ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 45, Number 2, 2015

ON PERMUTATION BINOMIALS

MOHAMED AYAD, KACEM BELGHABA AND OMAR KIHEL

ABSTRACT. Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. Let $f(x) = ax^n + x^m$ be a binomial with coefficients in $\mathbb{F}_q$ and $d = \gcd(n-m, q-1)$. In this paper, we prove that there does not exist any permutation binomial such that d satisfies certain congruence conditions, and we do some computations to list all non permutation binomials for $n - m = 3$ and $q \leq 100$.

1. Introduction. Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbb{F}_q$ is called a permutation polynomial of $\mathbb{F}_q$ if the induced map $f : \mathbb{F}_q \to \mathbb{F}_q$ is one to one. The study of permutation polynomials goes back to Hermite [**3**] for $\mathbb{F}_p$ and Dickson [**2**] for $\mathbb{F}_q$. Lidl and Mullen [**4**] formulated a list of open problems. Permutation monomials are completely understood; however, permutation binomials are not well understood. For some partial results on the subject, see [**5, 8, 10, 11**].

We fix some notation which will be used through this paper. The letter p always denotes a prime number and $\mathbb{F}_q$ the finite field containing $q = p^r$ elements. For any polynomial $g(x) \in \mathbb{F}_q[x]$, we denote by $\overline{g(x)}$ the unique polynomial of degree at most $q-1$, with coefficients in $\mathbb{F}_q$ such that $g(x) \equiv \overline{g(x)} \pmod{(x^q - x)}$. When we refer to a binomial $f(x)$ over $\mathbb{F}_q$, we always mean a polynomial $f(x) \in \mathbb{F}_q[x]$ of the form $f(x) = ax^n + x^m$ with the nonrestrictive condition $\gcd(m, n) = 1$ (see [**9,** Example 2.1]), $n > m$ and $a \neq 0$. Let $d = \gcd(n-m, q-1)$. It is well known that, if $d = 1$, then $f(x)$ is not a permutation of $\mathbb{F}_q$. The idea of examining d for the existence of permutation polynomials is not new. For recent references on permutation binomials and a general class of polynomials of the form $x^r f(x^{(q-1)/l})$, one can see ([**1, 6, 7, 12, 13, 14**]). In this paper, we prove that there does not

2010 AMS *Mathematics subject classification.* Primary 11T06, 12E20.
Keywords and phrases. Finite fields, permutation polynomials, Hermite-Dickson's theorem.
Received by the editors on March 25, 2013.
DOI:10.1216/RMJ-2015-45-2-389

exist any permutation binomial such that d satisfies certain congruence conditions. We do some computations to list all non permutation binomials of degree smaller than q for $n-m=3$ and $q \leq 100$.

2. Non existence of permutation binomials of certain shapes. An old and yet very useful result in the theory of permutation polynomials, is the following theorem proved by Hermite for the prime fields and Dickson in the general case.

Theorem 2.1. *Let p be a prime number, $q=p^r$ and $g(x) \in \mathbb{F}_q[x]$. Then $g(x)$ is a permutation polynomial if and only if*

(i) *$g(x)=0$ has a unique solution in $\mathbb{F}_q$.*
(ii) *For every $l \in \{1,\dots,q-2\}$, $\deg \overline{g^l(x)} \leq q-2$.*

We deduce from Theorem 2.1 the following corollary.

Corollary 2.2. *Let $f(x)=ax^n+x^m \in \mathbb{F}_q[x]$, such that $a \neq 0$ and $\gcd(m,n)=1$. Let $d=\gcd(n-m,q-1)$. Suppose $d \geq 2$. Then $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*:

(i) *$f(x)=0$ has a unique solution in $\mathbb{F}_q$.*
(ii) *For every $l \in \{1,\dots,q-2\}$ such that $d \mid l$, we have $\deg \overline{f^l(x)} \leq q-2$.*

