

基于 FPGA 交织编码的设计与实现

王 钢, 高宏亮

(哈尔滨工业大学 通信技术研究所, 黑龙江 哈尔滨 150001)

摘 要:介绍了一种适用于无线数据传输系统的纠错编码及数据交织方案. 本方案是用交织的方法, 将突发错误离散成随机错误, 然后用纠随机错误的增余汉明码给予纠正. 在介绍增余汉明码的编码方法和交织提高信道抗突发干扰能力的原理的基础上, 分析了此方案的纠错能力, 给出了采用 VHDL 语言实现增余汉明码和交织的方法, 并通过 Quartus II 软件进行仿真验证.

关键词:增余汉明码; 交织; FPGA

中图分类号: TN919.72 **文献标识码:** A **文章编号:** 1007-2683(2009)01-0063-04

Design and Implementation of Interleaved Coding Based on FPGA

WANG Gang, GAO Hong-liang

(Communications Technology Research Institute, Harbin Institute of Technology, Harbin 150001, China)

Abstract: This paper introduces an error-correcting coding and interleaving scheme in wireless data transmission system. The scheme uses interleaving to transmit burst errors into random errors, and then corrects the random errors by extended hamming code which usually used to correct random errors. After introducing the coding method of extended hamming code and the theory of improve the ability of anti-interference by using interleaving, we analyze its ability of error correction, then a method to implement the coding in VHDL language is given, and is validated by software simulation in Quartus II.

Key words: extended hamming code; interleaving; FPGA

1 引 言

汉明编码属于线性分组码, 具有原理简单、实现容易、纠错能力强等特点, 因而在现代数字通信系统中得到了广泛应用. 在前向纠错 (FEC) 系统中, 发端发送具有一定纠错能力的码, 收端译码时, 若传输中产生差错的数目在码的纠错能力之内, 译码器可以对差错进行定位并自动加以纠正. 反之, 若差错数目大于纠错能力则无能为力. 因此对于无线信道中的突发错误, 汉明码必须经过一定的处理, 以使其能够抵抗一定程度的突发错误. 交织技术使得信道的突发错误分散开来, 把突发差错信道改造成独立的随

机差错信道, 从而充分发挥纠错编码的作用. 因此在增余汉明码的基础上进行交织的方法可以使无线信道中的随机错误和突发错误都得以纠正, 很适合在小型无线数据传输系统中应用.

2 增余汉明码和交织的原理

2.1 增余汉明码的编译码原理

汉明码 (Hamming Code) 是由 Richard Hamming 于 1950 年提出的, 它属于线性分组编码方式.

设原代码的码长为 k bit, 附加纠错编码部分为 r bit, 当码字长度 $n = 2^r - 1$, $r = n - k$ 时就称这种线性分组码为汉明码. 其基本原理是: 将信息码元与监

督码元通过线性方程式联系起来,每一个监督位被编在传输码字的特定比特位置上.系统对于错误的码元无论是原有信息位中的,还是附加监督位中的都能把它分离出来.

对于一个 (7, 4) 汉明码, 它的校验矩阵为

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

在 (7, 4) 汉明码的基础上, 再增加一位监督元, 它取为所有码元的模 2 加, 这样使汉明码的最小码距 $d_{\min} = 4$, 可以在纠正一位错的同时检两位错, 这种线性分组码称为增余汉明码, 也称为扩展汉明码. 至此可以写出 (8, 4) 赠余汉明码的校验矩阵为

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (2)$$

发送码组 C 在传输过程中可能发生误码, 设接收到的码组为 $R = [r_{n-1}, r_{n-2}, \dots, r_0]$, 则收发码组之差为 $E = R - C = [e_{n-1}, e_{n-2}, \dots, e_0]$, 其中

$$e_i = \begin{cases} 0, & r_i = c_i \\ 1, & r_i \neq c_i \end{cases} \quad i = 1, 2, \dots, n-1 \quad (3)$$

上式也可写作 $R = C + E$, 在接收端计算 $S = RH^T = (C + E)H^T = CH^T + EH^T$, 由于 $CH^T = 0$, 所以 $S = EH^T$, S 称为接收码组 R 的校验子或伴随式. 由矩阵 H 进行译码, 根据所得的伴随式就可判断码字中哪一位码元发生了错误, 就可纠正一位随机错误. 伴随式只与错误图样 E 有关, 可以用 S 作为判别错误的参量, 如果 $S = 0$, 则接收到的是正确码字, 若 $S \neq 0$, 则说明 R 中存在着差错.

