J. Korean Math. Soc. **57** (2020), No. 4, pp. 1019–1030
https://doi.org/10.4134/JKMS.j190569
pISSN: 0304-9914 / eISSN: 2234-3008

TRACE EXPRESSION OF r-TH ROOT OVER FINITE FIELD

Gook Hwa Cho, Namhun Koo, and Soonhak Kwon

Abstract. Efficient computation of r-th root in $\mathbb{F}_q$ has many applications in computational number theory and many other related areas. We present a new r-th root formula which generalizes Müller's result on square root, and which provides a possible improvement of the Cipolla-Lehmer type algorithms for general case. More precisely, for given r-th power $c \in \mathbb{F}_q$, we show that there exists $\alpha \in \mathbb{F}_{q^r}$ such that

$$Tr\left(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}\right)^r = c,$$

where $Tr(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{r-1}}$ and α is a root of certain irreducible polynomial of degree r over $\mathbb{F}_q$.

1. Introduction

Let $r > 1$ be an integer and q be a power of a prime. Finding r-th root (or finding a root of $x^r = c$) in finite field $\mathbb{F}_q$ has many applications in computational number theory and in many other related topics. Some such examples include point halving and point compression on elliptic curves [16], where square root computations are needed. Similar applications for high genus curves require r-th root computation also.

Among several available root extraction methods of the equation $x^r - c = 0$, two algorithms are applicable for any integer $r > 1$; the Adleman-Manders-Miller [1] algorithm, a straightforward generalization of the Tonelli-Shanks

Received August 19, 2019; Accepted December 12, 2019.
2010 *Mathematics Subject Classification.* 11T06, 11Y16, 68W40.
Key words and phrases. Finite field, trace, r-th root, linear recurrence relation, Tonelli-Shanks algorithm, Adleman-Manders-Miller algorithm, Cipolla-Lehmer algorithm.
This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2019R1A6A1A11051177). Gook Hwa Cho was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (No. NRF-2018R1D1A1B07041716). Namhun Koo was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (No. 2016R1A5A1008055). Soonhak Kwon was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016R1D1A1B03931912, No. 2016R1A5A1008055 and No. 2019R1F1A1058920).

square root algorithm [17, 19] to the case of r-th roots, and the Cipolla-Lehmer [6, 11] algorithms. Due to the cumbersome extension field arithmetic need for the Cipolla-Lehmer algorithm, one usually prefers the Tonelli-Shanks or the Adleman-Manders-Miller, and other related researches [2, 3, 10] exist to improve the Tonelli-Shanks.

The efficiency of the Adleman-Manders-Miller algorithm depends on the exponent ν of r satisfying $r^\nu \mid q-1$ and $r^{\nu+1} \nmid q-1$, which makes the worst case complexity of the Adleman-Manders-Miller $O(\log r \log^4 q)$ [1, 4, 13] while the Cipolla-Lehmer can be executed in $O(r \log^3 q)$ [6, 11]. Even in the case of $r = 2$, it had been observed in [15] that, for the prime $p = 9 \times 2^{3354} + 1$, running the Tonelli-Shanks algorithm using various software such as Magma, Mathematica and Maple cost roughly 5 minutes, 45 minutes, 390 minutes, respectively while the Cipolla-Lehmer costs under 1 minute in any of the above softwares. It should be mentioned that such extreme cases (of p with $p-1$ divisible by high powers of 2) do happen in many cryptographic applications. For example, one of the NIST suggested curve [16] P-224 : $y^2 = x^3 - 3x + b$ over $\mathbb{F}_p$ uses the prime $p = 2^{224} - 2^{96} + 1$.

On the other hand, it is also true that the Adleman-Manders-Miller runs faster than the Cipolla-Lehmer for small exponent ν. A possible speed-up of the Cipolla-Lehmer comparable to the Tonelli-Shanks for low exponent ν was first given by Müller [15], where a special type of Lucas sequence corresponding to $f(x) = x^2 - Px + 1$ was used. The constant term 1 of $f(x)$ makes the given algorithm runs quite faster compared with the original Cipolla-Lehmer. A similar result for the case $r = 3$ was also obtained in [5].

In this paper, we show that the idea in [15] can be generalized to any integer $r > 1$. More precisely, for any r-th power c in $\mathbb{F}_q$, we can construct a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree r with constant term ± 1 such that the irreducibility of f implies that $\left\{Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}})\right\}^r = c$ where $f(\alpha) = 0$ and $Tr(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{r-1}}$ and the trace map $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as $Tr(\beta) = \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{r-1}}$. We mention that the case $r = 2$ (i.e., $\{Tr(\alpha^{\frac{q-1}{4}})\}^2 = c$) is the result in [15] and the case $r = 3$ (i.e., $\{Tr(\alpha^{\frac{q^2+q-2}{9}})\}^3 = c$) is shown in [5]. Therefore a possible existence of efficient linear recurrence relation computing $Tr(\alpha^m)$ guarantees the existence of efficient r-th root algorithm, where the cases $r = 2, 3$ are well-known.

