J. Korean Math. Soc. **52** (2015), No. 1, pp. 209–224
http://dx.doi.org/10.4134/JKMS.2015.52.1.209

POLYNOMIAL REPRESENTATIONS FOR n-TH ROOTS IN FINITE FIELDS

Seunghwan Chang, Bihtnara Kim, and Hyang-Sook Lee

Abstract. Computing square, cube and n-th roots in general, in finite fields, are important computational problems with significant applications to cryptography. One interesting approach to computational problems is by using polynomial representations. Agou, Deléglise and Nicolas proved results concerning the lower bounds for the length of polynomials representing square roots modulo a prime p. We generalize the results by considering n-th roots over finite fields for arbitrary $n > 2$.

1. Introduction

The problems of computing square roots and cube roots modulo a prime[1] are important computational problems and have significant applications to cryptography. In general, computation of n-th roots in finite fields appears in various aspects of cryptography.

There are efficient probabilistic algorithms for computing square roots modulo a prime, notably the algorithms due to Tonelli-Shanks [21, 20] and to Cipolla-Lehmer [4, 11]. Due to Schoof [19], there is a deterministic algorithm for square roots modulo a prime, which uses elliptic curves in an essential way. The algorithms of Tonelli-Shanks and Cipolla-Lehmer can be generalized to computing cube roots and more generally to computing n-th roots, but the efficiency of the algorithms is guaranteed only in certain cases. Computing n-th roots in a finite field can be carried out applying an algorithm due to Adleman, Manders and Miller [1], which extends the square root algorithm of Tonelli-Shanks. Recently, Barreto and Voloch [3] gave an efficient algorithm

Received May 30, 2014; Revised September 23, 2014.

2010 *Mathematics Subject Classification.* Primary 12E20, 68W40.

Key words and phrases. cube roots, n-th roots, finite fields.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (Grant Number: 2012R1A2A1A03006706).

[1] The hardness of computing square roots modulo a composite integer $N = pq$ with unknown factorization, for instance, is known to be computationally equivalent to that of integer factorization.

for n-th roots that can be applied to a large family of finite fields, which uses an idea of "inverting exponents."

One of the approaches to computational problems is to find polynomial functions that, for given instances, output solutions to the problems. Let us call this *polynomial representation* approach. This approach applied to the discrete logarithm problems for finite fields and elliptic curves have been investigated for example in [5, 8, 9, 10, 13, 14, 22, 23]. Recently, Satoh [15, 16, 17, 18] investigated the approach for the pairing inversion problem, which concerns bilinear pairings defined on elliptic curves over finite fields.

An interesting feature of polynomial representation approach is that once one obtains a polynomial representing a solution for a given computational problem and the number of non-zero coefficients of the polynomial is sufficiently small, one may get an efficient algorithm, by evaluating, for solving the problem.

In [2], Agou, Deléglise and Nicolas investigated polynomial representations in the case of square roots modulo a prime p. After they parametrize polynomials representing square roots modulo p, they investigated the *length*[2], i.e., the number of nonzero coefficients, of the representing polynomials. They prove that if $p-1 \equiv 2r \pmod{4r}$, then there exist at least 2^r polynomials $P(X) \in \mathbb{F}_p[X]$ which represents square roots in $\mathbb{F}_p^\times$ with $\deg P(X) < \frac{p-1}{2}$ and whose length is less than or equal to r. It is easy to see that if e is the largest positive integer such that $2^e \mid p-1$, then $p-1 \equiv 2 \cdot 2^{e-1} \pmod{2^2 \cdot 2^{e-1}}$ and in fact $r = 2^{e-1}$ is the smallest positive integer satisfying the congruence. They also prove that for all but finitely many primes p, 2^{e-1} gives the lower bound for the length of polynomials representing square roots. They suggest that "it would be possible to study, in the same way, cubic roots and more generally, n-th roots, for $n > 2$."

In this article, we initiate the investigation of polynomial representations in the general situation of n-th roots in finite fields. We generalize and extend the results of Agou, Deléglise and Nicolas [2] to the case of cube roots and the general case of n-th roots (for arbitrary n) in finite fields.

The rest of the article is organized as follows. In Section 2, we define what we mean by a polynomial representing n-th roots in $\mathbb{F}_q^\times$ and give a parametrization of the representing polynomials. In Section 3, we give a partial answer to the question of how small the length of a representing polynomial can be. Specifically, we prove a sufficient condition for existence of short representing polynomials, and apply it to the situation of cube roots to get representing polynomials of certain specific length, which turns out to be the minimum length in most cases. Finally, we investigate the lower bounds for the length of representing polynomials in Section 4. We prove that beside finitely many primes q every polynomial which represents n-th roots in $\mathbb{F}_q^\times$ has length at least n^{e-1}, where e is the largest positive integer such that $n^e \mid q-1$.

[2] In certain contexts, it is also called the *Hamming weight* of the polynomial.

Acknowledgements. The authors would like to thank the anonymous referee for valuable comments and suggestions, which improved the exposition of the article.

2. Polynomials representing n-th roots

The approach of Agou, Deléglise and Nicolas to computing square roots modulo a prime via polynomial representations can be generalized to n-th roots in a finite field for arbitrary $n \geq 2$. In this section, we give a definition of a polynomial representing n-th roots in a finite field and prove basic properties of those representing polynomials.

Before we begin, we give a summary of notations and assumptions that will be used throughout the article.

Notations:

- q is a power of a prime;
- $\mathbb{F}_q$ is a field with q elements;
- n is a positive integer;
- $e := v_n(q-1)$ is the largest non-negative integer such that $n^e \mid q-1$;
- $\operatorname{len} f(X)$ is the number of nonzero coefficients of a polynomial $f(X)$.

Assumptions:

- $n > 2$; (see [2] for the case $n = 2$)
- $n \mid q-1$. (see the paragraph right after Remark 2.4)

A basic tool for representing functions on finite fields as polynomials is the following classical result due to Lagrange.

Theorem 2.1 (Lagrange interpolation formula)**.** *Let $x_0, \ldots, x_{k-1} \in \mathbb{F}_q$ be k distinct elements. Let $y_0, \ldots, y_{k-1} \in \mathbb{F}_q$ be k (not necessarily distinct) elements. Then there exists unique $P(X) \in \mathbb{F}_q[X]$ with $\deg P(X) < k$ such that $P(x_i) = y_i$ for all $i \in \{0, \ldots, k-1\}$. An explicit formula for $P(X)$ is given by*

$$P(X) = \sum_{i=0}^{k-1} y_i \prod_{j=0, j\neq i}^{k-1} \frac{X - x_j}{x_i - x_j}.$$

The object that we are primarily interested in is the polynomial in $\mathbb{F}_q[X]$ which, considered as a function $P : \mathbb{F}_q \to \mathbb{F}_q$, outputs one of the n-th roots of the given input. Following [2], we formalize the notion as follows.

Definition 2.2. Let $S \subset \mathbb{F}_q^\times$ be a subset. We say that a polynomial $P(X) \in \mathbb{F}_q[X]$ *represents n-th roots in S* if

$$P(x^n)^n = x^n$$

for all $x \in S$.

