ON THE CURVE $Y^n = X^\ell(X^m + 1)$ OVER FINITE FIELDS

SAEED TAFAZOLIAN AND FERNANDO TORRES

ABSTRACT. Let $\mathcal{X}$ be the nonsingular model of a plane curve of type $y^n = f(x)$ over the finite field $\mathbf{F}$ of order q^2, where $f(x)$ is a separable polynomial of degree coprime to n. If the number of $\mathbf{F}$-rational points of $\mathcal{X}$ attains the Hasse-Weil bound, then the condition n divides $q+1$ is equivalente to the solubility of $f(x)$ in $\mathbf{F}$ [20]. In this paper, we investigate this condition for $f(x) = x^\ell(x^m + 1)$.

1. INTRODUCTION

Let $\mathcal{X}$ be a (projective, geometrically irreducible, nonsingular, algebraic) curve of genus $g = g(\mathcal{X}) > 0$ defined over the finite field $\mathbf{F} := \mathbb{F}_{q^2}$ of order q^2. We are interested in the size of the set $\mathcal{X}(\mathbf{F})$ of $\mathbf{F}$-rational points of $\mathcal{X}$ which by the Hasse-Weil bound does satisfy

$$|\#\mathcal{X}(\mathbf{F}) - (q^2 + 1)| \leq 2q \cdot g\,;$$

see for example [18, Thm. 5.2.3], [9, Thm. 9.18]. Indeed, our goal in this paper is to study a particular class of $\mathbf{F}$-*maximal curves*; that is, certain curves $\mathcal{X}$ over $\mathbf{F}$ of genus g such that

$$\#\mathcal{X}(\mathbf{F}) = q^2 + 1 + 2q \cdot g\,.$$

A basic obstruction here is Ihara's bound on the genus, namely $g \leq q(q-1)/2$; see for example [18, Prop. 5.3.3]. Moreover, by [15], $g(\mathcal{X}) = q(q-1)/2$ if and only if $\mathcal{X}$ is $\mathbf{F}$-isomorphic to the Hermitian curve $\mathcal{H}$ (over $\mathbf{F}$) which is defined in Remark 1.1 below. Further examples of $\mathbf{F}$-maximal curves arise from Serre's covering remark which asserts that any curve nontrivially $\mathbf{F}$-covered by a $\mathbf{F}$-maximal curve is also $\mathbf{F}$-maximal [22], [12], [11]; for example in [5], [8] the authors systematically investigated curves dominated by $\mathcal{H}$. Nevertheless, not every $\mathbf{F}$-maximal curve arise in this way as Korchmáros-Giulietti example [6] shows; see also [19]. Further properties of maximal curves can be found in [4] as well as in the books [9, Ch. 10], [18], [10].

For concret applications in Coding Theory, Finite Geometry, Combinatorics, or Cryptography it is desirable to work out with curves defined by plane models having a reasonably handling. For instance, let $n \geq 1$ be an integer and $f(x) \in \mathbf{F}[x]$ be a polynomial such

2010 MSC: 11G20, 11M38, 14G15, 14H25.

Keywords: finite field, maximal curve, Weierstrass semigroup, Kummer extension.

December 21, 2016.

that $y^n - f(x)$ is absolutely irreducible (cf. [14, Lemma 6.54], [17, Ch. 1, Lemma 3]). Then we are led to consider certain Kummer extensions of $\mathbb{P}^1 := \mathbb{P}^1(\bar{\mathbf{F}})$, namely

$$y^n = f(x)\,, \tag{1.1}$$

since they subsume several classical examples of curves over finite fields as we can see for example in [10], [14], [17].

Remark 1.1. The data $n = q + 1$ and $f(x) = x^{q+1} + 1$ (or $f(x) = x^q + x$) in (1.1) define the aforementioned Hermitian curve $\mathcal{H}$ (over $\mathbf{F}$); see [18, Ex. 6.4.3]. We have $g(\mathcal{H}) = q(q-1)/2$, $\#\mathcal{H}(\mathbf{F}) = q^3 + 1$ so that $\mathcal{H}$ is in fact $\mathbf{F}$-maximal. Conversely, as we mentioned above, the data on the genus and the number of $\mathbf{F}$-rational points characterize $\mathcal{H}$ [15].

