情 報 保 護 學 會 誌
第 16 巻 第 1 號, 2006. 2

고속의 저비용 갈로이스 場원소간의 연산장치설계에 대해

심 동 욱*, 권 봉 열*, 안 형 근**

요 약

현대의 디지털통신기기나, 오디오/비데오 전자기기엔 항상 비바이나리 에러정정복부호기가 사용되는데 그중 필수적으로 사용되는 Reed Solomon 복부호화기기를 설계할 때, 갈로이스장 내의 원소간 연산이 필수적으로 사용된다. 본논문에선 이 연산장치를 쉽고 빠르게 구현할 수 있는 효율적 설계법을 제시한다. 또한각 연산기에 대해 예를 들어 설명하고 증명했다.

1. 서 론

Reed Solomon coding theory is very famous well known nonbinary error correction method for Digital Electronic Devices (Consumer and Communication products.)[5].

In 3rd author's paper, new RS(Reed Solomon) Decoder, which is correcting 2 and 3 symbol errors,and encoder design method is proposed using Normalized error position stored ROM [2]. Here New Arithmatic operation described in thgis paper can be used . On the other hand Erasure correcting decoding algorithm, which can be used for design of RS Encoder , also use this operation. The New Arithmatic operator is much simpler and faster than before, So More efficient RS CODEC SOC(System On Chip) design is Possible[3,4].

In chapter 2, we briefly described the Structure of New Galois Field Arithmatic operator . For example we describe how to Convert $GF(2^4)$ elements to $GF(2^8)$ elements . $GF(2^4)$ arithamtic operation Execution unit position in the structure and then how to go back to $GF(2^8)$ from $GF(2^4)$. In chapter 3,we apply the New algorithm to the calculation of Inversion and Multiplying which is definitely much more simpler than direct $GF(2^8)$ operation circuit. Examples are given to prove the new circuit and we find that the algorithms are workinmg well. In Chapter 4 composite Arithmatic operator design methods are given especially for A^3 circuit and A/B (Dividing)circuit. This kind of Composite Arithmatic operation circuit can be used fast and efficient Chien Searching circuit which is finding error location in Reed Solomon Codec[1,4]

In chapter 5, Conclusions are made commenting that in Composite Galois arithmetic operation contains $A^{0.5}$ and $A^{1.5}$. $A^{0.5}$ can be calculated by calculating $\alpha^{255}A$ when A's exponent is odd number and otherwise we just calculate directly $A^{0.5}$. New Chien searching machine design which can be used for 4 symbol error correcting RS decoder is really the circuit which needs the efficient arithmetic operator described in this paper [8].

* 장영실 과학고 학생(yrrangel@naver.com, eva01kby@dreamwiz.com)
** 동명정보대학교 정보통신과(hkan@tit.ac.kr)

2. New GF(28) Arithmatic Operation Calculator Structure

In this section , we describe how to simplify the Inversion circuit using Galois subfield[1]. The circuit is used for divider HW in RS Codec. Using this and multiplier described in the former Author's paper[2], Most RS Codec circuit can be simplified and faster. In Fig. 1 we draw the New Arithmatic Operation circuit block diagram [1]. Here all arithmetic operations are done in $GF(2^4)$ field so Dramatically reducing gate counts and computational speed becomes much fasrer than the case in $GF(2^8)$. Multipler design using $GF(2^4)$ Sub field is described in the Next Section [2].

$GF(2^8)$ to $GF(2^4)$ is processed as follows.

Let α^k is in $GF(2^8)$ field as (b_0, b^1, ..., b_7), it can be expressed as $\alpha^k = a + b\beta$ where a and b is in $GF(2^4)$ field and β is in $GF(2^8)$. Here a and b are (z_0, z_1, z_2, z_3) and (z_4, z_5, z_6, z_7) respectively. All b_j, z_j (j=0 to 7) are in GF(2) = (0,1) . This means $\alpha k = \Sigma_{I=0}^{3} (z_I + \beta z_{I+3})\gamma^I$, $\gamma \in GF(2^8)$ and $\gamma^4 = \gamma^3+1$ ($GF(2^4)$ Primitive Polynomial)).

