ACTA ARITHMETICA
162.1 (2014)

A class of permutation trinomials over finite fields

by

Xiang-dong Hou (Tampa, FL)

1. Introduction. Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f \in \mathbb{F}_q[\mathtt{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. There is always great interest in permutation polynomials that appear in simple algebraic forms. In this connection, a considerable amount of research has been devoted to finding and understanding *permutation binomials*. For a few samples from a long list of publications on permutation binomials over finite fields, see [AW, C, H3, KL, MPW, MZ, T, VR, W1, W2]. As for *permutation trinomials*, there are not many theoretic results. Discoveries of infinite classes of permutation trinomials are less frequent than those of permutation binomials [BZ, B, G, LP].

The main results of the present paper are the following theorems.

Theorem 1.1. *Let q be odd and $f = -\mathtt{x} + t\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, where $t \in \mathbb{F}_q^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if $q \equiv 1 \pmod 8$ and $t^2 = -2$.*

Theorem 1.2. *Let $q > 2$ be even and $f = \mathtt{x} + t\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, where $t \in \mathbb{F}_q^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if $\mathrm{Tr}_{q/2}(1/t) = 0$.*

The polynomials in Theorems 1.1 and 1.2 arose from a recent study of certain permutation polynomials over finite fields defined by a functional equation [FHL] (we discuss this connection in Section 6). The same study also led to the discovery of a class of permutation binomials over $\mathbb{F}_{q^2}$ similar to the ones in the above theorems [H3]. However, the method of [H3] does not seem to work in the current situation, and we will discuss the reason in Section 4. The method of the present paper is different from that of [H3].

The proof of Theorem 1.2 is quite easy and will be given in Section 2. The proof of Theorem 1.1 is rather involved; here we briefly describe the strategy and method of the proof. For the sufficiency part, we try to show that for every $y \in \mathbb{F}_{q^2}$, the equation $f(x) = y$ has a solution $x \in \mathbb{F}_{q^2}$. This is quite

2010 *Mathematics Subject Classification*: Primary 11T06; Secondary 11T55.
Key words and phrases: discriminant, finite field, permutation polynomial.

DOI: 10.4064/aa162-1-3

obvious when $y \in \mathbb{F}_q$. When $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the problem is reduced to proving that a certain cubic polynomial over $\mathbb{F}_q$ is always reducible. For the necessity part, we use the criterion that $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = 0$ for $1 \le s \le q-2$. The sum $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s$ can be expressed as a double sum in terms of binomial coefficients, and can be made explicit for $s = (q-1)q$ and $1 + (q-2)q$. When $s = (q-1)q$, the equation $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = 0$ implies that $1 + 4t^{-2}$ is a square in $\mathbb{F}_q^*$; when $s = 1 + (q-2)q$, the equation implies that $t^2 = -2$.

The proof of Theorem 1.1 spans over three sections: proof of the sufficiency in Section 3, computation of $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s$ in Section 4, proof of the necessity in Section 5.

In [D2], Dobbertin developed a method to study certain types of permutation polynomials over finite fields through multivariate rational functions; see also [BZ, D1, M]. The technique used in the proof of the sufficiency part of Theorem 1.1 bears some resemblance to Dobbertin's method. However, on the whole, the two approaches are not the same.

Remark. The polynomial f in Theorems 1.1 and 1.2 can be written as $f = \mathtt{x}h(\mathtt{x}^{q-1})$, where $h(\mathtt{x}) = -1 + t\mathtt{x} + \mathtt{x}^2$. By [Z, Lemma 2.1], f is a PP of $\mathbb{F}_{q^2}$ if and only if $\mathtt{x}h(\mathtt{x})^{q-1}$ permutes the $(q-1)$th powers in $\mathbb{F}_{q^2}^*$. However, as described above, our approach does not rely on this observation.

2. Proof of Theorem 1.2. Recall that in Theorem 1.2, $q > 2$ is even and $t \in \mathbb{F}_q^*$.

Proof of Theorem 1.2. ($\Leftarrow$) Let $y \in \mathbb{F}_{q^2}$ be arbitrary. We show that the equation

$$x + tx^q + x^{2q-1} = y \tag{2.1}$$

has at most one solution $x \in \mathbb{F}_{q^2}$. Assume that $x \in \mathbb{F}_{q^2}$ is a solution of (2.1).

Case 1. Assume $y \neq 0$. Then $x \neq 0$. Put $\tau = x^{-q}y = x^{q-1} + x^{1-q} + t \in \mathbb{F}_q$. Then $x = (y/\tau)^q$ and (2.1) becomes

$$\left(\frac{y}{\tau}\right)^q + t\,\frac{y}{\tau} + \left(\frac{y}{\tau}\right)^{2-q} = y,$$

i.e.,

$$\frac{1}{\tau}(y^{q-1} + y^{1-q} + t) = 1. \tag{2.2}$$

Thus τ is unique, hence so is x.

Case 2. Assume $y = 0$. We show that (2.1) has no solution $x \in \mathbb{F}_{q^2}^*$. If, to the contrary, (2.1) has a solution $x \in \mathbb{F}_{q^2}^*$, then

$$x^{q-1} + x^{1-q} + t = 0. \tag{2.3}$$

Since $t \neq 0$, we have $x^{2(1-q)} \neq 1$, i.e., $x^{(q-1)^2} \neq 1$. Thus $x^{q-1} \notin \mathbb{F}_q$. By (2.3), x^{q-1} is a root of $\mathtt{x}^2 + t\mathtt{x} + 1 \in \mathbb{F}_q[\mathtt{x}]$. Then $\mathtt{x}^2 + t\mathtt{x} + 1$ must be irreducible over $\mathbb{F}_q$. Hence $\mathrm{Tr}_{q/2}(1/t) = 1$, which is a contradiction.