Example 2.3. The n-th power map $(\cdot)^n : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $x \mapsto x^n$ is a group homomorphism with kernel $\ker(\cdot)^n = \mu_{\gcd(n,q-1)}$. Suppose that $\gcd(n, q-1) = 1$. Then $\ker(\cdot)^n = \mu_{\gcd(n,q-1)} = 1$, and so the map $(\cdot)^n$ is an isomorphism. Thus, for every $t \in \mathbb{F}_q^\times$, there exists unique n-th root of t. Note that there exist $a, b \in \mathbb{Z}$ such that $an + b(q-1) = 1$, and one can efficiently compute such a and b using the extended Euclidean algorithm. Given $t \in \mathbb{F}_q^\times$, one can compute the unique n-th root of t by computing t^a, namely, $(t^a)^n = t^{an}t^{b(q-1)} = t^{an+b(q-1)} = t$. As a result, the monomial $P(X) = X^a$ represents n-th roots in $\mathbb{F}_q^\times$ where $a \in \mathbb{Z}_{>0}$ is such that $an + b(q-1) = 1$ for some $b \in \mathbb{Z}$. Indeed, given $t = x^n$ with $x \in \mathbb{F}_q^\times$, we have $P(t)^n = P(x^n)^n = (x^{an})^n = (x^{an}x^{b(q-1)})^n = x^n$.

Remark 2.4. Suppose that $P(X) \in \mathbb{F}_q[X]$ represents n-th roots in $\mathbb{F}_q^\times$. Then it is straightforward to check that $\alpha P(X)$ with $\alpha \in \mathbb{F}_q^\times$ represents n-th roots if and only if $\alpha \in \mu_n$.

For our purpose, we may narrow our focus to the situation that $n \mid q-1$, based on the following observation. Assume that $1 < n_0 := \gcd(n, q-1) < q-1$. We can write $n = n_0 n_1$ where $n_1 := n/n_0$. Note that $n_0 \mid q-1$ and $\gcd(n_1, q-1) = 1$. If $P(X)$ is a polynomial representing n_0-th roots in $\mathbb{F}_q^\times$, then the polynomial $P(X^a) = P(X) \circ X^a$, of the same length as $P(X)$, represents n-th roots in $\mathbb{F}_q^\times$, where X^a is a monomial that represents n_1-th roots in $\mathbb{F}_q^\times$ (cf. Example 2.3).

We are mainly interested in the case where $S = \mathbb{F}_q^\times$, but other subgroups of $\mathbb{F}_q^\times$ will be considered in proving our assertions; see Theorem 3.2. If K is a field and m is a positive integer not divisible by the characteristic char(K) of K, let us denote $\mu_m(K) := \{x \in \overline{K} : x^m = 1\}$. We will simply write μ_m for $\mu_m(\mathbb{F}_q)$ when $K = \mathbb{F}_q$.

If S is a subgroup of $\mathbb{F}_q^\times$, then $S = \mu_d$ for some positive divisor d of $q-1$. If ζ is a primitive root of $\mathbb{F}_q$, then $S = \mu_d = \{\zeta^{\frac{q-1}{d}i} \mid 0 \le i \le d-1\}$. If $n \mid d$ (recall that we assume $n \mid q-1$), then

$$S^n = \mu_d^n = \mu_{\frac{d}{n}} = \{\zeta^{\frac{(q-1)n}{d}i} \mid 1 \le i \le \tfrac{d}{n}\}.$$

Lemma 2.5. *Let $S = \mu_d \subset \mathbb{F}_q^\times$ where $n \mid d$. Let ζ be a primitive root of $\mathbb{F}_q$. The following are equivalent.*

(1) *$P(X)$ represents n-th roots in S;*
(2) *$P(t)^n = t$ for all $t \in S^n$;*
(3) *$P(\zeta^{\frac{(q-1)}{d}ni})^n = \zeta^{\frac{(q-1)}{d}ni}$ for all $i \in \{1, \dots, \frac{d}{n}\}$;*
(4) *$P(\zeta^{\frac{(q-1)}{d}ni})^n = \zeta^{\frac{(q-1)}{d}ni}$ for all $i \in \{0, \dots, \frac{d}{n}-1\}$.*

In particular, $P(X)$ represents n-th roots in $\mathbb{F}_q^\times (= \mu_{q-1})$ if and only if $P(\zeta^{ni})^n = \zeta^{ni}$ for all $i \in \{1, \dots, \frac{q-1}{n}\}$.

Proof. The equivalence between (1) and (2) is clear. We show that (2) and (3) are equivalent. As $n \mid d$, we have $S^n = \mu_{\frac{d}{n}}$. Clearly, (2) implies (3). Note that $\zeta^{\frac{q-1}{d}n}$ generates $S^n = \mu_{\frac{d}{n}}$. Thus, to verify that $P(t)^n = t$ for all $t \in S^n$, it suffices to check that $P((\zeta^{\frac{(q-1)}{d}i})^n)^n = (\zeta^{\frac{(q-1)}{d}i})^n$ for all $i \in \{1, \dots, \frac{d}{n}\}$. Note that (3) and (4) are equivalent as $\zeta^{\frac{q-1}{d}n\cdot 0} = 1 = \zeta^{\frac{q-1}{d}n\cdot\frac{d}{n}}$. □

Note that the notion of polynomial representing n-th roots does not depend on the choice of ζ. We fix a primitive root ζ of $\mathbb{F}_q$ once and for all for the rest of the article.

If $P(X)$ represents n-th roots in S, then for each $x^n \in S^n$, $P(x^n)$ is one of the n-th roots of x^n; $P(x^n)$ is not necessarily x. Since $(P(x^n)/x)^n = P(x^n)^n/x^n = 1$, one has $P(x^n)/x \in \mu_n$. If we set $\sigma_x := P(x^n)/x \in \mu_n$, we have $P(x^n) = \sigma_x x$. Thus, we are motivated to introduce the following.

Definition 2.6. Let K be a field with $\mathrm{char}(K) \nmid n$. We define

$$\Sigma_{q-1}(K) = \{\sigma = (\sigma_0, \ldots, \sigma_{\frac{q-1}{n}-1}) \mid \sigma_j \in \mu_n(K) \text{ for all } j = 0, \ldots, \tfrac{q-1}{n} - 1\}.$$

In general, one can analogously define

$$\Sigma_d(K) = \{\sigma = (\sigma_0, \ldots, \sigma_{\frac{d}{n}-1}) \mid \sigma_j \in \mu_n(K) \text{ for all } j = 0, \ldots, \tfrac{d}{n} - 1\}$$

if $d \mid q-1$. When $K = \mathbb{F}_q$ we simply write Σ_d for $\Sigma_d(\mathbb{F}_q)$. Note that $\#\Sigma_d = n^{\frac{d}{n}}$.

By applying Theorem 2.1, we parametrize, in terms of Σ_{q-1}, polynomials representing n-th roots in $\mathbb{F}_q^\times$.

Theorem 2.7. *We have the following.*

(1) *For each $\sigma \in \Sigma_{q-1}$, there exists unique $P_\sigma(X) \in \mathbb{F}_q[X]$ of degree $< \frac{q-1}{n}$ such that*

$$P_\sigma(\zeta^{ni}) = \sigma_i \zeta^i$$

for all $i \in \{0, \ldots, \frac{q-1}{n} - 1\}$. Moreover, if $P_\sigma(X) = \sum_{k=0}^{\frac{q-1}{n}-1} c_k X^k$, then the c_k is explicitly given by

$$c_k = -n \sum_{i=0}^{\frac{q-1}{n}-1} \sigma_i \zeta^{i(1-nk)}.$$

(2) *If $P(X) \in \mathbb{F}_q[X]$ represents n-th roots in $\mathbb{F}_q^\times$ and $\deg P(X) < \frac{q-1}{n}$, then $P(X) = P_\sigma(X)$ for some $\sigma \in \Sigma_{q-1}$.*

(3) *A polynomial $P(X) \in \mathbb{F}_q[X]$ represents n-th roots in $\mathbb{F}_q^\times$ if and only if $P(X) = P_\sigma(X) + (X^{\frac{q-1}{n}} - 1)H(X)$ for some $\sigma \in \Sigma_{q-1}$ and some $H(X) \in \mathbb{F}_q[X]$.*

