Low Complexity Cubing and Cube Root Computation over $\mathbb{F}_{3^m}$ in Polynomial Basis

Omran Ahmadi[1] and Francisco Rodríguez-Henríquez[2]

[1] Claude Shannon Institute, School of Mathematical Sciences

University College Dublin, Ireland

omran.ahmadi@ucd.ie

[2] Computer Science Department

Centro de Investigación y de Estudios Avanzados del IPN, México

francisco@cs.cinvestav.mx

Abstract

We present low complexity formulae for the computation of cubing and cube root over $\mathbb{F}_{3^m}$ constructed using special classes of irreducible trinomials, tetranomials and pentanomials. We show that for all those special classes of polynomials, field cubing and field cube root operation have the same computational complexity when implemented in hardware or software platforms. As one of the main applications of these two field arithmetic operations lies in pairing-based cryptography, we also give in this paper a selection of irreducible polynomials that lead to low cost field cubing and field cube root computations for supersingular elliptic curves defined over $\mathbb{F}_{3^m}$, where m is a prime number in the pairing-based cryptographic range of interest, namely, $m \in [47, 541]$.

keyword: Finite field arithmetic; cubing; cube root; characteristic three; cryptography

I. Introduction

Arithmetic over ternary extension fields $\mathbb{F}_{3^m}$ has gained an increasing importance in several relevant cryptographic applications, particularly in (hyper) elliptic curve cryptography. It has been shown that supersingular elliptic curves over $\mathbb{F}_{3^m}$ are excellent choices for the implementation of pairing-based cryptographic protocols [8]. Furthermore, some of the fastest algorithms known for pairing computations on these supersingular elliptic curves [2], [9], [10], [16], require the efficient computation of the basic arithmetic finite field operations such as field addition, subtraction, multiplication, division, exponentiation, cubing and cube root computation. In particular, cube root computation has become an important building block in the design of bilinear pairings [2], [9], [16].

The efficiency of finite field arithmetic implemented in hardware can be measured in terms of associated design space and time complexities. The space complexity is defined as the total amount of hardware resources needed to implement the circuit, i.e. the total number of logic gates required by the design. Time complexity, on the other hand, is simply defined as the total gate delay or critical path of the circuit, frequently formulated using gate delay units.

Let $P(x)$ be an irreducible monic polynomial of degree m over $\mathbb{F}_3$. Then, the ternary extension field $\mathbb{F}_{3^m}$ can be defined as,

$$\mathbb{F}_{3^m} \cong \mathbb{F}_3[x]/\left(P(x)\right).$$

Let A be an arbitrary element in the field $\mathbb{F}_{3^m}$ as described above. Then, the field cubing of A, denoted as $C = A^3$, can be computed by first cubing A as a polynomial, and then reducing the result modulo $P(x)$. Similarly, the field cube root of A, denoted as $A^{\frac{1}{3}}$, or simply, $\sqrt[3]{A}$, is the unique element $D \in \mathbb{F}_{3^m}$ such that $D^3 = A$, holds. Notice that in finite fields of characteristic three, cubing and cube root taking are automorphisms that preserve the base field.

In 2004, Barreto in [7] published an extension of a method previously used for square root computations in binary fields, to compute cube roots in ternary fields. Both approaches in the cases of binary and ternary fields are especially efficient when the finite field has been generated by a special class of irreducible trinomials.

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the irreducible monic polynomial $P(x)$, with an extension degree $m = 3u + r$, where $u \geq 1$ and $r \in \{0, 1, 2\}$. Let A be an arbitrary element of the field $\mathbb{F}_{3^m}$, that in polynomial basis can be written as,

$$A \;=\; \sum_{i=0}^{m-1} a_i x^i = \sum_{i=0}^{u-1+\lceil \frac{r}{2} \rceil} a_{3i} x^{3i} + x \cdot \sum_{i=0}^{u-1+\lfloor \frac{r}{2} \rfloor} a_{3i+1} x^{3i} + x^2 \cdot \sum_{i=0}^{u-1} a_{3i+2} x^{3i},$$

with $a_i \in \mathbb{F}_3$. Then, the field cube root $\sqrt[3]{A}$, can be computed as [7], [1]

$$\sqrt[3]{A} = \left(\sum_{i=0}^{u-1+\lceil \frac{r}{2} \rceil} a_{3i} x^i + x^{1/3} \cdot \sum_{i=0}^{u-1+\lfloor \frac{r}{2} \rfloor} a_{3i+1} x^i + x^{2/3} \cdot \sum_{i=0}^{u-1} a_{3i+2} x^i \right) \pmod{P(x)}. \qquad (1)$$

Using Eq. (1) one can compute a cube root by performing two third-length polynomial multiplications with the per-field constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$, that can be calculated offline. In the case that the Hamming weight of $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ is low, those two multiplications are simple to compute. Barreto showed in [7], that low Hamming weights for $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ can be obtained if one uses $P(x) = x^m + ax^k + b$, with $a, b \in \mathbb{F}_3$, and $m \equiv k \equiv r \pmod 3$, with $r \neq 0$. We stress that this is a strong restriction as those trinomials do not exist for every extension degree m.[2] We also note that if the degree of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ is strictly less than $2u + r - 1$, then the computation of Eq. (1) does not require a reduction process modulo $P(x)$.

In [1], Ahmadi et al. studied the Hamming weight of $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ in the general case of

[1]There is a typo in the first equation of Subsection 2.2 of [7], since the upper limit of the third summation should not be u but $u - 1$.

[2]In ternary fields $\mathbb{F}_{3^m}$, there exist 381 m values less than 1000 where at least one irreducible trinomial of degree m can be found. However, irreducible trinomials of the form $P(x) = x^m + ax^k + b$, with the property, $m \equiv k \equiv r \pmod 3$, are available in just 74 values out of the total of 168 prime numbers less than 1000 (about 44% of the cases).

irreducible trinomials where m is not congruent with k modulo 3. Authors in [1] showed that general irreducible trinomials can lead to high Hamming weights for the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$, thus making the computation of Eq. (1) expensive and therefore, less attractive. [3] In [2], and more recently in [16], several cube root friendly irreducible pentanomials for the extension degree $m = 509$ were reported. In [16], the pentanomials $P_1(x) = x^{509} - x^{477} + x^{445} + x^{32} - 1$ and $P_2(x) = x^{509} - x^{318} - x^{191} + x^{127} + 1$, were used. Those polynomials were then successfully utilized within a software library for computing bilinear pairings efficiently. However, authors in [2], [16] did not elaborate further in the search criteria used for finding cube root friendly pentanomials.

In this paper, we present a study of the computational efforts associated to field cubing and cube root calculation in ternary extension fields. We give a result useful for classifying trinomials that happen to be irreducible over $\mathbb{F}_3$. Furthermore, we present an extended version of the Barreto method, that is useful for finding families of cube root friendly irreducible trinomials, tetranomials and pentanomials. We also give the necessary and sufficient conditions required for having irreducible equally spaced tetranomials and pentanomials over $\mathbb{F}_3$. We present a careful complexity analysis of the field cubing computation and report a list of irreducible polynomials with prime extension degrees m in the range $m \in [47, 541]$, that lead to efficient computations of the cube root operation. Then, we discuss how the technique of mapping to a ring can be useful for speeding-up the cube root computation in certain ternary fields. Finally, we present a selection of irreducible polynomials that lead to low cost field cubing and field cube root computations for supersingular elliptic curves defined over $\mathbb{F}_{3^m}$. Supersingular elliptic curves have been found useful for the efficient computation of bilinear pairings.

The rest of this paper is organized as follows. In Section II, we give a short summary of the main results published in the open literature for computing field squaring and square roots. In Section III, we present a lemma that allows the classification of irreducible trinomial for odd extension degrees. We also give the computational cost of the field cubing operation when $P(x)$ happens to be a trinomial or a tetranomial. Then, in Section IV, we analyze the computational cost of the cube root operation when $P(x)$ is a special class of trinomial, tetranomial, pentanomial

[3] Authors in [2] state that there are extension degrees m where no irreducible trinomial yields sparse $x^{1/3}$. They give as an example an almost worst case for $m = 163$, where there exists an irreducible trinomial that yields $x^{\frac{1}{3}}$ with a Hamming weight of 162 nonzero terms.

and/or equally spaced polynomial. In Section VI, we show how the ring mapping idea can be used to accelerate the cube root computation in some ternary fields. Section VII presents a list of reduction polynomials that yield low cost cubings and cube roots for supersingular elliptic curves with large r-torsion subgroups over $\mathbb{F}_{3^m}$. Finally, in Section VIII some concluding remarks are drawn.

II. Previous Work on Field Squaring and Square Roots in Binary Fields

Since many techniques used in binary arithmetic can be extended to ternary arithmetic, we will recount in the rest of this Section the different approaches proposed across the years for computing field squaring and square root over binary fields.

A. Squaring

Let $\mathbb{F}_{2^m}$ be a binary extension field generated by an irreducible monic polynomial $P(x)$, and let A be an arbitrary element of that field. Then, the element A can be written in canonical (polynomial) basis as, $A = \sum_{i=0}^{m-1} a_i x^i$. Let us also assume that the extension degree m can be expressed as, $m = 2u+1$, with $u \geq 1$. Then, the polynomial squaring operation can be obtained as,

$$\begin{aligned} A^2 &= \left(\sum_{i=0}^{m-1} a_i x^i\right)^2 = \sum_{i=0}^{m-1} a_i x^{2i} = \sum_{i=0}^{u} a_i x^{2i} + \sum_{i=u+1}^{2u} a_i x^{2i} \\ &= \sum_{i=0}^{u} a_i x^{2i} + x^{2u+1} \sum_{i=1}^{u} a_{u+i} x^{2i-1} = \sum_{i=0}^{u} a_i x^{2i} + x^m \sum_{i=1}^{u} a_{u+i} x^{2i-1}. \end{aligned}$$

Hence, we can compute the field squaring operation defined as $C = A^2 \pmod{P(x)}$ as,

$$C = A^2 \pmod{P(x)} = \left(\sum_{i=0}^{u} a_i x^{2i} + x^m \sum_{i=1}^{u} a_{u+i} x^{2i-1}\right) \pmod{P(x)} \tag{2}$$

It is possible to implement efficiently Eq. (2) in software by extracting the two half-length vectors $A^L = (a_u, a_{u-1}, \cdots, a_1, a_0)$ and $A^H = (a_{2u}, a_{2u-1}, \cdots, a_{u+2}, a_{u+1})$, followed by one field multiplication of length $m/2$ bits by the per-field constant x^m. In the case that the irreducible polynomial $P(x)$ is a trinomial of the form, $P(x) = x^m + x^k + 1$, then $x^m = x^k + 1$ has a Hamming weight of 2. We stress that the reduction process modulo $P(x)$ stipulated in Eq. (2), should normally be performed. The only exception would be if $P(x)$ is an irreducible trinomial of the form, $P(x) = x^m + x + 1$. In this case, one can compute the field squaring operation without performing any reduction at all.