($\Rightarrow$) Assume to the contrary that $\mathrm{Tr}_{q/2}(1/t) = 1$. Then $\mathtt{x}^2 + t\mathtt{x} + 1$ is irreducible over $\mathbb{F}_q$. Let $x \in \mathbb{F}_{q^2}$ be a root of this polynomial. Then $x^{1+q} = \mathrm{N}_{q^2/q}(x) = 1$, hence $x = y^{q-1}$ for some $y \in \mathbb{F}_{q^2}$. Thus we have $y^{q-1} + y^{1-q} + t = 0$. Then (2.2) does not have any solution for τ. Following the argument in Case 1 of ($\Leftarrow$), we see that $f(x) = y$ has no solution $x \in \mathbb{F}_{q^2}$, which is a contradiction. ∎

3. Proof of Theorem 1.1, sufficiency. Recall that the discriminant of a cubic polynomial $g = \mathtt{x}^3 + b\mathtt{x}^2 + c\mathtt{x} + d$ over a field is given by

$$D(g) = -4c^3 - 27d^2 + b^2c^2 - 4b^3d + 18bcd.$$

We first prove a lemma which appeared as an exercise in [K, p. 53].

LEMMA 3.1. *If $g \in \mathbb{F}_q[\mathtt{x}]$ is an irreducible cubic polynomial, then $D(g)$ is a square in $\mathbb{F}_q^*$.*

Proof. $\mathbb{F}_{q^3}$ is the splitting field of g over $\mathbb{F}_q$. The Galois group $\mathrm{Aut}(\mathbb{F}_{q^3}/\mathbb{F}_q)$ of g over $\mathbb{F}_q$, as a permutation group of the roots of g, is $\langle (1,2,3) \rangle = A_3$. By [Hu, Chapter V, Corollary 4.7], $D(g)$ is a square of $\mathbb{F}_q^*$. ∎

Proof of Theorem 1.1. ($\Leftarrow$) Assume $q \equiv 1 \pmod 8$, $t \in \mathbb{F}_q^*$, $t^2 = -2$. For every $y \in \mathbb{F}_{q^2}$, we show that the equation

$$-x + tx^q + x^{2q-1} = y \tag{3.1}$$

has at least one solution $x \in \mathbb{F}_{q^2}$. If $y \in \mathbb{F}_q$, $x = y/t$ is a solution. So we assume $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Assume for the time being that $x \in \mathbb{F}_{q^2}$ satisfies (3.1). Put $\tau = x^{-q}y = t + x^{q-1} - x^{1-q}$. Since $(x^{q-1} - x^{1-q})^q = -(x^{q-1} - x^{1-q})$, we may write

$$\tau = t + \epsilon u, \tag{3.2}$$

where $\epsilon \in \mathbb{F}_{q^2}$, $\epsilon^{q-1} = -1$, and $u \in \mathbb{F}_q$. Making the substitution $x = (y/\tau)^q$ in (3.1), we have

$$-\left(\frac{y}{\tau}\right)^q + t\,\frac{y}{\tau} + \left(\frac{y}{\tau}\right)^{2-q} = y,$$

i.e.,

$$\frac{t-\tau}{\tau} + y^{1-q}\frac{\tau^q}{\tau^2} - y^{q-1}\frac{1}{\tau^q} = 0. \tag{3.3}$$

In the light of (3.2), we can write (3.3) as

$$\frac{-\epsilon u}{t+\epsilon u} + y^{1-q}\frac{t-\epsilon u}{(t+\epsilon u)^2} - y^{q-1}\frac{1}{t-\epsilon u} = 0. \tag{3.4}$$

A routine computation shows that (3.4) is equivalent to

$$u^3 - \frac{y^{q-1} - y^{1-q}}{\epsilon} u^2 + \frac{2 - 2t(y^{q-1} + y^{1-q})}{\epsilon^2} u + 2\,\frac{y^{q-1} - y^{1-q}}{\epsilon^3} = 0. \tag{3.5}$$

Note that the left side of (3.5) is a cubic polynomial in u with coefficients in $\mathbb{F}_q$.

At this point, it is necessary to reverse the above reasoning to ensure the correctness of the logic. If $u \in \mathbb{F}_q$ is a solution of (3.5), then $\tau = t + \epsilon u$ is a solution of (3.3), and consequently, $x = (y/\tau)^q$ is a solution of (3.1). Therefore, all we have to do is to show that

(3.6)

$$g(\mathtt{u}) := \mathtt{u}^3 - \frac{y^{q-1} - y^{1-q}}{\epsilon} \mathtt{u}^2 + \frac{2 - 2t(y^{q-1} + y^{1-q})}{\epsilon^2} \mathtt{u} + 2\,\frac{y^{q-1} - y^{1-q}}{\epsilon^3} \in \mathbb{F}_q[\mathtt{u}]$$

is reducible, where $\epsilon \in \mathbb{F}_{q^2}$, $\epsilon^{q-1} = -1$. (Note that the reducibility of g is independent of the choice of ϵ.)

If $y^{q-1} - y^{1-q} = 0$, g is clearly reducible. So we assume $y^{q-1} - y^{1-q} \neq 0$. Since $(y^{q-1} - y^{1-q})^q = -(y^{q-1} - y^{1-q})$, we may choose $\epsilon = y^{q-1} - y^{1-q}$. Let $s = y^{q-1} + y^{1-q} \in \mathbb{F}_q$. Then

$$s^2 - 4 = (y^{q-1} + y^{1-q})^2 - 4 = (y^{q-1} - y^{1-q})^2 = \epsilon^2,$$

which is a nonsquare in $\mathbb{F}_q^*$ since $\epsilon \notin \mathbb{F}_q$. We can express $g(\mathtt{u})$ in terms of t and s:

$$g(\mathtt{u}) = \mathtt{u}^3 - \mathtt{u}^2 + \frac{2 - 2ts}{s^2 - 4} \mathtt{u} + \frac{2}{s^2 - 4}.$$