The remainder of this paper is organized as follows: In Section 2, we introduce the related algorithms; Müller's square root algorithm and Cho et al.'s cube root algorithm, and the improved ideas. In Section 3, we propose a new r-th formula which has a possible application when combined with linear recurrence relations. Finally, in Section 4, we give concluding remarks and future works.

2. Related algorithms and the new idea

In this section, we explain Müller's square root algorithm [15]. And we briefly sketch Cho et al.'s cube root algorithm [5] which is inspired by the work of Müller on the quadratic case. Finally, we propose the improved ideas.

2.1. Müller's square root algorithm

A new Cipolla-Lehmer type algorithm for $r = 2$ was found by Müller [15]. For a given irreducible quadratic polynomial $f(x) = x^2 - Px + Q \in \mathbb{F}_q[x]$ with roots α and β, one has the corresponding Lucas sequence $s_k = \alpha^k + \beta^k$ for positive integer k. Computing s_k via the relation $s_k = Ps_{k-1} - Qs_{k-2}$ can be simple if $Q = 1$, that is, $f(x) = x^2 - Px + 1$.

Let Q be a square in $\mathbb{F}_q$. Assume that $q \equiv 1 \pmod 4$ and $f(x) = x^2 - Px + 1$ with $P = Q - 2$ is irreducible over $\mathbb{F}_q$. Letting $\alpha, \alpha^{-1} \in \mathbb{F}_{q^2}$ be roots of $f(x)$, Müller [15] found a square root of Q as $s_{\frac{q-1}{4}}$. Lucas sequence is well-known [15] that the sequence s_k satisfies

$$s_{2n} = s_n^2 - 2, \qquad s_{n+m} = s_n s_m - s_{n-m}$$

for positive integers n, m. Using the above relations, one can compute $s_{\frac{q-1}{4}}$ by the usual "double and add" method. Müller's algorithm requires $2\log q$ multiplications in $\mathbb{F}_q$ on average.

2.2. Cho et al.'s cube root algorithm

In [5], Cho et al. extended Müller's square root algorithm to a cube root algorithm. Let b be in $\mathbb{F}_q$ and suppose $f(x) = x^3 - 3x^2 + bx - 1$ is irreducible over $\mathbb{F}_q$. Suppose $f(\alpha) = 0$ with $\alpha \in \mathbb{F}_{q^3}$. Letting $h(x) = x^3 + (b-3)x - (b-3)$, it is shown in [5] that $h(1-\alpha) = 0$. In fact, one has

$$h(1 - x) = -f(x).$$

Therefore, the irreducibility of f implies the irreducibility of h and vice versa. Letting $Tr(\alpha) = \alpha + \alpha^q + \alpha^{q^2}$, the main result of Cho et al. [5] is given below.

Theorem 2.1 (Cho et al. [5])**.** *Suppose that $q \equiv 1 \pmod 9$ and c is a cubic residue in $\mathbb{F}_q$. Let $f(x) = x^3 - 3x^2 + bx - 1$ with $b = ct^3 + 3$ for some t and $f(\alpha) = 0$. If $f(x)$ is irreducible, then $t^{-1} \cdot Tr(\alpha^{\frac{q^2+q-2}{9}})$ is a cube root of c in $\mathbb{F}_q$.*

To compute $Tr(\alpha^{\frac{q^2+q-2}{9}})$, Cho et al. considered the third order characteristic sequences. Let $f(x) = x^3 - ax^2 + bx - c$ $(a, b, c \in \mathbb{F}_q)$ be irreducible over $\mathbb{F}_q$. The third order characteristic sequence s_k corresponding to $f(x)$ is defined as

$$s_k = as_{k-1} - bs_{k-2} + cs_{k-3}, \qquad k \geq 3.$$

If s_k has the initial state $s_0 = 3, s_1 = a$ and $s_2 = a^2 - 2b$, then s_k is called the characteristic sequence generated by $f(x)$ and one has

$$s_k(\alpha) = Tr(\alpha^k) = \alpha^k + \alpha^{kq} + \alpha^{kq^2}.$$

It is well-known [5, 9] that the sequence s_k satisfies

$$s_{2n} = s_n^2 - 2s_{-n}, \qquad s_{n+m} = s_n s_m - s_{n-m}s_{-m} + s_{n-2m}.$$

Using the above relations, one can compute $s_{\frac{q^2+q-2}{9}}$ by the usual "double and add" method. Cho et al.'s algorithm requires $15 \log q$ multiplications on average.