Then

$$
\begin{aligned}
Z0 &= b0+b1+b5 \\
Z1 &= b1+b3+b5 \\
Z2 &= b2+b3+b6 \\
Z3 &= b1+b3+b4+b6 \\
Z4 &= b1+b2+b3+b5+b6+b7 \\
Z5 &= b2+b5+b6 \\
Z6 &= b1+b2+b3+b4+b5+b6 \\
Z7 &= b1+b3+b4+b5 \qquad (1)
\end{aligned}
$$

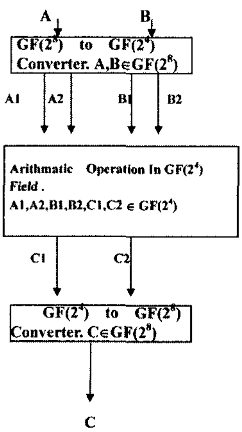


Fig1. New Galois Field Element in $GF(2^8)$ Arithmatic Caculator Structure

In the same way, From (1), we find $GF(2^4)$ to $GF(2^8)$ converter equation is , for example

$$
\begin{aligned}
B0 &= Z1 + Z0 + Z2 + Z6 + Z7 \\
B1 &= Z2 + Z1 + Z5 \\
B2 &= Z3 + Z5 + Z7 \\
B3 &= Z1 + Z6 + Z7 \\
B4 &= Z1 + Z7 \\
B5 &= Z5 + Z6 + Z7 \\
B6 &= Z3 + Z6 + Z5 \\
B7 &= Z1 + Z6 + Z4 + Z7 \qquad (2)
\end{aligned}
$$

now If we want calculate $C=A \cdot B$ ($A, B, C, \beta, \gamma \in GF(2^8)$), $A=A1+\beta A2$ and $B=B1+\beta B2$, $C=C1+\beta C2$ ($A1, A2, B1, B2, C1, C2 \in GF(2^4)$), then.

$$
\begin{aligned}
C &= (A1+\beta A2)(B1+\beta B2) \\
&= A1B1+A1B2+\gamma A2B2+\beta (A2B2+A1B2)
\end{aligned}
$$

$$
\begin{aligned}
\text{So } C1 &= A1B1+A1B2+\gamma A2B2 \\
C2 &= A2B2+A1B2 \qquad (3)
\end{aligned}
$$

This is the Arithmatic operator in $GF(2^4)$ for $GF(2^8)$ Multiplier [1].

Example 1

Using equation (1) ,If $A=\alpha^5$, Find A1 and A2.

Sol : A1=(Z_0, Z_1, Z_2, Z_3), A2=(Z_4, Z_5, Z_6, Z_7) so from equation (1), $A1= \alpha^{12}$, $A2= \alpha^6 \in GF(2^4)$.

Example 2

If $A1= \alpha^{12}$, $A2= \alpha^6$ using equation (2) Find A.

Sol : From Equation (2)

B0 = Z1 + Z0 + Z2 + Z6 +Z7=0
B1 = Z2 + Z1 +Z5 =0
B2 = Z3 + Z5 +Z7=0
B3= Z1 + Z6 +Z7=0
B4 = Z1 + Z7=0
B5 = Z5 + Z6 +Z7=1
B6 = Z3 + Z6 +Z5=0
B7 = Z1 + Z6 +Z4 +Z7=0

So A= α^5 This is correct.

3. Multiplying and Inverse Operation Calculator Design using New Algorithm

〈Inverse Calculator Design〉

Now A, A^{-1} in $GF(2^8)$ can be expressed as follows.

$A = X_0+X_1\beta$

$A^{-1} = Y_0+Y_1\beta$ (3)

So From A $A^{-1}=1$

$X_0Y_0+ \gamma X_1Y_1 =1$

$X_1 Y_0+(X_0 +X_1) Y_1 = 0$ (4)

Here X_0, X_1, Y_0, Y_1 $\in GF(2^4)$, $\beta$and $\gamma\in GF(2^8)$ also $\beta^2=\beta+\gamma$, then Y_0, Y_1 are represented as in (5)[1]:

$Y_0=(X_0+X_1)/\delta$

$Y_1=X_1/ \delta$

$\delta =X_0(X_0+X_1)+\gamma(X_1^2)$ (5)

Also if $X=(x_0, x_1, x_2, x_3)$, $\gamma X^2=(x_2+x_3, x_0+x_2 +x_3, X_3, x_1+x_2)$. So equation (5) is Desired Arithmatic Operation In $GF(2^4)$ in Fig.1. Here $C=AA^{-1} =C1+\beta C2=1$.