We proceed to compute the discriminant of g. We have

$$\begin{aligned}
D(g) &= -4\left(\frac{2 - 2ts}{s^2 - 4}\right)^3 - 27\left(\frac{2}{s^2 - 4}\right)^2 + \left(\frac{2 - 2ts}{s^2 - 4}\right)^2 + 4\frac{2}{s^2 - 4} \\
&\qquad - 18\,\frac{2 - 2ts}{s^2 - 4}\frac{2}{s^2 - 4} \\
&= -\frac{4}{(s^2 - 4)^3}\big[-8(ts - 1)^3 + 27(s^2 - 4) - (ts - 1)^2(s^2 - 4) \\
&\qquad - 2(s^2 - 4)^2 - 18(ts - 1)(s^2 - 4)\big] \\
&= -\frac{4}{(s^2 - 4)^3}\big[-8(t^3 s^3 - 3t^2 s^2 + 3ts - 1) \\
&\qquad + (s^2 - 4)(27 - t^2 s^2 + 2ts - 1 - 18ts + 18) - 2(s^4 - 8s^2 + 16)\big] \\
&= -\frac{4}{(s^2 - 4)^3}\big[-8(-2ts^3 + 6s^2 + 3ts - 1) \\
&\qquad + (s^2 - 4)(2s^2 - 16ts + 44) - 2(s^4 - 8s^2 + 16)\big] \\
&= -\frac{16}{(s^2 - 4)^3}(s^2 + 10ts - 50) = -\frac{16(s + 5t)^2}{(s^2 - 4)^3}.
\end{aligned}$$

Since $-16(s+5t)^2$ is a square of $\mathbb{F}_q$ and since s^2-4 is a nonsquare in $\mathbb{F}_q^*$, $D(g)$ is not a square in $\mathbb{F}_q^*$. By Lemma 3.1, g is reducible in $\mathbb{F}_q[\mathtt{u}]$. ∎

4. Computation of $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s$. Let $f=-\mathtt{x}+t\mathtt{x}^q+t\mathtt{x}^{2q-1}$, where $t\in\mathbb{F}_q^*$ and $q>2$. Let $0<s<q^2-1$ and write $s=\alpha+\beta q$, where $0\le\alpha,\beta\le q-1$. We have

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^s=\sum_{x\in\mathbb{F}_{q^2}^*} f(x)^s=\sum_{x\in\mathbb{F}_{q^2}^*} x^{\alpha q+\beta}(x^{q-1}-x^{1-q}+t)^{\alpha+\beta q}.$$

This sum is clearly 0 when $\alpha+\beta q\not\equiv 0 \pmod{q-1}$.

Now assume $\alpha+\beta q\equiv 0 \pmod{q-1}$. Since $0<\alpha+\beta q<q^2-1$, we must have $\alpha+\beta=q-1$. The above computation continues as follows:

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q}=\sum_{x\in\mathbb{F}_{q^2}^*} x^{(\alpha+1)(q-1)}(x^{q-1}-x^{1-q}+t)^{\alpha}(x^{1-q}-x^{q-1}+t)^{\beta}$$

$$=\sum_{x\in\mathbb{F}_{q^2}^*} x^{(\alpha+1)(q-1)}\sum_{i,j}\binom{\alpha}{i}\binom{\beta}{j}(x^{q-1}-x^{1-q})^{i+j}(-1)^j t^{\alpha+\beta-(i+j)}$$

$$=\sum_{x\in\mathbb{F}_{q^2}^*} x^{(\alpha+1)(q-1)}\sum_{i,j}\binom{\alpha}{i}\binom{\beta}{j}x^{(i+j)(q-1)}(1-x^{2(1-q)})^{i+j}(-1)^j t^{-(i+j)}$$

$$=\sum_{x\in\mathbb{F}_{q^2}^*}\sum_{i,j}\binom{\alpha}{i}\binom{\beta}{j}x^{(q-1)(\alpha+1+i+j)}(-1)^j t^{-(i+j)}\sum_{k}\binom{i+j}{k}(-1)^k x^{-2k(q-1)}$$

$$=\sum_{x\in\mathbb{F}_{q^2}^*}\sum_{i,j,k}\binom{\alpha}{i}\binom{\beta}{j}\binom{i+j}{k}(-1)^{k+j}t^{-(i+j)}x^{(q-1)(\alpha+1+i+j-2k)}$$

$$=-\sum_{\substack{i,j,k\ge 0\\ \alpha+1+i+j-2k\equiv 0\,(\mathrm{mod}\,q+1)}}\binom{\alpha}{i}\binom{\beta}{j}\binom{i+j}{k}(-1)^{k+j}t^{-(i+j)}.$$

It is easy to see that when $0\le i\le\alpha$, $0\le j\le\beta$, and $0\le k\le i+j$, we have

$$-(q+1)<\alpha+1+i+j-2k<2(q+1).$$

Therefore,

(4.1)

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q}=-\sum_{\substack{i,j,k\ge 0\\ \alpha+1+i+j-2k=0,\,q+1}}\binom{\alpha}{i}\binom{\beta}{j}\binom{i+j}{k}(-1)^{k+j}t^{-(i+j)}.$$

REMARK. In [H3], binomials of the form $h=t\mathtt{x}+\mathtt{x}^{2q-1}$, where $t\in\mathbb{F}_q^*$, were considered. The power sum $\sum_{x\in\mathbb{F}_{q^2}} h(x)^{\alpha+\beta q}$, where $\alpha,\beta\ge 0$ and $\alpha+\beta$

$= q-1$, was expressed in terms of two sums involving binomial coefficients; see [H3, Lemma 3.2]. Those two sums in [H3] are over one variable and essentially depend only on α but not on q (hence not on β). However, the sum in (4.1) is over two variables and depends on both α and q. These differences are the reason that the characteristic-free approach in [H3] has not worked in the current situation.