2.3. The improved ideas

Let $c \in \mathbb{F}_q$ be an r-th power in $\mathbb{F}_q$ with $q \equiv 1 \pmod r$. To find an r-th root of c, the Cipolla-Lehmer algorithm needs an irreducible polynomial $f(x) = x^r - b_{r-1}x^{r-1} - b_{r-2}x^{r-2} - \cdots - b_1 x + (-1)^r c \in \mathbb{F}_q[x]$ with constant term $(-1)^r c$, $b_i \in \mathbb{F}_q$. Letting $\alpha \in \mathbb{F}_{q^r}$ be a root of f, we get $\alpha^{1+q+q^2+\cdots+q^{r-1}} = c$ so that $\alpha^{\frac{\sum_{i=0}^{r-1} q^i}{r}}$ is an r-th root of c.

Irreducibility testing of f and the exponentiation $\alpha^{\frac{\sum_{i=0}^{r-1} q^i}{r}}$ (or computing $x^{\frac{\sum_{i=0}^{r-1} q^i}{r}} \pmod{f(x)}$) need many multiplications in $\mathbb{F}_q$, and the number of such multiplications depends on the coefficients of f. One may choose a low hamming-weight polynomial (i.e., trinomial) to reduce the cost of computing $x^{\frac{\sum_{i=0}^{r-1} q^i}{r}} \pmod{f(x)}$.

Note that letting the constant term of $f(x)$ to be ± 1 makes it impossible to use the Cipolla-Lehmer. For example, to apply the Cipolla-Lehmer for the computation of the roots of $x^2 - c = 0$, one has to use the polynomial $x^2 - bx + c$ not $x^2 - bx + 1$. However, as is done by Müller [15] for the quadratic case. In a similar way, Cho et al. [5] proposed the cube root algorithm to use the polynomial $x^3 - ax^2 + bx - 1$.

A wise choice of f of degree r gives a way to find the r-th root of $c \in \mathbb{F}_q$ as will be shown in the next sections. From now on, we will consider the characteristic sequence s_k which comes from the irreducible polynomial $f(x) = x^r - b_{r-1}x^{r-1} - b_{r-2}x^{r-2} - \cdots - b_1 x + (-1)^r \in \mathbb{F}_q[x]$, $b_i \in \mathbb{F}_q$. An r-th order characteristic sequence s_k corresponding to $f(x)$ is defined as

$$s_k = b_{r-1}s_{k-1} + b_{r-2}s_{k-2} + \cdots + s_{k-r}, \qquad k \geq r.$$

Then s_k can be expressed as

$$s_k = Tr(\alpha^k) = \alpha^k + \alpha^{kq} + \alpha^{kq^2} + \cdots + \alpha^{kq^{r-1}},$$

where α is a root of $f(x)$.

The main contribution of this paper is given below.

Theorem 2.2 (The main result)**.** *Suppose that* $q \equiv 1 \pmod{r^2}$ *and* $f(x) = (x + (-1)^r)^r + (-1)^{r+1}(b + (-1)^r r)x$ *is an irreducible polynomial over* $\mathbb{F}_q$ *with* $f(\alpha) = 0$. *Assume* $b + (-1)^r r$ *is an* r*-th power in* $\mathbb{F}_q$. *Then* $s_{\frac{(\sum_{i=0}^{r-1} q^i) - r}{r^2}}(\alpha)^r = b + (-1)^r r$.

The above result is a generalization of the cubic case of Cho et al. [5], and it will be proven in the next section.

3. New improved algorithm

3.1. Generalization of Cho et al.'s algorithm

In this subsection we generalize Cho et al.'s algorithm to $r > 1$. Please refer [5] for the case $r = 3$ and compare it with our generalization. Let r be an integer > 1 and let b be in $\mathbb{F}_q$ with $q \equiv 1 \pmod r$ such that

$$f(x) = (x + (-1)^r)^r + (-1)^{r+1}(b + (-1)^r r)x \tag{1}$$

is irreducible over $\mathbb{F}_q$. Suppose that α is a root of $f(x)$. If we set

$$\beta = (1 + \alpha + \alpha^{1+q} + \cdots + \alpha^{1+q+\cdots+q^{r-2}})^{\frac{1-q}{r}},$$

then we get $\beta^r = \alpha$. From now, we generalize the results in [5] for the case $r > 1$.

