Discrete Applied Mathematics 28 (1990) 309–312
North-Holland

COMMUNICATION

LOW COMPLEXITY NORMAL BASES FOR $F_{2^{mn}}$

Gérald E. SÉGUIN*

Department of Electrical and Computer Engineering, Royal Military College, Kingston, Ont., Canada K7K 5L0

Received 13 February 1990
Communicated by R.C. Read

If $C(r)$ denotes the minimum complexity of a normal basis for F_{2^r}, we show that if $m>1$, $n>1$ are two relatively prime integers, then $F_{2^{mn}}$ has a normal basis of complexity $C(m)C(n)$. Such a normal basis leads to a Massey–Omura multiplier for $F_{2^{mn}}$ which uses $C(m)C(n)$ *XOR* gates and $C(m)C(n)+1$ *AND* gates per dimension.

1. Introduction

In recent years there has been an interest in developing algorithms for multiplying in finite fields whose structure is amenable to VLSI implementation. Typically, such an algorithm is given the multiplicands as r-tuple and must produce the r-tuple which represents their product. The first successful algorithm is that due to Massey and Omura [3, 6] in which the basic idea is to represent the field elements with respect to a normal basis. However, the complexity of the Massey–Omura algorithm depends on which normal basis is used. The problem of finding normal bases of minimal complexity was studied by Mullin, Onyszchuk, Vanstone and Wilson [4]. In particular, they showed that the minimal complexity (the complexity of a normal basis corresponds to the number of *XOR* gates per dimension that a Massey–Omura multiplier requires) of a normal basis for F_{p^r} is at least $2r-1$ and they gave sufficient (and apparently necessary) conditions for the existence of a normal basis of complexity $2r-1$. This problem was further studied by Ash, Blake and Vanstone [1] who gave specific constructions of low complexity normal bases.

In this paper, we study multiplication in fields of the form $F_{2^{mn}}$, $m>1$, $n>1$ and where $\gcd(m,n)=1$. These fields are, at the moment, of no great interest in cryptography because of the result of Pohlig and Hellman [5]. Nevertheless, they may certainly be of interest in coding theory and perhaps, in future cryptographic schemes which do not rely on exponentiation. Specifically, we show that normal

* This work was supported in part by grant 0GP306288 from the Natural Sciences and Engineering Research Council of Canada held by the author at the École Polytechnique de Montréal.

bases of F_{2^m} and F_{2^n} of respective complexities C and C' can be combined to give a normal basis for $F_{2^{mn}}$ of complexity CC'.

2. Massey-Omura multipier for $F_{2^{mn}}$

In this section, we show how to obtain a Massey-Omura multiplier for the field $F_{2^{mn}}$, $m>1$, $n>1$ and $\gcd(m,n)=1$. The key to this result is the following simple lemma:

Lemma 1. *Let $m>1$, $n>1$ be two relatively prime integers. Let $B_1=\{\alpha_i \mid 0\le i\le m-1\}$ and $B_2=\{\beta_j \mid 0\le j\le n-1\}$ be bases, respectively, for F_{2^m} and F_{2^n} over F_2. Then $B=\{\alpha_i\beta_j \mid 0\le i\le m-1,\ 0\le j\le n-1\}$ is a basis for $F_{2^{mn}}$ over F_2. Moreover, if B_1 and B_2 are normal bases, then so is B.*

