ACTA ARITHMETICA
VIII (1963)

Pseudo-ordered polynomials over a finite field *

by

R. McConnel (Durham, N.C.)

1. Introduction. In 1902 F. R. Moulton [9] gave a construction of a non-Desarguesian plane. The construction essentially consists of using the real plane and the lines of the real plane, except that those lines with negative slope are "bent" on the x-axis. The question of generalizing Moulton's construction of a non-Desarguesian plane is discussed in a recent article by W. A. Pierce [10]. Pierce's generalized construction, which he calls a "Moulton construction", is valid for any field and a "pseudo-order" defined over the field. This generalized construction is basically determined by certain one-to-one functions of the field onto itself; these functions correspond to the "bending" of lines on the x-axis in Moulton's original paper.

One of Pierce's results gives necessary and sufficient conditions that his "Moulton construction" is an affine plane, and further, necessary and sufficient conditions that the resulting affine plane is non-Desarguesian. For a finite field these conditions reduce to an order-preserving property for the functions defining the "Moulton construction". In papers by L. Carlitz ([1], [2]) the one-to-one functions possessing the order-preserving property necessary to define affine planes and non-Desarguesian planes are explicitly determined for the case of a finite field.

In this paper generalizations of Carlitz's results mentioned above will be proved. It is anticipated that these generalizations will have geometrical applications, possibly related to the work of Järnefelt [5] and P. Kustaanheimo ([6], [7]).

This paper is part of a doctoral thesis written at Duke University under the direction of Professor Leonard Carlitz. The author wishes to express his graditude for the assistance rendered by Professor Carlitz during the preparation of this paper.

2. Notation and statement of main results. Let F be a finite field of order $q = p^n$, p a prime number. It is a known fact that any function

* Research supported in part by National Science Foundation grant G16485.

of F into itself can be represented by a polynomial with coefficients in F. A polynomial $f(x)$ over F is called a permutation polynomial if the values, $f(x)$ for $x \in F$, are distinct. For references see [3], chapter V; [4], chapter XVIII. Throughout the remainder of the paper, a function will mean any function of F into F.

Let d be an arbitrary divisor of $q-1$. Set $md = q-1$. Define the function

$$\Psi_d(x) = x^m \tag{2.1}$$

for any $x \in F$. Suppose the function $f(x)$ is normalized, that is,

$$f(0) = 0\,, \quad f(1) = 1 \tag{2.2}$$

and satisfies

$$\Psi_d\big(f(x)-f(y)\big) = \Psi_d(x-y) \tag{2.3}$$

for all $x, y \in F$. It is proved in sections 3 and 4 that such a function must be an automorphism of F, that is,

$$f(x) = x^{p^j}\,, \tag{2.4}$$

where $0 \leqslant j < n$ and $d \mid p^j-1$. It should be noted that any function satisfying (2.3) is obviously a permutation polynomial and any function given by (2.4) satisfies (2.2) and (2.3). This result reduces to Carlitz's Theorem [1] when $d = 2$ and p is an odd prime. In section 5 this result is generalized slightly by removing the restriction that $f(x)$ be normalized.

Now suppose d_1 and d_2 are any divisors of $q-1$ and set

$$q-1 = d_1 m_1 = d_2 m_2\,.$$

Put

$$\Psi_1(x) = x^{m_1}\,, \quad \Psi_2(x) = x^{m_2} \tag{2.5}$$

for any $x \in F$. Let λ and μ be any two fixed elements of F such that

$$\lambda^{d_1} = 1\,, \quad \mu^{d_2} = 1\,. \tag{2.6}$$

In section 5 it is proved that any function $f(x, y)$ of two variables which satisfies

$$\Psi_1\big(f(x, y)-f(z, y)\big) = \lambda\Psi_1(x-z)\,, \tag{2.7}$$

$$\Psi_2\big(f(x, y)-f(x, z)\big) = \mu\Psi_2(y-z) \tag{2.8}$$

for all $x, y, z \in F$ must be of the form

$$f(x, y) = ax^{p^i} + by^{p^j} + c \tag{2.9}$$

where $0 \leqslant i < n$, $0 \leqslant j < n$, $d_1 \mid p^i-1$, and $d_2 \mid p^j-1$. Moreover

$$\Psi_1(a) = \lambda \quad \text{and} \quad \Psi_2(b) = \mu\,.$$

Again it is to be noted that any function given by (2.9) satisfies (2.7) and (2.8).

In section 6 the result of the preceding paragraph is generalized to functions of m variables. The hypothesis for this generalization is that the function of m variables satisfies relationships of the same type as (2.7) or (2.8) for each coordinate and the conclusion is

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i x_i^{p^{r_i}} + b \qquad (0 \leqslant r_i < n)\,. \tag{2.10}$$

For a complete statement of this Theorem, see section 6. Carlitz's result [2] is obtained from this generalization when $d = 2$ and p is an odd prime.

3. Case I of Theorem 1. In this section we shall prove some preliminary results about any function satisfying (2.2) and (2.3). These results lead to a simple proof of our first Theorem for the case that the arbitrary divisor d of $q-1$ also divides $p-1$. We denote this condition by case I. In the next section we consider the case $d \nmid p-1$ and denote it by case II.

Recall that F is a finite field of order $q = p^n$ and, for an arbitrary divisor d of $q-1$, set $md = q-1$. Also

$$\Psi_d(x) = x^m \tag{3.1}$$

for all $x \in F$. We now formally state

THEOREM 1. *Suppose $f(x)$ is a function such that*

$$f(0) = 0\,, \quad f(1) = 1\,. \tag{3.2}$$

Then

$$\Psi_d\big(f(x)-f(y)\big) = \Psi_d(x-y) \tag{3.3}$$

for any $x, y \in F$ if and only if

$$f(x) = x^{p^j}\,, \tag{3.4}$$

where $0 \leqslant j < n$ and $d \mid p^j-1$.

Proof. We first note that

$$\Psi_d(x^{p^j}-y^{p^j}) = \Psi_d(x-y)$$

for all $x, y \in F$ if and only if

$$x^m(x^{m(p^j-1)}-1) = 0$$

for all $x \in F$. But this is true if and only if $d \mid p^j-1$. Hence the necessity of Theorem 1 is obvious and we need only show that any function satisfying (3.2) and (3.3) is an automorphism of F. In the paper of L. Carlitz [1],

the Theorem has been proved when $d = 2$. Thus we may assume $2 < d < q-1$.

For any fixed $c \in F$, let

$$y = f(x+c)-f(c)\,. \tag{3.5}$$

It follows that

$$\Psi_d(y) = \Psi_d\big(f(x+c)-f(c)\big) = \Psi_d(x)$$

from (3.3). Thus, as x runs through the elements of F such that $\Psi_d(x) = a$ for some $a \in F$, y also runs through the same elements. If u is an indeterminate, then

$$\prod_{\Psi_d(x)=a} [u-f(x+c)] = \prod_{\Psi_d(x)=a} [u-f(c)-x]\,. \tag{3.6}$$

By definition (3.1),

$$[\Psi_d(x)]^d = 1$$

for any $x \in F$. The equation $u^d-1 = 0$ has exactly d solutions, say $x_1, x_2, \ldots, x_d$. Hence

$$u^d-1 = (u-x_1)(u-x_2)\ldots(u-x_d)\,.$$

Replacing u by u^m, we obtain

$$u^{md}-1 = \prod_{i=1}^{d}(u^m-x_i)\,.$$

As $u^{md}-1 = u^{q-1}-1 = 0$ is satisfied by every non-zero element of F, each u^m-x_i has exactly m solutions. Whence

$$\prod_{\Psi_d(x)=x_i} (u-x) = u^m-x_i \quad (1 \leqslant i \leqslant d)\,.$$

Also

$$\prod_{\Psi_d(x)=x_i} [u-f(c)-x] = \big(u-f(c)\big)^m-x_i \quad (1 \leqslant i \leqslant d)\,. \tag{3.7}$$

Combining (3.6) and (3.7) we have

$$\prod_{\Psi_d(x)=x_i} [u-f(x+c)] = \big(u-f(c)\big)^m-x_i \quad (1 \leqslant i \leqslant d)\,.$$

Applying logarithmic differentiation we get

$$\sum_{\Psi_d(x)=x_i} \frac{1}{u-f(x+c)} = \frac{m\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^m-x_i} \quad (1 \leqslant i \leqslant d)\,. \tag{3.8}$$