Theorem 3.1 (Generalization of Theorem 1 in [5])**.** *Assuming* $f(\alpha) = 0$ *and* $q \equiv 1 \pmod r$*, we have*

$$\alpha^{\frac{1+q+q^2+\cdots+q^{r-1}}{r}} = (b+r)^{-\frac{q-1}{2}} \quad \textit{if } r \textit{ is even},$$
$$\alpha^{\frac{1+q+q^2+\cdots+q^{r-1}}{r}} = 1 \quad \textit{if } r \textit{ is odd}.$$

In particular, when r *is even and* $b+r$ *is a square in* $\mathbb{F}_q$*, one gets* $\alpha^{\frac{1+q+q^2+\cdots+q^{r-1}}{r}} = 1$.

Proof. By similar argument in proof of Theorem 1 of [5]

$$\alpha^{\frac{\sum_{i=0}^{r-1} q^i}{r}} = (b + (-1)^r r)^{-(q-1)\frac{\sum_{i=0}^{r-2}\sum_{j=0}^{i} q^j}{r}}.$$

Since $q \equiv 1 \pmod r$, we have

$$\sum_{i=0}^{r-2}\sum_{j=0}^{i} q^j \equiv \frac{r(r-1)}{2} \pmod r,$$

which is $\frac{r}{2} \pmod r$ when r is even, and is $0 \pmod r$ when r is odd. Noticing $b + (-1)^r r \in \mathbb{F}_q$, one has the desired result. □

From the above theorem, one obtains the following generalizations of the three corollaries in [5] :

Corollary 3.2 (Generalization of Corollary 1 in [5])**.** *Assume* $q \equiv 1 \pmod r$*. If* r *is even, further assume that* $b+r$ *is a square in* $\mathbb{F}_q$*. Then* $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r}}(\beta)^r = s_{\sum_{i=0}^{r-2} q^i}(\beta)^r$.

Corollary 3.3 (Generalization of Corollary 2 in [5]). *Assuming the same conditions as in the Lemma 3.2 and also assuming* $q \equiv 1 \pmod{r^2}$, *one has* $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(\alpha)^r = s_{\sum_{i=0}^{r-2} q^i}(\beta)^r$.

If $b + (-1)^r r$ is an r-th power in $\mathbb{F}_q$, one can explicitly find r-th root of $b + (-1)^r r$ as follows.

Corollary 3.4 (Generalization of Corollary 3 in [5]). *Assume that* $q \equiv 1 \pmod{r}$ *and* $b+(-1)^r r$ *is an* r*-th power in* $\mathbb{F}_q$, *then* $s_{\sum_{i=0}^{r-2} q^i}(\beta)^r = b+(-1)^r r$.

Now we are ready to prove the main theorem.

Proof of Theorem 2.2. We have

$$s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(\alpha)^r = s_{\sum_{i=0}^{r-2} q^i}(\beta)^r = b + (-1)^r r,$$

where the first equality comes from Corollary 3.3 and the second equality is Corollary 3.4. □

Now using the polynomial $f(x)$, we can find an r-th root for given r-th power c in $\mathbb{F}_q$. For given r-th power $c \in \mathbb{F}_q$, define $b = c - (-1)^r r$. If $f(x)$ with given coefficient b is irreducible, then $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f)$ is an r-th root of c. That is,

$$s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f)^r = b + (-1)^r r = c.$$

If the given f is not irreducible over $\mathbb{F}_q$, then we may twist c by random $t \in \mathbb{F}_q$ until we get irreducible f with $b = ct^r - (-1)^r r$. Then

$$s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f)^r = b + (-1)^r r = ct^r,$$

which implies $t^{-1} s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f)$ is an r-th root of c (See Table 1).

3.2. Closed formula for $Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}})$

In Theorem 2.2, we showed that, if $f(x) = (x + (-1)^r)^r + (-1)^{r+1}(b + (-1)^r r)x$ is an irreducible polynomial over $\mathbb{F}_q$ with $f(\alpha) = 0$, and if $b + (-1)^r r$ is an r-th power residue in $\mathbb{F}_q$, then $Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}})$ is an r-th root of $b+(-1)^r r$. Therefore efficient linear recurrence relations can be used to compute the trace values, where the cases $r = 2, 3$ are well-known Lucas type sequences. When $r > 3$, it is not so easy to find efficient linear recurrences but we can do better without using intermediate trace values s_k.