2.2 交织技术的基本理论

交织是通信系统中进行数据处理而采用的一种技术, 交织从其本质上来说就是一种实现最大限度的改变信息结构而不改变信息内容的技术. 输入的信息序列经过交织之后, 所得到的输出序列的顺序将发生改变. 长度为 N 的交织可以用 N 个整数 $\pi(0), \pi(1), \pi(2) \dots \pi(N-1)$ 来表示, 交织的过程可以理解为: 交织器在第 i 时刻的输出等于第 $\pi(i)$ 时刻的输入信号. 长度为 N 的交织器会引起 N 个单位的延时. 一个给定的交织, 其解交织就是把经过交织打乱之后的序列恢复成原始序列, 交织和解交织是两个互逆的过程. 在设计交织器时, 应考虑具体应用系统的数据帧的大小, 使交织深度在满足时延要求的前提下, 与数据帧大小一致, 或是数据帧长度的

整数倍^[1].

若信道编码只使用增余汉明码, 由于它只能纠正一位错误, 所以用于纠错时, 当发生了两位或两位以上的突发错误, 必然导致译码时错误不能纠正. 而加上交织后, 当码字中出现长度小于交织长度的突发错误时, 解交织后每 8 个码元中的错误不大于 1 位, 在译码时就能给以纠正. 因此采用交织技术可以大大提高信道抗突发干扰的能力.

3 方案的可靠性分析

最小码距为 $d_{\min}$ 的分组码, 能检出所有 $d_{\min} - 1$ 位或更少位错误的错误图样. 它不能检测出所有的 $d_{\min}$ 位错误, 但至少检出一些 (大部分) $d_{\min}$ 位或更多位的码元错误. 事实上, (n, k) 码能检出长度为 n 的 $(2^n - 2^k)$ 个错误图样. 因为禁用码字的个数为 $2^n - 2^k$, 收到禁用码字就等于检出错码.

令一个 (n, k) 线性分组码, A_i 为码组中重量为 i 的码字的个数, 码字集合的重量分布为 $A_0, A_1, \dots, A_n$. 这时码字在误码率 (转移概率) 为 p_e 的 BSC 信道的漏检概率为

$$P_u = \sum_{i=0}^n A_i p_e^i (1 - p_e)^{n-i} \quad (4)$$

其中: $p_e^i (1 - p_e)^{n-i}$ 为错误图样中出现 i 个 1, $n - i$ 个 0 的概率; A_i 为此错误图样分布正好错成许用码字的数量. 也就是错误图样等于许用码字的可能性就是漏检概率.

(8, 4) 赠余汉明码的重量分布为: $A_0 = 1, A_1 = A_2 = A_3 = 0, A_4 = 14, A_5 = A_6 = A_7 = 0, A_8 = 1$. 根据式 (4) 可得 $P_u = 14p^4 (1 - p)^4 + p^8$. 当 $p_e = 10^{-3}$ 时, 漏检概率为 1.4×10^{-11} .

当 (n, k) 分组码的最小码距为 $d = 2t + 1$ 时, 它可以纠正 t 个或更少的错误. 但实际上, 纠错能力为 d 的分组码还可以纠正一些 $t + 1$ 位或更多位错误的错误图样, 但较难精确计算, 其错误译码概率的上限为

$$P_E \leq \sum_{i=t+1}^n C_n^i p_e^i (1 - p_e)^{n-i} \quad (5)$$

对于 (8, 4) 赠余汉明码, 其错误译码概率的上限为 6×10^{-5} . 在无线突发信道中, 采用交织和不采用交织相比, 误码性能改善十分明显, 一般可以达到 2~3 个数量级^[2]. 因此, 采用增余汉明码和交织结合的编码方法可以将系统误码率从 10^{-3} 至少提高到 10^{-6} .

