基于AVR实现RS码的时域译码及其加速算法

杨守国[1]，　张振权[2]，　徐燕红[3]

(1. 空军工程大学导弹学院，陕西三原 713800；2. 西安交通大学电子与信息工程学院，陕西西安 710049；3. 69028部队，乌鲁木齐 830002)

摘要： RS码通常的译码方法是频域译码。文中介绍和分析了基于时域的RS码译码算法和它的一种加速算法，并结合AVR单片机的高速计算性能对这两种算法进行了仿真实验，根据实验结果对两种算法的性能进行了比较，实验表明，加速算法的效率明显高于前者。

关键词： RS码；纠错码；时域译码；AVR单片机

中图分类号： TN911　　**文献标识码：** A　　**文章编号：** 1009-3516(2006)03-0069-04

RS(Reed－Solomon)[1]码是由Reed和Solomon提出的一类多进制BCH码。在卫星通信和移动通信中的应用取得了很好效果。通常的译码是基于Berlekamp Massey提出的BM频域译码算法[2]。该算法首先对所接收到的数据进行基于伽罗华域$G(2^m)$的离散傅立叶变换(DFT)，即计算错误伴随式，然后进行BM迭代，最后还要进行离散傅立叶反变换(IDFT)。虽然这种译码方法具有速度快的特点，但是它要经过傅立叶变换和钱搜索，因此对系统资源的大量占用使得其成为无线数据通信中的瓶颈。为了避免这一问题，BLAHUT最早提出了将数据从频域变换到时域进行处理的基于时域的译码算法，但其缺点就是运算时间比较长[3]。为了提高时域译码算法的速度，Yousef R. Shayan等人对其进行了优化[4]。下面就以Yousef R. Shayan等人提出的时域算法和Richard E. Blahut提出的另一种加速算法为例，利用AVR单片机对这两种时域算法进行了实验仿真并对结果进行了分析比较。

1　RS码的时域译码算法

1.1　基于时域RS译码

基于时域RS译码算法简要如图1所示。

1.2　时域译码总体算法

设r是接收到的含噪声的RS(n,k)码组，码组长度为n。纠错能力是t，相应GF(2^m)的生成元为α，其生成多项式是$g=(x)=(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{d-1})$。经过$2t$次迭代后，可以求出错误位置多项式的时域表示式(即其IDFT)$W=W(2t)$，再经过$(n-2t)$次迭代就可以得出错误码元序列$e=s^{(n)}$，最后输出正确的码组：$C=V+e$。迭代运算中需要临时用到矢量$\boldsymbol{a}$和$\boldsymbol{b}$，以及变量L，d_r，δ_r。式中各个矢量长度均为n，i为矢量中各符号的下标，$i\in[0,n-1]$；循环迭代的次数是$(n+1)$，r是迭代计数，$r\in[0,n]$。初始状态是所有的$w_i^{(0)}$和$b_i^{(0)}$都等于1，$L_0=0$。算法具体步骤如下：

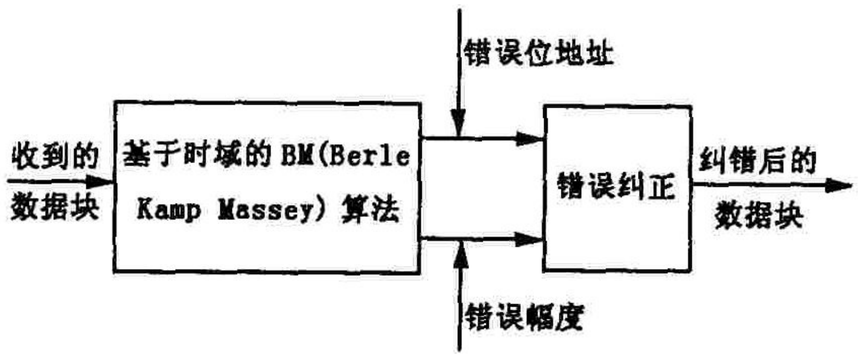

图1　时域RS译码简图

1) $r=0$时，各变量赋初值：$s^{(0)}=v_i\alpha^i$，$L=0$，$w_i=b_i=1$。

2) r取值为1至$2t$时，进行时域BM迭代运算求出w，$w_i=w_i^{(2t)}$。每步迭代运算过程如下：

收稿日期：2005－06－22
基金项目：军队科研基金资助项目
作者简介：杨守国(1971－)，男，四川广汉人，讲师，主要从事雷达及通信信号处理研究.