Example1

Let's Find Inverse of α^5, α^{-5} $\in GF(2^8)$ using Subfield GF(24) Arithmatic operation.

〈Solution〉

$A=\alpha^5 \in GF(2^8) = X_0 +X_1 \beta$.

From Eq. $X0 = \alpha^{12}$, $X_1 = \alpha^6 \in GF(2^4)$.

From Eq. $Y0= \alpha^{14}/ (\alpha^{13} + \alpha^{12} \alpha^{14}) =\alpha^9$.

Here $\gamma X_1^2 = \alpha^{13}$.

Also $Y1=1/ (\alpha5+\alpha7) = \alpha^{-14}=\alpha$.

Now Convert these to element in $GF(2^8)$.

Then b0=b1=b4=b7=0 and b2=b3=b5=b6 =0.

Hence this bi (i=0 to 7) represents $\alpha^{250} =\alpha^{-5}$ so Correct.

〈Multiplier Design〉

Now $A=A1+\beta A2$,$B=B1+\beta B2$ and $C=C1+\beta C2=AB$

So

$C1=A1B1+\gamma A2B2$ and

$C2=A2B2+B1A2+A1B2$ (6)

Equation (6) is the desired Desired Arithmatic Operation In $GF(2^4)$ in Fig.1[3,4].

Example2

If $A=\alpha^2$ and $B=\alpha^3 \in GF(2^8)$ Find C=AB

Sol : $A= A1+\beta A2$

$B=B1+\beta B2$,here from (1) $A1=\alpha^2$, $A2=\alpha^7$, $B1=\alpha^8$,

$B2=\alpha^2 \in GF(2^4)$.

Hence from (6)

$C1=\alpha^{12}$, $C2=\alpha^6$ $\in GF(2^4)$, and from (2) $C=\alpha^5 \in GF(2^8)$ and This is Correct.

Example3

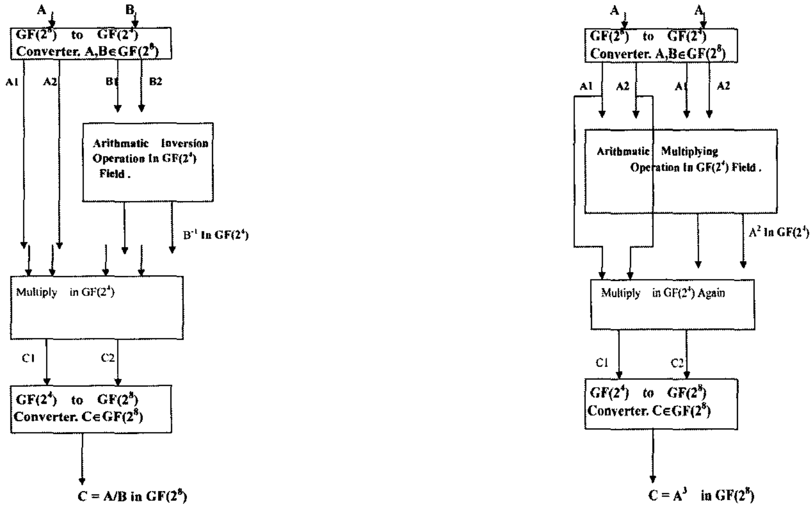
Show that if $A=(a0,a1,a2,a3) \in GF(2^4)$ then $\gamma A =(a3,a0,a1,a2+a3) \in GF(2^4)$

Proof : $A=a0+\gamma a1+\gamma^2a2+\gamma^3a3$ so $\gamma A=(a0+\gamma a1+\gamma^2a2+\gamma^3a3)$ $\gamma=(a3,a0,a1,a2+a3)$ because $\gamma^4=\gamma^3+1$[5,6,7].