For any integer $k \geq 0$, let $\alpha^k = \sum_{i=0}^{r-1} X_i(k)\alpha^i \in \mathbb{F}_q[\alpha]$. Then our r-th root $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(\alpha) = Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}})$ has a very simple algebraic relation among

TABLE 1. New r-th root algorithm for $\mathbb{F}_q$ with $q \equiv 1 \pmod{r^2}$

Input: An r-th power c in $\mathbb{F}_q$ Output: s satisfying $s^r = c$
Step 1: $t \leftarrow 1$, $b \leftarrow ct^r - (-1)^r r$, $f(x) \leftarrow (x + (-1)^r)^r + (-1)^{r+1}(b + (-1)^r r)x$
Step 2: **while** $f(x)$ is reducible over $\mathbb{F}_q$ Choose random $t \in \mathbb{F}_q$ $b \leftarrow ct^r - (-1)^r r$, $f(x) \leftarrow (x + (-1)^r)^r + (-1)^{r+1}(b + (-1)^r r)x$ **end while**
Step 3: $s \leftarrow s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f) \cdot t^{-1}$

the coefficient X_i's. That is, letting $m = \frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}$ be the exponent of α, we will prove that

$$Tr(\alpha^m) = X_0(m) - X_{r-1}(m)$$

in this subsection.

Lemma 3.5. *Let q be a prime power with $q \equiv 1 \pmod r$ and let $b \in \mathbb{F}_q$ such that $f(x) = (x+(-1)^r)^r+(-1)^{r+1}(b+(-1)^r r)x$ is irreducible over $\mathbb{F}_q$. Suppose $f(\alpha) = 0$. Then $Tr(\frac{1}{1+(-1)^r\alpha}) = 1$.*

Proof. Defining $h(x) \in \mathbb{F}_q[x]$ as

$$h(x) = x^r + (-1)^{r+1}(b + (-1)^r r)(x - 1), \tag{2}$$

one finds

$$h(1 + (-1)^r x) = (-1)^r f(x). \tag{3}$$

More precisely, one has the followings.

$$\begin{aligned} \text{For odd } r: \quad & f(x) = (x-1)^r + (b-r)x,\ h(x) = x^r + (b-r)x - (b-r), \\ & h(1-x) = -f(x), \\ \text{For even } r: \quad & f(x) = (x+1)^r - (b+r)x,\ h(x) = x^r - (b+r)x + (b+r), \\ & h(1+x) = f(x). \end{aligned}$$

Since α is a root of $f(x) = 0$, one get

$$h(1 + (-1)^r\alpha) = (-1)^r f(\alpha) = 0. \tag{4}$$

Therefore,

$$Tr(\frac{1}{1+(-1)^r\alpha}) = (1+(-1)^r\alpha)^{-1}+(1+(-1)^r\alpha)^{-q}+\cdots+(1+(-1)^r\alpha)^{-q^{r-1}}$$

$$= \frac{\sum_{j=0}^{r-1}\prod_{i=0,i\neq j}^{r-1}(1+(-1)^r\alpha)^{q^i}}{\prod_{i=0}^{r-1}(1+(-1)^r\alpha)^{q^i}}$$
$$= \frac{b+(-1)^r r}{b+(-1)^r r} = 1,$$

where the third equality comes from property of roots of $h(x)$. That is, the denominator $b+(-1)^r r$ is the constant term of $h(x)$ multiplied by $(-1)^r$ and is same to the numerator which is the coefficient of x in $h(x)$ multiplied by $(-1)^{r-1}$. This is clear when one sees the expression of $h(x)$ in the equation (2). □

It should be mentioned that another proof of the above lemma can be obtained by thinking of the reciprocal polynomial $x^r h(1/x)$.

Lemma 3.6. *Assume the same conditions as in Lemma 3.5 and further assume that $b+(-1)^r r$ is an r-th power residue in $\mathbb{F}_q$. Then one has*

$$\sum_{i=1}^{r-1}\alpha^{\frac{q^i-1}{r}} = -1 \quad \textit{and} \quad \sum_{i=1}^{r-1}\alpha^{\frac{1-q^i}{r}} = (-1)^r\alpha.$$

Proof. Since $h(1+(-1)^r\alpha)=0$, using the equation (2), one has

$$(1+(-1)^r\alpha)^r = (b+(-1)^r r)\alpha.$$

By taking $\frac{q-1}{r}$-th power to both sides, since $b+(-1)^r r$ is an r-th residue by the assumption,

$$(1+(-1)^r\alpha)^{q-1} = (b+(-1)^r r)^{\frac{q-1}{r}}\alpha^{\frac{q-1}{r}} = \alpha^{\frac{q-1}{r}}. \tag{5}$$

