

CRC 生成与同构逆序校验方法

梁海华, 盘丽娜, 李克清

(常熟理工学院 计算机科学与工程学院, 江苏 常熟 215500)

摘 要: 循环冗余校验码(CRC)被广泛应用于通信领域, CRC 生成有两种电路: I 型、II 型. 现有的逆序校验方法是基于 II 型电路生成、I 型电路逆序校验, 存在 CRC 生成与逆序校验电路不同构的问题, 不利于模块化设计. 根据 I、II 型电路特性, 基于全状态转移矩阵, 给出一般情况下, 即 CRC 生成电路寄存器为非零初态时, CRC 生成 I 型或 II 型对应的同构 I 型或 II 型逆序校验方法. 生成与逆序校验同构后, 中间处理电路结构不变, 参数不同, 可以根据需要对其进行优化, 提高处理速率. 最后, 通过实例计算, 验证了同构逆序校验方法的正确性.

关键词: 循环冗余校验; 同构逆序校验; I 型电路; II 型电路; 非零初态; 全状态转移矩阵

中图分类号: TN915

文献标识码: A

文章编号: 1000-7180(2014)09-0167-03

CRC and Isomorphic Reverse Decoding

LIANG Hai-hua, PAN Li-na, LI Ke-qing

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

Abstract: Cyclic Redundancy Check (CRC) has already been used in the field of computer network widely. There are two kind of simple architecture processing bits serially: Type I, Type II. The existing reverse CRC method based on generating checksum by II and decoding it by I, the circuits were different so that model design was not easy. Depending on property of circuit I and II, full state transition matrix, CRC and its isomorphic reverse decoding method was derived even if initial register's state was not zeros. Thus, processing architecture is same but parameters is different when generating and decoding CRC. Architecture can be optimized to improve the processing rate if needed. Finally, examples verified the correctness of isomorphic reverse decoding.

Key words: Cyclic Redundancy Check (CRC); Isomorphic Reverse Decoding; Type I; Type II; Non-zero initial state; Full State Transition Matrix

1 引言

在计算机通信领域, 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^[1-2], Peterson 提出了两种串行编码电路^[3-4], 即 I 型、II 型电路. Liang^[5]提出了一种快速逆序校验方法, 该方法为 II 型电路生成 CRC 校验值, 通过 I 型电路进行 CRC 逆序校验, 但是 CRC 生成与校验电路结构不同, 无法对 CRC 处理进行模块化设计. 本文从电路

的状态矩阵入手, 根据 I 型、II 型电路的等价特性提出一种同构逆序 CRC 校验方法, 解决 CRC 生成电路寄存器为任意状态(零或非零)时, CRC 生成与逆序校验电路不同构问题.

2 I 型、II 型等效电路

首先给出假设, 生成多项式的最高次幂是 m (长度为 $m+1$), $(p_0, p_1, \dots, p_{m-1}, 1)$ 为生成多项式的低次项到高次项的系数, 校验序列长度为 m , 并行处理长度为 w , $x_i (1 \leq i \leq m)$ 为寄存器 i 的状态, 输入的处理数据为 $b_0 b_1 \dots b_n$.

收稿日期: 2013-11-28; 修回日期: 2014-01-12

基金项目: 国家自然科学基金资助项目(61202440, 61300186)

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[7]可知如下结论:

图1(其中G1、G2表示开关电路)的状态方程为 $\mathbf{X} = \mathbf{F}^w \otimes \mathbf{X} \oplus \mathbf{D}$ (此处 $\otimes$ 、 $\oplus$ 为模2运算), $\mathbf{D} = [0 \cdots 0 \mid b_0 \cdots b_{w-1}]^T$ 为 w 位输入, $\mathbf{X} = (x_m \cdots, x_2, x_1)^T$ 表示系统的初始状态(零时刻), $\mathbf{X}$ 表示 w 时刻的系统状态 ($w \leq m$), 其中 $\mathbf{F} =$

$$\begin{bmatrix} p_{m-1} & 1 & 0 & \cdots & 0 \\ p_{m-2} & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_1 & 0 & 0 & \cdots & 1 \\ p_0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

