A Trace Based $GF(2^n)$ Inversion Algorithm

Haining Fan
fhn@tsinghua.edu.cn

Abstract

By associating Fermat's Little Theorem based $GF(2^n)$ inversion algorithms with the multiplicative Norm function, we present an additive Trace based $GF(2^n)$ inversion algorithm. For elements with Trace value 0, it needs 1 less multiplication operation than Fermat's Little Theorem based algorithms in some $GF(2^n)$s.

Index Terms

Finite field, Inversion algorithm, Norm, Trace.

Efficient implementation of $GF(2^n)$ inversion is important for practical applications and can be found in, for example, Feng's algorithm [1] (received on March 13, 1987 and published in October 1989), which "requires the same number of multiplications as Itoh and Tsujii's algorithm" [2] in [3] (received on July 8, 1987 and published in 1988). These algorithms are based on the fact that $GF(2^n)^*$ is a cyclic group of order $2^n - 1$, i.e., $\forall A \in GF(2^n)^*$,

$$A^{-1} = A^{2^n-2} = A^{2^{n-1}} \cdot A^{2^{n-2}} \cdot A^{2^{n-3}} \cdots A^{2^2} \cdot A^{2^1} = \prod_{i=1}^{n-1} A^{2^i}.$$

The complexities of Feng's algorithm and Itoh-Tsujii's algorithm are:

$$\lfloor \log_2(n-1) \rfloor + HammingWeight(n-1) - 1 \text{ multiplications and } n-1 \text{ squarings.}$$

The above A^{-1} expression itself is close to that of the multiplicative Norm function, which is defined as

$$Norm(A) = \prod_{i=0}^{n-1} A^{2^i}.$$

This viewpoint leads us to consider the additive absolute Trace function, which is defined as

$$Tr(A) = \sum_{i=0}^{n-1} A^{2^i}.$$

If $Tr(A) = \sum_{i=0}^{n-1} A^{2^i} = 0$, then we have $A = \sum_{i=1}^{n-1} A^{2^i}$ and can express A^{-1} as

$$A^{-1} = A^{-2} \sum_{i=1}^{n-1} A^{2^i} = \sum_{i=1}^{n-1} A^{2^i-2} = \sum_{j=0}^{n-2} (A^2)^{2^j-1}.$$

We now give some examples to show the computational produce of this formula for A such that $Tr(A) = 0$.

A. Example $GF(2^3)$

Because $0 = Tr(A) = A + A^2 + A^4$, we have $A = A^2 + A^4$ and $A^{-1} = 1 + A^2$.

This additive formula needs 0 multiplication, 1 addition and 1 squaring. But the multiplicative formula $A^{-1} = A^6 = A^2 A^4$ needs 1 multiplication and 2 squarings.

We note that the above "1+ " operation in a polynomial basis is only a bit NOT operation, and can be merged into a VLSI squarer.

B. Example $GF(2^4)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8$, we have $A = A^2 + A^4 + A^8$ and

$$A^{-1} = 1 + A^2 + A^6 = 1 + A^2 + A^2A^4.$$

This additive formula needs 1 multiplication, 2 additions and 2 squarings. But the multiplicative formula $A^{-1} = A^{14} = A^2A^4A^8$ needs 2 multiplications and 3 squarings.

C. Example $GF(2^5)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16}$, we have $A = A^2 + A^4 + A^8 + A^{16}$ and

$$A^{-1} = 1 + A^2 + A^6 + A^{14} = 1 + A^2 + A^2A^4 + A^2A^4A^8.$$

This additive formula needs 2 multiplications, 3 additions and 3 squarings. The multiplicative formula $A^{-1} = A^{30} = A^2A^4A^8A^{16} = (A^2A^4)(A^2A^4)^4$ needs 2 multiplications and 4 squarings.

D. Example $GF(2^6)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16} + A^{32}$, we have $A = A^2 + A^4 + A^8 + A^{16} + A^{32}$ and

$$A^{-1} = 1 + A^2 + A^6 + A^{14} + A^{30} = 1 + (A + A^3)^2 + [A^7 + A^{15}]^2 = 1 + \{(A + A^3) + [(A + A^3)^4A^3]\}^2.$$

This additive formula needs 2 multiplications, 3 additions and 4 squarings. The multiplicative formula $A^{-1} = A^{62} = A^2A^4A^8A^{16}A^{32} = [A(A^2A^4)(A^2A^4)^4]^2$ needs 3 multiplications and 5 squarings.