Proof. From Theorem 2.1, we have only to prove that if $l \in \{1,\dots,q-2\}$ and $d \nmid l$, then $\deg \overline{f^l(x)} \leq q-2$. Let k be an integer, and let $\overline{k}$ be the integer in $\{1,\dots,q-1\}$ such that $k \equiv \overline{k} \pmod{q-1}$. Then, modulo x^q-x, we have

$$x^k \equiv \begin{cases} 1 & \text{if } k=0 \\ x^{\overline{k}} & \text{if } k \neq 0. \end{cases}$$

It follows that if $k>0$, then $x^k \equiv x^{q-1} \pmod{x^q-x}$ if and only if $k \equiv 0 \pmod{q-1}$. Suppose that there exists $l \in \{1,\dots,q-2\}$ with $d \nmid l$ such that $\deg \overline{f^l(x)} = q-1$. We deduce from

$$(ax^n+x^m)^l = \sum_{j=0}^{l} \binom{l}{j} a^j x^{nj+m(l-j)} = \sum_{j=0}^{l} \binom{l}{j} a^j x^{(n-m)j+lm} \tag{2.1}$$

that there exists an integer $j \in \{0, \ldots, l\}$ such that

$$x^{(n-m)j+lm} \equiv x^{q-1} \pmod{x^q - x}.$$

Hence, $(n-m)j + lm > 0$ and $(n-m)j + lm \equiv 0 \pmod{q-1}$. Since $d = \gcd(n-m, q-1)$, then $d \mid (n-m)$ and $d \mid q-1$. But $\gcd(n, m) = 1$ implies that $\gcd(d, m) = 1$. Then $d \mid l$ which is a contradiction. □

One of the main results in this paper is the following theorem.

Theorem 2.3. *Let $f(x)$ be a binomial such that $d > 1$. If $p \equiv 1 \pmod{d^2}$, then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*

For the proof of Theorem 2.3, we need the following lemma.

Lemma 2.4. *Let $f(x)$ be a binomial such that $d > 1$. Let $l \in \{1, \ldots, q-2\}$ be such that $d \mid l$. Then the following assertions are equivalent*:

(i)

$$\deg f^l(x) \le q - 2 \tag{2.2}$$

(ii)

$$\sum_{\substack{j=0 \\ (n-m)j+lm \equiv 0 \pmod{q-1}}}^{l} \binom{l}{j} a^j = 0 \tag{2.3}$$

(iii)

$$\sum_{\lambda=0}^{\gamma_l} \binom{l}{j_0 + \lambda(q-1)/d} \left(a^{(q-1)/d}\right)^{\lambda} = 0, \tag{2.4}$$

where j_0 is the smallest nonnegative integer ≥ 0 satisfying

$$j_0 \equiv \frac{-lm}{(n-m)} \left(\bmod \frac{q-1}{d}\right) \equiv \frac{-lm}{d} / \frac{n-m}{d} \left(\bmod \frac{q-1}{d}\right)$$

and γ_l is the largest integer λ such that

$$j_0 + \lambda(q-1)/d \le l.$$

Proof. From equation (2.1), $\deg \overline{f^l(x)} \leq q-2$ if and only if

$$\sum_{\substack{j=0 \\ (n-m)j+lm\equiv 0 \pmod{q-1}}}^{l} \binom{l}{j} a^j = 0 \tag{2.5}$$

The condition $(n-m)j + lm \equiv 0 \pmod{q-1}$ is equivalent to

$$\frac{(n-m)}{d} j + \frac{l}{d} m \equiv 0 \left(\mod \frac{q-1}{d} \right),$$

which is equivalent to

$$j \equiv \frac{-lm}{(n-m)} \left(\mod \frac{q-1}{d} \right), \tag{2.6}$$

where j_0 is the smallest nonnegative integer satisfying (2.6). Then $j \equiv j_0 \pmod{(q-1)/d}$. Hence, equation (2.5) is equivalent to

$$\sum_{\lambda=0}^{\gamma_l} \binom{l}{j_0 + \lambda(\frac{a-1}{d})} \left((a)^{\frac{q-1}{d}} \right)^{\lambda} = 0,$$

where γ_l is the largest integer λ such that $j_0 + \lambda(\frac{q-1}{d}) \leq l$. □

