Some Remarks on Efficient Inversion in Finite Fields

Christof Paar *

presented at: 1995 IEEE International Symposium on Information Theory, Whistler, B.C., Canada, p. 58, Sept. 17-22, 1995

Abstract

This contribution is concerned with bit parallel inverters over finite fields. Two alternative approaches for inversion with low complexity which were proposed in the late nineteen eighties will be reviewed. Previously they seem to have received relatively little attention in the scientific community. Both methods are based on multiple field extension of $GF(2)$. We will try to restate the two algorithms in a clear fashion. It will be shown that one architecture is a generalization of the other's architecture core algorithm. As an impressive example of the advantage of inverters operating over extension fields, the optimized complexity of a bit parallel inverter in the important field $GF(2^8)$ will be computed, resulting in a surprisingly low gate count.

1 Introduction

Galois field arithmetic has wide spread applications in contemporary communication systems, in particular in cryptography and in channel coding. Modern applications in many cases call for VLSI implementations of the arithmetic modules in order to satisfy the high speed requirements. Assuming a standard, dual or normal base representation of the field elements, addition is a relatively inexpensive operation, whereas multiplication and division/inversion are costly in terms of gate count and delay. Most references which deal with inverters propose bit serial architectures. The major argument for applying bit serial architectures rather than bit parallel ones is that the gate consumption of the latter is too high. However, since there is a space-time trade-off, bit parallel architectures tend to be faster which makes them attractive for many applications. The best traditional approach based on Fermat's Theorem requires $\lfloor \log_2(k-1) \rfloor + H_w(k-1) - 1$ multiplications and $k-1$ squarrings in $GF(2^k)$ [1, Theorem 2], where $H_w(\cdot)$ denotes the Hamming weight of the operand's binary representation. We claim that by applying the alternative approaches developed hereafter, bit parallel inversion is possible with a moderate gate count.

*The research was done while the author was with the Institute for Experimental Mathematics, University of Essen, Germany; he is now with Worcester Polytechnic Institute.

2 Two Architectures over Multiple Extension Fields

This section restates two previously suggested architectures.

Inversion in Extension Fields of Degree Two

The first architecture was proposed by Morii-Kasahara [2] in 1989 and reintroduced in 1991 in [3]. The architecture is based on an algorithm which makes use of a field extension of degree two.

The core part of the architecture is the following. Let us consider an element A from $GF((2^{k/2})^2)$ in a canonical representation: $A(x) = a_0 + a_1 x$, where $a_0, a_1 \in GF(2^{k/2})$. There exists always an irreducible field polynomial of the form $P(x) = x^2 + x + p_0$, where $p_0 \in GF(2^{k/2})$ [4]. If the inverse of A is denoted as $B = A^{-1} = b_0 + b_1 x$, the equation

$$\begin{aligned} A \cdot B &= (a_0 + a_1 x)(b_0 + b_1 x) \bmod P(x) \\ &= [a_0 b_0 + p_0 a_1 b_1] + [a_0 b_1 + a_1 b_0 + a_1 b_1] x = 1 \end{aligned}$$

must be satisfied, which is equivalent to a set of two linear equations in b_0, b_1 over $GF(2^{k/2})$ whose solution is:

$$\left.\begin{aligned} b_0 &= \tfrac{a_0 + a_1}{\Delta} \\ b_1 &= \tfrac{a_1}{\Delta} \end{aligned}\right\}, \tag{1}$$

where $\Delta = a_0(a_0 + a_1) + p_0 a_1^2$.

The computation of the two Equations (1) requires 1 inversion, 3 general multiplications, 2 additions, 1 constant multiplication with p_0 and 1 squaring. All these operations are performed in $GF(2^{k/2})$. The algorithm can be applied recursively leading to so-called tower fields. The main advantage of this algorithm is that the inversion is now performed in the subfield which is supposed to be considerably easier than in the field $GF(2^k)$. The algorithm from above can be applied recursively, leading to so-called tower fields of the form $GF((\cdots((q^2)^2)\cdots)^2)$.

Inversion in Composite Fields

The second architecture was proposed in the last section of Itoh-Tsujii's paper from 1988 [1, Section 6]. It is based on so-called composite fields which are finite fields with two extensions. The composite fields considered here are of the form $GF((2^n)^m)$. The basic property of the underlying algorithm is that inversion in $GF((2^n)^m)$ is reduced to inversion in the subfield $GF(2^n)$.

