New Cube Root Algorithm Based on Third Order Linear Recurrence Relation in Finite Field

Gookhwa Jo, Namhum Koo, EunHye Ha, and Soonhak Kwon*

E-mail : shkwon@skku.edu*

Department of Mathematics, Sungkyunkwan University, Suwon, S. Korea

Just a Part of References :

- S. Müller, *On the computation of square roots in finite fields*, Design, Codes and Cryptography, Vol.31, pp. 301-312, 2004
- G. Gong and L. Harn, *Public key cryptosystems based on cubic finite field extensions*, IEEE Trans. Information Theory, Vol.45, pp. 2601-2605, 1999
- N. Nishihara, R. Harasawa, Y. Sueyoshi, and A. Kudo, *A remark on the computation of cube roots in finite fields*, preprint

Root Extraction Algorithms in $\mathbb{F}_q$

Finding r-th root in $\mathbb{F}_q$ has many applications in computational number theory and many other related areas.

Two standard algorithms for computing r-th root in finite field:

1. Tonelli-Shanks square root algorithm
   - Adleman-Manders-Miller r-th root algorithm
2. Cipolla-Lehmer type algorithms
   - Müller square root algorithm
   - Nishihara cube root algorithm

Adleman-Manders-Miller algorithm : straightforward generalization of Tonelli-Shanks square root algorithm

Müller square root algorithm : Cipolla-Lehmer + Lucas Sequence Technique

Nishihara cube root algorithm : Cipolla-Lehmer + Efficient Irreducibility Test for Cubic Polynomial

Complexity of Tonelli-Shanks and Cipolla-Lehmer over $\mathbb{F}_q$ for Cube Root Extraction

Tonelli-Shanks:

best case $O(\log^3 q)$ when $\nu_3(q-1)$ is small
worst case $O(\log^4 q)$ when $\nu_3(q-1)$ is large

where $\nu = \nu_3(q-1)$ means $3^\nu | q-1,\ 3^{\nu+1} \not| q-1$

Cipolla-Lehmer:

average case $O(\log^3 q)$: does not dependent on $\nu = \nu_3(q-1)$

extension field arithmetic $\in \mathbb{F}_{q^3}$ is a bottleneck

Hence, refinement of Cipolla-Lehmer is desirable.

Input:	A cubic residue a in $\mathbb{F}_q$
Output:	A cube root of a
Step 1:	Choose an element b in $\mathbb{F}_q$ at random.
Step 2:	Check $f(x) = x^3 + bx - a$ is irreducible over $\mathbb{F}_q$. If not, go to Step 1.
Step 3:	Return $x^{(q^2+q+1)/3} \pmod{f(x)}$.

Nishihara's method :
Cipolla-Lehmer + Dickson's irreducibility criterion for cubic polynomial

Dickson's irreducibility criterion for $f(x) = x^3 + bx - a$: $f(x)$ is irreducible over $\mathbb{F}_q$ iff the following two conditions are satisfied;

1. $D = -(4b^3 + 27a^2)$ is nonzero quadratic residue in $\mathbb{F}_q$
2. $\frac{1}{2}(a + 3^{-2}\sqrt{-3D})$ is a cubic non-residue in $\mathbb{F}_q$

Müller's square root algorithm with Lucas sequences

Let Q be a quadratic residue in $\mathbb{F}_q$.

Assume

1. $q \equiv 1 \pmod 4$,
2. $f(x) = x^2 - Px + 1$ with $P = Q - 2$ is irreducible.

Letting α, α^{-1} be roots of f, we find a square root of Q as

$$\begin{aligned} Tr(\alpha^{\frac{q-1}{4}}) = s^2_{\frac{q-1}{4}} &= (\alpha^{(q-1)/4} + \alpha^{-(q-1)/4})^2 \\ &= \alpha^{-1}\alpha^{(q+1)/2} + \alpha\alpha^{-(q+1)/2} + 2 \\ &= \alpha^{-1} + \alpha + 2 = P + 2 = Q \end{aligned}$$

The cost of computing $s_{\frac{q-1}{4}}$ is small because it comes from $x^2 - Px + 1$ not from $x^2 - Px + Q$.