5. Proof of Theorem 1.1, necessity. Let $p = \operatorname{char} \mathbb{F}_q$ and let $\mathbb{Z}_p$ be the ring of p-adic integers. For $z \in \mathbb{Z}_p$ and $a \in \mathbb{Z}$ with $a \ge 0$, written in the form $z = \sum_{n\ge 0} z_n p^n$, $a = \sum_{n\ge 0} a_n p^n$, $0 \le z_n, a_n \le p-1$, we have

$$\binom{z}{a} \equiv \prod_{n\ge 0} \binom{z_n}{a_n} \pmod p.$$

Therefore, if $z, z' \in \mathbb{Z}_p$ are such that $\nu_p(z-z') > \log_p a$, where ν_p is the p-adic order, then $\binom{z}{a} \equiv \binom{z'}{a} \pmod p$.

LEMMA 5.1. *Let $z \in \mathbb{F}_q^*$ and write $\mathtt{x}^2+\mathtt{x}-z = (\mathtt{x}-r_1)(\mathtt{x}-r_2)$, $r_1, r_2 \in \mathbb{F}_{q^2}$. Then*

$$\sum_{0\le k\le q/2} \binom{-k}{k} z^k = \begin{cases} 1/2 & \text{if } r_1 = r_2 \in \mathbb{F}_q, \\ 1 & \text{if } r_1, r_2 \in \mathbb{F}_q,\ r_1 \ne r_2, \\ 0 & \text{if } r_1, r_2 \notin \mathbb{F}_q. \end{cases}$$

Proof. We denote the constant term of a Laurent series in $\mathtt{x}$ by ct( ). We have

$$\begin{aligned} \sum_{0\le k\le q/2} \binom{-k}{k} z^k &= \sum_{0\le k\le q-1} \binom{-k}{k} z^k \\ &\qquad (\text{when } q/2 < k \le q-1,\ \tbinom{-k}{k} \equiv \tbinom{q-k}{k} = 0 \pmod p) \\ &= \sum_{0\le k\le q-1} \operatorname{ct}\left(\frac{1}{\mathtt{x}^k(1+\mathtt{x})^k}\right) z^k \\ &= \operatorname{ct}\left[\sum_{0\le k\le q-1} \left(\frac{z}{\mathtt{x}(1+\mathtt{x})}\right)^k\right] = \operatorname{ct}\left(\frac{1-(z/(\mathtt{x}(1+\mathtt{x})))^q}{1-z/(\mathtt{x}(1+\mathtt{x}))}\right) \\ &= \operatorname{ct}\left[\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\left(1-z\left(\frac{1}{\mathtt{x}}-\frac{1}{1+\mathtt{x}}\right)^q\right)\right] \\ &= \operatorname{ct}\left(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\,\frac{-z}{\mathtt{x}^q}\right) = \operatorname{ct}\left[\left(1+\frac{z}{\mathtt{x}(1+\mathtt{x})-z}\right)\frac{-z}{\mathtt{x}^q}\right] \\ &= \operatorname{ct}\left(\frac{-z^2}{\mathtt{x}^q}\,\frac{1}{\mathtt{x}^2+\mathtt{x}-z}\right) = \operatorname{ct}\left(\frac{-z^2}{\mathtt{x}^q}\,\frac{1}{(\mathtt{x}-r_1)(\mathtt{x}-r_2)}\right). \end{aligned} \tag{5.1}$$

First assume $r_1 = r_2$. We must have $r_1 = -1/2$. By (5.1), we see that

$$\begin{aligned}\sum_{0\le k\le q/2}\binom{-k}{k}z^k &= \mathrm{ct}\left(\frac{-z^2}{\mathtt{x}^q}(\mathtt{x}-r_1)^{-2}\right)\\ &= \mathrm{ct}\left(\frac{-z^2}{\mathtt{x}^q}\,r_1^{-2}\left(1-\frac{\mathtt{x}}{r_1}\right)^{-2}\right)\\ &= -\frac{z^2}{r_1^2}\binom{-2}{q}\left(-\frac{1}{r_1}\right)^q\\ &= -\frac{z^2}{r_1^{q+2}} \qquad \left(\tbinom{-2}{q}\equiv -1 \pmod p\right)\\ &= -\frac{z^2}{r_1^3}\\ &= -r_1 \qquad (-z = r_1^2)\\ &= \frac{1}{2}.\end{aligned}$$

Now assume $r_1 \neq r_2$. By (5.1), we have

$$\begin{aligned}&\sum_{0\le k\le q/2}\binom{-k}{k}z^k\\ &\quad= \mathrm{ct}\left[\frac{-z^2}{\mathtt{x}^q}\left(\frac{1}{\mathtt{x}-r_1}-\frac{1}{\mathtt{x}-r_2}\right)\frac{1}{r_1-r_2}\right]\\ &\quad= \mathrm{ct}\left[\frac{z^2}{r_1-r_2}\,\frac{1}{\mathtt{x}^q}\left(\frac{1}{r_1}\,\frac{1}{1-\frac{\mathtt{x}}{r_1}}-\frac{1}{r_2}\,\frac{1}{1-\frac{\mathtt{x}}{r_2}}\right)\right]\\ &\quad= \frac{z^2}{r_1-r_2}\left(\frac{1}{{r_1}^{q+1}}-\frac{1}{{r_2}^{q+1}}\right)\\ &\quad= \frac{-z^2}{(r_1r_2)^{q+1}}\,\frac{r_1^{q+1}-r_2^{q+1}}{r_1-r_2} = -\frac{r_1^{q+1}-r_2^{q+1}}{r_1-r_2}\\ &\quad= \begin{cases}-\dfrac{r_1^2-r_2^2}{r_1-r_2} = -(r_1+r_2) = 1 & \text{if } r_1, r_2 \in \mathbb{F}_q,\\ 0 & \text{if } r_1, r_2 \text{ are conjugates over } \mathbb{F}_q.\end{cases}\end{aligned}$$