Proof. (1) The first claim is immediate from the Lagrange interpolation formula (Theorem 2.1). To prove the second claim, it suffices to check that $P_\sigma(X)$ defined by the formula satisfies the conditions of the first claim. Indeed, if we set $P(X) = \sum_{k=0}^{\frac{q-1}{n}-1} c_k X^k$ with $c_k = -n \sum_{i=0}^{\frac{q-1}{n}-1} \sigma_i \zeta^{i(1-nk)}$, then for all $i \in \{0, \ldots, \frac{q-1}{n} - 1\}$ we have

$$P(\zeta^{ni}) = -n \sum_{k=0}^{\frac{q-1}{n}-1} \sum_{j=0}^{\frac{q-1}{n}-1} \sigma_j \zeta^{j(1-nk)} (\zeta^{ni})^k$$

$$
\begin{aligned}
&= -n\sum_{j=0}^{\frac{q-1}{n}-1}\sigma_j\zeta^j\sum_{k=0}^{\frac{q-1}{n}-1}\zeta^{(i-j)nk}\\
&= -n\sum_{j=0,\,j\neq i}^{\frac{q-1}{n}-1}\sigma_j\zeta^j\cdot\frac{1-\zeta^{(i-j)(q-1)}}{1-\zeta^{(i-j)n}}-n\sigma_i\zeta^i\cdot\frac{q-1}{n}\\
&= -n\sigma_i\zeta^i\cdot\frac{q-1}{n}\\
&= \sigma_i\zeta^i.
\end{aligned}
$$

Thus, $P(X) = P_\sigma(X)$ by the uniqueness assertion of Theorem 2.1.

(2) Suppose that $P(X)$ represents n-th roots in $\mathbb{F}_q^\times$ and $\deg P(X) < \frac{q-1}{n}$. Let $\sigma_i = P(\zeta^{ni})/\zeta^i \in \mu_n$ for each $i \in \{0,\ldots,\frac{q-1}{n}-1\}$ and $\sigma = (\sigma_0,\ldots,\sigma_{\frac{q-1}{n}-1}) \in \Sigma_{q-1}$. We claim that $P(X) = P_\sigma(X)$. Note that for all $i \in \{0,\ldots,\frac{q-1}{n}-1\}$, we have $P(\zeta^{ni}) = \sigma_i\zeta^i = P_\sigma(\zeta^{ni})$. Thus, $P(X) = P_\sigma(X)$ by the uniqueness assertion of Theorem 2.1.

(3) If $P(X) \in \mathbb{F}_q[X]$ represents n-th roots in $\mathbb{F}_q^\times$, write $P(X) = R(X) + (X^{\frac{q-1}{n}} - 1)H(X)$ where $R(X), H(X) \in \mathbb{F}_q[X]$ and $\deg R(X) < \frac{q-1}{n}$. It is straightforward to check that $R(X)$ represents n-th roots in $\mathbb{F}_q^\times$. As $\deg R(X) < \frac{q-1}{n}$, $R(X) = P_\sigma(X)$ for some $\sigma \in \Sigma_{q-1}$. The converse is straightforward. □

We will simply say *representing polynomials* meaning "polynomials representing n-th roots in $\mathbb{F}_q^\times$" whenever there seems no confusion.

3. Short representing polynomials

In the previous section, we identified the polynomials that represent n-th roots in $\mathbb{F}_q^\times$. In this section and the next, we are interested in the length of the polynomial that represents n-th roots in $\mathbb{F}_q^\times$.

In the current section, we want to "locate" some representing polynomials that are "short," having relatively small number of nonzero coefficients. As a main theorem (Theorem 3.2 below) of this section we will prove a sufficient condition for the existence of representing polynomials that are short. This generalizes in a natural way Theorem 2 of [2], which applies to all odd primes q to produce polynomials representing square roots in $\mathbb{F}_q^\times$ of length $\le 2^e$ where e is the largest positive integer such that $2^e \mid q-1$; see Theorem 3 of [2].

Before getting into main results of this section, we take a look at a simple lemma concerning the length of polynomials, which had been proven in [2]. Recall that we denote the length of a polynomial $P(X)$ by $\operatorname{len} P(X)$.

Lemma 3.1 (Lemma 1 of [2]). *Let K be a field and let $m \in \mathbb{Z}_{>0}$. For every polynomial $P(X) \in K[X]$ we have $\operatorname{len} R(X) \le \operatorname{len} P(X)$ where $R(X)$ is the remainder in the Euclidean division of $P(X)$ by $X^m - 1$.*

Proof. Note that the remainder in the division of the monomial X^k by $X^m - 1$ is $X^{\overline{k}}$ where $\overline{k}$ is the remainder in the division of k by m. Thus, if $P(X) = \sum a_i X^i$, then $R(X) = \sum a_i X^{\overline{i}}$. Clearly we have $\operatorname{len} R(X) \leq \operatorname{len} P(X)$. □

We are ready to prove a theorem, which asserts that a certain congruence guarantees existence of representing polynomials with lengths bounded above by a certain positive integer that is involved in the congruence.

Theorem 3.2. *Let $r \in \mathbb{Z}_{>0}$ be such that $q \equiv 1 - \delta nr \pmod{\delta n^2 r}$ for some $\delta \in \{1, \ldots, n-1\}$ with $\gcd(\delta, n) = 1$. Then there exist at least n^{r/r_0} polynomials $P(X) \in \mathbb{F}_q[X]$ representing n-th roots in $\mathbb{F}_q^\times$ such that $\deg P(X) < \frac{q-1}{n}$ and $\operatorname{len} P(X) \leq r$, where r_0 is the product, counting multiplicities, of all primes dividing r but not dividing n. In particular, if every prime divisor of r divides n, then there exist at least n^r polynomials $P(X) \in \mathbb{F}_q[X]$ representing n-th roots in $\mathbb{F}_q^\times$ such that $\deg P(X) < \frac{q-1}{n}$ and $\operatorname{len} P(X) \leq r$.*

Proof. First we prove the theorem under the assumption that every prime divisor of r divides n. Write $q - 1 = -\delta nr + \delta n^2 rk$ with $k \in \mathbb{Z}_{>0}$. Since $\gcd(\delta, n) = 1$, there exists $\gamma \in \{1, \ldots, n-1\}$ such that $\gamma\delta \equiv 1 \pmod{n}$. Write $\gamma\delta = 1 + nl$ with $l \in \mathbb{Z}_{>0}$. Then $\gamma(q-1) = \gamma(-\delta nr + \delta n^2 rk) = -(1+nl)nr + \gamma\delta n^2 rk = -nr + n^2 r(-l + \gamma\delta k)$. Thus, $\gamma(q-1) \equiv -nr \pmod{n^2 r}$, so that $\frac{\gamma(q-1)+nr}{n^2 r} \in \mathbb{Z}_{>0}$.

Note that $\mu_{nr} \subset \mathbb{F}_q^\times$ since $nr \mid q-1$. Let

$$\mathcal{Q} = \{Q(X) \in \mathbb{F}_q[X] \mid Q(x^n)^n = \frac{1}{x^n} \; \forall x \in \mu_{nr}, \; \deg Q(X) < r\}.$$

Namely, elements of $\mathcal{Q}$ are precisely the polynomials of degree $< r$ that "represent the reciprocals of n-th roots in μ_{nr}." The cardinality of $\mathcal{Q}$ is n^r by a similar argument as in the proof of Theorem 2.7. For each $Q(X) \in \mathcal{Q}$, we will be able to construct $P(X)$ satisfying the desired properties in the theorem.

