文章编号:1674 - 2869(2009)12 - 0073 - 06

数字电视译码电路中改进型欧几里德算法

张天瑜
(无锡市广播电视大学机电工程系,江苏 无锡 214011)

摘　要:为了简化数字电视译码电路的复杂性,提出一种改进型欧几里德算法.该算法利用多项式带余除法的相关推论,通过矩阵的列变换来求解关键方程,这样可以快速地得到商式和余式,从而可以减少迭代运算的次数.与传统欧几里德算法相比,该算法在求解关键方程的过程中能够更方便地得到错误值多项式和错误位置多项式,并且能够减少硬件电路的复杂性,提高 RS 码的译码速度.

关键词:RS 码;多项式带余除法;关键方程;改进型欧几里德算法;列变换
中图分类号:TN 943　　文献标识码:A

0　引　言

1960 年由麻省理工学院林肯实验室的 Reed 和 Solomon 提出的 RS 码是非二元 BCH 码的一个重要子类,它是一类最大距离可分码.在伽罗瓦域(Galois Field, GF) $GF(2^m)$上的 $RS(n,k)$码中,输入信号码长为 n,被分成 $k\times m$ 个比特一组,每组包括 k 个信息符号,每个符号由 m 个比特组成,它具有同时纠正 $0.5(n-k)$ 个突发错误和 $0.5(n-k)$个随机错误的能力[1-2].RS 码是一种重要的分组码,目前被广泛运用于数字电视、移动电视、空间卫星通信中.由于 RS 码具有诸多优点,它在信息可靠传输中的良好应用前景已经引起世界各国学术界以及 IT 业界的高度重视.目前在纠错编码领域,RS 码已成为继 Turbo 码之后最受瞩目的又一研究热点[3-6].在 RS 译码的过程中,最重要的是关键方程的求解,通常采用的是 Berlekamp Massey 算法和传统欧几里德算法.Berlekamp-Massey 算法需要很多下标传递的操作,所以该算法的实现过程比较复杂.传统欧几里德算法是对 BCH 码提出的译码算法,但该算法没有运用到 RS 码是一种特殊的 BCH 码这一特性,它需要许多的乘法操作和控制电路[7-9].本文提出一种改进型欧几里德算法,通过矩阵的列变换来求解关键方程,可以减少迭代运算的次数,能够减少硬件电路的复杂性,提高 RS 码的译码速度.

1　RS 译码的基本流程

RS 译码的基本流程如图 1 所示.

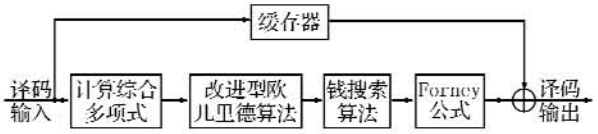

图 1　RS 译码的基本流程

Fig. 1　Basic process of RSdecoding

RS 译码过程的分析思路为:

(1)利用接收到的码元多项式 $r(x)$,计算出伴随值 $S_i(i=0,1,\cdots,2t-1)$,进而构造出综合多项式 $S(x)$.

(2)设 $\Lambda(x)$为错误位置多项式,结合关键方程 $\Omega(x)=\Lambda(x)S(x)\bmod x^{2t}$,利用改进型欧几里德算法,经过迭代求出错误位置多项式 $\Lambda(x)$和错误值多项式 $\Omega(x)$.

(3)对错误位置多项式 $\Lambda(x)$,利用钱搜索(Chien Search)算法求出其错误位置.

(4)利用 Forney 公式,求出错误值进而纠错,错误值的表达式为

$$Y_j=\frac{\Omega(X_j^{-1})}{-X_j^{-1}\Lambda'(X_j^{-1})}\quad(X_j=\alpha^j,1\leqslant j\leqslant v,\ 0\leqslant v\leqslant t) \tag{1}$$

式(1)中,t 为错误容限,即最多能纠正的错误字节的个数.