Remark 1.2. Let $n, m \geq 1$ be integers such that $\gcd(q, n) = 1$. We modify the shape of the Hermitian curve above by considering the curves $\mathcal{F}(n, m)$ and $\mathcal{C}(n, m)$ defined respectively by

$$y^n = x^m + 1\,, \quad \text{and} \quad y^n = x^m + x\,.$$

We notice that $\mathcal{F}_n := \mathcal{F}(n, n)$ is just the Fermat curve of degree n and clearly the condition

$$q + 1 \equiv 0 \pmod{n}\,, \tag{1.2}$$

is closely related to the $\mathbf{F}$-maximality of $\mathcal{F}_n$ via Serre's covering remark since in this case $\mathcal{F}_n$ is $\mathbf{F}$-covered by $\mathcal{H}$; indeed, the following holds true:

(I) Let $\gcd(q, m) = 1$. Then $\mathcal{F}(n, m)$ is $\mathbf{F}$-maximal if and only if both n, m satisfy (1.2); see [21].

Now let $\gcd(q, m-1) = \gcd(n, m) = 1$. Then

(II) $\mathcal{C}(n, m)$ is $\mathbf{F}$-maximal only if n satisfies (1.2) and $m - 1$ divides $q^2 - 1$; see [20, Prop. 4.4].

A characterization of the $\mathbf{F}$-maximality of $\mathcal{C}(n, m)$ is so far much involved as it requires addicional arithmetical constrains on the parameters q and m. For example, suppose $q = p^a$, $p > 2$, $m = p^b$ with b a divisor of a. Then $\mathcal{C}(n, m)$ is $\mathbf{F}$-maximal if and only if n satisfies (1.2) [20, Thm. 4.7].

Remark 1.3. In general in (1.1) we can assume from the very begining that (see for example [17, p. 51])

$$q^2 - 1 \equiv 0 \pmod{n}\,. \tag{1.3}$$

There are $\mathbf{F}$-maximal curves defined by (1.1), where (1.2) is not satisfied; in fact, consider the curves defined by $y^n = x^{q-1}(x + 1)$ with q and n satisfying (1.3). These curves are $\mathbf{F}$-covered by the Hermitian curve $\mathcal{H}$ since $y^{q^2-1} = x^{q-1}(x + 1)$ is another plane model of $\mathcal{H}$ (see [5, Ex. 6.3]).

To explain the role of condition (1.2) in the context of $\mathbf{F}$-maximal curves defined by (1.1) we point out Theorem 3.2 in [20], where under the hypothesis of the separability of $f(x)$, it is shown that (1.2) is indeed equivalent to the solubility of $f(x)$ in $\mathbf{F}$. In this paper we investigate this property in case that $f(x)$ has a multiple root; more precisely, for $\gcd(q, nm) = 1$, we consider curves $\mathcal{X}(n, \ell, m)$ defined by plane models of the form

$$y^n = x^\ell(x^m + 1)\,. \tag{1.4}$$

These curves generalize those in Remarks 1.1, 1.2, and a condition of type (1.2) above allows us to investigate their maximality via Lemma 2.4 below, where it is shown that $\mathcal{X}(n, \ell, m)$ is in fact $\mathbf{F}$-covered by the Fermat curve $\mathcal{F}_{nm}$.

The main result in this paper is the following.

Theorem 1.4. *Let q be a power of a prime, n, ℓ, m integers such that n is prime, $n > \ell \geq 0$, $m \geq 1$, and $(\ell, m) \notin \{(0, 1), (n-1, 1)\}$. Assume $\gcd(q, nm) = 1$. Let $\mathcal{X} = \mathcal{X}(n, \ell, m)$, be the curve defined by (1.4), and suppose there are at least two $\mathbf{F}$-rational points which are totally ramified for the morphism $x : \mathcal{X} \to \mathbb{P}^1$.*

1. *If $\mathcal{X}$ is $\mathbf{F}$-maximal, then $q + 1 \equiv 0 \pmod{n}$.*
2. *If in addition $\gcd(n, m) = 1$, and we also have $q + 1 \equiv 0 \pmod{m}$, then $\mathcal{X}$ is $\mathbf{F}$-maximal if and only if $q + 1 \equiv 0 \pmod{nm}$.*