Denote $A = \alpha^{\frac{q-1}{r}} + \alpha^{\frac{q^2-1}{r}} + \cdots + \alpha^{\frac{q^{r-1}-1}{r}}$. Then,

$$\begin{aligned}
A &= \alpha^{\frac{q-1}{r}} + \alpha^{\frac{(q-1)(1+q)}{r}} + \cdots + \alpha^{\frac{(q-1)(1+q+\cdots+q^{r-2})}{r}} \\
&= (1+(-1)^r\alpha)^{q-1} + (1+(-1)^r\alpha)^{(q-1)(1+q)} + \cdots \\
&\quad + (1+(-1)^r\alpha)^{(q-1)(1+q+\cdots+q^{r-2})} \\
&= (1+(-1)^r\alpha)^{q-1} + (1+(-1)^r\alpha)^{q^2-1} + \cdots + (1+(-1)^r\alpha)^{q^{r-1}-1} \\
&= \frac{Tr(1+(-1)^r\alpha) - (1+(-1)^r\alpha)}{1+(-1)^r\alpha} = -1,
\end{aligned}$$

where the second equality comes from the equation (5), and last equality comes from $Tr(1+(-1)^r\alpha)=0$ which is clear from the equation (2).

Now denote $B = \alpha^{\frac{1-q}{r}} + \alpha^{\frac{1-q^2}{r}} + \cdots + \alpha^{\frac{1-q^{r-1}}{r}}$ and let $\gamma = \frac{1}{1+(-1)^r\alpha}$, then $B = \gamma^{q-1} + \gamma^{q^2-1} + \cdots + \gamma^{q^{r-1}-1}$ again by (5). Then

$$\begin{aligned}
\gamma B &= \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{r-1}} \\
&= Tr(\gamma) - \gamma = 1 - \gamma,
\end{aligned}$$

where the last equality comes from Lemma 3.5. Therefore $B = \frac{1-\gamma}{\gamma} = (-1)^r\alpha$. □

Now we are ready to state our final theorem which gives a simple expression of r-th root $Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}})$ of the r-th power residue $b + (-1)^r r$ which was obtained in Theorem 2.2.

Theorem 3.7. *Suppose that* $q \equiv 1 \pmod{r^2}$ *where q is a prime power and* $r > 1$ *is an integer, and suppose that* $f(x) = (x+(-1)^r)^r+(-1)^{r+1}(b+(-1)^r r)x$ *is an irreducible polynomial over* $\mathbb{F}_q$ *with* $f(\alpha) = 0$. *Let* $c = b + (-1)^r r$ *be an r-th power residue in* $\mathbb{F}_q$. *Then one has*

$$Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}) = a_0 - a_{r-1} \in \mathbb{F}_q,$$

where $\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}} = a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} \in \mathbb{F}_q[\alpha]$.

Proof. We have

$$\begin{aligned} Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}) &= \sum_{j=0}^{r-1} \alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2} q^j} \\ &= \alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}} \left(1 + \sum_{j=1}^{r-1} \alpha^{\frac{1-q^j}{r}} \right) \\ &= (a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1})(1 + (-1)^r\alpha) \\ &= a_0 - a_{r-1}, \end{aligned}$$

where the second equality comes from Theorem 3.1, the third equality comes from Lemma 3.6, and the last equality comes from the fact that the constant term of $(-1)^r a_{r-1}\alpha^r$ as a $\mathbb{F}_q$-linear combination of $1, \alpha, \ldots, \alpha^{r-1}$ is $-a_{r-1}$. □

By Theorem 3.7, we can find an r-th root for given r-th power c in $\mathbb{F}_q$. In Step 3 of Table 1, $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f) \cdot t^{-1}$ is a root of c. That is,

$$s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f) \cdot t^{-1} = Tr(\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}) \cdot t^{-1} = (a_0 - a_{r-1}) \cdot t^{-1},$$

where $\alpha^{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}} = a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} \in \mathbb{F}_q[\alpha]$.

3.3. Simple formulas for $q \not\equiv 1 \pmod{r^2}$

Our theorem and examples were explained on the assumption of $q \equiv 1 \pmod{r^2}$. However it should be mentioned that one can find an r-th root of c when $q \not\equiv 1 \pmod{r^2}$ easily. For example, when $r = 2$ and $q \equiv 3 \pmod 4$, a square root of a quadratic residue c is given by $c^{\frac{q+1}{4}}$. Also when $r = 3$ and $q \not\equiv 1 \pmod 9$, one has the followings. When $q \equiv 2 \pmod 3$, a cube root of c

is given as $c^{\frac{2q-1}{3}}$. When $q \equiv 4 \pmod 9$, a cube root of cubic residue c is given by $c^{\frac{2q+1}{9}}$. When $q \equiv 7 \pmod 9$, a cube root of cubic residue c is given by $c^{\frac{q+2}{9}}$. Thus the computational cost of finding cube root of c when $q \not\equiv 1 \pmod 9$ is just one exponentiation in $\mathbb{F}_q$.

These closed formulas are not obtained by ad-hoc method. In fact, one has the following simple result of r-th root when $q \not\equiv 1 \pmod{r^2}$.

