Theoretical Comparison of Root Computations in Finite Fields*

Ryuichi HARASAWA^{†a)}, Yutaka SUEYOSHI[†], and Aichi KUDO^{††}, *Members*

SUMMARY In the paper [4], the authors generalized the Cipolla-Lehmer method [2], [5] for computing square roots in finite fields to the case of r -th roots with r prime, and compared it with the Adleman-Manders-Miller method [1] from the experimental point of view. In this paper, we compare these two methods from the theoretical point of view.

key words: root computation, finite field, complexity

1. Introduction

Solving algebraic equations over finite fields $\mathbb{F}_q$ is one of the most fundamental topics in computer algebra. The typical equations are of the form

$$x^r = a,$$

given a natural integer $r (\geq 2)$ and an r -th residue element a in the base field.

An important application of r -th root computations in $\mathbb{F}_q$ to computer science is to construct an algebraic curve cryptosystem and a geometric Goppa code using curves of the form $y^r = f(x)$ (e.g., (hyper-)elliptic and super-elliptic curves) over $\mathbb{F}_q$.

For square roots (i.e., $r = 2$), there exist two well-known methods: the Tonelli-Shanks method [6], [7] and the Cipolla-Lehmer method [2], [5]. The idea of the former method is to reduce the computation of square roots in $\mathbb{F}_q$ to that in the Sylow 2-subgroup of $\mathbb{F}_q^*$, and the idea of the latter method is to apply the norm map of $\mathbb{F}_{q^2}$ into $\mathbb{F}_q$. The Tonelli-Shanks method can be extended to the case of r -th roots with r prime, which is called the Adleman-Manders-Miller method [1] (the AMM method for short). The authors extended the Cipolla-Lehmer method to the case of r -th roots with r prime [4], which we call the HSK method. In [4], we further estimated the complexities of the AMM and the HSK methods, and compared them from the experimental point of view.

In this paper, we compare the theoretical complexities of the AMM and the HSK methods. As in the case of square

root computation, the AMM method is more efficient than the HSK method if the largest integer v with $r^v \mid q-1$ is not so large. In this paper, given r and the size of q (i.e., $\log_2 q$), we determine the boundary value of v for the efficiency of these two methods.

2. Root Computation in Finite Fields

In this section, we describe the AMM method [1] and the HSK method [4] for the r -th root computations in finite fields.

Let $\mathbb{F}_q$ be a finite field with q elements, r a prime with $r \mid q-1$, and v the largest integer such that $r^v \mid q-1$.

From now on, we assume $v \geq 2$, because it is easy to compute r -th roots in $\mathbb{F}_q$ for the other cases [4, Section 2].

We present the computational procedures of the AMM method and the HSK method in Tables 1 and 2, respectively.

Furthermore, we can perform Step 2 in Table 2 more efficiently by setting $y \leftarrow x - \alpha$ and by changing the representation of the exponent as

$$\begin{aligned} & \frac{q^{r-1} + \cdots + q + 1}{r} \\ &= \frac{(q^{r-1} - 1) + \cdots + (q - 1) + r}{r} \\ &= \{q^{r-2} + 2q^{r-3} + \cdots + (r-2)q + (r-1)\} \frac{q-1}{r} + 1. \end{aligned}$$

Table 1 AMM algorithm.

Input:	An r -th residue a in $\mathbb{F}_q$.
Output:	An r -th root of a .
Step 1:	Choose an r -th non-residue element b in $\mathbb{F}_q$ by checking whether $b^{(q-1)/r} \neq 1$.
Step 2:	$g \leftarrow b^{(q-1)/r^v}$, $h \leftarrow a^{(q-1)/r^v}$. (We see that g is a primitive r^v -th root of unity and that $h \in \langle g^r \rangle$.)
Step 3:	Compute c_i 's ($0 \leq c_i < r$) s.t. $h = g^{c_1 r + c_2 r^2 + \cdots + c_{v-1} r^{v-1}}$. $g' \leftarrow g^{r^{v-1}}$, $k \leftarrow h$. (The multiplicative group $\langle g' \rangle$ is of order r .) for i from 1 to $v-1$: Compute c_i such that $k^{r^{v-1-i}} = g'^{c_i}$ (that is, a discrete logarithm problem on $\langle g' \rangle$). $k \leftarrow (k/g^{c_i r^i})$. end for
Step 4:	$\alpha \leftarrow g^{c_1 + c_2 r + \cdots + c_{v-1} r^{v-2}}$ (that is, α is an r -th root of h).
Step 5:	Return $\alpha^l a^m$, where two integers l, m satisfy $\{(q-1)/r^v\}l + rm = 1$. (By the definition of v , we have $\gcd((q-1)/r^v, r) = 1$.)