Lemma 2.5 (Lucas)**.** *Let A and B be two positive integers such that*

$$A = a_0 + a_1 p + \cdots + a_s p^s$$

and

$$B = b_0 + b_1 p + \cdots + b_s p^s$$

with $0 \leq a_i < p$ and $0 \leq b_i < p$ for every $i \in \{1, \ldots, s\}$. Then

$$\binom{A}{B} \equiv \prod_{i=0}^{s} \binom{a_i}{b_i} \pmod{p}.$$

Proof of Theorem 2. We will show that equation (2.4) does not hold for $l = \frac{q-1}{d}$. Let M be the unique integer such that $0 \leq M < \frac{q-1}{d}$ and $M \equiv \frac{m}{(n-m)/d} \pmod{\frac{q-1}{d}}$. Let j_0 be the integer in equation (2.4).

Then

$$\begin{aligned} j_0 &= -\frac{l}{d}M + \lambda_0\frac{q-1}{d} \\ &= -\frac{q-1}{d^2}M + \lambda_0\frac{q-1}{d} \\ &= \frac{q-1}{d^2}(-M + \lambda_0 d). \end{aligned}$$

The above integer j_0 is the smallest nonnegative integer that can be written under the form $j_0 = \frac{q-1}{d^2}(-M + \lambda_0 d)$, for a certain integer λ_0. Obviously, $-M + \lambda_0 d < d$, otherwise $-M + (\lambda_0 - 1)d \geq 0$, which contradicts the minimality of j_0. Suppose that $-M + \lambda_0 d = 0$, then $d \mid M$. Since $M = m(\frac{n-m}{d})^{-1} + \mu\frac{q-1}{d}$ for a certain $\mu \in \mathbb{Z}$ and

$$\left(\frac{n-m}{d}\right)^{-1} \in \left\{1, \ldots, \frac{q-1}{d} - 1\right\} \quad \text{and} \quad d \mid \frac{q-1}{d},$$

then $d \mid m$; hence, $d \mid n$, which is a contradiction to $\gcd(m, n) = 1$. Therefore,

$$0 < -M + \lambda_0 d < d \quad \text{and} \quad j_0 = \frac{q-1}{d^2}M_0,$$

with $0 < M_0 = -M + \lambda_0 d < d$. Then $j_0 > 0$ and γ_l in equation (4) verifies

$$j_0 + \gamma_l\frac{q-1}{d} \leq l = \frac{q-1}{d}.$$

Hence, $\gamma_l = 0$.

Equation (2.4) is equivalent to $\binom{\frac{q-1}{d}}{j_0} = 0$. On the other hand,

$$\frac{q-1}{d} = \frac{p-1}{d} + \frac{p-1}{d}p + \cdots + \frac{p-1}{d}p^{r-1}$$

and

$$j_0 = \frac{q-1}{d^2}M_0 = \frac{p-1}{d^2}M_0 + \frac{p-1}{d^2}M_0 p + \cdots + \frac{p-1}{d^2}M_0 p^{r-1},$$

with

$$\frac{p-1}{d^2}M_0 < \frac{p-1}{d^2}d = \frac{p-1}{d} < p - 1.$$

Then, Lemma 2.5 implies that

$$\binom{\frac{q-1}{d}}{j_0} \equiv \binom{\frac{p-1}{d}}{M_0 \frac{p-1}{d^2}}^r \not\equiv 0 \pmod{p}.$$

Hence, $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$. □

Corollary 2.6. *Let $f(x)$ be a binomial. If $p \equiv 1 \pmod{(n-m)^2}$, then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*

Proof. We have $d = \gcd(n-m, q-1) = n-m$. If $n-m = 1$, then $f(x)$ is not a permutation polynomial by the observation made in the introduction of this paper. If $n-m \geq 2$, the result follows from Theorem 2. □

Corollary 2.7. *Let $f(x)$ be a binomial. If $p \equiv 1 \pmod 4$ and $\gcd(n-m, q-1) = 2$, then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*

Proof. The hypothesis of Theorem 2.3 is verified with $d = \gcd(n-m, q-1) = 2$. □