We start with the trivial notation $A^{-1} = (A^r)^{-1} A^{r-1}$. If the auxiliary parameter[1] r is defined as

$$r := \frac{2^{nm} - 1}{2^n - 1} = 1 + 2^n + 2^{2n} + 2^{3n} + \cdots + 2^{(m-1)n},$$

[1] r corresponds to the parameter a in the original paper.

we obtain the important property [4]:

$$A^r \in GF(2^n), \quad \forall A \in GF((2^n)^m). \tag{2}$$

We are now able to state a four step algorithm for computing the inverse of A:

Step 1 Compute A^{r-1} (Exponentiation in $GF((2^n)^m)$.)

Step 2 Compute $A^{r-1}A = A^r$ (Multiplication in $GF((2^n)^m)$, where the product is an element of $GF(2^n)$.)

Step 3 Compute $(A^r)^{-1} = A^{-r}$ (Inversion in $GF(2^n)$.)

Step 4 Compute $A^{-r}A^{r-1} = A^{-1}$ (Multiplication of an element from $GF(2^n)$ with an element from $GF((2^n)^m)$.)

3 A Relation Between the Two Architectures

Itoh and Tsujii's architecture is based on composite fields $GF((2^n)^m)$. It can be shown that Morii and Kasahara's core algorithm is a special case of this architecture.

In order to establish the relation, the composite fields considered are $GF((2^n)^2)$. The field polynomial is $P(x) = x^2+x+p_0$. An arbitrary field element is represented by $A(x) = a_1x+a_0$, its inverse by $B := A^{-1} = b_1x + b_0$. The parameter r is now $r = (2^{2n}-1)/(2^n-1) = 2^n+1$. By denoting $x^{r-1} = s_1x + s_0$, Step 1 of the algorithm is:

$$A^{r-1} = (a_1x + a_0)^{r-1} = a_1x^{r-1} + a_0 = [a_1s_1]x + [a_1s_0 + a_0]. \tag{3}$$

The computation in Step 2 is:

$$A^r = A^{r-1}A = [a_0a_1s_1 + a_1^2s_0 + a_0a_1 + a_1^2s_1]x + [a_0a_1s_0 + a_0^2 + a_1^2s_1p_0]. \tag{4}$$

However, A^r is an element of the subfield and therefore its coefficient at x is zero. Using this, a relation between the coefficients can be established: $a_1s_0+a_0 = (a_0+a_1)s_1$. Inserting this auxiliary relation into the Equations (3) and (4) results in new expressions for Step 1 and Step 2, respectively

$$\begin{aligned} A^{r-1} &= s_1(a_1x + [a_1 + a_0]), \\ &\text{and} \\ A^r &= s_1[a_0(a_1 + a_0) + a_1^2p_0]. \end{aligned} \tag{5}$$

Step 3 is the inversion of A^r:

$$(A^r)^{-1} = s_1^{-1}\,[a_0(a_1 + a_0) + a_1^2p_0]^{-1}.$$

The result in Step 4 is computed as $B = A^{r-1}(A^r)^{-1}$:

$$\begin{aligned} B(x) &= b_1 x + b_0 \\ &= A^{r-1}(A^r)^{-1} = \frac{a_1 x + (a_1 + a_0)}{a_0(a_1 + a_0) + a_1^2 p_0}. \end{aligned} \tag{6}$$

Equation (6) is exactly the same as the resulting Equations (1) of the core algorithm of Morii and Kasahara. If only one field extension is used for the tower inverter, its architecture is the same as the architecture of Itoh and Tsujii's inverter in standard base in the field $GF((2^n)^2)$. Moreover, Itoh and Tsujii's architecture can be viewed as a generalization of Morii and Kasahara's core algorithm. However, it is not true that it is a generalization of Morii and Kasahara's *architecture*, since this is based on tower fields, i.e. multiple field extensions of degree two.

4 An Inverter over $GF(2^8)$

The Galois field $GF(2^8)$ is of great technical importance since it was standardized for use in error correction schemes for space communication [5] and on compact disks.