Our Contribution : Extended Müller's result for $r = 2$ to the general case - cubic, quintic, $\cdots$. Our method applies to any r-th residue with r prime but the cubic case will be discussed here for simplicity.

The Third Order Linear Recurrence Sequences

Let $f(x) = x^3 - ax^2 + bx - c$, $a, b, c \in \mathbb{F}_q$ be irreducible over $\mathbb{F}_q$.

A third-order linear recurrence sequence $\{s_k\}$ with characteristic polynomial $f(x)$ 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 $f(x)$.

Letting $f(\alpha) = 0$, we denote such $s_k = \alpha^k + \alpha^k q + \alpha^{kq^2}$ as

$$s_k(f) \quad \text{or} \quad s_k(a, b, c) \quad \text{or} \quad s_k(\alpha)$$

The sequence s_k satisfies

1. $s_{2n} = s_n^2 - 2c^n s_{-n}$,
2. $s_{n+m} = s_n s_m - c^m s_{n-m} s_{-m} + c^m s_{n-2m}$

The above computation becomes simple when $c = 1$.

Complexity of Computing s_k for $f(x) = x^3 - ax^3 + bx^2 - 1$

Let $k = \sum_{i=0}^{r} k_i 2^{r-i}$ be a binary representation of k, and let $z_0 = k_0 \neq 0, z_j = k_j + 2z_{j-1},\ j = 1, 2, \cdots, r$.

Then $z_r = k$ and s_k can be computed as

When $k_j = 0$,

1. $s_{z_j - 1} = s_{z_{j-1}} s_{z_{j-1}-1} - b s_{-z_{j-1}} + s_{-(z_{j-1}+1)}$
2. $s_{z_j} = s_{z_{j-1}}^2 - 2 s_{-z_{j-1}}$
3. $s_{z_j + 1} = s_{z_{j-1}} s_{z_{j-1}+1} - a s_{-z_{j-1}} + s_{-(z_{j-1}-1)}$

When $k_j = 1$,

1. $s_{z_j - 1} = s_{z_{j-1}}^2 - 2 s_{-z_{j-1}}$
2. $s_{z_j} = s_{z_{j-1}} s_{z_{j-1}+1} - a s_{-z_{j-1}} + s_{-(z_{j-1}-1)}$
3. $s_{z_j + 1} = s_{z_{j-1}+1}^2 - 2 s_{(-z_{j-1}+1)}$

Thus, the complexity of computing both of s_k and s_{-k} is $9 \log_2 k$ F_q-multiplications on average.

Our method : polynomial choice, $f(\alpha) = 0, \alpha = \beta^3$

Let $f(x) = x^3 - 3x^2 + bx - 1$ be irreducible over $\mathbb{F}_q$ with $f(\alpha) = 0$ and $q \equiv 1 \pmod 3$. The norm of f or the product of all the conjugates of α is

$$\alpha^{1+q+q^2} = 1$$

Classical result of Hilbert Theorem 90 or direct calculation over the finite field extension $\mathbb{F}_{q^3}/\mathbb{F}_q$ says that there exists $\beta \in \mathbb{F}_{q^3}$ such that $\beta^3 = \alpha$. That is, using the property $\alpha^{1+q+q^2} = 1$, one can show that

$$\alpha(1 + \alpha + \alpha^{1+q})^q = 1 + \alpha + \alpha^{1+q}$$

Therefore letting $\beta = (1 + \alpha + \alpha^{1+q})^{\frac{1-q}{3}}$, we get

$$\beta^3 = (1 + \alpha + \alpha^{1+q})^{1-q} = \alpha$$

Our method : properties of α

Let $h(x) = x^3 + (b-3)x - (b-3)$.
Then $h(1-\alpha) = 0$. More precisely, $h(1-x) = -f(x)$.
The irreducibility of f implies the irreducibility of h. Thus

$$(1-\alpha)^{1+q+q^2} = (b-3) \tag{1}$$

On the other hand, from
$0 = h(1-\alpha) = (1-\alpha)^3 + (b-3)(1-\alpha) - (b-3)$, we get

$$(1-\alpha)^3 = (b-3)\alpha \tag{2}$$

By taking $\frac{1+q+q^2}{3}$-th power to both sides of the above expression,

$$(1-\alpha)^{1+q+q^2} = (b-3)^{\frac{1+q+q^2}{3}} \alpha^{\frac{1+q+q^2}{3}} \tag{3}$$

Comparing two expressions (1) and (3), we get

$$\alpha^{\frac{1+q+q^2}{3}} = (b-3)^{-\frac{q^2+q-2}{3}} = (b-3)^{-\frac{(q-1)(q+2)}{3}} = 1 \tag{4}$$

since $q \equiv 1 \pmod 3$ and $b-3 \in \mathbb{F}_q$.