B. Square Root

One straightforward method for computing p-th roots in prime extension fields is based on Fermat's Little Theorem which establishes that for any element $A \in \mathbb{F}_{p^m}$, the identity $A^{p^m} = A$ holds. Therefore, $\sqrt[p]{A}$ may be computed as $D = A^{p^{m-1}}$ with a computational cost of $m-1$ field exponentiations to the power p.[4]

A potentially much more efficient approach for computing square roots over binary extension fields, was presented by Fong et al. in [15] based on the following observation. Let A be an arbitrary element in $\mathbb{F}_{2^m}$ represented in the polynomial basis as $A = \sum_{i=0}^{m-1} a_i x^i$. Then, $\sqrt{A}$ can be expressed in terms of the square root of x as,

$$A^{\frac{1}{2}} = \left(\sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} a_{2i} x^i + x^{\frac{1}{2}} \sum_{i=0}^{\lfloor \frac{m-3}{2} \rfloor} a_{2i+1} x^i \right) \pmod{P(x)}. \tag{3}$$

It is possible to implement efficiently Eq. (3) in software by extracting the two half-length vectors $A_{even} = (a_{m-1}, a_{m-3}, \cdots, a_2, a_0)$ and $A_{odd} = (a_{m-2}, a_{m-4}, \cdots, a_3, a_1)$, followed by one field multiplication of length $m/2$ bits by the pre-computed constant $x^{\frac{1}{2}}$. However, in the case that the irreducible polynomial $P(x)$ is a trinomial, $P(x) = x^m + x^n + 1$ with m an odd prime number, then the square root of an arbitrary element $A \in \mathbb{F}_{2^m}$ can be obtained at a very low price: the computation of some few additions and shift operations [15].[5] Furthermore, Rodríguez-Henríquez et al. showed in [22] that for all practical cases, the cost of computing in hardware the square root over binary fields generated with irreducible trinomials, is not more expensive than the computational effort required for computing field squarings.

Based on the technique used for trinomials, Avanzi in [5], [6], published a method that can find irreducible polynomials, other than trinomials, that lead to low-weight constants $x^{\frac{1}{2}}$. His method can be summarized as follows. Let us assume that there exists an m-degree polynomial,

[4]This is the method suggested in [18], for computing square roots over binary extension fields.

[5]It is noticed that there exist 545 values of m less than 1000 for which at least one irreducible trinomial of degree m over $\mathbb{F}_2$ can be found. Restricting ourselves to extension degrees where m is a prime number, from the total of 168 prime numbers less than 1000, irreducible trinomials can be found for just 82 values (only 48% of the cases).

irreducible over $\mathbb{F}_2$, that can be written as $P(x) = x \cdot U(x)^2 + 1$, where $U(x)$ is an $\frac{m-1}{2}$-degree polynomial of even weight. Then, it follows that the per-field constant $x^{\frac{1}{2}}$ will be given by, $x^{\frac{1}{2}} = xU(x)$. [6]

Using the above approach to guide his search of irreducible polynomials, Avanzi was able to find a rich family of square root friendly irreducible pentanomials and heptanomials that produce constants $x^{\frac{1}{2}}$ with low Hamming weight. By virtue of Eq. (3), this implies that one can calculate the field square root operation with a computational effort comparable to that required by irreducible trinomials. Avanzi's square root friendly polynomials became a good option for binary extension fields with degree extensions m where no irreducible trinomial can be found.

Other pentanomials that lead to fast computation of the square root over $\mathbb{F}_{2^m}$, were published independently by Ahmadi et al. in [3], where two square root friendly irreducible pentanomials for the extension degrees $m = 163, 283$, and one irreducible trinomial for $m = 233$, were used with advantage for speeding-up the computation of the scalar multiplication on Koblitz curves. Furthermore, in [23], Scott proposed to use irreducible pentanomials that can assure both, fast modular reductions and square root computations in software implementations. To this end, he suggested to work with m-degree irreducible pentanomials of the form $P(x) = x^m + x^{k_1} + x^{k_2} + x^{k_3} + 1$, such that $m - k_1 \equiv m - k_2 \equiv m - k_3 \equiv 0 \pmod{w}$, where w is the word length of the target processor and m is a prime number. These irreducible pentanomials cannot always be found for a given extension degree m. However, less efficient alternatives were also suggested in [23].

Finally Panairo and Thompson studied in [21] the computation of p-th roots in finite fields of odd characteristic p, with $p \geq 5$, where irreducible binomials can be found.

III. Field Cubing Computation

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the irreducible monic polynomial $P(x)$, and let A be an arbitrary element of that field. Then, the element A can be written in canonical basis as, $A = \sum_{i=0}^{m-1} a_i x^i$, $a_i \in \mathbb{F}_3$, where the extension degree m can be written as, $m = 3u + r$,

[6] We stress that this method will always produce irreducible polynomials of the form, $P(x) = x \cdot U(x)^2 + 1 = x^m + x^{k_1} + \ldots + x^{k_l} + 1$, with $m \equiv k_1 \ldots \equiv k_l \equiv 1 \pmod{2}$.

with $u \geq 1$ and $r \in \{0, 1, 2\}$. Then, one can compute the polynomial cubing A^3 as,

$$\begin{aligned} A^3 &= \left(\sum_{i=0}^{m-1} a_i x^i\right)^3 = \sum_{i=0}^{m-1} a_i x^{3i} \\ &= \sum_{i=0}^{u} a_i x^{3i} + \sum_{i=u+1}^{2u+r-1} a_i x^{3i} + \sum_{i=2u+r}^{3u+r-1} a_i x^{3i} \\ &= C_0 + x^{3u+r} C_1 + x^{6u+2r} C_2, \end{aligned}$$

where,

$$C_0 = \sum_{i=0}^{u} a_i x^{3i}, \quad C_1 = \sum_{i=1}^{u+r-1} a_{i+u} x^{3i-r}, \text{and} \quad C_2 = \sum_{i=r}^{u+r-1} a_{i+2u} x^{3i-2r}. \tag{4}$$

Then, the field cubing operation defined as $C = A^3 \pmod{P(x)}$ can be performed as,

$$\begin{aligned} C = A^3 \pmod{P(x)} &= \left(C_0 + x^{3u+r} C_1 + x^{6u+2r} C_2\right) \pmod{P(x)} \\ &= \left(C_0 + x^{m} C_1 + x^{2m} C_2\right) \pmod{P(x)}. \end{aligned} \tag{5}$$

Eq. (5) states that the cubing operation can be computed by determining the constants x^m and x^{2m}, which are per-field constants, and therefore they can be pre-computed offline. In the rest of this Section we will study several classes of trinomials and tetranomials, and we will give closed formulae for the field cubing operation.

A. Irreducible Trinomials

1) Classification of Ternary Trinomials: Let us consider ternary extension fields constructed using irreducible trinomials of the form $P(x) = x^m + ax^k + b$, with $m \geq 2$ and $a, b \in \mathbb{F}_3$. Then, the following results are useful.

Theorem 3.1: Let $m > 2$ be an odd number. Then, if k is odd we have that, $P_0(x) = x^m + x^k + 1$ and $P_1(x) = x^m + x^k - 1$ are always reducible over $\mathbb{F}_3$ and $P_3(x) = x^m - x^k + 1$ is irreducible if and only if $P_2(x) = x^m - x^k - 1$ is irreducible over $\mathbb{F}_3$.
If k is even, then $P_0(x)$ and $P_2(x) = x^m - x^k - 1$ are always reducible over $\mathbb{F}_3$ and $P_3(x)$ is irreducible if and only if $P_1(x) = x^m + x^k - 1$ is irreducible.

Proof: From Table I we see that $P_0(1) = 0$ and hence $P_0(x)$ is always reducible. Similarly we see that if k is odd, then $P_1(-1) = 0$ and hence in this case $P_1(x)$ is reducible. Moreover, as shown in Table I, we see that if k is even then $P_1(x) = -P_3(-x)$. Thus, if k is even we have that $P_1(x)$ is irreducible if and only if $P_3(x)$ is irreducible over $\mathbb{F}_3$. The remaining claims can be deduced in a similar way from Table I.

TABLE I

IRREDUCIBILITY CONDITIONS OVER $\mathbb{F}_3$ FOR TRINOMIALS OF THE FORM $P(x) = x^m + ax^k + b$, WITH $a, b \in \mathbb{F}_3$.

	k odd	k even
$P_0(x) = x^m + x^k + 1$	$P_0(1) = 0$	$P_0(1) = 0$
$P_1(x) = x^m + x^k - 1$	$P_1(-1) = 0$	$P_1(x) = -P_3(-x)$
$P_2(x) = x^m - x^k - 1$	$P_2(x) = -P_3(-x)$	$P_2(-1) = 0$
$P_3(x) = x^m - x^k + 1$	$P_3(x) = -P_2(-x)$	$P_3(x) = -P_1(-x)$

■

Hence, without loss of generality, we will study in the rest of this subsection irreducible trinomials of the form, $P(x) = x^m - x^k + 1$. We say that a trinomial where $m \equiv k \pmod 3$ is a *cube root friendly* trinomial. If additionally the condition $k < \frac{m}{2}$ holds, we say that $P(x)$ is a *preferred* trinomial.

