

多级分块 CRC 的快速配置方法

梁海华, 盘丽娜

(常熟理工学院 计算机科学与工程学院, 江苏 常熟 215500)

摘 要: 分块循环冗余校验(CRC)方法能够满足高速通信链路要求. 针对现在方法主要通过多项式公式推导和查表法实现, 较难推广的问题, 提出一种快速配置方法. 首先, 使用状态矩阵推导出 CRC 并行计算方法. 通过矩阵变换, 将余数计算和余数变换合并, 简化计算步骤, 实现多通道与并行位宽混合的多级分块 CRC 计算方法; 对长度可变数据的计算, 实现生成多项式、通道数、单通道并行处理位宽的任意配置. 仿真结果表明该方法进一步提高了分块 CRC 校验速度, 且增加通道数比并行位宽扩展更能提高运算性能.

关键词: 循环冗余校验; 快速配置; 多级分块; 生成多项式; 通道数; 并行位宽

中图分类号: TN915

文献标识码: A

文章编号: 1000-7180(2014)06-0060-04

Multilevel Block CRC's Fast Configuration

LIANG Hai-hua, PAN Li-na

(School of Computer Science and Engineering, Changshu Institute of Technology, Changshu 215500, China)

Abstract: Block Cyclic Redundancy Check (CRC) can meet the requirement of high-speed link. To overcome the drawbacks of the present CRC computation method which based on calculation of polynomial and lookup table, a fast configuration method was proposed. First of all, CRC parallel calculation method is derived by state matrix. According to the matrix exchanging, combined remainder calculation with remainder transformation to simplify the computation process. Multilevel block CRC computation is a hybrid method of multichannel and parallel width in which generator polynomial, the number of channels and the width of parallel processing can set arbitrarily. Simulation results show that new method can further improve the performance of CRC's computation, increasing number of channels is more efficient than expanding parallel width.

Key words: cyclic redundancy check (CRC); fast configuration; multilevel block; generator polynomial; number of channels; parallel width

1 引言

目前, 在计算机通信领域, 由于数据在传输或存储过程中会受到各种干扰产生误码, 从而需要进行数据校验来确保数据的完整性. 循环冗余校验(Cyclic Redundancy Check, CRC)是一种常用的方法^[1], 为了满足高速链路的需求, 文献[2]提出了分块校验的概念, 并给出了公式推导; Xu^[3]对其进行改进, 提出了多通道并行的计算方法, 其中每一个块的校验值需要两步计算获得, 最后, 所有分块校验值

异或获得 CRC 校验值(如图 1 所示); 两步计算即为余数计算和余数变换, 主要通过查表法或硬件电路实现. 针对上述方法通过多项式公式推导获得^[2-5], 较难快速推广和实现的问题. 本文从状态分析入手, 简化计算步骤, 分析多通道数 N 、并行位宽 w 对性能的影响.

2 并行 CRC 校验

首先给出假设, 生成多项式 $G(X) = p_m X^m + p_{m-1} X^{m-1} \cdots + p_1 X + p_0$ 的最高次幂是 m (长度为 m

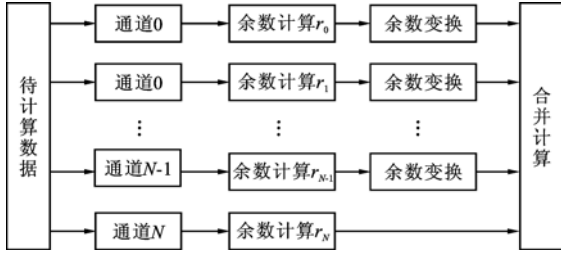


图 1 分块 CRC 多通道运算

+1), ($p_0, p_1, \dots, p_{m-1}, p_m$) 为生成多项式的低次项到高次项的系数, p_0, p_m 均为 1, 校验序列长度为 m , 为了使得 CRC 值生成与校验模块通用, 选用图 2 作为基本电路, 进行分析。