Manuscript received September 19, 2013.

Manuscript revised November 25, 2013.

[†]The authors are with the Graduate School of Engineering, Nagasaki University, Nagasaki-shi, 852-8521 Japan.

^{††}The author is with a Professor Emeritus at Nagasaki University, Nagasaki-shi, 852-8521 Japan.

*This work was partially supported by the Japan Society for the Promotion of Science (JSPS) under the Grant-in-Aid for challenging Exploratory Research No. 24650009.

a) E-mail: harasawa@cis.nagasaki-u.ac.jp

DOI: 10.1587/transfun.E97.A.1378

Table 2 HSK algorithm.

Input:	An r -th residue a in $\mathbb{F}_q$.
Output:	An r -th root of a .
Step 1: Find an irreducible monic polynomial $f(x)$ of degree r with constant term $(-1)^r a$.	
Choose an element α in $\mathbb{F}_q$ s.t. $\beta = (-1)^r(\alpha^r - a)$ is an r -th non-residue. $f(x) \leftarrow (x - \alpha)^r - \beta$.	
Step 2:	Return $x^{\frac{q^{r-1} + \dots + q + 1}{r}} \bmod f(x)$.

More precisely:

Step 2-1: Compute

$$g(y) := (\cdots ((y + \alpha)^q (y + \alpha)^2)^q \cdots)^q (y + \alpha)^{r-1} \bmod (y^r - \beta).$$

Step 2-2: Compute $h(y) := g(y)^{\frac{q-1}{r}} \bmod (y^r - \beta)$.

Step 2-3: Return $h(y)(y + \alpha) \bmod (y^r - \beta)$.

3. Theoretical Comparison of AMM and HSK

In this section, we describe the theoretical complexities of the AMM and the HSK methods, and compare them.

Before considering the complexity, we assume that, for a given r -th residue element a and a random element α in $\mathbb{F}_q$, the probability that the element $(-1)^r(\alpha^r - a)$ is an r -th non-residue is nearly $1 - (1/r) (\geq 1/2)$. This assumption implies that, for the computational procedure of the HSK method, the average number of the iteration of Step 1 in Table 2 is at most two. We remark that the assumption holds if r is sufficiently small as compared with q (e.g., $r = O(\log q)$) [4, Appendix].

To estimate the complexity, we define two positive numbers $d (\leq 1)$ and $\delta (\leq 1)$ as follows:

- It takes $O(r^d)$ operations on $\mathbb{F}_q$ to solve a discrete logarithm problem on the subgroup in $\mathbb{F}_q^*$ of order r . For example, we can take $d = 1$ for the exhaustive search and $d = 0.5$ for the rho method.
- It takes $O(r^{1+\delta})$ operations on $\mathbb{F}_q$ to perform a multiplication of two polynomials over $\mathbb{F}_q$ of degree at most r . For example, we can take $\delta = 1$ for the classical method, $\delta = 0.59$ for the Karatsuba method and $\delta = o(1)$ for the FFT method [3, Definition 8.26].

We then see from [4] that the complexities of the AMM method and the HSK method can be evaluated as $O(\log_2 q + v^2 \log_2 r + vr^d)$ and $O((r + \log_2 q)r^{1+\delta})$ operations on $\mathbb{F}_q$, respectively.

In order to compare the AMM method and the HSK method, we further introduce a non-negative number ϵ , and variables x, y as follows:

- We define ϵ as $\epsilon = (\log_2(\log_2 r))/\log_2 r$, namely, $\log_2 r = r^\epsilon$.
- We define x and y as $x = (\log_2(\log_2 q))/\log_2 r$ and $y = \log_2 v/\log_2 r$, namely, $\log_2 q = r^x$ and $v = r^y$, respectively.

