

并行 CRC-32 校验码生成算法研究及其实现

郭熙业, 苏绍璟, 王跃科

(国防科学技术大学 机电工程与自动化学院仪器系, 湖南 长沙 410073)

摘要: 在分析串行结构 CRC 生成算法的基础上, 提出了一种高效的 8bit 并行 CRC-32 校验码生成算法。利用该算法在特定 FPGA 芯片上实现了任意字节的 CRC-32 校验码的生成模块, 该模块仅占用 93 个逻辑单元, 最高数据吞吐量可达 2 400Mbps。

关键词: 并行 CRC-32 状态转移矩阵

随着网络数据业务的快速增长, 以太网作为局域网的发展主流经历了从 10Mbps、100Mbps 到 1Gbps 的过程, 目前正向 10Gbps 以太网方向发展。千兆以太网数据速率达到了 Gbps 级, 若辅以其他技术, 就可以支持多媒体应用, 因而以太网化应用领域日益广泛。然而, 千兆以太网中物理层具有潜在的不稳定性, 例如, 在依赖链路和数据特性的基础上, 在发送帧中加入足够的冗余信息, 就能够在接收端检测出错误并安排受损帧的重发。虽然循环冗余校验 CRC(Cyclic Redundancy Check)具有强大的检错能力并在以太网的数据链路层 MAC 部分实现中得到应用。但传统意义上串行移位结构的 CRC, 其数据吞吐量远远达不到千兆以太网 1Gbps 的要求。本文在深入分析串行结构 CRC 生成算法的基础上, 设计并实现了一种针对 8bit 宽度数据输入的并行 CRC-32 校验码生成算法。

1 串行结构 CRC-32 校验码生成方法的分析

CRC 校验码的编码方法是用待发送的二进制数据 $t(x)$ 乘上 x^r 再除以生成多项式 $g(x)$ 完成的, 最后的余数即为 CRC 校验码, 其中, r 为生成多项式的阶数。根据上述原理, 在串行结构的实现方法中采用移位寄存器构成除法电路, 寄存器的数量与生成多项式 $g(x)$ 的阶数一致。数据 $t(x) \cdot x^r$ 以二进制位方式依次串行输入除法电路中, 当数据输入完毕时, 除法电路中寄存器的值即为生成的 CRC 校验码。

千兆以太网协议中规定, 采用 CRC-32 的方式对数据进行编码, 其生成的多项式为: $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$ 。对应的串行结构 CRC-32 校验码生成原理如图 1 所示。

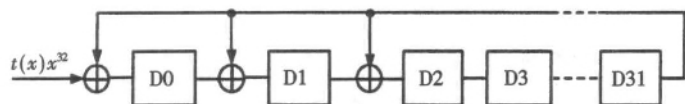


图 1 串行结构 CRC-32 校验码生成原理

当 $t(x)$ 为 8bit 时, 可将数据表示为多项式: $t_7x^7+t_6x^6+t_5x^5+t_4x^4+t_3x^3+t_2x^2+t_1x^1+t_0$, 多项式的系数即为待编码的二进制数据。串行结构内寄存器的初始值为 '0', 电路开始工作后, 二进制数据序列 $(t_7, t_6, t_5, t_4, t_3, t_2, t_1, t_0, 0, 0, \dots, 0)$ 按照从左至右的次序输入除法电路(其中 '0' 的个数为 32), 当数据序列输入完毕时, 除法电路中寄存器的值即为生成的 CRC-32 校验码^[1]。该电路具有以下特点:

(1) 由于寄存器的初始值为零, 因此, 在二进制数据序列 $(t_7, t_6, t_5, t_4, t_3, t_2, t_1, t_0)$ 输入除法电路过程中, D31 的反馈值始终为 0, 从而保证了二进制序列在数据移位过程中不受反馈值 '异或' 运算的影响。当 $(t_7, t_6, t_5, t_4, t_3, t_2, t_1, t_0)$ 输入完毕时, 寄存器(D0, D1, D2, D3, D4, D5, D6, D7)的值对应为: $(t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7)$, 其他寄存器的值为 '0'。

(2) 在 $(t_7, t_6, t_5, t_4, t_3, t_2, t_1, t_0)$ 输入完毕后, 随后输入 32 个 '0', 由于 '0' 在 '异或' 运算中不起作用, 因此, 输入 '0' 的过程可认为是除法电路在没有输入数据的情况下进行自反馈式的移位运算。

因为在千兆以太网中, 数据传输速率达到了 Gbps 级, 如果采用每个时钟周期计算 1bit 数据的串行结构, 很难实现 CRC 校验码的生成。因此, 有必要研究并行的 CRC 校验码编码方法。

2 8bit 并行 CRC-32 校验码生成方法的原理

自反馈的移位运算可以采用状态转移矩阵表示, $i+1$ 次移位后寄存器的状态 Q_{i+1} 与 i 次移位后寄存器的状态 Q_i 之间的关系可通过状态矩阵 A 表示为: $Q_{i+1}=AQ_i$, 进一步又可得到第 i 次的状态 Q_i 可通过初始状态 Q_0 表示为:

$$Q_i=A^iQ_0 \quad (1)$$

CRC-32 的状态转移矩阵 A 如图 2 所示。

结合串行结构的特点(2)及公式(1), 可得出: 当二进制序列 $(t_7, t_6, t_5, t_4, t_3, t_2, t_1, t_0, 0, 0, \dots, 0)$ 输入完毕时, 寄存


```

        crc_out := (others => '-');
    else
        fcs_shifted(23 downto 0) := fcs(31 downto 8);
        fcs_shifted(31 downto 24) := x"00";
        fcs <= fcs_shifted xor crc;
    end if;
    fcs_out <= (others => '-');
    elsif crc_en = '0' then
        fcs_out <= not fcs;
        fcs <= (others => '-');
        fcs_shifted := (others => '-');
        crc_out := (others => '-');
    end if;
end if;
end process;
end check_crc;