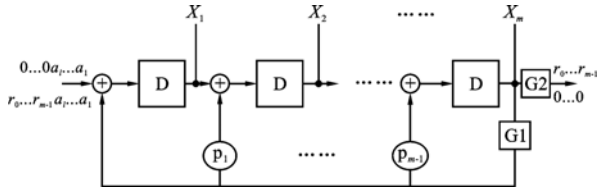


图 2 CRC 运算电路

计算 CRC 校验值时, 输入为 $a_1 \dots a_i 0 \dots 0$, 其中零为 m 个, $a_1 \dots a_i$ 为消息序列, 输出 $r_{m-1} \dots r_1 r_0$ 为生成的校验值, 寄存器初始状态 $INIT = (x_m \dots, x_2, x_1)$ 可以根据实际情况设置; 而校验 CRC 值时, 若无错误发生, 寄存器初始状态也为 $INIT = (x_m \dots, x_2, x_1)$, 输入为 $a_1 \dots a_i r_{m-1} \dots r_0$, 输出为全零序列, 否则有错误发生。

文献[6]中提出了常用的系统分析方法——状态矩阵分析法, 由文献[2]可知如下结论:

图 2 的状态方程为 $\mathbf{X}' = \mathbf{F}^w \otimes \mathbf{X} \oplus \mathbf{D}$ (此处 $\otimes$ 为异或、与构成的矩阵操作), $\mathbf{X} = (x_m \dots, x_2, x_1)^T$ 表示系统的初始状态 (零时刻), $\mathbf{D} = [0 \dots 0 \mid b_0 \dots b_{w-1}]^T$ 为 w 位输入, $\mathbf{X}'$ 表示 w 时刻的系统状态

$$(\omega \leq m), \text{ 其中 } \mathbf{F} = \begin{bmatrix} p_{m-1} & 1 & 0 & \dots & 0 \\ p_{m-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ p_1 & 0 & 0 & \dots & 1 \\ p_0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

该 m 维的方阵存在如下性质 $\mathbf{F}^i = [\mathbf{F}^{i-1} \otimes \mathbf{P} \mid \mathbf{F}^{i-1} \text{左}$

$$\text{起 } m-1 \text{ 列}], \text{ 其中 } \mathbf{P} = \begin{bmatrix} p_{m-1} \\ p_{m-2} \\ \dots \\ p_1 \\ p_0 \end{bmatrix}. \text{ 文献[7]将上述状态}$$

方程扩展到 $w > m$ 条件下。

设 m 位寄存器的初始值为 $INIT = 0$ 、输入处理

序列为 $a_1 \dots a_L$, 根据上述状态方程, 并行位宽为 m 位时, 计算结果 R 可进行如下推导 (如图 3 所示):

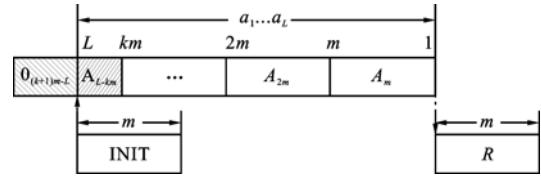


图 3 分块处理

$$\mathbf{R} = \mathbf{F}^m \otimes$$

$$\left[\dots \left[\mathbf{F}^m \otimes \left[\mathbf{F}^m \otimes \begin{bmatrix} 0_{(k+1)m-L} \\ \mathbf{A}_{L-km} \end{bmatrix} \oplus \mathbf{A}_{km} \right] \oplus \mathbf{A}_{(k-1)m} \right] \dots \right] \oplus \mathbf{A}_m = \mathbf{F}^{km} \otimes \begin{bmatrix} 0_{(k+1)m-L} \\ \mathbf{A}_{L-km} \end{bmatrix} \oplus \mathbf{F}^{(k-1)m} \otimes \mathbf{A}_{km} \oplus \mathbf{F}^{(k-2)m} \otimes \mathbf{A}_{(k-1)m} \dots \oplus \mathbf{F}^m \otimes \mathbf{A}_m = [\mathbf{F}^{L-m-1} \otimes \mathbf{P} \mathbf{F}^{L-m-2} \otimes \mathbf{P} \dots \mathbf{F} \otimes \mathbf{P} \mathbf{P} \mathbf{I}_{m \times m}] \otimes \begin{bmatrix} \mathbf{A}_{L-km} \\ \mathbf{A}_{km} \\ \dots \\ \mathbf{A}_m \end{bmatrix}$$