Given $Q(X) \in \mathcal{Q}$, we define a polynomial

$$S(X) = X^{\frac{\gamma(q-1)+nr}{n^2 r}} Q\left(X^{\frac{\gamma(q-1)}{nr}}\right) \in \mathbb{F}_q[X],$$

noting that $\frac{\gamma(q-1)+nr}{n^2 r}, \frac{\gamma(q-1)}{nr} \in \mathbb{Z}_{\geq 0}$. First, we observe that $S(X)$ represents n-th roots in $\mathbb{F}_q^\times$:

$$S(x^n)^n = \left(x^{\frac{\gamma(q-1)+nr}{nr}}\right)^n Q\left(\left(x^{\frac{\gamma(q-1)}{nr}}\right)^n\right)^n = x^{\frac{\gamma(q-1)+nr}{r}} \left(x^{\frac{\gamma(q-1)}{nr}}\right)^{-n} = x^n$$

for all $x \in \mathbb{F}_q^\times$, since $(\mathbb{F}_q^\times)^{\frac{\gamma(q-1)}{nr}} \subset \mu_{nr}$. Next, we have $\operatorname{len} S(X) = \operatorname{len} Q(X) \leq \deg Q(X) + 1 \leq r$ since $\deg Q(X) < r$. Lastly, we look at the degree of $S(X)$: $\deg S(X) \leq \frac{\gamma(q-1)+nr}{n^2 r} + (r-1)\frac{\gamma(q-1)}{nr} = \frac{\gamma(q-1)}{n} + \frac{nr+(1-n)\gamma(q-1)}{n^2 r} < \frac{\gamma(q-1)}{n}$ since $nr + (1-n)\gamma(q-1) = nr(1 + (1-n)(nk-1)\gamma\delta) < 0$.

Now we define $P(X)$ to be the remainder in the Euclidean division of $S(X)$ by $X^{\frac{q-1}{n}} - 1$. By the assertion (3) of Theorem 2.7, $P(X)$ represents n-th roots in $\mathbb{F}_q^\times$. By Lemma 3.1, $\operatorname{len} P(X) \le \operatorname{len} S(X) \le r$. Clearly, $\deg P(X) < \frac{q-1}{n}$. In fact, $P(X) = S(X)$ if and only if $\deg S(X) < \frac{q-1}{n}$.

What remains to be seen is that the association $Q(X) \mapsto P(X)$ is one-to-one. Suppose that $Q_1(X), Q_2(X) \in \mathcal{Q}$ with $Q_1(X) \ne Q_2(X)$ and that $P_1(X), P_2(X)$ are the resulting polynomials of the association, respectively. We are going to show that $P_1(X) \ne P_2(X)$. There exist $T_1(X), T_2(X) \in \mathbb{F}_q[X]$ such that

$$X^{\frac{\gamma(q-1)+nr}{n^2r}} Q_i\left(X^{\frac{\gamma(q-1)}{nr}}\right) = (X^{\frac{q-1}{n}} - 1)T_i(X) + P_i(X)$$

for $i \in \{1, 2\}$. As $\gcd(\gamma, n) = 1$, we have $\gcd(\gamma, r) = 1$ (by the assumption in the beginning of the proof) and the map $x \mapsto x^\gamma$ defines an automorphism on μ_r. In particular, we have

$$\mu_r = \{\zeta^{\frac{\gamma(q-1)}{r}}, \zeta^{\frac{2\gamma(q-1)}{r}}, \ldots, \zeta^{\frac{r\gamma(q-1)}{r}}\}.$$

(Recall that ζ is the fixed primitive root of $\mathbb{F}_q$.) Since $Q_1(X), Q_2(X) \in \mathcal{Q}$ and $Q_1(X) \ne Q_2(X)$, the polynomials $Q_1(X)$ and $Q_2(X)$ define distinct functions on $\mu_{nr}^n = \mu_r$, i.e., there exists $j \in \{1, \ldots, r\}$ such that $Q_1(\zeta^{\frac{j\gamma(q-1)}{r}}) \ne Q_2(\zeta^{\frac{j\gamma(q-1)}{r}})$. Let $x \in \mathbb{F}_q^\times$ be such that $x^{\frac{\gamma(q-1)}{r}} = \zeta^{\frac{j\gamma(q-1)}{r}}$; one can take $x = \zeta^j$ for instance. Then $P_i(x^n) = x^{\frac{\gamma(q-1)+nr}{nr}} Q_i(\zeta^{\frac{j\gamma(q-1)}{r}})$. We have $P_1(x^n) \ne P_2(x^n)$ since $Q_1(\zeta^{\frac{j\gamma(q-1)}{r}}) \ne Q_2(\zeta^{\frac{j\gamma(q-1)}{r}})$. Thus, $P_1(X) \ne P_2(X)$.

Now we turn to the case that some prime divisor of r does not divide n. Let r_0 be the product, counting multiplicities, of all primes s such that $s \mid r$ and $s \nmid n$. Then $\delta_1 := \delta r_0$, $r_1 := r/r_0$ satisfy the congruence $q \equiv 1 - \delta_1 n r_1 \pmod{\delta_1 n^2 r_1}$. Now every prime divisor of r_1 divides n. By what we have proven already there exist at least n^{r_1} polynomials $P(X) \in \mathbb{F}_q[X]$ representing n-th roots in $\mathbb{F}_q^\times$ such that $\deg P(X) < \frac{q-1}{n}$, $\operatorname{len} P(X) \le r_1 < r$, and we are done. □

Theorem 3.3. *Assume that $n = 3$ and that q is odd. Then $q - 1 \equiv \delta \cdot 3^e \pmod{\delta \cdot 3^{e+1}}$ for unique $\delta \in \{1, 2\}$. As a consequence, there exist at least $3^{3^{e-1}}$ polynomials $P(X) \in \mathbb{F}_q[X]$ that represent cube roots in $\mathbb{F}_q^\times$ and $\operatorname{len} P(X) \le 3^{e-1}$.*

Proof. As $e = v_3(q - 1)$, there exists unique $\delta \in \{1, 2\}$ such that $q - 1 \equiv \delta \cdot 3^e \pmod{3^{e+1}}$. Write $q - 1 = \delta \cdot 3^e + 3^{e+1}k$ with $k \in \mathbb{Z}_{\ge 0}$. If $\delta = 1$, we are done. If $\delta = 2$, then k is even since both $\delta \cdot 3^e$ and $q - 1$ are even. Thus, $q - 1 = \delta \cdot 3^e + \delta \cdot 3^{e+1}k'$ where $k' = k/2 \in \mathbb{Z}_{\ge 0}$. □

By Theorem 3.3, the minimum length of representing polynomials for cube roots is bounded above by 3^{e-1}; also note that, by Theorem 3 of [2], the minimum length of representing polynomials for square roots is bounded by 2^{e-1}. It will be interesting to see if this phenomena persists for arbitrary n. In Theorem 4.1 of Section 4, we will prove that for all but finitely many primes q such that $v_n(q - 1) = e$, the length of representing polynomials is bounded below by n^{e-1}.

Now we investigate the relationship between existence of monomials and binomials that represent n-th roots in $\mathbb{F}_q^\times$ and $e = v_n(q-1)$, starting with an example.

Example 3.4. Let $q = 13$, $n = 3$ and $r = 1$. Then $q = 1 - 2nr + 2n^2r$, i.e., $\delta = 2$ in the congruence of Theorem 3.2; $e = 1$. Note that $\mu_3 = \{1, 3, 9\}$. There are precisely 3 polynomials that represent cube roots in $\mathbb{F}_q^\times$, i.e., $P_1(X) = X^3, P(X) = 3X^3, P(X) = 9X^3$. For instance, $P_1(\zeta^{3i})^3 = ((\zeta^{3i})^3)^3 = \zeta^{3i}$ as $\zeta^{24i} = 1$ by Fermat's theorem.