We remark that $0 \leq \epsilon \leq (e \cdot \log_e 2)^{-1} \approx 0.531$, and

Fig. 1 Complexity of AMM in the case $d \geq \epsilon$. **Fig. 2** Complexity of AMM in the case $d \leq \epsilon$.

that $y < x - \epsilon$. Indeed, for the range of ϵ , the inequality $\epsilon \geq 0$ holds for $r \geq 2$, with equality in the case of $r = 2$ (recall that r is a prime number). Letting $t = \log_2 r$ (i.e., $\epsilon = (\log_2 t)/t$), we have $d\epsilon/dt = (1 - \log_e t)/(t^2 \log_e 2)$. Therefore the maximal value of ϵ is $(e \cdot \log_e 2)^{-1}$ at $t = e$ (i.e., $r = 2^e \approx 6.58$). For the relation between x and y , since $r^v \leq q - 1 < q$ holds by the definition of v , we have $r^y = v < \log_r q = \log_2 q / \log_2 r = r^x / \log_2 r$. So we get the relation $y \log_2 r < x \log_2 r - \log_2(\log_2 r)$, namely, $y < x - \epsilon$.

Using the notation above, we can evaluate the complexity of the AMM method as

$$O(r^x + r^{2y+\epsilon} + r^{y+d}) = \begin{cases} O(r^x) & (y \leq \frac{1}{2}x - \frac{1}{2}\epsilon, y \leq x - d), \\ O(r^{2y+\epsilon}) & (y \geq \frac{1}{2}x - \frac{1}{2}\epsilon, y \geq d - \epsilon), \\ O(r^{y+d}) & (y \geq x - d, y \leq d - \epsilon), \end{cases}$$

which is shown in Figs. 1 and 2.

In the same way, we can evaluate the complexity of the HSK method as

$$O((r + r^x)r^{1+\delta}) = \begin{cases} O(r^{2+\delta}) & (x \leq 1), \\ O(r^{x+1+\delta}) & (x \geq 1), \end{cases}$$

which is shown in Fig. 3.

In the following, we compare the complexities of the AMM and the HSK methods by comparing the exponents of r in the evaluations above (recall that $y < x - \epsilon$, $\epsilon \geq 0$ and

Fig. 3 Complexity of HSK.

Fig. 4 Comparison between AMM and HSK for complexity.

$0 < d, \delta \leq 1$):

- (i) In the case of $y \leq \frac{1}{2}x - \frac{1}{2}\epsilon$, $y \leq x - d$:
We have

$$x < \begin{cases} 2 + \delta & (x \leq 1), \\ x + 1 + \delta & (x \geq 1), \end{cases}$$

which implies that the AMM method is more efficient than the HSK method.

- (ii) In the case of $y \geq \frac{1}{2}x - \frac{1}{2}\epsilon$, $y \geq d - \epsilon$:
If $x \leq 1$, then $2y + \epsilon < 2x - \epsilon < 2 + \delta$ holds, which implies that the AMM method is more efficient than the HSK method. If $x \geq 1$, then the AMM method is more efficient than the HSK method if and only if $2y + \epsilon < x + 1 + \delta$, namely, $y < \frac{1}{2}x + \frac{1}{2}(1 + \delta - \epsilon)$.
- (iii) In the case of $y \geq x - d$, $y \leq d - \epsilon$:
We have

$$y + d \leq \begin{cases} 2d - \epsilon < 2 + \delta & (x \leq 1), \\ x + d - \epsilon < x + 1 + \delta & (x \geq 1), \end{cases}$$

which implies that the AMM method is more efficient than the HSK method.

We show the result in Fig. 4. In the domain named “AMM”, the AMM method is more efficient than the HSK method. On the other hand, in the domain named “HSK”, the HSK method is more efficient than the AMM method.