若电路的初始状态为非零, 根据图 2 的状态方程及以上的推导可知, 校验值需要增加一项 $\mathbf{F}^L \otimes INIT$, 即

$$\mathbf{R} = [\mathbf{F}^{L-m-1} \otimes \mathbf{P} \mathbf{F}^{L-m-2} \otimes \mathbf{P} \dots \mathbf{F} \otimes \mathbf{P} \mathbf{P} \mathbf{I}_{m \times m}] \otimes \begin{bmatrix} \mathbf{A}_{L-km} \\ \mathbf{A}_{km} \\ \dots \\ \mathbf{A}_m \end{bmatrix} \oplus (\mathbf{F}^L \otimes INIT) = \left[[\mathbf{F}^{L-m-1} \otimes \mathbf{P} \mathbf{F}^{L-m-2} \otimes \mathbf{P} \dots \mathbf{F} \otimes \mathbf{P} \mathbf{P}] \otimes \begin{bmatrix} \mathbf{A}_{L-km} \\ \mathbf{A}_{km} \\ \dots \\ \mathbf{A}_m \end{bmatrix} \right] \oplus \mathbf{A}_m \oplus (\mathbf{F}^L \otimes INIT) \quad (1)$$

3 多级分块 CRC 校验

为了提高运算速度, 需要并行处理数据块, 根据矩阵计算的特点, 可将式(1)进行多通道处理, 每一项都可以作为一个通道处理; 其中 $[\mathbf{F}^{L-m-1} \otimes$

$$\mathbf{P} \mathbf{F}^{L-m-2} \otimes \mathbf{P} \dots \mathbf{F} \otimes \mathbf{P} \mathbf{P}] \otimes \begin{bmatrix} \mathbf{A}_{L-km} \\ \mathbf{A}_{km} \\ \dots \\ \mathbf{A}_m \end{bmatrix}$$

可以进一步分块多通道处理, 设分块数为 $n \geq 1$, 每个分块处理的比特为 W , 故令 $\mathbf{F}_w = [\mathbf{F}^{W-1} \otimes \mathbf{P} \mathbf{F}^{W-2} \otimes \mathbf{P} \dots \mathbf{F} \otimes \mathbf{P} \mathbf{P}]$, 处理数据长度必须满足 $L \leq N \times W + m$, N 为可用

的最大通道数; $l = L - m$, 实际使用通道数 $n = \lceil \frac{l}{W} \rceil$ ($\lceil x \rceil$ 表示向上取整); 分块 CRC 多通道运算的配置如图 4 所示, 虚线框内左边表示将数据分成 n 块, 右边 $\Gamma_W, F^W \otimes \Gamma_W, \dots, F^{(N-1)W} \otimes \Gamma_W$ 表示对通道内 W 比特的序列进行运算。

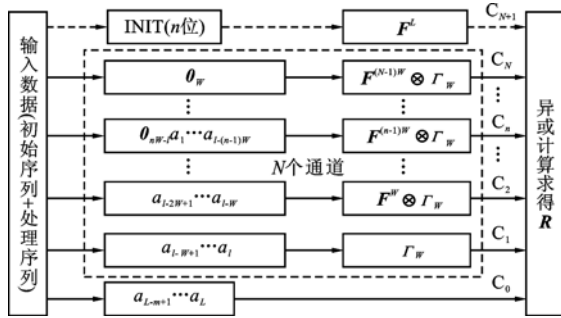


图 4 分块 CRC 多通道配置方法

单通道内的 $\Gamma_W, \dots, F^{(n-1)W} \otimes \Gamma_W$ 运算, 可以进一步分块, 形成如图 4 中虚线框内的多通道运算, 构成两级多通道处理; 也可以根据不同的并行位宽 $1 \leq w \leq W$ 进行运算^[7-8], 如图 5 所示 ($c_1 \dots c_w$ 为每个通道需要处理的序列), 形成多通道与并行位宽混合的两级处理, 其中 $\Gamma_w = [F^{w-1} \otimes P F^{w-2} \otimes P \dots F \otimes P P]$, 当 W 能被 w 整除时, $t = w$, 否则 $t = W - (\lceil \frac{W}{w} \rceil - 1) \times w$ 。