In Section 2 we study some arithmetical and geometrical properties of the curve $\mathcal{X}(n, \ell, m)$. We mainly recall the formula for its genus (Lemma 2.1) which is used to compute *small* elements in the spectrum $\mathbf{M}(q^2)$ for the genera of maximal curves over $\mathbf{F}$ (see Examples 3.6, 3.8, 3.9). For the sake of completeness, in Remark 2.6 we compute the Weierstrass semigroup at the point over $x = \infty$ whenever $\gcd(n, \ell + m) = 1$.

In Section 3 we state the proof of Theorem 1.4; here Corollary 3.1 generalizes this result under tight arithmetical restrictions as Remark 3.3 shows.

2. On the curve $\mathcal{X}(n, \ell, m)$

Throughout, let q be a power of a prime, n, ℓ, m be integers such that $n \geq 1$, $\ell \geq 0$, $m \geq 1$ with $\gcd(q, nm) = 1$. Let $\mathcal{X} := \mathcal{X}(n, \ell, m)$ be the Kummer extension defined by (1.4) over $\mathbf{F} = \mathbb{F}_{q^2}$. In this section we shall point out some geometrical and arithmetical properties of $\mathcal{X}$. To start with we notice that $x : \mathcal{X} \to \mathbb{P}^1$ is a separable morphism of degree n.

Lemma 2.1. *Notation as above. The genus g of $\mathcal{X}$ satisfies*:

$$2g = (n-1)m + 2 - \gcd(n, \ell) - \gcd(n, \ell + m)\,.$$

Proof. Apply the Riemann-Hurwitz formula to x. □

Remark 2.2. To compute g of $\mathcal{X}$ above, without loss of generality, we can assume $n > \ell$; othewise, let $\ell = \alpha n + \beta$ with $0 \leq \beta < n$. Then $\mathcal{X}(n, \ell, m)$ is $\mathbf{F}$-birational to $\mathcal{X}(n, \beta, m)$ via $(x, y) \mapsto (x, y/x^{\alpha})$.

Remark 2.3. Let $\mathcal{X} = \mathcal{X}(n, \ell, m)$ with $n > \ell \geq 0$, $n > 1$, $m \geq 1$. Then $g = g(\mathcal{X}) = 0$ if and only if $(n, \ell, m) \in \{(2, 0, 2), (n, 0, 1), (n, n-1, 1)\}$.

It is easy to check that all the cases listed above for (n, ℓ, m) give curves of genus zero by Lemma 2.1. Conversily, if $g = 0$, then from this result $(n-1)m + 2 = \gcd(n, \ell) + \gcd(n, \ell + m)$ so that $(n-1)m \leq 2n - 2$ and hence $m \leq 2$. Let $m = 2$; i.e., $n = \gcd(n, \ell)$, $n = \gcd(n, \ell + 2)$. These computations imply $\ell = 0$ and $n = 2$.

Let $m = 1$; i.e. $n + 1 = s + t$ with $s = \gcd(n, \ell)$, $t = \gcd(n, \ell + 1)$. We can assume $\ell \geq 1$. Clearly $\gcd(s, t) = 1$ and hence st divides n. In particular, $s + t \geq st + 1$; i.e., $(s-1)(t-1) \leq 0$. It follows that $s = 1$, or $t = 1$. In the latter case $s = n$ and so $\ell \geq n$. Thus $s = 1$, $t = n$ and so $n = \ell + 1$.

Lemma 2.4. *Assume* $\gcd(q, nm) = 1$. *The curve* $\mathcal{X} = \mathcal{X}(n, \ell, m)$ *is* $\mathbf{F}$*-covered by the Fermat curve* $\mathcal{F}_{nm} : z^{nm} = u^{nm} + 1$. *In particular,* $\mathcal{X}$ *is* $\mathbf{F}$*-maximal provided that* nm *divides* $q + 1$.