From Fig. 4, we obtain some observations:

Table 3 Upper bounds of $\log_2 q$ for which AMM is more efficient than HSK, independent of the values of v .

r	7	11	13	17	19	23
$\log_2 q$	137.6	418.6	625.4	1181.3	1533.5	2393.0

Table 4 Upper bounds of v for which AMM is more efficient than HSK ($\log_2 q = 500$).

r	3	5	7	11
v (Ex)	60	80	110	140
v (Th)	53.3	73.4	93.4	132.2
Ex/Th	1.13	1.09	1.18	1.06

Table 5 Upper bounds of v for which AMM is more efficient than HSK ($\log_2 q = 1000$).

r	3	5	7	11	13
v (Ex)	100	130	150	200	230
v (Th)	75.4	103.8	132.1	187.0	213.7
Ex/Th	1.33	1.25	1.14	1.07	1.08

Table 6 Upper bounds of v for which AMM is more efficient than HSK ($\log_2 q = 2000$).

r	3	5	7	11	13	17	19
v (Ex)	140	190	210	280	320	420	420
v (Th)	106.6	146.7	186.8	264.5	302.2	376.0	412.3
Ex/Th	1.31	1.30	1.12	1.06	1.06	1.12	1.02

- If $\log_2 q < r^{1+\delta+\epsilon}$ (i.e., $x < 1 + \delta + \epsilon$), then the AMM method is more efficient than the HSK method, independent of the values of v .
- If $\log_2 q > r^{1+\delta+\epsilon}$ (i.e., $x > 1 + \delta + \epsilon$), then the boundary value of v for two methods is $r^{\frac{1}{2}x + \frac{1}{2}(1+\delta-\epsilon)}$. Namely, the AMM method is more efficient than the HSK method if and only if $v < r^{\frac{1}{2}x + \frac{1}{2}(1+\delta-\epsilon)}$.

If we apply the classical method for operations on $\mathbb{F}_q$ (i.e., $\delta = 1$), then we see from the first observation above that the AMM method is more efficient than the HSK method if $\log_2 q < r^{1+\delta+\epsilon} = 3^{2+\{(\log_2(\log_2 3))/\log_2 3\}} \approx 14.3$ (resp. $5^{2+\{(\log_2(\log_2 5))/\log_2 5\}} \approx 58.0$) for the cube (resp. fifth) root computation. In Table 3, we show the approximate upper bounds of $\log_2 q$, namely, $r^{1+\delta+\epsilon} = r^{2+\{(\log_2(\log_2 r))/\log_2 r\}}$ for some other values of r . We note that the theoretical estimation on the upper bounds of $\log_2 q$ is consistent with our experimental results in [4], where we implemented r -th root computations in $\mathbb{F}_q$ for $\log_2 q = 500, 1000, 2000$ and $3 \leq r \leq 23$.

Similarly, under the condition $\delta = 1$, we show the approximate boundary values of v (i.e., the upper bounds of v in terms of r and q for which the AMM method is more efficient than the HSK method) based on both the experimental results in [4] (denoted by “Ex”) and the theoretical estimation $r^{\frac{1}{2}x + \frac{1}{2}(1+\delta-\epsilon)}$ (denoted by “Th”) in Tables 4–6. Since both the AMM and the HSK methods are randomized algorithms, the theoretical boundary values of v are consistent with the experimental boundary values.

4. Conclusion

In this paper, we compared the theoretical complexities of the AMM and the HSK methods for computing r -th roots in finite fields $\mathbb{F}_q$, and estimated some boundary values for efficiency of these two methods.

Acknowledgments

We are grateful to the referee for his/her helpful comments.

References

- [1] L. Adleman, K. Manders and G. Miller, "On taking roots in finite fields," Proc. 18th IEEE Symposium on Foundations on Computer Science (FOCS), pp.175–178, 1977.
 - [2] M. Cipolla, "Un metodo per la risoluzione della congruenza di secondo grado," Rendiconto dell'Accademia delle Scienze Fisiche e Matematiche, Napoli, vol.9, pp.154–163, 1903.
 - [3] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, Second ed., Cambridge, 2003.
 - [4] R. Harasawa, Y. Sueyoshi, and A. Kudo, "Root computation in finite fields," IEICE Trans. Fundamentals, vol.E96-A, no.6, pp.1081–1087, June 2013.
 - [5] D.H. Lehmer, Computer technology applied to the theory of numbers, Studies in Number Theory, pp.117–151, Prentice-Hall, Englewood Cliffs, NJ, 1969.
 - [6] D. Shanks, Five number-theoretic algorithms, Proc. 2nd Manitoba Conf. Numer. Math., pp.51–70, Manitoba, Canada, 1972.
 - [7] A. Tonelli, Bemerkung über die Auflösung quadratischer Congruenzen, Göttinger Nachrichten, pp.344–346, 1891.
-