FORMULAS FOR CUBE ROOTS IN $\mathbb{F}_{3^m}$

OMRAN AHMADI, DARREL HANKERSON, AND ALFRED MENEZES

Abstract. We determine the number of nonzero coefficients (called the Hamming weight) in the polynomial representation of $x^{1/3}$ in $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f)$, where $f \in \mathbb{F}_3[x]$ is an irreducible trinomial.

Keywords: cube roots, finite field arithmetic.

1. Introduction

Fast arithmetic in finite fields $\mathbb{F}_{q^m}$ is important for the efficient implementation of discrete logarithm cryptosystems. Finite fields of characteristic two have received special attention because their arithmetic can be efficiently implemented in both hardware and software. More recently, there has been increased interest in fast arithmetic for characteristic three finite fields (e.g. see [9, 10, 11, 13]) because there are supersingular elliptic curves over $\mathbb{F}_{3^m}$ that are very well suited to the implementation of pairing-based cryptographic protocols [4, 7]. The fastest algorithms known for pairing computations on these supersingular elliptic curves require the evaluation of cube roots in $\mathbb{F}_{3^m}$ [5, 3]. Thus it is worthwhile to have fast algorithms for computing cube roots in $\mathbb{F}_{3^m}$. Of particular interest is the case where $\mathbb{F}_{3^m}$ is represented as $\mathbb{F}_3[x]/(f)$ for an irreducible trinomial $f \in \mathbb{F}_3[x]$ because multiplication can then be accelerated considerably (e.g. see [8]).

Cube roots in $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f)$ can be efficiently computed as follows. Suppose that $m \equiv 1 \pmod 3$ (the cases $m \equiv 0, 2 \pmod 3$ are similar). If $\alpha = \sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}_{3^m}$, then

$$\alpha^{1/3} = \sum_{i=0}^{(m-1)/3} a_{3i} x^i + x^{1/3} \sum_{i=0}^{(m-4)/3} a_{3i+1} x^i + x^{2/3} \sum_{i=0}^{(m-4)/3} a_{3i+2} x^i. \tag{1}$$

If the field elements $x^{1/3}$ and $x^{2/3}$ are precomputed, then computing cube-roots via (1) requires only two polynomial multiplications. These multiplications can be accelerated if the polynomial representations of $x^{1/3}$ and $x^{2/3}$ are sparse. Indeed, Barreto [2] observed that if $f(x) = x^m + ax + b$ is a trinomial and $m \equiv k \pmod 3$, then $x^{1/3}$ and $x^{2/3}$ have very low Hamming weights (cf. Theorem 2).

In this paper, we determine the Hamming weight of $x^{1/3}$, denoted $\mathrm{wt}(x^{1/3})$, in all cases where $\mathbb{F}_{3^m}$ is represented as $\mathbb{F}_3[x]/(f)$ and $f(x) = x^m + ax^k + b \in$

Date: April 29, 2006.

$\mathbb{F}_3[x]$ is an irreducible trinomial. The case where $m \not\equiv -k \pmod 3$ is considered in §2. The more complicated case where $m \equiv -k \pmod 3$ is handled in §3. Finally, Appendix A includes a computer-generated table listing $\mathrm{wt}(x^{1/3})$ for all irreducible trinomials of degrees $m \in [2, 56]$.

We conclude this section by noting that the computation of square roots in characteristic two finite fields $\mathbb{F}_{2^m}$ can also be accelerated if $\mathbb{F}_{2^m}$ is represented as $\mathbb{F}_2[x]/(f)$ for an irreducible trinomial $f \in \mathbb{F}_2[x]$ and $x^{1/2}$ has low Hamming weight (e.g. see [6]). The following result, whose proof is similar to the proofs of Theorems 3 and 4, characterizes $\mathrm{wt}(x^{1/2})$.

Theorem 1. Let $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(f)$ where $f(x) = x^m + x^k + 1$ is irreducible over $\mathbb{F}_2$. If m is even, then

$$\mathrm{wt}(x^{1/2}) = \begin{cases} 1, & \text{if } m = 2k \text{ and } k > 1, \\ 2, & \text{if } k = 1, \\ 3, & \text{otherwise.} \end{cases}$$

Let δ denote an integer that is either 0, 1 or 2. If m is odd, then

$$\mathrm{wt}(x^{1/2}) = \begin{cases} 2, & \text{if } k \text{ is odd,} \\ \lfloor \frac{m-3}{k} \rfloor + 3, & \text{if } k \text{ is even and } \gcd(m,k) = 1, \\ \lceil \frac{m-1}{2k} \rceil + \lceil \frac{m-k-1}{2k} \rceil + \delta, & \text{if } k \text{ is even and } \gcd(m,k) > 1. \end{cases}$$

2. The case $m \not\equiv -k \pmod 3$

Theorem 2. [2] Let $f(x) = x^m + ax^k + b$ be an irreducible polynomial over $\mathbb{F}_3$ where $m \equiv k \pmod 3$. Then

$$\mathrm{wt}(x^{1/3}) = \begin{cases} 3, & \text{if } m \equiv k \equiv 1 \pmod 3, \\ 2, & \text{if } m \equiv k \equiv 2 \pmod 3. \end{cases}$$

Theorem 3. Let $f(x) = x^m + ax^k + b$ be an irreducible polynomial over $\mathbb{F}_3$ where $m \equiv 0 \pmod 3$ and $k \equiv 1 \pmod 3$. Then

$$\mathrm{wt}(x^{1/3}) = \begin{cases} 3, & \text{if } m \neq 3k \text{ and } k \neq 1, \\ 1, & \text{if } m = 3k \text{ and } a = 1, \\ 2, & \text{if } m = 3k \text{ and } a = -1, \\ 2, & \text{if } k = 1. \end{cases}$$

