Palestine Journal of Mathematics

Vol. 5(Special Issue: 1) (2016) , 167–174

Constacyclic Codes Over The Ring $F_p + vF_p + v^2F_p$

Mohammed M. Al-Ashker and Mariam I. Satariah

Communicated by Taher Abualrub

MSC 2010 Classifications: Primary 94B05; Secondary 51E22.

Keywords and phrases: Constacyclic codes, Polynomial generator, Generator set in standard form.

Abstract. In this paper, we study constacyclic codes over the ring $R = F_p + vF_p + v^2F_p$, where p is an odd prime and $v^3 = v$. The polynomial generators of all constacyclic codes over R are characterised and their dual codes are also determined.

1 Introduction

Since the discovery that many good non-linear codes over finite fields are ac- tually closely related to linear codes over Z_4 via the Gray map (see [1]), codes over finite rings have received a great deal of attention (e.g. see [11]-[7], [9]). In these studies, most of them are concentrated on the case that the ground rings associated with codes are finite chain rings. However, it turns out that optimal codes over non-chain rings exist. In [2], Yildiz and Karadeniz considered linear codes over the ring $R_1 = F_2 + uF_2 + vF_2 + uvF_2$ with $u^2 = v^2 = 0$ and $uv = vu$; some good binary codes were obtained as the images of cyclic codes over R_1 under two Gray maps. In [10], Zhu, Wang and Shi studied the structure and properties of cyclic codes over $F_2 + vF_2$, where $v^2 = v$; the authors showed that cyclic codes over the ring are principally generated. In the subsequent paper [8], Zhu and Wang investigated a class of constacyclic codes over $F_p + vF_p$ with p being an odd prime and $v^2 = v$. It was proved that the image of a $(1 - 2v)$-constacyclic code of length n over $F_p + vF_p$ under the Gray map is a distance-invariant cyclic code of length $2n$ over F_p and $(1 - 2v)$-constacyclic codes over the ring are principally generated. In [13] constacyclic codes over $F_p + vF_p$ where studied by Guanghui and Bocong. These rings in the mentioned papers are finite not chain rings.

In this paper, we mainly study the structure of constacyclic codes over $R = F_p + vF_p + v^2F_p$ of arbitrary length and also discuss the dual of these codes.

2 Breliminaries

Let F_p be the finite field of order p and ${F_p}^*$ the multiplicative group of F_p, where p is an odd prime. It is known that $F_p[x]/\langle x^n - \lambda\rangle$ is a principal ideal ring for any element λ in ${F_p}^*$. If $p(x) + \langle x^n - \lambda\rangle \in F_p[x]/\langle x^n - \lambda\rangle$, then the ideal generated by $p(x) + \langle x^n - \lambda\rangle$, denoted by $\langle p(x)\rangle$, is the smallest ideal in $F_p[x]/\langle x^n - \lambda\rangle$ containing $p(x)+\langle x^n - \lambda\rangle$. In addition, we adopt the notation $[g(x)]$ to denote the ideal in $F_p[x]/\langle x^n - \lambda\rangle$ generated by $g(x)+\langle x^n - \lambda\rangle$ with $g(x)$ being a monic divisor of $x^n - \lambda$; in that case, $g(x)$ is called a generator polynomial. Throughout this paper, R denotes the commutative ring $F_p + vF_p + v^2F_p = \{a + vb + v^2c | a, b, c \in F_p\}$ with $v^3 = v$. Recall that R is a principal ideal ring and has six non-trivial ideals, namely $\langle v\rangle$ = $\{va : a \in F_p\}$, $\langle 1 + v\rangle$ = $\{(1 + v)b : b \in F_p\}$, $\langle -1 + v\rangle$ = $\{(-1 + v)c : c \in F_p\}$, $\langle 1 - v^2\rangle$ = $\{(1 - v^2)d : d \in F_p\}$, $\langle v + v^2\rangle$ = $\{(v + v^2)e : e \in F_p\}$ *and* $\langle -v + v^2\rangle$ = $\{(-v + v^2)f : f \in F_p\}$, and the maximal ideals in R are $\langle v\rangle, \langle 1 + v\rangle$ and $\langle -1 + v\rangle$, hence R is not a chain ring. Let R^n be R-module of n-tuples over R. A linear code C of length n over R is an R-submodule of R^n. For any linear code C of length n over R, the dual $C^\perp$ is defined as $C^\perp = \{u \in R^n | u.w = 0 \text{ for any } w \in C\}$, where $u.w$ denotes the standard Euclidean inner product of u and w in R^n. Note that $C^\perp$ is linear whether or not C is linear. The Gray map ψ from R to $F_p \oplus F_p \oplus F_p$ given by $\psi(c) = (a + b, b + c, 2a + c)$, is a ring isomorphism, which means that

R is isomorphic to the ring $F_p \oplus F_p \oplus F_p$. Therefore R is a finite Frobenius ring. If C is linear, then $|C||C^\perp| = |R|^n$ (See [6]).

Let θ be a unit in R. A linear code C of length n over R is called θ-constacyclic if for every $(c_0, c_1, ..., c_{n-1}) \in C$, we have $(\theta c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$. It is well known that a θ-constacyclic code of length n over R can be identified with an ideal in the quotient ring $R[x]/\langle x^n - \theta\rangle$ via the R-module isomorphism as follows:

$$R^n \to R[x]/\langle x^n - \theta\rangle$$

$$(c_0, c_1, ..., c_{n-1}) \mapsto (c_0 + c_1 x + ... + c_{n-1}x^{n-1})(mod\, \langle x^n - \theta\rangle).$$

If $\theta = 1$, θ-constacyclic codes are just cyclic codes and while $\theta = -1$, θ-constacyclic codes are known as negacyclic codes.