Consequently

$$\begin{aligned}\sum_{x\in F} \frac{\Psi_d(x)}{u-f(x+c)} &= \sum_{i=1}^{d} \sum_{\Psi_d(x)=x_i} \frac{x_i}{u-f(x+c)} \\ &= \sum_{i=1}^{d} \frac{x_i m\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^m-x_i} \\ &= \frac{m\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^{md}-1} \sum_{i=1}^{d} x_i \frac{\big(u-f(c)\big)^{md}-1}{\big(u-f(c)\big)^m-x_i} \\ &= \frac{md\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^{md}-1}\,.\end{aligned} \tag{3.9}$$

Continuing, we have

$$\begin{aligned}\sum_{x\in F} \frac{\Psi_d(x)}{u-f(x+c)} &= \frac{md\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^{md}-1} = -\frac{\big(u-f(c)\big)^{m-1}}{\big(u-f(c)\big)^{md}-1} \\ &= -\frac{\big(u-f(c)\big)^m}{\big(u-f(c)\big)^q-\big(u-f(c)\big)} = -\frac{\big(u-f(c)\big)^m}{u^q-u}\,.\end{aligned}$$

Therefore

$$\sum_{x\in F} \frac{\Psi_d(x)}{u-f(x+c)} = -\frac{\big(u-f(c)\big)^m}{u^q-u}\,. \tag{3.10}$$

Using

$$u^q-u = [u-f(x+c)]^q-[u-f(x+c)]\,,$$

we have

$$\sum_{x\in F} \Psi_d(x)\,\big[\big(u-f(x+c)\big)^{md}-1\big] = -\big(u-f(c)\big)^m\,.$$

As

$$\sum_{x\in F} \Psi_d(x) = 0\,,$$

then

$$\sum_{x\in F} \Psi_d(x)[u-f(x+c)]^{md} = -\big(u-f(c)\big)^m\,. \tag{3.11}$$

Since the sum on the left remains the same when a linear transformation is applied,

$$\sum_{x\in F} \Psi_d(x-c)\,[u-f(x)]^{md} = -\big(u-f(c)\big)^m\,. \tag{3.12}$$

Expanding equation (3.12) and then equating coefficients of the u's, we obtain

$$\sum_{x\in F}(x-c)^m\binom{md}{r}f^r(x)=0 \qquad (0\leqslant r<m(d-1)) \tag{3.13}$$

and

$$\sum_{x\in F}(x-c)^m\binom{md}{m-r}x^{m(d-1)}f^r(x)=(-1)^{m+1}\binom{m}{r}f^r(c) \qquad (0\leqslant r\leqslant m)\,. \tag{3.14}$$

As $f(x)$ is a permutation polynomial and $f(0)=0$, the residue modulo x^q-x of $f^r(x)$ is a polynomial of degree $<q-1$ with constant term zero. Thus let

$$f^r(x)=\sum_{j=1}^{md-1}b_j^{(r)}x^j \qquad (1\leqslant r<md)\,.$$

By substituting this in equations (3.13) and (3.14) and equating coefficients of the c's, we obtain

$$\binom{md}{r}\binom{m}{s}\sum_{j=1}^{md-1}b_j^{(r)}\sum_{x\in F}x^{m+j-s}=0 \qquad (0\leqslant r<m(d-1);\ 0\leqslant s\leqslant m)\,, \tag{3.15}$$

$$(-1)^s\binom{md}{m-r}\binom{m}{s}\sum_{j=1}^{md-1}b_j^{(r)}\sum_{x\in F}x^{md+j-s}=(-1)^{m+1}\binom{m}{r}b_s^{(r)} \tag{3.16}$$

$$(0\leqslant r\leqslant m;\ 0\leqslant s\leqslant md)\,.$$

In order to simplify equations (3.15) and (3.16), we use the known formulas

$$\binom{md}{r}\equiv(-1)^r\ (\mathrm{mod}\,p) \qquad (0\leqslant r\leqslant md)$$

and

$$\sum_{x\in F}x^s=\begin{cases}-1 & (md\,|\,s)\,,\\ 0 & (md\nmid s)\,.\end{cases}$$

Thus equations (3.15) and (3.16) reduce to

$$\binom{m}{s}b^{(r)}_{m(d-1)+s}=0 \qquad (0\leqslant r<m(d-1)\,,\ 0\leqslant s\leqslant m)\,, \tag{3.17}$$

$$(-1)^s\binom{m}{s}b_s^{(r)}=(-1)^r\binom{m}{r}b_s^{(r)} \qquad (0\leqslant r\leqslant m\,,\ 0\leqslant s\leqslant md)\,. \tag{3.18}$$

If $n=1$, that is, $md=p-1$, then, by equation (3.18), $r\leqslant m$ implies $\deg f^r(x)\leqslant m$. If $\deg f(x)=k>1$, choose the least positive r such that $kr>m$. Then $r\leqslant m$; for otherwise,

$$kr>k+m\,,$$

as $k,\ m\geqslant 2$. Also

$$kr<md=p-1\,.$$

For, if not, then

$$kr\geqslant md>2m\geqslant m+k\,,$$

as $k\leqslant m$ and $d>2$. Thus $r\leqslant m$ and $\deg f^r(x)=kr>m$. This contradiction completes the proof for the case $n=1$.

Let $n\geqslant 2$. Put

$$m=a_0+a_1p+\ldots+a_{n-1}p^{n-1}\,, \quad \text{where} \quad 0\leqslant a_i\leqslant p-1 \tag{3.19}$$

for all i. Let M denote the set of integers

$$\beta_0+\beta_1p+\ldots+\beta_{n-1}p^{n-1}\,, \tag{3.20}$$

where $0\leqslant\beta_i\leqslant a_i$. It is a known result [8] that $\binom{m}{r}$ is prime to p if and only if $r\in M$. By equation (3.18), if $r\in M$, then $b_s^{(r)}=0$ for $s>m$. Thus $\deg f^r(x)\leqslant m$. If also $s\in M$, then by (3.18), $b_s^{(r)}=0$. Thus when $r\in M$, the only nonzero coefficients $b_s^{(r)}$ of $f^r(x)$ are those for which $s\in M$.

We now show that $f(x)$ is a monomial in x. Since $p\nmid q-1$, then $a_0\geqslant 1$. Thus 1 and $m-1$ are in M. Hence $\deg f^{m-1}(x)\leqslant m$ and $\deg f(x)\leqslant m$. As

$$f^{m-1}(x)f(x)=f^m(x)=x^m$$

by hypothesis (3.3),

$$f(x)=x^k$$

for some $k\in M$. Let

$$k=\gamma_0+\gamma_1p+\ldots+\gamma_{n-1}p^{n-1}\,, \tag{3.21}$$

where $0\leqslant\gamma_i\leqslant a_i$. Since the only nonzero coefficients $b_s^{(r)}$ of $f^r(x)$ for any $r\in M$ are those for which $s\in M$, then the residue modulo $q-1$ of rk is in M for any $r\in M$.

To facilitate the remaining discussion, we make the following definition. The set of integers A is said to be closed with respect to $a\in A$, or briefly, closed, if for any $b\in A$, $ba\in A$. Thus we have that the set M is closed with respect to k. Note that equality for the set M is congruence modulo $q-1$.

We now restrict ourselves to case I, that is, we assume $d\,|\,p-1$. The notation and general results in the preceding paragraphs will be used again in section 4.

To prove case I, we note that

$$m=\frac{q-1}{d}=\frac{p-1}{d}(1+p+\ldots+p^{n-1})\,.$$

The set M consists of the integers

$$\beta_0+\beta_1 p+\ldots+\beta_{n-1}p^{n-1} \quad (0\leqslant\beta_i\leqslant(p-1)/d)$$

and

$$k=\gamma_0+\gamma_1 p+\ldots+\gamma_{n-1}p^{n-1} \quad (0\leqslant\gamma_i\leqslant(p-1)/d)\,.$$

If the largest $\gamma_i\geqslant 2$, choose the least positive integer r such that $\gamma_i r>(p-1)/d$. Then $r\leqslant m$ and hence $r\in M$. We now show that $kr<q-1$. It will suffice to show that $\gamma_i r<p-1$ for all i. Suppose

$$\gamma_i r\geqslant p-1=\frac{p-1}{2}+\frac{p-1}{2}>\frac{p-1}{d}+\frac{p-1}{d}\geqslant\frac{p-1}{d}+\gamma_i\,,$$

as $d\geqslant 3$. Then $\gamma_i(r-1)>(p-1)/d$. Thus for the largest γ_i, $\gamma_i(r-1)>(p-1)/d$. This contradicts our choice of r. Thus $rk<q-1$. Hence $f^r(x)=x^{rk}$ and $r\in M$, but $rk\notin M$. This contradicts the fact that M is closed with respect to k. Therefore $\gamma_i\leqslant 1$ for any i.