首先计算偏差量 d_r

$$d_r = \sum_{i=0}^{n-1} w_i^{r-1} s_i^{r-1} \tag{1}$$

当 $d_r \neq 0$ 且 $2L_{r-1} \leqslant r-1$ 时,变量 $\delta_r = 1$,否则 $\delta_r = 0$。进行以下迭代运算:

$$L_r = \delta_r(r - L_{r-1}) + (1-\delta_r)L_{r-1} \tag{2}$$

$$\begin{bmatrix} w_i^{(r)} \\ b_i^{(r)} \end{bmatrix} = \begin{bmatrix} 1 & -d_r w^{(-i)} \\ d_r^{-1}\delta_r & (1-\delta_r)w^{(-i)} \end{bmatrix} \begin{bmatrix} w_i^{(r-1)} \\ b_i^{(r-1)} \end{bmatrix} \tag{3}$$

$$s_i^{(r)} = s_i^{(r-1)} \alpha^i \tag{4}$$

3) $r = 2t+1$ 至 $n-1$ 时,每步迭代运算过程为

$$d_r = \sum_{i=0}^{n-1} w_i s_i^{(r-1)} \tag{5}$$

$$s_i^{(r)} = \alpha^i (s_i^{(r-1)} - d_i) \tag{6}$$

4) $r = n$ 时,求出错误码元序列 e

$$d_n = \sum_{i=0}^{n-1} w_i s_i^{(n-1)} \tag{7}$$

$$e_i = s_i^{(n)} = s_i^{(n-1)} - d_n \tag{8}$$

5) 当 i 取值为 0 至 $n-1$ 时,做以下操作:

$$a_i = w_i^{(n)} e_i \tag{9}$$

6) 如果执行式(9) 操作得到所有对于 i 取值为 0 至 $n-1$ 的 a_i 都为零,则

$$C = V + e \tag{10}$$

否则表示实际出错的位数大于该 RS 码的纠错能力 t,则

$$C = V \tag{11}$$

2 RS 码的时域译码算法加速改进

以上可以看出时域算法的复杂度只和码组长度 n 有关系,与纠错能力 t 没有关系。算法基本迭代次数为 n^2。它有两方面的缺点:一方面当 n 很大的时候,如 RS(255,239) 码它的基本迭代次数为 65 025 次,使得译码时间很长;二是当 n 相同但纠错能力 t 不同时所花费的时间基本是一样的,这样使得译码的效率不高。为了加速时域译码的速度,Richard E. Blahut 提出了另一种加速算法,使得算法迭代次数为 $2nt$[4]。其算法具体步骤如下:

1) $r = 0$ 时,各变量赋初值:

$$w_i^0 = \lambda_i^0 = \gamma_i^0 = 1; \xi_i^0 = \zeta_i^0 = \mu_i^0 = 0; L_0 = K_0 = 1 \tag{12}$$

2) r 取值为 1 至 $2t$ 时,同样进行迭代运算,其过程如下:

首先计算偏差量 d_r

$$d_r = \sum_{i=0}^{n-1} v_i \lambda_i^{r-1} \alpha^{ir} \tag{13}$$

当 $d \neq 0$ 且 $2L_{r-1} \leqslant r-1$ 时,变量 $\delta_r = 1$,否则 $\delta_r = 0$。进行以下迭代运算:

$$L_r = \delta_r(r - L_{r-1}) + (1-\delta_r)L_{r-1} \tag{14}$$

$$K_r = \delta_r d_r^{-1} + (1-\delta_r)K_{r-1} \tag{15}$$

$$\begin{bmatrix} \lambda_i^r \\ \gamma_i^r \\ \xi_i^r \\ \zeta_i^r \end{bmatrix} = \begin{bmatrix} 1 & -d_r K_{r-1}\omega^{-i} & 0 & 0 \\ d_r^{-1}\delta_r & (1-\delta_r)\omega^{-i} & 0 & 0 \\ 0 & -d_r & 1 & -d_r\omega^{-i} \\ 0 & (1-\delta_r) & d_r^{-1}\delta_r & (1-\delta_r)\omega^{-i} \end{bmatrix} \begin{bmatrix} \lambda_i^{r-1} \\ \gamma_i^{r-1} \\ \xi_i^{r-1} \\ \zeta_i^{r-1} \end{bmatrix} \tag{16}$$