Let A, B and C be codes over R. We denote $A \oplus B \oplus C = \{a + b + c | a \in A, b \in B, c \in C\}$. Note that any element d of R^n can be expressed as $d = a + vb + v^2c = v(a + b + c) + (-v + v^2)(a + c) + (1 - v^2)a$, where $a, b, c \in F_p^n$. Let C be a linear code of length n over R. Define
$C_v = \{b \in F_p^n | va + (-v + v^2)b + (1 - v^2)c \in C \text{ for some } a, c \in F_p^n\}$,
$C_{-v+v^2} = \{c \in F_p^n | va + (-v + v^2)b + (1 - v^2)c \in C \text{ for some } a, b \in F_p^n\}$,
$C_{1-v^2} = \{a \in F_p^n | va + (-v + v^2)b + (1 - v^2)c \in C \text{ for some } b, c \in F_p^n\}$.
Obviously, C_v, C_{-v+v^2} and C_{1-v^2} are linear codes over F_p. By definition of C_v, C_{-v+v^2} and C_{1-v^2}, we have that C can be uniquely expressed as $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$. It can be routine to check that for any elements $a \in C_{1-v^2}$, $b \in C_v$ and $c \in C_{-v+v^2}$, we get $va + (-v + v^2)b + (1 - v^2)c \in C$; in particular, $|C| = |C_{-v+v^2}||C_v||C_{1-v^2}|$.

3 Constacyclic Codes Over The Ring $R = F_p + vF_p + v^2F_p$

In this subsection, we let $R_{p,n} = R_p[x]/\langle x^n - \theta\rangle$ with $\theta = \lambda + v\mu + v^2\kappa$ being a unit in R_p, where λ, μ and κ are elements in F_p. As usual, we identify R_n with the set of all polynomials over R_p of degree less than n. Let $f_1(x), f_2(x), ..., f_s(x) \in R_n$. The ideal generated by $f_1(x), f_2(x), ..., f_s(x)$ will be denoted by $\langle f_1(x), f_2(x), ..., f_s(x)\rangle$.
The following lemma characterizes the units in R_p.

Lemma 3.1. *Let $\theta = \lambda + v\mu + v^2\kappa$ be an element in R_p, where λ, μ and κ are elements in F_p. Then if $\theta = \lambda + v\mu + v^2\kappa$ is a unit of R_p, then $\lambda \neq 0$ and $\lambda - \mu + \kappa \neq 0$.*

Proof. Suppose that $\theta = \lambda + v\mu + v^2\kappa$ is a unit of R_p. Then there exists elements $a, b, c \in F_p$ and $\theta' = a + vb + v^2c$ such that $\theta\theta' = 1$, that is; $(\lambda + v\mu + v^2\kappa)(a + vb + v^2c) = \lambda a + v(\lambda b + \mu a + \mu c + \kappa b) + v^2(\lambda c + \mu b + \kappa a + \kappa c) = 1$. So we have the following:
$\lambda a = 1$ (1),
$(\lambda + \kappa)b + \mu a + \mu c = 0$ (2) and
$(\lambda + \kappa)c + \mu b + \kappa a = 0$ (3)
from (1) we have $\lambda \neq 0$ and $a \neq 0$, in (3) if $\lambda + \kappa = 0$, $\mu = 0$ we have $\kappa a = 0$ and since $a \neq 0$, so $\kappa = 0$, which implies that $\lambda = 0$ which is contradiction. Hence $\lambda + \kappa \neq 0$ or $\mu \neq 0$. So we have three cases:

Case(1) : if $\lambda + \kappa \neq 0$ and $\mu = 0$, we have $\lambda - \mu + \kappa \neq 0$.

Case(2) : if $\lambda + \kappa = 0$ and $\mu \neq 0$, we have $\lambda - \mu + \kappa \neq 0$.

Case(3) : if $\lambda + \kappa \neq 0$ and $\mu \neq 0$, we want to prove that $\lambda - \mu + \kappa \neq 0$. Let for contrary that $\lambda - \mu + \kappa = 0$, then $\lambda + \kappa = \mu$, by substituting in (2), we have $\mu(a + b + c) = 0$, since $\mu \neq 0$, then $a + b + c = 0$, that is $b + c = -a$, but by substituting in (3), we have $\mu(c + b) + \kappa a = 0$, then $-\mu a + \kappa a = 0$, hence $a(\kappa - \mu) = 0$, and since $a \neq 0$, then $\kappa - \mu = 0$, and by the assumption that $\lambda - \mu + \kappa = 0$, we have $\lambda = 0$ which make a contradiction. Therefore $\lambda - \mu + \kappa \neq 0$. □

Note that the converse of the last Lemma is not true. For example $2 + v + 2v^2$ is unit in R_3 but $\lambda - \mu + \kappa = 2 - 1 + 2 = 0$.

Theorem 3.2. *Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a linear code of length n over R. Then C is θ-constacyclic code of length n over R if and only if C_{1-v^2} is the zero code, C_v is $(\lambda-\mu+\kappa)$-constacyclic code and C_{-v+v^2} is λ-constacyclic code of length n over F_p.*