If $k\neq p^j$, then

$$k=p^s+\ldots+p^t\,,$$

where $0\leqslant s<t\leqslant n-1$. We now show that there is an $r\in M$ such that $rk\notin M$, which is a contradiction. To prove this, it will suffice to show that there is an $r\in M$ such that

$$r(1+\ldots+p^u)\notin M\,,$$

where $0<u\leqslant n-1$. For, if this is true, choose an $r\in M$ such that

$$r(1+\ldots+p^{t-s})\notin M\,.$$

Then, as M is closed with respect to p^s and with respect to p^{n-s},

$$rp^s(1+\ldots+p^{t-s})\notin M\,,$$

that is, $rk\notin M$.

In order to show there is an $r\in M$ such that

$$r(1+\ldots+p^u)\notin M\,,$$

let

$$h=1+\ldots+p^u\,,$$

where $0<u\leqslant n-1$. Then

$$\left(1+\left(\frac{p-1}{d}\right)p^{n-u}\right)h=1+\ldots+p^u+\left(\frac{p-1}{d}\right)p^{n-u}+\ldots+\left(\frac{p-1}{d}\right)p^n$$
$$\equiv\left[\left(\frac{p-1}{d}\right)+1\right]+\ldots+p^u+\left(\frac{p-1}{d}\right)p^{n-u}+\ldots \pmod{q-1}\,.$$

Hence

$$\left(1+\left(\frac{p-1}{d}\right)p^{n-u}\right)h\notin M\,,\quad\left(1+\frac{p-1}{d}p^{n-u}\right)\in M\,.$$

This completes the proof for the case $d|p-1$.

4. Case II of Theorem 1. To complete the proof of Theorem 1, we need only investigate the case $d\nmid p-1$. In order to do this, we need to determine an explicit formula for m, which was defined by (3.19). But first we must determine the subscripts of the nonzero coefficients in the p-adic representation of m. Let

$$M^*=\{i\colon a_i\neq 0\}\,, \tag{4.1}$$

the set of subscripts of nonzero coefficients in the p-adic representation of m. Let

$$K^*=\{j\colon \gamma_j\neq 0\}\,, \tag{4.2}$$

the set of subscripts of nonzero coefficients in the p-adic representation of k. Let

$$\delta=(K^*\cup\{n\})\,, \tag{4.3}$$

the greatest common divisor of the integers in $K^*\cup\{n\}$. Set $n=g\delta$. In order that the definitions of the sets K^* and M^* be consistent with the definition of the set M, equality for the sets K^* and M^* must be congruence modulo n. We also note here that $K^*\subseteq M^*$.

In order to simplify the notation in the following discussion, we set

$$\varrho(i,j)=ip^j\,.$$

The function ϱ has the following properties:

PROPERTY 1. *If $i\in M^*$ and $j\in K^*$, then $\varrho(\gamma_j,i+j)\in M$ and $i+j\in M^*$.*

PROPERTY 2. *If $i\in M^*$ and $0\leqslant\beta\leqslant a_i$, then $\varrho(\beta,i)k\in M$. In particular, $\varrho(a_i,i)k\in M$ for any $i\in M^*$.*

To see that Property 1 is true we need only note that, for any $i\in M^*$, the fact that M is closed with respect to k means $\varrho(1,i)k\in M$. Hence $\varrho(1,i)\varrho(\gamma_j,j)=\varrho(\gamma_j,i+j)\in M$ and also $i+j\in M^*$. Property 2 is proved by noting that $0\leqslant\beta\leqslant a_i$ and $i\in M^*$ implies $\varrho(\beta,i)\in M$. Hence, by the closure property of M, $\varrho(\beta,i)k\in M$. In the remaining portion of this section we will use these properties repeatedly to determine a representation of m.

LEMMA 1. *Let the set M be closed with respect to k. Then there exist integers $0=j_1<j_2<\ldots<j_e$ in M^* such that*

$$M^*=\bigcup_{z=1}^{e}M_z^*\,,\quad \text{where}\quad M_z^*=\{c\delta+j_z\colon 0\leqslant c<g\}\,.$$

Moreover the sets M_z^* are disjoint.

As $\delta=(K^*\cup\{n\})$, then there exist integers a_i and an integer a such that

$$\sum_{i\in K^*}a_i i+an=\delta\,.$$

For any $a_i \leqslant 0$, let $a_i' > 0$ be such that $a_i'n + a_i > 0$. Then

$$\delta = \sum_{i \in K^*} a_i i + an \equiv \sum_{i \in K^*} b_i i \pmod{n},$$

where

$$b_i = \begin{cases} a_i & \text{if} \quad a_i > 0, \\ a_i'n + a_i & \text{if} \quad a_i \leqslant 0. \end{cases}$$

Hence $b_i > 0$ for all $i \in K^*$. For any $i_1 \in K^*$, $2i_1 \in M^*$ by Property 1. As $2i_1 \in M^*$ and $i_1 \in K^*$, then $3i_1 \in M^*$, again by Property 1. Thus, by repeated applications of Property 1, any multiple of i_1 is in M^*. In particular, $b_{i_1} i_1 \in M^*$. Suppose $i_2 \in K^*$, $i_2 \neq i_1$. By Property 1, for any $ci_1 \in M^*$, we have $ci_1 + i_2 \in M^*$. Now applying Property 1 to $ci_1 + i_2 \in M^*$ and $i_2 \in K^*$, we have $ci_1 + 2i_2 \in M^*$. Hence by repeated applications of Property 1, we have $ci_1 + fi_2 \in M^*$ for any $c \geqslant 0$, $f \geqslant 0$. In particular, $b_{i_1} i_1 + b_{i_2} i_2 \in M^*$. Thus by repeatedly applying Property 1, it is obvious that

$$\sum_{i \in K^*} b_i i \in M^*,$$

that is, $\delta \in M^*$. It is also clear that any multiple of δ is in M^*.

Put

$$M_1^* = \{c\delta : 0 \leqslant c < g\}.$$

Thus $M_1^* \subseteq M^*$. Suppose $M^* - M_1^* \neq \varphi$. Let j_2 be the smallest integer in $M^* - M_1^*$. Then $j_2 \neq 0$ as $0 \in M_1^*$. Suppose $i_1 \in K^*$. As $j_2 \in M^*$, then by Property 1, $i_1 + j_2 \in M^*$. Applying Property 1 to $i_1 + j_2 \in M^*$ and $i_1 \in K^*$, we have $2i_1 + j_2 \in M^*$. Hence, by repeated applications of Property 1, we have $ci_1 + j_2 \in M^*$ for any $c \geqslant 0$. Suppose $i_2 \in K^*$, $i_2 \neq i_1$. Then, as $ci_1 + j_2 \in M^*$, we have $ci_1 + i_2 + j_2 \in M^*$. Applying Property 1 again, we have $ci_1 + 2i_2 + j_2 \in M^*$. Repeated applications of Property 1 leads to $ci_1 + fi_2 + j_2 \in M^*$ for any $c \geqslant 0$, $f \geqslant 0$. It is now obvious that

$$\sum_{i \in K^*} b_i i + j_2 \equiv \delta + j_2 \pmod{n}$$

is in M^*. Also any integer of the form $c\delta + j_2$ for $c \geqslant 0$ is in M^*.

Let

$$M_2^* = \{c\delta + j_2 : 0 \leqslant c < g\}.$$

Then $M_1^* \cup M_2^* \subseteq M^*$. If $M^* - (M_1^* \cup M_2^*) \neq \varphi$, we use the same method as above to obtain a third set

$$M_3^* = \{c\delta + j_3 : 0 \leqslant c < g\},$$

where j_3 is the least integer in $M^* - (M_1^* \cup M_2^*)$. Thus we have $M_1^* \cup M_2^* \cup M_3^* \subseteq M^*$. We continue until

$$M^* - \bigcup_{z=1}^{e} M_z^* = \varphi.$$

Thus

$$M^* = \bigcup_{z=1}^{e} M_z^*.$$

Moreover, $0 < j_2 < j_3 < \ldots < j_e$. Let

$$L = \{0, j_2, j_3, \ldots, j_e\}. \tag{4.4}$$

We next note that the sets M_z^* each contain g distinct integers $(\mathrm{mod}\, n)$ and are disjoint. For $c\delta + j_v \equiv f\delta + j_v \pmod{n}$ implies $c\delta \equiv f\delta \pmod{n}$ and hence $c \equiv f \pmod{g}$, a contradiction. Thus the elements of M_z^* are distinct $(\mathrm{mod}\, n)$. Also $c\delta + j_v \equiv f\delta + j_u \pmod{n}$ implies $j_v \equiv j_u + (f-c)\delta \pmod{n}$. But, by our choice of j_v, this is impossible unless $v = u$ and $f = c$. Thus the sets M_z^* are disjoint and the Lemma is proved.