For the application of Morii-Kasahara's architecture the decomposition of $GF(2^8)$ into $GF((2^4)^2)$ is considered. Let $Q(y) = y^4 + y + 1$ be the primitive polynomial generating $GF(2^4)$ with $Q(\omega) = 0$ and $P(x) = x^2 + x + \omega^{14}$ the primitive polynomial generating the composite field. $P(x)$ is the best possible irreducible polynomial since multiplication with ω^{14} requires only 1 XOR gate. It was determined through an exhaustive search. For computing the inverse of an element according to Equations (1) in hardware, the following modules, providing arithmetic in $GF(2^4)$, must be realized:

- For parallel inversion in the subfield a direct approach is the most efficient one. In [6, Appendix A] closed formulas are provided which allow inversion with not more than 15 XOR/10 AND gates.
- To the three general multiplications, the multiplier [7] can be applied. This results in a gate count of $3(15\,\text{XOR} + 16\,\text{AND}) = 45\,\text{XOR} + 48\,\text{AND}$.
- The two additions require $2 \cdot 4 = 8$ XOR gates.
- Constant multiplication with $p_0 = \omega^{14}$ requires 1 XOR gate.
- Squaring of an element requires 2 XOR gates.

Summation of the partial complexities shows that bit parallel inversion is possible with not more than 71 XOR/58 AND gates.

This gate count is remarkably low. It is interesting to compare this complexity with bit parallel *multiplication*. For instance, the multiplier of Mastrovito [7], which is one of the best traditional architectures, has a gate count of 84 XOR/64 AND.

5 Conclusions and Further Research

It has been shown that the decomposition of Galois fields $GF(2^k)$ can be utilized for the construction of efficient bit parallel inverters. For certain fields, in particular for $GF(2^8)$, and inverter can be realized with a gate count equal or smaller than that of a multiplier. This result is contrary to common belief. As a consequence, for certain fields, one might be able to avoid sophisticated algorithm refinements which aim for the reduction of the number of finite field divisions (see e.g. [8]).

For technical applications it will be helpful to provide generators $x^2 + x + p_0$ for tower fields with *multiple* field extensions of degree two. Lists with irreducible polynomials over non-prime fields are very rare in literature. These polynomials should possess optimized coefficients p_0 with respect to the constant multiplication complexity. A theoretical question arising here is whether general statements regarding the complexity of the coefficients p_0 are possible.

One should also investigate how the implementation of communication systems utilizing Galois field arithmetic is affected by multiple field extensions. In general, this approach seems promising since multiplier architectures over composite and tower fields can also be realized very efficiently [3] [9].

References

[1] T. Itoh and S. Tsujii, "A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases," *Information and Computation*, vol. 78, pp. 171–177, 1988.

[2] M. Morii and M. Kasahara, "Efficient construction of gate circuit for computing multiplicative inverses over $GF(2^m)$," *Transactions of the IEICE*, vol. E 72, pp. 37–42, January 1989.

[3] V. Afanasyev, "On the complexity of finite field arithmetic," in *5th Joint Soviet-Swedish Intern. Workshop on Information Theory*, (Moscow, USSR), pp. 9–12, January 1991.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*. Reading, Massachusetts: Addison-Wesley, 1983.

[5] H. Kummer, *Recommendation for space data system standards: Telemetry channel coding: Issue-1*. Consult. Comm. Space Data Syst., September 1983.

[6] C. Paar, *Efficient VLSI Architectures for Bit-Parallel Computation in Galois Fields*. PhD thesis, (Engl. transl.), Institute for Experimental Mathematics, University of Essen, Essen, Germany, June 1994.

[7] E. Mastrovito, "VLSI design for multiplication over finite fields $GF(2^m)$," in *Lecture Notes in Computer Science 357*, pp. 297–309, Springer-Verlag, Berlin, March 1989.

[8] W. L. Eastman, "Inside Euclid's algorithm," in *Coding Theory and Design Theory, Part I, IMA Vol. Appl. Math.*, pp. 113–127, Springer-Verlag, New York, 1990.

[9] C. Paar, "A parallel Galois field multiplier with low complexity based on composite fields," in *6th Joint Swedish-Russian Workshop on Information Theory*, (Mölle, Sweden), pp. 320–324, August 22–27 1993.