Proof. Let $m = 3u$ and $k = 3v + 1$. Since $x^{3u} + ax^{3v+1} + b = 0$ in $\mathbb{F}_{3^m}$, we have

$$x^{3v+1} = -a(x^{3u} + b)$$

and hence

$$x^{1/3} = -ax^{-v}(x^u + b) = -a(x^{u-v} + bx^{-v}).$$

If $k = 1$, then $v = 0$ and hence $\mathrm{wt}(x^{1/3}) = 2$. Suppose now that $k > 1$. We need to compute x^{-v} in $\mathbb{F}_{3^m}$. From $x^{3u} + ax^{3v+1} + b = 0$ we have

$$x^{-v} = -b(x^{3u-v} + ax^{2v+1})$$

and so

$$x^{1/3} = -a(x^{u-v} - x^{3u-v} - ax^{2v+1}).$$

If $m \neq 3k$ then $u - v \neq 2v + 1$, and consequently $\mathrm{wt}(x^{1/3}) = 3$. Also, if $m = 3k$ then $u - v = 2v + 1$, and hence $\mathrm{wt}(x^{1/3}) = 1$ if $a = 1$, and $\mathrm{wt}(x^{1/3}) = 2$ if $a = -1$. □

Theorem 4. Let $f(x) = x^m + ax^k + b$ be an irreducible polynomial over $\mathbb{F}_3$ where $m \equiv 0 \pmod 3$ and $k \equiv 2 \pmod 3$. Then $\mathrm{wt}(x^{1/3}) \leq 5$.

Proof. Let $m = 3u$ and $k = 3v + 2$. Since $x^{3u} + ax^{3v+2} + b = 0$ in $\mathbb{F}_{3^m}$, we have

$$x^{2/3} = -a(x^{u-v} + bx^{-v})$$

and so

$$x^{4/3} = x^{2u-2v} + x^{-2v} - bx^{u-2v}.$$

Now, $x^{-2v} = -b(x^{3u-2v} + ax^{v+2})$, and hence

$$x^{4/3} = x^{2u-2v} - bx^{3u-2v} - abx^{v+2} - bx^{u-2v}.$$

It follows that

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

If $u - 2v - 1 \geq 0$, then $\mathrm{wt}(x^{1/3}) \leq 4$. Otherwise

$$x^{u-2v-1} = -b(x^{4u-2v-1} + ax^{u+v+1}),$$

which shows that $\mathrm{wt}(x^{1/3}) \leq 5$. □

The proofs of the following theorems are omitted because they are quite similar to the proofs of Theorems 3 and 4 but are more tedious.

Theorem 5. Let $f(x) = x^m + ax^k + b$ be an irreducible polynomial over $\mathbb{F}_3$ where $m \equiv 1 \pmod 3$ and $k \equiv 0 \pmod 3$. Then $\mathrm{wt}(x^{1/3}) \in \{l, l+1, l+2\}$, where $l = \lceil \frac{m-1}{3k} \rceil + \lceil \frac{m-1-k}{3k} \rceil$.

Theorem 6. Let $f(x) = x^m + ax^k + b$ be an irreducible polynomial over $\mathbb{F}_3$ where $m \equiv 2 \pmod 3$ and $k \equiv 0 \pmod 3$. Then $\mathrm{wt}(x^{1/3}) \in \{l, l+1, l+2, l+3\}$, where $l = \lceil \frac{2m-1}{3k} \rceil + \lceil \frac{2m-1-k}{3k} \rceil + \lceil \frac{2m-1-2k}{3k} \rceil$.

3. The case $m \equiv -k \pmod 3$

Theorem 7. Let $f(x) = x^m + ax^k + b$ be an irreducible trinomial over $\mathbb{F}_3$ where $m \equiv -k \pmod 3$. Then $\mathrm{wt}(x^{1/3}) \in \{\frac{m}{d} - 2, \frac{m}{d} - 1, \frac{m}{d}\}$, where $d = \gcd(m, k)$.

The remainder of the section is devoted to the proof of Theorem 7. Since $m \equiv -k \pmod 3$, we can consider three cases: $m = 2k$, $m \geq 2k + 3$, and $m \leq 2k - 3$.

3.1. **The case $m = 2k$.** The order of an irreducible polynomial $f(x)$ over $\mathbb{F}_q$ is the smallest positive integer e such that $f(x) \mid x^e - 1$ in $\mathbb{F}_q[x]$.

Theorem 8. [12, Theorem 3.9] Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n and order e and let t be a positive integer. Then $f(x^t)$ is irreducible over $\mathbb{F}_q$ if and only if

(i) $\gcd(t, \frac{q^n-1}{e}) = 1$;
(ii) each prime factor of t divides e; and
(iii) if $4 \mid t$, then $4 \mid q^n - 1$.

Lemma 9. [1] Let m, k be positive integers such that the power of 2 which divides m is greater than that of k. Then $x^m + ax^k + b \in \mathbb{F}_3[x]$ is irreducible over $\mathbb{F}_3$ if and only if $x^m - ax^k + b$ is irreducible over $\mathbb{F}_3$.

It follows from Lemma 9 that if $f(x) = x^{2k} + ax^k + b$ is irreducible over $\mathbb{F}_3$ then $b = -1$. On the other hand since

$$x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x^4 - 1)(x^2 + x - 1)(x^2 - x - 1)$$

in $\mathbb{F}_3[x]$, Theorem 8 implies that k must be a power of 2. Thus $f(x) = x^{2R} \pm x^R - 1$ where $R = 2^r$ for some r. Regardless of sign, $f(x)$ is a factor of $x^{4R} + 1$. Hence $x^{4R} = -1$ in $\mathbb{F}_{3^{2R}}$ and so $x = -x^{4R+1}$. Now, if r is odd, then $3 \mid 4R + 1$ and consequently $x^{1/3} = -x^{(4R+1)/3}$ and $\mathrm{wt}(x^{1/3}) = 1$. If r is even, then

$$x = x^{2R+1} \pm x^{R+1} = x^{2R+1} \mp x^{4R}x^{R+1} = x^{2R+1} \mp x^{5R+1}.$$

Thus $x^{1/3} = x^{(2R+1)/3} \mp x^{(5R+1)/3}$ and $\mathrm{wt}(x^{1/3}) = 2$.