Now put

$$N = \{0, 1, 2, \ldots, n-1\}. \tag{4.5}$$

If $M^* \neq N$, let w be the least integer not in M^*. Then the set of integers

$$w, w+\delta, \ldots, w+(n-\delta) \tag{4.6}$$

are incongruent $(\mathrm{mod}\, n)$ and are not in M^*. For $w + c\delta \equiv w + f\delta \pmod{n}$ implies $c\delta \equiv f\delta \pmod{n}$, or $c \equiv f \pmod{g}$, a contradiction. If $w + c\delta \equiv j + f\delta \pmod{n}$ for some $j \in L$, then $w \equiv j + (f-c)\delta \pmod{n}$, a contradiction as $w \notin M^*$. Moreover, for any distinct $j + u\delta$ and $j + (u+1)\delta$ in M^*, there exist an integer of the form $w + c\delta$ not in M^* such that

$$j + u\delta < w + c\delta < j + (u+1)\delta.$$

We now see that

$$m = \sum_{j \in L} \sum_{z=0}^{g-1} a_{z\delta + j} p^{z\delta + j}, \tag{4.7}$$

where $a_{z\delta+j} \neq 0$ for all z and j.

If Theorem 1 is false, then

$$k = \gamma_{s\delta} p^{s\delta} + \ldots + \gamma_{t\delta} p^{t\delta} \qquad (0 \leqslant s < t < g), \tag{4.8}$$

where $\gamma_{s\delta} \geqslant 1$ and $\gamma_{t\delta} \geqslant 1$.

Let

$$\gamma' = \max_{i \in K^*} \gamma_i, \tag{4.9}$$

$$a' = \min_{i \in M^*} a_i. \tag{4.10}$$

We note here that $\gamma' \leqslant \alpha'$. For, if $\gamma' = \gamma_{u\delta}$ and $\alpha' = a_{v\delta+j}$ for some $j \in L$, then $[(n-u+v)\delta+j] \in M^*$. Thus, by Property 1, $\varrho(\gamma_{u\delta}, (n-u+v)\delta+j+u\delta) \in M$; that is,

$$\gamma_{u\delta} p^{(n-u+v)\delta+j+u\delta} \equiv \gamma_{u\delta} p^{v\delta+j} \pmod{q-1}$$

is in M. Thus $\gamma_{u\delta} \leqslant a_{v\delta+j}$, that is, $\gamma' \leqslant \alpha'$.

We now show that $\gamma' = 1$. To do this we consider two cases, namely

(i) $M^* = N$,

(ii) $M^* \neq N$.

We note that $\gamma' = 1$ is obvious for the case $p = 2$, which is excluded from the proofs of the following two Lemmas.

LEMMA 2. *Let the set M be closed with respect to k. Suppose $M^* = N$. Then*

$$\gamma' = \max_{i \in K^*} \gamma_i = 1$$

and

$$m = \sum_{j \in L} a_j \sum_{z=0}^{g-1} p^{z\delta+j} .$$

We first show that $\alpha' < p/2$. For $\alpha' > p/2$ implies that

$$m > \frac{p}{2}(1+\ldots+p^{n-1}) = \frac{p}{p-1}\cdot\frac{q-1}{2} > \frac{q-1}{2} .$$

But $m = (q-1)/d < (q-1)/2$. Thus $\alpha' < p/2$. As $\gamma' \leqslant \alpha'$, then $1 \leqslant \gamma' < p/2$. Suppose $2 \leqslant \gamma' < p/2$. Let r be the least positive integer such that $r\gamma' > \alpha'$. Then $r \leqslant \alpha'$ and $r\gamma' < p$. For

$$r\gamma' \geqslant p = \frac{p}{2}+\frac{p}{2} > \gamma'+\alpha'$$

implies $(r-1)\gamma' > \alpha'$, contradicting our choice of r. Let $\alpha' = a_u$ and $\gamma' = \gamma_v$ for $u \in M^*$ and $v \in K^*$. As $r \leqslant \alpha'$ and $u+(n-v) \in M^*$, then $\varrho(r, u+(n-v))k \in M$ by Property 2. As $r\gamma' < p$, then

$$r\gamma_v p^{u+(n-v)+v} \equiv r\gamma_v p^u \equiv r\gamma' p^u \pmod{q-1}$$

is in M. But as $r\gamma' > \alpha' = a_u$, this is a contradiction. Thus $\gamma' = 1$.

We now show that $a_{u\delta+j} = a_{v\delta+j}$, where $j \in L$. Suppose $v < u$. As $v\delta+j \in M^*$, then Property 2 implies $\varrho(a_{v\delta+j}, v\delta+j)k \in M$. Since $\gamma' = 1$, then $\varrho(a_{v\delta+j}, v\delta+j+i_1) \in M$ for any $i_1 \in K^*$. Thus, for $i_1 \in K^*$, $a_{v\delta+j} \leqslant a_{v\delta+j+i_1}$ and $v\delta+j+i_1 \in M^*$. Hence by Property 2, $\varrho(a_{v\delta+j}, v\delta+j+i_1)k \in M$. As $\gamma' = 1$, we have $\varrho(a_{v\delta+j}, v\delta+j+i_1+i_2) \in M$ for any $i_1, i_2 \in K^*$. It is now obvious that we can raise the exponent of p by Property 2 until we obtain

$$v\delta+j+\sum_{i \in K^*} b_i(u-v)i \equiv u\delta+j \pmod{n} .$$

Thus we have $\varrho(a_{v\delta+j}, u\delta+j) \in M$. Hence $a_{v\delta+j} \leqslant a_{u\delta+j}$. Also by Property 2, $\varrho(a_{u\delta+j}, u\delta+j)k \in M$ because $u\delta+j \in M^*$. Since $\gamma' = 1$, then $\varrho(a_{u\delta+j}, u\delta+j+i_1) \in M$ for any $i_1 \in K^*$. Thus $a_{u\delta+j} \leqslant a_{u\delta+j+i_1}$ for any $i_1 \in K^*$. By applying Property 2 again, we have $\varrho(a_{u\delta+j}, u\delta+j+i_1)k \in M$. As $\gamma' = 1$, then $\varrho(a_{u\delta+j}, u\delta+j+i_1+i_2) \in M$. It is now obvious that by repeatedly applying Property 2, we can raise the exponent of p until we obtain

$$u\delta+j+\sum_{i \in K^*} b_i(n-(u-v))i \equiv v\delta+j \pmod{n} .$$

Thus $\varrho(a_{u\delta+j}, v\delta+j) \in M$. Hence $a_{u\delta+j} \leqslant a_{v\delta+j}$. Therefore $a_{u\delta+j} = a_{v\delta+j}$.

Lemma 2 gives us an explicit formula for m and the value of γ' when $M^* = N$. The following Lemma disposes of the remaining case.