4 增余汉明码编译码的 FPGA 实现

增余汉明码的编译码可以按照增余汉明码编译原理,用 VHDL 语言进行程序实现,并通过 Quartus II 软件进行仿真.图 1 和图 2 分别为 (8,4) 增余汉明码的编码和译码仿真图.在图 2 中 decoding_error=0 表明无误码或者有一位错误,可以纠正,decoding_error=1 表明有一位以上的错误,不可以纠正,此时译码结果输出 0000.将上述结果与理论上编译码结果对照可知仿真结果准确无误.

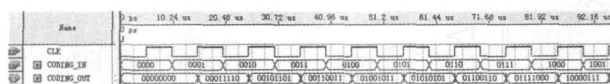


图 1 (8,4) 增余汉明码的编码时序仿真图

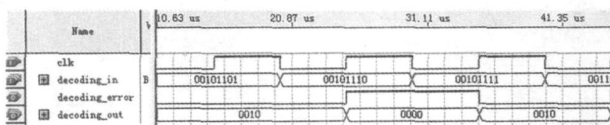


图 2 (8,4) 增余汉明码的译码时序仿真图

5 交织技术 FPGA 实现

对于不同交织器而言,区别只是交织表不一样,在电路中表现为读写地址的顺序不同^[3].因此,可以得到如下设计思路:一片 ROM 存放交织地址,一片 RAM 作随机存储器,由一个计数器产生顺序地址.当需要顺序地址时,选择器选择计数器的输出送至 RAM 地址线;当需要交织地址时,先将计数器的输出送至 ROM 地址总线,选择器再选择从 ROM 读出的交织地址送至 RAM 的地址线,由此可得框图如图 3 所示.

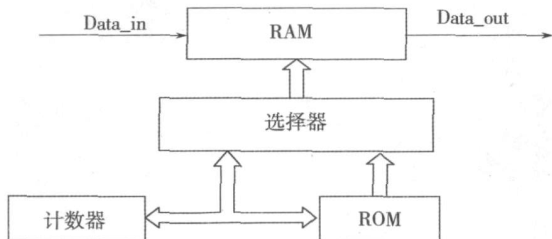


图 3 交织器框图

交织时,计数器产生的顺序地址分别作为 RAM 的写入地址和 ROM 的读出地址,ROM 读出的数据

作 RAM 的读出地址;反交织时,计数器产生的顺序地址作为 ROM 的读出地址和 RAM 的读出地址.从 ROM 读出的数据作 RAM 的写入地址.

交织器的实现主要有固定交织和随机交织两种方法,随机交织的思想使编码的性能达到最佳^[4],但不易于硬件实现.为了容易验证结果的正确性,本文用 VHDL 语言编程实现了 5×6 行列交织,并通过 Quartus II 软件进行仿真验证.若要实现其他的交织器,区别只是交织表不一样.其流程如图 4 所示.图 5 为截取的一段仿真波形,在 start 上升沿后开始交织,在 clk 的上升沿对 RAM 进行写入,经过 30 个脉冲后开始读出.由图 5 可知,写入的二进制码流为: 111101100110001101100011100001 写入完毕后,由图可见,读出的数据为: 110111000010100111000101010111.将上述结果和交织表对照可知仿真结果准确无误.