3.2. **The case $m \geq 2k + 3$.** Let $x^{1/3} = \sum_{i=0}^{m-1} a_i x^i$ in $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f)$. Then $x = \sum_{i=0}^{m-1} a_i x^{3i}$ in $\mathbb{F}_{3^m}$. Equivalently, we can say that there exists a polynomial $g(x) \in \mathbb{F}_3[x]$ such that

$$h(x) := \sum_{i=0}^{m-1} a_i x^{3i} - x = g(x)f(x). \tag{2}$$

Our proof consists of a constructive method for simultaneously finding polynomials $g(x)$ and $h(x)$ satisfying (2); $x^{1/3}$ can thereafter be determined from $h(x)$.

3.2.1. *An Example.* We illustrate the aforementioned constructive method with an example. Consider $f(x) = x^7 - x^2 + 1$ which is irreducible over $\mathbb{F}_3$. The unsigned monomials of $g(x)$ appear in the second column of Table 1; the distribution of monomials into Sections is as prescribed by Table 3 which handles the general case. The unsigned monomials (before any simplification) of the product $g(x)f(x)$ appear in the third column. Notice that the monomials in the three rows of the third column of Section I are obtained by multiplying the monomials in the second column of Section I by x^7, x^2 and 1 (the unsigned monomials of $f(x)$), respectively. The other monomials in the third column of the table are obtained in an analogous way.

	$g(x)$				$g(x)f(x)$			
I	x^{11}	x^8	x^5	x^2	x^{18}	x^{15}	x^{12}	x^9
					x^{13}	x^{10}	x^7	x^4
					x^{11}	x^8	x^5	x^2
II	x^6	x^3	1		x^{13}	x^{10}	x^7	
					x^8	x^5	x^2	
					x^6	x^3	1	
III	x^4				x^{11}			
					x^6			
					x^4			
IV	x^1				x^8			
					x^3			
					x^1			

TABLE 1. Example with $f(x) = x^7 - x^2 + 1$.

Examination of the third column of Table 1 reveals that x^1 appears once, x^8 appears three times, and if x^i appears where $3 \nmid i$ and $i \notin \{1, 8\}$ then it appears exactly twice. Also x^i, where $3 \mid i$ and $i < 21$, appears at least once and at most twice in the third column.

We now start signing the terms of $g(x)$ in such a way that $g(x)f(x)$ when simplified is in the desired form (2). Since the coefficient of x in $h(x)$ is -1, x^1 in $g(x)$ must be assigned a minus sign. This results in a minus sign for x^8 and a plus sign for x^3 in the third column of Section IV of Table 1 (see also Table 2). Since x^8 appears three times in the third column, all three

	$g(x)$				$g(x)f(x)$			
I	$+x^{11}$	$-x^8$	$-x^5$	$-x^2$	$+x^{18}$	$-x^{15}$	$-x^{12}$	$-x^9$
					$-x^{13}$	$+x^{10}$	$+x^7$	$+x^4$
					$+x^{11}$	$-x^8$	$-x^5$	$-x^2$
II	$+x^6$	$-x^3$	-1		$+x^{13}$	$-x^{10}$	$-x^7$	
					$-x^8$	$+x^5$	$+x^2$	
					$+x^6$	$-x^3$	-1	
III	$-x^4$				$-x^{11}$			
					$+x^6$			
					$-x^4$			
IV	$-x^1$				$-x^8$			
					$+x^3$			
					$-x^1$			

TABLE 2. Example with $f(x) = x^7 - x^2 + 1$ (cont'd).

occurrences of x^8 must be assigned minus signs for otherwise these terms would not cancel when $f(x)g(x)$ is simplified. Now we consider the x^8 term

that appears in the third column of Section I. Since this x^8 must have a minus sign, we assign a minus sign to the x^8 term in the second column, resulting in a plus sign for the x^{10} term and a minus sign for the x^{15} term in Section I. Since x^{10} does not appear in the simplified form of $h(x)$, this in turn implies that the x^{10} term in the third column of Section II must have a minus sign. Hence the x^3 term in the second column of Section II must be assigned a minus sign and consequently the x^5 term in the third column of Section II has a plus sign. Next we consider the sign of the other x^5 term in the third column. We continue this signing procedure until all the terms of $g(x)$ have been signed (see Table 2). After simplification, we obtain

$$g(x) = x^{11} - x^8 + x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$$

and

$$h(x) = (x^{18} - x^{15} - x^{12} - x^9 - x^6 - 1) - x,$$

from which we have

$$x^{1/3} = x^6 - x^5 - x^4 - x^3 - x^2 - 1.$$

3.2.2. *General Case.* We begin by assuming that $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f)$ where $f(x) = x^m - x^k + 1$, $m \equiv 1 \pmod 3$, $k \equiv 2 \pmod 3$, $\gcd(m, k) = 1$, and $m \geq 2k + 3$.

As in the previous example, our goal is to find $g(x)$ such that $h(x) = g(x)f(x)$ after simplification is in the desired form (2). In Table 3, which is analogous to Table 1, the unsigned monomials of $g(x)$ appear in the second column, and the unsigned monomials (before any simplification) of the product $g(x)f(x)$ appear in the third column. More precisely, the monomials in the three rows of the third column of Section I are obtained by multiplying the monomials in the second column of Section I by x^m, x^k and 1, respectively. The other monomials in the third column are obtained in an analogous way. If x^u, x^v, x^w are the three monomials in the third column that are obtained by multiplying a particular monomial of $g(x)$ by the (unsigned) monomials of $f(x)$, then $C = (x^u, x^v, x^w)$ is called a *triple* and we write $S(C) = \{x^u, x^v, x^w\}$. For every such triple, exactly one of u, v, w is divisible by 3, one is congruent to 1 (mod 3), and one is congruent to 2 (mod 3) — this is because the monomials $(x^m, x^k, 1)$ of $f(x)$ satisfy the property.

Examination of the third column of Table 3 reveals the following:

(1) x^1 appears once.
(2) x^{m+1} appears three times.
(3) If $3 \nmid i$ and $i \notin \{1, m + 1\}$, then either x^i does not appear or it appears exactly twice.
(4) If $3 \mid i$ and $i < 3m$, then x^i appears at least once and at most twice.

In the following we show how the entries of $g(x)$ can be signed so that $g(x)f(x)$ after simplification is in the desired form (2).