Proof. $\Rightarrow$) Let $(r_0, r_1, ..., r_{n-1})$ be an arbitrary element in C_{1-v^2}, $(q_0, q_1, ..., q_{n-1})$ be an arbitrary element in C_v and $(s_0, s_1, ..., s_{n-1})$ be an arbitrary element in C_{-v+v^2}. We assume that $c_i = vr_i + (-v+v^2)q_i + (1-v^2)s_i$, $i = 0, 1, ..., n-1$; hence we get $(c_0, c_1, ..., c_{n-1}) \in C$. Since C is a θ-constacyclic code of length n over R, then $(\theta c_{n-1}, c_0, ..., c_{n-2}) \in C$. Note that:
$\theta c_{n-1} = (\lambda + v\mu + v^2\nu)[vr_{n-1} + (-v+v^2)q_{n-1} + (1-v^2)s_{n-1}] = v\lambda r_{n-1} + v^2\mu r_{n-1} + v\kappa r_{n-1} + (-v+v^2)\lambda q_{n-1} + (-v+v^2)(-\mu)q_{n-1} + (-v+v^2)\kappa q_{n-1} + (1-v^2)\lambda s_{n-1} = v(\lambda+\kappa)r_{n-1} + v^2\mu r_{n-1} + (-v+v^2)[(\lambda-\mu+\kappa)q_{n-1}] + (1-v^2)[\lambda s_{n-1}] \in C$ (since C is linear), then $r_{n-1} = 0$ and $(\theta c_{n-1}, c_0, c_1, ..., c_{n-2}) = (-v+v^2)((\lambda-\mu+\kappa)q_{n-1}, q_0, ..., q_{n-2}) + (1-v^2)(\lambda s_{n-1}, s_0, ..., s_{n-2}) \in C$. Therefore $((\lambda-\mu+\kappa)q_{n-1}, q_0, ..., q_{n-2}) \in C_v$ and $(\lambda s_{n-1}, s_0, ..., s_{n-2}) \in C_{-v+v^2}$, which implies that C_{1-v^2} is zero code, C_v and C_{-v+v^2} are $(\lambda-\mu+\kappa)$-constacyclic and λ-constacyclic codes of length n over F_p, respectively.
$\Leftarrow$ Suppose that C_{1-v^2} is zero code, C_v and C_{-v+v^2} are $(\lambda-\mu+\kappa)$-constacyclic and λ-constacyclic codes of length n over F_p, respectively. Let $(c_0, c_1, ..., c_{n-1}) \in C$, where $c_i = vr_i + (-v+v^2)q_i + (1-v^2)s_i$, $i = 0, 1, ..., n-1$. It follows that $(q_0, q_1, ..., q_{n-1}) \in C_v$ and $(s_0, s_1, ..., s_{n-1}) \in C_{-v+v^2}$. Note that $(\theta c_{n-1}, c_0, ..., c_{n-2}) = (-v+v^2)((\lambda-\mu+\kappa)q_{n-1}, q_0, ..., q_{n-2}) + (1-v^2)(\lambda s_{n-1}, s_0, ..., s_{n-2}) \in (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2} = C$. Hence C is θ-constacyclic code of length n over R. □

Theorem 3.3. *Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R. Then $C = \langle (-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x) \rangle$, where $g_v(x)$ and $g_{-v+v^2}(x)$ are the generator polynomials of C_v and C_{-v+v^2}, respectively.*

Proof. Since C_v and C_{-v+v^2} are $(\lambda-\mu+\kappa)$-constacyclic and λ-constacyclic codes of length n over F_p, respectively, we will assume that the generator polynomials of C_v and C_{-v+v^2} are $g_v(x)$ and $g_{-v+v^2}(x)$, respectively. Then $(-v+v^2)g_v(x) \in (-v+v^2)C_v \subseteq C$ and $(1-v^2)g_{-v+v^2} \in (1-v^2)C_{-v+v^2} \subseteq C$, hence $\langle (-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x) \rangle \subseteq C$.
Let $f(x) \in C$. Since $C = (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$, then there are $s'(x) = g_v(x)s(x) \in C_v$ and $u'(x) = g_{-v+v^2}(x)u(x) \in C_{-v+v^2}$ such that $f(x) = (-v+v^2)s'(x) + (1-v^2)u'(x) = (-v+v^2)g_v(x)s(x) + (1-v^2)g_{-v+v^2}u(x)$, where $s(x), u(x) \in F_p[x] \subseteq R_p[x]$. Hence $f(x) \in \langle (-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x) \rangle$. Therefore $C \subseteq \langle (-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x) \rangle$.
This gives that $C = \langle (-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x) \rangle$. □

Proposition 3.4. *Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R_p and $g_v(x)$, $g_{-v+v^2}(x)$ are generator polynomials of C_v and C_{-v+v^2}, respectively. Then $|C| = p^{3n - deg(g_v(x)) - deg(g_{-v+v^2}(x))}$.*

Proof. Since $|C| = |C_v||C_{-v+v^2}||C_{1-v^2}|.Then, |C| = p^{3n - deg(g_v(x)) - deg(g_{-v+v^2}(x))}$. □

Here we have three canonical projections defined as follows:

$$\sigma : R_p = F_p + vF_p + v^2F_p \to F_p$$
$$va + (-v+v^2)b + (1-v^2)c \longmapsto a;$$
$$\rho : R_p = F_p + vF_p + v^2F_p \to F_p$$
$$va + (-v+v^2)b + (1-v^2)c \longmapsto b;$$

and

$$\tau : R_p = F_p + vF_p + v^2F_p \to F_p$$
$$va + (-v+v^2)b + (1-v^2)c \longmapsto c.$$

Denote by r^σ, r^ρ and r^τ the images of an element $r \in R_p$ under these three projections, respectively. These three projections can be extended naturally from R_p^n to F_p^n and from $R_p[x]$ to

$F_p[x]$.

Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}$, where $a_i \in R_p$ for $0 \le i \le n-1$, and we denote $f(x)^\sigma = a_0^\sigma + a_1^\sigma x + ... + a_{n-1}^\sigma x^{n-1}$; $f(x)^\rho = a_0^\rho + a_1^\rho x + ... + a_{n-1}^\rho x^{n-1}$; $f(x)^\tau = a_0^\tau + a_1^\tau x + ... + a_{n-1}^\tau x^{n-1}$.

Hence $f(x)$ has a unique expression as $f(x) = vf(x)^\sigma + (-v+v^2)f(x)^\rho + (1-v^2)f(x)^\tau$

For a code C of length n over R_p, $a \in R_p$. The submodule quotiont is a linear code of length n over R_p, defined as follows:

$$(C : a) = \left\{r \in R_p^n | ar \in C\right\}.$$

Theorem 3.5. *Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R_p. If $C = \langle(-v+v^2)h_1(x), (1-v^2)h_2(x)\rangle$, where $h_1(x)$, $h_2(x) \in F_p[x]$ are monic with $h_1(x)/(x^n - (\lambda - \mu + \kappa))$ and $h_2(x)/(x^n - \lambda)$, then $C_v = [h_1(x)]$ and $C_{-v+v^2} = [h_2(x)]$, that is, $h_1(x)$ and $h_2(x)$ are the generator polynomials of constacyclic codes of C_v and C_{-v+v^2}, respectively.*

Proof. We shall prove the theorem by carrying out of the following steps:

Step(1) :If $C = (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$, then $(C : (-v+v^2))^\rho = C_v$ and $(C : (1-v^2))^\tau = C_{-v+v^2}$.