设输入的处理序列 $b_0 b_1 \cdots b_n 0_{m-1} \cdots 0_0$ 为 $a_1 \cdots a_L$ ($L = n + 1 + m$)、 $\mathbf{P} = (p_{m-1} \ p_{m-2} \ \cdots \ p_1 \ 1)^T$ 、 $\mathbf{INIT} = (x_m \ x_{m-1} \ \cdots \ x_2 \ x_1)^T$, 参考文献[8]推导可得校验值的全状态矩阵表示

$$\mathbf{R} = (\mathbf{F}^L \otimes \mathbf{INIT}) \oplus$$

$$\left(\left[\mathbf{F}^{L-m-1} \otimes \mathbf{P} \mathbf{F}^{L-m-2} \otimes \mathbf{P} \cdots \mathbf{F} \otimes \mathbf{P} \mathbf{P} \mathbf{I}_{m \times m} \right] \otimes \begin{bmatrix} a_1 \\ a_2 \\ \cdots \\ a_L \end{bmatrix} \right) \quad (1)$$

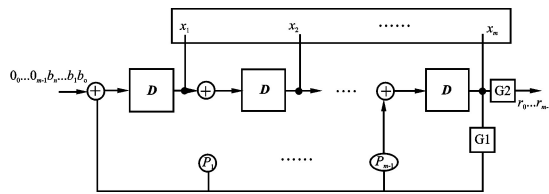


图1 $p_m X^m + p_{m-1} X^{m-1} + \cdots + p_1 X^1 + p_0$ ($p_0 = 1, p_m = 1$) 对应的 I 型 CRC 生成电路

图2存在类似结果 $\mathbf{X} = \mathbf{F}^w \otimes (\mathbf{X} \oplus \mathbf{D})$, $\mathbf{D} = [b_0 \cdots b_{w-1} \mid 0 \cdots 0]^T$ 为 w 位输入, $\mathbf{X} = (x_m, \cdots, x_2, x_1)^T$ 表示系统的初始状态(零时刻), $\mathbf{X}$ 表示 w 时刻的系统状态 ($w \leq m$), 其中 $\mathbf{F}$ 同上. 设输入的处理序列 $b_0 b_1 \cdots b_n$ 为 $a_1 \cdots a_L$ ($L = n + 1$)、 $\mathbf{P}$ 同上, $\mathbf{INIT}$ 同上为 m 位寄存器的初始值, 通过推导可得校验值的全状态矩阵表示

$$\mathbf{R} = (\mathbf{F}^L \otimes \mathbf{INIT}) \oplus$$

$$\left(\left[\mathbf{F}^{L-1} \otimes \mathbf{P} \mathbf{F}^{L-2} \otimes \mathbf{P} \cdots \mathbf{F} \otimes \mathbf{P} \mathbf{P} \right] \otimes \begin{bmatrix} a_1 \\ a_2 \\ \cdots \\ a_L \end{bmatrix} \right) \quad (2)$$

比较式(1)、(2)发现,由于 L 值在式(1)中比式(2)中大 m , 两式中第二项相等, 第一项相差 $\mathbf{F}^m$. 因

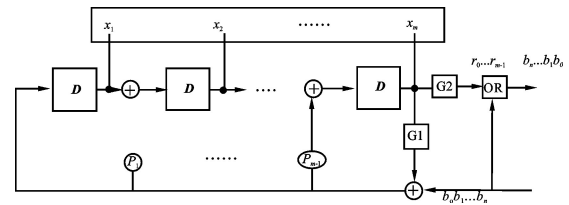


图2 $p_m X^m + p_{m-1} X^{m-1} + \cdots + p_1 X^1 + p_0$ ($p_0 = 1, p_m = 1$) 对应 II 型 CRC 生成电路

此,若图1中的初始状态为 $\mathbf{INIT}$, 图2中的初始状态为 $\mathbf{F}^m \otimes \mathbf{INIT}$ 时, I 型、II 型电路生成的 CRC 值相等, 两种电路等效; 同理, 若图2中的初始状态为 $\mathbf{INIT}$, 图1中的初始状态为 $\mathbf{F}^{-m} \otimes \mathbf{INIT}$ ($\mathbf{F}^{-1}$ 为 $\mathbf{F}$ 的逆矩阵, 文献[5]已证明其存在), 两种电路也等效.