∎

LEMMA 5.2. *Let $z \in \mathbb{F}_q^*$ and assume that $\mathtt{x}^2+\mathtt{x}-z$ has two distinct roots in $\mathbb{F}_q$. Then*

$$\sum_{0\le k\le (q-1)/2}\binom{-k}{k+1}z^k = 1.$$

Proof. The computation is similar to that for Lemma 5.1. Write $\mathtt{x}^2+\mathtt{x}-z = (\mathtt{x}-r_1)(\mathtt{x}-r_2)$, where $r_1, r_2 \in \mathbb{F}_q$, $r_1 \neq r_2$. We have

$$\begin{aligned}
&\sum_{0\le k\le (q-1)/2} \binom{-k}{k+1} z^k \\
&= \sum_{0\le k\le q-1} \binom{-k}{k+1} z^k - \binom{-(q-1)}{q} z^{q-1} \\
&\qquad\qquad \text{(when } (q-1)/2 < k < q-1,\ \tbinom{-k}{k+1} \equiv 0 \pmod p\text{)} \\
&= \sum_{0\le k\le q-1} \mathrm{ct}\left(\frac{1}{\mathtt{x}^{k+1}(1+\mathtt{x})^k}\right) z^k + 1 \\
&\qquad\qquad \text{(since } \tbinom{-(q-1)}{q} \equiv \tbinom{q^2-(q-1)}{q} = \tbinom{1+(q-1)q}{q} \equiv \tbinom{q-1}{1} \equiv -1 \pmod p\text{)} \\
&= \mathrm{ct}\left[\frac{1}{\mathtt{x}} \sum_{0\le k\le q-1} \left(\frac{z}{\mathtt{x}(1+\mathtt{x})}\right)^k\right] + 1 \\
&= \mathrm{ct}\left[\frac{1}{\mathtt{x}} \frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\left(1 - \frac{z}{\mathtt{x}^q} + \frac{z}{(1+\mathtt{x})^q}\right)\right] + 1 \\
&= \mathrm{ct}\left[\frac{1+\mathtt{x}}{\mathtt{x}(1+\mathtt{x})-z}\left(1 + \frac{z}{(1+\mathtt{x})^q}\right) - \frac{z}{\mathtt{x}^{q+1}} \frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\right] + 1 \\
&= -\frac{1}{z}(1+z) + \mathrm{ct}\left[\frac{-z}{\mathtt{x}^{q+1}}\left(1 + \frac{z}{\mathtt{x}(1+\mathtt{x})-z}\right)\right] + 1 \\
&= -\frac{1}{z} + \mathrm{ct}\left(\frac{-z^2}{\mathtt{x}^{q+1}} \frac{1}{(\mathtt{x}-r_1)(\mathtt{x}-r_2)}\right) \\
&= -\frac{1}{z} + \frac{z^2}{r_1-r_2}\left(\frac{1}{r_1^{q+2}} - \frac{1}{r_2^{q+2}}\right) \\
&\qquad\qquad \text{(see the computation in the proof of Lemma 5.1)} \\
&= -\frac{1}{z} + \frac{z^2}{r_1-r_2}\left(\frac{1}{r_1^3} - \frac{1}{r_2^3}\right) = -\frac{1}{z} - \frac{z^2}{(r_1r_2)^3} \frac{r_1^3-r_2^3}{r_1-r_2} \\
&= -\frac{1}{z} + \frac{1}{z}(r_1^2 + r_1r_2 + r_2^2) \quad (r_1r_2 = -z) \\
&= -\frac{1}{z} + \frac{1}{z}\left[(r_1+r_2)^2 - r_1r_2\right] = -\frac{1}{z} + \frac{1}{z}(1+z) = 1. \ \blacksquare
\end{aligned}$$

LEMMA 5.3. *Let $z \in \mathbb{F}_q^*$ and assume that $\mathtt{x}^2+\mathtt{x}-z$ has two distinct roots in $\mathbb{F}_q$. Then*

$$\sum_{0\le k\le (q-1)/2} (k+1)\binom{-k}{k+1} z^k = \frac{2z}{1+4z}.$$

Proof. We have

$$\begin{aligned}(5.2)\quad \sum_{0\le k\le (q-1)/2}(k+1)\binom{-k}{k+1}z^k &= \sum_{0\le k\le q-2}(k+1)\binom{-k}{k+1}z^k\\ &= \sum_{0\le k\le q-2}(k+1)\,\mathrm{ct}\left(\frac{1}{\mathtt{x}^{k+1}(1+\mathtt{x})^k}\right)z^k\\ &= \mathrm{ct}\left[\frac{1}{\mathtt{x}}\sum_{0\le k\le q-2}(k+1)\left(\frac{z}{\mathtt{x}(1+\mathtt{x})}\right)^k\right].\end{aligned}$$

Since

$$\sum_{1\le k\le q-1}k\mathtt{y}^{k-1}=\frac{d}{d\mathtt{y}}\sum_{0\le k\le q-1}\mathtt{y}^k=\frac{d}{d\mathtt{y}}\left(\frac{1-\mathtt{y}^q}{1-\mathtt{y}}\right)=\frac{1-\mathtt{y}^q}{(1-\mathtt{y})^2},$$

it follows that

$$\begin{aligned}(5.3)\quad \sum_{0\le k\le q-2}(k+1)\left(\frac{z}{\mathtt{x}(1+\mathtt{x})}\right)^k &= \frac{1-(z/(\mathtt{x}(1+\mathtt{x})))^q}{(1-z/(\mathtt{x}(1+\mathtt{x})))^2}\\ &= \left(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\right)^2\left(1-\frac{z}{\mathtt{x}^q}+\frac{z}{(1+\mathtt{x})^q}\right).\end{aligned}$$