Let $a \in (C : (-v+v^2))$, then $(-v+v^2)a \in C$. Setting $a = va^\rho + (-v+v^2)a^\rho + (1-v^2)b$, where $b \in F_p^n$. Hence $(-v+v^2)a^\rho = (-v+v^2)[va^\rho + (-v+v^2)a^\rho + (1-v^2)b] = (-v+v^2)a \in C$. Therefore $a^\rho \in C_v$, which implies that $(C : (-v+v^2))^\rho \subseteq C_v$. Let $y \in C_v, C_{1-v^2}$, then there exists $z \in F_p^n$ such that $vy + (-v+v^2)y + (1-v^2)z \in C$. Note that $(-v+v^2)y = (-v+v^2)[vy + (-v+v^2)y + (1-v^2)z] \in (-v+v^2)C \subseteq C$ and $y = vy + (-v+v^2)y + (1-v^2)y$, so $y \in (C : (-v+v^2))$ and $y^\rho = y$. Hence $C_v \subseteq (C : (-v+v^2))^\rho$. Therefore $(C : (-v+v^2))^\rho = C_v$.

Let $c \in (C : (1-v^2))$, then $(1-v^2)c \in C$. Setting $c = va'(x) + (-v+v^2)b'(x) + (1-v^2)c^\tau$, where $a'(x), b'(x) \in F_p^n$. Hence $(1-v^2)[va'(x) + (-v+v^2)b'(x) + (1-v^2)c^\tau] = (1-v^2)c \in C$. Therefore $c^\tau \in C_{-v+v^2}$, which implies that $(C : (1-v^2))^\tau \subseteq C_{-v+v^2}$. Let $y \in C_{-v+v^2}$, then there exists $w, z \in F_p^n$ such that $vw + (-v+v^2)z + (1-v^2)y \in C$. Note that $(1-v^2)y = (1-v^2)[vw + (-v+v^2)z + (1-v^2)y] \in (1-v^2)C \subseteq C$ and $y = vy + (-v+v^2)y + (1-v^2)y$, so $y \in (C : (1-v^2))$ and $y = y^\tau$. Hence $C_{-v+v^2} \subseteq (C : (1-v^2))^\tau$. Therefore $(C : (1-v^2))^\tau = C_{-v+v^2}$.

Step(2) :If $C = \langle(-v+v^2)h_1(x), (1-v^2)h_2(x)\rangle$,then $(C : (-v+v^2))^\rho = [h_1(x)]$ and $(C : (1-v^2))^\tau = [h_2(x)]$.

Let $f(x) \in (C : (-v+v^2))$, then $(-v+v^2)f(x) \in C$. So we have that $(-v+v^2)f(x) = (-v+v^2)h_1(x)s_1(x) + (1-v^2)h_2(x)t_1(x)$, for some $s_1(x), t_1(x) \in R_{p,n}$. Write $f(x) = (-v+v^2)f(x)^\rho + (1-v^2)f(x)^\tau$, $s_1(x) = (-v+v^2)s_1(x)^\rho + (1-v^2)s_1(x)^\tau$ and $t_1(x) = (-v+v^2)t_1(x)^\rho + (1-v^2)t_1(x)^\tau$, where $f(x)^\rho, f(x)^\tau, s_1(x)^\rho, s_1(x)^\tau, t_1(x)^\rho, t_1(x)^\tau \in F_p[x]$. Thus $(-v+v^2)[(-v+v^2)f(x)^\rho + (1-v^2)f(x)^\tau] = (-v+v^2)h_1(x)[(-v+v^2)s_1(x)^\rho + (1-v^2)s_1(x)^\tau] + (1-v^2)h_2(x)[(-v+v^2)t_1(x)^\rho + (1-v^2)t_1(x)^\tau]$. Thus $2(-v+v^2)f(x)^\rho = 2(-v+v^2)h_1(x)s_1(x)^\rho + (1-v^2)h_2(x)t_1(x)^\tau$, which forces that $f(x)^\rho = h_1(x)s_1(x)^\rho$. This shows that $f(x)^\rho \in [h_1(x)]$. Therefor $(C : (-v+v^2))^\rho \subseteq [h_1(x)]$. Conversely; if $f(x) \in [h_1(x)]$, then $f(x) = h_1(x)r_1(x)$, for some $r_1(x) \in F_p[x]$. Hence $(-v+v^2)f(x) = (-v+v^2)h_1(x)r_1(x) \in \langle(-v+v^2)h_1(x), (1-v^2)h_2(x)\rangle = C$, which shows that $f(x) \in (C : (-v+v^2))$; note that $f(x) = vf(x) + (-v+v^2)f(x) + (1-v^2)f(x)$, so $f(x) = f(x)^\rho$. Hence $f(x) \in (C : (-v+v^2))^\rho$. We obtain that $[h_1(x)] \subseteq (C : (-v+v^2))^\rho$. Then we have $(C : (-v+v^2))^\rho = [h_1(x)]$.

Now we prove the second equality in this step.