Theorem 2.8. *Let $f(x)$ be a binomial such that $d > 1$. Suppose that there exists an integer $\delta > \frac{d}{2}$ such that $n \equiv 0 \pmod{2\delta}$ and $q \equiv 1 \pmod{2\delta}$. Then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*

Proof. We will prove that equation (2.3) does not hold for

$$l = \frac{q-1}{2\delta} \leq q-2.$$

Since

$$(n-m)l + lm = nl = \frac{n}{2\delta}(q-1) \equiv 0 \pmod{q-1},$$

then one of the values of j is l. Then

$$l = \frac{q-1}{2\delta} = j_0 + \lambda\left(\frac{q-1}{d}\right).$$

We have

$$l = j_0 + \lambda\frac{q-1}{d} > j_0 + \lambda\frac{q-1}{2\delta} = j_0 + \lambda l,$$

which implies that $\lambda = 0$ and $l = j_0$. Hence, equation (2.3) reduces to $\binom{l}{l} = 0$, which is a contradiction. Then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$. □

Theorem 2.9. *Let $f(x) = ax^n + x^m$ be a binomial. Suppose that n is even, $p \neq 2$, $n \equiv m \pmod 9$ and $\gcd(n-m, q-1) = 3$. Then the following assertions hold*:

(i) *If $p \equiv -1 \pmod 3$, then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*
(ii) *If $p \equiv 1 \pmod 3$ and for every primitive cubic root of unit ζ in $\mathbb{F}_p$, the polynomial $g(x) = \zeta a x^{n-m} + 1$ has no root in $\mathbb{F}_q$, then $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$.*

Proof. Suppose that $f(x)$ is a permutation polynomial, then equation (2.3) holds for $l = \frac{q-1}{2}$. From the equality

$$(n-m)\frac{q-1}{6} + \frac{q-1}{2}m = \frac{n+2m}{6}(q-1)$$

and the hypothesis n is even, we deduce that one of the values of j in equation (2.3) is $j = \frac{q-1}{6}$. Hence,

$$\frac{q-1}{6} = j_0 + \lambda\frac{q-1}{3},$$

which implies that $\lambda = 0$ and $j_0 = \frac{q-1}{6}$. We have

$$l = \frac{q-1}{2} = \frac{q-1}{6} + \frac{q-1}{3} = j_0 + \frac{q-1}{3}.$$

Hence, equation (2.3) reduces to

$$\binom{l}{j_0}(a)^{j_0} + (a)^l = 0.$$

Then

$$(a)^{\frac{q-1}{3}} + \binom{\frac{q-1}{2}}{\frac{q-1}{6}} = 0;$$

hence,

$$(a)^{\frac{q-1}{3}} = -\binom{\frac{q-1}{2}}{\frac{q-1}{6}}$$

Let $\epsilon = -\binom{\frac{q-1}{2}}{\frac{q-1}{6}}$. Clearly, ϵ is a cubic root of unity. If (i) holds, the unique cubic root of unity in $\mathbb{F}_p$ is 1, then $\epsilon = 1$ and $(a)^{\frac{q-1}{3}} = 1$. Since

$$\frac{q-1}{3} \quad \text{and} \quad \frac{n-m}{3}$$

are relatively prime, then, there exists x and y in $\mathbb{Z}$ such that

$$x\frac{n-m}{3} + y\frac{q-1}{3} = 1.$$

It follows that

$$a = (a)^{x(\frac{n-m}{3})} \cdot (a)^{y(\frac{q-1}{3})} = (a)^{x(\frac{n-m}{3})} = \left[(a)^{x^2(\frac{n-m}{9})}\right]^{(n-m)}.$$

Let $c = a^{x^2(\frac{n-m}{9})}$. Then

$$\frac{-1}{a} = \left(\frac{-1}{c}\right)^{n-m}.$$

Hence, $f(0) = f(-1/c) = 0$, which implies that f is not one-to-one, which is a contradiction.