具体的译码步骤如下:

(1)伴随值的计算

求解伴随值的电路如图 2 所示.由于 RS 码的根所在的伽罗瓦域与码元取值的伽罗瓦域相同,都为 $GF(2^m)$,所以根 α^i 对应的极小多项式为一次多项式 $x-\alpha^i$.设 b_i 为 $r(x)$除以 $x-\alpha^i$ 的余式,则 $r(x)=q_i(x)(x\mid\alpha^i)\mid b_i$,所以 $S_i=r(\alpha^i)=b_i$,从

收稿日期:2009 - 09 - 25

作者简介:张天瑜(1980 -),男,江苏无锡人,讲师,硕士.研究方向:无线通信技术、通信系统仿真、信道编解码.

而得到综合多项式为

$$S(x)=S_0+S_1x+\cdots S_{2t-1}x^{2t-1} \quad (2)$$

定义错误位置多项式为

$$\Lambda(x)=(1-\alpha^{j_1}x)(1-\alpha^{j_2}x)\cdots(1-\alpha^{j_v}x)=\Lambda_0+\Lambda_1x+\cdots+\Lambda_vx^v \quad (3)$$

其中错误位置多项式的 v 个根可表示为 α^{j_1}，α^{j_2}，…，α^{j_v}，$\Lambda(x)$ 各次项的系数 Λ_0，Λ_1，…，Λ_v 与 α^{j_1}，α^{j_1}，α^{j_2}，…，α^{j_v}，$\Lambda(x)$ 都是未知的.

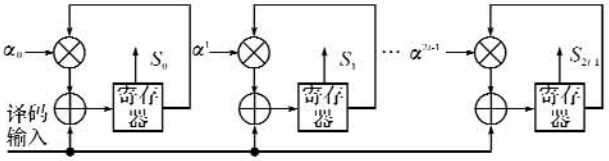

图2 求解伴随值的电路

Fig. 2 Circuit of solving syndrome values

(2)错误位置的计算

通过计算错误位置多项式的根即可确定错误位置，这通常用钱搜索算法来实现，钱搜索算法的电路图如图3所示. 钱搜索算法是把伽罗瓦域中的元素 α^0，α^1，…，α^{n-1} 逐一代入错误位置多项式中，检验是否为其根. 可以证明，要判断接收到的码元多项式 r_{n-1} 是否有错，只要检验 $\Lambda_1(\alpha^l)+\cdots+\Lambda_v(\alpha^l)^v=-1$，$(v\leqslant t)$ 是否成立即可.

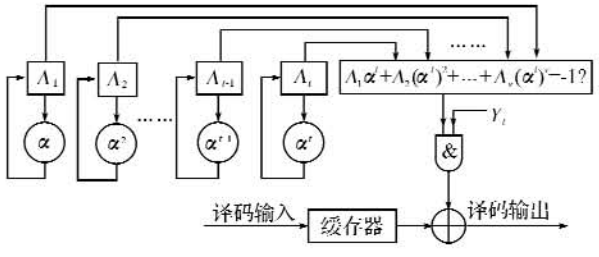

图3 钱搜索算法的电路图

Fig. 3 Circuit diagram of Chien search algorithm

(3)错误值的计算

利用 Forney 公式，错误值由式(1)确定.

2 传统欧几里德算法

传统的欧几里德算法中迭代运算的示意图如图4所示.

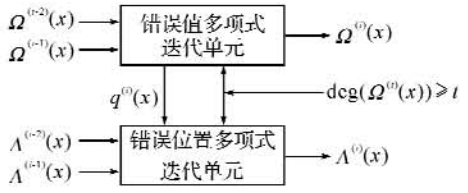

图4 传统欧几里德算法中迭代运算的示意图

Fig. 4 Iterative operation schematic diagram in traditional Euclidean algorithm

传统欧几里德算法是对关键方程 $\Omega(x)=\Lambda(x)S(x) \bmod x^{2t}$ 进行逐次迭代，直到 $\deg(\Omega^{(i)}(x))<t$ 为止，然后求解 $\Omega(x)$、$\Lambda(x)$. 由关键方程可知，存在 $\theta(x)$，使得 $\Omega(x)=x^{2t}\theta(x)+S(x)\Lambda(x)$ 成立，按下列条件进行初始化：