Let $f(x) \in (C : (1-v^2))$, then $(1-v^2)f(x) \in C$. So we have that $(1-v^2)f(x) = (-v+v^2)h_1(x)s_2(x) + (1-v^2)h_2(x)t_2(x)$, for some $s_2(x), t_2(x) \in R_p^n$. Write $f(x) = (-v+v^2)f(x)^\rho + (1-v^2)f(x)^\tau$, $s_2(x) = (-v+v^2)s_2(x)^\rho + (1-v^2)s_2(x)^\tau$ and $t_2(x) = (-v+v^2)t_2(x)^\rho + (1-v^2)t_2(x)^\tau$, where $f(x)^\rho, f(x)^\tau, s_2(x)^\rho, s_2(x)^\tau, t_2(x)^\rho, t_2(x)^\tau \in F_p[x]$. Thus $(1-v^2)[(-v+v^2)f(x)^\rho + (1-v^2)f(x)^\tau] = (-v+v^2)h_1(x)[(-v+v^2)s_2(x)^\rho + (1-v^2)s_2(x)^\tau] + (1-v^2)h_2(x)[(-v+v^2)t_2(x)^\rho + (1-v^2)t_2(x)^\tau]$. Thus $(1-v^2)f(x)^\tau = 2(-v+v^2)h_1(x)s_2(x)^\rho + (1-v^2)h_2(x)t_2(x)^\tau$, which forces that $f(x)^\tau = h_2(x)t_2(x)^\tau$. This shows that $f(x)^\tau \in [h_2(x)]$. Therefore $(C : (1-v^2))^\tau \subseteq [h_2(x)]$. Conversely; if $f(x) \in [h_2(x)]$, then $f(x) = h_2(x)r_2(x)$, for some $r_2(x) \in F_p[x]$. Hence $(1-v^2)f(x) = (1-v^2)h_2(x)r_2(x) \in$

$\langle(-v+v^2)h_1(x),(1-v^2)h_2(x)\rangle = C$, which shows that $f(x) \in (C : (1-v^2))$; note that $f(x) = vf(x)+(-v+v^2)f(x)+(1-v^2)f(x)$, so $f(x) = f(x)^\tau$. Hence $f(x) \in (C : (1-v^2))^\tau$. We obtain that $[h_2(x)] \subseteq (C : (1-v^2))^\tau$. Then we have $(C : (1-v^2))^\tau = [h_2(x)]$.
By the above tow steps, we can obtain our desired results. Specially, $h_1(x)$ and $h_2(x)$ are the generator polynomials of constacyclic codes C_v and C_{-v+v^2}, respectively. □

Definition 3.1. Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R. We say that the set $S = \{(-v+v^2)g_1(x),(1-v^2)g_2(x)\}$ is generating set in standard form for the θ-constacyclic code $C = \langle S\rangle$ if both the following two conditions are satisfied:

(1) for each $i \in \{1,2\}$, $g_i(x)$ is either monic in $F_p[x]$ or equals to 0;
(2) if $g_1(x) \neq 0$, then $g_1(x)|(x^n-(\lambda-\mu+\kappa))$; if $g_2(x) \neq 0$, then $g_2(x)|(x^n-\lambda)$.

Now combining Theorem 3.3 and 3.5, the following result is obtained.

Theorem 3.6. *Any nonzero constacyclic code $C = (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ over R has a unique generating set in standard form.*

Corollary 3.7. *Let C be an ideal in R_n, then there exists a unique polynomial $g(x) = (-v+v^2)g(x)^\rho + (1-v^2)g(x)^\tau \in C$ such that $C = \langle g(x)\rangle$ with $g(x)^\rho$ and $g(x)^\tau$ being monic in $F_p[x]$. In particular, R_n is a principal ideal ring.*

Proof. According to Theorem 3.6 we have $C = \langle(-v+v^2)g_v(x),(1-v^2)g_{-v+v^2}(x)\rangle$, where $\{(-v+v^2)g_v(x),(1-v^2)g_{-v+v^2}(x)\}$ is a generating set in standard form for C. Let $g(x) = (-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)$. Note that

$$2(-v+v^2)g_v(x) = (-v+v^2)g(x) = (-v+v^2)[(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)] \in C$$

and

$$(1-v^2)g_{-v+v^2} = (1-v^2)g(x) = (1-v^2)[(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)] \in C.$$

Hence $2(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x) = (-v+v^2)g(x)+(1-v^2)g(x) \in C$, then $v^2g(x)-vg(x)+g(x)-v^2g(x) = g(x)(1-v) \in C$ and it is belong to $\langle g(x)\rangle$. Thus $C \subseteq \langle g(x)\rangle$ and since $g(x) = (-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x) \in C$. So $\langle g(x)\rangle \subseteq C$. Therefore $C = \langle g(x)\rangle$.
Finally, we prove the uniqueness of such a polynomial. Suppose that $C = \langle h(x)\rangle$. Write $h(x) = (-v+v^2)h(x)^\rho+(1-v^2)h(x)^\tau$, where $h(x)^\rho$ and $h(x)^\tau$ are monic in $F_p[x]$. In the following we shall prove that $h(x)^\rho = g_v(x)$ and $h(x)^\tau = g_{-v+v^2}(x)$. Since $C = \langle h(x)\rangle$ and $(-v+v^2)h(x) \in C$, so $h(x) \in (C : (-v+v^2))$, that is, $h(x)^\rho \in (C : (-v+v^2))^\rho = C_v$. Then $g_v(x)|h(x)^\rho$, similarly we have that $g_{-v+v^2}(x)|h(x)^\tau$. On the other hand, there exists some polynomial $s(x) \in R_n$ such that $(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x) = [(-v+v^2)s_v(x)^\rho+(1-v^2)s_{-v+v^2}(x)^\tau][(-v+v^2)h(x)^\rho+(1-v^2)h(x)^\tau] = 2(-v+v^2)s_v(x)^\rho h(x)^\rho+(1-v^2)s_{-v+v^2}(x)^\tau h(x)^\tau$, it follows that $2s_v(x)^\rho h(x)^\rho = g_v(x)$ and $s_{-v+v^2}(x)^\tau h(x)^\tau = g_{-v+v^2}(x)$. Hence $h(x)^\rho|g_v(x)$ and $h(x)^\tau|g_{-v+v^2}(x)$. Therefore we obtain that $h(x)^\rho = g_v(x)$ and $h(x)^\tau = g_{-v+v^2}(x)$, which is the required results. □