```

程序中: 'clk' 代表时钟信号, 'crc_en' 代表使能信号, 'rst' 代表复位信号, 'data_in' 代表输入的任意的 8bit 数据, 'fcs_out' 代表生成的校验码。另外, 程序中 'crc' 和 't' 满足图 3 所示的运算关系。由于这部分描述在前面已经介绍过, 因此在程序中省略。

目前, 该方法已在 Altera 公司的 StratixGX40 系列 FPGA 芯片上实现, 仅占用 93 个逻辑单元, 便可实现任意字节的 CRC-32 校验码的计算, 最高数据吞吐量达到 2400Mbps, 完全能够满足千兆以太网的数据传输速度要求。图 4 为输入特定 10 个字节时校验码生成模块的仿真结果, 生成的校验码与低速率情况下采用串行结构生

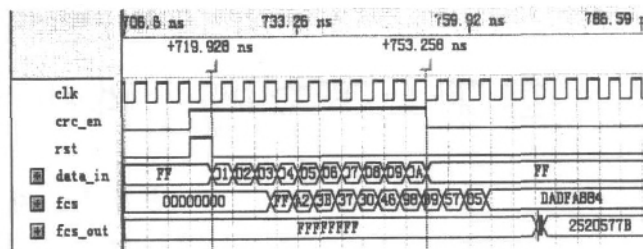


图 4 多字节 CRC-32 校验码生成模块仿真波形

成的校验码完全一致。

本文以千兆以太网 CRC-32 校验码的生成算法作为研究对象, 深入分析了串行结构的实现方法, 并根据数据 '0' 在异或运算中不影响运算结果的特性, 总结出串行结构实现方法的两个特点, 并在此基础上提出一种高效的 8bit 并行 CRC-32 校验码生成算法。该算法与传统的利用状态转移矩阵实现并行运算的方法相比^[3], 其状态转移方程更加简单, 校验码可由输入的 8bit 数据经过 '异或' 运算直接得到, 从而更加便于硬件实现。

参考文献

- [1] 王新梅, 肖国镇. 纠错码—原理与方法[M]. 西安: 电子科技大学出版社, 1991.
- [2] CUNNINGHAM D G, PH.D, LANE W G, et al. 千兆以太网[M]. 北京: 清华大学出版社, 2000.
- [3] NG S L, DEWAR B. Parallel realization of ATM cell header CRC[J]. Communications, 1996, (19): 257-263.
- [4] 朱荣华. 一种 CRC 并行计算原理及实现方法[J]. 电子学报, 1999, 27(4): 143-145.

(收稿日期: 2006-10-10)



赛灵思推出新型低成本 SPARTAN- DSP 系列

XtremeDSP 解决方案为无线和视频应用带来突破性的价格、性能和功耗优势组合

全球可编程解决方案领先供应商赛灵思公司 (Xilinx, Inc. (NASDAQ: XLNX)) 日前宣布推出首个低成本 Spartan™-DSP 系列产品以及相应的开发板和增强设计软件, 极大地扩展了其 XtremeDSP™ 解决方案的产品线, 并且在价格、性能和功耗三合一组合方面为数字信号处理树立了新的标杆。Spartan- DSP 以业界最低的成本价格提供了高达 20GMACS (每秒十亿次乘法累计) 的 DSP 功能, 而价格不到 30 美元。与同类的其它高性能可配置 DSP 器件相比, 该系列产品的动态功耗降低达 50%。

新推出 Spartan- DSP 系列之后, XtremeDSP 产品线就有了三个针对 DSP 优化的平台。丰富的器件选择为 DSP 工程师提供了巨大的灵活性, 从而使他们能够选择最佳的器件性能组合来满足应用要求, 并可方便地实现不同平台间的设计移植。作为 Spartan- DSP 系列中的第一个平台, Spartan- 3A DSP 是一款成本效益最高的器件, 专门针对无线、视频和消费应用而优化, 这与性能更高的 Virtex™- DSP 系列形成互补, 相得益彰。Virtex™- DSP 系列中的 Virtex- 4 SX 和 Virtex- 5 SXT 平台瞄准的是高端应用, 如无线基站和包括监控、广播以及 3D 医疗图像在内的高分辨率视频应用。

这些最新产品可帮助设计人员更高效地实现日前成为趋势的 FPGA 可编程 DSP 协处理平台。在信号处理系统中, FPGA 经常与可编程 DSP (如 TI 的 TMS320 系列) 互补, 在信号处理链中实现系统逻辑复用和合并、新外设或总线接口以及性能加速器。此外, Spartan- 3A DSP 器件是赛灵思公司基于平台的 DSP 战略和 XtremeDSP 解决方案路线图的一部分。第三方 DSP 产品和服务供应商构成的全面行业生态系统为赛灵思的 DSP 战略和 XtremeDSP 解决方案路线图提供了强大支持。欢迎访问 www.xilinx.com/cn

(赛灵思公司供稿)