$$\Omega^{(-1)}(x)=x^{2t},\theta^{(-1)}(x)=1,\ \Lambda^{(-1)}(x)=0$$

$$\Omega^{(0)}(x)=S(x),\ \theta^{(0)}(x)=0,\ \Lambda^{(0)}(x)=1$$

假定 $\Omega^{(i-2)}(x)$、$\Omega^{(i-1)}$ 已知，$\Omega^{(i-2)}(x)$ 除以 $\Omega^{(i-1)}$ 的商式为 $q^{(i)}(x)$，余式为 $\Omega^{(i)}(x)$，则关键方程的迭代式可表示为

$$\Omega^{(i)}(x)=\Omega^{(i-2)}(x)+\Omega^{(i-1)}(x)q^{(i)}(x) \quad (4)$$

同时 $\Lambda^{(i)}$ 按 $\Lambda^{(i)}x=\Lambda^{(i-2)}(x)+\Lambda^{(i-1)}(x)q^{(i)}(x)$ 进行迭代，直到 $\deg(\Omega^{(i)}(x))<t$ 为止，此时求解出的 $\Omega^{(i)}(x)$、$\Lambda^{(i)}(x)$ 就是最终要求解的 $\Omega(x)$、$\Lambda(x)$.

由于传统欧几里德算法需要计算出 $\Omega^{(i-2)}$ 与 $\Omega^{(i-1)}(x)$ 的商式 $q^{(i)}(x)$，而求商式运算的电路其实现过程特别复杂. 为了减少硬件电路的复杂性，提高芯片的译码速度，需要对传统欧几里德算法进行改进.

3 改进型欧几里德算法

由多项式带余除法可知，若被除式的次数小于除式的次数时，根据商式和余式的唯一性可知，此时所得的商式为零，余式就是被除式. 所以如果被除式和除式满足上述关系时，商式和余式便可以很容易确定[10-12]. 不过在传统欧几里德算法中，需要迭代相除的多项式未必满足这一条件. 为了利用上述结论，可以将被除式减去除式，然后再与构造出的一个多项式相乘，把它们的乘积作为新的被除式，使得该被除式的次数小于除式的次数，而这里需要构造出的多项式可以根据原来被除式和除式的特征经过若干次迭代来确定. 把经过迭代之后所得到的被除式和除式相除，所得到的商式就是构造出的多项式，余式就是最后生成的被除式. 在改进型欧几里德算法中，前一过程的迭代方程称为预处理方程，后一过程的迭代方程称为更新方程.

为了明确改进型欧几里德算法中的迭代原理，首先引入多项式带余除法，即对任意两个多项式 $f(x)$、$g(x)$ 而言，存在唯一的多项式 $q(x)$、$r(x)$，使得 $f(x)=g(x)q(x)+r(x)$ 成立，其中 $\deg((r(x))<\deg(g(x))$，或者 $r(x)=0$. $q(x)$、$r(x)$ 分别称为 $f(x)$ 除以 $g(x)$ 的商式和余式. 由多项式带余除法可得出这样一个推论：对任意两个多项式 $f(x)$、$g(x)$ 而言，存在多项式 $u(x)$、$q(x)$、$r(x)$，使得 $f(x)-u(x)g(x)=g(x)q(x)+r(x)$ 成立，其中 $\deg(r(x))<\deg(g(x))$，或者 $r(x)=0$，$\deg(f(x)-u(x)g(x))<\deg(g(x))$，进而得到

$u(x)+q(x)$、$r(x)$分别就是 $f(x)$除以 $g(x)$的商式和余式.

改进型欧几里德算法的主要思路也是把迭代后错误值多项式的次数作为是否向下迭代的判据,若继续向下迭代,则把错误值多项式的商式用于错误位置多项式的迭代,否则迭代运算结束.改进型欧几里德算法的框架如图 5 所示.

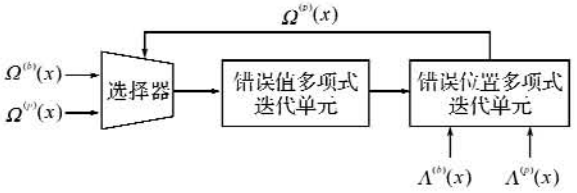

图 5　改进型欧几里德算法的框架

Fig. 5　Frame of modified Euclidean algorithm

改进型欧几里德算法中迭代运算的硬件结构如图 6 所示.在图 6 中虚线的上半部分为错误值处理单元,下半部分为错误位置处理单元.