2) Irreducible Trinomials $P(x) = x^m - x^k + 1$, with $m \equiv k \equiv r \pmod 3$: Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the trinomial $P(x) = x^m - x^k + 1$, irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m = 3u + r$, $1 \leq u$ and $k = 3v + r$, $0 \leq v$, with $m \equiv k \equiv r \pmod 3$, $r \neq 0$ and $u - 2v \geq 1$. Then, we can write $x^m = x^k - 1$ and $x^{2m} = \left(x^k - 1\right)^2 = x^{2k} + x^k + 1$. Using Eq. (5), we can compute the field cubing as,

$$C^3 = C_0 + x^m C_1 + x^{2m} C_2 = \left(C_0 - C_1 + C_2 + x^k(C_1 + C_2) + x^{2k} C_2\right) \pmod{P(x)}.$$

In order to further expand the above result, it becomes useful to define $C_1^L, C_1^H, C_2^L, C_2^H$ as,

$$\begin{aligned} C_1 &= \sum_{i=1}^{u+r-1} a_{i+u} x^{3i-r} = \sum_{i=1}^{u-v} a_{i+u} x^{3i-r} + x^{3(u-v)} \sum_{i=1}^{v+r-1} a_{i+2u-v} x^{3i-r} \\ &= C_1^L + x^{3(u-v)} C_1^H, \end{aligned}$$

where the polynomials C_1^L and C_1^H have degrees $3(u-v)-r$ and $3v+2r-3$, respectively.

$$\begin{aligned} C_2 &= \sum_{i=r}^{u+r-1} a_{i+2u}x^{3i-2r} = \sum_{i=r}^{u-v+r-1} a_{i+2u}x^{3i-2r} + x^{3(u-v)} \sum_{i=r}^{v+r-1} a_{i+3u-v}x^{3i-2r} \\ &= C_2^L + x^{3(u-v)}C_2^H, \end{aligned}$$

where the polynomials C_2^L and C_2^H have degrees $3(u-v-1)+r$ and $3v+r-3$, respectively. We also define C_2^{LL}, C_2^{HH} as follows,

$$\begin{aligned} C_2 &= \sum_{i=r}^{u+r-1} a_{i+2u}x^{3i-2r} = \sum_{i=r}^{u-2v} a_{i+2u}x^{3i-2r} + x^{3(u-2v)-r} \sum_{i=1}^{2v+r-1} a_{i+3u-2v}x^{3i-r} \\ &= C_2^{LL} + x^{3(u-2v)-r}C_2^{HH}, \end{aligned}$$

where the polynomials C_2^{LL} and C_2^{HH} have degrees $3(u-2v)-2r$ and $6v+2r-3$, respectively. We recall that $3(u-v) = m-k$, $3(u-2v)-r = m-2k$. Thus, we have

$$\begin{aligned} C^3 &= C_0 - C_1 + C_2 + x^k(C_1 + C_2) + x^{2k}C_2 \pmod{P(x)} \qquad (6) \\ &= C_0 - C_1 + C_2 + x^k(C_1^L + x^{m-k}C_1^H + C_2^L + x^{m-k}C_2^H) + x^{2k}(C_2^{LL} + x^{m-2k}C_2^{HH}) \\ &= C_0 - C_1 + C_2 - (C_1^H + C_2^H + C_2^{HH}) + x^k(C_1^L + C_1^H + C_2^L + C_2^H + C_2^{HH}) + x^{2k}C_2^{LL}. \end{aligned}$$

3) An Example: Let $\mathbb{F}_{3^{13}}$ be a field generated with the irreducible trinomial, $P(x) = x^{13} - x^4 + 1$, with $m = 3u+1 = 3\cdot 4+1 = 13$, $r = 1$ and $k = 3v+1 = 3\cdot 1+1 = 4$. Let $A = \sum_{i=0}^{12} a_i x^i$ be an arbitrary element of that field. Then according with the definitions given above, we have:

$$\begin{aligned} C_0 &= \textstyle\sum_{i=0}^{4} a_i x^{3i} &&= a_0 + a_1x^3 + a_2x^6 + a_3x^9 + a_4x^{12} \\ C_1 &= \textstyle\sum_{i=1}^{4} a_{4+i} x^{3i-1} &&= a_5x^2 + a_6x^5 + a_7x^8 + a_8x^{11} \\ C_2 &= \textstyle\sum_{i=1}^{4} a_{8+i} x^{3i-2} &&= a_9x + a_{10}x^4 + a_{11}x^7 + a_{12}x^{10} \end{aligned}$$

and

$$
\begin{aligned}
C_1^L &= \sum_{i=1}^{u-v} a_{i+u}x^{3i-r} = \sum_{i=1}^{3} a_{4+i}x^{3i-1} = a_5x^2 + a_6x^5 + a_7x^8. \\
C_1^H &= \sum_{i=1}^{v+r-1} a_{i+2u-v}x^{3i-r} = \sum_{i=1}^{1} a_{7+i}x^{3i-1} = a_8x^2. \\
C_2^L &= \sum_{i=r}^{u-v+r-1} a_{i+2u}x^{3i-2r} = \sum_{i=1}^{3} a_{8+i}x^{3i-2} = a_9x + a_{10}x^4 + a_{11}x^7. \\
C_2^H &= \sum_{i=r}^{v+r-1} a_{i+3u-v}x^{3i-2r} = \sum_{i=1}^{1} a_{11+i}x^{3i-2} = a_{12}x; \\
C_2^{LL} &= \sum_{i=r}^{u-2v} a_{i+2u}x^{3i-2r} = \sum_{i=1}^{2} a_{8+i}x^{3i-2} = a_9x + a_{10}x^4; \\
C_2^{HH} &= \sum_{i=1}^{2v+r-1} a_{i+3u-2v}x^{3i-r} = \sum_{i=1}^{2} a_{10+i}x^{3i-2} = a_{11}x^2 + a_{12}x^5.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
C = A^3 &= C_0 - C_1 + C_2 - (C_1^H + C_2^H + C_2^{HH}) + x^k(C_1^L + C_1^H + C_2^L + C_2^H + C_2^{HH}) + x^{2k}C_2^{LL} \\
&= a_0 + (a_9 - a_{12})x + (-a_5 - a_8 - a_{11})x^2 + a_1x^3 + a_{10}x^4 + \\
&\quad +(-a_6 + a_9)x^5 + (a_2 + a_5 + a_8 + a_{11})x^6 + a_{11}x^7 + (-a_7 + a_{10})x^8 + \\
&\quad +(a_3 + a_6 + a_9 + a_{12})x^9 + a_{12}x^{10} + (-a_8 + a_{11})x^{11} + (a_4 + a_7 + a_{10})x^{12}.
\end{aligned}
$$

4) Complexity Analysis: In the following we will assume that the field addition and field subtraction operations can be computed at the same cost in the base field $\mathbb{F}_3$.

The area complexity cost of the field cubing operation can be directly deduced from Eq. (6), along with the definitions of $C_1^L, C_1^H, C_2^L, C_2^H, C_2^{LL}$ and C_2^{HH}, as described next.

We first notice from Eq. (4) that each of the m coefficients of the words C_0, C_1 and C_2 is associated with different powers x^i, for $i = 0, \ldots, m-1$. Hence, the term $C_0 - C_1 + C_2$ of Eq. (6) is free of overlaps, and consequently, it can be implemented without cost in hardware, i.e., with no addition/subtraction operations. Furthermore, it can be noticed that the words C_1^L, C_2^L, C_2^{LL} and C_1^H, C_2^H, C_2^{HH} appear in Eq. (6) once and twice, respectively.

Therefore, the total number of $\mathbb{F}_3$ field adder/subtracter modules required for computing Eq. (6)

is upper bounded by, [7]

$$
\begin{aligned}
\text{\# of adder blocks} &\le |C_1^L| + |C_2^L| + |C_2^{LL}| + 2\left[|C_1^H| + |C_2^H| + |C_2^{HH}|\right] \\
&= (u-v) + (u-v) + (u-2v-r+1) + \\
&\quad +2\left[(v+r-1) + v + (2v+r-1)\right] \\
&= 3u + 4v + 3r - 3 = m + \frac{2}{3}(2k+r) - 3.
\end{aligned}
$$

TABLE II

CANDIDATE REDUCTION TRINOMIALS FOR $\mathbb{F}_{3^m}$, $P(x) = x^m - x^k + 1$ OF DEGREE $m \in [47, 541]$ ENCODED AS $m(k)$, WITH m A PRIME NUMBER. PTR=PREFERRED TRINOMIALS. CRF=CUBE ROOT FRIENDLY TRINOMIALS.

$m(k)$	**Type**	$m(k)$	**Type**	$m(k)$	**Type**	$m(k)$	**Type**
47(32)	CRF	167(71)	PTr	277(97)	PTr	431(365)	CRF
59(17)	PTr	179(59)	PTr	313(187)	CRF	433(262)	CRF
61(7)	PTr	181(37)	PTr	337(25)	PTr	443(188)	PTr
71(20)	PTr	191(71)	PTr	347(65)	PTr	457(67)	PTr
73(1)	PTr	193(64)	PTr	349(223)	CRF	467(92)	PTr
83(32)	PTr	227(11)	PTr	359(122)	PTr	479(221)	PTr
97(16)	PTr	229(79)	PTr	373(25)	PTr	491(11)	PTr
107(11)	PTr	239(5)	PTr	383(80)	PTr	503(35)	PTr
109(13)	PTr	241(88)	PTr	409(136)	PTr	541(145)	PTr
131(47)	PTr	251(26)	PTr	419(26)	PTr		
157(22)	PTr	263(104))	PTr	421(13)	PTr		

Table II shows prime extension degrees $m \in [47, 541]$, for which there exist preferred or cube root friendly irreducible trinomials. In that table we have selected the irreducible trinomials of the form $P(x) = x^m - x^k + 1$, with the smallest possible middle term degree k. In the interval $[47, 541]$ there are a total of 86 prime numbers, but only for 42 of them, a preferred or cube root friendly irreducible trinomial can be found.

B. Irreducible Tetranomials $P(x) = x^m + ax^{k_1} + bx^{k_2} + c$, with $m \equiv k_1 \equiv k_2 \equiv r \pmod 3$

Besides trinomials, the next simple option would be to try to find irreducible tetranomials of the form, $P(x) = x^m + ax^{k_1} + bx^{k_2} + c$, with $a, b, c \in \mathbb{F}_3$. If the restriction, $m \equiv k_1 \equiv k_2 \equiv r$

[7] In the following, the operator $|\cdot|$ represents the length in trits of the term being computed.

$\pmod 3$ hold, we say that $P(x)$ is a *cube root friendly* tetranomial. If additionally the condition $k_1 < \frac{m}{2}$ holds, we say that $P(x)$ is a *preferred* tetranomial. Table III shows some extensions where there exist no irreducible trinomials and thus, the only option is to work with irreducible tetranomials or pentanomials.

Let us write the extension degree m as, $m = 3u + r$, $u \geq 1$ and $k_1 = 3v + r$, $k_2 = 3w + r$, with $0 \leq w < v < u$, with $m \equiv k_1 \equiv k_2 \equiv r \pmod 3$, $r \neq 0$ and $u - 2v \geq 1$.