Now we give the definition of polynomial Gray map over R_n. Let $f(x) \in R_n$ with degree less than n, then $f(x)$ can be expressed as $f(x) = r(x)+vq(x)+v^2s(x)$, where $r(x),q(x),s(x) \in F_p[x]$ and their degrees are less than n. Let $\theta = \lambda+v\mu+v^2\kappa \in R^*$.
Define the polynomial Gray map as follows:

$$\Phi_\theta : R_n \to F_p[x]/(x^{2n}-1).$$

$$f(x) = r(x)+vq(x)+v^2s(x) \longmapsto \lambda(\lambda-\mu+\kappa)s(x)+x^n[\mu r(x)-\kappa r(x)-(\lambda-\mu+\kappa)s(x)].$$

Obviously the above polynomial Gray map Φ_θ is well-defined. If $\mu,\kappa \neq 0$, then the map Φ_θ is bijection.

Theorem 3.8. *Let C be a θ-constacyclic code of length n over R with a generating set in standard form $\{(-v+v^2)g_v(x),(1-v^2)g_{-v+v^2}(x)\}$. Then $\Phi_\theta(C) \subseteq \langle g_v(x)g_{-v+v^2}(x)\rangle$.*

Proof. Since $g_v(x)|(x^n-(\lambda-\mu+\kappa))$ and $g_{-v+v^2}(x)|(x^n-\lambda)$, then there exist $q_1(x), q_2(x) \in F_p[x]$ such that:
$x^n-(\lambda-\mu+\nu) = g_v(x)q_1(x)$ and $x^n-\lambda = g_{-v+v^2}(x)q_2(x)$. By the proof of Corollary 3.7, we have that $\big\langle(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)\big\rangle$. Let $f(x)$ be an element in C. Then $f(x) = [(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)]h(x)$, for some $h(x) \in R_n$. Since $h(x)$ can be written as $h(x) = vh(x)^\sigma+(-v+v^2)h(x)^\rho+(1-v^2)h(x)^\tau$, where $h(x)^\sigma$, $h(x)^\rho$ and $h(x)^\tau \in F_p[x]$, it follows that
$f(x) = [(-v+v^2)g_v(x)+(1-v^2)g_{-v+v^2}(x)][vh(x)^\sigma+(-v+v^2)h(x)^\rho+(1-v^2)h(x)^\tau] = (-v^2+v)g_v(x)h(x)^\sigma+(-2v+2v^2)g_v(x)h(x)^\rho+(1-v^2)g_{-v+v^2}(x)h(x)^\tau = g_{-v+v^2}(x)h(x)^\tau + v(g_v(x)h(x)^\sigma-2g_v(x)h(x)^\rho)+v^2(-g_v(x)h(x)^\sigma+2g_v(x)h(x)^\rho-g_{-v+v^2}(x)h(x)^\tau)$. Then we have that:
$\Phi_\theta(f(x)) = \lambda(\lambda-\mu+\kappa)[-g_v(x)h(x)^\sigma+2g_v(x)h(x)^\rho-g_{-v+v^2}(x)h(x)^\tau]+x^n[\mu g_{-v+v^2}(x)h(x)^\tau - \kappa g_{-v+v^2}(x)h(x)^\tau-(\lambda-\mu+\kappa)(-g_v(x)h(x)^\sigma+2g_v(x)h(x)^\rho-g_{-v+v^2}(x)h(x)^\tau)] =$
$\lambda g_{-v+v^2}(x)h(x)^\tau(x^n-(\lambda-\mu+\kappa))-(\lambda-\mu+\kappa)[-g_v(x)h(x)^\sigma+2g_v(x)h(x)^\rho](x^n-\lambda) =$
$\lambda g_{-v+v^2}(x)h(x)^\tau g_v(x)q_1(x)-(\lambda-\mu+\kappa)[-g_v(x)h(x)^\sigma+2g_v(x)h(x)^\rho]g_{-v+v^2}(x)q_2(x) =$
$\lambda g_{-v+v^2}(x)h(x)^\tau g_v(x)q_1(x)-(\lambda-\mu+\kappa)g_v(x)[-h(x)^\sigma+2h(x)^\rho]g_{-v+v^2}q_2(x) =$
$g_v(x)g_{-v+v^2}(x)[\lambda h(x)^\tau q_1(x)-(\lambda-\mu+\kappa)(-h(x)^\sigma+2h(x)^\rho)q_2(x)] \in \langle g_v(x)g_{-v+v^2}(x)\rangle$. Hence $\Phi_\theta(C) \subseteq \langle g_v(x)g_{-v+v^2}(x)\rangle$. □

Corollary 3.9. *Let $\theta = 1+v-v^2$ or $-1-v+v^2$ and let $C = vC_{1-v^2}\oplus(-v+v^2)C_v\oplus(1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R with generating set in standard form $\big\{(-v+v^2)g_v(x),(1-v^2)g_{-v+v^2}(x)\big\}$. Then $\Phi_\theta(C) = [g_v(x)g_{-v+v^2}(x)]$.*

Proof. Note that $g_v(x)|(x^n-(\lambda-\mu+\kappa))$ and $g_{-v+v^2}(x)|(x^n-\lambda)$, where $\lambda+v\mu+v^2\kappa = 1+v-v^2$ or $-1-v+v^2$, then $(x^n-(\lambda-\mu+\kappa))(x^n-\lambda) = (x^{2n}-1)$. Hence $g_v(x)g_{-v+v^2}(x)|(x^{2n}-1)$, which shows that $g_v(x)g_{-v+v^2}(x)$ is the generator polynomial for cyclic code $\langle g_v(x)g_{-v+v^2}(x)\rangle$, that is, $\langle g_v(x)g_{-v+v^2}(x)\rangle = [g_v(x)g_{-v+v^2}]$. By Theorem 3.8, we have that $\Phi_\theta(C) \subseteq [g_v(x)g_{-v+v^2}]$. On the other hand, $|\Phi_\theta(C)| = |C| = p^{2n-deg(g_v(x))-deg(g_{-v+v^2}(x))}$ and $|[g_v(x)g_{-v+v^2}(x)]| = p^{2n-deg(g_v(x))-deg(g_{-v+v^2}(x))}$. Hence, $\Phi_\theta(C) = [g_v(x)g_{-v+v^2}(x)]$. □

For a unit θ of R_p, the θ-constacyclic shift τ_λ on R_p is the shift

$$\tau_\lambda(x_0, x_1, ..., x_n) = (\lambda x_{n-1}, x_0, ..., x_{n-2})$$

.