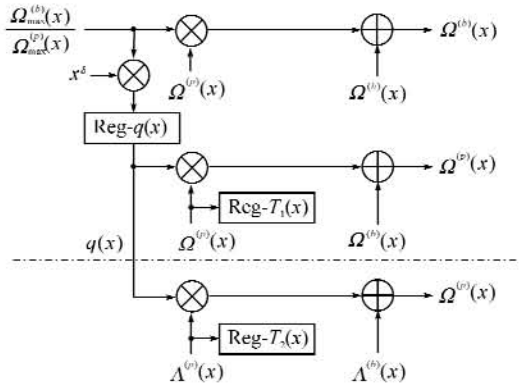

图 6　改进型欧几里德算法中迭代运算的硬件结构

Fig. 6　Hardware structure of iterative operation in modified Euclidean algorithm

从上述分析可以看出,传统欧几里德算法在求解商式的过程中需要进行多次的迭代运算,这会导致 RS 码出现较大的时间延迟,从而影响 RS 码的译码性能,因此,需要对传统欧几里德算法进行改进.为了减少迭代运算的次数,考虑在求解关键方程的过程中,如何能够较快地计算出 $\Omega^{(i-2)}(x)$与 $\Omega^{(i-1)}(x)$的商式 $q^{(i)}(x)$.为了叙述方便,将 $\Omega^{(i-2)}(x)$与 $\Omega^{(i-1)}(x)$分别用 $f(x)$与 $g(x)$代替.设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

$\boldsymbol{CF}=[a_0,a_1,\cdots,a_{n-1},a_n]^{\mathrm{T}}$ 为 $f(x)$的系数向量.

$$\boldsymbol{G}=\begin{pmatrix} b_0 & 0 & \cdots & 0 & 0 \\ \vdots & b_0 & \ddots & \vdots & \vdots \\ b_{m-1} & \vdots & \ddots & 0 & \vdots \\ b_m & b_{m-1} & \ddots & b_0 & 0 \\ 0 & b_m & \ddots & \vdots & b_0 \\ \vdots & 0 & \ddots & b_{m-1} & \vdots \\ \vdots & \vdots & \ddots & b_m & b_{m-1} \\ 0 & 0 & \cdots & 0 & b_m \end{pmatrix}$$

为 $g(x)$的系数矩阵,$\boldsymbol{CQ}$ 和 $\boldsymbol{CR}$ 分别为 $f(x)$除以 $g(x)$的商式 $q(x)$和余式 $r(x)$的系数矩阵.

由 $f(x)=g(x)q(x)+r(x)$可知,$\boldsymbol{CF}=\boldsymbol{G}(\boldsymbol{CQ})+\boldsymbol{CR}$.构造 $n-m+2$阶可逆矩阵

$$\boldsymbol{T}=\begin{pmatrix} \boldsymbol{I}_{n-m+1} & -\boldsymbol{CQ} \\ \boldsymbol{0} & 1 \end{pmatrix}$$

由此可得

$$(\boldsymbol{G}\quad \boldsymbol{CF})\boldsymbol{T}=(\boldsymbol{G}\quad \boldsymbol{CF})\begin{pmatrix} \boldsymbol{I}_{n-m+1} & -\boldsymbol{CQ} \\ \boldsymbol{0} & 1 \end{pmatrix}=(\boldsymbol{G}\quad \boldsymbol{CR}) \tag{5}$$

$$(-\boldsymbol{I}_{n-m+1}\quad 0)\boldsymbol{T}=(-\boldsymbol{I}_{n-m+1}\quad 0)\begin{pmatrix} \boldsymbol{I}_{n-m+1} & -\boldsymbol{CQ} \\ \boldsymbol{0} & 1 \end{pmatrix}=(-\boldsymbol{I}_{n-m+1}\quad \boldsymbol{CQ}) \tag{6}$$

从式(5)和式(6)中可以看出,$(\boldsymbol{G}\quad \boldsymbol{CF})$通过列变换可得$(\boldsymbol{G}\quad \boldsymbol{CR})$,同样$(-\boldsymbol{I}_{n-m+1}\quad 0)$通过列变换可得$(\boldsymbol{G}\quad \boldsymbol{CQ})$,即

$$\begin{pmatrix} \boldsymbol{G} & \boldsymbol{CF} \\ -\boldsymbol{I}_{n-m+1} & 0 \end{pmatrix}\xrightarrow{\text{列变换}}\begin{pmatrix} \boldsymbol{G} & \boldsymbol{CR} \\ -\boldsymbol{I}_{n-m+1} & \boldsymbol{CQ} \end{pmatrix} \tag{7}$$