4. Composite Arithmatic Operation Calculator Design

Divider and A3 calculation can be decomposed into 2 or more parts.. For example A/B is composed of A multiply by B 1 and A3 is A Multiply by A and then we multiply A again to A2 result. In this case Dividing and A3 calculation can be done as in the circuit in Fig 2 (a) and Fig2(b).

Example is as below [8].



(a) (b)

Fig 2 (a). Composite Arithmatic Operator Divider In GF(2^8) (b). Composite Arithmatic Operator A3 In GF(2^8)

<u>Example</u>

Let's Find A/B , when $A=\alpha^2$, $B=\alpha^5 \in$ GF(2^8) using Subfield GF(2^4) Arithmatic Composite operation.

〈Solution〉

From example1 of previous section,

$\alpha^5=\alpha^9+\beta\alpha$ and from example2 of previous section $\alpha^2=\alpha^2 + \alpha^7\beta$ so as in Fig2(a) and using equation (6), we find $C=C1+\beta C2 =\alpha^{11}+\gamma\alpha^8+(\alpha^{16} +\alpha^8 +\alpha^3)\beta$.

Now we find (Zi ,i=0~3 : 0001) and (Zi ,i=4~7 : 0010) . So from equation (2), we find $C=A/B \in GF(2^8)$ = (10110101) = $\alpha^{252} =\alpha^{-3}$ and This really Correct

5. Coclusion

In this paper various Arithmatic operation calculator design methods are proposed and gave examples to show working well. The methods are very fast and cost effective because GF(2^4) arithmetic operations are much more simpler and faster than that those in GF(2^8). We can also calculate root ($A^{0.5}$) and Plus (+) or Minus(-) operation but it is as EXOR operation. So All the Arithmatic oiperations in Galois Field are suggested here and proved.

References

[1] US patent number 5227992, " Operational Method and Apparatus over GF(2^m) using a Subfield GF(2m/2)", Man young Lee, Hyeong Keon An et al., 1993 Jul. 13

[2] Hyeong Keon An, "2 Error Correcting RS Decoder design", IDEC Conference Paper, 2004

[3] Hyeong Keon An, TS Joo et al, " The New RS Ecc Codec For Digital Audio and Video", IEEE CES Conference paper , PP112 115, 1992

[4] Lee Man Young, " BCH coding and Reed Solomon Coding theory," 1990, Minumsa(Daewoo Academic Press).

[5] Sunghoon Kwon and Hyunchul Shin, " Anarea efficient VLSI architecture of Reed Solomon decoder/encoder for digital VCRs, " IEEE Transactions on Consumer Electronics, Vol. 43, No.4, Nov. 1997

[6] Kwang Y.Liu, " Architecture for VLSI

design of Reed Solomon Decoders, "IEEE Transactions on Computers. Vol.33, No.2, Feb. 1984

[7] Hsu, I.K. , I.S.Reed, "The VLSI Implementation of a Reed Solomon Encoder Using Berlekamp's Bit Serial Multiplier Algorithm", IEEE Trans. On Computer, Vol.C 33, No.10, pp.906 911(1984).

[8] 안 형근 ," 디지털 오디오/비디오, 통신용 전자기기를 위한 Reed Solomon 복부호기 설계에 대해", 대한전자공학회지, TC 42, pp 13-18, 11월 2005년

〈著 者 紹 介〉

안 형 근 (Hyeong-Keon An)

He received B.Engineering Degree in electrical engineering from Seoul National University, Seoul , KOREA , in 1979 and M.S degree in electrical science from Korea Advanced Institute of Science and Technology , Seoul ,Korea in 1981, and the Ph.D. degree in electrical engineering from State University of New York at Stony Brook , NY, USA., in 1988. In 1988, he joined Samsung Electronics Co. Ltd as a Senior Researcher working for designing System LSI for 10 years. From 1998 to 1999 , He worked for Telson Electronics Corp. working for CDMA handphone design. In 2000, he joined Tong Myoung University in Busan as a Professor in Dept. Of Information and Telecommunication engineering . He has interests in designing CDMA and GSM hand phone and also in System LSI (Non Memory) design. He also operates Venture Comapany for Producing various Mobile phones and GPS/MP3 Engines.