Our method : relation between α and β I

Since $\alpha = \beta^3$, we may rewrite the equation (2) as

$$(1-\alpha)^3 = (b-3)\beta^3 \tag{5}$$

Assume $b - 3 = c^3$ for some c in $\mathbb{F}_q$. Then from $(1-\alpha)^3 = c^3\beta^3$, we get

$$(1-\alpha) = \omega c \beta \tag{6}$$

for some cube root of unity ω in $\mathbb{F}_q$.

Now letting $g(x) = x^3 - a'x^2 + b'x - c'$ $(a', b', c' \in \mathbb{F}_q)$ be the irreducible polynomial of β over $\mathbb{F}_q$,

$$\begin{aligned} \omega c Tr(\beta) &= Tr(\omega c \beta) = Tr(1-\alpha) \\ &= (1-\alpha) + (1-\alpha)^q + (1-\alpha)^{q^2} \\ &= 3 - (\alpha + \alpha^q + \alpha^{q^2}) = 0 \end{aligned} \tag{7}$$

Therefore, assuming $c \neq 0$, we get $a' = Tr(\beta) = 0$. Also we have $1 = \alpha^{\frac{1+q+q^2}{3}} = \beta^{1+q+q^2} = c'$.

Our method : relation between α and β II

Using the following simple identity

$$(A+B+C)^3 = A^3+B^3+C^3+3(A+B+C)(AB+BC+CA)-3ABC$$

with $A = \beta^{1+q}, B = \beta^{q+q^2}, C = \beta^{1+q^2}$, we get

$$(\beta^{1+q} + \beta^{q+q^2} + \beta^{1+q^2})^3 =$$
$$\alpha^{1+q} + \alpha^{q+q^2} + \alpha^{1+q^2} + 3(\beta^{1+q} + \beta^{q+q^2} + \beta^{1+q^2})(\beta + \beta^q + \beta^{q^2}) - 3 \quad (8)$$

which can be expressed as

$$b'^3 = b + 3b'a' - 3 = b - 3 \quad (9)$$

For given irreducible polynomial $f(x) = x^3 - ax^2 + bx - 1$ with $f(\alpha) = 0$, recall the sequence s_k is defined as

$$s_k = s_k(\alpha) = s_k(f) = Tr(\alpha^k) = \alpha^k + \alpha^{qk} + \alpha^{q^2k}.$$

Our method : $s_{\frac{q^2+q-2}{9}}(\alpha) = s_{\frac{q^2+q-2}{3}}(\beta)$

We have

$$\begin{aligned} s_{\frac{q^2+q-2}{3}}(\alpha)^3 &= (\alpha^{\frac{q^2+q-2}{3}} + \alpha^{q\frac{q^2+q-2}{3}} + \alpha^{q^2\frac{q^2+q-2}{3}})^3 \\ &= (\alpha^{-1} + \alpha^{-q} + \alpha^{-q^2})^3 \\ &= (\alpha^{q+q^2} + \alpha^{1+q^2} + \alpha^{1+q})^3 = s_{q+1}(\alpha)^3 = b^3 \end{aligned} \tag{10}$$

Now we are interested in the following two irreducible polynomials

$$f(x) = x^3 - 3x^2 + bx - 1, \quad g(x) = x^3 + b'x - 1$$

with $f(\alpha) = 0, g(\beta) = 0$ and $\alpha = \beta^3$.