As a matter of fact, one can prove a criterion for the existence of representing monomials.

Proposition 3.5. *There exists a monomial $P(X) = aX^i \in \mathbb{F}_q[X]$ that represents n-th roots in $\mathbb{F}_q^\times$ if and only if $q - 1 \equiv \delta n \pmod{n^2}$ for some $\delta \in \{1, \dots, n-1\}$ with $\gcd(\delta, n) = 1$. In particular, if n is a prime, then there exists a monomial representing n-th roots in $\mathbb{F}_q^\times$ if and only if $e := v_n(q-1) = 1$.*

Proof. ($\Rightarrow$) Suppose that $P(X) = aX^i$ represents n-th roots in $\mathbb{F}_q^\times$. We may assume that $i > 0$. We have $1 = P(1)^n = a^n$, so that $a \in \mu_n$. We have $\zeta^n = P(\zeta^n)^n = a^n(\zeta^{ni})^n = \zeta^{n^2 i}$, which implies that $\zeta^{n(ni-1)} = 1$. Since ζ generates $\mathbb{F}_q^\times$, we have $n^e \mid q-1 \mid n(ni-1)$, and so $n^{e-1} \mid ni-1$. Thus, $e = 1$. Now, we write $q - 1 = \delta n + kn^2$ where $\delta \in \{1, \dots, n-1\}$, $k \in \mathbb{Z}_{>0}$, and show that $\gcd(n, \delta) = 1$. Again as $\zeta^{n(ni-1)} = 1$, the exponent $n(ni-1)$ must be divisible by $q - 1 = \delta n + kn^2$. Then $\delta + kn \mid ni - 1$. Hence $\gcd(n, \delta) = 1$.

($\Leftarrow$) Let $C = \frac{q-1}{n}\gamma \in \mathbb{Z}_{>0}$, where $\gamma \in \mathbb{Z}_{>0}$ is such that $\gamma\delta \equiv -1 \pmod{n^2}$. Note that

$$\frac{C+1}{n} = \frac{1}{n}\left(\frac{q-1}{n}\gamma + 1\right) = \frac{(q-1)\gamma + n}{n^2} \in \mathbb{Z}_{>0}$$

since $(q-1)\gamma + n \equiv (q-1)\gamma - \gamma\delta n \equiv \gamma(q - 1 - \delta n) \equiv 0 \pmod{n^2}$. We claim that $P(X) = X^{\frac{C+1}{n}}$ represents n-th roots in $\mathbb{F}_q^\times$. Indeed, we have $P(x^n)^n = ((x^n)^{\frac{C+1}{n}})^n = (x^n)^C x^n = x^{(q-1)\gamma} x^n = x^n$ for all $x \in \mathbb{F}_q^\times$. □

Note that the criterion in Proposition 3.5 only depends on $e = v_n(q-1)$ and $\frac{q-1}{n^e} \pmod{n}$. In view of Theorem 3.2 and a result on square roots (Theorem 5 of [2]), we can prove the following propositions on the existence of representing binomials.

Proposition 3.6. *If there exists a binomial $P(X) \in \mathbb{F}_q[X]$ that represents cube roots in $\mathbb{F}_q^\times$, then $e = v_3(q-1) = 1$.*

Proof. Suppose that we are given a binomial $P(X) \in \mathbb{F}_q[X]$ that represents cube roots in $\mathbb{F}_q^\times$. Let $R(X)$ be the remainder in the division of $P(X)$ by $X^{\frac{q-1}{3}} - 1$. If $R(X)$ is a monomial, then $e = 1$ by Proposition 3.5, and we are done. Thus, we may assume that $P(X) = aX^i + bX^j$ with $0 \le i < j < \frac{q-1}{3}$ and $a, b \in \mathbb{F}_q^\times$.

Suppose $3^2 \mid q-1$, and we will get a contradiction. Since $P(x^3)^3 = x^3$ for all $x \in \mathbb{F}_q^\times$, the polynomial $X^{q-1}-1$ divides

$$P(X^3)^3 - X^3 = a^3X^{9i} + 3a^2bX^{6i+3j} + 3ab^2X^{3i+6j} + b^3X^{9j} - X^3.$$

Then we have

$$a^3X^{\overline{9i}} + 3a^2bX^{\overline{6i+3j}} + 3ab^2X^{\overline{3i+6j}} + b^3X^{\overline{9j}} - X^{\overline{3}} = 0,$$

where $\overline{k}$ denotes the remainder in the division of k by $q-1$; see the proof of Lemma 3.1. As $3 \mid q-1$, we have $q \geq 4$. Noting that $e = v_3(q-1) = 1$ when $q = 4$, we assume that $q > 4$, which implies that $\overline{3} = 3$. Clearly, $\overline{9i}$ and $\overline{9j}$ cannot be 3 since $9 \mid q-1$ and $9 \nmid 9i-3, 9j-3$. Hence, two out of $\overline{9i}, \overline{6i+3j}, \overline{3i+6j}$, $\overline{9j}$ and $\overline{3}$ are equal to an integer and the remaining three to a different one. Thus, either $\overline{6i+3j}$ or $\overline{3i+6j}$ must be equal to 3. The only possibility is that we have $\overline{9i} = \overline{9j}$ and $\overline{6i+3j} = \overline{3i+6j} = 3$; for instance, if $\overline{6i+3i} = \overline{9i} = \overline{9j}$, then $q-1 \mid 9i-(6i+3j) = 3(i-j)$, which is impossible since $0 <\mid i-j \mid< \frac{q-1}{3}$. As a result, we have $\frac{q-1}{3} \mid (2i+j-1)$ and $\frac{q-1}{3}(i+2j-1)$, which implies $\frac{q-1}{3} \mid (2i+j-1)-(i+2j-1) = i-j$, which is a contradiction. □

Proposition 3.7. *If there exists a binomial $P(X) \in \mathbb{F}_q[X]$ that represents 4-th roots in $\mathbb{F}_q^\times$, then $e = v_4(q-1) = 1$.*

Proof. Suppose that we are given a binomial $P(X) \in \mathbb{F}_q[X]$ that represents 4-th roots in $\mathbb{F}_q^\times$. By the same argument as in the proof of Proposition 3.6, we may assume that $P(X) = aX^i + bX^j$ with $0 \leq i < j < \frac{q-1}{4}$ and $a, b \in \mathbb{F}_q^\times$.

Suppose $4^2 \mid q-1$, and we will get a contradiction. Since $P(x^4)^4 = x^4$ for all $x \in \mathbb{F}_q^\times$, the polynomial $X^{q-1}-1$ divides

$$P(X^4)^4 - X^4 = a^4X^{16i} + 4a^3bX^{12i+4j} + 6a^2b^2X^{8i+8j} + 4ab^3X^{4i+12j} + b^4X^{16j} - X^4,$$

and so we have

$$a^4X^{\overline{16i}} + 4a^3bX^{\overline{12i+4j}} + 6a^2b^2X^{\overline{8i+8j}} + 4ab^3X^{\overline{4i+12j}} + b^4X^{\overline{16j}} - X^{\overline{4}} = 0.$$

Similarly as in the proof of Proposition 3.6, we note that:

- we may assume $q > 5$ and have $\overline{4} = 4$ as a consequence (the main assertion holds automatically when $q = 5$);
- $\overline{16i}$ and $\overline{16j}$ cannot be 4: if $\overline{16i} = 4$, then $4^2 \mid q-1 \mid 16i-4$, which is impossible. Similarly for $\overline{16j}$.