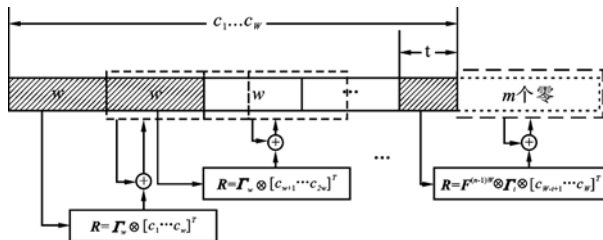


图 5 单通道内并行运算流程

上述图中每个 CRC 块可以再根据图 4 或图 5 进行多通道或并行位宽处理, 形成多级分块 CRC 运算

表 1 n (个)、 w (位) 分别对运算性能的影响

$n \times w$	(n, w)	耗时/s	(n, w)	耗时/s	(n, w)	耗时/s	(n, w)	耗时/s	$n \geq 2$ 平均耗时/s
1	(1, 1)	5.96							
2	(1, 2)	2.38	(2, 1)	1.93					1.93
3	(1, 3)	1.58	(3, 1)	1.06					1.06
4	(1, 4)	1.19	(2, 2)	0.68	(4, 1)	0.7			0.69
6	(1, 6)	0.8	(2, 3)	0.46	(3, 2)	0.34			0.4
8	(1, 8)	0.6	(2, 4)	0.34	(4, 2)	0.21			0.28
9	(1, 9)	0.54	(3, 3)	0.23					0.23
12	(1, 12)	0.4	(2, 6)	0.23	(3, 4)	0.17	(4, 3)	0.14	0.18
16	(1, 16)	0.31	(2, 8)	0.17	(4, 4)	0.11			0.14

方法。

对于可变长度数据 L , 由于通道 C_{N+1} 中需要计算 F^L , 无法满足快速配置的要求, 根据 CRC 运算电路特性, 当生成 CRC 值时, 设置输入的处理序列 $(a_1 \dots a_L) = (x_m \dots, x_2, x_1, a_0, a_1 \dots a_l, 0 \dots 0)$, 当为 CRC 校验时, 设置 $(a_1 \dots a_L) = (x_m \dots, x_2, x_1, a_0, a_1 \dots a_l, r_{m-1} \dots r_0)$; 同时去掉通道 C_{N+1} , 可提高对可变长度数据的处理速度。

4 实验与分析

为了探讨分块数 n 、并行位宽 w 对性能的影响, 根据图 4、图 5 的快速配置方法, 通过 MATLAB 进行模拟实验, 60 000 位伪随机序列作为输入, 求生成多项式 CRC16 的校验值 R 。取 $n = (1, 2, 3, 4)$ 、 $w = (1, 2, 3, 4, 6, 8, 9, 12, 16)$, 通过曲线拟合方法给出了两级分块多通道运算的耗时情况, 如图 6 所示。

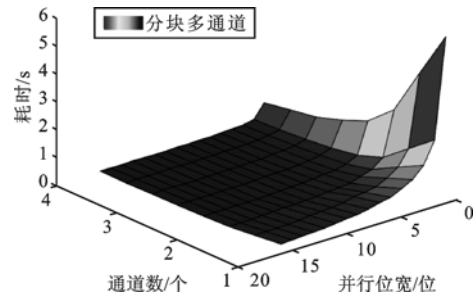


图 6 不同通道数、并行位宽下的运算耗时

当 $n = 1$ 位时, 即为文献[8]中描述的并行处理方法; 通过观察图 6 可知, w 的增加能够显著提高运算性能, 同时通道数 n 的能够进一步的提高运算性能。通过表 1 可分析 n 、 w 分别对性能的影响; 比较表 1 中的第 1 列、第 3 列与第 10 列数据, 发现多通道对运算性能的提高达到或超过单通道的 $n \times w$ 倍(文献[3]所述); 若 $n \times w$ 相同时, 比较表 1 中的每一行数据, 可知相对于 w 的增加, 通道数 n 的增加更能够提高性能。

5 结束语

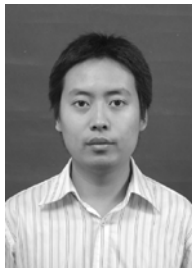
本文提出了一种CRC计算的多级分块快速配置方法,实验表明相对于并行位宽的增大,通道数的增加更能够提高运算性能.根据快速配置方法,通过硬件集成与实现^[9-11]鲁棒、高速的可变多级分块多通道CRC电路,提高运算性能需要进一步的探讨.

