文章编号：1672-2892(2010)01-0007-05

采用路径搜索的并行 RS 编码器 IP 自动生成方法

杨一波，李广军

(电子科技大学 通信与信息工程学院，四川 成都 611731)

摘 要：根据 RS 编码器的特点，提出了一种可以实现任意编码多项式、任意并行倍数的并行 RS 编码器 IP 的自动生成方法。该方法基于并行计算中数据路径的自动搜索求得编码矩阵，生成有限域运算电路，从而使得编码器所有 HDL 代码可以由软件自动生成。设计了一款 9 倍并行 RS(255,223)码编码器，综合结果表明：结合门级优化策略，所生成的并行编码器使用资源较少，且电路工作频率相对原始单倍处理电路基本保持不变。

关键词：知识产权；Reed-Solomon 码；编码器；并行计算；路径搜索

中图分类号：TN911.21 文献标识码：A

Automatic generation of parallel RS encoder IP based on datapath search method

YANG Yi-bo，LI Guang-jun

(School of Communication and Information Engineering，UESTC，Chengdu Sichuan 611731，China)

Abstract：Parallel encoders are often used in fiber communication networks. This study introduced an automatic generation method for parallel Reed-Solomon(RS) code encoder Intellectual Property(IP) based on the automatic searching for datapath in parallel computation and auto-generation of the Gaolis computation circuit. The uniform structure made its HDL codes easily generated by software. The synthesis result of the designed 9*parallel RS(255,223) encoder showed that with gate-level optimization, this automatic implementation used less resources, and maintained the same working frequency with the original circuit.

Key words：Intellectual Property；Reed-Solomon code；encoder；parallel implementation；datapath searching

RS 码是一类多进制 BCH 码，具有良好的纠错能力，特别适合于纠正连续突发错误，因此被大量用于光纤通信系统中。随着现代通信系统的不断发展，前向纠错(Forward Error Correction，FEC)电路处理带宽不断上升，在最高处理时钟受限的条件下，只有通过多路并行处理的方式，使用多倍资源以换取吞吐率的提升。

RS 编码器电路可以分为 2 种：一种为基于线性反馈移位寄存器(Linear Feedback Shift Register，LFSR)结构[1]；另一种是在第一种基础上修正的 RS 编码器电路。由于电路带有环路，流水展开等方式不能够有效提高系统吞吐率[2]，因此在 RS 编码器并行应用方向，已有的研究均是采用数学推导，在算法级实现并行编码，同时通过超前运算缩减运算强度，尽量缩短电路关键路径[3-6]。此外，并行编码电路也可应用于可动态重构处理器上[7]。但以上参考文献中介绍的电路不能同时优化电路速度与面积，且均没有考虑在 RS 编码器应用时需要的有限域运算电路，因此本文除提出并行 RS 编码器结构外，也提出一种自动化的有限域运算电路设计方法。

1 使用路径搜索算法得到并行编码矩阵

本节基于图 1 所示的 LFSR 结构编码电路，介绍了一种新的路径搜索算法，使用该算法可以生成并行编码器的编码矩阵，用来表示电路中寄存单元的更新行为。

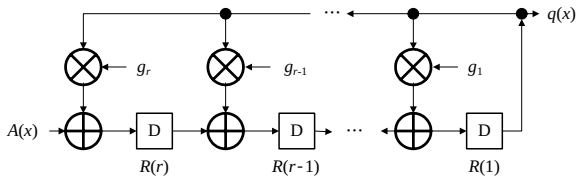

Fig.1 RS encoder of LFSR structure
图 1 LFSR 结构的 RS 编码器电路图

收稿日期：2009-07-06；修回日期：2009-08-17

设 $R_k(n)$表示从当前时刻开始 k 周期后寄存器 $R(n)$的值。则 $R_0(n)$表示当前时刻寄存器 $R(n)$的值。$g(n)$代表 LFSR 多项式除法器中 n 阶有限域乘法器系数。在 N 倍并行处理电路中，寄存单元在每一个周期的更新值可以看作是原有电路对应寄存单元于 N 周期后的更新值。将除法多项式首次项系数归一化并简单推导后得到：

$$R_{N+k}\left(n\right)=R_k\left(n+N\right)+\sum_{l=0}^{N-1}g_{n+l}R_{N+k-1-l} \tag{1}$$