As in the previous example, we first sign the entries of the Section IV triple (x^{m+1}, x^{k+1}, x^1); the monomials x^{m+1} and x^1 get negative signs,

	$g(x)$						$g(x)f(x)$				
I	x^{2m-3}	$\cdots$	$\cdots$	x^{k+6}	x^{k+3}	x^k	x^{3m-3}	$\cdots$	$\cdots$	$\cdots$	x^{m+k}
							x^{2m+k-3}	$\cdots$	$\cdots$	$\cdots$	x^{2k}
							x^{2m-3}	$\cdots$	$\cdots$	$\cdots$	x^k
II	x^{m+k-3}	$\cdots$	x^6	x^3	1		x^{2m+k-3}	$\cdots$	$\cdots$	x^m	
							x^{m+2k-3}	$\cdots$	$\cdots$	x^k	
							x^{m+k-3}	$\cdots$	$\cdots$	1	
III	x^{m-3}	$\cdots$	x^{2k+3}	x^{2k}			x^{2m-3}	$\cdots$	x^{m+2k}		
							x^{m+k-3}	$\cdots$	x^{3k}		
							x^{m-3}	$\cdots$	x^{2k}		
IV	x^1						x^{m+1}				
							x^{k+1}				
							x^1				

TABLE 3. Table for $f(x) = x^m - x^k + 1$, $m \equiv 1 \pmod 3$, $k \equiv 2 \pmod 3$, $\gcd(m,k) = 1$, $m \geq 2k+3$.

while x^{k+1} gets a positive sign. We then sign the entries of the triple $C_0 = (x^{2m+1}, x^{m+k+1}, x^{m+1})$ in Section I; the resulting signed triple is $(-x^{2m+1}, +x^{m+k+1}, -x^{m+1})$. After that we sign the entries of the Section II triple $C_1 = (x^{m+k+1}, x^{2k+1}, x^{k+1})$ to obtain $(-x^{m+k+1}, +x^{2k+1}, -x^{k+1})$; this triple was chosen because it has a monomial, namely x^{m+k+1}, in common with C_0 which is different from x^{m+1} and whose exponent is not divisible by 3. Notice that the power of the common entry x^{m+k+1} is congruent to 1 (mod 3). The next signed triple is $C_2 = (-x^{m+2k+1}, +x^{3k+1}, -x^{2k+1})$ in Section I; the entry in common between C_1 and C_2 is x^{2k+1} whose power is congruent to 2 (mod 3). This signing procedure is continued until we cannot move to an unsigned triple.

We claim that the signing procedure terminates when we visit the triple in Section II that contains x^{m+1}. Suppose that the triples visited are C_0, $C_1, \ldots, C_{l+1}$ (in that order). If $1 \leq i \leq l$, then $|S(C_{i-1}) \cap S(C_i)| = |S(C_i) \cap S(C_{i+1})| = 1$ where the monomials in the two intersections are different and their powers are not congruent to zero modulo 3. Let x^w be the monomial in C_{l+1} for which $3 \nmid w$ and $x^w \notin C_l$. Then since every x^j where $3 \nmid j$ and $j \notin \{1, m+1\}$ appears exactly zero or two times among the triples, we have $x^w \notin S(C_i)$ for $1 \leq i \leq l-1$. Hence $x^w \in S(C_0)$. Since $S(C_0) \cap S(C_1) \neq x^{m+1}$, it follows that $S(C_{l+1}) \cap S(C_0) = x^{m+1}$. Since the signing procedure never visits Section IV after leaving it, C_{l+1} must be the triple in Section II containing x^{m+1}.

We now show that the signing procedure visits all the triples. Denote by $d(C_j)$ the power of the unique monomial of C_j whose power is divisible by 3. We have $d(C_0) = 2m+1$ and $d(C_{l+1}) = m-k+1$. Let $C_j \cap C_{j+1} = \{x^{z_j}\}$. The following statements can be deduced from the signing procedure:

(1) If C_j is in Section I and C_{j+1} is in Section II, then $z_j \equiv 1 \pmod 3$ and $d(C_j) - d(C_{j+1}) = 2m - k$.
(2) If C_j is in Section II, then C_{j+1} is in Section I, $z_j \equiv 2 \pmod 3$, and $d(C_{j+1}) - d(C_j) = m + k$.
(3) If C_j is in Section I and C_{j+1} is in Section III, then $z_j \equiv 1 \pmod 3$ and $d(C_j) - d(C_{j+1}) = m - 2k$.
(4) If C_j is in Section III, then C_{j+1} is in Section I, $z_j \equiv 2 \pmod 3$, and $d(C_{j+1}) - d(C_j) = 2m - k$.
(5) C_l is in Section I since C_{l+1} is in Section II.

Now we have

$$d(C_{l+1}) - d(C_0) = \sum_{j=0}^{l} d(C_{j+1}) - d(C_j). \tag{3}$$

Since in the procedure every move from Section I to Section II which is not the last move is followed by a return to Section I, we may assume that we have moved u times from Section I to Section II and returned to Section I. Similarly we can assume that we have moved v times from Section I to Section III and returned to Section I. It follows from (3) that

$$\begin{aligned} d(C_{l+1}) - d(C_0) &= u\big(-(2m-k) + (m+k)\big) + v\big(-(m-2k) + (2m-k)\big) \\ &\quad - (2m-k) \\ &= (m-k+1) - (2m+1), \end{aligned}$$

and thus

$$m(-u+v-1) + k(2u+v+2) = 0. \tag{4}$$

Now, $u \le (m+k-3)/3$ and $v \le (m-2k)/3$, so $2u+v+2 \le m$. Since $\gcd(m,k) = 1$, we see that the solution to (4) is $u = (m+k-3)/3$ and $v = (m-2k)/3$, and hence the total number of triples visited during the signing procedure is $2u+2v+2 = (4m-2k)/3$. This is exactly the number of the triples in Sections I, II and III.