Proof. Let $A=\{\sum_i \sum_j a_{ij}\alpha_i\beta_j \mid a_{ij}\in F_2\}$, then A is a subring of $F_{2^{mn}}$, hence automatically a subfield, say F_{2^k}. Since $F_{2^m}\subset F_{2^k}$ and $F_{2^n}\subset F_{2^k}$, it follows that $m \mid k$ and $n \mid k$, hence $mn \mid k$ and so $k=mn$. Since the dimension of $F_{2^{mn}}$ over F_2 is mn, the result follows. Next suppose $\alpha_i=\alpha^{2^i}$, $0\le i\le m-1$ and $\beta_j=\beta^{2^j}$, $0\le j\le n-1$, then $(\alpha\beta)^{2^k}=\alpha^{2^k}\beta^{2^k}$ where k in α^{2^k} may be reduced modulo m and k in β^{2^k} may be reduced modulo n. Hence, $(\alpha\beta)^{2^k}$ is of the form $\alpha^{2^i}\beta^{2^j}$, $0\le i\le m-1$, $0\le j\le n-1$. To complete the proof, we need only show that the smallest positive integer k for which $(\alpha\beta)^{2^k}=\alpha\beta$ is mn. If $(\alpha\beta)^{2^k}=\alpha\beta$, then $\alpha^{2^k-1}=(\beta^{-1})^{2^k-1}\in F_2$ since $F_{2^m}\cap F_{2^n}=F_2$. Hence $\alpha^{2^k-1}=\beta^{2^k-1}$, $((\beta^{-1})^{2^k-1}=1$ implies that $\beta^{2^k-1}=1)$, and so if M is the order of α, then $M \mid 2^k-1$. But the smallest positive integer l such that $M \mid 2^l-1$ is m and so $m \mid k$. Similarly, we conclude that $n \mid k$ and so $mn \mid k$ and we are done. □

Suppose γ^{2^j}, $0\le j\le r-1$ is a normal basis for F_{2^r} and that

$$\gamma^{2^i}\gamma^{2^j}=\sum_l \lambda_{i,j}^{(l)}\gamma^{2^l},\quad \lambda_{i,j}^{(l)}\in F_2,$$

then the Hamming weight of the $r\times r$ matrix

$$\Lambda_l=(\lambda_{i,j}^{(l)})$$

is independent of l (see Mullin et al. [4]) and is called the complexity of the normal basis generated by γ and denoted $C_r(\gamma)$. We shall call the minimum of the $C_r(\gamma)$ computed over all normal bases for F_{2^r}, the complexity of F_{2^r} and denote it $C(r)$. It is known [4] that $C(r)\ge 2r-1$ and if $C(r)=2r-1$, then F_{2^r} has an *optimal normal basis*.

If we represent the elements of F_{2^r} in the normal basis α^{2^j}, $0\le j\le r-1$, then the Massey-Omura multiplier uses $C_r(\alpha)$ *XOR* gates and $C_r(\alpha)+1$ *AND* gates [3, 6]. The following corollary to Lemma 1 shows that $C(mn)\le C(m)C(n)$ if $mn>1$ and $\gcd(m,n)=1$ (we set $C(1)=1$).

Corollary. *Let $mn>1$, $\gcd(m,n)=1$, $\{\alpha^{2^i} \mid 0\le i\le m-1\}$, $\{\beta^{2^j} \mid 0\le j\le n-1\}$ normal bases, respectively, for F_{2^m} and F_{2^n}. Then $\alpha\beta$ generates a normal basis for $F_{2^{mn}}$ with complexity $C_{mn}(\alpha\beta)=C_m(\alpha)C_n(\beta)$. In particular, $C(mn)\le C(m)C(n)$.*

Proof. The only thing to prove is that $C_{mn}(\alpha\beta)=C_m(\alpha)C_n(\beta)$. To this end, let

$$\alpha^{2^i}\alpha^{2^j}=\sum_k \lambda_{i,j}^{(k)}\alpha^{2^k}, \quad \lambda_{i,j}^{(k)}\in F_2, \tag{1}$$

$$\beta^{2^r}\beta^{2^s}=\sum_l \gamma_{r,s}^{(l)}\beta^{2^l}, \quad \gamma_{r,s}^{(l)}\in F_2, \tag{2}$$

and let $\Lambda_k=(\lambda_{i,j}^{(k)})$, $\Gamma_l=(\gamma_{r,s}^{(l)})$. Multiplying the left-hand sides of (1) and (2) and equating it to the product of the right-hand sides, we get

$$\begin{aligned}(\alpha\beta)^{2^{u(i,r)}}(\alpha\beta)^{2^{v(j,s)}}=\alpha^{2^i}\beta^{2^r}\alpha^{2^j}\beta^{2^s}&=\sum_k\sum_l \lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}\alpha^{2^k}\beta^{2^l}\\&=\sum_k\sum_l \lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}(\alpha\beta)^{2^{c(k,l)}}\end{aligned} \tag{3}$$