For this class of irreducible tetranomials, we have,

$$\begin{aligned} x^m &= -ax^{k_1} - bx^{k_2} - c; \\ x^{2m} &= \left(-ax^{k_1} - bx^{k_2} - c\right)^2 = x^{2k_1} - acx^{k_1} + 1 + x^{2k_2} - abx^{(k_1+k_2)} - cbx^{k_2} \end{aligned}$$

Once again, we can use Eq. (5) for computing the field cubing operation,

$$\begin{aligned} C^3 &= C_0 + x^m C_1 + x^{2m} C_2 \\ &= [C_0 - cC_1 + C_2 - ax^{k_1}(C_1 + cC_2) - bx^{k_2}(C_1 + cC_2) + \\ &\quad +x^{2k_1}C_2 + x^{2k_2}C_2 - abx^{k_1+k_2}C_2] \pmod{P(x)}. \end{aligned}$$

Using the same approach employed in Subsection III-A.4, the computational complexity of the above formula can be estimated as,

$$\begin{aligned} \#\text{ of adders} &\leq (u - v) + (u - v) + (u - 2v - r + 1) + 3\left[(v + r - 1) + v + (2v + r - 1)\right] + \\ &\quad +(u - w) + (u - w) + (u - 2w - r + 1) + 3\left[(w + r - 1) + w + (2w + r - 1)\right] + \\ &\quad +(u - v - w - r + 1) + 3\left[v + w + r - 1\right] \\ &= 7u + 10v + 10w + 12r - 12 = 2m + 3(k_1 + k_2) + u + v + w + 4r - 12. \end{aligned}$$

IV. Formulae for Cube Root Computation

A. *Irreducible Trinomials* $P(x) = x^m - x^k + 1$, *with* $m \equiv k \equiv r \pmod 3$

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the trinomial $P(x) = x^m - x^k + 1$, irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m = 3u + r$, $u \geq 1$ and $k = 3v + r$, $0 \leq v < u$, with $m \equiv k \equiv r \pmod 3$ and $r \in [1, 2]$. In [7] it was found that for $r = 1$ we have,

$$x^{2/3} = -x^{u+1} + x^{v+1}; \quad x^{1/3} = x^{2u+1} + x^{u+v+1} + x^{2v+1}.$$

TABLE III

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, GIVING LOW COST CUBINGS AND/OR CUBE ROOTS. THE VALUE $N(M)$ IS LISTED WHERE N IS THE TOTAL NUMBER OF ADDERS/SUBTRACTERS OVER $\mathbb{F}_3$ REQUIRED AND M IS THE NUMBER OF ADDER DELAYS NEEDED FOR COMPUTING THE OPERATION. PT= PREFERRED TETRANOMIALS. EST= EQUALLY SPACED TETRANOMIALS. ESP= EQUALLY SPACED PENTANOMIALS. CRFP = CUBE ROOT FRIENDLY PENTANOMIALS.

Reduction polynomial	Type	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$	$N(M)$ c^3	$N(M)$ $\sqrt[3]{c}$
$x^{41}+x^{24}-x^{17}+x^7-1$	$CRFP$	$x^{39}+x^{31}+x^{23}+x^{22}-x^{14}+x^5$	$-x^{20}+x^{12}+x^3$	125(3)	92(3)
$x^{43}+x^{30}+x^{17}-x^{13}-1$	$CRFP$	$-x^{19}+x^9+x^6$	$x^{38}+x^{28}+x^{25}+x^{18}-x^{15}+x^{12}$	126(3)	89(3)
$x^{100}+x^{75}+x^{50}+x^{25}+1$	ESP	x^{42}	x^{84}	51(1)	51(1)
$x^{160}+x^{120}+x^{80}-x^{40}-1$	ESP	$-x^{67}-x^{27}$	$x^{134}-x^{94}+x^{54}$	224(2)	159(2)
$x^{163}-x^{99}+x^{64}+x^{35}-1$	$CRFP$	$x^{76}+x^{43}+x^{12}$	$x^{152}-x^{119}-x^{88}+x^{86}-x^{55}+x^{24}$	490(3)	355(3)
$x^{233}-x^{141}+x^{92}+x^{49}-1$	$CRFP$	$x^{217}-x^{170}-x^{125}+x^{123}-x^{78}+x^{33}$	$x^{109}+x^{62}+x^{17}$	709(3)	512(3)
$x^{311}+x^{17}+x^{11}+1$	PT	$-x^{104}-x^6-x^4$	$x^{208}-x^{110}-x^{108}+x^{12}-x^{10}+x^8$	750(3)	723(3)
$x^{397}+x^{31}+x^{25}+1$	PT	$x^{265}-x^{143}-x^{141}+x^{21}-x^{19}+x^{17}$	$-x^{133}-x^{11}-x^9$	966(3)	924(3)
$x^{500}+x^{375}+x^{250}+x^{125}+1$	ESP	x^{417}	x^{209}	51(1)	51(1)
$x^{507}+x^{338}+x^{169}-1$	EST	$x^{451}-x^{282}+x^{113}$	$-x^{226}-x^{57}$	451(2)	394(2)

whereas for $r=2$ we have,

$$x^{1/3}=-x^{u+1}+x^{v+1};\quad x^{2/3}=x^{2u+2}+x^{u+v+2}+x^{2v+2}.$$

From above results, it follows that when dealing with irreducible trinomials of this kind, we do not need to perform the reduction modulo $P(x)$ indicated in Eq. (1).

In the following we will apply Barreto's trick to the case of irreducible tetranomials.

B. Tetranomials

Let $\mathbb{F}_{3^m}$ be a ternary field generated by the tetranomial $P(x)=x^m+ax^{k_1}+bx^{k_2}+c$ irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m=3u+r$, $u\geq 1$ and $k_1=3v+r$, $k_2=3w+r$, with $0\leq w<v<u$, and $m\equiv k_1\equiv k_2\equiv r \pmod 3$, $r\neq 0$. Once again, using Eq. (1) one can compute a cube root by finding the per-field constants $x^{1/3}$ and $x^{2/3}$.

1) case $r=1$: For $r=1$, we observe that $-c=x^m+ax^{k_1}+bx^{k_2}$, which implies

$$-cx^2=x^2(x^m+ax^{k_1}+bx^{k_2})=x^{3(u+1)}+ax^{3(v+1)}+bx^{3(w+1)}.$$

Hence, $x^{2/3} = -cx^{u+1} - acx^{v+1} - bcx^{w+1}$. From this we deduce that

$$x^{4/3} = x^{2(u+1)} - ax^{u+v+2} + x^{2(v+1)} + x^{2(w+1)} - bx^{u+w+2} - abx^{v+w+2},$$

and thus dividing both sides of the above equation by x we get

$$x^{1/3} = x^{2u+1} - ax^{u+v+1} - bx^{u+w+1} + x^{2v+1} + x^{2w+1} - abx^{v+w+1}.$$

2) case $r = 2$: For $r = 2$, we observe that $-c = x^m + ax^{k_1} + bx^{k_2}$, which implies,

$$-cx = x(x^m + ax^{k_1} + bx^{k_2}) = x^{3(u+1)} + ax^{3(v+1)} + bx^{3(w+1)}$$

Hence, $x^{1/3} = -cx^{u+1} - acx^{v+1} - bcx^{w+1}$. We can directly obtain $x^{2/3}$ by computing,

$$\begin{aligned} x^{2/3} = (x^{1/3})^2 &= (-cx^{u+1} - acx^{v+1} - bcx^{w+1})^2 \\ &= x^{2(u+1)} - ax^{u+v+2} + x^{2(v+1)} + x^{2(w+1)} - bx^{u+w+2} - abx^{v+w+2}. \end{aligned}$$

From the above results, it turns out that for this class of tetranomials, we do not need to carry out the reduction process indicated in Eq. (1).

C. Pentanomials

Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible pentanomial of the form, $P(x) = x^m - ax^{m-d} + x^{m-2d} + ax^d - 1$, with $a \neq 0$, and where m is an odd prime number that can be written as, $m = 3u + r$, where $m \equiv r \pmod 3$, $r \neq 0$, and $d = 3v + r$ is a positive integer so that $d < \lceil \frac{m}{2} \rceil$. Then, $x^m = ax^{m-d} - x^{m-2d} - ax^d + 1$, which implies,

$$\begin{aligned} x^{m+d} &= ax^m - x^{m-d} - ax^{2d} + x^d \\ &= x^{m-d} - ax^{m-2d} - x^d + a - x^{m-d} - ax^{2d} + x^d = -ax^{m-2d} - ax^{2d} + a; \\ x^{m+d+1} &= -ax^{2d+1} - ax^{m-2d+1} + ax; \\ x^{m+d+2} &= -ax^{2d+2} - ax^{m-2d+2} + ax^2. \end{aligned} \tag{7}$$

It is noticed that, $m + d \equiv 2d \equiv m - 2d \equiv -r \pmod 3$. In the following, we distinguish two cases.

1) case $r=1$: If $r=1$, from Eq. (7) we can write, $\sqrt[3]{x} = ax^{\frac{m+d+1}{3}} + x^{\frac{2d+1}{3}} + x^{\frac{m-2d+1}{3}}$, which implies,

$$\begin{aligned}
\sqrt[3]{x^2} &= \left(ax^{\frac{m+d+1}{3}} + x^{\frac{2d+1}{3}} + x^{\frac{m-2d+1}{3}}\right)^2 \\
&= x^{2\frac{m+d+1}{3}} + x^{2\frac{2d+1}{3}} + x^{2\frac{m-2d+1}{3}} - ax^{\frac{m+3d+2}{3}} - ax^{\frac{2m-d+2}{3}} - x^{\frac{m+2}{3}}.
\end{aligned}$$

2) case $r=2$: If $r=2$, from Eq. (7) we can write, $\sqrt[3]{x^2} = ax^{\frac{m+d+2}{3}} + x^{\frac{2d+2}{3}} + x^{\frac{m-2d+2}{3}}$. Furthermore, we have,

$$\begin{aligned}
\sqrt[3]{x} &= \sqrt[3]{x^2}\left(x^{\frac{m+d-1}{3}} + x^{\frac{2d-1}{3}} + x^{\frac{m-2d-1}{3}}\right) \\
&= (ax^{\frac{m+d+2}{3}} + x^{a\frac{2d+2}{3}} + x^{\frac{m-2d+2}{3}})(x^{\frac{m+d-1}{3}} + x^{\frac{2d-1}{3}} + x^{\frac{m-2d-1}{3}}) \\
&= x^{\frac{2m+2d+1}{3}} - ax^{\frac{m+3d+1}{3}} - ax^{\frac{2m-d+1}{3}} + x^{\frac{4d+1}{3}} - x^{\frac{m+1}{3}} + x^{\frac{2m-4d+1}{3}}.
\end{aligned}$$

We stress that the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to this class of pentanomials force us to carry out the reduction post-computation indicated in Eq. (1).