The signing procedure guarantees that if x^i appears in two triples, where $3 \nmid i$ and $i \notin \{1, m+1\}$, then the two instances of x^i receive opposite signs and therefore cancel each other when $g(x)f(x)$ is simplified. The monomials x^{m+1} in Sections I and IV both receive minus signs at the start of the signing procedure. The following argument shows that the third occurrence of x^{m+1} in Section II also receives a minus sign at the end of the procedure, and thus the three x^{m+1} terms cancel each other when $g(x)f(x)$ is simplified. Let $e(C_i)$ denote the sign of the third entry of the triple C_i. We have $e(C_0) = -1$ and $e(C_l) = e(C_{l+1})$. Suppose that C_j and C_{j+2} are in Section I. It is easy to see that if C_{j+1} is in Section II then $e(C_j) = e(C_{j+2})$, and if C_{j+1} is in Section III then $e(C_j) = -e(C_{j+2})$. Thus, since there are $v = (m-2k)/3$ moves in total from Section I to Section III and back to Section I, we have $e(C_{l+1}) = (-1)^v e(C_0) = (-1)^{v+1}$. Now, m must be odd because otherwise Lemma 9 and the condition $\gcd(m,k) = 1$ would imply that $x^m + x^k + 1$ is

irreducible over $\mathbb{F}_3$. Hence $v = (m-2k)/3$ is also odd and so $e(C_{l+1}) = 1$. Since x^{m+1} is the middle entry of C_{l+1}, it gets a minus sign and this shows that the signing procedure terminates successfully.

Finally, we determine the Hamming weight of $g(x)f(x)$. It can easily be seen that if C_j is in Section III, then C_{j+2} is in Section II and $d(C_j) = d(C_{j+2})$. Moreover, the common entry in C_j and C_{j+2} is given the same sign. Consequently, if $3 \mid i$ and x^i occurs in both Section II and Section III, then the two occurrences receive the same sign. Also, the x^{k+1} term in Section IV is assigned a plus sign, while x^{k+1} in C_1 is assigned a minus sign. Thus after simplifying, the only powers of x that appear with nonzero coefficients in $g(x)f(x)$ are x and x^i where $3 \mid i$, $0 \le i \le 3m-3$, and $i \ne k+1$. Hence $\mathrm{wt}(x^{1/3}) = m-1$, which establishes Theorem 7 in the case where $f(x) = x^m - x^k + 1$, $m \equiv 1 \pmod 3$, $k \equiv 2 \pmod 3$, $\gcd(m,k) = 1$, and $m \ge 2k+3$.

In the case where $\gcd(m,k) = d > 1$, we modify Table 3 by deleting all terms x^j for which $j \not\equiv 1 \pmod d$. The third column of the resulting table has the following properties:

(1) x^1 appears once.
(2) x^{m+1} appears three times.
(3) If $3 \nmid i$ and $i \notin \{1, m+1\}$, then either x^i does not appear or it appears exactly twice.
(4) If $3 \mid i$, $i < 3m$, and $i \equiv 1 \pmod d$, then x^i appears at least once and at most twice.

The same signing procedure can now be applied to the terms of this modified table.

The proof of Theorem 7 in the remaining cases (with $m \ge 2k+3$) can be handled in a similar manner. When $m \equiv 1 \pmod 3$ and $f(x) = x^m + x^k - 1$ or $x^m - x^k - 1$, Table 3 can be used with the appropriate $f(x)$. The case $m \equiv 2 \pmod 3$ uses Tables 4 and 5.

3.3. **The case $m \le 2k-3$.** Tables 6, 7 and 8, which are analogous to Tables 3, 4 and 5, can be used to complete the proof of Theorem 7.

References

[1] O. Ahmadi, "On the distribution of irreducible trinomials over $\mathbb{F}_3$", *Finite Fields and Their Applications*, to appear.

[2] P. Barreto, "A note on efficient computation of cube roots in characteristic 3", Cryptology ePrint Archive: Report 2004/305, 2004.

[3] P. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, "Efficient pairing computation on supersingular abelian varieties", Cryptology ePrint Archive: Report 2004/375, 2004.

[4] P. Barreto, H. Yim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 354-368.

	$g(x)$	$g(x)f(x)$
I	x^{2m-3} $\cdots$ $\cdots$ x^{k+6} x^{k+3} x^k	x^{3m-3} $\cdots$ $\cdots$ $\cdots$ x^{m+k} x^{2m+k-3} $\cdots$ $\cdots$ $\cdots$ x^{2k} x^{2m-3} $\cdots$ $\cdots$ $\cdots$ x^k
II	x^{m+k-3} $\cdots$ x^6 x^3 1	x^{2m+k-3} $\cdots$ $\cdots$ x^m x^{m+2k-3} $\cdots$ $\cdots$ x^k x^{m+k-3} $\cdots$ $\cdots$ 1
III	x^{m-3} $\cdots$ x^{2k+3} x^{2k}	x^{2m-3} $\cdots$ x^{m+2k} x^{m+k-3} $\cdots$ x^{3k} x^{m-3} $\cdots$ x^{2k}
IV	x^1	x^{m+1} x^{k+1} x^1
V	x^{k+1}	x^{m+k+1} x^{2k+1} x^{k+1}

TABLE 4. Table for $f(x) = x^m + ax^k + b$, $m \equiv 2 \pmod 3$, $k \equiv 1 \pmod 3$, $\gcd(m, k) = 1$, $k \neq 1$, $m \geq 2k + 3$.

	$g(x)$	$g(x)f(x)$
I	x^{2m-3} $\cdots$ $\cdots$ x^7 x^4 x^1	x^{3m-3} $\cdots$ $\cdots$ $\cdots$ x^{m+1} x^{2m-2} $\cdots$ $\cdots$ $\cdots$ x^2 x^{2m-3} $\cdots$ $\cdots$ $\cdots$ x^1
II	x^{m-2} $\cdots$ x^6 x^3 1	x^{2m-2} $\cdots$ $\cdots$ x^m x^{m-1} $\cdots$ $\cdots$ x^1 x^{m-2} $\cdots$ $\cdots$ 1
III	x^{m-3} $\cdots$ x^5 x^2	x^{2m-3} $\cdots$ x^{m+2} x^{m-2} $\cdots$ x^3 x^{m-3} $\cdots$ x^2

TABLE 5. Table for $f(x) = x^m + ax + b$, $m \equiv 2 \pmod 3$, $m \geq 5$.

[5] I. Duursma and H.-S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$", *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, 2894 (2003), 111-123.