E. Example $GF(2^7)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64}$, we have $A = A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64}$ and

$$A^{-1} = 1 + A^2 + A^6 + A^{14} + A^{30} + A^{62} = 1 + A^2 + (A^3 + A^7)^2 + [A^{15} + A^{31}]^2 = 1 + A^2 + \{(A^3 + A^7) + [(A^3 + A^7)^4A^3]\}^2.$$

This additive formula needs 3 multiplications, 4 additions and 5 squarings. The multiplicative formula $A^{-1} = A^{126} = A^2A^4A^8A^{16}A^{32}A^{64} = \{(A \cdot A^2A^4)(A \cdot A^2A^4)^8]\}^2$ needs 3 multiplications and 6 squarings.

F. Example $GF(2^8)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128}$, we have $A = A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128}$ and

$$A^{-1} = 1 + A^2 + A^6 + A^{14} + A^{30} + A^{62} + A^{126} = 1 + (A + A^3 + A^7)^2 + [A^{15} + A^{31} + A^{63}]^2 = 1 + \{(A + A^3 + A^7) + [(A + A^3 + A^7)^8A^7]\}^2.$$

This additive formula needs 3 multiplications, 4 additions and 6 squarings. But the multiplicative formula $A^{-1} = A^{254} = A^2A^4A^8A^{16}A^{32}A^{64}A^{128} = \{A(A \cdot A^2A^4)^2(A \cdot A^2A^4)^{16}\}^2$ needs 4 multiplications and 7 squarings.

There are 14 degree-8 irreducible polynomials over $GF(2)$ whose roots are of Trace 0. Therefore, there are 112 Trace-0 elements in $GF(2^8) - GF(2^4)$.

G. Bad example $GF(2^9)$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128} + A^{256}$, we have
$A = A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128} + A^{256}$ and

$$\begin{aligned} A^{-1} &= 1 + A^2 + A^6 + A^{14} + A^{30} + A^{62} + A^{126} + A^{254} \\ &= 1 + A^2 + [(A^3 + A^7 + A^{15}) + (A^{31} + A^{63} + A^{127})]^2 \\ &= 1 + A^2 + [(A^3 + A^7 + A^{15}) + (A^3 + A^7 + A^{15})^8A^7]^2. \end{aligned}$$

This additive formula needs 4 multiplications, 5 additions and 7 squarings. But the multiplicative formula $A^{-1} = A^{510} = A^2A^4A^8A^{16}A^{32}A^{64}A^{128}A^{256} = [(A^1A^2A^4A^8)(A^1A^2A^4A^8)^{16}]^2$ needs 3 multiplications and 8 squarings.

H. 3-split example $GF(2^{11})$

Because $0 = Tr(A) = A + A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128} + A^{256} + A^{512} + A^{1024}$, we have $A = A^2 + A^4 + A^8 + A^{16} + A^{32} + A^{64} + A^{128} + A^{256} + A^{512} + A^{1024}$ and

$$\begin{aligned} A^{-1} &= 1 + A^2 + A^6 + A^{14} + A^{30} + A^{62} + A^{126} + A^{254} + A^{510} + A^{1022} \\ &= 1 + \{(A^1 + A^3 + A^7) + (A^{15} + A^{31} + A^{63}) + (A^{127} + A^{255} + A^{511})\}^2 \\ &= 1 + \{(A^1 + A^3 + A^7) + [(A^1 + A^3 + A^7)^8 A^7] + [(A^1 + A^3 + A^7)^8 A^7]^8 A^7\}^2. \end{aligned}$$

This additive formula needs 4 multiplications, 5 additions and 9 squarings. The multiplicative formula $A^{-1} = A^{2046} = A^2 A^4 A^8 A^{16} A^{32} A^{64} A^{128} A^{256} A^{512} A^{1024} = [(A^1 A^2 A^4 A^8 A^{16})(A^1 A^2 A^4 A^8 A^{16})^{32}]^2$ needs 4 multiplications and 10 squarings.