D. Existence of Cube Root Friendly Fewnomials

Algorithms presented in the previous section depend on the existence of irreducible polynomials of a special form. From the results of [25] it follows that if $m \equiv 5, 7 \pmod{12}$, then there is no irreducible trinomial $P(x) = x^m - x^k + 1$, with $m \equiv k \equiv r \pmod 3$. In fact one can use methods of [4], [13], [25] to show that if $m \equiv 5, 7 \pmod{12}$, then there is no irreducible polynomial $P(x) = x^m + a_1x^{k_1} + \cdots + a_lx^{k_l} + 1$ such that $m \equiv k_1 \equiv \cdots \equiv k_l \pmod 3$. Thus in this case one has to look for other types of polynomials which are cube root friendly and yield efficient algorithm for cube root computation. The family of pentanomials suggested in the previous Section can serve as a candidate for cube root friendly polynomials.

V. EQUALLY SPACED POLYNOMIALS

Irreducible Equally Spaced Polynomials have the same space separation between two consecutive non-zero coefficients. They can be defined as

$$p(x) = x^m + p_{(k-1)d}x^{(k-1)d} + \cdots + p_{2d}x^{2d} + p_dx^d + p_0 \ , \tag{8}$$

where $m = kd$ and $p_{id} \in \mathbb{F}_3^*$ for $i = 0, 1, 2, \ldots, k-1$. The ESP specializes to the all-one-polynomials when $d = 1$, i.e., $p(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$, and to the equally spaced trinomials when $d = \frac{m}{2}$, i.e., $p(x) = x^m + p_{\frac{m}{2}} x^{\frac{m}{2}} + p_0$.

In the rest of this Section we give a complete classification of equally spaced tetranomial and pentanomials that are irreducible over $\mathbb{F}_3$, and then we show how one can compute cube roots in the extension ternary fields constructed from some classes of these polynomials. In particular, we indicate a family of pentanomials where both of the associated constants, namely, $\sqrt[3]{x}$ and $\sqrt[3]{x^2}$, happen to have an ideal Hamming weight of one.

A. Classification of irreducible equally spaced tetranomials and pentanomials over $\mathbb{F}_3$

The following theorem is the main tool in our classification. Notice that order of a polynomial $f(x) \in \mathbb{F}_q[x]$ whose constant term is nonzero is the least positive integer e such that $f(x)|x^e - 1$ in $\mathbb{F}_q[x]$.

Theorem 5.1: [20, Theorem 3.9] Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e over $\mathbb{F}_q$, and let t be a positive integer. Then $f(x^t)$ is irreducible over $\mathbb{F}_q$ if and only if

(i) $\gcd(t, \frac{q^m-1}{e}) = 1$;

(ii) each prime factor of t divides e; and

(iii) if $4 \mid t$, then $4 \mid q^m - 1$.

Corollary 5.2: [8] An equally spaced tetranomial $f(x)$ over $\mathbb{F}_3$ is irreducible if and only if $f(x)$ satisfies one of the following:

- $f(x) = x^{3d} + x^{2d} + x^d - 1$ or $x^{3d} - x^{2d} - x^d - 1$ and $d = 13^i$ for some $i \geq 0$,
- $f(x) = x^{3d} + x^{2d} - x^d + 1$ or $x^{3d} - x^{2d} + x^d + 1$ and $d = 2^i 13^j$ where $i = 0, 1$ and $j \geq 0$.

Proof: The only irreducible tetranomials of degree 3 over $\mathbb{F}_3$ are $x^3 + x^2 + x - 1, x^3 - x^2 - x - 1, x^3 + x^2 - x + 1, x^3 - x^2 + x + 1$ whose orders in $\mathbb{F}_3[x]$ are $13, 13, 26$ and 26, respectively. Now the claim follows from the above theorem. ■

Similarly we can prove the following for pentanomials.

[8] This result was not in the first draft of the paper submitted to the journal. In the first round of the reviews, one of the anonymous reviewers conjectured that irreducible equally spaced tetranomials over $\mathbb{F}_{3^m}$ exist iff $m = 3 \cdot 13^i$, for $i = 0, 1, 2, \ldots$. Now this result gives a complete answer to that conjecture.

Corollary 5.3: An equally spaced pentanomial $f(x)$ over $\mathbb{F}_3$ is irreducible if and only if $f(x)$ satisfies one of the following:

- $f(x) = x^{4d} + x^{3d} + x^{2d} + x^d + 1$ or $x^{4d} - x^{3d} + x^{2d} - x^d + 1$ and $d = 5^i$ for some $i \geq 0$,
- $f(x)$ is one of the four polynomials $x^{4d} - x^{3d} - x^{2d} + x^d - 1$, $x^{4d} + x^{3d} + x^{2d} - x^d - 1$, $x^{4d} + x^{3d} - x^{2d} - x^d - 1$, $x^{4d} - x^{3d} + x^{2d} + x^d - 1$ where $d = 2^i 5^j$ for some $i, j \geq 0$.

Proof: The only irreducible pentanomials of degree 4 over $\mathbb{F}_3$ are $x^4+x^3+x^2+x+1, x^4-x^3+x^2-x+1, x^4-x^3-x^2+x-1, x^4+x^3+x^2-x-1, x^4+x^3-x^2-x-1, x^4-x^3+x^2+x-1$ whose orders in $\mathbb{F}_3[x]$ are $5, 10, 80, 80, 80$ and 80, respectively. Now the claim follows from the above theorem.

■

B. Equally Spaced Tetranomials

Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible equally spaced tetranomial of the form, $p(x) = x^m + ax^{2d} + x^d - a$, where $m = 3d$, $a \in \mathbb{F}_3^*$. Then, we have that $x^m = -ax^{2d} - x^d + a$, which implies,

$$\begin{aligned} x^{m+d} &= -ax^{3d} - x^{2d} + ax^d \\ &= x^{2d} + ax^d - 1 - x^{2d} + ax^d = -ax^d - 1; \\ x^{m+d+1} &= -ax^{d+1} - x; \\ x^{m+d+2} &= -ax^{d+2} - x^2. \end{aligned} \tag{9}$$

It is noticed that $m + d = 4d \equiv d \pmod 3$. In the following, we distinguish two cases.

1) Case $d \equiv 1 \pmod 3$: From the last equality of Eq. (9), we have, $x^2 = -ax^{d+2} - x^{m+d+2}$, and since $d \equiv 1 \pmod 3$, we have, $m+d+2 \equiv 4d+2 \equiv 0 \pmod 3$, and $d+2 \equiv 0 \pmod 3$. Therefore, we can write, $\sqrt[3]{x^2} = -(ax^{\frac{d+2}{3}} + x^{\frac{4d+2}{3}})$. Moreover, since $x = -ax^{d+1} - x^{4d+1}$, it implies that,

$$\sqrt[3]{x} = -\sqrt[3]{x^2}(ax^{\frac{d-1}{3}} + x^{\frac{4d-1}{3}}) = (ax^{\frac{d+2}{3}} + x^{\frac{4d+2}{3}})(ax^{\frac{d-1}{3}} + x^{\frac{4d-1}{3}}).$$

2) Case $d \equiv 2 \pmod 3$: From the second last equality of Eq. (9), we have, $x = -ax^{d+1} - x^{m+d+1}$. Therefore, $\sqrt[3]{x} = -ax^{\frac{d+1}{3}} - x^{\frac{4d+1}{3}}$ and

$$\sqrt[3]{x^2} = (-ax^{\frac{d+1}{3}} - x^{\frac{4d+1}{3}})^2 = x^{2\frac{d+1}{3}} - ax^{\frac{5d+2}{3}} + x^{2\frac{4d+1}{3}}.$$

Furthermore, the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to equally spaced tetranomials, force us to have a reduction process post-computation. Concrete examples of irreducible equally spaced tetranomials can be found in Table III.

C. Equally Spaced Pentanomials

Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible equally spaced pentanomial of the form, $p(x) = x^m + ax^{3d} + x^{2d} + cx^d + ac$, where $m = 4d$ and where d is a positive integer not a multiple of 3. Then, $x^m = -ax^{3d} - x^{2d} - cx^d - ac$, which implies,

$$\begin{aligned} x^{m+d} &= -ax^{4d} - x^{3d} - cx^{2d} - acx^d \\ &= x^{3d} + ax^{2d} + acx^d + c - x^{3d} - cx^{2d} - acx^d = (a-c)x^{2d} + c; \\ x^{m+d+1} &= (a-c)x^{2d+1} + cx; \\ x^{m+d+2} &= (a-c)x^{2d+2} + cx^2. \end{aligned} \tag{10}$$

It is noticed that $m + d = 5d \equiv 2d \pmod 3$. In the following, we distinguish two cases.

1) Case $d \equiv 1 \pmod 3$: If $d \equiv 1 \pmod 3$, then from the second last equality of Eq. (10), we have, $x = (1-ac)x^{2d+1} + cx^{m+d+1}$. Therefore, $\sqrt[3]{x} = (1-ac)x^{\frac{2d+1}{3}} + cx^{\frac{5d+1}{3}}$ and

$$\sqrt[3]{x^2} = \left((1-ac)x^{\frac{2d+1}{3}} + cx^{\frac{5d+1}{3}}\right)^2 = (ac-1)x^{2\frac{2d+1}{3}} + (a-c)x^{\frac{7d+2}{3}} + x^{2\frac{5d+1}{3}}.$$

2) Case $d \equiv 2 \pmod 3$: If $d \equiv 2 \pmod 3$, then from the last equality of Eq. (10), we have, $x^2 = (1-ac)x^{2d+2} + cx^{m+d+2}$. Therefore, $\sqrt[3]{x^2} = (1-ac)x^{\frac{2d+2}{3}} + cx^{\frac{5d+2}{3}}$, whereas,

$$\begin{aligned} \sqrt[3]{x} &= \sqrt[3]{x^2}((1-ac)x^{\frac{2d-1}{3}} + cx^{\frac{5d-1}{3}}) \\ &= \left((1-ac)x^{\frac{2d+2}{3}} + cx^{\frac{5d+2}{3}}\right)\left((1-ac)x^{\frac{2d-1}{3}} + cx^{\frac{5d-1}{3}}\right) \\ &= (ac-1)x^{\frac{4d+1}{3}} + (a-c)x^{\frac{7d+1}{3}} + x^{\frac{10d+1}{3}}. \end{aligned}$$

Notice that by selecting $a = c$, one will get the pleasant case where the Hamming weight of both $\sqrt[3]{x}$ and $\sqrt[3]{x^2}$, is equal to one. Unfortunately, although irreducible equally spaced pentanomials are more abundant than their tetranomials counterpart, they are still very rare. For $m \leq 1000$, there are only 20 extensions m where at least one irreducible equally spaced pentanomial exists. Concrete examples of irreducible equally spaced pentanomials can be found in Table III. It is noted that the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to this class of pentanomials, force us to have a reduction process post-computation indicated in Eq. (1).