从数据流的角度来看，式(1)可以表示为寄存单元值在电路中通过各自的传输路径，分别乘以各自的路径增益后传递到同一点，相加后得到特定寄存单元的更新值。数据传输路径可以分为两类：第一类是依照时钟节拍，沿移位寄存链向右移位，此种路径没有路径增益；另一类为通过反馈环路 $R(1)$的值乘以相应系数后反馈至相应输入端。由于 $R(1)$为所有反馈路径的起点，故所有节点数据如果需要通过反馈路径，就要首先通过移位路径到达 $R(1)$才能进行反馈。因此，$R_{N+k}(1)$可以表示为：

$$R_{N+k}\left(1\right)=\sum_{l=0}^{N}f\left(R_k\left(1+l\right),N-l\right) \tag{2}$$

式中 $f(x,k)$代表数据 x 从 $R(1)$开始，经过 k 周期后汇聚于 $R(1)$的值。从图 1 可以看出，$R(1)$数据通过某一反馈路径乘以系数 g_k，再经过移位路径回到 $R(1)$共耗时 k 周期。因此，所有的此类数据路径均可以表示为一个整数序列向量，序列中整数元素的和为 N，每个序列元素分别代表了某一反馈路径。由于更新值可以表示为 $R(1)$与所有反馈增益的积，因此

$$f\left(R\left(1\right),N\right)=\sum_l R\left(1\right)g_l=R\left(1\right)\sum_l g_l=R\left(1\right)g'_N \tag{3}$$

式中：g_l 为第 l 条路径的增益之积；g'_N 为 N 周期循环路径总增益，其可以通过对起点终点均为 $R(1)$的路径进行搜索后累加得到。

路径搜索算法可以建模为整数 N 的拆分及排序问题，对正整数 N 进行拆分的算法可以使用如图 2 所示的递归函数表示。搜索得到的路径再经由增益计算累加函数求得其累计增益值，增益函数算法如图 3 所示。其中向量 $\boldsymbol{p}$_number 表示对 x 的拆分序列中不同的整数元素所构成的向量，$\boldsymbol{p}$_degree 代表 $\boldsymbol{p}$_number 中各项元素在拆分序列中的出现次数。由以上算法求得的 acc_sum 即为经历 N 周期，起点终点均为 $R(1)$的所有路径的总增益 g'_N。

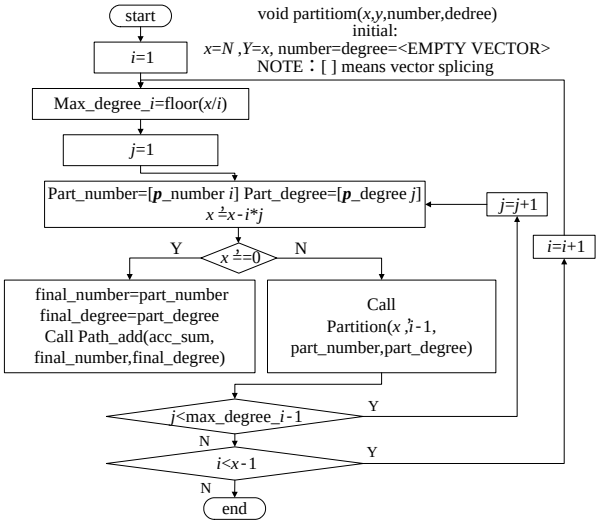

Fig.2 Automatic datapath search algorithm
图 2 路径搜索算法示意图

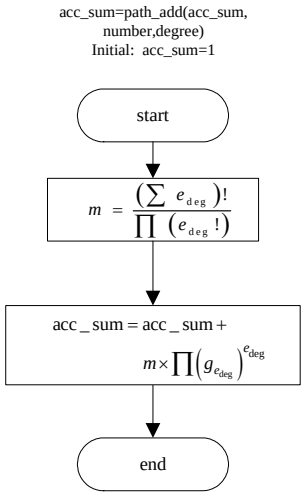

Fig.3 Gain accumulation function
图 3 增益累加函数示意图

求得路径增益后，计算并行编码矩阵。由式(2)可得：

$$\boldsymbol{R}'_{\text{return}}=\left[R_{k+N-1}\left(1\right)\quad R_{k+N-2}\left(1\right)\quad\cdots\quad R_k\left(1\right)\right]^{\mathrm{T}}=\boldsymbol{G}\bullet\boldsymbol{R} \tag{4}$$