3 同构逆序校验电路

由文献[5]可知, 如图2所示寄存器任意初始状态的 II 型 CRC 生成电路, 可以通过图3所示的 I 型电路(寄存器为零初态)进行校验, 电路输出结果为生成电路寄存器状态的逆序.

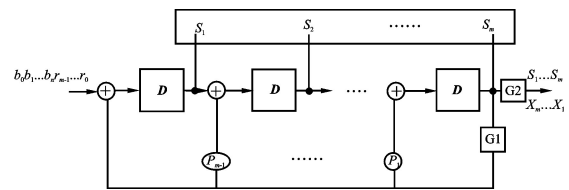


图3 $p_m X^m + p_{m-1} X^{m-1} + \cdots + p_1 X^1 + p_0$ ($p_0 = 1, p_m = 1$) 对应的逆序校验电路

上述 CRC 生成与逆序校验电路结构不相同, 为了生成与校验电路同构. 假设 CRC 生成采用 I 型电路(图1), 其初始状态为 $\mathbf{INIT} = (x_m \ x_{m-1} \ \cdots \ x_2 \ x_1)^T$, 输入序列为 $b_0 b_1 \cdots b_n 0_{m-1} \cdots 0_0$, 其等效电路为初始状态为 $\mathbf{F}^m \otimes \mathbf{INIT}$ 、输入序列为 $b_0 b_1 \cdots b_n$ 的 II 型电路(图2), I 型、II 型对应的生成多项式相同, 输出结果相同; II 型电路对应的 I 型逆序校验电路(图3), 计算结果为 $\mathbf{F}^m \otimes \mathbf{INIT}$ 的逆序, 而 I 型电路的同构逆序校验需要判断计算结果是否等于 $\mathbf{INIT}$.

需要将图3生成的结果 $S_m \ S_{m-1} \ \cdots \ S_2 \ S_1$

逆序、左乘 $\mathbf{F}^{-m}$ 获得 $\mathbf{INIT}$, 即 $\mathbf{INIT} = \mathbf{F}^{-m} \otimes \begin{bmatrix} S_1 \\ S_2 \\ \cdots \\ S_m \end{bmatrix}$,

文献[5]中可知

$$\mathbf{F}^{-1} = \begin{bmatrix} 0 & \cdots & 0 & 0 & 1 \\ 1 & \cdots & 0 & 0 & p_{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & 0 & p_2 \\ 0 & \cdots & 0 & 1 & p_1 \end{bmatrix}$$

$$\mathbf{F} = \begin{bmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{m-1} & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

通过观察可知 $\mathbf{F}^m \otimes \begin{bmatrix} S_m \\ S_{m-1} \\ \cdots \\ S_1 \end{bmatrix}$ 的计算结果为 **INIT** 的逆

序, $\mathbf{F}^m \otimes \begin{bmatrix} S_m \\ S_{m-1} \\ \cdots \\ S_1 \end{bmatrix}$ 对应为图3中输入序列末尾增加了

m 位零输入处理,其等效电路如图4所示,该图即为 I 型生成电路的同构逆序校验电路。

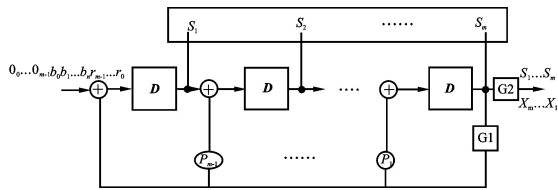


图4 I型生成电路的同构逆序校验电路

同理,可得图2所示 II 型生成电路同构逆序校验电路。

假设 CRC 生成采用 II 型电路(图2),其初始状态为 **INIT** = $(x_m \ x_{m-1} \ \cdots \ x_2 \ x_1)^T$, 输入序列为 $b_0 b_1 \cdots b_n$, 其等效电路为初始状态为 $\mathbf{F}^{-m} \otimes \mathbf{INIT}$ 、输入序列为 $b_0 b_1 \cdots b_n 0_{m-1} \cdots 0_0$ 的 I 型电路(图1);图1对应的同构逆序校验电路为图4所示的 I 型电路,该 I 型电路可以直接转换为 II 型电路,区别是不需要输入序列后面的 m 位零,输出结果为 $\mathbf{F}^{-m} \otimes \mathbf{INIT}$ 的逆序,故需要将输出结果逆序后左乘 $\mathbf{F}^m$,求得 **INIT**,具体电路如图5所示。