LEMMA 3. *Let the set M be closed with respect to k. Suppose $M^* \neq N$. Then*

$$\gamma' = \max_{i \in K^*} \gamma_i = 1$$

and

$$m = \sum_{j \in L} a_j \sum_{z=0}^{g-1} p^{z\delta+j} .$$

To prove $\gamma' = 1$ when $M^* \neq N$, we first show that, for any $j \in L$, $a_{u\delta+j} = a_{v\delta+j}$. We note that in this case there is a w such that $0 < w < n$ and $w \notin M^*$. Moreover, if w is selected as the least such integer, then $w+c\delta \notin M^*$ for $0 \leqslant c < g$. Let $j \in L$ and suppose $a_{u\delta+j} < a_{v\delta+j}$. Let $r = \varrho(a_{v\delta+j}, v\delta+j) \in M$. Hence $rk \in M$, that is,

$$a_{v\delta+j}\gamma_{s\delta} p^{(s+v)\delta+j} + \ldots + a_{v\delta+j}\gamma_{t\delta} p^{(v+t)\delta+j} \tag{4.11}$$

is in M. Between the residue (mod n) of $(s+v)\delta+j$ and the residue (mod n) of the subscript of the next nonzero coefficient in rk there is at least one number of the form $w+c\delta \notin M^*$. This is true for any two successive subscripts of nonzero coefficients in rk. Also there is a number of the form $w+c\delta$ which is greater than the largest subscript of the nonzero coefficients in rk or is less than the smallest subscript of the nonzero coefficients in rk. Thus there can be no addition of terms appearing in (4.11) when rk is reduced (mod $q-1$). Hence we have $\varrho(\gamma_{i_1}a_{v\delta+j}, v\delta+j+i_1) \in M$ for any $i_1 \in K^*$. Therefore $\varrho(a_{v\delta+j}, v\delta+j+i_1) \in M$ for any $i_1 \in K^*$. Thus $a_{v\delta+j} \leqslant a_{v\delta+j+i_1}$ for any $i_1 \in K^*$. Hence by Property 2, $\varrho(a_{v\delta+j}, v\delta+j+i_1)k \in M$. Again we note that there can be no addition of terms when $\varrho(a_{v\delta+j}, v\delta+j+i_1)k$ is reduced (mod $q-1$). Therefore $\varrho(\gamma_{i_2}a_{v\delta+j}, v\delta+j+i_1+i_2) \in M$ for any $i_1, i_2 \in K^*$. Thus $\varrho(a_{v\delta+j}, v\delta+j+i_1+i_2) \in M$ for any $i_1, i_2 \in K^*$. We can continue to use Property 2 until the exponent of p is

$$v\delta+j+\sum_{i \in K^*} b_i(n-(v-u))i \equiv u\delta+j \pmod{n} . \tag{4.12}$$

Thus we have $\varrho(\gamma_i a_{v\delta+j}, u\delta+j) \in M$ for some $i \in K^*$. If $a_{v\delta+j}\gamma_i < p$, then $a_{v\delta+j}\gamma_i \leqslant a_{u\delta+j}$. But then $a_{v\delta+j} \leqslant a_{u\delta+j}$, a contradiction. If $a_{v\delta+j}\gamma_i > p$ then $a_{u\delta+j} = p-1 \geqslant a_{v\delta+j} > a_{u\delta+j}$. Hence $a_{u\delta+j} = a_{v\delta+j}$ for any $j \in L$.

We now show that $\gamma' = 1$ when $M^* \neq N$. Suppose $\gamma' \geqslant 2$ and $\gamma' > p/2$. Let w be the least integer such that $w \notin M^*$. Then $w \neq 0$, $w-1 \geqslant 0$, and $w-1 \in M^*$. Let $\gamma' = \gamma_{u\delta}$ and $w-1 = v\delta+j$ for some $j \in L$. As $a' \geqslant \gamma' \geqslant 2$ and $[(n+v-u)\delta+j] \in M^*$, we have by Property 2

$$2p^{(n+v-u)\delta+j}k \in M\,. \tag{4.13}$$

Following the same method of reasoning as used above, we see that there is no addition of terms in (4.13) when reduced $(\mathrm{mod}\, q-1)$. Thus we have

$$2\gamma' p^{(n+v-u)\delta+u\delta+j} \in M\,.$$

But

$$2\gamma' p^{(n+v-u)\delta+u\delta+j} \equiv 2\gamma' p^{v\delta+j}\ (\mathrm{mod}\, q-1)$$

and $p < 2\gamma' \leqslant 2(p-1)$. Hence

$$\begin{aligned} 2\gamma' p^{v\delta+j} &\equiv (2\gamma'-p)p^{v\delta+j} + p^{v\delta+j+1} \\ &\equiv (2\gamma'-p)p^{w-1} + p^w\ (\mathrm{mod}\, q-1)\,. \end{aligned} \tag{4.14}$$

Thus $a_w \neq 0$, which contradicts the hypothesis that $w \notin M^*$.

Suppose $2 \leqslant \gamma' < p/2$. Let w be the least integer such that $w \notin M^*$. Then $w \neq 0$, $w-1 \geqslant 0$, and $w-1 \in M^*$. Let $\gamma' = \gamma_{u\delta}$ and $w-1 = v\delta+j$ for some $j \in L$. Select the least β such that $\beta\gamma' > a_{w-1}$. Then $\beta \leqslant a_{w-1} = a_{v\delta+j}$. Thus $\beta \leqslant a_{x\delta+j}$ for any x such that $0 \leqslant x < g$ as these coefficients are all equal. As $[(n+v-u)\delta+j] \in M^*$, then, by Property 2,

$$\beta p^{(n+v-u)\delta+j}k \in M\,. \tag{4.15}$$

By the same reasoning as used previously, we see there is no addition of terms in (4.15) when reduced $(\mathrm{mod}\, q-1)$. Hence

$$\beta\gamma_{u\delta} p^{(n+v-u)\delta+j+u\delta} \in M\,.$$

But

$$\beta\gamma_{u\delta} p^{(n+v-u)\delta+j+u\delta} \equiv \beta\gamma' p^{v\delta+j}\ (\mathrm{mod}\, q-1)\,. \tag{4.16}$$

If $\beta\gamma' < p$, we have a contradiction because $\beta\gamma' > a_{v\delta+j}$. If $p < \beta\gamma' < p^2/2$, then

$$\beta\gamma' p^{v\delta+j} \equiv (\lambda p+\varepsilon)p^{v\delta+j} \equiv \varepsilon p^{v\delta+j} + \lambda p^w\ (\mathrm{mod}\, q-1)\,, \tag{4.17}$$

where $\beta\gamma' = \lambda p+\varepsilon$, $1 \leqslant \lambda < p/2$, and $1 \leqslant \varepsilon < p$. Hence $a_w \neq 0$, contradicting our hypothesis that $w \notin M^*$. This completes the proof of Lemma 3.

From Lemmas 2 and 3 we now have

$$m = \sum_{j\in L} a_j \sum_{z=0}^{g-1} p^{z\delta+j} \tag{4.18}$$

and

$$k = p^{s\delta} + \ldots + p^{t\delta} \quad (0 \leqslant s < t < g)\,. \tag{4.19}$$

With m given explicitly by equation (4.18) we can complete the proof of Theorem 1. Suppose $M^* = N$ and let $a' = a_{u\delta+j}$ for some $j \in L$. As noted in Lemma 2, $a' < p/2$ since $M^* = N$. Let

$$r = a_{u\delta+j}p^{(n-t+u)\delta+j} + p^{(n-s+u)\delta+j}\,,$$

which is in M. Then

$$\begin{aligned} rk = a_{u\delta+j}p^{u\delta+j+[n-(t-s)]\delta} + \ldots + a_{u\delta+j}p^{u\delta+j} + \\ + p^{u\delta+j} + \ldots + p^{u\delta+j+(t-s)\delta} \end{aligned} \tag{4.20}$$

is in M. But the coefficient of $p^{u\delta+j}$ in rk is $a_{u\delta+j}+1$, which is greater than $a_{u\delta+j}$. Thus, if $a_{u\delta+j}+1 \leqslant p-1$, we have a contradiction. If $p \geqslant 4$, then

$$a_{u\delta+j}+1 = a'+1 < \frac{p}{2}+1 \leqslant p-1\,.$$

As $M^* = N$ excludes the cases $p = 2$ or 3, this completes the proof of Theorem 1 when $M^* = N$.

Suppose $M^* \neq N$. Let w be the least integer such that $w \notin M^*$. Then $w \neq 0$, $w-1 \geqslant 0$, and $w-1 \in M^*$. Let $w-1 = u\delta+j$ for some $j \in L$ and

$$r = a_{u\delta+j}p^{(n-t+u)\delta+j} + p^{(n-s+u)\delta+j}\,.$$

Then $r \in M$ and hence

$$\begin{aligned} rk = a_{u\delta+j}p^{u\delta+j+[n-(t-s)]\delta} + \ldots + a_{u\delta+j}p^{u\delta+j} + \\ + p^{u\delta+j} + \ldots + p^{u\delta+j+(t-s)\delta} \end{aligned} \tag{4.21}$$

must be in M. But the coefficient of $p^{u\delta+j}$ is $a_{u\delta+j}+1$, which is greater than $a_{u\delta+j}$. If $a_{u\delta+j}+1 \leqslant p-1$, we have a contradiction. If $a_{u\delta+j}+1 = p$, then

$$(a_{u\delta+j}+1)p^{u\delta+j} = p^{u\delta+j+1} = p^w \in M\,.$$

This contradicts our hypothesis that $w \notin M^*$ and completes the proof of Theorem 1.

