doi:10.16055/j.issn.1672-058X.2015.0008.004

最优正规基下并行乘法器的设计*

苏丹丹[1], 付　萍[2]
(1.罗定职业技术学院,广东 罗定 527200;2.北京昌平区回龙观中学,北京 102200)

摘　要:利用简单的组合逻辑电路分别在Ⅰ型和Ⅱ型最优正规基上设计出了新的并行乘法器,其中Ⅰ型最优正规基并行乘法器所需异或门数为 $3n-4$,与门数为 n,Ⅱ型最优正规基并行乘法器所需异或门数为 $2n-2$,与门数为 n;与 Sunar 和 Koc 于 2001 年在Ⅱ型最优正规基上提出的并行正规基乘法器对照,此乘法器大大减少了所需要的门数,从而有效地降低了硬件消耗的资源.

关键词:有限域;最优正规基;乘法器;门数
中图分类号:O154.2　　**文献标识码**:A　　**文章编号**:1672-058X(2015)08-0014-05

有限域计算(即加法,减法,乘法和求逆等)被广泛用于编码理论,计算机代数学和密码学[1,2].有限域计算尤其乘法计算极大地影响着各种密码算法的加/解密速度,因此,设计性能优越的乘法器显得尤其重要.各种乘法器的算法极大地依赖于有限域基的选择.有限域有多种基,如多项式基、正规基等.在这些基中,使用正规基对算术操作的硬件执行是非常有效的.1986 年,Omura 和 Massey 首次在文献[3]中提出正规基乘法器.

根据 Menezes 在文献[1]中所列举的数据,在 $n\in[2,2\ 001]$ 范围内属于Ⅰ型最优正规基的 m 有 117 个,属于Ⅱ型最优正规基的 m 有 319 个.因此,研究最优正规基是非常有意义的.尽管 Massey-Omura 正规基乘法器对Ⅰ型和Ⅱ型最优正规基都有效,但所需异或门数为 $2n(n-1)$.基于 Massey-Omura 乘法器,2001 年,Sunar 和 Koc 在文献[4]中在Ⅱ型最优正规基上提出了一种并行正规基乘法器,其所需异或门数为 $1.5n(n-1)$,与门数为 n^2.文中利用简单的组合逻辑电路分别在Ⅰ型和Ⅱ型最优正规基上设计出新的并行乘法器,其中Ⅰ型最优正规基并行乘法器所需异或门数为 $3n-4$,与门数为 n,Ⅱ型最优正规基并行乘法器所需异或门数为 $2n-2$,与门数为 n.与 Sunar-Koc 正规基乘法器对照,此乘法器大大减少了所需要的门数,从而有效地降低了硬件消耗的资源.

1　相关引理和定理

引理 1[5]　设 $N=\{\alpha_i\mid i=0,1,\cdots,n-1\}$ 和 $B=\{\beta_i\mid i=0,1,\cdots,n-1\}$ 为 E 在 F 上互为对偶的两组基,则对任意 $u\in E$,有

$$u=\sum_{i=0}^{n-1}Tr(\beta_i u)\,\alpha_i=\sum_{j=0}^{n-1}Tr(\alpha_j u)\,\beta_j$$

引理 2[6]　设 $N=\{\alpha^{q^i}\mid i=0,1,\cdots,n-1\}$ 为 E 在 F 上的一组Ⅰ型最优正规基,$T=(t_{i,j})$ 为其乘法表。则当 $j=0,1,\cdots,n-1$ 时,有

$$t_{\frac{n}{2},j}=-1$$

收稿日期:2015-05-08;**修回日期**:2015-06-20.
* **基金项目**:国家自然科学基金资助项目(10990011).
作者简介:苏丹丹(1980-),女,湖北随州人,讲师,硕士研究生,从事应用数论研究.