式中：$\boldsymbol{G}=\begin{bmatrix}g'_{N-1} & g'_{N-2} & \cdots & g'_0\\ g'_{N-2} & g'_{N-3} & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ g'_0 & 0 & \cdots & 0\end{bmatrix}$；$\boldsymbol{R}=\left[R_k\left(1\right)\quad R_k\left(2\right)\quad\cdots\quad R_k\left(N\right)\right]^{\mathrm{T}}$。

将式(4)代入式(1)可得：

$$R_{N+k}\left(n\right)=R_k\left(n+N\right)+\sum_{l=0}^{N-1}g_{n+l}R_{N+k-1-l}(1)=$$
$$R_k\left(n+N\right)+\left[g_n\quad g_{n+1}\quad\cdots\quad g_{n+N-1}\right]\bullet\boldsymbol{R}'_{\text{return}}= \tag{5}$$
$$R_k\left(n+N\right)+\left[g_n\quad g_{n+1}\quad\cdots\quad g_{n+N-1}\right]\bullet\boldsymbol{G}\bullet\boldsymbol{R}=R_k\left(n+N\right)+\boldsymbol{G}'\bullet\boldsymbol{R}$$

综上所述，采用路径搜索算法得到并行编码矩阵的步骤如下：

步骤 1：采用本文提出的路径搜索及累加算法，在给定并行倍数 N 以及除法多项式系数情况下，计算相应的 0~N-1 周期循环路径总增益 g'_l，$l=0,1,\cdots,N-1$。

步骤 2：将 g'_l 代入式(4)及式(5)，计算系数矩阵 $\boldsymbol{G}'$，该矩阵即为所求的并行编码矩阵。

2　有限域运算单元的自动生成算法

由于 RS 编码器中的乘法运算均为有限域乘法，因此可以采用超前运算的方式简化乘法器结构，节约资源[1]。但在实际应用过程中，不可能对各种系数的常系数乘法器做逐一推导。本文提出一种 $GF\left(2^8\right)$ 上的常系数乘法器自动生成算法，$GF\left(2^8\right)$ 有限域上的加法为两输入多项式对应位系数做异或操作，因此 $GF\left(2^8\right)$ 有限域上的加法电路即是 8 个并行的异或门，在此不再赘述。

$GF\left(2^8\right)$ 有限域上的乘法可以表示为：

$$c\left(x\right)\equiv a\left(x\right)b\left(x\right)\quad\left(\bmod g\left(x\right)\right) \tag{6}$$

式中：$a(x)$,$b(x)$为输入的有限域元素多项式；$c(x)$为积有限域元素多项式；$g(x)$为有限域本源多项式。

根据有限域乘法规则，乘法运算分为 2 步：首先将输入多项式相乘，得到阶数不高于 14 的多项式 $d(x)=a(x)b(x)$，再将 $d(x)$对本源多项式 $g(x)$求模。对于确定有限域 $GF\left(2^8\right)$，其本源多项式 $g(x)$为定值，因此可以将求模运算简化为方程组求解，求得 $c(x)$各阶系数与 $d(x)$系数的关系。如对于本源多项式 $g(x)=x^8+x^4+x^3+x^2+1$ 生成的有限域，有：

$$\begin{cases}c[7]=d[7]+d[11]+d[12]+d[13]\\ \quad\vdots\\ c[0]=d[0]+d[8]+d[13]+d[14]+d[12]\end{cases} \tag{7}$$

多项式 $d(x)$各项系数的运算公式为：

$$d_m=\begin{cases}\sum_{i=7}^{m-7}a_ib_{m-i} & 7<m\le 14\\ \sum_{i=0}^{m}a_mb_{m-i} & 0\le m\le 7\end{cases} \tag{8}$$

根据式(7)~式(8)，可以实现并行高速 $GF\left(2^8\right)$ 有限域任意系数乘法器电路。由于常系数乘法器的乘法系数已知(假设为 b)，因此可以对式(8)做超前运算，将式(8)的乘法运算结果以如下二进制向量方式存储：

$$\boldsymbol{d}\left[i\right]=\left[d_0\left[i\right]\quad\cdots\quad d_6\left[i\right]\quad d_7\left[i\right]\right],i=0,1,2,\cdots,13 \tag{9}$$