Proposition 3.8 (Generalization of Proposition 1 in [5]). *Let q be a prime power such that $q \equiv 1 \pmod r$ but $q \not\equiv 1 \pmod{r^2}$. Assume that* $\gcd(\frac{q-1}{r}, r) = 1$. *Then, for given r-th power c in $\mathbb{F}_q$, an r-th root of c can be computed by the cost of one exponentiation in $\mathbb{F}_q$. In particular, if r is a prime, then the condition* $\gcd(\frac{q-1}{r}, r) = 1$ *is automatically satisfied so that the cost of finding r-th root of c is just one exponentiation.*

Proof. We claim that there is an integer θ depending only on r and q but not on c such that

$$(A)\ \theta < rq, \qquad (B)\ r^2 \mid \theta, \qquad (C)\ \left(c^{\frac{\theta}{r^2}}\right)^r = c.$$

The condition (C) of the above equation says that $c^{\frac{\theta}{r}} = c$, i.e., $c^{\frac{\theta - r}{r}} = 1$. Since c is an r-th power in $\mathbb{F}_q$, this condition can be satisfied if $\theta \equiv r \pmod{(q-1)}$. Therefore writing $\theta = r + k(q-1)$, the condition (B) says that one should have $r + k(q-1) \equiv 0 \pmod{r^2}$, which is equivalent to the following equation

$$1 + k\frac{q-1}{r} \equiv 0 \pmod r. \tag{6}$$

Since $\gcd(\frac{q-1}{r}, r) = 1$, the above equation has unique solution $k \pmod r$. Now the condition (C) is satisfied because $\theta = kq + r - k \le (r-1)q + 1 < rq$. Finally, if r is a prime, then the assumption $q \not\equiv 1 \pmod{r^2}$ implies $\gcd(\frac{q-1}{r}, r) = 1$. □

Example 1. When $r = 5$, the equation (6) becomes $1 + k\frac{q-1}{5} \equiv 0 \pmod 5$. Therefore depending on the values of $\frac{q-1}{5} \pmod 5$, the corresponding $k \pmod 5$ is uniquely determined and they are

$$\left(\frac{q-1}{5}, k\right) = (1,4), (2,2), (3,3), (4,1).$$

Since $\frac{q-1}{5} \equiv j \pmod 5$ implies $q \equiv 5j + 1 \pmod{5^2}$, we have the following table of pairs of $q \pmod{5^2}$ and corresponding $\theta = kq + 5 - k$

$$(q \pmod{25},\ \theta) = (6, 4q+1), (11, 2q+3), (16, 3q+2), (21, q+4).$$

For example, when $q \equiv 6 \pmod{25}$, the 5-th root of c is given as $c^{\frac{4q+1}{25}}$, and when $q \equiv 11 \pmod{25}$, the 5-th root of c is given as $c^{\frac{2q+3}{25}}$, etc.

Remarks. 1. The reason why we only consider the case $r \mid q-1$ (i.e., $q \equiv 1 \pmod r$) is as follows. If $r \nmid q-1$, then one has $\gcd(r, q-1) = 1$ and there are a, b satisfying $ra + (q-1)b = 1$. Thus for any $c \in \mathbb{F}_q$, we have $c = c^{ra+(q-1)b} = (c^a)^r$. That is, any element c is an r-th powers of c^a.

2. For r-th root extraction, considering the cases $r = prime$ is enough for practical purposes. For example, to find 4-th root of $c \in \mathbb{F}_q$, we only have to use square root algorithm twice instead of using 4-th root algorithm once, and the complexity of two applications of square root algorithm is lower than that of one application of 4-th root algorithm.

4. Conclusions

Randomly selected monic polynomial over $\mathbb{F}_q$ of degree r with nonzero constant term is irreducible with probability $\frac{1}{r}$ (For an explanation, see [14, 18]). Even if our choice of f in (1) is not really random, experimental evidence (using software tools such as MAPLE and SAGE) shows that $\frac{1}{r}$ of such f is irreducible, which implies that an irreducible f can be found after r random tries. Irreducibility testings of low degree polynomials are well understood and can be implemented efficiently, see [7, 12, 14, 18]. Therefore the algorithm in Table 1 is dominated by the complexity of step 3 which computes $s_{\frac{(\sum_{i=0}^{r-1} q^i)-r}{r^2}}(f)$. For $r = 2, 3$, i.e., for quadratic and cubic polynomials, the well-known linear recurrence sequences give faster algorithms than previously proposed Cipolla-Lehmer type algorithms. For $r > 3$, there are some known recurrence relations, for example in [8]. However, we can't ensure that r-th order linear recurrence sequence is efficient for $r > 3$. When $r > 3$, we can find r-th root using classic "square and multiply" by polynomial $f(x)$ with constant term ± 1. This method is efficient than Cipolla-Lehmer algorithm using random polynomial. However those might not be the best recurrence relations to compute $s_m(f)$ and further study is needed.