Assuming $q \equiv 1 \pmod 9$, we get $q^2 + q - 2 \equiv 0 \pmod 9$ and

$$\begin{aligned} s_{\frac{q^2+q-2}{9}}(\alpha) &= Tr(\alpha^{\frac{q^2+q-2}{9}}) = Tr((\beta^3)^{\frac{q^2+q-2}{9}}) \\ &= Tr(\beta^{\frac{q^2+q-2}{3}}) = s_{\frac{q^2+q-2}{3}}(\beta) \end{aligned} \tag{11}$$

Therefore from the equation (10) and (9),

$$s_{\frac{q^2+q-2}{9}}(\alpha)^3 = s_{\frac{q^2+q-2}{3}}(\beta)^3 = s_{q+1}(\beta)^3 = b'^3 = b - 3 \qquad (12)$$

Now using the polynomial $f(x) = x^3 - 3x^2 + bx - 1$, we can find a cube root for given cubic residue Q in $\mathbb{F}_q$ as follows;
For given cubic residue $Q \in \mathbb{F}_q$, define $b = Q + 3$. If $f(x)$ with given coefficient b is irreducible, then $s_{\frac{q^2+q-2}{9}}(f)$ is a cube root of Q. That is,

$$s_{\frac{q^2+q-2}{9}}(f)^3 = b - 3 = Q.$$

If the given f is not irreducible over $\mathbb{F}_q$, then we twist Q by random $t \in \mathbb{F}_q$ until we get irreducible f with $b = Qt^3 + 3$. Then

$$s_{\frac{q^2+q-2}{9}}(f)^3 = b - 3 = Qt^3,$$

which implies $t^{-1}s_{\frac{q^2+q-2}{9}}(f)$ is a cube root of Q.

New Cube Root Algorithm for $\mathbb{F}_q$ with $q \equiv 1 \pmod 9$

Input: cubic residue $Q \neq 0 \in \mathbb{F}_q$, Output: s satisfying $s^3 = Q$

1. $b \leftarrow Q + 3, \quad f(x) \leftarrow x^3 - 3x^2 + bx - 1$
2. While $f(x)$ is reducible over $\mathbb{F}_q$
   choose random $t \in \mathbb{F}_q$
   $b \leftarrow Qt^3 + 3, \; f(x) \leftarrow x^3 - 3x^2 + bx - 1$
   End While
3. $s \leftarrow s_{\frac{q^2+q-2}{9}}(f) \cdot t^{-1}$

The output s is indeed a cube root of Q because
$s^3 = s_{\frac{q^2+q-2}{9}}(f)^3 \cdot t^{-3} = Qt^3 \cdot t^{-3} = Q$.

When $q \not\equiv 1 \pmod 9$ **: 1.** If $q \equiv 2 \pmod 3$, a cube root of Q is given as $Q^{\frac{2q-1}{3}}$. **2.** If $q \equiv 4 \pmod 9$, a cube root of cubic residue Q is given by $Q^{\frac{2q+1}{9}}$. **3.** If $q \equiv 7 \pmod 9$, a cube root of cubic residue Q is given by $Q^{\frac{q+2}{9}}$.

Complexity Estimation

Randomly selected monic polynomial over $\mathbb{F}_q$ of degree 3 with nonzero constant term is irreducible with probability $\frac{1}{3}$. Even if our choice of f is not really random, experimental evidence implies that one third of such f is irreducible.

Computing $s_{\frac{q^2+q-2}{9}}$: $9\log_2 \frac{q^2+q-2}{9} \approx 18\log_2 q$ $\mathbb{F}_q$-multiplications.

Irreducibility testing : Using Dickson's formula, $4\log_2 q$ $\mathbb{F}_q$-multiplications at most.

Total cost : $4 \cdot 3 + 18 = 30\log_2 q$ multiplications in $\mathbb{F}_q$

Speed up can be achieved if better irreducibility testing is used.

The complexity of Adleman-Manders-Miller cube root algorithm costs $O(\log_2 q + t^2)$ multiplications in $\mathbb{F}_q$ with $3^t || q-1$.

Conclusion

- We proposed a new Cube Root Algorithm using linear recurrence relation arising from a cubic polynomial with constant term -1.
- The related linear recurrence is easy to compute and has low computational complexity.
- Complexity estimation shows that proposed algorithm is better than Adleman-Manders-Miller when t is sufficiently large, but the implementation is needed to verify which t is a threshold value.
- Our idea can be generalized to the case of r-th root extraction : We obtained a closed formula for r-th root for any odd prime r.
- Bottleneck of our approach is the irreducibility testing of a polynomial f of degree r : efficient irreducibility testing is needed.