当 $i=0,1,\cdots,n-1$,且 $i\neq\frac{n}{2}$时,

$$t_{i,j}=\begin{cases}1,若\ q^j\equiv q^i+1(\bmod\ n+1)\\0,其\quad 他\end{cases}$$

引理 3[7]　设 $N=\{\alpha^{q^i}\mid i=0,1,\cdots,n-1\}$ 为 E 在 F 上的一组Ⅰ型最优正规基,则 N 的对偶基为

$$B=\{\beta_i=-(n+1)^{-1}+(n+1)^{-1}\alpha_{\frac{n}{2}+i}\mid i=0,1,\cdots,n-1\}$$

定理 1[8]　设 $n+1$ 是素数,q 是模 $n+1$ 的一个原根,则 F 上 n 个非单位元的 $n+1$ 次单位根是线性无关的,且组成 E 在 F 上一组最优正规基,记为 $N=\{\alpha^{q^i}\mid i=0,1,\cdots,n-1\}=\{\alpha^j\mid j=1,2,\cdots,n\}$,这里 α 是一个 $n+1$ 次本原单位根,称 N 为 E 在 F 上的一组Ⅰ型最优正规基。

引理 4[6]　设 $N=\{\alpha^{2^i}\mid i=0,1,\cdots,n-1\}$ 为 F_{2^n}在 F_2 上的一组Ⅱ型最优正规基,$T=(t_{i,j})$ 为其乘法表,则

$$t_{0,j}=\begin{cases}1,若\ j=1\\0,其\quad 他\end{cases}$$

$$t_{n-1,j}=\begin{cases}1,若\ j=n-1\ 或\ 2^{j+1}\equiv\pm 3(\bmod 2n+1)\\0,其\quad 他\end{cases}$$

而当 $i=1,2,\cdots,n-2$ 时,有

$$t_{i,j}=\begin{cases}1,若\ 2^j\equiv\pm(2^i\pm 1)(\bmod 2n+1)\\0,其\quad 他\end{cases}$$

引理 5[9]　设 $N=\{\alpha^{2^i}\mid i=0,1,\cdots,n-1\}$ 为 F_{2^n}在 F_2 上的一组Ⅱ型最优正规基,则 N 是自对偶正规基。

2　算法设计

设 $X,Y\in F_{2^n}$,元素 X 和 Y 分别用最优正规基 N 及其对偶基 B 表示为

$$X=x_0\alpha_0+x_1\alpha_1+\cdots+x_{n-1}\alpha_{n-1}$$

$$Y=y_0\beta_0+y_1\beta_1+\cdots+y_{n-1}\beta_{n-1}$$

设二者的乘积用对偶基表示为

$$XY=(xy)_0\beta_0+(xy)_1\beta_1+\cdots+(xy)_{n-1}\beta_{n-1}$$

则由引理 1 知 $\forall i=0,1,\cdots,n-1$,

$$\begin{aligned}(xy)_i&=Tr(XY\alpha_i)=Tr(Y(x_0\alpha_0+x_1\alpha_1+\cdots+x_{n-1}\alpha_{n-1})\alpha_i)=\\&x_0Tr(Y\alpha_0\alpha_i)+x_1Tr(Y\alpha_1\alpha_i)+\cdots+x_{n-1}Tr(Y\alpha_{n-1}\alpha_i)=\\&x_0Tr(Y(\alpha_0\alpha_{-i})^{2^i})+x_1Tr(Y(\alpha_0\alpha_{1-i})^{2^i})+\cdots+\\&x_{n-1}Tr(Y(\alpha_0\alpha_{n-1-i})^{2^i})\end{aligned}$$

(其中足标均取模 n 的最小非负剩余).