Therefore, by (5.2) and (5.3),

$$\begin{aligned}&\sum_{0\le k\le (q-1)/2}(k+1)\binom{-k}{k+1}z^k = \mathrm{ct}\left[\frac{1}{\mathtt{x}}\left(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\right)^2\left(1-\frac{z}{\mathtt{x}^q}+\frac{z}{(1+\mathtt{x})^q}\right)\right]\\
&= \mathrm{ct}\left[-\frac{z}{\mathtt{x}^{q+1}}\left(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x})-z}\right)^2\right] = \mathrm{ct}\left[-\frac{z}{\mathtt{x}^{q+1}}\left(1+\frac{z}{\mathtt{x}(1+\mathtt{x})-z}\right)^2\right]\\
&= \mathrm{ct}\left[-\frac{z}{\mathtt{x}^{q+1}}\left(1+\frac{z}{r_1-r_2}\left(\frac{1}{\mathtt{x}-r_1}-\frac{1}{\mathtt{x}-r_2}\right)\right)^2\right]\\
&\qquad\qquad (\text{as } \mathtt{x}^2+\mathtt{x}-z=(\mathtt{x}-r_1)(\mathtt{x}-r_2),\ r_1,r_2\in\mathbb{F}_q,\ r_1\ne r_2)\\
&= \mathrm{ct}\left[-\frac{z}{\mathtt{x}^{q+1}}\left(\frac{2z}{r_1-r_2}\left(\frac{1}{\mathtt{x}-r_1}-\frac{1}{\mathtt{x}-r_2}\right)\right.\right.\\
&\qquad\qquad \left.\left.+\frac{z^2}{(r_1-r_2)^2}\left(\frac{1}{(\mathtt{x}-r_1)^2}+\frac{1}{(\mathtt{x}-r_2)^2}-\frac{2}{(\mathtt{x}-r_1)(\mathtt{x}-r_2)}\right)\right)\right]\\
&= \mathrm{ct}\left[-\frac{z^2}{\mathtt{x}^{q+1}}\left(\frac{2}{r_1-r_2}\left(\frac{1}{\mathtt{x}-r_1}-\frac{1}{\mathtt{x}-r_2}\right)+\frac{z}{(r_1-r_2)^2}\left(\frac{1}{(\mathtt{x}-r_1)^2}-\frac{1}{(\mathtt{x}-r_2)^2}\right)\right.\right.\\
&\qquad\qquad \left.\left.-\frac{2z}{(r_1-r_2)^2}\,\frac{1}{r_1-r_2}\left(\frac{1}{\mathtt{x}-r_1}-\frac{1}{\mathtt{x}-r_2}\right)\right)\right]\\
&= \mathrm{ct}\left[-\frac{z^2}{\mathtt{x}^{q+1}}\left(\left(\frac{2}{r_1-r_2}-\frac{2z}{(r_1-r_2)^3}\right)\left(-\frac{1}{r_1}\,\frac{1}{1-\mathtt{x}/r_1}+\frac{1}{r_2}\,\frac{1}{1-\mathtt{x}/r_2}\right)\right.\right.\\
&\qquad\qquad \left.\left.+\frac{z}{(r_1-r_2)^2}\left(\frac{1}{r_1^2}\,\frac{1}{(1-\mathtt{x}/r_1)^2}+\frac{1}{r_2^2}\,\frac{1}{(1-\mathtt{x}/r_2)^2}\right)\right)\right]\end{aligned}$$

$$= -z^2\bigg[\bigg(\frac{2}{r_1-r_2}-\frac{2z}{(r_1-r_2)^3}\bigg)\bigg(-\frac{1}{r_1}\Big(\frac{1}{r_1}\Big)^{q+1}+\frac{1}{r_2}\Big(\frac{1}{r_2}\Big)^{q+1}\bigg)$$
$$+\frac{z}{(r_1-r_2)^2}\bigg(\frac{1}{r_1^2}\binom{-2}{q+1}\Big(-\frac{1}{r_1}\Big)^{q+1}+\frac{1}{r_2^2}\binom{-2}{q+1}\Big(-\frac{1}{r_2}\Big)^{q+1}\bigg)\bigg]$$
$$= -z^2\bigg[\bigg(\frac{2}{r_1-r_2}-\frac{2z}{(r_1-r_2)^3}\bigg)\Big(-\frac{1}{r_1^3}+\frac{1}{r_2^3}\Big)+\frac{z}{(r_1-r_2)^2}\Big(\frac{2}{r_1^4}+\frac{2}{r_2^4}\Big)\bigg]$$
$$\text{(since } \tbinom{-2}{q+1}\equiv 2 \pmod p\text{)}$$
$$= -2z^2\bigg[\bigg(\frac{1}{r_1-r_2}-\frac{z}{(r_1-r_2)^3}\bigg)\frac{r_1^3-r_2^3}{(r_1r_2)^3}+\frac{z}{(r_1-r_2)^2}\,\frac{r_1^4+r_2^4}{(r_1r_2)^4}\bigg]$$
$$= -2z^2\bigg[\bigg(1-\frac{z}{(r_1-r_2)^2}\bigg)\frac{r_1^2+r_1r_2+r_2^2}{-z^3}+\frac{1}{z^3}\,\frac{r_1^4+r_2^4}{(r_1-r_2)^2}\bigg]$$
$$= -\frac{2}{z}\bigg[\bigg(\frac{z}{(r_1-r_2)^2}-1\bigg)(1+z)+\frac{(r_1^2-r_2^2)^2+2r_1^2r_2^2}{(r_1-r_2)^2}\bigg]$$
$$= -\frac{2}{z}\bigg[\bigg(\frac{z}{(r_1-r_2)^2}-1\bigg)(1+z)+(r_1+r_2)^2+\frac{2z^2}{(r_1-r_2)^2}\bigg]$$
$$= -\frac{2}{z}\bigg[\bigg(\frac{z}{1+4z}-1\bigg)(1+z)+1+\frac{2z^2}{1+4z}\bigg]=\frac{2z}{1+4z}.\ \blacksquare$$

Proof of Theorem 1.1. Recall that in Theorem 1.1 we assume that q is odd and $t\in\mathbb{F}_q^*$.

