ACTA ARITHMETICA
XLVI (1986)

# Commuting polynomial vectors over an integral domain

by

RUDOLF LIDL (Hobart, Australia) and GARY L. MULLEN (Univeristy Park, Pa.)

**1. Introduction.** Numerous papers have been written concerning polynomials which commute under composition, see for example, [1]–[3], [8]–[10], [14], [17]. Because of the following result, the classical Chebyshev polynomials $T_n$ of the first kind in one variable are of special interest. In [1] Bertram showed that over an integral domain of characteristic zero, if $n \geqslant 2$ and the polynomial $f$ of degree $k \geqslant 1$ commutes under substitution with $T_n$, then $f = T_k$ if $n$ is even and $f = \pm T_k$ if $n$ is odd.

In the present paper we shall consider the problem of commuting polynomial vectors in two variables. In particular, in Section 3 we shall determine all polynomial vectors in two variables which, under componentwise composition, commute with two dimensional generalizations of the Chebyshev polynomials which were first considered by Dunn and Lidl [4], [5] and Lidl and Wells [13]. In Section 5 we present some results which extend to several variables, some of the ideas of Wells [17] and Mullen [14] concerning polynomials over finite fields which commute with linear permutations.

**2. Preliminaries.** If $R$ is an integral domain of characteristic not two, let $R[x, y]$ denote the ring of polynomials in two indeterminates $x$ and $y$ over $R$. If $f_1 \in R[x, y]$, define the degree of $f_1$ to be the total degree of $f_1$. If $f_1, f_2 \in R[x, y]$ then let $f = (f_1, f_2) \in (R[x, y])^2$ and define the degree of $f$ to be the maximum of the degrees of $f_1$ and $f_2$.

We say that $f, g \in (R[x, y])^2$ *commute* if

$$f \circ g = g \circ f \tag{2.1}$$

where $\circ$ denotes componentwise composition. Thus (2.1) implies that

$$f_1(g_1, g_2) = g_1(f_1, f_2) \quad \text{and} \quad f_2(g_1, g_2) = g_2(f_1, f_2).$$

The classical Chebyshev polynomials in one variable defined by $T_0 = 1$, $T_1 = x$, and $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ for $n \geqslant 2$, were extended to several variables in a series of papers [4]–[6] and [12]–[13]. Before proceeding with our investigation of commuting polynomial vectors, we shall list some properties of the generalized Chebyshev polynomials that will prove to be useful in our later work.

If $n \in Z$, let $P_n(x, y)$ be defined by the functional equation

$$P_n(x, y) = u^n + v^n + w^n$$

where

$$x = u+v+w, \quad y = uv+uw+vw, \quad \text{and} \quad uvw = 1.$$

Using the notation of [4], $P_n(x, y)$ may also be defined by

$$P_n(x, y) = (1/2) P_{n,0}^{-1/2}(x, y; 1)$$

where $P_{n,m}^{-1/2}$ is given in Definition 2.1 of [4]. The polynomials $P_n(x, y)$ are known as *generalized Chebyshev polynomials* in two variables. Multi-dimensional Chebyshev polynomials have been studied in [4] and [12]–[13].

Similarly if $n \in Z^+$, let $Q_n(x, y)$ be defined by

$$Q_n(x, y) = u^n + v^n$$

where

$$x = u+v \quad \text{and} \quad y = uv.$$

Again following the notation of [4], $Q_n(x, y) = P_{n,0}^{-1/2}(x; y)$. In Lausch and Nöbauer [10], the notation $g_n(y, x)$ for $y = a \in R$ has also been used for these polynomials, called *Dickson polynomials*.