$$\begin{bmatrix} \omega_i^{(r)} \\ \mu_i^{(r)} \end{bmatrix} = \begin{bmatrix} 1 & -d_r K^{r-1}\alpha^{-i} \\ d_r^{-1}\delta_r & (1-\delta_r)\omega^{-i} \end{bmatrix} \begin{bmatrix} \omega_i^{(r-1)} \\ \mu_i^{(r-1)} \end{bmatrix} \tag{17}$$

3) $r = 2t$ 时,求出 $\lambda_i, i \in [0, n-1]$ 的值,假如 $\lambda_i = 0$ 那么

$$C_i = V_i + \omega_i^{2t}/\zeta_i^{2t} \tag{18}$$

否则

$$C_i = V_i \tag{19}$$

3 实验仿真结果

为了验证以上两种算法的正确性和比较它们的性能,采用 Atmel 公司的 Atmega128 高速嵌入式单片机

为实验平台。AVR高速嵌入式单片机是近年来第一个发布的8位RISC MCU,执行大多数指令只需一个时钟周期,速度较快。32个通用寄存器直接与ALU相连,消除了运算瓶颈。内嵌可串行下载或自我编程的FLASH和EPROM,具有灵活的运行方式[5~7]。

实验中选择运行时钟频率为12 MHz,仿真软件环境为AVR studio4.07。采用不同码组长度 n 和不同纠错能力 t 的RS(n,k)码进行比较。实验结果如表1和表2所示。

表1　几种不同RS码译码性能比较

RS码组	RS时域译码一般算法			RS时域译码加速方法		
	CYCLE	运行时间/μs	译码效率/(bit·s^{-1})	CYCLE	运行时间/μs	译码效率/(bit·s^{-1})
RS(255,239)t=8	46 390 736	3 865 894.67	528	8 063 783	671 981.92	3 035
RS(255,247)t=4	47 692 200	3 974 350.00	513	6 359 268	529 939.00	3 849
RS(127,111)t=8	6 499 699	541 641.58	1 641	2 234 876	186 239.67	4 773
RS(127,119)t=4	6 827 759	568 979.92	1 562	1 691 811	140 984.25	6 305

表2　错误个数 t 不同时译码性能比较

	RS(127,119)时域译码一般算法			RS(127,119)时域译码加速算法		
	CYCLE	运行时间/μs	译码效率/(bit·s^{-1})	CYCLE	运行时间/μs	译码效率/(bit·s^{-1})
t=1	6 495 939	541 328.35	1 642	745 573	62 131.08	14 308
t=2	6 629 259	552 438.75	1 609	1 135,103	94 591.92	9 398
t=3	6 728 432	560 702.67	1 585	1 365,103	113 758.58	7 841
t=4	6 827 759	568 979.92	1 562	1 691,811	140 984.25	6 305

从实验结果可以得出以下结论:

1)正确性。根据实验的仿真结果进行比较,假设以上两种方法的输入数据都相同,由实验结果可以看出两种方法的输出结果是一致的。

2)效率性。根据表1和表2可以清楚地看出:第二种加速算法所消耗的时间明显比第一种算法少。第一种算法译码所需的时间主要和码长 n 的值和信息位数 k 有关系,n 和 k 越大所需要的时间越长;第二种加速算法译码所需的时间主要和码长 n 和纠错能力 t 有关系。在纠错能力一定的情况下,译码的总耗时和码长 n 有关系,n 越大则所需要的时间就越长。在同样的RS(n,k)中,译码的时间也和信息在传输中错误的个数有关系,它随着错误个数的增加而增加。第一种算法随着纠错能力 t 的增加所需要的时间在减少,而第二种算法则随着纠错能力 t 的增加所需要的时间在增大。因此当检验码在码组中占的比例较大的时候,即 $2t/n \geq 1/4$ 时第一种算法也是一种非常有效的算法。

3)应用性。以上实验数据是基于AVR单片机实现的,但是算法可以比较完整地移植到DSP等芯片中,也可以开发专门的RS译码芯片以满足用户的需要。

4　结束语

该文将基于频域的思想引入到时域中,完成了RS码的时域译码,然后在此基础上验证了一种加速算法,并对它们的性能进行了比较。在实际工程应用中,可以根据硬件的情况和实际的需求有选择地使用。

参考文献:

[1]　王新梅. 纠错码原理与方法[M]. 西安:西安电子科技大学出版社,1991.