于是

$$d_m=\sum_{i=0}^{7}\boldsymbol{d}_i\left[m\right]a_i \tag{10}$$

按照式(7)将相应 $\boldsymbol{d}[i]$向量相加，即为输出有限域符号 $c(x)$对应于 $a(x)$的向量表示方式。最后按照计算结果生成相应 HDL 文件即可。对于不同的有限域运算，只需根据所使用的本源多项式，利用软件编程重新计算求模运算公式，再按照本节介绍方式自动生成即可。

3　采用路径搜索算法的并行 RS 编码器电路

使用路径搜索算法得到并行编码矩阵并添加相应的控制电路后，可以得到如图 4 所示的并行 RS 编码器电路

(以 9 倍并行 RS(255,223)编码器为例)，其中寄存单元更新乘加电路如图 5 所示。该并行编码电路的电路时序图如图 6 所示，可见其电路结构相当工整。整个编码器电路 HDL 代码均可由软件工具自动产生。对于不同的并行倍数，只需根据编码矩阵更改乘法器输入系数，添加或删减相应有限域运算电路即可。

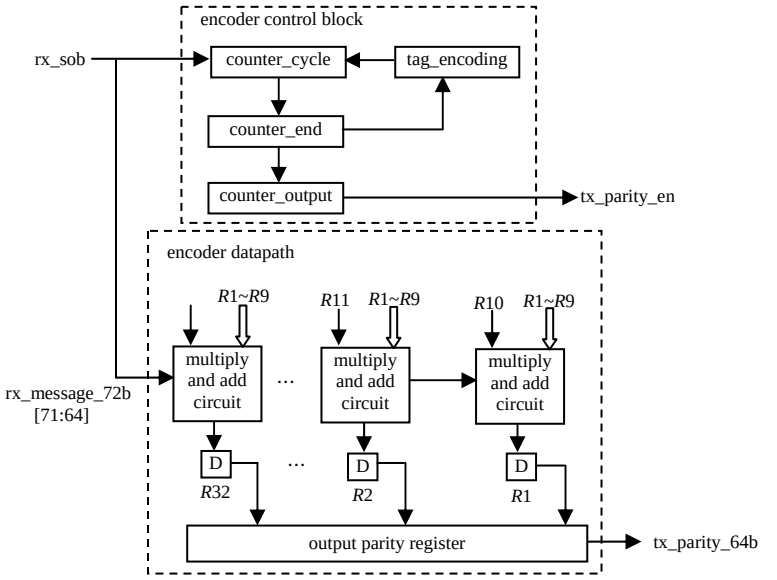

Fig.4 Structure of 9*parallel RS(255,223) encoder
图 4 9 倍并行 RS(255,223)编码器结构图

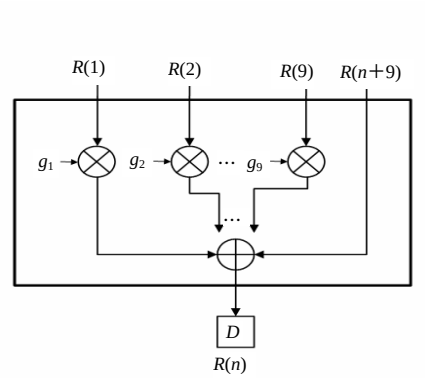

Fig.5 Register refresh mac circuit
图 5 寄存单元更新乘加电路图

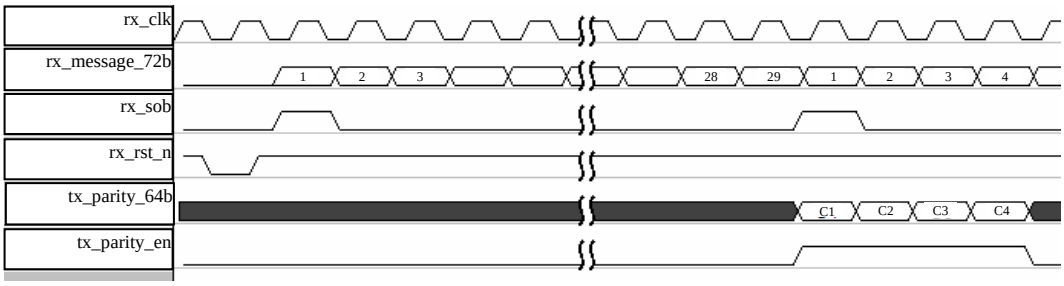

Fig.6 Timing of designed encoder
图 6 编码器编码时序图

采用本文所设计的 N 倍并行编码器，使用 $N\times r$ 个有限域乘法器，r 个 N+1 输入有限域加法器，寄存单元数目不变。由于每一个 N+1 输入加法器可以使用树形结构，因此电路资源大致为原有单倍运算电路的 N 倍。所生成电路的 MAX-FANOUT 不变，仍为 LFSR 结构电路级数 r。与文献[3-5]中所提出的并行电路不同，本算法生成的电路中具有最大 FANOUT 的节点均由寄存单元 $R(1)$驱动，因此，可以通过对寄存单元 $R(1)$至 $R(N)$做复制使用(N 为并行倍数)，进一步降低电路中的 MAX-FANOUT 值，提升系统工作频率。

本算法生成并行除法电路的关键路径为一个有限域乘法器与一个 N+1 输入加法链。由于乘法器的复杂度远高于加法器，且加法链可以采取树形结构，显著降低其延时，因此本次实现的并行电路基本上与图 1 所示的单倍编码具有相同的工作频率。使用 SYNOPSYS 公司的 Design Compiler 将本文设计电路与基于图 1 所示的单倍编码电路以及采用文献[4]中算法设计的 RS 编码器做综合对比，结果表明：结合门级优化策略，本文所设计的并行编码电路的实际资源消耗低于理论值(即原有单倍运算电路的 N 倍)，且其工作速度只比原有单倍编码电路降低 1%，在实际应用过程中可以忽略。综合结果如表 1 所示。

表 1 电路综合结果
Table1 Synthesis results

algorithm	original	this paper	reference[4]