VI. Ring mapping and root computation

One approach proposed in the literature for carrying out the arithmetic of the finite field $\mathbb{F}_{p^m}$ is the embedding of $\mathbb{F}_{p^m}$ in a larger ring and performing all the arithmetic operations in the ring and projecting the result back to the original field. If ring is chosen properly, then field arithmetic can be sped up. This idea is known as the ring mapping. In the following example taken from [24] we briefly explain this technique in the context of squaring and square-root taking in the binary fields (The author in [24] credits this example to Ito and Tsujii [19].).

Suppose for some m, $P(x) = x^m + x^{m-1} + \ldots + x + 1$ is irreducible over $\mathbb{F}_2$ (notice that m has to be an even number since otherwise $P(1) = 0$ and hence $P(x)$ is not irreducible). Then, we have $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(P(x))$. Now $x^{m+1} + 1 = (x + 1)P(x)$. This implies that

$$R_2 = \frac{\mathbb{F}_2[x]}{(x^{m+1} + 1)} \cong \mathbb{F}_{2^m} \times \mathbb{F}_2.$$

Regarding $\mathbb{F}_{2^m}$ and R_2 as vector spaces over the binary field $\mathbb{F}_2$,

$$\{1, x, x^2, \ldots, x^{m-1}\}$$

and

$$\{1, x, x^2, \ldots, x^{m-1}, x^m\}$$

are standard bases for $\mathbb{F}_{2^m}$ and R_2 over $\mathbb{F}_2$, respectively. Squaring and square-root taking are very simple in R_2. If $b = a_m x^m + \ldots + a_2 x^2 + a_1 x + a_0$ is an element of R_2, then from Eq. (2) and the fact that $x^{m+1} = 1$ in R_2 it follows that

$$b^2 = a_{m/2} x^m + a_m x^{m-1} + a_{m/2-1} x^{m-2} + a_{m-1} x^{m-3} + \ldots + a_2 x^4 + a_{m/2+2} x^3 + a_1 x^2 + a_{m/2+1} x + a_0.$$

Since square-root taking is just the inverse operation of squaring, thus one can take the root of an element easily too. Further information on how this can be used to square or take the square root of an element of $\mathbb{F}_{2^m}$ can be found in [24].

In [24], it has been mentioned that the above idea can be generalized to other finite fields. Here we show the details of applying the above idea to cubing and cube root taking.

Now suppose for some m, $P(x) = x^m + x^{m-1} + \ldots + x + 1$ is irreducible over $\mathbb{F}_3$ (this implies that $m \neq 2 \pmod 3$ (see [24])). Then $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(P(x))$. We have $x^{m+1} - 1 = (x-1)P(x)$. Thus

$$R_3 = \frac{\mathbb{F}_3[x]}{(x^{m+1}-1)} \cong \mathbb{F}_{3^m} \times \mathbb{F}_3.$$

The same as before $\{1, x, x^2, \ldots, x^{m-1}\}$ and $\{1, x, x^2, \ldots, x^{m-1}, x^m\}$ are standard bases for $\mathbb{F}_{3^m}$ and R_3 over $\mathbb{F}_3$, respectively. Now if we assume that $m \equiv 1 \pmod 3$, then from $x^{m+1} = 1$ in R_3, it follows that $x^{\frac{1}{3}} = x^{\frac{m+2}{3}}$ and $x^{\frac{2}{3}} = x^{2\frac{m+2}{3}}$. Thus if $b = a_m x^m + \ldots + a_2 x^2 + a_1 x + a_0$ is an element of R_3, then from Eq. (1), it follows that

$$\begin{aligned} b^{1/3} = \quad & a_{m-2}x^m + a_{m-5}x^{m-1} + a_{m-8}x^{m-2} + \ldots + a_2 x^{(2m+4)/3} \\ + \quad & a_m x^{(2m+1)/3} + +a_{m-3}x^{(2m-2)/3} + \ldots + a_1 x^{(m+2)/3} \\ + \quad & a_{m-1}x^{(m-1)/3} + \ldots + a_3 x + a_0. \end{aligned}$$

Similar formula can be obtained for the case when m is divisible by 3. For how one can move back and forth from $\mathbb{F}_{3^m}$ to R_3 see [24]. Notice that one drawback of the above method is that the embedding mentioned above works just for composite m while most of the time we are interested in prime m. One possible alternative strategy when m is such that the above method does not work and there is no preferred irreducible trinomial of degree m, is to look for trinomials or tetranomials of preferred shape which have degrees higher than m and are divisible by an irreducible polynomial of degree m. If such a trinomial or tetranomial exists, then one can use the idea of ring mapping to accelerate the root computation. For further information about this method we refer the interested reader to [14] and references therein.

VII. Applications to Pairing-Based Cryptography

Let E be a supersingular elliptic curve defined by the equation $E : y^2 = x^3 - x + b$, with $b \in \{-1, 1\}$. Then the set of $\mathbb{F}_{3^m}$-rational points on E is defined as [17], [26],

$$E(\mathbb{F}_{3^m}) = \{(x, y) \in \mathbb{F}_{3^m} \times \mathbb{F}_{3^m} : y^2 - x^3 + x - b = 0\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity. It is known that $E(\mathbb{F}_{3^m})$ forms an additive Abelian group with respect to the elliptic point addition operation. The number of rational points in $E(\mathbb{F}_{3^m})$, denoted $\#E(\mathbb{F}_{3^m})$, is called the order of E over $\mathbb{F}_{3^m}$, which in the case of this class of elliptic curves is given as $N = 3^m + 1 + \mu b 3^{(m+1)/2}$, with

$$\mu = \begin{cases} +1 & \text{if } m \equiv 1,\, 11 \pmod{12}, \\ -1 & \text{if } m \equiv 5,\, 7 \pmod{12}. \end{cases}$$

Let ℓ be a large prime factor of N, so that $\ell^2 \nmid N$. Then, we can write $N = i \cdot \ell$, where i is a small positive integer. A subgroup of order ℓ is known as an ℓ-torsion group, denoted $E(\mathbb{F}_{3^m})[\ell]$. If P is a rational point on E, then $[i]P$, the point resulting from adding i copies of P, belongs to the ℓ-torsion subgroup. The embedding degree of E with respect to ℓ is the smallest positive integer k such that $\ell | q^k - 1$. For the specific case of supersingular curves over $\mathbb{F}_{3^m}$, we have $k = 6$, and the modified Tate pairing of order ℓ is defined as the bilinear map, $\hat{e} : E(\mathbb{F}_{3^m})[\ell] \times E(\mathbb{F}_{3^m})[\ell] \longrightarrow \mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^\ell$.

Assuming that $\frac{m-1}{2}$ is an even integer, the total number of $\mathbb{F}_{3^m}$ field operations required for computing the Tate pairing using the algorithm described in [12] is of $25\frac{m-1}{4} + 6$, $82\frac{m-1}{4} + 8$, m and $m + 1$ multiplications, additions, cubings and cube roots, respectively. Additionally, in order to obtain a unique representative of the coset $(\mathbb{F}^*_{3^{6m}})^\ell$, one needs to perform a final exponentiation operation by raising the computed value $\hat{e}(P, Q)$ to the $M = \left(3^{3m} - 1\right) \cdot (3^m + 1) \cdot \left(3^m + 1 - \mu b 3^{(m+1)/2}\right)$ power. As described in [10], the cost of the final exponentiation is of $3m + 3$ field cubing operations plus 73 field multiplications, one field inversion and about $3m + 175$ field additions. Furthermore, authors in [11] describe an alternative procedure able to achieve a faster computation of the final exponentiation by reducing the number of required addition operations and by trading $3m + 3$ field cubing operations with $3m - 3$ field cube root calculations.

TABLE IV
REDUCTION POLYNOMIALS THAT YIELD LOW COST CUBINGS AND/OR CUBE ROOTS FOR SUPERSINGULAR ELLIPTIC CURVES DEFINED BY THE EQUATION $y^2 = x^3 - x + b$, WITH LARGE ℓ-TORSION SUBGROUPS OVER $\mathbb{F}_{3^m}$, WITH m A PRIME NUMBER IN THE RANGE $[47, 541]$

m	b	μ	$\#E(\mathbb{F}_{3^m})$	ℓ	recommended reduction polynomial
47	-1	1	$283r$	$\left(3^{47} - 3^{24} + 1\right)/283$	$x^{47} - x^{32} + 1$
53	-1	-1	$48973r$	$\left(3^{53} + 3^{27} + 1\right)/48973$	$x^{53} + x^{42} + x^{31} - x^{11} - 1$
79	-1	-1	r	$\left(3^{79} + 3^{40} + 1\right)$	$x^{79} - x^{51} + x^{28} + x^{23} - 1$
97	1	1	$7r$	$\left(3^{97} + 3^{49} + 1\right)/7$	$x^{97} - x^{16} + 1$
163	-1	-1	r	$\left(3^{163} + 3^{82} + 1\right)$	$x^{163} - x^{99} + x^{64} + x^{35} - 1$
167	1	1	$7r$	$\left(3^{167} + 3^{84} + 1\right)/7$	$x^{167} - x^{71} + 1$
193	-1	1	r	$\left(3^{193} - 3^{97} + 1\right)$	$x^{193} - x^{64} + 1$
239	-1	1	r	$\left(3^{239} - 3^{120} + 1\right)$	$x^{239} - x^{5} + 1$
317	-1	-1	r	$\left(3^{317} + 3^{159} + 1\right)$	$x^{317} - x^{267} + x^{217} + x^{50} - 1$
353	-1	-1	r	$\left(3^{353} + 3^{177} + 1\right)$	$x^{353} - x^{249} + x^{145} + x^{104} - 1$
509	1	-1	$7r$	$\left(3^{509} - 3^{255} + 1\right)/7$	$x^{509} + x^{294} - x^{215} + x^{79} - 1$

From the above description of the Tate pairing arithmetic operation costs, one can conclude that efficient hardware and/or software implementations of the Tate pairing over $E(\mathbb{F}_{3^m})$ supersingular curves require the usage of cube root friendly reduction polynomials. Otherwise the computational effort needed for calculating cubing and cube root operations over $\mathbb{F}_{3^m}$ may become comparable to the field multiplication cost. On the other hand, it is desirable to have ℓ as large as possible so that the discrete logarithm problem associated to pairing-based cryptography remains as a hard computational problem. Hence, in the context of pairing computation an important design task consists of finding extension degrees m where N has large prime factors ℓ and where a cube root friendly irreducible polynomial can be found.