Several results concerning these polynomials will prove to be useful. These results include

$$P_n(x, y) = P_{-n}(y, x), \tag{2.2}$$

$$P_n(x, y) = \sum_{i=0}^{[n/2]} \sum_{j=0}^{[n/3]} d_{ij} x^{n-2i-3j} y^i, \quad n \in Z^+, \tag{2.3}$$

where

$$d_{ij} = \frac{n(-1)^i}{n-i-2j} \binom{n-i-2j}{i+j} \binom{i+j}{i}$$

is an integer with $d_{00} = 1$ and $d_{10} = -n$.

$$Q_n(x, y) = \sum_{i=0}^{[n/2]} e_i x^{n-2i} y^i \tag{2.4}$$

where

$$e_i = \frac{n(-1)^i}{n-i} \binom{n-i}{i}$$

is an integer with $e_0 = 1$ and $e_1 = -n$.



For these and other details regarding generalized Chebyshev polynomials, the reader should consult Dunn and Lidl [4]–[5] and Lidl and Wells [13].

Throughout this paper let $G_n \doteq (P_n, P_{-n})$ and $H_n = (Q_n, y^n)$ so that for the few values of $n$ we have

| $n$ | $P_n$ | $P_{-n}$ | $Q_n$ | $y^n$ |
|---|---|---|---|---|
| 0 | 3 | 3 | 2 | 1 |
| 1 | $x$ | $y$ | $x$ | $y$ |
| 2 | $x^2-2y$ | $y^2-2x$ | $x^2-2y$ | $y^2$ |
| 3 | $x^3-3xy+3$ | $y^3-3xy+3$ | $x^3-3xy$ | $y^3$ |
| 4 | $x^4-4x^2y+2y^2+4x$ | $y^4-4xy^2+2x^2+4y$ | $x^4-4x^2y+2y^2$ | $y^4$ |

We note that in the notation of [13], $G_n = g(2, n, 1)$ and $H_n = g(2, n, 0)$.

If $\varphi(x, y) = (x+y+(xy)^{-1}, x^{-1}+y^{-1}+xy)$ then it is easy to check that

$$\varphi(x, y) = \varphi(y, x) = \varphi((xy)^{-1}, y) = \varphi(x, (xy)^{-1}) \tag{2.5}$$

and from the definition of $G_n$ it can be seen that

$$G_n \circ \varphi(x, y) = (x^n+y^n+(xy)^{-n}, x^{-n}+y^{-n}+(xy)^n) = \varphi(x^n, y^n). \tag{2.6}$$

Similarly if $\theta(x, y) = (x+y, xy)$ then

$$\theta(x, y) = \theta(y, x) \tag{2.7}$$

and from the definition of $H_n$ we have

$$H_n \circ \theta(x, y) = (x^n+y^n, x^n y^n) = \theta(x^n, y^n). \tag{2.8}$$

**3.** In the first part of this section we will determine all polynomial vectors over $R$ which commute with $G_n$ where $n \geqslant 2$. We will then determine all polynomial vectors over $R$ which commute with $H_n$. First however, we prove a lemma which will be very useful in our later work. If $p \in Z$ and $g \in R(x, y)$ has degree strictly less than $p$ we will write $g(x, y) = O(p)$. As usual, the degree of a rational function $g = r/s$ is defined as $\deg r - \deg s$. We now prove

LEMMA 3.1. *If*

$$f(x, y) = \sum_{i+j \leqslant m} a_{ij} x^i y^j \in R(x, y)$$

*has only finitely many terms, is of degree $m \geqslant 1$ and has the property that*

$$f(x^n, y^n) = [f(x, y)]^n + O(mn-p)$$

*where $n \geq 2$, the characteristic of $R$ does not divide $n$, and $p \geq 1$, then there exists an integer $r$ with $0 \leq r \leq m$ such that*

$$f(x, y) = \alpha x^r y^{m-r} + O(m-p)$$

*where $\alpha^{n-1} = 1$.*

Proof. Let $f(x, y) = \sum_{i+j \leq m} a_{ij} x^i y^j$ so that

$$\sum a_{ij} x^{ni} y^{nj} = \left[\sum a_{ij} x^i y^j\right]^n + O(mn-p). \tag{3.1}$$

Since $f$ has degree $m$ the set $\{i \mid a_{i,m-i} \neq 0\}$ is non-empty. Let $r$ be the minimal element of this set. By equating coefficients of $x^{nr} y^{n(m-r)}$ in (3.1) we have $a_{r,m-r}^{r-1} = 1$.