Thus, there must exist a partition $\mathcal{P}$ of the set

$$\{(\overline{16i}, 1), (\overline{12i+4j}, 2), (\overline{8i+8j}, 3), (\overline{4i+12j}, 4), (\overline{16j}, 5), (\overline{4}, 6)\}$$

of six elements such that each member of $\mathcal{P}$ has cardinality at least 2, and so the cardinality of $\mathcal{P}$ is either 2 or 3. Thus, there cannot be more than 3 non-equivalent elements. Note the following.

- $\overline{16i}$ cannot be $\overline{12i+4j}$ (and $\overline{16j}$ cannot be $\overline{4i+12j}$): if $\overline{16i} = \overline{12i+4j}$, then $q-1 \mid 16i-(12i+4j) = 4(i-j)$, so that $\frac{q-1}{4} \mid i-j$, which is impossible. Similarly for $\overline{16j}$.

- $\overline{12i+4j}$ and $\overline{4i+12j}$ cannot be $\overline{8i+8j}$: similar to the item just above.

We analyze the situation by dividing into two cases according to whether $\overline{12i+4j}$ and $\overline{4i+12j}$ coincide, each of which leads to a contradiction.
Case 1. Assume that $\overline{12i+4j}=\overline{4i+12j}$.

We have $q-1 \mid 12i+4i-(4i+12j)=8(i-j)$, so that $\frac{q-1}{4} \mid 2(j-i)$. Then $2(j-i)=\frac{q-1}{4}$ since $0 \leq i < j < \frac{q-1}{4}$. It is straightforward to check that $\overline{16i}=\overline{16j}$. Also note that $\overline{8i+8j} \neq 4$; otherwise we would have $16 \mid 16i-4$, which is impossible. Now $\overline{12i+4j}=\overline{4i+12j}$ constitutes an equivalent class $C_1 \in \mathcal{P}$ and $\overline{16i}=\overline{16j}$ another distinct class C_2, namely, $\{(\overline{12i+4j},2),(\overline{4i+12j},4)\} \subset C_1$ and $\{(\overline{16i},1),(\overline{16j},5)\} \subset C_2$. Note that we cannot have $\overline{12i+4j}=\overline{4i+12j}=4$; if we do, we get $16 \mid 12i+4j-4, 4i+12j-4$ and so $16 \mid 16(i+j)-8$, which is impossible. We conclude that $\overline{4}=4$ is equal to none of $\overline{16i}, \overline{12i+4j}, \overline{8i+8j}, \overline{4i+12j}, \overline{16j}$. But this contradicts the fact that each class in $\mathcal{P}$ contains at least two elements.
Case 2. Assume that $\overline{12i+4j} \neq \overline{4i+12j}$.

Note that each of $\overline{12i+4j}$, $\overline{4i+12j}$ and $\overline{8i+8j}$ forms distinct equivalent class. Then each of $\overline{16i}$, $\overline{16j}$ and 4 must be equal to exactly one of $\overline{12i+4j}$, $\overline{4i+12j}$, $\overline{8i+8j}$. (i) If $4=\overline{8i+8j}$, then $16 \mid 8(i+j)-4$, a contradiction. (ii) If $4=\overline{12i+4j}$, then $\overline{16i}=\overline{4i+12j}$ and $\overline{16j}=\overline{8i+8j}$, which implies that $\frac{q-1}{4} \mid 3(i-j)$ and $\frac{q-1}{4} \mid 2(j-i)$. Then $\frac{q-1}{4} \mid i-j$, which is a contradiction. (iii) The case $4=\overline{4i+12j}$ is similar to (ii). □

One can expect that the result holds in general, in other words, for $n \geq 3$, if there exists a binomial $P(X) \in \mathbb{F}_q[X]$ that represents n-th roots in $\mathbb{F}_q^\times$, then $e=v_n(q-1) \leq 1$.

4. Lower bounds for the lengths of representing polynomials

A natural question related to Theorem 3.2 and Theorem 3.3 of the previous section is whether there exist polynomials $P(X) \in \mathbb{F}_q[X]$ representing n-th roots with strict inequality $\operatorname{len} P(X) < n^{e-1}$. In the present section, we are going to give an answer to the question, restricted to the case that q is a prime. We assume that q denotes a prime number throughout this section.

Given $e \in \mathbb{Z}_{>0}$, let $[e]$ denote the set of all *primes* $q \in \mathbb{Z}$ such that $v_n(q-1)=e$. Denote by $[e]^-$ the subset of $[e]$ consisting of elements q such that there exists a polynomial $P(X) \in \mathbb{F}_q[X]$ that represents n-th roots in $\mathbb{F}_q^\times$ with $\operatorname{len} P(X) < n^{e-1}$. Set $[e]^+ = [e] \setminus [e]^-$, so that $[e]$ is the disjoint union of $[e]^-$ and $[e]^+$.

Theorem 4.1. *The set $[e]^-$ is finite.*

Thus, beside a finite number of exceptional primes q, n^{e-1} gives the lower bound for the length of representing polynomials. To prove the theorem, we follow the overall strategy of [2]. A challenge in dealing with the case $n>2$ is to be able to lift roots of unity in finite fields $\mathbb{F}_q$ to (the ring of integers of) a number field in such a way that the lifting followed by reduction modulo a certain prime ideal induces a group isomorphism, which is a nontrivial task[3]. Before proving Theorem 4.1, we prove a lemma which ensures the existence of such a characteristic zero lift of n-th roots of unity in finite characteristic.

Let $\zeta_n \in \mathbb{C}$ be a primitive n-th root of unity and let $K = \mathbb{Q}(\zeta_n)$. We denote by $\mathcal{O}_K$ the ring of integers of K. We denote by $N_{L/K}$ the norm of a finite separable field extension L/K.

Lemma 4.2. *Let $\mathfrak{q} \subset \mathcal{O}_K$ be a prime ideal lying over q. If $q \nmid n$, then* $\operatorname{ord}(\zeta_n \bmod \mathfrak{q}) = n$ *as a group element of* $(\mathcal{O}_K/\mathfrak{q})^{\times}$*.*

Proof. First we prove the simplest case that n is a prime. Clearly, $\operatorname{ord}(\zeta_n \bmod \mathfrak{q})$ divides n as $(\zeta_n \bmod \mathfrak{q})^n = \zeta_n^n \bmod \mathfrak{q} = 1 \bmod \mathfrak{q}$. If $\operatorname{ord}(\zeta_n \bmod \mathfrak{q}) = 1$, then $1 - \zeta_n \in \mathfrak{q}$. But this is impossible since $n\mathcal{O}_K = \mathfrak{p}^{n-1}$ where $\mathfrak{p} = (1-\zeta_n) \triangleleft \mathcal{O}_K$. Thus, $\operatorname{ord}(\zeta_n \bmod \mathfrak{q}) = n$ as n is a prime.