Proposition 3.10. *Let C be a θ-constacyclic code of length n over R_p. Then the dual code $C^\perp$ for C is a θ-constacyclic code of length n over R_p.*

Proof. Let C be a θ-constacyclic code of length n over R_p. Consider arbitrary elements $x \in C^\perp$ and $y \in C$. Because C is θ-constacyclic, $\tau_\theta^{n-1}(y) \in C$. Thus, $0 = x.\tau_\theta^{n-1}(y) = \lambda\tau_{\lambda^{-1}}(x).y = \tau_{\lambda^{-1}}(x).y$, which means that $\tau_\theta^{-1}(x) \in C^\perp$. Therefore, $C^\perp$ is closed under the τ_θ^{-1}-shift; i.e, $C^\perp$ is a θ-constacyclic code. □

Let $g_v(x)h_v(x) = x^n-(\lambda-\mu+\kappa)$ and $g_{-v+v^2}(x)h_{-v+v^2}(x) = x^n-\lambda$. Let $\widetilde{h}_v(x) = x^{deg(h_v(x))}h_v(\frac{1}{x})$ and $\widetilde{h}_{-v+v^2}(x) = x^{deg(h_{-v+v^2}(x))}h_{-v+v^2}(x)(\frac{1}{x})$ be the reciprocal polynomials of $h_v(x)$ and $h_{-v+v^2}(x)$, respectively. We write $h_v^*(x) = \frac{1}{h_v(0)}\widetilde{h}_v(x)$ and $h^*_{-v+v^2}(x) = \frac{1}{h_{-v+v^2}(0)}\widetilde{h}_{-v+v^2}(x)$.

Theorem 3.11. *Let $C = vC_{1-v^2}\oplus(-v+v^2)C_v\oplus(1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R. Then $C^\perp = (-v+v^2)C_v^\perp\oplus(1-v^2)C^\perp_{-v+v^2}$.*

Proof. From Theorem 3.2, C_v and C_{-v+v^2} are constacyclic codes over F_p. Then $C_v^\perp$ and $C^\perp_{-v+v^2}$ are constacyclic code over F_p. Let $g_v(x)$ and $g_{-v+v^2}(x)$ are generator polynomials for C_v and C_{-v+v^2}, respectively. Then $C_v^\perp = [h_v^*(x)]$ and $C^\perp_{-v+v^2} = [h^*_{-v+v^2}(x)]$. Thus we have that $|C_v^\perp| = p^{deg(g_v(x))}$ and $|C^\perp_{-v+v^2}| = p^{deg(g_{-v+v^2}(x))}$.

For any $a \in C_v^{\perp}$, $b \in C_{-v+v^2}^{\perp}$ and $c = (-v+v^2)r + (1-v^2)q \in C$, where $r \in C_v$, $q \in C_{-v+v^2}$, we have that

$$\begin{aligned} c.((-v+v^2)a + (1-v^2)b) &= ((-v+v^2)r + (1-v^2)q)((-v+v^2)a + (1-v^2)b) \\ &= 2(-v+v^2)r.a + (1-v^2)q.b \\ &= 0, \end{aligned}$$

and hence $(-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp} \subseteq C^{\perp}$.
Furthermore, suppose that $(-v+v^2)a + (1-v^2)b = (-v+v^2)a' + (1-v^2)b'$, where $a, a' \in C_v^{\perp}$ and $b, b' \in C_{-v+v^2}^{\perp}$, then $(-v+v^2)(\ a-a'\ ) = (1-v^2)(\ b'-b\ )$, so $(-v+v^2)(\ a-a'\ ) = v^2[(-v+v^2)(\ a-a'\ )] = v^2[(1-v^2)(\ b'-b\ )] = 0$. Hence $a = a'$, which forces $b = b'$. Thus every element c of $(-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp}$ has a unique expression as $(-v+v^2)r + (1-v^2)q$, where $r \in C_v^{\perp}$, $q \in C_{-v+v^2}^{\perp}$. This shows that

$$|(-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp}| = |C_v^{\perp}||C_{-v+v^2}^{\perp}|$$

$$p^{deg(g_v(x))+deg(g_{-v+v^2}(x))}.$$

Finally, by Proposition 3.4, $|C| = p^{3n-deg(g_v(x))-deg(g_{-v+v^2}(x))}$. Since R_p is a Frobenius ring, $|C||C^{\perp}| = |R_p|^n$, so

$$\begin{aligned} |C^{\perp}| = \frac{|R_p|^n}{|C|} &= \frac{p^{3n}}{p^{3n-deg(g_v(x))-deg(g_{-v+v^2}(x))}} \\ &= p^{deg(g_v(x))+deg(g_{-v+v^2}(x))} \\ &= |(-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp}|. \end{aligned}$$

Note that $(-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp} \subseteq C^{\perp}$ as above, we have that $C^{\perp} = (-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp}$, as required. □

Theorem 3.12. *With notations as above. Let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R with generating set in standard form $\{(-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x)\}$. Then*

(1) $C^{\perp} = \left\langle (-v+v^2)h_v^*(x), (1-v^2)h_{-v+v^2}^*(x) \right\rangle$ and $|C^{\perp}| = p^{deg(g_v(x))+deg(g_{-v+v^2}(x))}$;

(2) $C^{\perp} = \left\langle (-v+v^2)h_v^*(x) \oplus (1-v^2)h_{-v+v^2}^*(x) \right\rangle$;

(3) $\Phi_\theta(C^{\perp} \subseteq \left\langle h_v^*(x)h_{-v+v^2}^*(x) \right\rangle$.