gate/s	2 004	8 830	9 049
critical path/ns	3.08	3.11	3.29
max operation frequency/MHz	324	321	303
bandwidth/Gbps	2.59	23.1	21.8

4　结论

本文针对 RS 编码器的特点，提出了一种基于路径搜索算法的 RS 编码电路 IP 的自动生成方法，它能够实现任意编码多项式、任意并行倍数并行 RS 编码。采用本文提出算法，编码器电路结构工整，HDL 代码可以由软件工具自动生成，并以一款 9 倍并行 RS(255,223)编码器电路为例进行了实际设计，Design Compiler 综合结果表明：所生成电路相对原有并行电路实现方案使用资源数目较少，小于原型电路使用资源的 9 倍，且速度相对原型单倍编码电路速度基本保持一致。

参考文献：

[1] 王新梅,肖国镇. 纠错码—原理与方法[M]. 修订版. 西安:西安电子科技大学出版社, 2001.
[2] Parhi K K. VLSI 数字信号处理系统—设计与实现[M]. 陈弘毅,等译. 北京:机械工业出版社, 2004.
[3] Michael Sprachmann. Automatic Generation of Parallel CRC Circuits[J]. IEEE Design and Test of Computers, 2001,18(3): 108-114.
[4] 张军,王志功,胡庆生,等. 高速并行 BCH(2184,2040)编码器的 VLSI 优化设计[J]. 电路与系统学报, 2006,11(1):88-94.
[5] Parhi K K. Eliminatin the Fanout Bottleneck in Parallel Long BCH Encoders[C]// 2004 IEEE International conference on Communication. 2004,5:2611-2615.
[6] Giuseppe Campobello,Giuseppe Patane,Marco Russo. Parallel CRC Realization[J]. IEEE TRANS ON COMPUTERS, 2003, 52(10):1312-1319.
[7] Claudio Mucci,Luca Vanzolini,Hario Mirimin,et al. Implementation of Parallel LFSR-based Applications on an Adaptive DSP featuring a Pipelined Configurable Gate Array[C]// Design,test and automation. Europe 2008, 2008:1444-1449.

作者简介：

杨一波(1984-)，男，成都市人，在读硕士研究生，主要研究方向为通信专用集成电路设计. email:schollyang@uestc.edu.cn.

李广军(1950-)，男，河北省保定市人，教授，博士生导师,主要研究方向为通信系统中的信号与信息处理、通信 ASIC 及 SOC 设计、嵌入式系统设计、有线/无线通信系统、接入技术、多媒体通信系统及接口设计等.