, 工学硕士. 研究方向为信息安全、神经网络.

(上接第 57 页)

- [8] He Jinjin, Wang Zhongfeng, Cui Zhiqiang, et al. Towards an optimal trade-off of Viterbi decoder design [C]// IEEE Int. Symposium, Circuits and Systems. Island of Kos: IEEE Circuits and System Society. 2009: 3030-3033.
- [9] Truong T K, Shih M T, Reed I S, et al. A VLSI design for a trace-back Viterbi Decoder[J]. IEEE Trans Com-

mun, 1992, 40(3): 616-624.

作者简介:

桂琼 女, (1985-), 硕士研究生. 研究方向为专用集成电路设计和应用.

李晓江 男, (1972-), 硕士生导师. 研究方向为专用集成电路设计和应用.