It is worth noting that the proof of Theorem 1 when $d \nmid p-1$ is also valid when $d \mid p-1$.

5. Generalization of Theorem 1 to functions of two variables. We shall now generalize Theorem 1. In Theorem 2 we relax the condition that the function be normalized. We then prove Theorem 3, which is a generalization of Theorem 2 to functions of two variables.

Recall that d is an arbitrary divisor of $q-1$ and $md = q-1$. Also

$$\Psi_d(x) = x^m \tag{5.1}$$

for any $x \in F$.

THEOREM 2. *Let λ be a fixed element of F satisfying $\lambda^d = 1$. Let $f(x)$ be any function such that*

$$\Psi_d\big(f(x)-f(y)\big) = \lambda\Psi_d(x-y) \tag{5.2}$$

for any $x, y \in F$. Then

$$f(x) = ax^{p^i}+b \tag{5.3}$$

for some i in the range $0 \leqslant i < n$. Moreover

$$\Psi_d(a) = \lambda\,. \tag{5.4}$$

Proof. Let

$$f(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m \qquad (a_0 \neq 0) \tag{5.5}$$

be any polynomial satisfying the hypothesis of the theorem. By hypothesis (5.2), $f(x)$ is a permutation polynomial. Consider the polynomial

$$g(x) = \frac{f(x)-a_m}{f(1)-a}\,. \tag{5.6}$$

It is easily seen that $g(x)$ is a normalized permutation polynomial such that

$$\Psi_d\big(g(x)-g(y)\big) = \Psi_d(x-y) \tag{5.7}$$

for all $x, y \in F$. Hence $g(x)$ satisfies the hypothesis of Theorem 1. Therefore

$$g(x) = x^{p^i} \tag{5.8}$$

for some i in the range $0 \leqslant i < n$. Combining (5.6) and (5.8) we obtain the desired result.

We now generalize Theorem 2 to include functions of two variables. Recall that d_1 and d_2 are any divisors of $q-1$ and

$$m_1d_1 = m_2d_2 = q-1\,.$$

Also

$$\Psi_1(x) = x^{m_1}\,, \qquad \Psi_2(x) = x^{m_2} \tag{5.9}$$

for all $x \in F$. Let λ and μ be fixed elements of F such that

$$\lambda^{d_1} = 1\,, \qquad \mu^{d_2} = 1\,. \tag{5.10}$$

THEOREM 3. *Let $f(x, y)$ be a polynomial in x and y with coefficients in F. Then*

$$\Psi_1\big(f(x, y)-f(z, y)\big) = \lambda\Psi_1(x-z)\,, \tag{5.11}$$

$$\Psi_2\big(f(x, y)-f(x, z)\big) = \mu\Psi_2(y-z) \tag{5.12}$$

for all $x, y, z \in F$ if and only if

$$f(x) = ax^{p^i}+by^{p^j}+c\,, \tag{5.13}$$

where $0 \leqslant i < n$, $0 \leqslant j < n$, $d_1 | p^i-1$, and $d_2 | p^j-1$. Moreover

$$\Psi_1(a) = \lambda \quad \text{and} \quad \Psi_2(b) = \mu\,.$$

Proof. The necessity of Theorem 3 follows easily from the same argument used in the proof of the necessity of Theorem 1. It is also obvious that, for any polynomial of the form (5.13) which satisfies (5.11) and (5.12), we must have $d_1 | p^i-1$ and $d_2 | p^j-1$. Hence we need only prove that any polynomial satisfying (5.11) and (5.12) must be given by (5.13) with

$$\Psi_1(a) = \lambda \quad \text{and} \quad \Psi_2(b) = \mu\,.$$

Let y be any fixed element of F. Then from Theorem 2, we have

$$f(x, y) = ax^{p^i}+b\,, \qquad \Psi_1(a) = \lambda \qquad (0 \leqslant i < n)\,.$$

Similarly, for any fixed x,

$$f(x, y) = cy^{p^j}+d\,, \qquad \Psi_2(c) = \mu \qquad (0 \leqslant j < n)\,.$$

Therefore

$$f(x, y) = a(y)x^{p^{i(y)}}+b(y) \tag{5.14}$$

and

$$f(x, y) = c(x)y^{p^{j(x)}}+d(x)\,, \tag{5.15}$$

where $a(y), b(y), c(x), d(x)$ may be chosen to be polynomials in their respective variables with coefficients in F. Also $i(y)$ and $j(x)$ satisfy $0 \leqslant i(y) < n$ and $0 \leqslant j(x) < n$ for any $x, y \in F$.

For the case $n = 1$, equations (5.14) and (5.15) imply

$$f(x, y) = axy+bx+cy+d\,. \tag{5.16}$$

But, by hypothesis (5.11),

$$\Psi_1[(ay+b)(x-z)] = \lambda\Psi_1(x-z)$$

for all $x, y, z \in F$. Setting $x-z = 1$ results in

$$\Psi_1(ay+b) = \lambda$$

for all $y \in F$. If $a \neq 0$, then, for $y = -b/a$, we have

$$\Psi_1(0) = 0 = \lambda .$$

Hence $a = 0$ and the Theorem is proved for $n = 1$.

In the general case let

$$M_r = \{y : i(y) = r\} ,$$

where $0 \leqslant r < n$. Let $g_r(y)$ be the unique polynomial of degree $< q$ such that

$$g_r(y) = \begin{cases} 1 & (y \in M_r) , \\ 0 & (y \notin M_r) . \end{cases}$$

Then, by (5.14),

$$f(x, y) = a(y) \sum_{r=0}^{n-1} g_r(y) x^{p^r} + b(y)$$

or

$$f(x, y) = \sum_{r=0}^{n-1} a_r(y) x^{p^r} + b(y) , \tag{5.17}$$

where $a_r(y)$ for $0 \leqslant r \leqslant n-1$ is a polynomial in y only. Similarly, using (5.15) we have that

$$f(x, y) = \sum_{r=0}^{n-1} c_r(x) y^{p^r} + d(x) , \tag{5.18}$$

where $c_r(x)$ is a polynomial in x for $0 \leqslant r \leqslant n-1$.

From (5.17) and (5.18) it is evident that

$$f(x, y) = \sum_{s=0}^{n-1} \sum_{r=0}^{n-1} a_{rs} x^{p^s} y^{p^r} + \sum_{s=0}^{n-1} b_s x^{p^s} + \sum_{r=0}^{n-1} c_r y^{p^r} + d , \tag{5.19}$$

where a_{rs}, b_s, c_r, and d are elements of F. Applying hypothesis (5.11), we have

$$\Psi_1\Big[\sum_{s=0}^{n-1} \sum_{r=0}^{n-1} a_{rs}(x-z)^{p^s} y^{p^r} + \sum_{s=0}^{n-1} b_s (x-z)^{p^s} \Big] = \lambda \Psi_1(x-z)$$

for all $x, y, z \in F$. Setting $y = 0$, we have

$$\Psi_1\Big[\sum_{s=0}^{n-1} b_s (x-z)^{p^s} \Big] = \lambda \Psi_1(x-z)$$

for all x, $z \in F$. Thus the function

$$h(x) = \sum_{s=0}^{n-1} b_s x^{p^s}$$

satisfies the hypothesis of Theorem 2 and hence all $b_s = 0$ except one, say b_{s_0}. Moreover $\Psi_1(b_{s_0}) = \lambda$. A similar argument applies to the coefficients c_r in (5.19) by using hypothesis (5.12). Thus we have

$$f(x, y) = \sum_{s=0}^{n-1} \sum_{r=0}^{n-1} a_{rs} x^{p^s} y^{p^r} + b_{s_0} x^{p^{s_0}} + c_{r_0} y^{p^{r_0}} + d , \tag{5.20}$$

where $\Psi_1(b_{s_0}) = \lambda$ and $\Psi_2(c_{r_0}) = \mu$.