($\Rightarrow$) 1° Let $\alpha=0$ and $\beta=q-1$ in (4.1). We have

$$0=\sum_{x\in\mathbb{F}_{q^2}} f(x)^{(q-1)q} = -\sum_{\substack{j,k\ge 0\\ 1+j-2k=0,\,q+1}}\binom{q-1}{j}\binom{j}{k}(-1)^{k+j}t^{-j}$$
$$= -\sum_{\substack{j,k\ge 0\\ 0\le j\le q-1\\ 1+j-2k=0}}\binom{j}{k}(-1)^k t^{-j}\qquad (\tbinom{q-1}{j}\equiv(-1)^j \pmod p)$$
$$= -\sum_{1\le k\le q/2}\binom{2k-1}{k}(-1)^k t^{1-2k} = -\sum_{1\le k\le q/2}\binom{-k}{k}t^{1-2k}$$
$$= -t\bigg(\sum_{0\le k\le q/2}\binom{-k}{k}t^{-2k}-1\bigg).$$

Thus

$$\sum_{0\le k\le q/2}\binom{-k}{k}t^{-2k}=1. \tag{5.4}$$

Put $z=t^{-2}$. Then by (5.4) and Lemma 5.1, $\mathtt{x}^2-\mathtt{x}-z$ has two distinct roots in $\mathbb{F}_q$, i.e., $1+4z$ is a square in $\mathbb{F}_q^*$.

2° Let $\alpha=1$ and $\beta=q-2$ in (4.1). We have

$$\begin{aligned}
0 &= \sum_{x\in\mathbb{F}_{q^2}} f(x)^{1+(q-2)q}\\
&= -\sum_{\substack{j,k\ge 0\\ 2+j-2k=0,\,q+1}}\binom{q-2}{j}\binom{j}{k}(-1)^{k+j}t^{-j}\\
&\quad -\sum_{\substack{j,k\ge 0\\ 3+j-2k=0,\,q+1}}\binom{q-2}{j}\binom{1+j}{k}(-1)^{k+j}t^{-1-j}\\
&= -\sum_{1\le k\le q/2}\binom{q-2}{2k-2}\binom{2k-2}{k}(-1)^k t^{2-2k}\\
&\quad +\sum_{2\le k\le (q+1)/2}\binom{q-2}{2k-3}\binom{2k-2}{k}(-1)^k t^{2-2k}+1\\
&= -\sum_{1\le k\le \frac{q}{2}}(2k-1)\binom{-k+1}{k}t^{2-2k}-\sum_{2\le k\le \frac{q+1}{2}}(2k-2)\binom{-k+1}{k}t^{2-2k}+1\\
&\qquad \big(\text{since } \tbinom{q-2}{2k-2}\equiv 2k-1,\ \tbinom{q-2}{2k-3}\equiv -(2k-2)\ (\mathrm{mod}\ p)\big)\\
&= -\sum_{1\le k\le (q+1)/2}(4k-3)\binom{-k+1}{k}t^{2-2k}+1\\
&= -\sum_{0\le k\le (q-1)/2}(4k+1)\binom{-k}{k+1}t^{-2k}+1\\
&= -4\sum_{0\le k\le (q-1)/2}(k+1)\binom{-k}{k+1}z^k+3\sum_{0\le k\le (q-1)/2}(k+1)\binom{-k}{k+1}z^k+1\\
&\qquad (\text{as } z=t^{-2})\\
&= -4\,\frac{2z}{1+4z}+3\cdot 1+1 \quad (\text{by Lemmas 5.2, 5.3})\\
&= 4\,\frac{1+2z}{1+4z}.
\end{aligned}$$

So we have $z=-1/2$, i.e., $t^2=-2$. By 1°, $1+4z=-1$ is a square in $\mathbb{F}_q^*$. Since both -1 and -2 are squares in $\mathbb{F}_q^*$, we have $q\equiv 1\ (\mathrm{mod}\ 8)$. ∎

6. The polynomial $g_{n,q}$. The polynomial $f = -\mathtt{x} + t\mathtt{x}^q + \mathtt{x}^{2q-1}$ considered in the present paper is closely related to another class of polynomials which we will discuss briefly in this section.

For each prime power q and integer $n \geq 0$, the functional equation

$$\sum_{a \in \mathbb{F}_q} (\mathtt{x} + a)^n = g_{n,q}(\mathtt{x}^q - \mathtt{x})$$

defines a polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$, where $p = \operatorname{char} \mathbb{F}_q$. The polynomial $g_{n,q}$ was introduced in [H1] as the q-ary version of the *reversed Dickson polynomial*. ($g_{n,2}$ is the reversed Dickson polynomial in characteristic 2.) The rationale and incentive for studying the class $g_{n,q}$ are the fact that the class contains many interesting new PPs; see [FHL, H2]. We are interested in triples of integers $(n, e; q)$ for which $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, and we call such triples *desirable*. Among the known desirable triples $(n, e; q)$, n frequently appears in the form $n = q^a - q^b - 1$, $0 < b < a < pe$.

Let us consider triples of the form

$$(q^a - q^b - 1, e; q), \quad e \geq 2,\ 0 < b < a < pe. \tag{6.1}$$

(We assume $e \geq 2$ since all desirable triples with $e = 1$ have been determined [FHL, Corollary 2.2].) It is known that if $(a, b) = (2, 1)$ and $\gcd(q - 2, q^e - 1) = 1$, or if $a \equiv b \equiv 0 \pmod e$, then the triple (6.1) is desirable. It is also conjectured that the converse of the above statement is true for $e \geq 3$. When $e = 2$, the situation becomes very interesting and complicated [FHL, Section 5 and Table 1]. It is known that for $q > 2$ and $i > 0$,

$$g_{q^{2i}-q-1,q}(\mathtt{x}) \equiv (i-1)\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}.$$