[6] K. Fong, D. Hankerson, J. López and A. Menezes, "Field inversion and point halving revisited", *IEEE Transactions on Computers*, 53 (2004), 1047-1059.

[7] S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", *Algorithmic Number Theory: 5th International Symposium*, Lecture Notes in Computer Science, 2369 (2002), 324-337.

[8] J. von zur Gathen and M. Nöcker, "Polynomial and normal bases for finite fields", *Journal of Cryptology*, 18 (2005), 337-355.

[9] P. Grabher and D. Page, "Hardware acceleration of the Tate pairing in characteristic three", *Cryptographic Hardware and Embedded Systems – CHES 2005*, Lecture Notes in Computer Science, 3659 (2005), 398-411.

	$g(x)$	$g(x)f(x)$
I	x^{2m-3} $\dots$ x^{k+6} x^{k+3} x^k	x^{3m-3} $\dots$ $\dots$ x^{m+k} x^{2m+k-3} $\dots$ $\dots$ x^{2k} x^{2m-3} $\dots$ $\dots$ x^k
II	x^{m+k-3} $\dots$ $\dots$ x^6 x^3 1	x^{2m+k-3} $\dots$ $\dots$ $\dots$ x^m x^{m+2k-3} $\dots$ $\dots$ $\dots$ x^k x^{m+k-3} $\dots$ $\dots$ $\dots$ 1
III	x^{2k-3} $\dots$ x^{m+3} x^m	x^{m+2k-3} $\dots$ x^{2m} x^{3k-3} $\dots$ x^{m+k} x^{2k-3} $\dots$ x^m
IV	x^1	x^{m+1} x^{k+1} x^1

TABLE 6. Table for $f(x) = x^m + ax^k + b$, $m \equiv 1 \pmod 3$, $k \equiv 2 \pmod 3$, $\gcd(m,k) = 1$, $m \leq 2k-3$.

	$g(x)$	$g(x)f(x)$
I	x^{2m-3} $\dots$ x^{k+6} x^{k+3} x^k	x^{3m-3} $\dots$ $\dots$ x^{m+k} x^{2m+k-3} $\dots$ $\dots$ x^{2k} x^{2m-3} $\dots$ $\dots$ x^k
II	x^{m+k-3} $\dots$ $\dots$ x^6 x^3 1	x^{2m+k-3} $\dots$ $\dots$ $\dots$ x^m x^{m+2k-3} $\dots$ $\dots$ $\dots$ x^k x^{m+k-3} $\dots$ $\dots$ $\dots$ 1
III	x^{2k-3} $\dots$ x^{m+3} x^m	x^{m+2k-3} $\dots$ x^{2m} x^{3k-3} $\dots$ x^{m+k} x^{2k-3} $\dots$ x^m
IV	x^1	x^{m+1} x^{k+1} x^1
V	x^{k+1}	x^{m+k+1} x^{2k+1} x^{k+1}

TABLE 7. Table for $f(x) = x^m + ax^k + b$, $m \equiv 2 \pmod 3$, $k \equiv 1 \pmod 3$, $\gcd(m,k) = 1$, $k \neq m-1$, $m \leq 2k-3$.

[10] K. Harrison, D. Page and N. Smart, "Software implementation of finite fields of characteristic three", *LMS Journal of Computation and Mathematics*, 5 (2002), 181-193.

[11] T. Kerins, W. Marnane, E. Popovici and P. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three", *Cryptographic Hardware and Embedded Systems – CHES 2005*, Lecture Notes in Computer Science, 3659 (2005), 412-426.

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

	$g(x)$	$g(x)f(x)$
I	$x^{2m-3} \quad \cdots \quad x^{m+5} \quad x^{m+2} \quad x^{m-1}$	$x^{3m-3} \quad \cdots \quad \cdots \quad x^{2m-1}$ $x^{3m-4} \quad \cdots \quad \cdots \quad x^{2m-2}$ $x^{2m-3} \quad \cdots \quad \cdots \quad x^{m-1}$
II	$x^{2m-4} \quad \cdots \quad \cdots \quad x^6 \quad x^3 \quad 1$	$x^{3m-4} \quad \cdots \quad \cdots \quad \cdots \quad x^m$ $x^{3m-5} \quad \cdots \quad \cdots \quad \cdots \quad x^{m-1}$ $x^{2m-4} \quad \cdots \quad \cdots \quad \cdots \quad 1$
III	$x^{2m-5} \quad \cdots \quad x^{m+3} \quad x^m$	$x^{3m-5} \quad \cdots \quad x^{2m}$ $x^{3m-6} \quad \cdots \quad x^{2m-1}$ $x^{2m-5} \quad \cdots \quad x^m$
IV	x^1	x^{m+1} x^m x^1

TABLE 8. Table for $f(x) = x^m + ax^{m-1} + b$, $m \equiv 2 \pmod 3$, $m \geq 5$.

[13] D. Page and N. Smart, "Hardware implementation of finite fields of characteristic three", *Cryptographic Hardware and Embedded Systems – CHES 2002*, Lecture Notes in Computer Science, 2523 (2002), 529-539.

Appendix A

Table 9: Irreducible trinomials $f(x) = x^m + ax^k + b$ and Hamming weight of $x^{1/3}$ in $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f)$, for $2 \le m \le 56$.