Suppose that (ii) holds. We have $(a)^{\frac{q-1}{3}} = \epsilon$. Then $\epsilon^3 = 1$, i.e., ϵ is a root of unity in $\mathbb{F}_p$. Using the above Bezout identity, we obtain

$$\begin{aligned} a &= (a)^{x(\frac{n-m}{3})} \cdot (a)^{y(\frac{q-1}{3})} \\ &= \epsilon^y \, (a)^{x(\frac{n-m}{3})} \\ &= \epsilon^y \left(\epsilon^y \, (a)^{x(\frac{n-m}{3})}\right)^{x(\frac{n-m}{3})} \\ &= \epsilon^{y(1+x(\frac{n-m}{3}))} \left((a)^{x^2(\frac{n-m}{9})}\right)^{n-m} \\ &= \epsilon^y \left((a)^{x^2(\frac{n-m}{9})}\right)^{n-m}. \end{aligned}$$

Let $c = a^{x^2 \frac{n-m}{9}}$. Then $a = \epsilon^y (c)^{n-m}$. Hence, $\eta a(-1/c)^{n-m} + 1 = 0$, where $\eta = \epsilon^{-y}$. If $\eta = 1$, then $f(0) = f(-1/c) = 0$, which is a contradiction to f is one-to-one. If $\eta = \zeta$ is a primitive cubic root of unity, then $g(-1/c) = 0$, where $g(x) = \zeta a x^{n-m} + 1$, which is exactly the hypothesis in (ii). □

Remark 2.10. The conditions on p and n in Theorem 2.9 can be stated as follows:

(i) $p \equiv 2$ or $5 \pmod 9$ and $n \equiv 2$ or $4 \pmod 6$.
(ii) $p \equiv 4$ or $7 \pmod 9$ and $n \equiv 1$ or $2 \pmod 3$.

Theorem 2.11. *Let k and d be positive integers such that $d \geq 2$, $1 \leq k \leq d-1$, $d \mid q-1$ and $d^2 < q-1$. Then, for any $a \in \mathbb{F}_q$, the polynomial $f(x) = ax^{m+d} + x^m$ does not permute $\mathbb{F}_q$ if m satisfies one of the following conditions.*

(i) $m = k(q-1)/d$.
(ii) $m = u + k(q-1)/d$ *with*

$$\frac{q-1}{d} - d \leq u \leq \frac{q-1}{d} - 1$$

and

$$\binom{d}{\frac{q-1}{d} - u} \neq 0 \pmod p.$$

Proof. Suppose that $f(x)$ permutes $\mathbb{F}_q$ for some $a \in \mathbb{F}_q^\star$ and some m satisfying (i) or (ii). Then a is a root of (2.4) for $l = d$. The integer $j = j_0 + \lambda(q-1)/d$ appearing in this equation fulfills the conditions $0 \leq j \leq d$ and $j + m \equiv 0 \pmod{(q-1)/d}$. If $\lambda \geq 1$, then $j \geq (q-1)/d > d$, which is excluded. It follows that $\lambda = 0$, $j_0 \equiv -m \pmod{(q-1)/d}$ and equation (3) reduces to $\binom{d}{j_0} \equiv 0 \pmod p$. In case (i), we obtain $j_0 = 0$, and then $\binom{d}{0} \equiv 0 \pmod p$, a contradiction. In the second case we have $j_0 = \frac{q-1}{d} - u$ and the integer $\binom{d}{\frac{q-1}{d} - u}$ is nonzero modulo p by assumption. Therefore, we also get a contradiction in this case. □

Example 2.12. Let $d = 3$ and $q = p^r$. The conditions relating d and q in this theorem read $q \equiv 1 \pmod 3$ and $q - 1 > 9$. Suppose that $3 \nmid (q-1)/3$, and let $m = k(q-1)/3$ with $k \in \{1, 2\}$ or $m = 2(q-1)/3 - c$, with $c = 1, 2, 3$. Then for any $a \in \mathbb{F}_q^\star$, the polynomial $f(x) = ax^{m+3} + x^m$ does not permute $\mathbb{F}_q$.

Here is the complete list of all binomials of degree smaller than q obtained in this way for $n - m = 3$ and $q \leq 100$.

$q = 13$, $f(x) = ax^7 + x^4$, $ax^{11} + x^8$, $ax^8 + x^5$, $ax^9 + x^6$, $ax^{10} + x^7$.