情形 1:若 N 为Ⅰ型最优正规基,则由引理 2 得 $\forall i=0,1,\cdots,n-1$ 且 $i\neq\frac{n}{2}$,有 $\alpha_0\alpha_i=\alpha_j$,其中 $j=0,1,\cdots,n-1$且 $2^j\equiv 2^i+1(\bmod n+1)$.以及 $\alpha_0\alpha_{\frac{n}{2}}=\sum_{s=0}^{n-1}\alpha_s$,故

$$\begin{aligned}(xy)_0&=x_0Tr(Y\alpha_{j_0})+\cdots+x_{\frac{n}{2}-1}Tr(Y\alpha_{j_{\frac{n}{2}-1}})+x_{\frac{n}{2}}Tr\Big(Y\sum_{s=0}^{n-1}\alpha_s\Big)+\\&x_{\frac{n}{2}+1}Tr(Y\alpha_{j_{\frac{n}{2}+1}})+\cdots+x_{n-1}Tr(Y\alpha_{j_{n-1}})\end{aligned}$$

又由引理 1 知:

$$\begin{aligned}(xy)_0&=x_0y_{j_0}+\cdots+x_{\frac{n}{2}-1}y_{j_{\frac{n}{2}-1}}+x_{\frac{n}{2}}(y_0+y_1+\cdots+y_{n-1})+\\&x_{\frac{n}{2}+1}y_{j_{\frac{n}{2}+1}}+\cdots+x_{n-1}y_{j_{n-1}}\end{aligned}\qquad(1)$$

同理有:

$$\begin{aligned}
(xy)_1 &= x_0y_{j_{n-1}+1} + \cdots + x_{\frac{n}{2}}y_{j_{\frac{n}{2}-1}+1} + x_{\frac{n}{2}+1}(y_1 + y_2 + \cdots + y_{n-1} + y_0) + \\
&\quad x_{\frac{n}{2}+2}y_{j_{\frac{n}{2}+1}+1} + \cdots + x_{n-1}y_{j_{n-2}+1} \\
(xy)_2 &= x_0y_{j_{n-2}+2} + \cdots + x_{\frac{n}{2}+1}y_{j_{\frac{n}{2}-1}+2} + x_{\frac{n}{2}+2}(y_2 + \cdots + y_{n-1} + y_0 + y_1) + \\
&\quad x_{\frac{n}{2}+3}y_{j_{\frac{n}{2}+1}+2} + \cdots + x_{n-1}y_{j_{n-3}+2} \\
&\quad \vdots \qquad\qquad \vdots \\
(xy)_{n-1} &= x_0y_{j_1+n-1} + \cdots + x_{\frac{n}{2}-2}y_{j_{\frac{n}{2}-1}+n-1} + x_{\frac{n}{2}-1}(y_{n-1} + y_0 + \cdots + y_{n-2}) + \\
&\quad x_{\frac{n}{2}}y_{j_{\frac{n}{2}+1}+n-1} + \cdots + x_{n-1}y_{j_0+n-1}
\end{aligned} \tag{2}$$

其中足标均取模 n 的最小非负剩余.

进而,由引理3可知 $\forall i=0,1,\cdots,n-1,\beta_i=1+\alpha_{\frac{n}{2}+i}$.又由定理1的证明可知 $\sum_{s=0}^{n-1}\alpha_s = \alpha + \alpha^2 + \cdots + \alpha^n = 1$,故

$$\begin{aligned}
XY &= (xy)_0\beta_0 + (xy)_1\beta_1 + \cdots + (xy)_{n-1}\beta_{n-1} = \\
&\quad (xy)_0(1+\alpha_{\frac{n}{2}}) + (xy)_1(1+\alpha_{\frac{n}{2}+1}) + \cdots (xy)_{n-1}(1+\alpha_{\frac{n}{2}-1}) = \\
&\quad (xy)_0(1+\alpha_{\frac{n}{2}}) + \cdots + (xy)_{\frac{n}{2}-1}(1+\alpha_{n-1}) + \\
&\quad (xy)_{\frac{n}{2}}(1+\alpha_0) + \cdots + (xy)_{n-1}(1+\alpha_{\frac{n}{2}-1}) = \\
&\quad ((xy)_{\frac{n}{2}+1} + \cdots + (xy)_{n-1} + (xy)_0 + \cdots + (xy)_{\frac{n}{2}-1})\alpha_0 + \\
&\quad ((xy)_{\frac{n}{2}+2} + \cdots + (xy)_{n-1} + (xy)_0 + \cdots + (xy)_{\frac{n}{2}})\alpha_1 + \\
&\quad \vdots \qquad\qquad \vdots \qquad + \\
&\quad ((xy)_{\frac{n}{2}} + \cdots + (xy)_{n-1} + (xy)_0 + \cdots + (xy)_{\frac{n}{2}-2})\alpha_{n-1} = \\
&\quad (xy)'_0\alpha_0 + (xy)'_1\alpha_1 + \cdots + (xy)'_{n-1}\alpha_{n-1}
\end{aligned} \tag{3}$$