Irreducible $x^{1/3}$ trinomial	wt	Irreducible $x^{1/3}$ trinomial	wt	Irreducible $x^{1/3}$ trinomial	wt	Irreducible $x^{1/3}$ trinomial	wt	Irreducible $x^{1/3}$ trinomial	wt
$x^{2}\pm x^{1}-1$	2	$x^{15}-x^{13}\pm 1$	3	$x^{26}-x^{14}+1$	2	$x^{37}-x^{15}\pm 1$	4	$x^{47}-x^{32}+1$	2
$x^{3}-x^{1}\pm 1$	2	$x^{16}\pm x^{4}-1$	3	$x^{26}-x^{18}+1$	6	$x^{37}-x^{22}+1$	3	$x^{47}+x^{32}-1$	2
$x^{3}-x^{2}+1$	3	$x^{16}\pm x^{6}-1$	4	$x^{26}\pm x^{19}-1$	24	$x^{37}+x^{22}-1$	3	$x^{48}\pm x^{8}-1$	4
$x^{3}+x^{2}-1$	3	$x^{16}\pm x^{7}-1$	3	$x^{26}-x^{24}+1$	6	$x^{37}-x^{24}+1$	4	$x^{48}\pm x^{40}-1$	3
$x^{4}\pm x^{1}-1$	3	$x^{16}\pm x^{8}-1$	1	$x^{27}-x^{7}\pm 1$	3	$x^{37}+x^{24}-1$	4	$x^{50}-x^{6}+1$	20
$x^{4}\pm x^{2}-1$	1	$x^{16}\pm x^{9}-1$	4	$x^{27}-x^{20}+1$	5	$x^{37}-x^{25}\pm 1$	3	$x^{50}-x^{12}+1$	12
$x^{4}\pm x^{3}-1$	3	$x^{16}\pm x^{10}-1$	3	$x^{27}+x^{20}-1$	5	$x^{37}-x^{31}\pm 1$	3	$x^{50}-x^{38}+1$	2
$x^{5}-x^{1}\pm 1$	5	$x^{16}\pm x^{12}-1$	2	$x^{28}\pm x^{2}-1$	13	$x^{38}-x^{4}+1$	18	$x^{50}-x^{44}+1$	2
$x^{5}-x^{4}+1$	3	$x^{17}-x^{1}\pm 1$	17	$x^{28}\pm x^{13}-1$	3	$x^{38}-x^{16}+1$	17	$x^{51}-x^{1}\pm 1$	2
$x^{5}+x^{4}-1$	3	$x^{17}-x^{16}+1$	15	$x^{28}\pm x^{15}-1$	4	$x^{38}-x^{22}+1$	17	$x^{51}-x^{50}+1$	5
$x^{6}\pm x^{1}-1$	2	$x^{17}+x^{16}-1$	15	$x^{28}\pm x^{26}-1$	12	$x^{38}-x^{34}+1$	17	$x^{51}+x^{50}-1$	5
$x^{6}-x^{2}+1$	2	$x^{18}\pm x^{7}-1$	3	$x^{29}-x^{4}+1$	28	$x^{39}-x^{7}\pm 1$	3	$x^{52}\pm x^{7}-1$	3
$x^{6}-x^{4}+1$	3	$x^{18}-x^{8}+1$	4	$x^{29}+x^{4}-1$	28	$x^{39}-x^{13}\pm 1$	2	$x^{52}\pm x^{9}-1$	6
$x^{6}\pm x^{5}-1$	5	$x^{18}-x^{10}+1$	3	$x^{29}-x^{25}\pm 1$	27	$x^{39}-x^{26}+1$	3	$x^{52}\pm x^{14}-1$	25
$x^{7}-x^{2}+1$	6	$x^{18}\pm x^{11}-1$	5	$x^{30}\pm x^{1}-1$	2	$x^{39}+x^{26}-1$	3	$x^{52}\pm x^{15}-1$	5
$x^{7}+x^{2}-1$	6	$x^{19}-x^{2}+1$	18	$x^{30}-x^{4}+1$	3	$x^{39}-x^{32}+1$	5	$x^{52}\pm x^{25}-1$	3
$x^{7}-x^{5}\pm 1$	6	$x^{19}+x^{2}-1$	18	$x^{30}-x^{14}+1$	4	$x^{39}+x^{32}-1$	5	$x^{52}\pm x^{27}-1$	4
$x^{8}\pm x^{2}-1$	2	$x^{19}-x^{8}+1$	18	$x^{30}-x^{16}+1$	3	$x^{40}\pm x^{1}-1$	3	$x^{52}\pm x^{37}-1$	3
$x^{8}\pm x^{3}-1$	8	$x^{19}+x^{8}-1$	18	$x^{30}-x^{26}+1$	5	$x^{40}\pm x^{3}-1$	11	$x^{52}\pm x^{38}-1$	24
$x^{8}\pm x^{4}-1$	2	$x^{19}-x^{11}\pm 1$	18	$x^{30}\pm x^{29}-1$	5	$x^{40}\pm x^{10}-1$	3	$x^{52}\pm x^{43}-1$	3
$x^{8}\pm x^{5}-1$	2	$x^{19}-x^{17}\pm 1$	17	$x^{31}-x^{5}\pm 1$	30	$x^{40}\pm x^{13}-1$	3	$x^{52}\pm x^{45}-1$	4
$x^{8}\pm x^{6}-1$	4	$x^{20}\pm x^{5}-1$	2	$x^{31}-x^{11}\pm 1$	30	$x^{40}\pm x^{15}-1$	4	$x^{53}-x^{13}\pm 1$	52
$x^{9}-x^{4}+1$	3	$x^{20}\pm x^{15}-1$	4	$x^{31}-x^{20}+1$	30	$x^{40}\pm x^{25}-1$	3	$x^{53}-x^{22}+1$	51
$x^{9}+x^{4}-1$	3	$x^{21}-x^{5}\pm 1$	4	$x^{31}+x^{20}-1$	30	$x^{40}\pm x^{27}-1$	4	$x^{53}+x^{22}-1$	51
$x^{9}-x^{5}\pm 1$	4	$x^{21}-x^{16}+1$	3	$x^{31}-x^{26}+1$	29	$x^{40}\pm x^{30}-1$	2	$x^{53}-x^{31}\pm 1$	51
$x^{10}-x^{2}+1$	4	$x^{21}+x^{16}-1$	3	$x^{31}+x^{26}-1$	29	$x^{40}\pm x^{37}-1$	3	$x^{53}-x^{40}+1$	51
$x^{10}-x^{8}+1$	3	$x^{22}-x^{4}+1$	3	$x^{32}\pm x^{5}-1$	2	$x^{40}\pm x^{39}-1$	3	$x^{53}+x^{40}-1$	51