Suppose there is a non-zero term of degree greater than or equal to $m-p$. Choose $(s, t) \neq (r, m-r)$ so that $a_{st} \neq 0$, $s+t$ is maximal, and $s$ minimal. Consider the coefficient of $(x^r y^{m-r})^{n-1}(x^s y^t)$ in (3.1). We have

$$\left(r(n-1)+s, (m-r)(n-1)+t\right) \neq (ns, nt) \neq \left(nr, n(m-r)\right)$$

so that the coefficient of this term on the left-hand side of (3.1) is zero. The degree of this term is

$$m(n-1)+(s+t) \geq m(n-1)+(m-p) = mn-p$$

so that the coefficient of it on the right-hand side of (3.1) is $na_{r,m-r}^{n-1} a_{st}$, which is non-zero. This completes the proof of the lemma.

We will now prove the following result which is analogous to Bertram's result in [1] for the classical Chebyshev polynomials of the first kind.

Theorem 3.2. *Suppose $n \geq 2$ and the characteristic of $R$ does not divide $n$. If $f \in (R[x, y])^2$ is of degree $m \geq 1$, then $f$ commutes with $G_n$ if and only if $f$ is of the form*

$$f = (\alpha P_m, \alpha^2 P_{-m}) \quad \text{or} \quad f = (\alpha P_{-m}, \alpha^2 P_m) \tag{3.2}$$

*where $\alpha = 1$ if $n \not\equiv 1 \pmod 3$ or $\alpha^3 = 1$ if $n \equiv 1 \pmod 3$.*

Proof. For necessity, it is shown in Section 5 of [13] that $G_m$ commutes with $G_n$ so that by (2.3), we see that $(\alpha P_m, \alpha^2 P_{-m})$ commutes with $G_n$. Hence if $f = (f_1, f_2)$ commutes with $G_n$, then using (2.2) we have

$$f_2(P_n, P_{-n}) = P_{-n}(f_1, f_2) = P_n(f_2, f_1).$$

Similarly

$$f_1(P_n, P_{-n}) = P_{-n}(f_2, f_1)$$

so that $(f_2, f_1)$ commutes with $G_n$ and thus $(\alpha^2 P_{-m}, \alpha P_m)$ commutes with $G_n$. Since $\alpha^3 = 1$ we see that $(\alpha P_{-m}, \alpha^2 P_m)$ commutes with $G_n$.



Conversely, suppose that $f = (f_1, f_2)$ commutes with $G_n$ for $n \geq 2$ where $n$ does not divide the characteristic of $R$. For $i = 1, 2$ let the degree of $f_i$ be $m_i$ and let $m = \max\{m_1, m_2\}$. Since $f \circ G_n = G_n \circ f$ we have

$$f \circ G_n \circ \varphi = G_n \circ f \circ \varphi. \tag{3.3}$$

From (2.6) we see that $G_n \circ \varphi(x, y) = \varphi(x^n, y^n)$ so that if we let $h = f \circ \varphi$ then (3.3) becomes

$$h(x^n, y^n) = G_n \circ h(x, y). \tag{3.4}$$

Let $h = (h_1, h_2)$ where for $i = 1, 2$ the degree of $h_i$ is $p_i$. We shall now consider three cases:

Case 1: $p_2 > p_1$. Let

$$h_2(x, y) = \sum_{-2m_2 \leq i+j \leq p_2} a_{ij} x^i y^j$$

so that the second component of (3.4) becomes

$$\sum a_{ij} x^{ni} y^{nj} = P_{-n}\left(h_1, \sum a_{ij} x^i y^j\right). \tag{3.5}$$