4 实例验证

以宽带码分多址/时分同步码分多址/长期演进(Wideband Code Division Multiple Access/Time Division-Synchronous Code Division Multiple Access/Long Term Evolution, WCDMA/TD-SCD-

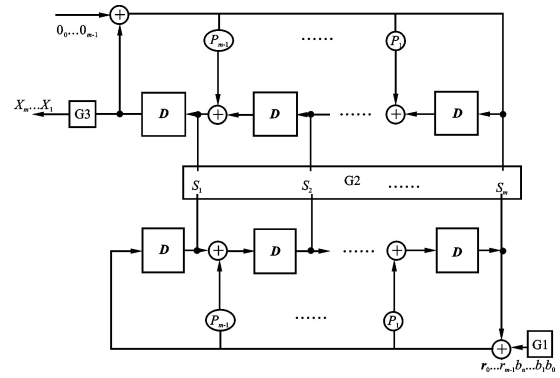


图5 II型生成电路的同构逆序校验电路

MA/LTE)中基带芯片都用到得编码长度为 $m=8$ 的 CRC 编码为例,即 CRC 编码生成多项式为 $X^8 + X^7 + X^4 + X^3 + X + 1$, 设处理序列 $(b_0 b_1 \cdots b_n) = (11001100110110)$, 生成电路寄存器初始状态为 $\{\mathbf{INIT} = (00110110)^T$ 。

如图1所示, I 型电路生成 CRC 值, 其中 $(p_{m-1} \cdots p_2, p_1, 1) = (10011011)$, 输入序列为 $(b_0 b_1 \cdots b_n 0_{m-1} \cdots 0_0) = (1100110011011000000000)$, 通过计算可得 CRC 校验值 $\mathbf{R} = (01011001)$; 如果图4所示, I 型同构电路的初始状态为全零, 输入序列为 $(r_0 \cdots r_{m-1} \ b_n \ \cdots \ b_0 0_{m-1} \ \cdots \ 0_0) = (100110100110110011001100000000)$, 其中 $(p_1, p_2 \cdots p_{m-1}, 1) = (10110011)$, 计算可得结果 (01101100) , 为 **INIT** 的逆序, 故校验正确。

如图2所示, II 型电路生成 CRC 值, 其中 $(p_{m-1} \cdots p_2, p_1, 1) = (10011011)$, 输入序列为 $(b_0 b_1 \cdots b_n) = (11001100110110)$, 通过计算可得 CRC 校验值 $\mathbf{R} = (01100011)$; 如图5所示, II 型同构电路的初始状态为全零, 输入序列为 $(r_0 \cdots r_{m-1} \ b_n \ \cdots \ b_0) = (1100011001101100110011)$, 下半部分电路计算完成后, 电路状态 $(S_m \cdots S_2 S_1) = (11000000)$, 上半部分电路输入 $m=8$ 位零, 相当于无输入条件下, 自运行 $m=8$ 次, 最终获得结果为 (00110110) , 与 **INIT** 相等, 故校验正确。

因此, I 型、II 型同构逆序校验电路均能完成校验操作。

5 结束语

本文针对任意初始状态的 CRC 生成电路及其逆序校验电路不同结构的问题, 提出 I 型、II 型两种同构逆序校验方法。最终, CRC 生成与逆序校验电路为同种结构, 对于 I 型生成电路, 同构校验电路需

(下转第 172 页)

采用 31×31 的检测效果最佳,本文中采用 31×31 的窗口,同时通过实验将 M_0 取为 5, α_0 取为 1.