For the general case, let $n = p_1^{e_1} \cdots p_s^{e_s}$ where the p_j are distinct primes different from q and $e_j \geq 1$. We need to show that $1 - \zeta_n^{n/p_j} \notin \mathfrak{q}$ for all $j \in \{1, \ldots, s\}$. It suffices to prove it for $j = 1$ (by permuting the indices). Suppose that $1 - \zeta_n^k \in \mathfrak{q}$ where $k = n/p_1 = p_1^{e_1-1} p_2^{e_2} \cdots p_s^{e_s}$. Note that ζ_n^k is a primitive p_1-th root of unity. The minimal polynomial of $1 - \zeta_n^k$ is $\Phi_{p_1}(1 - X)$ where $\Phi_{p_1}(X) = \frac{X^{p_1}-1}{X-1} = X^{p_1-1} + \cdots + X + 1$ is the p_1-th cyclotomic polynomial. Then $N_{\mathbb{Q}(\zeta_n^k)/\mathbb{Q}}(1 - \zeta_n^k) = \Phi_{p_1}(1-0) = p_1$. Thus, $N_{K/\mathbb{Q}}(1 - \zeta_n^k) = N_{\mathbb{Q}(\zeta_n^k)/\mathbb{Q}}(N_{K/\mathbb{Q}(\zeta_n^k)}(1-\zeta_n^k)) = N_{\mathbb{Q}(\zeta_n^k)/\mathbb{Q}}((1-\zeta_n^k)^{[K:\mathbb{Q}(\zeta_n^k)]}) = N_{\mathbb{Q}(\zeta_n^k)/\mathbb{Q}}((1-\zeta_n^k))^{[K:\mathbb{Q}(\zeta_n^k)]} = p_1^{[K:\mathbb{Q}(\zeta_n^k)]} = p_1^{p_1^{e_1-1}(p_2-1)p_2^{e2}\cdots(p_s-1)p_s^{e_s}}$. As a consequence, we have $(1 - \zeta_n^k) \mid (p_1^{p_1^{e_1-1}(p_2-1)p_2^{e2}\cdots(p_s-1)p_s^{e_s}})$. Thus, $\mathfrak{q} \nmid (1 - \zeta_n^k)$. Indeed, if $\mathfrak{q} \mid (1-\zeta_n^k)$, then $\mathfrak{q} \mid p_1$, which is impossible since $\mathfrak{q} \mid q$. Now, as $1-\zeta_n^{n/p_j} \notin \mathfrak{q}$ for all $j \in \{1, \ldots, s\}$, we have $\zeta_n^{n/p_j} \not\equiv 1 \pmod{\mathfrak{q}}$. Thus, $\operatorname{ord}(\zeta_n \pmod{\mathfrak{q}}) = n$. □

Corollary 4.3. *The canonical surjection $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{q}$ induces a group isomorphism $\pi : \langle \zeta_n \rangle \to \langle \zeta_n \bmod \mathfrak{q} \rangle$.*

We now prove two more lemmas needed in the proof of Theorem 4.1. For each $\epsilon \in \Sigma_{n^e}$, define $A_\epsilon(X) = \sum_{i=0}^{n^{e-1}-1} \epsilon_i X^i \in \mathbb{F}_q[X]$. We denote by $\overline{\cdot} : \mathbb{Z}[X] \to \mathbb{F}_q[X], f(X) \mapsto \overline{f}(X)$ the reduction modulo q map. Recall that $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n \in \mathbb{C}$ is a primitive n-th root of unity. Note that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ is the ring of integers of K. Denote by $\widehat{\cdot} : \mu_n = \langle \zeta^{\frac{q-1}{n}} \rangle \to \langle \zeta_n \rangle$ the group homomorphism defined by $\widehat{\zeta^{\frac{q-1}{n}}} = \zeta_n$, which is an isomorphism by Corollary 4.3. In fact, the inverse map $\pi^{-1} : \langle \zeta_n \bmod \mathfrak{q} \rangle \to \langle \zeta_n \rangle$ is equal to $\widehat{\cdot}^{\,i}$ for some $i \in \mathbb{Z}$ with $\gcd(i, n) = 1$. Let $\widehat{A}_\epsilon(X) = \sum_{i=0}^{n^{e-1}-1} \widehat{\epsilon}_i X^i \in \mathcal{O}_K[X]$ be the characteristic zero lift of $A_\epsilon(X)$ via the isomorphism $\widehat{\cdot} : \mu_n \to \langle \zeta_n \rangle$.

Let us denote by $\operatorname{Res}(f, g)$ the resultant of two polynomials with coefficients in a commutative ring R with unity. Note that $\operatorname{Res}(f, g) \in R$.

[3] When $n = 2$, there is a canonical lift of $\mu_2 = \{\pm 1\} \subset \mathbb{F}_q$ to $\mathbb{Z}$, which works for all q.

Lemma 4.4. *For every $\epsilon \in \Sigma_{n^e}$, we have* $\mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e}) \neq 0$.

Proof. If $e = 1$, then $\widehat{A}_\epsilon(X) \in \mathcal{O}_K^\times$ and the assertion holds. We may assume $e > 1$. Suppose that $\widehat{A}_\epsilon$ and Φ_{n^e} have a common root $\zeta_{n^e}^i$ (in $\overline{\mathbb{Q}}$), where $i \in \{1, \ldots, n^e\}$ with $\gcd(n, i) = 1$. Note that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n^e}^i)] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]/[\mathbb{Q}(\zeta_{n_e}^i) : \mathbb{Q}] = \phi(n^e)/\phi(n) = n^{e-1} > n^{e-1} - 1 = \deg \widehat{A}_\epsilon(X)$. On the other hand, the minimal polynomial of $\zeta_{n^e}^i$ over $\mathbb{Q}(\zeta_n)$ must divide $\widehat{A}_\epsilon$, and so we have $[\mathbb{Q}(\zeta_{n_e}^i) : \mathbb{Q}(\zeta_n)] \leq \deg \widehat{A}_\epsilon(X)$, which is a contradiction. □

Lemma 4.5. *If $q \in [e]^-$, then there exists $\epsilon = (\epsilon_0, \ldots, \epsilon_{n^{e-1}-1}) \in \Sigma_{n^e}$ such that*

$$\mathrm{Res}(A_\epsilon, \overline{\Phi}_{n^e}) = 0 \in \mathbb{F}_q.$$

Proof. For brevity we set $w := \zeta^{\frac{q-1}{n^e}}$. Then $\mu_{n^e} = \{\zeta^{\frac{q-1}{n^e}i} \mid 1 \leq i \leq n^e\} = \{w^i \mid 1 \leq i \leq n^e\}$. Suppose that $P(X) \in \mathbb{F}_q[X]$ represents n-th roots in $\mathbb{F}_q^\times$. Let $R(X) \in \mathbb{F}_q[X]$ be the unique polynomial with $\deg R(X) < n^{e-1}$ such that $P(X) = (X^{n^{e-1}} - 1)H(X) + R(X)$ for some $H(X) \in \mathbb{F}_q[X]$. Then $R(X)$ represents n-th roots in μ_{n^e}:

$$R(w^{in})^n = (P(w^{in}) - (w^{in^e} - 1)H(w^{in}))^n = P(w^{in})^n = w^{in}$$

for all $i \in \{1, \ldots, n^{e-1}\}$. For each $i \in \{0, \ldots, n^{e-1} - 1\}$, if we set $\epsilon_i := R(w^{in})/w^i \in \mu_n$, then we have $R(w^{in}) = \epsilon_i w^i$. By the Lagrange interpolation formula (Theorem 2.1), we have

$$\begin{aligned} R(X) &= \sum_{i=0}^{n^{e-1}-1} \epsilon_i w^i \prod_{j=0, j\neq i}^{n^{e-1}-1} \frac{X - w^{jn}}{w^{in} - w^{jn}} \\ &= \sum_{i=0}^{n^{e-1}-1} \epsilon_i w^i \frac{X^{n^{e-1}} - 1}{X - w^{in}} \frac{w^{in}}{n^{e-1}} \\ &= \frac{1}{n^{e-1}} \sum_{i=0}^{n^{e-1}-1} \sum_{j=0}^{n^{e-1}-1} \epsilon_i w^{i(1-nj)} X^j \\ &= \frac{1}{n^{e-1}} \sum_{j=0}^{n^{e-1}-1} A_\epsilon(w^{1-nj}) X^j. \end{aligned}$$

Since $\mathrm{len}\, R(X) < n^{e-1}$, there exists $j \in \{0, \ldots, n^{e-1} - 1\}$ such that $A_\epsilon(w^{1-nj}) = 0$. Noting that $\overline{\Phi}_{n^e}(w^{1-nj}) = 0$, we conclude that $\mathrm{Res}(A_\epsilon, \overline{\Phi}_{n^e}) = 0$. □

Now we proceed to prove Theorem 4.1. Eventually, we will prove that $\#[e]^- \leq \#\{\mathfrak{q} \triangleleft \mathcal{O}_K \mid \mathfrak{q}$ is prime and divides $\Pi_e\}$, where Π_e is a nonzero ideal of $\mathcal{O}_K$.