Proof. (1) By Proposition 3.10, $C^{\perp}$ is a θ-constacyclic code over R_p; by Theorem 3.11, we have that $C^{\perp} = (-v+v^2)C_v^{\perp} \oplus (1-v^2)C_{-v+v^2}^{\perp}$, where according to Theorem 3.2 $C_v^{\perp}$ and $C_{-v+v^2}^{\perp}$ are two constacyclic codes over F_p. Since $h_v^*(x)$ and $h_{-v+v^2}^*(x)$ are generator polynomials for $C_v^{\perp}$ and $C_{-v+v^2}^{\perp}$, respectively, we have that $\left\{(-v+v^2)h_v^*(x), (1-v^2)h_{-v+v^2}^*(x)\right\}$ is the generating set in standard form for $C^{\perp}$. So $C^{\perp} = \left\langle (-v+v^2)h_v^*(x), (1-v^2)h_{-v+v^2}^*(x) \right\rangle$. In addition, $|C^{\perp}| = |C_v^{\perp}||C_{-v+v^2}^{\perp}| = p^{deg(g_v(x))}.p^{deg(g_{-v+v^2}(x))} = p^{deg(g_v(x))+deg(g_{-v+v^2}(x))}$.
(2) Since $\left\{(-v+v^2)h_v^*(x), (1-v^2)h_{-v+v^2}^*(x)\right\}$ is the generating set in standard form for $C^{\perp}$, according to the proof of Corollary 3.7 we have that

$$C^{\perp} = \left\langle (-v+v^2)h_v^*(x) \oplus (1-v^2)h_{-v+v^2}^*(x) \right\rangle$$

.
(3) Similar to the proof of Theorem 3.9. □

Theorem 3.13. *Let $\theta = 1+v-v^2$ or $-1-v+v^2$ and let $C = vC_{1-v^2} \oplus (-v+v^2)C_v \oplus (1-v^2)C_{-v+v^2}$ be a θ-constacyclic code of length n over R with generating set in standard form $\{(-v+v^2)g_v(x), (1-v^2)g_{-v+v^2}(x)\}$. Then*

(1) $\Phi_\theta(C^\perp) = [h_v^*(x)h^*_{-v+v^2}(x)]$.
(2) $\Phi_\theta(C^\perp) = (\Phi_\theta(C))^\perp$.

Proof. (1) According to the proof of Corollary 3.9, we can obtain the result.
(2) Note the facts that

$$\Phi_\theta(C) = [g_v(x)g_{-v+v^2}(x)]\ ,\ \Phi_\theta(C^\perp) = [h_v^*(x)h^*_{-v+v^2}(x)],$$

we have

$$\begin{aligned}\Phi_\theta(C)^\perp &= [g_v(x)g_{-v+v^2}(x)]^\perp \\ &= [h_v^*(x)h^*_{-v+v^2}(x)] \\ &= \Phi_\theta(C^\perp),\end{aligned}$$

which is the required result. □

Example 3.1. *In* $F_3[x]$

$$x^3+1 = (x+1)^3;$$
$$x^3-1 = (x+2)^3.$$

Let C be the $(-1-v+v^2)$*-constacyclic code of length 3 over* $F_3+vF_3+v^2F_3$ *with generating polynomial:*
$g(x) = (-v+v^2)(x+1)+(1-v^2)(x+2) = v^2x - vx + v^2 - v + x - v^2x + 2 - 2v^2 = x(1-v)-(1+v+v^2)$.
The Gray image $\Phi_\theta(C)$ *is a* $[6,4,2]$ *code over* F_3 *with generator polynomial* $(x+1)(x+2)$.

References

[1] A. R. Hammons , Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole, The Z_4 linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40(2), 301-319(1994).

[2] B. Yildiz, S. Karadeniz, Linear codes over $F_2+uF_2+vF_2+uvF_2$, Des. Codes Cryptogr. 54,61-81(2010).

[3] H. Q. Dinh, Constacyclic codes of length 2^s over Galois extension rings of F_2+uF_2, IEEE Trans. Theory 55,1730-1740(2009).

[4] H. Q. Dinh, Constacyclic codes of length ps over $F_{p^m}+uF_{p^m}$, J. Algebra 324,940-950(2010).

[5] H. Q. Dinh, S. R. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50(8),1728-1744(2004).

[6] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121, 555-575(1999).

[7] K. Guenda, T. A. Gulliver, MDS and self-dual codes over rings, Finite Fields Appl. 18,1061-1075(2012).

[8] S. Zhu, L. Wang, A class of constacyclic codes over F_p+vF_p and its Gray image, Discrete Math. 311,2677-2682(2011).

[9] S, Zhu, X. Kai, Dual and self-dual negacyclic codes of even length over Z_{2^a} , Discrete Math. 309,2382-2391(2009).

[10] S. Zhu, Y. Wang, M. Shi, Some results on cyclic codes over F_2+vF_2, IEEE Trans. Inform. Theory 56(4),1680-1684(2010).

[11] T. Abualrub, I. Siap, Constacyclic codes over F_2+uF_2, J. Franklin Inst. 346,520-529(2009).

[12] T. Blackford, Negacyclic codes over Z_4 of even length, IEEE Trans. Theory, 49,1417-1424(2003).

[13] Z.Guanghui and C.Bocong, Constacyclic codes over F_p+vF_p, arxiv:1301.06669v1[csit]4 Jan. (2013).

Author information

Mohammed M. Al-Ashker and Mariam I. Satariah, Mathematics Department, Faculty of Science, Islamic University of Gaza, Gaza, P.O. Box 108, Palestine.
E-mail: `mashker@iugaza.edu.ps`

Received: May 22, 2015.

Accepted: January 21, 2016