where in (3) $(\alpha\beta)^{2^{u(i,r)}}=\alpha^{2^i}\beta^{2^r}$ etc. Actually, we can give an explicit expression for $u(i,r)$, $v(j,s)$ etc. by invoking the chinese remainder theorem; but such explicit knowledge is not required for our purposes. Looking at (3) it becomes apparent that $C_{mn}(\alpha\beta)$ is the number of 1's that occur in $\lambda_{i,j}^{(k)}\gamma_{r,j}^{(l)}$ as i, r run over $0,1,\dots,m-1$ and j, s run over $0,1,\dots,n-1$. But this is clearly the product of the weights of the matrices Λ_k and Γ_l, hence $C_{mn}(\alpha\beta)=C_m(\alpha)C_n(\beta)$. In fact, the elements $\lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}$ define an $mn\times mn$ matrix, which if properly organized, is the usual tensor product of Λ_k and Γ_l. □

We remark that sometimes $C(mn)=C(m)C(n)$. Consulting the table of $C(r)$ given in Mullin et al. [4], we find, for example, that $C(15)=C(3)C(5)$, $C(20)=C(4)C(5)$, $C(21)=C(3)C(7)$, $C(22)=C(2)C(11)$ and $C(24)=C(3)C(8)$. A slight extension of the above arguments shows that if $n=n_1n_2\cdots n_s$, $\gcd(n_i,n_j)=1$ for every i and j, if $i\ne j$, then

$$C(n)\le\prod_1^s C(n_i).$$

When using $\alpha\beta$ to generate a normal basis for $F_{2^{mn}}$ as described above, we may represent the elements of $F_{2^{mn}}$ either as

$$\sum_{i=0}^{mn-1} a_i(\alpha\beta)^{2^i} \quad \text{or} \quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{i,j}\alpha^{2^i}\beta^{2^j}.$$

This will not affect the complexity of the Massey–Omura multiplier; but cyclic shifting in the second of these representations takes the following form:

$$\left(\sum_i\sum_j a_{i,j}\alpha^{2^i}\beta^{2^j}\right)^2=\sum_i\sum_j a_{i,j}\alpha^{2^{i+1}}\beta^{2^{j+1}}=\sum_i\sum_j a_{i-1,j-1}\alpha^{2^i}\beta^{2^j},$$

i.e.,

$$(a_{i,j}) \to (a_{i-1,j-1})$$

instead of

$$(a_i) \to (a_{i-1}).$$

We have therefore shown that we can construct a Massey-Omura multiplier for $F_{2^{mn}}$ which uses $C(m)C(n)$ *XOR* gates per dimension and $C(m)C(n)+1$ *AND* gates per dimension. If F_{2^m} and F_{2^n} have optimal normal bases, then these numbers become:

$$4mn-2(m+n)+1 \quad \textit{XOR} \text{ gates per dimension}$$

and

$$4mn-2(m+n)+2 \quad \textit{AND} \text{ gates per dimension.}$$

3. Conclusions

In this paper we have shown that if $m>1$, $n>1$ are relatively prime, then $F_{2^{mn}}$ has a normal basis of complexity $C(m)C(n)$ where $C(r)$ is the complexity of F_{2^r}. In particular, $C(mn) \leq C(m)C(n)$. This poses the interesting problem of determining the integers n for which $C(n) = \prod_{i=1}^{k} C(n_i)$ for some factorization $n = n_1 n_2 \cdots n_k$ of n with $\gcd(n_i, n_j) = 1$ for every i, j, $i \neq j$.

References

[1] D.W. Ash, I.F. Blake and S.A. Vanstone, Low complexity normal bases, Discrete Appl. Math. 25 (1989) 191–210.

[2] T. Itoh and S. Tsujii, Structure of parallel multipliers for a class of fields GF(2^m), Inform. and Comput. 83 (1989) 21–40.

[3] J.L. Massey and J.K. Omura, Computational method and apparatus for finite field arithmetic, U.S. Patent Application, Submitted.

[4] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, Optimal normal bases in GF(p^n), Discrete Appl. Math. 22 (1989) 149–161.

[5] S.C. Pohlig and M.E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Trans. Inform. Theory 24 (1) (1978) 106–110.

[6] C.C. Wang, T.K. Truong, H.M. Shao, L.J. Deutsch, J.K. Omura and I.S. Reed, VLSI architectures for computing multiplications and inverses in GF(2^m), IEEE Trans. Comput. 34 (1985) 709–717.