改进型欧几里德算法与传统欧几里德算法的不同之处是,传统欧几里德算法在求解关键方程时,用到的商式是通过多项式相除得到的,而改进型欧几里德算法在求解关键方程时,用到的商式则是通过矩阵的列变换直接得到的,这样就可以减少迭代运算的次数.由于迭代运算不但会造成大的时间延迟,而且还因为里面包含大量的乘法器和除法器,从而造成硬件电路的实现非常困难.因此改进型欧几里德算法能够较少时间延迟,降低硬件电路的复杂性,提高 RS 码的译码速度.

以 RS(204,188)码为例,Berlekamp Massey 算法、传统欧几里德算法和改进型欧几里德算法所需要的硬件资源和译码速度的对比如表 1 所示.

表 1　3 种算法中硬件资源和译码速度的对比

Tab. 1　Comparison of hardware resources and decoding speed in three algorithms

算法类型	欧几里德单元的个数	乘法器总数	除法器总数	延迟周期的个数
Berlekamp-Massey 算法	0	24	4	770
传统欧几里德算法	4	16	32	420
改进型欧几里德算法	4	12	8	340

由表 1 可以看出，与 Berlekamp-Massey 算法和传统欧几里德算法相比，改进型欧几里德算法能够节省更多的乘法器和除法器，并且可以减少更多延迟周期的个数. 由于在伽罗瓦域中的乘法器电路和除法器电路非常复杂，因此改进型欧几里德算法能够降低硬件电路的复杂性，提高 RS 码的译码速度.

4 仿真实验与结果分析

基于功能强大的 MATLAB/Simulink 平台，构建一个 RS 编译码的系统仿真架构，以产生 RS 编码数据. RS(204,188)编译码的系统仿真架构如图 7 所示，其中加入误码模块和译码模块是为了验证 RS 编码的正确性. 然后把得到的编码数据加入错误用 VCS 软件来进行 FPGA 仿真实验.

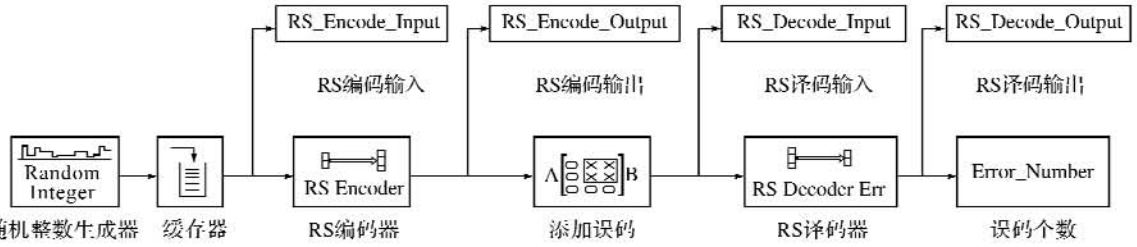

图 7 基于 MATLAB/Simulink 平台的 RS 编译码的系统仿真架构

Fig. 7 System simulation framework of RS encoding and decoding based on MATLAB/Simulink platform

在利用改进型欧几里德算法来进行译码时，由于 RS(204,188)的错误容限为 8，即一帧数据最多能纠正 8 个错误字节. 所以分以下 3 种情况来进行仿真实验.

(1)误码个数在错误容限以内

假设受到干扰的影响，原来经过编码后的 204 个字节中有 4 个错误字节，错误值依次为十六进制数 01、01、02、02，利用改进型欧几里德算法得到的仿真图如图 8 所示. 从图 8 可以看出，经过译码后能够确定错误位置和错误值. 误码经过纠错后，原来的 4 个错误字节得到了纠正，即错误字节的个数在 RS(204,188)的错误容限以内时，误码能够得到全部的纠正.