Note that $g_{q^{2i}-q-1,q}(\mathtt{x}^{q^2-q-1}) \equiv (i-1)\mathtt{x} - i\mathtt{x}^{2q-1} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}$, where $\mathtt{x}^{q^2-q-1}$ is a PP of $\mathbb{F}_{q^2}$. So $g_{q^{2i}-q-1,q}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(i-1)\mathtt{x} - i\mathtt{x}^{2q-1}$ is. The attempt to determine the desirable triples of the form $(q^{2i} - q - 1, 2; q)$ has led to a more general result: In [H3], all PPs of $\mathbb{F}_{q^2}$ of the form $t\mathtt{x} + \mathtt{x}^{2q-1}$, $t \in \mathbb{F}_q^*$, have been determined. For $q > 2$ and $i > 0$, we also have

$$g_{q^{2i+1}-q-1,q}(\mathtt{x}) \equiv -\mathtt{x}^{q^2-2} + i\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}.$$

Note that $g_{q^{2i+1}-q-1,q}(\mathtt{x}^{q^2-q-1}) \equiv i\mathtt{x} - \mathtt{x}^q - i\mathtt{x}^{2q-1} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}$, which is of course the prototype of the polynomial f considered in the present paper. The following corollary immediately follows from Theorem 1.1. (Note that $i^2 = -1/2$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv 1$ or $3 \pmod 8$.)

Corollary 6.1. *Suppose that q is odd, $i > 0$, and $i \not\equiv 0 \pmod p$. Then $(q^{2i+1} - q - 1, 2; q)$ is desirable if and only if $p \equiv 1$ or $3 \pmod 8$, $q \equiv 1 \pmod 8$, and $i^2 = -1/2$.*

The corresponding corollary of Theorem 1.2 is already known [FHL, Theorem 5.9(ii)].

7. Hindsight of Theorem 1.1. Assume $q \equiv 1 \pmod 8$ and $t \in \mathbb{F}_q^*$, $t^2 = -2$. Then by Theorem 1.1 and (4.1), we have

$$\sum_{\substack{i,j,k\geq 0\\ \alpha+1+i+j-2k=0,\, q+1}} \binom{\alpha}{i}\binom{\beta}{j}\binom{i+j}{k}(-1)^{k+j}t^{-(i+j)} = 0 \tag{7.1}$$

for all integers $\alpha, \beta \geq 0$ with $\alpha+\beta = q-1$. We have not found any direct proof of (7.1). We refer the interested readers to [H4, §7] for a further discussion of (7.1).

Acknowledgements. This research was partly supported by NSA (grant no. H98230-12-1-0245).

References

[AW] A. Akbary and Q. Wang, *A generalized Lucas sequence and permutation binomials*, Proc. Amer. Math. Soc. 134 (2006), 15–22.

[BZ] S. Ball and M. Zieve, *Symplectic spreads and permutation polynomials*, in: Finite Fields and Applications, Lecture Notes in Comput. Sci. 2948, Springer, Berlin, 2004, 79–88.

[B] F. Brioschi, *Un teorema sulla teoria delle sostituzioni*, Rend. Reale Ist. Lombardo Sci. Lett. (2) 12 (1879), 483–485.

[C] L. Carlitz, *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc. 68 (1962), 120–122.

[D1] H. Dobbertin, *Almost perfect nonlinear power functions on* GF(2^n)*: the Niho case*, Inform. and Comput. 151 (1999), 57–72.

[D2] H. Dobbertin, *Uniformly representable permutation polynomials*, in: Sequences and Their Applications (Bergen, 2001), Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002, 1–22.

[FHL] N. Fernando, X. Hou and S. D. Lappano, *A new approach to permutation polynomials over finite fields, II*, Finite Fields Appl. 22 (2013), 122–158.

[G] A. Grandi, *Un teorema sulla rappresentazione analitica delle sostituzioni sopra un numero primo di elementi*, Giorn. Mat. Battaglini 19 (1881), 238–245.

[H1] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A 118 (2011), 448–454.

[H2] X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. 18 (2012), 492–521.

[H3] X. Hou, *A class of permutation binomials over finite fields*, J. Number Theory 133 (2013), 3549–3558.

[H4] X. Hou, *A class of permutation trinomials over finite fields*, arXiv:1303.0568 (2013).

[HMSY] X. Hou, G. L. Mullen, J. A. Sellers and J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. 15 (2009), 748–773.

[Hu] T. W. Hungerford, *Algebra*, Springer, New York, 1980.

[K] I. Kaplansky, *Fields and Rings*, Chicago Lectures in Math., Univ. of Chicago Press, Chicago, IL, 1995.

[KL] S. Y. Kim and J. B. Lee, *Permutation polynomials of the type* $x^{1+((q-1)/m)}+ax$, Commun. Korean Math. Soc. 10 (1995), 823–829.

[LP] J. B. Lee and Y. H. Park, *Some permutation trinomials over finite fields*, Acta Math. Sci. 17 (1997), 250–254.

[MPW] A. Masuda, D. Panario and Q. Wang, *The number of permutation binomials over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes*, Electron. J. Combin. 13 (2006), res. paper 65.

[MZ] A. M. Masuda and M. E. Zieve, *Permutation binomials over finite fields*, Trans. Amer. Math. Soc. 361 (2009), 4169–4180.

[M] W. More, *Permutation polynomials based on multivariate rational functions*, in: Contributions to General Algebra 17, Heyn, Klagenfurt, 2006, 149–160.

[T] G. Turnwald, *Permutation polynomials of binomial type*, in: Contributions to General Algebra 6, Hölder–Pichler–Tempsky, Vienna, 1988, 281–286.

[VR] N. N. Vasilyev and M. A. Rybalkin, *Permutation binomials and their groups*, J. Math. Sci. 179 (2011), 679–689.

[W1] D. Wan, *Permutation polynomials over finite fields*, Acta Math. Sinica (N.S.) 3 (1987), 1–5.

[W2] D. Wan, *Permutation binomials over finite fields*, Acta Math. Sinica (N.S.) 10 (1994), Special Issue, 30–35.

[Z] M. E. Zieve, *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.

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida
Tampa, FL 33620, U.S.A.
E-mail: xhou@usf.edu

Received on 28.5.2013
and in revised form on 17.10.2013 (7462)