In $P_{-n}$, the coefficient of $y^{n-1}$ is zero and thus (3.5) yields

$$\sum a_{ij} x^{ni} y^{nj} = \left(\sum a_{ij} x^i y^j\right)^n + O\left(p_2(n-1)\right). \tag{3.6}$$

Since $h_2(x, y)$ has the form given in Lemma 3.1, we may apply the lemma so that there exists an integer $r$ with $0 \leq r \leq p_2$ such that $a_{r,p_2-r}^{n-1} = 1$, and moreover if $i+j \geq 0$, and $(i, j) \neq (r, p_2-r)$, then $a_{ij} = 0$. For simplicity of notation let $a_{r,p_2-r} = \beta$ so that

$$h_2 = \beta x^r y^{p_2-r} \sum_{-2m_2 \leq i+j \leq 0} a_{ij} x^i y^j \tag{3.7}$$

where $\beta^{n-1} = 1$.

Since $\varphi(x, y) = \varphi(y, x)$ we have $h_2(x, y) = h_2(y, x)$ and thus $a_{p_2-r,r} = a_{r,p_2-r} \neq 0$ so that $p_2 - r = r$ and hence $2r = p_2$.

From (2.5), the coefficients of $(xy)^{-r} y^r = x^{-r}$ and $x^r(xy)^{-r} = y^{-r}$ are equal to the coefficient of $x^r y^r$ which is $\beta$. Suppose that $a_{ij} \neq 0$ for some $i+j < 0$ with $(i, j) \neq (0, -r)$ or $(-r, 0)$. Then the coefficients of $x^{-i} y^{j-i}$ and $x^{i-j} y^{-j}$ are non-zero so that either $j-2i \geq 0$ or $i-2j \geq 0$. Thus either $r = -i$ or $r = j-i$ which implies that $(i, j) = (-r, 0)$ or else $r = -j$ or $r = i-j$ so that $(i, j) = (0, -r)$. In either case we have a contradiction.

Substituting into (3.7) gives

$$h_2 = \beta(x^r y^r + x^{-r} + y^{-r}) \tag{3.8}$$

where $\beta^{n-1} = 1$ and $2r = p_2$. From (2.6) we have $h_2 = \beta P_{-r} \circ \varphi$ so that $f_2 = \beta P_{-r}$. Since the degree of $f_2$ is $m_2 = r$ we see that

$$f_2 = \beta P_{-m_2} \tag{3.9}$$

where $\beta^{n-1} = 1$.

Now let $l=(l_1, l_2)$ where $l(x, y)=h(x^{-1}, y^{-1})$. Hence from (3.8) and (3.9) we obtain

$$l_2=\beta\left(x^{m_2}+y^{m_2}+(xy)^{-m_2}\right). \tag{3.10}$$

From (3.4)

$$h(x^{-n}, y^{-n})=G_n\circ h(x^{-1}, y^{-1})$$

so that

$$l(x^n, y^n)=G_n\circ l(x, y). \tag{3.11}$$

Let $l_1=\sum_{i+j\leqslant q} b_{ij}x^i y^j$ be of degree $q$. From the second component of (3.11) we have

$$\begin{aligned}\beta\left(x^{nm_2}+y^{nm_2}+(xy)^{-nm_2}\right) &= P_{-n}\left(l_1, \beta\left(x^{m_2}+y^{m_2}+(xy)^{-m_2}\right)\right) \\ &= \beta^n[x^{m_2}+y^{m_2}+(xy)^{-m_2}]^n+O\left((n-1)\max\{m_2, q\}+1\right).\end{aligned} \tag{3.12}$$

From the coefficient of $x^{(n-1)m_2}y^{m_2}$ in (3.12) we have $0=n\beta^n+k$ for some constant $k$ so that $k=-n\beta\neq 0$. For $n\geqslant 2$, $(n-1)q\geqslant nm_2$ so that $q>m_2$.