Finally, we note that:

1. It is easy to obtain the Trace of an element for practical applications where the $GF(2^n)$ generating irreducible polynomial $f(u)$ is often an irreducible trinomial or pentanomial, see [4] Section 5.1.45 and 5.1.46 or [5], [6] and [7] etc. For example, if $f(u) = u^{233} + u^{74} + 1$ and x is a root of $f(u)$, then $Tr(\sum_{i=0}^{232} a_i x^i) = a_0 + a_{159}$ needs only a single bit XOR [8].

2. Because $(Tr(A) - 0)(Tr(A) - 1) = A^{2^n} - A$, the number of $GF(2^n)$ elements with 0 Trace is 2^{n-1}.

3. When $Tr(A) = \sum_{i=0}^{n-1} A^{2^i} = 0$, the expression $A^{-1} = \sum_{j=0}^{n-2} (A^2)^{2^j - 1}$ is a summation of $n-1$ terms. When $Tr(A) = \sum_{i=0}^{n-1} A^{2^i} = 1$, the expression $A^{-1} = \sum_{i=0}^{n-1} A^{2^i - 1}$ is a summation of n terms.

4. For composite field $GF(2^{nm})$, we may use the Trace t from $GF(2^{nm})$ to $GF(2^n)$, e.g., from $GF(2^8)$ to $GF(2^4)$. If $t \neq 0$ then we need to calculate t^{-1} in $GF(2^n)$.

5. We checked only $n < 15$.

EPILOGUE

This work was inspired by my course taught on 2020-4-15, "Rabin Cryptosystem & Factoring Polynomials over Finite Fields": To find a zero divisor in $GF(p)[u]$ where p is odd, Cantor and Zassenhaus used $A^{(p^n-1)/2}$. For $GF(2)[u]$, one may use the Trace function [9].

Back to 2008, I found it is hard to explain the N-*residue* and the definition of Montgomery's multiplication operation to students. In 2009, I realized that the N-*residue* is just the generalized remainder defined in the following generalized division algorithm [10], and then gave a systematic interpretation of the definition of Montgomery's multiplication.

Theorem 1: $\forall m > 0, a, R^{-1} \in \mathbb{Z}$ s.t. $\gcd(m, R^{-1}) = 1$, there exist unique integers q, r with $0 \le r < m$ s.t. $a = mq + R^{-1}r$.

Based on this generalized remainder, we also derived asymmetric Karatsuba-type multiplication formulae for the first time.

Teaching is interesting.

References

[1] G. Feng, "A VLSI architecture for fast inversion in $GF(2^m)$," IEEE Transactions on Computers, vol. 38, no. 10, pp. 1383–1386, Oct. 1989.

[2] N. Takagi, J. Yoshiki, and K. Takagi, "A fast algorithm for multiplicative inversion in $GF(2^m)$ using normal basis," IEEE Transactions on Computers, vol. 50, no. 5, pp. 394–398, May 2001.

[3] T. Itoh and S. Tsujii, "A fast algorithm for computing multiplicative inverses in $GF(2^m)$," Inform. Comp., vol. 78, pp. 171–177, 1988.

[4] G. L. Mullen and D. Panario, Handbook of Finite Fields. CRC Press, 2013.

[5] I. E. Shparlinski, "On the number of zero trace elements in polynomial bases for $\mathbb{F}_{2^n}$," Rev. Mat. Complut., pp. 177–180, 2005.

[6] O. Ahmadi and A. Menezes, "On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$," Designs, Codes and Cryptography, vol. 37, pp. 493–507, 2005.

[7] R. M. Avanzi, "Another look at square roots and traces (and quadratic equations) in fields of even characteristic," in Selected Areas in Cryptography, SAC-2007, 2007, pp. 138–154.

[8] B. King and B. Rubin, "Improvements to the point halving algorithm," in ACISP 2004, LNCS 3108, 2004, pp. 262–276.

[9] J. Gathen and D. Panario, "Factoring polynomials over finite fields: A survey," J. Symbolic Computation, vol. 31, pp. 3–17, 2001.

[10] H. Fan, J. Sun, M. Gu, and K. Lam, "Obtaining more Karatsuba-like formulae over the binary field," IET Information Security, vol. 6, no. 1, pp. 14–19, 2012.