参考文献:

- [1] Tanenbaum A S. Computer networks[M]. 5th ed. New Jersey: Prentice Hall, 2010.
- [2] Ji H M, Killian E. Fast parallel CRC algorithm and implementation on a configurable processor[C]//2002 IEEE International Conference on Communications. CA, USA:IEEE, 2002:1813-1817.
- [3] 徐展琦,裴昌幸,董淮南.一种通用多通道并行CRC计算及其实现[J].南京邮电大学学报:自然科学版, 2008,28(2):53-57.
- [4] Nguyen G D. Fast CRCs[J]. IEEE Transactions on Computers, 2009,58(10):1321-1331.
- [5] Do Y J, Yoon S R, Kim T Y, et al. Highspeed parallel architecture for software based CRC[C]//2008 Consumer Communications and Networking Conference. NV, USA:IEEE, 2008:74-78.

- [6] Gajic Z. 线性动态系统与信号[M]. 王立琦,译. 西安:西安交通大学出版社,2004.
- [7] 梁海华,盘丽娜,赵秀兰,等. CRC查询表及其并行矩阵生成方法[J]. 计算机科学, 2012(S1):154-158.
- [8] 李双喜. 快速循环冗余校验编码方法及装置:中国, 200910085524.4[P]. 2010-12-01.
- [9] 王江,张盛兵,袁晓林. 面向IP复用的可配置并行CRC计算模块设计[J]. 计算机工程与科学, 2009, 31(1):103-105.
- [10] 阳璞琼,何怡刚,谭阳红,等. 超高频RFID系统CRC电路设计[J]. 电路与系统学报, 2009, 14(2):18-21.
- [11] 袁海洋,江先阳,刘锋,等. 应用于ROHC的CRC算法硬件实现[J]. 微电子学, 2011, 41(5):736-740.

作者简介:



梁海华 男,(1981-),硕士,讲师.研究方向为计算机数据通信、网络安全.

盘丽娜 女,(1981-),硕士,讲师.研究方向为通信网络规划与信道容量优化.

(上接第59页)

时采用粗调、细调结合的方式确定 r 的值,既能对图像各区域的方块效应有很好的去除效果,又能很好的对图像的纹理信息进行保护,进而更有效地去除块效应.

参考文献:

- [1] Tai S C, Chen Y R, Chen C Y, et al. Low complexity deblocking method for DCT coded video signal[J]. IEEE Proceedings Vision, Image and Signal Processing, 2006, 153(1):46-56.
- [2] Shen Meiyin, Kuo C C J. Review of postprocessing techniques for compression artifact removal[J]. Journal of Visual Communication and Image Representation, 1998,9(1):2-14.
- [3] Lisowska A. Moments-based fast wedgelet transform[J]. Math Imaging Vis, 2011, 39(2):180-192.
- [4] Friedrich F, Demaret L, Führ H, et al. Efficient moment computation over polygonal domains with an application to rapid wedgelet approximation[J]. SIAM J.

Scient. Comput., 2007,29(2):842-863.

- [5] Karunaseker S A, Kingsbury N G. A distortion measure for blocking artifacts in image based on human visual sensitivity[J]. IEEE Trans. on Image Processing, 1995, 4(6): 713-724.
- [6] Reeve H, Lim J. Reduction of blocking effect in image coding[C]//Acoustics, Speech, and Signal Processing; IEEE International Conference on ICASSP '83. Boston, 1983(8):1212-1215.
- [7] Zhang Xuequan, Gu Xiaodong, Sun Huixian. Deblock algorithm for compressed image based on adaptive space domain filtering[J]. Computer Engineering, 2009, 35(4): 218-220.

作者简介:

谢芳 女,(1988-),硕士研究生.研究方向为图像处理.

段昶 男,(1979-),博士研究生.研究方向为图像处理.

曹建蜀 男,(1970-),博士研究生,硕士生导师.研究方向为信号处理.