References

[1] L. Adleman, K. Manders, and G. Miller, *On taking roots in finite fields*, in 18th Annual Symposium on Foundations of Computer Science (Providence, R.I., 1977), 175–178, IEEE Comput. Sci., Long Beach, CA, 1977.

[2] A. O. L. Atkin, *Probabilistic primality testing*, summary by F. Morain, Inria Research Report **1779** (1992), 159–163,

[3] D. Bernstein, *Faster square root in annoying finite field*, Preprint, Available from http://cr.yp.to/papers/sqroot.pdf, 2001.

[4] Z. Cao, Q. Sha, and X. Fan, *Adleman-Manders-Miller root extraction method revisited*, in Information security and cryptology, 77–85, Lecture Notes in Comput. Sci., **7537**, Springer, Heidelberg, 2012. https://doi.org/10.1007/978-3-642-34704-7_6

[5] G. H. Cho, N. Koo, E. Ha, and S. Kwon,, *New cube root algorithm based on the third order linear recurrence relations in finite fields*, Des. Codes Cryptogr. **75** (2015), no. 3, 483–495. https://doi.org/10.1007/s10623-013-9910-8

[6] M. Cipolla, *Un metodo per la risolutione della congruenza di secondo grado*, Rendiconto dell'Accademia Scienze Fisiche e Matematiche, Napoli, Ser. 3, **9** (1903), 154–163.

[7] I. B. Damgård and G. S. Frandsen, *Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers*, J. Symbolic Comput. **39** (2005), no. 6, 643–652. https://doi.org/10.1016/j.jsc.2004.02.006

[8] K. J. Giuliani and G. Gong, *A new algorithm to compute remote terms in special types of characteristic sequences*, in Sequences and their applications—SETA 2006, 237–247,

Lecture Notes in Comput. Sci., **4086**, Springer, Berlin, 2006. https://doi.org/10.1007/11863854_20
[9] G. Gong and L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2601–2605. https://doi.org/10.1109/18.796413
[10] F. Kong, Z. Cai, J. Yu, and D. Li, *Improved generalized Atkin algorithm for computing square roots in finite fields*, Inform. Process. Lett. **98** (2006), no. 1, 1–5. https://doi.org/10.1016/j.ipl.2005.11.015
[11] D. H. Lehmer, *Computer technology applied to the theory of numbers*, in Studies in Number Theory, 117–151, Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N.J.), 1969.
[12] R. Lidl and H. Niederreiter, *Finite fields*, second edition, Encyclopedia of Mathematics and its Applications, **20**, Cambridge University Press, Cambridge, 1997.
[13] S. Lindhurst, *An analysis of Shanks's algorithm for computing square roots in finite fields*, in Number theory (Ottawa, ON, 1996), 231–242, CRM Proc. Lecture Notes, **19**, Amer. Math. Soc., Providence, RI, 1999.
[14] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of finite fields*, The Kluwer International Series in Engineering and Computer Science, **199**, Kluwer Academic Publishers, Boston, MA, 1993. https://doi.org/10.1007/978-1-4757-2226-0
[15] S. Müller, *On the computation of square roots in finite fields*, Des. Codes Cryptogr. **31** (2004), no. 3, 301–312. https://doi.org/10.1023/B:DESI.0000015890.44831.e2
[16] NIST, *Digital Signature Standard*, Federal Information Processing Standard 186-3, National Institute of Standards and Technology, Available from http://csrc.nist.gov/ publications/fips/, 2000.
[17] D. Shanks, *Five number-theoretic algorithms*, in Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972), 51–70. Congressus Numerantium, VII, Utilitas Math., Winnipeg, MB, 1973.
[18] I. Shparlinski, *Finite fields*: *Theory and computation*, Springer, 1999.
[19] A. Tonelli, *Bemerkung über die Auflösung quadratischer Congruenzen*, Göttinger Nachrichten (1891), 344–346.

Gook Hwa Cho
Institute of Mathematical Sciences
Ewha Womans University
Seoul 03760, Korea
Email address: ghcho@ewha.ac.kr

Namhun Koo
Institute of Mathematical Sciences
Ewha Womans University
Seoul 03760, Korea
Email address: nhkoo@ewha.ac.kr

Soonhak Kwon
Department of Mathematics
Sungkyunkwan University
Suwon 16419, Korea
Email address: shkwon@skku.edu