[2]　Bernard Sklar. Digital Communications Fundamentals and Applications[M]. New Jersey:Prentice - Hall, 2001.

[3]　Blahut R E. A Universal Reed - Solomon Decoder[J]. IBM J Res Develop,1984.28(2):150 - 158.

[4]　Shayan Y R,Le - Ngoc T,Bhargava V K. A Versatile Time - domain Reed - Solomon Decoder[J]. IEEE Journal on Selected Areas in Communications,1990,8(8):1535 - 1542.

[5]　李　勋,耿德根. AVR单片机应用技术[M]. 北京:北京航空航天大学出版社,2002.

[6]　耿德根,宋建国. AVR高速嵌入式单片机原理与应用[M]. 北京:北京航空航天大学出版社,2001.

[7]　冯存前,张永顺,韩英臣. ELMS算法及其变步长算法研究[J]. 空军工程大学学报(自然科学版),2004,5(6):77 - 79.

(编辑:田新华)

The Implementation of RS Decoding Based on Time -domain and its Accelerated Algorithm in AVR

YANG Shou - guo1 , ZHANG Zhen -quan2, XU Yah - hong3

(1. The Missile Institute, Air Force Engineering University, Sanyuan, Shaanxi 713800, China; 2. School of Electronic and Information Engineering, Xi' an Jiaotong University, Xi' an, Shaanxi 710049, China; 3. PLA Unit 69028, Wulumuqi 830002, China)

Abstract:The usual decoding method of RS code is based on frequency - domain. In this paper, an algorithm based on time - domain and its accelerated algorithm for RS decoding are introduced and analyzed. At the same time, the simulation experiments are done according to the high - speed calculation performance of the AVR micro -controller. The experiment shows that the accelerated algorithm is much more efficient than the former. Finally, the performances of the two algorithms are compared based on the experimental results.

Key words: RS code; error - correcting code ; time - domain decoding; AVR micro - controller

(上接第 57 页)

[3] Parlitz U,Chua L O, Kocarev L,at el. Transmission of Digital Signals by Chaotic Synchronization[J]. Bifurcation and Chaos, 1992,2(4):973 -977.

[4] 黄 河,朱双鹤,曹国雄,等. 混顿信号发生器的实验研究[J]. 空军工程大学学报(自然科学版),2002,3(5):48 -51.

[5] Kaptaniak T, Chua L O , Zhong G Q. Experimental Synchronization of Chaos Using Continuous Control[J]. Bifurcation and Chaos,1992,4(2):483 -488.

[6] Yang T,Chua L. O. Impulsive Stabilization for Control and Synchronization of Chaotic Systems:Theroy and Application in Secure Communication[J]. IEEE Trans. on Circuit and System,1997,144(10):975 -988.

[7] 王国红,李 彦. 改进蔡氏电路的混沌同步研究[J]. 空军工程大学学报(自然科学版),2004,5(6):56 -59.

[8] 王国红,段小虎. 基于变形蔡氏电路的混顿保密通信研究[J]. 空军工程大学学报(自然科学版),2005,6(4):49 -51.

(编辑:门向生)

Study Progress of the Key Techniques in Chaotic Secure Communication

WANG Guo - hong

(The Science Institute, Air Force Engineering University, Xi'an, Shaanxi 710051, China)

Abstract: Chaotic secure communication has been a hot topic of the research in communication field recently. Chaotic synchronization is a basis of realizing chaotic communication. The effect of the parameter mismatch degree on the chaotic synchronization in the Chua's circuits is discussed in this paper. The results of this study are that the mismatch degrees of different parameters have different effects on the chaotic synchronization. This is of great use in practice, so different precision dements can be selected according to the effect of the parameter mismatch degree on the chaotic synchronization.

Key words: chaos; secure communication ; chaotic synchronization