We list in Table IV, cube root friendly reduction polynomial for a selection of prime extension degrees $m \in [47, 541]$ that enjoy large ℓ-torsion subgroups. For a given extension degree m, we look first for preferred trinomials or cube root friendly trinomials. Otherwise, if we cannot find such irreducible trinomials, we try to find preferred tetranomials or pentanomials as the ones defined in Section IV. [9]

[9]The equations for $\sqrt[3]{x}$ and $\sqrt[3]{x^2}$ associated to each one of the polynomials listed in Table IV can be found in Appendix A.

VIII. Conclusion

In this paper we investigated the computational cost associated with field cubing and cube root computation in ternary extension fields $\mathbb{F}_{3^m}$, generated by special classes of irreducible polynomials. We presented cube root friendly families of irreducible trinomials, tetranomials and pentanomials that exist for most prime extension degrees m, which are the cases of interest in modern cryptographic applications. More specifically, in the range $[47, 541]$, there exist a total of 86 prime numbers. Using the irreducible trinomials, tetranomials and pentanomials discussed in Section IV, we are able to propose a reduction polynomial for all the 86 instances except for $m = 89, 149, 151, 283, 449, 463, 521$. The proposed polynomials are listed in Appendix A, along with the corresponding values of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$.

Acknowledgment

The authors would like to thank Darrel Hankerson, Jean-Luc Beuchat and the anonymous referees for their valuable comments that greatly helped to improve the presentation of this paper. The second author acknowledges support from CONACyT through the CONACyT project number 90543-Y.

References

[1] O. Ahmadi, D. Hankerson, and A. Menezes. Formulas for cube roots in $\mathbb{F}_{3^m}$. *Discrete Applied Mathematics*, 155(3):260–270, 2007.

[2] O. Ahmadi, D. Hankerson, and A. Menezes. Software implementation of arithmetic in $\mathbb{F}_{3^m}$. In Claude Carlet and Berk Sunar, editors, *WAIFI*, volume 4547 of *Lecture Notes in Computer Science*, pages 85–102. Springer, 2007.

[3] O. Ahmadi, D. Hankerson, and F. Rodríguez-Henríquez. Parallel formulations of scalar multiplication on Koblitz curves. *Special Issue on Cryptography in Computer System Security Journal of Universal Computer Science*, 14:481–504, 2008.

[4] O. Ahmadi and A. Menezes. Irreducible polynomials of maximum weight. *Util. Math.*, 72:111–123, 2007.

[5] R. Avanzi. Another look at square roots (and other less common operations) in fields of even characteristic. In C. M. Adams, A. Miri, and M. J. Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 138–154. Springer, 2007.

[6] R. Avanzi. Another look at square roots and traces (and quadratic equations) in fields of even characteristic. Cryptology ePrint Archive, Report 2007/103, 2007. `http://eprint.iacr.org/`.

[7] P.S.L.M. Barreto. A note on efficient computation of cube roots in characteristic 3. Cryptology ePrint Archive, Report 2004/305, 2004. `http://eprint.iacr.org/`.

[8] P.S.L.M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In M. Yung, editor, *Advances in Cryptology – CRYPTO 2002*, number 2442 in Lecture Notes in Computer Science, pages 354–368. Springer, 2002.

[9] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, and F. Rodríguez-Henríquez. A comparison between hardware accelerators for the modified tate pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$. In S.D. Galbraith and K.G. Paterson, editors, *Pairing 2008*, number 5209 in Lecture Notes in Computer Science, pages 297–315. Springer, 2008.

[10] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase, and T. Takagi. Algorithms and arithmetic operators for computing the η_t pairing in characteristic three. *IEEE Transactions on Computers – Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis*, 57(11):1454–1468, November 2008.

[11] J.-L. Beuchat, J. Detrey, N. Estibals, E. Okamoto, and F. Rodríguez-Henríquez. Fast architectures for the η_T pairing over small-characteristic supersingular elliptic curves. Cryptology ePrint Archive, Report 2009/398, 2009.

[12] J.-L. Beuchat, E. López-Trejo, L. Martínez-Ramos, S. Mitsunari, and F. Rodríguez-Henríquez. Multi-core implementation of the Tate pairing over supersingular elliptic curves. In J.A. Garay, A. Miyaji, and A. Otsuka, editors, *Cryptology and Network Security – CANS 2009*, number 5888 in Lecture Notes in Computer Science, pages 413–432. Springer, 2009.

[13] A.W. Bluher. A Swan-like theorem. *Finite Fields Appl.*, 12(1):128–138, 2006.

[14] C. Doche. Redundant trinomials for finite fields of characteristic 2. In C. Boyd and J.-M. González Nieto, editors, *Information Security and Privacy, 10th Australasian Conference, ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 122–133. Springer, 2005.

[15] K. Fong, D. Hankerson, J. López, and A. Menezes. Field inversion and point halving revisited. *IEEE Trans. Computers*, 53(8):1047–1059, 2004.

[16] D. Hankerson, A. Menezes, and M. Scott. *Software Implementation of Pairings*, chapter 12. Cryptology and Information Security. IOS Press, to appear.

[17] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Cryptography*. Springer-Verlag, New York, 2004.

[18] IEEE standards documents. *IEEE P1363: Standard specifications for public key cryptography. Draft Version D18*. IEEE, November 2004. `http://grouper.ieee.org/groups/1363/`.

[19] B. Ito and S. Tsujii. Structure of a parallel multipliers for a class of fields GF(2^m) using normal bases. *Information and Computers*, 83:21–40, 1989.

[20] A. Menezes, I. Blake, S. Gao, R. Mullin, S. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. Kluwer, 1993.

[21] D. Panairo and D. Thompson. Efficient pth root computations in finite fields of characteristic p. *Designs, Codes and Cryptography*, To appear in 2009.

[22] F. Rodríguez-Henríquez, G. Morales-Luna, and J. López. Low-complexity bit-parallel square root computation over GF(2^m) for all trinomials. *IEEE Trans. Computers*, 57(4):472–480, 2008.

[23] M. Scott. Optimal irreducible polynomials for GF(2^m) arithmetic. Cryptology ePrint Archive, Report 2007/192, 2007. `http://eprint.iacr.org/`.

[24] J.H. Silverman. Fast multiplication in finite fields GF(2^{n}). In Çetin Kaya Koç and Christof Paar, editors, *CHES*, volume 1717 of *Lecture Notes in Computer Science*, pages 122–134. Springer, 1999.

[25] J. von zur Gathen. Irreducible trinomials over finite fields. *Math. Comp.*, 72(244):1987–2000 (electronic), 2003.

[26] L.C. Washington. *Elliptic Curves – Number Theory and Cryptography*. CRC Press, 2nd edition, 2008.

APPENDIX A

In Tables V and VI we list the reduction polynomials for $\mathbb{F}_{3^m}$ yielding low cost cubings and/or cube roots, with m a prime number in the range $[47, 307]$ and $[311, 541]$, respectively. We also

TABLE V

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, YIELDING LOW COST CUBINGS AND/OR CUBE ROOTS, WITH m A PRIME NUMBER IN THE RANGE $[47, 307]$