Proof. The $\mathbf{F}$-covering is giving by $(z, u) \mapsto (x, y) := (u^n, u^{\ell} z^m)$. The Fermat curve $\mathcal{F}_{nm}$ is covered by the Hermitian curve $\mathcal{H} : v^{q+1} = u^{q+1} + 1$ and hence $\mathcal{X}$ is $\mathbf{F}$-maximal by the Serre's covering remark. □

Now we recall some fundamental geometrical facts concerning a $\mathbf{F}$-maximal curve $\mathcal{X}$. Let $P_0 \in \mathcal{X}(\mathbf{F})$, $P \in \mathcal{X}$, and $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism relative to $\mathbf{F}$. Then the following equivalence of divisors is satisfied ([4, Lemma 1.1]):

$$(q+1)P_0 \sim qP + \mathbf{\Phi}(P)\,. \tag{2.1}$$

Next we point out a key property concerning Weierstrass semigroups at rational points; it was already noticed in e.g. [21] and for the sake of completeness we state a proof.

Proposition 2.5. *Let* $\mathcal{X}$ *be a* $\mathbf{F}$*-maximal curve,* P, Q *two different* $\mathbf{F}$*-rational points of* $\mathcal{X}$. *Let* a *be a non-negative integer such that* $aP \sim aQ$. *Then* $\gcd(q+1, a)$ *belongs to the Weierstrass semigroup* $H(P)$.

Proof. From (2.1) we have $(q+1)P \sim (q+1)Q$, and the result follows as there exists $r, s \in \mathbb{Z}$ such that $\gcd(q+1, a) = r(q+1) + sa$. □

By the sake of completeness, we end up this section by computing the Weierstrass semigroup of $\mathcal{X}(n, \ell, m)$ in a special case.

Remark 2.6. Let n, ℓ, m be integers such that $n > \ell \geq 0$, $n > 1$, $m \geq 1$. We assume $\gcd(n, \ell + m) = 1$ and thus there is just one point $P \in \mathcal{X} = \mathcal{X}(n, \ell, m)$ over $x = \infty$. We shall compute the Weierstrass semigroup $H = H(P)$ at P.

For $i = 1, \dots, n-1$, let $L_i = iL - nt_{i\ell}$, where $L := \ell + m$ and $t_{i\ell} := \lfloor i\ell/n \rfloor$. Observe that $L_1 = L$

Claim. *H is generated by the set $\Sigma = \{n, L_1, \dots, L_{n-1}\}$.*

Proof of the Claim. Let $v = v_P$ be the valuation at P. Then $v(y) = -L$ and $v(x) = -n$. The functions $z_i := y^i/x^{t_{i\ell}}$ are regular outside P, and $v(z_i) = -iL + nt_{i\ell} = -L_i$. This means that H contains the semigroup $S = \langle \Sigma \rangle$ generated by Σ. Thus it is enough to show that $g(S)$, the genus of S, satisfies Lemma 2.1. We notice that $L_i \equiv iL \pmod n$ and hence Σ is a complete set of residues module n; thus

$$g \leq g(S) = \lfloor L_1/n \rfloor + \ldots + \lfloor L_{n-1}/n \rfloor .$$

Since $L_i = \lfloor L_i/n \rfloor n + r_i$ with $0 \leq r_i < n$ and $r_i \neq r_j$ for $i \neq j$, after some computations we get $g = g(S)$.

3. The main result

Let $\mathcal{X} = \mathcal{X}(n, \ell, m)$ be the curve defined by (1.4); let us recall that $\gcd(q, nm) = 1$. Let $x : \mathcal{X} \to \mathbb{P}^1$ and $P, Q \in \mathcal{X}(\mathbf{F})$ be two different points which are totally ramified for x.

Proof of Theorem 1.4. (1) We have $\operatorname{div}(x) = nP - nQ$, and thus by Proposition 2.5, $d = \gcd(q+1, n)$ belongs to the Weierstrass semigroup of $\mathcal{X}$ at P (or at Q). Since n is prime by hypothesis, $d = 1$ or $d = n$. If $d = 1$, $g(\mathcal{X}) = 0$ and Remark 2.3 gives $(n, \ell, m) \in \{(2, 0, 2), (n, 0, 1), (n, n-1, 1)$. If $(n, \ell, m) = (2, 0, 2)$, q is odd and so 2 divides $q + 1$. This shows the first part of the result.