To complete the proof of Theorem 3 we need only show that the matrix $[a_{rs}]$ of coefficients in (5.20) is the zero matrix. Applying hypothesis (5.11) to $f(x, y)$ we have

$$\Psi_1\Big[\sum_{s=0}^{n-1} \sum_{r=0}^{n-1} a_{rs} y^{p^r} (x-z)^{p^s} + b_{s_0} (x-z)^{p^{s_0}} \Big] = \lambda \Psi_1(x-z)$$

for all $x, y, z \in F$. For a fixed y, let

$$h(x) = \sum_{s=0}^{n-1} \Big[\sum_{r=0}^{n-1} a_{rs} y^{p^r} \Big] x^{p^s} + b_{s_0} x^{p^{s_0}} . \tag{5.21}$$

Then $h(x)$ satisfies the hypothesis of Theorem 2 and must be a monomial in x. If $a_{rs_0} = 0$ for $r = 0, \ldots, n-1$, then $[a_{rs}]$ is the zero matrix because $h(x)$ always contains the nonzero term $b_{s_0} x^{p^{s_0}}$.

We now show that, for $p > 2$, any nonzero elements in the matrix $[a_{rs}]$ must occur in the s_0-column. Suppose $a_{r_1 s_1} \neq 0$ for some $s_1 \neq s_0$ and $a_{r_2 s_0} \neq 0$. Consider the polynomials

$$\sum_{r=0}^{n-1} a_{rs_0} y^{p^r} + b_{s_0} , \tag{5.22}$$

$$\sum_{r=0}^{n-1} a_{rs_1} y^{p^r} . \tag{5.23}$$

There are at least $q - p^{n-1}$ values of $y \in F$ for which the polynomial in (5.22) is nonzero. The same is true for the polynomial in (5.23). But $h(x)$ must be a monomial in x. Thus the elements of F for which the polynomial in (5.22) is nonzero are distinct from elements of F for which the polynomial in (5.23) is nonzero. Thus

$$2(q - p^{n-1}) \leqslant q$$

or $p \leqslant 2$, a contradiction. Therefore, for $p > 2$, the only nonzero elements in $[a_{rs}]$ occur in the s_0-column. In a similar manner we prove that, for $p > 2$, the only nonzero elements in $[a_{rs}]$ occur in the r_0-row. Hence, for $p > 2$, the only element in $[a_{rs}]$ which can be nonzero is $a_{r_0 s_0}$.

To obtain the same result for the case $p = 2$, we use the following

LEMMA 4. *Let F be a finite field of order $q = 2^n$. Suppose*

$$x^{2^n} - x = \Big[\sum_{r=0}^{n-1} a_r x^{2^r}\Big]\Big[\sum_{s=0}^{n-1} b_s x^{2^s} + 1\Big],$$

where $a_r, b_s \in F$. Then

$$a_r = \eta^{2^r - 1} \quad \text{and} \quad b_r = \eta^{2^r}$$

for some $\eta \neq 0$.

Proof. Equating coefficients we obtain the following identities:

$$\begin{aligned} &a_0 = 1, \\ &a_1 = a_0 b_0 = b_0, \quad && b_1 = a_1 b_0 = a_1^2, \\ &a_2 = a_1 b_1 = a_1^3, \quad && b_2 = a_2 b_0 = a_1^4, \\ &a_3 = a_2 b_2 = a_1^7, \quad && b_3 = a_3 b_0 = a_1^8, \\ &\cdots\cdots\cdots\cdots && \cdots\cdots\cdots\cdots \\ &a_r = a_1^{2^r - 1}, && b_r = a_1^{2^r}. \end{aligned}$$

Setting $\eta = a$ we obtain the desired result.

We now consider the matrix $[a_{rs}]$ for $p = 2$. First we show that at most 2 columns, or 2 rows, can contain nonzero elements. Suppose there are w columns in the matrix $[a_{rs}]$ containing nonzero elements and let

$$(5.24) \qquad \sum_{r=0}^{n-1} a_r y^{2^r}, \quad \ldots, \quad \sum_{r=0}^{n-1} a_{rs_0} y^{2^r} + b_{s_0}, \quad \ldots, \quad \sum_{r=0}^{n-1} a_{rw-1} y^{2^r}$$

be the corresponding polynomials defined by the rows in $[a_{rs}]$ containing nonzero elements. For any $y \in F$, the function $h(x)$, defined by (5.21), must be monomial in x. Therefore, for any y, y must be a root of $w-1$ of the polynomials in (5.24). Thus the system of polynomials in (5.24) must have at least $(w-1)2^n$ roots. But this system of polynomials has at most $w2^{n-1}$ roots. Hence $(w-1)2^n \leqslant w2^{n-1}$ or $2 \leqslant w/(w-1)$. This inequality is satisfied if and only if $w \leqslant 2$. Thus the matrix can contain at most 2 columns with nonzero elements. Moreover, if there are any columns containing nonzero elements, one of the columns must be the s_0-column. A similar result is true for the rows in the matrix $[a_{rs}]$.

When $p = 2$, suppose $a_{r_2 s_0} \neq 0$ for some r_2 and $a_{r_1 s_1} \neq 0$ for some $s_1 \neq s_0$. Since $h(x)$ is a monomial in x, then the polynomials

$$(5.25) \qquad \sum_{r=0}^{n-1} a_{rs_0} y^{2^r} + b_{s_0}, \quad \sum_{r=0}^{n-1} a_{rs_1} y^{2^r}$$

must have precisely 2^{n-1} roots and cannot have a root in common. Thus for any $y \in F$,

$$\Big[\sum_{r=0}^{n-1} a_{rs_0} y^{2^r} + b_{s_0}\Big]\Big[\sum_{r=0}^{n-1} a_{rs_1} y^{2^r}\Big] = 0.$$

Therefore

$$\Big[\sum_{r=0}^{n-1} a_{rs_0} y^{2^r} + b_{s_0}\Big]\Big[\sum_{r=0}^{n-1} a_{rs_1} y^{2^r}\Big] = \xi(y^{2^n} - y)$$

for some $\xi \in F$ such that $\xi \neq 0$. Applying Lemma 4, we have that all the elements in the s_0-column and all the elements in the s_1-column are nonzero. By a similar argument we have the same result for the rows of the matrix $[a_{rs}]$. This is a contradiction unless $n = 2$. But for $p = 2$ and $n = 2$ Theorem 3 is obvious.

We have shown that the only element in the matrix $[a_{rs}]$ which can be nonzero is $a_{r_0 s_0}$. Therefore

$$(5.26) \qquad f(x, y) = a_{rs} x^{p^s} y^{p^r} + b_s x^{p^s} + c_r y^{p^r} + d,$$

where $s = s_0$ and $r = r_0$.

Now applying hypothesis (5.11) to formula (5.26) we have

$$\Psi_1\big(a_{rs} y^{p^r}(x-z)^{p^s} + b_s (x-z)^{p^s}\big) = \lambda \Psi_1(x-z)$$

for all $x, y, z \in F$. Letting $x - z = 1$, this becomes

$$\Psi_1(a_{rs} y^{p^r} + b_s) = \lambda$$

for all $y \in F$. If $a_{rs} \neq 0$, then, for

$$y = -(b_s/a_{rs})^{p^{n-r}},$$

we have $\Psi_1(0) = \lambda$. Therefore $a_{rs} = 0$ and

$$f(x, y) = b x^{p^s} + c y^{p^r} + d,$$

where $\Psi_1(b) = \lambda$ and $\Psi_2(c) = \mu$.

6. Generalization to functions of m variables. We now want to generalize Theorem 3 to functions of m variables. Suppose we have m arbitrary divisors of $q-1$, that is,

$$(6.1) \qquad d_s \mid q-1 \quad (s = 1, \ldots, m).$$

Let

$$(6.2) \qquad \Psi_s(x) = x^{(q-1)/d_s} \quad (s = 1, \ldots, m)$$

for any $x \in F$. For each $i = 1, \ldots, m$ let λ_i be a fixed element of F such that

$$(6.3) \qquad \lambda_i^{d_i} = 1.$$

We now formally state

THEOREM 4. *Let $f(x_1, \ldots, x_m)$ be a polynomial in $x_1, \ldots, x_m$ with coefficients in F. Then*

$$\Psi_s[f(x_1, \ldots, x_{s-1}, x_s, x_{s+1}, \ldots, x_m) - f(x_1, \ldots, x_{s-1}, y_s, x_{s+1}, \ldots, x_m)] = \lambda_s \Psi_s(x_s - y_s) \quad (s = 1, 2, \ldots, m) \tag{6.4}$$

for all x_i, y_i in F if and only if

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i x_i^{p^{r_i}} + b \quad (0 \leqslant r_i < n) \tag{6.5}$$

where

$$\Psi_i(a_i) = \lambda_i, \quad d_i | p^{r_i} - 1$$

for all $i = 1, 2, \ldots, m$.