(2)误码个数达到错误容限

假设受到干扰的影响，原来经过编码后的 204 个字节中有 8 个错误字节，错误值依次为十六进制数 01、02、03、04、05、06、07、08，利用改进型欧几里德算法得到的仿真图如图 9 所示. 从图 9 可以看出，经过译码后也能够确定错误位置和错误值. 误码经过纠错后，原来的 8 个错误字节得到了纠正，即 RS(204,188)的错误容限是能够达到的.

(3)误码个数超过错误容限

假设受到干扰的影响，原来经过编码后的 204 个字节中有 9 个错误字节，错误值依次为十六进制数 01、02、03、04、05、06、07、08、09，利用改进型欧几里德算法得到的仿真图如图 10 所示. 从图 10 可以看出，经过译码后不能确定错误位置和错误值，原来的 9 个错误字节没有得到纠正，这是由于误码个数超过了 RS(204,188)的错误容限所导致的.

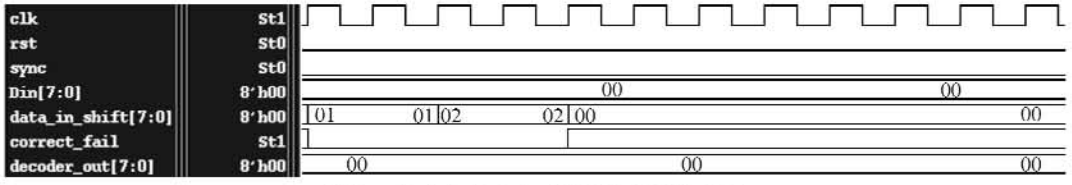

图 8 误码个数为 4 时 RS 译码的仿真图

Fig. 8 Simulation figure of RS decoding with 4 error code numbers

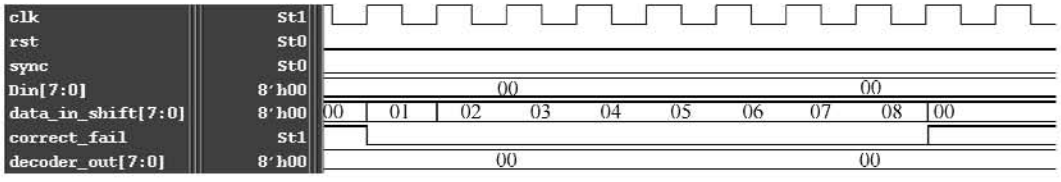

图 9 误码个数为 8 时 RS 译码的仿真图

Fig. 9 Simulation figure of RS decoding with 8 error code numbers

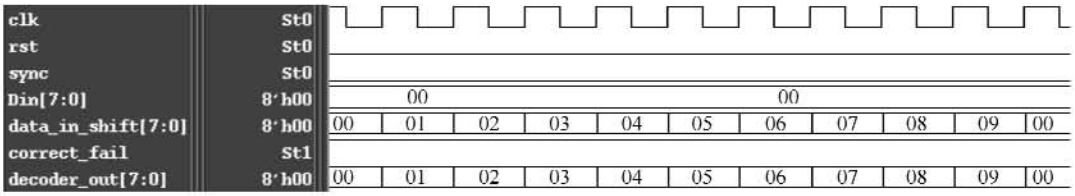

图 10　误码个数为 9 时 RS 译码的仿真图

Fig. 10　Simulation figure of RS decoding with 9 error code numbers

5　结　语

由于 Berlekamp-Massey 算法和传统欧几里德算法的硬件电路实现复杂,译码速度较慢,本文通过多项式带余除法的相关推论,提出一种改进型欧几里德算法,该算法的创新之处在于通过矩阵的列变换来求解关键方程,可以减少迭代运算的次数,能够减少硬件电路的复杂性,提高 RS 码的译码速度.这对于 RS 码在数字电视中的应用具有一定的实用价值.

参考文献:

[1] Wu Y Q. New list decoding algorithms for Reed-Solomon and BCH codes [J]. IEEE Transactions on Information Theory, 2008,54(8):3611 - 3630.

[2] Krachkovsky V Y, Ashley J J, Williamson C J, et al. Syndrome Reed-Solomon decoding using bit reliabilities [J]. IEEE Transactions on Magnetics, 2008,44(1):223 - 227.