$q=5^2$, $f(x)=ax^{11}+x^8$, $ax^{19}+x^{16}$, $ax^{16}+x^{13}$, $ax^{17}+x^{14}$, $ax^{18}+x^{15}$.
$q=31$, $f(x)=ax^{13}+x^{10}$, $ax^{23}+x^{20}$, $ax^{20}+x^{17}$, $ax^{21}+x^{18}$, $ax^{22}+x^{19}$.
$q=43$, $f(x)=ax^{17}+x^{14}$, $ax^{31}+x^{28}$, $ax^{28}+x^{25}$, $ax^{29}+x^{26}$, $ax^{30}+x^{27}$.
$q=7^2$, $f(x)=ax^{19}+x^{16}$, $ax^{35}+x^{32}$, $ax^{32}+x^{29}$, $ax^{33}+x^{30}$, $ax^{34}+x^{31}$.
$q=61$, $f(x)=ax^{23}+x^{20}$, $ax^{43}+x^{40}$, $ax^{40}+x^{37}$, $ax^{41}+x^{38}$, $ax^{42}+x^{39}$.
$q=67$, $f(x)=ax^{25}+x^{22}$, $ax^{47}+x^{44}$, $ax^{44}+x^{41}$, $ax^{45}+x^{42}$, $ax^{46}+x^{43}$.
$q=79$, $f(x)=ax^{29}+x^{26}$, $ax^{55}+x^{52}$, $ax^{52}+x^{49}$, $ax^{53}+x^{50}$, $ax^{54}+x^{51}$.
$q=97$, $f(x)=ax^{35}+x^{32}$, $ax^{67}+x^{64}$, $ax^{64}+x^{61}$, $ax^{65}+x^{62}$, $ax^{66}+x^{63}$.

Acknowledgments. The authors express their gratitude to the anonymous referee for constructive suggestions to improve an earlier draft of this paper. The third author was supported in part by NSERC.

REFERENCES

1. A. Akbary and Q. Wang, *On polynomials of the form $x^r f(x^{(q-1)/l})$*, Int. J. Math. Math. Sci. **2007**, Article ID 23408, 7 pages.

2. L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. Math. **11** (1896/97), 161–183.

3. C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

4. R. Lidl and G.L. Mullen, *When does a polynomial permute the elements of the field?*, The Amer. Math. Month. **95** (1988), 243–246.

5. R. Lidl and H. Niedereiter, *Finite fields*, in *Encyclopedia of mathematics and its applications*, Cambridge University Press, Cambridge, 2008.

6. A. Masuda and M. Zieve, *Permuation binomials over finite fields*, Trans. Amer. Math Soc. **361** (2009), 4169–4180.

7. ———, *Nonexistence of permutation binomials of certain shapes*, Electr. J. Comb. **14** (2007), Note 15, 5 pp.

8. C. Small, *Permutation binomials*, Inter. J. Math. Math. Sci. **13** (1990), 337–342.

9. ———, *Arithmetic of finite fields*, Marcel Dekker, Inc., New York, 1991.

10. G. Turnwald, *Permutation polynomials of binomial type*, in *Contributions to general algebra* 6, Holder-Pichler-Tempsky, Vienna, 1988.

11. D.Q. Wan and R. Lidl, *On permutation polynomials*, Finite Fields Appl. **8** (2002), 311–322.

12. L. Wang, *On permutation polynomials*, Finite Fields Appl. **8** (2002), 311–322.

13. M. Zieve, *Some families of permutation polynomails over finite fields*, Int. J. Num. Theor. **4** (2008), 851–857.

14. ———, *On some permutation polynomials over* $\mathbb{F}_q$ *of the form* $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc. **137** (2009), 2209–2216.

Laboratoire de Mathématiques Pures et Appliquées, Université du Littoral, F-62228 Calais, France
Email address: **ayad@lmpa.univ-littoral.fr**

Laboratoire de Mathématiques et ses Applications, Université d'Oran à Es Senia, Bp 1524, Algeria
Email address: **belghaba.kacem@univ-oran.dz**

Department of Mathematics, Brock University, Ontario, Canada L2S 3A1
Email address: **okihel@brocku.ca**