(2) The second parte of the main result follows from Lemma 2.4.

We generalize Theorem 1.4 under certain arithmetical constrains.

Corollary 3.1. *Let $\mathcal{X} = \mathcal{X}(n, \ell, m)$. Assume that $n = n_1 \dots n_s$ is a product of pairwise different primes with $n_i > \ell \geq 0$ and $(\ell, m) \notin \{(0, 1), (n_i - 1, 1)\}$ for each $i = 1, \dots, s$. If $\mathcal{X}$ is $\mathbb{F}$-maximal, then $q + 1 \equiv 0 \pmod n$.*

If in addition $\gcd(n, m) = 1$ and $q + 1 \equiv 0 \pmod m$, then $\mathcal{X}$ is $\mathbf{F}$-maximal if and only if $q + 1 \equiv 0 \pmod{nm}$.

Proof. By Serre's covering remark each curve $\mathcal{X}(n_i, \ell, m)$ is $\mathbf{F}$-maximal. We can apply now Theorem 1.4 to conclude that n_i divides $q + 1$, and the result follows. □

From this result and Lemma 2.4 we obtain:

Corollary 3.2. *Let $\mathcal{X} = \mathcal{X}(n, \ell, 1)$ where $n = n_1 \dots n_s$ is a product of pairwise different primes with $n_i > \ell > 0$ and $\ell \neq n_i - 1$ for each $i = 1, \dots, s$.*

Then $\mathcal{X}$ is $\mathbb{F}$-maximal if and only if $q + 1 \equiv 0 \pmod n$.

Remark 3.3. The arithmetical hypotheses in Corollary 3.2 are necessary. For example, for $q > 2$ this result is clearly false for $\mathcal{X}(q^2-1, q-1, 1)$; as a matter of fact here we cannot apply Corollary 3.1 since $\gcd(q^2-1, q-1) > 1$.

Remark 3.4. We already mentioned that the genus g of a $\mathbf{F}$-maximal curve is upper bounded by Ihara's bound $q(q-1)/2$. Indeed, the spectrum $\mathbf{M}(q^2)$ for the genera of $\mathbf{F}$-maximal curves is contained in the set:

$$[0, g_3] \cup \{g_2\} \cup \{g_1\}\,, \quad \text{where} \tag{3.1}$$

$g_3 = g_3(q^2) = \lfloor (q^2-q+4)/6 \rfloor\,, \quad g_2 = g_2(q^2) = \lfloor (q-1)^2/4 \rfloor\,, \quad g_1 = g_1(q^2) = q(q-1)/2\,.$

Computing $\mathbf{M}(q^2)$ is so far an interesting and widly open problem for $q \geq 8$; see e.g. [2].

Remark 3.5. From Lemmas 2.1, 2.4 we have the following criterion: Let $g \geq 0$ be an integer and q a power of a prime. Then $g \in \mathbf{M}(q^2)$ if there exists nonnegative integers n, ℓ, m such that

$$nm = 2g + m - 2 + \gcd(n, \ell) + \gcd(n, \ell + m) \quad \text{with } nm \mid (q+1)\ . \tag{3.2}$$

Example 3.6. Applying Remark 3.5 with $\ell = m = 1$, condition (3.2) reads $n = 2g + \gcd(n, 2)$. In particular any nonnegative integer $g \in \mathbf{M}(q^2)$ for infinitely many q (compare with [5, Remark 6.2]).

We have $1 \in \mathbf{M}(q^2)$ (resp. $2 \in \mathbf{M}(q^2)$) provided that $q \equiv 2 \pmod 3$, or $q \equiv 3 \pmod 4$ (resp. $q \equiv 4 \pmod 5$, or $q \equiv 5 \pmod 6$). Indeed it is known that there exists $S \in \mathbb{N}$ such that $\{1, 2\} \in \mathbf{M}(q^2)$ for any $q \geq S$ (Serre [16]). This leads us to the following arithmetical question:

Question 3.7. Given a large q and $g = 1, 2$, are there nonnegative integers n, ℓ, m such that (3.2) holds true?