[3] Albanese M, Spalvieri A. Two algorithms for soft-decision decoding of Reed-Solomon codes, with application to multilevel coded modulations [J]. IEEE Transactions on Communications, 2008, 56(10):1569 - 1574.

[4] Kang K. Probabilistic analysis of data interleaving for Reed-Solomon coding in BCMCS [J]. IEEE Transactions on Wireless Communications, 2008, 7(10):3878 - 3888.

[5] 刘　军,刘黎志,黄　浩. 一种无线嵌入式数字卫星接收系统的模块化设计 [J]. 武汉工程大学学报, 2008,30(4):99 - 102.

[6] 刘　书,潘成胜,张德育. Mobile Agent 在网络系统监控中数据采集的设计与应用 [J]. 武汉工程大学学报, 2009,31(3):77 - 80.

[7] Lee K, O'Sullivan M E. List decoding of Reed-Solomon codes from a Gröbner basis perspective [J]. Journal of Symbolic Computation, 2008, 43(9):645 - 658.

[8] Chang Y W, Jeng J H, Truong T K. An efficient Euclidean algorithm for Reed-Solomon code to correct both errors and erasures [C]. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, Canada, 2003: 895 - 898.

[9] Chang Y W, Truong T K., Jeng J H. VLSI architecture of modified Euclidean algorithm for Reed-Solomon Code [J]. Information Sciences, 2003,155(1-2):139 - 150.

[10] Lee S, Lee H, Shin J, et al. A high-speed pipelined degree-computationless modified Euclidean algorithm architecture for Reed-Solomon decoders [C]. IEEE International Symposium on Circuits and Systems, New Orleans, LA, 2007:901 - 904.

[11] Lee H, Azam A. Pipelined recursive modified Euclidean algorithm block for low-complexity, high-speed Reed-Solomon decoder [J]. Electronics Letters, 2003,39(19):1371 - 1372.

[12] Fournaris A P, Koufopavlou O. Applying systolic multiplication-inversion architectures based on modified extended Euclidean algorithm for GF(2^k) in elliptic curve cryptography [J]. Computers & Electrical Engineering, 2007,33(5-6):333 - 348.

Modified Euclidean algorithm in digital TV decoding circuit

ZHANG Tian-yu

(Department of Mechanical and Electrical Engineering, Wuxi Radio & Television University, Wuxi 214011, China)

Abstract: To simplify the complexity of digital TV decoding circuit, a modified Euclidean algorithm is proposed. The proposed algorithm use the related deduction of division with reminder of polynomials

and the key equation is solved by column transformation of matrix. Then the formula of quotient and reminder can be got quickly which can reduce the times of iterative operation. Compared with the traditional Euclidean algorithm, the proposed algorithm can easily get error value polynomial and error locator polynomial in the process of solving the key equation. Moreover, it can simplify the complexity of hardware circuit and improve RS decoding speed.

Key words: Reed-Solomon code; division with reminder of polynomials; key equation; modified Euclidean algorithm; column transformation

本文编辑:陈晓苹

☆

(上接第72页)

参考文献:

[1] 中国设备监理协会.设备工程监理技术与方法[M].北京:中国人事出版社,2007:169.

[2] 邵晓双,屈成忠,鞠彦忠.质量投机行为对投标的影响研究[J].武汉工程大学学报,2009,31(1):83-85.

[3] 造价工程师考试教材编审组.工程造价计价与控制[M].北京:中国计划出版社,2009:157.

[4] 陈伟亚,马玉明,袁 兵,等.化工企业循环经济模式与可持续发展战略研究[J].武汉工程大学学报,2009,31(6):36-40.

Evaluation methods of importing hardware and software devices

SHEN Wei

(School of Environmental and Civil Engineering, Wuhan institute of Technology, Wuhan 430074, China)

Abstract: Based on the investigation and research, the thesis put emphasis on the research of the pricing methods of importing hardware and software devices, to confirm the base and calculation formulas of importing devices software technology which is not definite now, and to standardize the overseas transport charges, overseas transportation insurance, tariff and some subpodinate charges. It also supplied some examples to analyze and explain, and had great significance to direct the construction budget of introducing project.

Key words: FOB price; CIF price; import equipment; incidental charges; domestic incidental expenses

本文编辑:陈晓苹