Proof of Theorem 4.1. Define[4] $\Pi_e := \mathrm{lcm}_{\epsilon \in \Sigma_{n^e}}(\mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e}))$ as an ideal of $\mathcal{O}_K$ where $(\mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e})) = \mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e}) \cdot \mathcal{O}_K$ is the principal ideal of $\mathcal{O}_K$ generated by $\mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e})$. Note that Π_e is a *nonzero* ideal of $\mathcal{O}_K$ by Lemma 4.4. Let $\mathcal{F} := \{\mathfrak{q} \lhd \mathcal{O}_K \mid \mathfrak{q} \text{ is prime and divides } \Pi_e\}$, which is a finite set.

Claim: If $q \in [e]^-$, then q lies below some $\mathfrak{q} \in \mathcal{F}$.

Let $q \in [e]^-$ be given. We need to prove that there exists a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ such that $\mathfrak{q} \mid q$ and $\mathfrak{q} \mid \Pi_e$. Namely, we need to show that (q) and Π_e are not coprime. It suffices to show that there exists a prime ideal $\mathfrak{q}$ and $\epsilon \in \Sigma_{n^e}$ such that $\mathfrak{q} \mid q$ and $\mathfrak{q} \mid \mathrm{Res}(\widehat{A}_\epsilon, \Phi_{n^e})$. By Lemma 4.5, there exists $\epsilon = (\epsilon_0, \ldots, \epsilon_{n^{e-1}-1}) \in \Sigma_{n^e}$ such that $\mathrm{Res}(A_\epsilon, \overline{\Phi}_{n^e}) = 0$. By Corollary 4.3, there exists $\nu = (\nu_0, \ldots, \nu_{n^{e-1}-1}) \in \mu_n(K)^{n^{e-1}}$ such that $\widehat{\nu}_j \bmod \mathfrak{q} = \epsilon_j$ for all $j \in \{0, \ldots, n^{e-1}-1\}$. Since Φ_{n^e} is monic, $\mathrm{Res}(A_\epsilon, \overline{\Phi}_{n^e}) = 0$ implies that $\mathrm{Res}(\widehat{A}_\nu, \Phi_{n^e}) + \mathfrak{q} = \pi(\mathrm{Res}(\widehat{A}_\nu, \Phi_{n^e})) = 0 = \mathfrak{q} \in \mathcal{O}_K/\mathfrak{q}$.[5] (Note that $\widehat{A}_\nu + \mathfrak{q} = A_{\widehat{\nu}} + \mathfrak{q} = A_\epsilon$.) In other words, $\mathrm{Res}(\widehat{A}_\nu, \Phi_{n^e}) \in \mathfrak{q}$ or $\mathfrak{q} \mid \mathrm{Res}(\widehat{A}_\nu, \Phi_{n^e})$. Thus, we have $\mathfrak{q} \in \mathcal{F}$. Since precisely one prime can lie blow each prime ideal $\mathfrak{q} \in \mathcal{F}$, we have $\#[e]^- \leq \#\mathcal{F} < \infty$. □

Remark 4.6. In the context of n-th roots for arbitrary n, Theorem 3.2 has rather restricted applicability. To be able to guarantee existence of short representing polynomials in all possible cases, more refined techniques seem to be needed. We content ourself by noting that Theorem 3.2, combined with Theorem 4.1, gives almost complete answer for the case $n = 3$ regarding the lower bound for the length.

References

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

[2] S. J. Agou, M. Deléglise, and J.-L. Nicolas, *Short polynomial representations for square roots modulo p*, Des. Codes Cryptogr. **28** (2003), no. 1, 33–44.

[3] P. S. L. M. Barreto and J. F. Voloch, *Efficient computation of roots in finite fields*, Des. Codes Cryptogr. **39** (2006), no. 2, 275–280.

[4] M. Cipolla, *Un metodo per la risoluzione della congruenza di secondo grado*, Napoli Rend. **9** (1903), 154–163.

[5] D. Coppersmith and I. Shparlinski, *On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping*, J. Cryptology **13** (2000), no. 3, 339–360.

[6] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Third Edition, Cambridge University Press, Cambridge, 2013.

[7] E. Kiltz and A. Winterhof, *On the interpolation of bivariate polynomials related to the Diffie-Hellman mapping*, Bull. Aust. Math. Soc. **69** (2004), no. 2, 305–315.

[8] T. Lange and A. Winterhof, *Polynomial interpolation of the elliptic curve and XTR discrete logarithm*, Computing and combinatorics, 137–143, Lecture Notes in Comput. Sci., 2387, Springer, Berlin, 2002.

[4] We can do this as $\mathcal{O}_K$ is a Dedekind domain, admitting unique factorization of ideals into products of prime ideals.

[5] See, for example, Lemma 6.25 of [6].

[9] ______, *Interpolation of the discrete logarithm in $\mathbb{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$*, Discrete Appl. Math. **128** (2003), no. 1, 193–206.

[10] ______, *Interpolation of the elliptic curve Diffie-Hellman mapping*, Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003), 51–60, Lecture Notes in Comput. Sci., 2643, Springer, Berlin, 2003.

[11] D. H. Lehmer, *Computer technology applied to the theory of numbers*, In William J. Leveque, editor, Studies in number theory, volume 6 of MAA Studies in Mathematics, pages 117–151, Englewood Cliffs, New Jersey, Prentice-Hall, 1969.

[12] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, 20. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[13] G. L. Mullen and D. White, *A polynomial representation for logarithms in $GF(q)$*, Acta Arith. **47** (1986), no. 3, 255–261.

[14] H. Niederreiter, *A short proof for explicit formulas for discrete logarithms in finite fields*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), no. 1, 55–57.

[15] T. Satoh, *On polynomial interpolations related to Verheul homomorphisms*, LMS J. Comput. Math. **9** (2006), 135–158.

[16] ______, *On degrees of polynomial interpolations related to elliptic curve cryptography*, Coding and cryptography, 155–163, Lecture Notes in Comput. Sci., 3969, Springer, Berlin, 2006.

[17] ______, *On pairing inversion problems*, Pairing-based cryptography-Pairing 2007, 317–328, Lecture Notes in Comput. Sci., 4575, Springer, Berlin, 2007.

[18] ______, *Closed formulae for the Weil pairing inversion*, Finite Fields Appl. **14** (2008), no. 3, 743–765.

[19] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494.

[20] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972), 51–70. Congressus Numerantium, No. VII, Utilitas Math., Winnipeg, Man., 1973.

[21] A. Tonelli, *Bemerkung über die Auflösung quadratischer Congruenzen*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen, pp. 344–346, 1891.

[22] Z.-X. Wan, *A shorter proof for an explicit formula for discrete logarithms in finite fields*, Discrete Math. **308** (2008), no. 21, 4914–4915.

[23] A. Winterhof, *Polynomial interpolation of the discrete logarithm*, Des. Codes Cryptogr. **25** (2002), no. 1, 63–72.

Seunghwan Chang
Institute of Mathematical Sciences
Ewha Womans University
Seoul 120-750, Korea
E-mail address: `schang@ewha.ac.kr`

Bihtnara Kim
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: `bihtnr@gmail.com`

Hyang-Sook Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: hsl@ewha.ac.kr