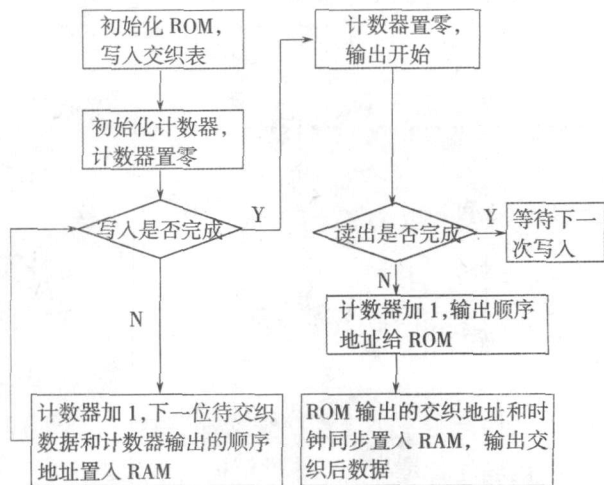


图 4 交织程序的设计流程

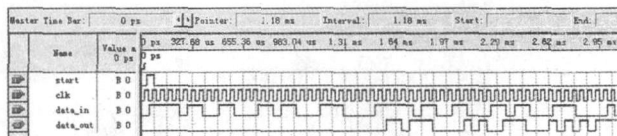


图 5 交织时序仿真图

若输入是连续的比特流,由于交织技术的存在使得编码过程是按数据帧来进行处理的,因此需要缓存数据帧以保证编码过程的出入平衡^[5].可采用图 6 所示的方案对数据进行处理,一个 RAM 接收顺序输入数据,同时另一个 RAM 输出交织后的数据;当接收完一帧数据的同时也刚好发送完前一帧数据,此时交换 2 个 RAM 的工作方式,然后重复上述操作.这样就可以实现对数据的连续处理.

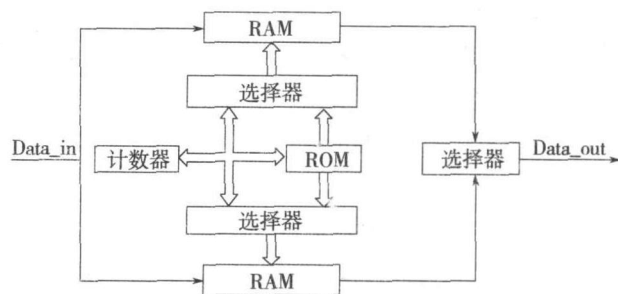


图 6 对数据的连续处理框图

6 结 语

在增余汉明码的基础上进行交织的方法可使通信中的突发错误得以纠正,交织使得在码率不变的前提下,提高系统的可靠性.文中给出了基于 FPGA 的该方案的实现方法,该方法具有通用性,对于不同的交织方法,只是 ROM 中存储的交织表不一

样,易于仿真测试和修改,加强了系统的灵活性.该方案已成功应用于某数据指令传输系统中,证明该方案切实可行.

参 考 文 献:

- [1] 卢明林,毕成余. Turbo 码中交织器的设计及性能分析 [J]. 信息技术, 2007 (5): 150 - 152
- [2] 左艳军,席志红. 无线突发信道中抗突发错误 BCH 码交织编码的性能分析 [J]. 应用科技, 2004, 31 (8): 19 - 21.
- [3] 杨海芬. Turbo 码编译码方法研究与实现 [D]. 成都:西南交通大学, 2003: 32 - 35.
- [4] ANDERSON J D, GLAVIKUS A. Interleaver Design for Turbo Coding [J]. Proc. Inter Symp. on Turbo Codes and Related Topics, 1997, 9: 255 - 258
- [5] 江 森,苏祥芳,肖东亮. 卷积 Turbo 码编码器及 CPLD 实现 [J]. 武汉大学学报 (理学版), 2001, 47 (3): 359 - 363.

(编辑:付长缨)

(上接第 62 页)

6 结 语

本文构造了一类新型门限代理签名. 这个新型的代理签名是基于双线性对的门限代理签名方案,并且能够进行代理保护. 经过分析,该方案既安全又有效率,适合应用于移动电子商务的各个方面.

参 考 文 献:

- [1] MANBO M, USUDA K, OKAMOTO E. Proxy Signatures for Delegating Signing Operation [C] // Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, 1996: 48 - 57.

- [2] MANBO M, USUDA K, OKAMOTO E. Proxy Signatures: Delegation of the Power to Sign Messages [J]. IECE Trans. Fundam., 1996, E79 - A (9): 1338 - 1354.
- [3] SUN H M, LEE N Y, WANG H T. Threshold Proxy signatures [J]. IEEE Proc. Computers & Digital Techniques, 1999: 146 (5): 259 - 263.
- [4] 李继国,曹珍富. 一个改进的门限代理签名方案 [J]. 计算机研究与发展, 2002, 39 (11): 1513 - 1518
- [5] SUN H M. A Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers [J]. Computer Communications, 1999, 22 (8): 717 - 722.

(编辑:付长缨)