$x^{11}-x^{2}+1$	2	$x^{22}\pm x^{5}-1$	21	$x^{32}\pm x^{8}-1$	2	$x^{41}-x^{1}\pm 1$	41	$x^{54}\pm x^{1}-1$	2
$x^{11}+x^{2}-1$	2	$x^{22}-x^{6}+1$	5	$x^{32}\pm x^{12}-1$	8	$x^{41}-x^{40}+1$	39	$x^{54}\pm x^{13}-1$	3
$x^{11}-x^{3}\pm 1$	10	$x^{22}-x^{16}+1$	3	$x^{32}\pm x^{14}-1$	2	$x^{41}+x^{40}-1$	39	$x^{54}-x^{14}+1$	4
$x^{11}-x^{8}+1$	2	$x^{22}\pm x^{17}-1$	20	$x^{32}\pm x^{16}-1$	2	$x^{42}\pm x^{7}-1$	3	$x^{54}-x^{40}+1$	3
$x^{11}+x^{8}-1$	2	$x^{22}-x^{18}+1$	4	$x^{32}\pm x^{18}-1$	7	$x^{42}-x^{10}+1$	3	$x^{54}\pm x^{41}-1$	5
$x^{11}-x^{9}\pm 1$	6	$x^{23}-x^{3}\pm 1$	18	$x^{32}\pm x^{20}-1$	2	$x^{42}-x^{32}+1$	5	$x^{54}\pm x^{53}-1$	5
$x^{12}\pm x^{2}-1$	4	$x^{23}-x^{5}\pm 1$	2	$x^{32}\pm x^{24}-1$	4	$x^{42}\pm x^{35}-1$	5	$x^{55}-x^{11}\pm 1$	4
$x^{12}\pm x^{10}-1$	3	$x^{23}-x^{8}+1$	2	$x^{32}\pm x^{27}-1$	6	$x^{43}-x^{17}\pm 1$	42	$x^{55}-x^{23}\pm 1$	54
$x^{13}-x^{1}\pm 1$	3	$x^{23}+x^{8}-1$	2	$x^{33}-x^{5}\pm 1$	4	$x^{43}-x^{26}+1$	42	$x^{55}-x^{26}+1$	54
$x^{13}-x^{4}+1$	3	$x^{23}-x^{15}\pm 1$	6	$x^{33}-x^{28}+1$	3	$x^{43}+x^{26}-1$	42	$x^{55}+x^{26}-1$	54
$x^{13}+x^{4}-1$	3	$x^{23}-x^{18}+1$	6	$x^{33}+x^{28}-1$	3	$x^{44}\pm x^{3}-1$	32	$x^{55}-x^{29}\pm 1$	54
$x^{13}-x^{6}+1$	4	$x^{23}+x^{18}-1$	6	$x^{34}-x^{2}+1$	16	$x^{44}\pm x^{10}-1$	21	$x^{55}-x^{32}+1$	54
$x^{13}+x^{6}-1$	4	$x^{23}-x^{20}+1$	2	$x^{34}-x^{32}+1$	15	$x^{44}\pm x^{34}-1$	20	$x^{55}+x^{32}-1$	54
$x^{13}-x^{7}\pm 1$	3	$x^{23}+x^{20}-1$	2	$x^{35}-x^{2}+1$	2	$x^{44}\pm x^{41}-1$	2	$x^{55}-x^{44}+1$	3
$x^{13}-x^{9}\pm 1$	4	$x^{24}\pm x^{4}-1$	3	$x^{35}+x^{2}-1$	2	$x^{45}-x^{17}\pm 1$	4	$x^{55}+x^{44}-1$	3
$x^{13}-x^{12}+1$	3	$x^{24}\pm x^{20}-1$	5	$x^{35}-x^{17}\pm 1$	2	$x^{45}-x^{28}+1$	3	$x^{56}\pm x^{3}-1$	40
$x^{13}+x^{12}-1$	3	$x^{25}-x^{3}\pm 1$	8	$x^{35}-x^{18}+1$	7	$x^{45}+x^{28}-1$	3	$x^{56}\pm x^{4}-1$	13
$x^{14}\pm x^{1}-1$	14	$x^{25}-x^{6}+1$	5	$x^{35}+x^{18}-1$	7	$x^{46}\pm x^{5}-1$	45	$x^{56}\pm x^{5}-1$	2
$x^{14}-x^{4}+1$	6	$x^{25}+x^{6}-1$	5	$x^{35}-x^{33}\pm 1$	6	$x^{46}-x^{6}+1$	8	$x^{56}\pm x^{26}-1$	2
$x^{14}-x^{10}+1$	5	$x^{25}-x^{19}\pm 1$	3	$x^{36}\pm x^{14}-1$	4	$x^{46}-x^{10}+1$	3	$x^{56}\pm x^{30}-1$	7
$x^{14}\pm x^{13}-1$	12	$x^{25}-x^{22}+1$	3	$x^{36}\pm x^{22}-1$	3	$x^{46}-x^{16}+1$	3	$x^{56}\pm x^{51}-1$	6
$x^{15}-x^{2}+1$	4	$x^{25}+x^{22}-1$	3	$x^{37}-x^{6}+1$	6	$x^{46}-x^{30}+1$	4	$x^{56}\pm x^{52}-1$	12
$x^{15}+x^{2}-1$	4	$x^{26}-x^{2}+1$	2	$x^{37}+x^{6}-1$	6	$x^{46}-x^{36}+1$	4	$x^{56}\pm x^{53}-1$	2
$x^{15}-x^{7}\pm 1$	3	$x^{26}\pm x^{7}-1$	25	$x^{37}-x^{12}+1$	4	$x^{46}-x^{40}+1$	3		
$x^{15}-x^{8}+1$	4	$x^{26}-x^{8}+1$	2	$x^{37}+x^{12}-1$	4	$x^{46}\pm x^{41}-1$	44		
$x^{15}+x^{8}-1$	4	$x^{26}-x^{12}+1$	8	$x^{37}-x^{13}\pm 1$	3	$x^{47}-x^{15}\pm 1$	10		

Omran Ahmadi, Department of Combinatorics & Optimization, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
E-mail address: oahmadid@uwaterloo.ca

Darrel Hankerson, Department of Mathematics and Statistics, Auburn University, Auburn, AL 36849, USA
E-mail address: hankedr@auburn.edu

Alfred Menezes, Department of Combinatorics & Optimization, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
E-mail address: ajmeneze@uwaterloo.ca