Example 3.8. Let $\ell = 2$, $m = 1$. In this case (3.2) becomes $n = 2g - 1 + \gcd(n, 2) + \gcd(n, 3)$. Hence if $g \equiv 0, 3 \pmod 6$ and $2g + 3 \mid (q+1)$, or $g \equiv 1, 4 \pmod 6$ and $2g + 4 \mid (q+1)$, then $g \in \mathbf{M}(q^2)$.

For instance $7 \in \mathbf{M}(17^2)$ but this information cannot be obtained from Example 3.6.

Example 3.9. Let q be a prime power, n a divisor of $q+1$, $\ell = q-1$, $m = 1$. Then by Lemma 2.1 the genus of g of $\mathcal{X}(n, q-1, 1)$ satisfies $2g = n - \gcd(n, q-1)$. In particular for $n = q+1$ we obtain $q/2 \in \mathbf{M}(q^2)$ (resp. $(q-1)/2 \in \mathbf{M}(q^2)$) if q is even (resp. odd).

Question 3.10. For a large prime power q, it is true that $[0, \lfloor q/2 \rfloor] \subseteq \mathbf{M}(q^2)$ with $\lfloor q/2 \rfloor + 1 \notin \mathbf{M}(q^2)$? (cf. [2], [13]).

Acknowledgments. The authors were in part supported respectively by IPM grant No. 93140117, and by CNPq-Brazil grant 308326/2014-8.

References

[1] A. Aguglia, G. Korchmáros and F. Torres, *Plane maximal curves*, Acta Arith. **98** (2001), 165–179.

[2] N. Arakelian, S. Tafazolian and F. Torres, *On the spectrum for the genera of maximal curves over small fields*, arXiv: 1609.04797.

[3] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28** (2000), 4707–4728.

[4] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves*, J. Number Theory **67** (1997), 29–51.

[5] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of Hermitian function fields*, Composito Math. **120** (2000), 137–170.

[6] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), 229–245.

[7] A. Garcia and S. Tafazolian, *Certain maximal curves and Cartier operators*, Acta Arith. **135** (2008), 199–218.

[8] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Curves covered by the Hermitian curve*, Finite Fields Appl. **12** (2006), 539–564.

[9] J. W.P, Hirschfeld, G. Korchmáros and F. Torres, " Algebraic curves over a finite field", Princeton Univ. Press, 2008.

[10] N. E. Hurt, "Many Rational Points: Coding Theory and Algebraic Geonetry", Kluwer, 2003.

[11] A. Kazemifard, A. R. Naghipour and S. Tafazolian, *A note on superspecial and maximal curves*, Bull. Iranian Math. Soc. **39** (2013), 405–413.

[12] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris **305** (1987), 729–732.

[13] www.manypoints.org, "manYPoints–Table of Curves with Many Points".

[14] R. Lidl and H. Niederreiter, "Finite Fields", Addison-Wesley, 1983.

[15] H-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[16] J.P. Serre, *Résumé des cours de 1983–1984*, Ann. Collége de France (1984), 79–83.

[17] S.A. Stepanov, "Arithmetic of Algebraic Curves", Consultans Bureau, 1994.

[18] H. Stichtenoth, "Algebraic function fields and codes", second ed., Grad. Texts in Math., vol. 254, Springer–Verlag, 2009.

[19] S. Tafazolian, A. Teherán-Herrera, F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curves*, J. Pure Appl. Algebra **220**(3) (2016), 1122–1132.

[20] S. Tafazolian and F. Torres, *On the curve $y^n = x^m + x$ over finite fields*, J. Number Theory **145** (2014), 51–66.

[21] S. Tafazolian and F. Torres, *On maximal curves of Fermat type*, Adv. Geom. **13** (2013), 613–617.

[22] J. Tate, *Endomorphisms of Abelian Varieties over Finite Fields*, Invent. Math. **2** (1996), 134–144.

School of Mathematics,, Institute for Research in Fundamental Sciences (IPM),, P.O. Box 19395-5746, Teheran, Iran.

E-mail address: tafazolian@gmail.com

IMECC/UNICAMP, R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP, Brazil.

E-mail address: ftorres@ime.unicamp.br