The proof of the necessity of Theorem 4 is similar to that for Theorem 1. Also, for any polynomial of the form (6.5) which satisfies (6.4), we must have $d_i | p^{r_i} - 1$ for all i. Thus we need only show that any polynomial satisfying (6.4) must be given by (6.5) with $\Psi_i(a_i) = \lambda_i$ for all i.

The proof goes by induction on m. Theorem 2 applies when $m = 1$ and Theorem 3 applies when $m = 2$. Thus suppose the Theorem is true for some $m \geqslant 2$ variables. For a fixed $x = x_{m+1}$, hypothesis (6.4) and the induction hypothesis imply

$$f(x_1, \ldots, x_m, x) = \sum_{i=1}^{m} a_i(x) x_i^{p^{r_i(x)}} + b(x). \tag{6.6}$$

For a fixed $x_1, \ldots, x_m$, we have by Theorem 2,

$$f(x_1, \ldots, x_m, x) = a(x_1, \ldots, x_m) x^{p^{r(x_1, \ldots, x_m)}} + c(x_1, \ldots, x_m). \tag{6.7}$$

In a method similar to the one used in the proof of Theorem 3, we may write (6.6) and (6.7) as

$$f(x_1, \ldots, x_m, x) = \sum_{j=0}^{n-1} \sum_{i=1}^{m} a_{ij}(x) x_i^{p^j} + b(x), \tag{6.8}$$

$$f(x_1, \ldots, x_m, x) = \sum_{j=0}^{n-1} a_j(x_1, \ldots, x_m) x^{p^j} + c(x_1, \ldots, x_m), \tag{6.9}$$

where $a_{ij}(x)$, $b(x)$, $a_j(x_1, \ldots, x_m)$ and $c(x_1, \ldots, x_m)$ are polynomials in their respective variables with coefficients in F. Comparison of (6.8) and (6.9) yields

$$f(x_1, \ldots, x_m, x) = \sum_{k=0}^{n-1} \sum_{j=0}^{n-1} \sum_{i=1}^{m} a_{ijk} x_i^{p^j} x^{p^k} + \sum_{j=0}^{n-1} b_j x^{p^j} + \sum_{j=0}^{n-1} \sum_{i=1}^{m} c_{ij} x_i^{p^j} + d \tag{6.10}$$

where a_{ijk}, b_j, c_{ij}, and d are elements of F.

Applying hypothesis (6.4) to equation (6.10) results in

$$\Psi_{m+1}\Big[\sum_{k=0}^{n-1} \sum_{j=0}^{n-1} \sum_{i=1}^{m} a_{ijk} x_i^{p^j} (x-y)^{p^k} + \sum_{j=0}^{n-1} b_j (x-y)^{p^j}\Big] = \lambda_{m+1} \Psi_{m+1}(x-y)$$

for all x_i, x, y in F. Thus for $x_1 = \ldots = x_m = 0$, we have

$$\Psi_{m+1}\Big[\sum_{j=0}^{n-1} b_j (x-y)^{p^j}\Big] = \lambda_{m+1} \Psi_{m+1}(x-y)$$

for all $x, y \in F$. Hence the function

$$\sum_{j=0}^{n-1} b_j x^{p^j}$$

satisfies the hypothesis of Theorem 2. Therefore all the b_j's are zero except one, say b_{j_0}. Moreover $\Psi_{m+1}(b_{j_0}) = \lambda_{m+1}$.

For any i such that $1 \leqslant i \leqslant m$, the application of hypothesis (6.4) to equation (6.10) yields

$$\Psi_i\Big[\sum_{k=0}^{n-1} \sum_{j=0}^{n-1} a_{ijk} (x_i - y_i)^{p^j} x^{p^k} + \sum_{j=0}^{n-1} c_{ij} (x_i - y_i)^{p^j}\Big] = \lambda_i \Psi_i(x_i - y_i).$$

Setting $x = 0$, we have

$$\Psi_i\Big[\sum_{j=0}^{n-1} c_{ij} (x_i - y_i)^{p^j}\Big] = \lambda_i \Psi_i(x_i - y_i)$$

for all $x_i, y_i \in F$. Therefore the function

$$\sum_{j=0}^{n-1} c_{ij} x_i^{p^j}$$

satisfies the hypothesis of Theorem 2 for each i such that $1 \leqslant i \leqslant m$. Thus for each i the coefficients c_{ij} are zero except for one, say c_{ij_i}. Moreover $\Psi_i(c_{ij_i}) = \lambda_i$ for each i. Therefore (6.10) reduces to

$$f(x_1, \ldots, x_m, x) = \sum_{k=0}^{n-1} \sum_{j=0}^{n-1} \sum_{i=1}^{m} a_{ijk} x_i^{p^j} x^{p^k} + b x^{p^{j_0}} + \sum_{i=1}^{m} c_i x_i^{p^{j_i}} + d, \tag{6.11}$$

where $b = b_{j_0}$ and $c_i = c_{ij_i}$.

We must yet show that all the coefficients a_{ijk} are zero. Applying hypothesis (6.4) to equation (6.11) results in the following identities:

$$(6.12)\qquad \Psi_{m+1}\Big[\sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\sum_{s=1}^{m} a_{sjk}x_s^{p^j}(x-y)^{p^k}+b(x-y)^{p^{j_0}}\Big] = \lambda_{m+1}\Psi_{m+1}(x-y)\,,$$

$$(6.13)\qquad \Psi_i\Big[\sum_{k=0}^{n-1}\sum_{j=0}^{n-1} a_{ijk}x^{p^k}(x_i-y_i)^{p^j}+c_i(x_i-y_i)^{p^{j_i}}\Big] = \lambda_i\Psi_i(x_i-y_i) \qquad (i=1,\ldots,m)$$

for any $x_i, y_i, x, y \in F$. For a fixed i, we set $x_s = 0$ in (6.12) when $s \neq i$ and obtain

$$(6.14)\qquad \Psi_{m+1}\Big[\sum_{k=0}^{n-1}\sum_{j=0}^{n-1} a_i x_i^{p^j}(x-y)^{p^k}+b(x-y)^{p^{j_0}}\Big] = \lambda_{m+1}\Psi_{m+1}(x-y)$$

for all $x_i, x, y \in F$. Put

$$h_i(x, x_i) = \sum_{k=0}^{n-1}\sum_{j=0}^{n-1} a_{ijk}x^{p^k}x_i^{p^j}+bx^{p^{j_0}}+c_ix_i^{p^{j_i}}\,.$$

Then equations (6.13) and (6.14) show that $h_i(x, x_i)$ satisfies the hypothesis of Theorem 3. Therefore

$$\sum_{k=0}^{n-1}\sum_{j=0}^{n-1} a_{ijk}x^{p^k}x_i^{p^j} = 0$$

for any x and x_i in F. This is impossible unless $a_{ijk} = 0$ for all j and k. Since this is true for any i such that $1 \leqslant i \leqslant m$, we have

$$f(x_1, \ldots, x_m, x) = bx^{p^{j_0}}+\sum_{i=1}^{m} c_ix_i^{p^{j_i}}+d\,,$$

where $\Psi_{m+1}(b) = \lambda_{m+1}$ and $\Psi_i(c_i) = \lambda_i$. This completes the inductive proof.

References

[1] L. Carlitz, *A theorem on permutations in a finite field*, Proc. of the Amer. Math. Soc. 11 (1960), pp. 456-459.

[2] — *A theorem on „ordered" polynomials in a finite field*, Acta Arith. 7 (1962), pp. 167-172.

[3] L. E. Dickson, *Linear groups*, Leipzig 1901.

[4] L. E. Dickson, *History of the theory of numbers*, vol. 3, Washington 1923.

[5] G. Järnefelt, *Reflections on a finite approximation to Euclidean geometry, Physical and astronomical prospects*, Ann. Acad. Sci. Fennicae, Series A, I, (1951), no. 96.

[6] P. Kustaanheimo, *On the relation of order in geometries over a Galois field*, Soc. Fennica, Commentationes Physico-Mathematicae 20 (1957), no. 8.

[7] — *On the relation of order in finite geometries*, Rend. Math. e delle sue Appl. 16 (1957), pp. 292-296.

[8] E. Lucas, *Sur les congruences des nombres eulériennes et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. de France 6 (1878), pp. 49-54.

[9] F. R. Moulton, *A simple non-Desarguesian plane*, Trans. Amer. Math. Soc. 3 (1902), pp. 192-195.

[10] W. A. Pierce, *Moulton planes*, Canadian Journ. Math. 13 (1961), pp. 427-436.

Reçu par la Rédaction le 17. 5. 1962