其中足标均取模 n 的最小非负剩余.

情形2:若 N 为Ⅱ型最优正规基,则由引理4知 $\alpha\alpha_0=\alpha_1,\alpha\alpha_{n-1}=\alpha_{n-1}+\alpha_t$,其中 $t=0,1,\cdots,n-1$ 且 $2^{t+1}\equiv\pm3 \pmod{2n+1}$.以及 $\forall i=1,2,\cdots,n-2$,有 $\alpha\alpha_i=\alpha_m+\alpha_k$,其中 $m,k=0,1,\cdots,n-1,2^m\equiv2^i+1 \pmod{2n+1},2^k\equiv-(2^i+1) \pmod{2n+1}$,故

$$\begin{aligned}
(xy)_0 &= x_0Tr(Y\alpha_1) + x_1Tr(Y(\alpha_{m_0}+\alpha_{k_0})) + \cdots + x_{n-2}Tr(Y(\alpha_{m_{n-3}}+\alpha_{k_{n-3}})) + \\
&\quad x_{n-1}Tr(Y(\alpha_{n-1}+\alpha_t))
\end{aligned}$$

又由引理1知:

$$(xy)_0 = x_0y_1 + x_1(y_{m_0}+y_{k_0}) + \cdots + x_{n-2}(y_{m_{n-3}}+y_{k_{n-3}}) + x_{n-1}(y_{n-1}+y_t) \tag{4}$$

类似地可得:

$$\begin{aligned}
(xy)_1 &= x_0(y_0 + y_{t+1}) + x_1y_2 + x_2(y_{m_0+1} + y_{k_0+1}) + \\
&\quad x_3(y_{m_1+1} + y_{k_1+1}) + \cdots + x_{n-1}(y_{m_{n-3}+1} + y_{k_{n-3}+1}), \\
(xy)_2 &= x_0(y_{m_{n-3}+2} + y_{k_{n-3}+2}) + x_1(y_1 + y_{t+2}) + x_2y_3 + \\
&\quad x_3(y_{m_0+2} + y_{k_0+2}) + \cdots + x_{n-1}(y_{m_{n-4}+2} + y_{k_{n-4}+2}) \\
&\quad \vdots \qquad\qquad \vdots \\
(xy)_{n-1} &= x_0(y_{m_0+n-1} + y_{k_0+n-1}) + \cdots + x_{n-3}(y_{m_{n-3}+n-1} + y_{k_{n-3}+n-1}) + \\
&\quad x_{n-2}(y_{n-2} + y_{t+n-1}) + \cdots + x_{n-1}y_0
\end{aligned} \tag{5}$$

其中足标均取模 n 的最小非负剩余.

进而由引理5可知 N 是自对偶的,故

$$\begin{aligned}
XY &= (xy)_0\beta_0 + (xy)_1\beta_1 + \cdots + (xy)_{n-1}\beta_{n-1} = \\
&\quad (xy)'_0\alpha_0 + (xy)'_1\alpha_1 + \cdots + (xy)'_{n-1}\alpha_{n-1}
\end{aligned}$$

综上所述,完成一次乘法计算需要3步:

(Ⅰ) 确定 $y_{j_0},y_{j_1},\cdots,y_{j_{\frac{n}{2}-1}},y_{j_{\frac{n}{2}+1}},\cdots,y_{j_{n-1}}$及 $y_t,y_{m_0},y_{m_1},\cdots,y_{m_{n-3}},y_{k_0}$,从而获得所需的 $y_i,i=0,1,\cdots,n-1$.