5 实验结果

采用常用的 lena 和 carmer 两幅图像进行本算法和文献中算法的分析比较,对比了 canny 算法、传统小波提取算法在取不同阈值下(阈值取 0.1 和 0.2)的提取效果和本文算法的边缘提取效果.普通的 canny 算法和基本小波方法能够较好地提取图像中的主要边缘,但是随着阈值的不同,对边缘细节的提取有较为明显的变化,当阈值较小时,提取结果中会出现较多的冗余边缘信息,不能突出主要边缘信息;当阈值较大时,提取结果中对边缘细节或较为微弱的边缘信息描述不够,边缘信息描述的不够丰富.而本文提出的算法能够较好的解决这个问题.在边缘提取中,通过对阈值实现自适应设定,能够在不同的边缘信息中选择不同的阈值,对图像中的主要边缘有清晰的表示,同时对边缘中的微弱信息也有一定的反映,能够在检测到主要边缘的同时又对微弱边缘有较好区分和检测,能够较为丰富的表现图像的边缘信息.

参考文献:

- [1] 季虎,孙即祥,邵晓芳,等. 图像边缘提取方法及展望[J]. 计算机工程与应用, 2004, (14), 70-73.

(上接第 169 页)

逆序输入且末尾添 m 个零,可获得生成电路的初始状态的逆序;对于 II 型生成电路,同构校验电路需逆序输入,输出结果需要逆序后左乘 F^m (图 5 是其中一种实现方案),获得生成电路的初始状态.

参考文献:

- [1] TANENBAUM A S. Computer Networks (4th Edition) [M]. New Jersey: Prentice Hall, 2003: 192-200.
 [2] 斯廷森. 密码学原理与实践[M]. 冯登国, Douglas R Stinson, 等译. 3 版. 北京: 电子工业出版社, 2009.
 [3] STINSON D R. Cryptography theory and practice third edition [M]. London: Chapman and Hall, 2005.
 [4] Peterspm W W, B D T. Cyclic codes for error detection [J]. Proceedings of The Institute of Radio Engineers, 1961, 49(1): 228-235.
 [5] Shieh M D, Sheu M H, Chen CH H. A systematic approach for parallel CRC computations [J]. Journal of Information Science and Engineering, 2001(17): 445-461.

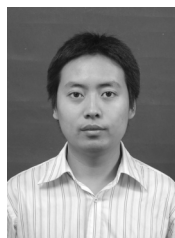
- [2] 解梅, 马争, 顾德仁. 小波变换在有噪图像边缘检测中的应用[J]. 系统工程与电子技术, 2000, 22(1): 25-27, 46.
 [3] 邹柏贤, 张然, 苗军. Prewitt 图像边缘检测方法的改进[J]. 微电子学与计算机, 2013, 30(5): 23-26.
 [4] 杜文亮, 刘晓东, 吕园园. 基于 C-Canny 算子与灰度空间的彩色图像边缘检测[J]. 微电子学与计算机, 2010, 27(4): 17-20.
 [5] 杜慧茜, 梅文博, 苏广川. 一种固定阈值的毫米波图像边缘检测方法[J]. 微电子学与计算机, 2005, 22(4): 1-3, 7.
 [6] 文武, 苗放. 基于小波的多尺度边缘检测在遥感图像处理中的应用[J]. 微电子学与计算机, 2013, 30(2): 18-20.
 [7] 郭玮玮, 黄贤武. 基于样条小波的有噪图像边缘检测方法[J]. 计算机应用, 2001, 21(10): 47-48.
 [8] 高国荣, 刘冉等. 一种改进的基于小波变换的图像边缘提取算法[J]. 武汉大学学报: 理学版, 2005, 51(5): 615-619.
 [9] 程正兴. 小波分析算法与应用[M]. 西安: 西安交通大学出版社, 1998.
 [10] 连静, 王珂. 基于 B 样条小波的自适应阈值多尺度边缘检测[J]. 吉林大学学报: 工学版, 2005, 35(5): 542-546.

作者简介:

李红女, (1976-), 讲师. 研究方向为图像处理.

- [6] 梁海华, 盘丽娜. 快速 CRC 逆序校验方法[J]. 计算机应用, 2013(7): 1833-1835.
 [7] 嘉杰克. 线性动态系统与信号[M]. 王立琦, 韩崇昭, 译. 西安: 西安交通大学出版社, 2004.
 [8] Campobello G, Patane G, Russo M. Parallel CRC realization [J]. IEEE Transactions on Computers, 2003, 52(10): 1312.

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.

李克清 男, (1966-), 博士, 教授. 研究方向为无线传感网络、网络服务质量.