Reduction polynomial	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$
$x^{47} - x^{32} + 1$	$-x^{16} + x^{11}$	$x^{32} + x^{27} + x^{22}$
$x^{53} + x^{42} + x^{31} - x^{11} - 1$	$x^{43} + x^{32} + x^{29} + x^{21} - x^{18} + x^{15}$	$-x^{22} + x^{11} + x^{8}$
$x^{59} - x^{17} + 1$	$-x^{20} + x^{6}$	$x^{40} + x^{26} + x^{12}$
$x^{61} - x^{7} + 1$	$x^{41} + x^{23} + x^{5}$	$-x^{21} + x^{3}$
$x^{67} - x^{45} + x^{23} + x^{22} - 1$	$x^{30} + x^{15} + x^{8}$	$x^{60} - x^{45} - x^{38} + x^{30} - x^{23} + x^{16}$
$x^{71} - x^{20} + 1$	$-x^{24} + x^{7}$	$x^{48} + x^{31} + x^{14}$
$x^{73} - x + 1$	$x^{49} + x^{25} + x$	$-x^{25} + x$
$x^{79} - x^{51} + x^{28} + x^{23} - 1$	$x^{36} + x^{19} + x^{8}$	$x^{72} - x^{55} - x^{44} + x^{38} - x^{27} + x^{16}$
$x^{83} - x^{32} + 1$	$-x^{28} + x^{11}$	$x^{56} + x^{39} + x^{22}$
$x^{97} - x^{16} + 1$	$x^{65} + x^{38} + x^{11}$	$-x^{33} + x^{6}$
$x^{101} - x^{81} + x^{61} + x^{20} - 1$	$x^{81} - x^{61} - x^{54} + x^{41} - x^{34} + x^{27}$	$x^{41} + x^{21} + x^{14}$
$x^{103} + x^{54} - x^{49} + x^{5} - 1$	$-x^{51} + x^{33} + x^{2}$	$x^{102} + x^{84} + x^{66} + x^{53} - x^{35} + x^{4}$
$x^{107} - x^{11} + 1$	$-x^{36} + x^{4}$	$x^{72} + x^{40} + x^{8}$
$x^{109} - x^{13} + 1$	$x^{73} + x^{41} + x^{9}$	$-x^{37} + x^{5}$
$x^{113} - x^{87} + x^{61} + x^{26} - 1$	$x^{93} - x^{67} - x^{64} + x^{41} - x^{38} + x^{35}$	$x^{47} + x^{21} + x^{18}$
$x^{127} - x^{111} + x^{95} + x^{16} - 1$	$x^{48} + x^{32} + x^{11}$	$x^{96} - x^{80} + x^{64} - x^{59} - x^{43} + x^{22}$
$x^{131} - x^{83} + 1$	$-x^{44} + x^{28}$	$x^{88} + x^{72} + x^{56}$
$x^{137} + x^{72} - x^{65} + x^{7} - 1$	$x^{135} + x^{111} + x^{87} + x^{70} - x^{46} + x^{5}$	$-x^{68} + x^{44} + x^{3}$
$x^{139} + x^{120} + x^{101} - x^{19} - 1$	$-x^{53} + x^{34} + x^{13}$	$x^{106} + x^{87} + x^{68} + x^{66} - x^{47} + x^{26}$
$x^{157} - x^{22} + 1$	$x^{105} + x^{60} + x^{15}$	$-x^{53} + x^{8}$
$x^{163} - x^{99} + x^{64} + x^{35} - 1$	$x^{76} + x^{43} + x^{12}$	$x^{152} - x^{119} - x^{88} + x^{86} - x^{55} + x^{24}$
$x^{167} - x^{71} + 1$	$-x^{56} + x^{24}$	$x^{112} + x^{80} + x^{48}$
$x^{173} - x^{147} + x^{121} + x^{26} - 1$	$x^{133} - x^{107} - x^{84} + x^{81} - x^{58} + x^{35}$	$x^{67} + x^{41} + x^{18}$
$x^{179} - x^{59} + 1$	$-x^{60} + x^{20}$	$x^{120} + x^{80} + x^{40}$
$x^{181} - x^{37} + 1$	$x^{121} + x^{73} + x^{25}$	$-x^{61} + x^{13}$
$x^{191} - x^{71} + 1$	$-x^{64} + x^{24}$	$x^{128} + x^{88} + x^{48}$
$x^{193} - x^{64} + 1$	$x^{129} + x^{86} + x^{43}$	$-x^{65} + x^{22}$
$x^{197} - x^{117} + x^{80} + x^{37} - 1$	$x^{185} - x^{146} + x^{107} - x^{105} - x^{66} + x^{25}$	$x^{93} + x^{54} + x^{13}$
$x^{199} - x^{177} + x^{155} + x^{22} - 1$	$x^{74} + x^{52} + x^{15}$	$x^{148} - x^{126} + x^{104} - x^{89} - x^{67} + x^{30}$
$x^{211} - x^{189} + x^{167} + x^{22} - 1$	$x^{78} + x^{56} + x^{15}$	$x^{156} - x^{134} + x^{112} - x^{93} - x^{71} + x^{30}$
$x^{223} + x^{144} - x^{79} + x^{65} - 1$	$-x^{101} + x^{53} + x^{22}$	$x^{202} + x^{154} + x^{123} + x^{106} - x^{75} + x^{44}$
$x^{227} - x^{11} + 1$	$-x^{76} + x^{4}$	$x^{152} + x^{80} + x^{8}$
$x^{229} - x^{79} + 1$	$x^{153} + x^{103} + x^{53}$	$-x^{77} + x^{27}$
$x^{233} - x^{141} + x^{92} + x^{49} - 1$	$x^{217} - x^{170} - x^{125} + x^{123} - x^{78} + x^{33}$	$x^{109} + x^{62} + x^{17}$
$x^{239} - x^{5} + 1$	$-x^{80} + x^{2}$	$x^{160} + x^{82} + x^{4}$
$x^{241} - x^{88} + 1$	$x^{161} + x^{110} + x^{59}$	$-x^{81} + x^{30}$
$x^{251} - x^{26} + 1$	$-x^{84} + x^{9}$	$x^{168} + x^{93} + x^{18}$
$x^{257} - x^{165} + x^{92} + x^{73} - 1$	$x^{233} - x^{178} - x^{141} + x^{123} - x^{86} + x^{49}$	$x^{117} + x^{62} + x^{25}$
$x^{263} - x^{104} + 1$	$-x^{88} + x^{35}$	$x^{176} + x^{123} + x^{70}$
$x^{269} + x^{150} - x^{119} + x^{31} - 1$	$x^{259} + x^{209} + x^{159} + x^{140} - x^{90} + x^{21}$	$-x^{130} + x^{80} + x^{11}$
$x^{271} + x^{246} + x^{221} - x^{25} - 1$	$-x^{99} + x^{74} + x^{17}$	$x^{198} + x^{173} + x^{148} + x^{116} - x^{91} + x^{34}$
$x^{277} - x^{97} + 1$	$x^{185} + x^{125} + x^{65}$	$-x^{93} + x^{33}$
$x^{281} - x^{231} + x^{181} + x^{50} - 1$	$x^{221} - x^{171} - x^{144} + x^{121} - x^{94} + x^{67}$	$x^{111} + x^{61} + x^{34}$
$x^{293} - x^{285} + x^{277} + x^{8} - 1$	$x^{201} - x^{193} + x^{185} - x^{106} - x^{98} + x^{11}$	$x^{101} + x^{93} + x^{6}$
$x^{307} + x^{258} + x^{209} - x^{49} - 1$	$-x^{119} + x^{70} + x^{33}$	$x^{238} + x^{189} + x^{152} + x^{140} - x^{103} + x^{66}$

list the values of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ generated by the proposed polynomials.

In the range $[47, 541]$, there exist a total 86 prime numbers. Using the irreducible trinomials and pentanomials discussed in Section IV, we are able to propose a reduction polynomial for all the 86 instances, excepting for $m = 89, 151, 149, 283, 449, 463, 521$.

TABLE VI

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, YIELDING LOW COST CUBINGS AND/OR CUBE ROOTS, WITH m A PRIME NUMBER IN THE RANGE $[311, 541]$

Reduction polynomial	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$
$x^{311}+x^{17}+x^{11}+1$	$-x^{104}-x^{6}-x^{4}$	$x^{208}-x^{110}-x^{108}+x^{12}-x^{10}+x^{8}$
$x^{313}-x^{187}+1$	$x^{209}+x^{167}+x^{125}$	$-x^{105}+x^{63}$
$x^{317}-x^{267}+x^{217}+x^{50}-1$	$x^{245}-x^{195}-x^{156}+x^{145}-x^{106}+x^{67}$	$x^{123}+x^{73}+x^{34}$
$x^{331}+x^{246}+x^{161}-x^{85}-1$	$-x^{139}+x^{57}+x^{54}$	$x^{278}+x^{196}+x^{193}+x^{114}-x^{111}+x^{108}$
$x^{337}-x^{25}+1$	$x^{225}+x^{121}+x^{17}$	$-x^{113}+x^{9}$
$x^{347}-x^{65}+1$	$-x^{116}+x^{22}$	$x^{232}+x^{138}+x^{44}$
$x^{349}-x^{223}+1$	$x^{233}+x^{191}+x^{149}$	$-x^{117}+x^{75}$
$x^{353}-x^{249}+x^{145}+x^{104}-1$	$x^{305}-x^{222}-x^{201}+x^{139}-x^{118}+x^{97}$	$x^{153}+x^{70}+x^{49}$
$x^{359}-x^{122}+1$	$-x^{120}+x^{41}$	$x^{240}+x^{161}+x^{82}$
$x^{367}-x^{303}+x^{239}+x^{64}-1$	$x^{144}+x^{80}+x^{43}$	$x^{288}-x^{224}-x^{187}+x^{160}-x^{123}+x^{86}$
$x^{373}-x^{25}+1$	$x^{249}+x^{133}+x^{17}$	$-x^{125}+x^{9}$
$x^{379}+x^{264}+x^{149}-x^{115}-1$	$-x^{165}+x^{77}+x^{50}$	$x^{330}+x^{242}+x^{215}+x^{154}-x^{127}+x^{100}$
$x^{383}-x^{80}+1$	$-x^{128}+x^{27}$	$x^{256}+x^{155}+x^{54}$
$x^{389}-x^{249}+x^{140}+x^{109}-1$	$x^{353}-x^{270}-x^{213}+x^{187}-x^{130}+x^{73}$	$x^{177}+x^{94}+x^{37}$
$x^{397}+x^{31}+x^{25}+1$	$x^{265}-x^{143}-x^{141}+x^{21}-x^{19}+x^{17}$	$-x^{133}-x^{11}-x^{9}$
$x^{401}+x^{210}-x^{191}+x^{19}-1$	$x^{395}+x^{325}+x^{255}+x^{204}-x^{134}+x^{13}$	$-x^{198}+x^{128}+x^{7}$
$x^{409}-x^{136}+1$	$x^{273}+x^{182}+x^{91}$	$-x^{137}+x^{46}$
$x^{419}-x^{136}+1$	$-x^{140}+x^{46}$	$x^{280}+x^{186}+x^{92}$
$x^{421}-x^{13}+1$	$x^{281}+x^{145}+x^{9}$	$-x^{141}+x^{5}$
$x^{431}-x^{365}+1$	$-x^{144}+x^{122}$	$x^{288}+x^{266}+x^{244}$
$x^{433}-x^{262}+1$	$x^{289}+x^{232}+x^{175}$	$-x^{145}+x^{88}$
$x^{439}-x^{231}+x^{208}+x^{23}-1$	$x^{216}+x^{139}+x^{8}$	$x^{432}-x^{355}+x^{278}-x^{224}-x^{147}+x^{16}$
$x^{443}-x^{188}+1$	$-x^{148}+x^{63}$	$x^{296}+x^{211}+x^{126}$
$x^{457}-x^{67}+1$	$x^{305}+x^{175}+x^{45}$	$-x^{153}+x^{23}$
$x^{461}+x^{432}+x^{403}-x^{29}-1$	$x^{327}+x^{298}+x^{269}+x^{183}-x^{154}+x^{39}$	$-x^{164}+x^{135}+x^{20}$
$x^{467}-x^{92}+1$	$-x^{156}+x^{31}$	$x^{312}+x^{187}+x^{62}$
$x^{479}-x^{221}+1$	$-x^{160}+x^{74}$	$x^{320}+x^{234}+x^{148}$
$x^{487}-x^{255}+x^{232}+x^{23}-1$	$x^{240}+x^{155}+x^{8}$	$x^{480}-x^{395}+x^{310}-x^{248}-x^{163}+x^{16}$
$x^{491}-x^{11}+1$	$-x^{164}+x^{4}$	$x^{328}+x^{168}+x^{8}$
$x^{499}-x^{327}+x^{172}+x^{155}-1$	$x^{224}+x^{115}+x^{52}$	$x^{448}-x^{339}-x^{276}+x^{230}-x^{167}+x^{104}$
$x^{503}-x^{35}+1$	$-x^{168}+x^{12}$	$x^{336}+x^{180}+x^{24}$
$x^{509}+x^{294}-x^{215}+x^{79}-1$	$x^{483}+x^{385}+x^{287}+x^{268}-x^{170}+x^{53}$	$-x^{242}+x^{144}+x^{27}$
$x^{523}+x^{414}+x^{305}-x^{109}-1$	$-x^{211}+x^{102}+x^{73}$	$x^{422}+x^{313}+x^{284}+x^{204}-x^{175}+x^{146}$
$x^{541}-x^{145}+1$	$x^{361}+x^{229}+x^{97}$	$-x^{181}+x^{49}$