(Ⅱ) 利用(1),(2),(3),(4)式计算$(xy)_0,(xy)_1,\cdots,(xy)_{n-1}$.

(Ⅲ) 若 N 为Ⅰ型最优正规基,利用(3)式把 XY 在对偶基 B 上转换到最优正规基 N 上表示.

第一步可借助计算机工具(使用 C/C++/Matlab 程序)确定,第二、三步由简单的组合逻辑电路实现.第一步简单的 Matlab 程序如下:

```
a=[];
    b=[y_1,y_2,...,y_{n-1},y_0];
    c=[];
    for  i=0:n/2-1
        for  j=0:n-1
                d=2^i+1
                if  mod(2^j,n+1)==mod(d,n+1)
                    a=[a,j];
                end
        end
    end
    for  i=0:n/2+1
        for  j=0:n-1
                d=2^i+1
                if  mod(2^j,n+1)==mod(d,n+1)
                    a=[a,j];
                end
        end
    end
    for  e=0:n-1
        for  f=1:n-1
            g=a(f);
                if  g+e>n
                    h=g+e-n;
                    c=[c,b(h)];
                else if  g+e==0
                        c=[c,b(n)];
                else
                c=[c,b(g+e)];
        end
        end
    end
```

输出结果为

$$
\begin{aligned}
c=[\,& y_{j_0}y_{j_1}\cdots y_{j_{\frac{n}{2}-1}}y_{j_{\frac{n}{2}+1}}\cdots y_{j_{n-1}}\\
& y_{j_0+1}y_{j_1+1}\cdots y_{j_{\frac{n}{2}-1}+1}y_{j_{\frac{n}{2}+1}+1}\cdots y_{j_{n-1}+1}\\
& y_{j_0+2}y_{j_1+2}\cdots y_{j_{\frac{n}{2}-1}+2}y_{j_{\frac{n}{2}+1}+2}\cdots y_{j_{n-1}+2}\\
& \qquad\vdots\qquad\qquad\qquad\vdots\\
& y_{j_0+n-1}y_{j_1+n-1}\cdots y_{j_{\frac{n}{2}-1}+n-1}y_{j_{\frac{n}{2}+1}+n-1}\cdots y_{j_{n-1}+n-1}\,]
\end{aligned}
$$

确定 $y_t,y_{m_0},y_{m_1},\cdots,y_{m_{n-3}},y_{k_0},y_{k_1},\cdots,y_{k_{n-3}}$程序类似.

3　算法复杂度的简单分析

若 N 为Ⅰ型最优正规基,在计算$(xy)_i,i=0,1,\cdots,n-1$ 时,所需的异或门数为 $2n-2$,与门数为 n;在计算$(xy)'_i,i=0,1,\cdots,n-1$ 时,所需的异或门数为 $n-2$.综合所需的异或门数为 $3n-4$,与门数为 n.若 N 为Ⅱ型最优正规基,在计算$(xy)_i=(xy)'_i,i=0,1,\cdots,n-1$ 时,所需的异或门数为 $2n-2$,与门数为 n.

设计将复杂和消耗资源的工作由计算机工具处理(使用 C/C++/Matlab 程序),而实际设计的硬件电路最后形式是简单的组合逻辑电路,且该最优正规基下的并行乘法器,Ⅰ型最优正规基并行乘法器所需异或门数为 $3n-4$,与门数为 n,Ⅱ型最优正规基并行乘法器所需异或门数为 $2n-2$,与门数为 n.

参考文献:

[1] MENEZES A J.Applications of Finite Fields[M].Boston:Kluwer Academic,1993

[2] LIDL R,NIEDERREITER H.Introduction to Finite Fields and Their Applications[M].New York:Cambridge University Press,1994

[3] OMURA J,MASSEY J.Computational Method and Apparatus for Finite Field Arithmetic.US Patent Number 4587627[P].1986

[4] SUNAR B,KOC C K.An Efficient Optimal Normal Basis Type Ⅱ multiplier[J].IEEE Trans on Computer,2001,50(5):83-87

[5] GEISELLMANN W,GOLLMANN D.Duality and Normal Basis Multiplication[J].Cryptography and Coding Ⅲ,1991(187):195

[6] 廖群英,孙琦.有限域上最优正规基的乘法表[J].数学学报,2005,48(5):947-954

[7] WAN Z X, ZHOU K. On the Complexity of the Dual Basis of a Type Ⅰ Optimal Normal Basis[J]. Finite Fields and Their Applications, 2007, 13: 411-417
[8] MULLIN R, ONYSZCHUK I, VANSTONE S, et al. Optimal Normal Bases in $GF(p^n)$[J]. Discrete Applied Math, 1988-1989, 22: 149-161
[9] LIAO Q Y, SUN Q. Normal Bases and Their Dual-bases Over Finite Fields[J]. Acta Mathematica Sinica, English Series, 2006, 22(3): 845-848

Parallel Multiplier Design based on optimal Normal Basis

SU Dan-dan[1], FU Ping[2]

(1. Luoding Polytechnic, Luoding 527200, China; 2. Beijing Changping Huilongguan School, Beijing 102200, China)

Abstract: A new parallel multiplier is designed by simple combinational logic circuits based on type I optimal normal basis and type Ⅱ optimal normal basis respectively. For the type I optimal normal basis, the parallel multiplier needs 3n-4 XOR gates and n AND gates, for the type Ⅱ optimal normal basis, the parallel multiplier needs 2n-2 XOR gates and n AND gates. Compared with the normal basis parallel multiplier based on type Ⅱ optimal normal basis proposed by Sunar and Koc in 2001, this multiplier greatly reduces required gates so as to effectively decrease the resources of consumption.

Key words: finite fields; optimal normal basis; multipliers; gates

(上接第8页)

参考文献:

[1] DAI Y H, LIAO L Z. New Conjugacy Conditions and Related Nonlinear Conjugate Gradient Methods[J]. Appl Math Optim, 2001, 43(1): 87-101
[2] SAMAN B K, REZA G. The Dai-Liao Nonlinear Conjugate Gradient Method with Optimal Parameter Choices[J]. European Journal of Operational Research, 2014, 234(3): 625-630
[3] ZHOU W J, ZHANG L. A Nonlinear Conjugate Gradient Method Based on the MBFGS Secant Condition [J]. Optimization Methods and Soft-ware, 2006, 21(5): 707-714
[4] DAI Y H. Convergence Properties of Nonlinear Conjugate Gradient Methods[J]. SIAM J Optim, 2000, 10(2): 345-358
[5] MOREE J J, GARBOW B S, HILLSTROM K E. Testing Unconstrained Optimization Software [J]. ACM Trans Math Software, 1981, 7(1): 136-140

The Modified DL Conjugate Gradient Method with Optimal Parameter Choices

WU Shuang-jiang

(School of Mathematics and Science, Chongqing Normal University, Chongqing 401331, China

Abstract: Making use of the solution of matrix condition number, based on the MBFGS secant condition, the parameter t of modified DL conjugate gradient method is for solution and modified DL conjugate gradient method with optimal parameter choices is presented. If line search direction satisfies descent condition and step size is obtained by strong Wolfe line search, globally convergence for general functions is proved. Finally, the value effectiveness of the new conjugate gradient method is compared.

Key words: conjugate gradient method; strong Wolfe line search; condition number; global convergence