From the first component of (3.11) we have

$$\begin{aligned}\sum b_{ij}x^{ni}y^{nj} &= P_n\left(\sum b_{ij}x^i y^j, \beta\left(x^{m_2}+y^{m_2}+(xy)^{-m_2}\right)\right) \\ &= \left(\sum b_{ij}x^i y^j\right)^n+O\left((n-1)q\right)\end{aligned}$$

since $q>m$ and the coefficient of $x^{n-1}$ in $P_n$ is zero. Thus by Lemma 3.1 there exists an integer $s$ with $0\leqslant s\leqslant q$ such that $b_{s,q-s}^{n-1}=1$ and $b_{ij}=0$ for $(i, j)\neq(s, q-s)$ with $i+j\geqslant 0$.

Similarly using (2.5) we obtain

$$l_1=\alpha\left((xy)^{m_1}+x^{-m_1}+y^{-m_1}\right) \tag{3.13}$$

where $\alpha^{n-1}=1$ so that $h_1=\alpha\left(x^{m_1}+y^{m_1}+(xy)^{-m_1}\right)$ and thus $f_1=\alpha P_{m_1}$. Combining this with (3.9) we have

$$f=(\alpha P_{m_1}, \beta P_{-m_2}) \tag{3.14}$$

where $\alpha^{n-1}=\beta^{n-1}=1$.

We now show that $m_1=m_2$. To this end, consider the first component of (3.13) so that $h_1(x^n, y^n)=P_n(h_1, h_2)$. Hence

$$\begin{aligned}\alpha\left(x^{m_1 n}+y^{m_1 n}+(xy)^{-m_1 n}\right) &= \alpha^n\left(x^{m_1}+y^{m_1}+(xy)^{-m_1}\right)^n+\sum_{i+j<n} c_{ij}h_1^i h_2^j \\ &= \alpha x^{m_1 n}+n\alpha x^{m_1(n-1)}y^{m_1}+\ldots\end{aligned} \tag{3.15}$$

where each $c_{ij}\in R$. Since $n\alpha\neq 0$ there exist integers $i$ and $j$ with $i+j<n$ such that $c_{ij}\neq 0$ and

$$x^{m_1(n-1)}y^{m_1}=(x^{m_1})^i(xy)^{m_2 j}=x^{m_1 i+m_2 j}y^{m_2 j}.$$



Thus $m_1(n-1)=m_1 i+m_2 j$ and $m_1=m_2 j$ so that $i=n-2$. Since $i+j<n$ and $j\neq 0$, we have $j=1$ and thus $m_1=m_2$.

From (2.5) we know that $c_{n-2,1}=-n$ so that the coefficient of $x^{m_1(n-1)}y^{m_1}$ in (3.15) is $0=-n\alpha+n\alpha^{n-2}\beta$ and hence $\beta=\alpha^2$. Since $P_n(x, y)=P_{-n}(y, x)$ we have $\alpha=\beta^2$ so that $\alpha^3=1$. If $n\not\equiv 1 \pmod 3$ then (3.13) implies that $\alpha=1$. This completes the proof in Case 1.

Case 2: $p_2<p_1$. If we consider the transformation $k=(h_2, h_1)$ then we can use an argument analogous to that used in Case 1 to show that $f$ must be of the desired form.

Case 3: $p_2=p_1$. In this case equation (3.6) becomes

$$\sum a_{ij}x^{ni}y^{nj}=\left(\sum a_{ij}x^i y^j\right)^n+O\left(p_2(n-1)+1\right). \tag{3.16}$$

Using Lemma 3.1 and an argument analogous to that used in Case 1, we obtain

$$h_2=\beta\left((xy)^{m_2}+x^{-m_2}+y^{-m_2}+k_2\right) \tag{3.17}$$

where $\beta^{n-1}=1$ and $k_2\in R$. Applying the same argument to the first component we have

$$h_1=\alpha\left((xy)^{m_1}+x^{-m_1}+y^{-m_1}+k_1\right) \tag{3.18}$$

where $\alpha^{n-1}=1$ and $k_1\in R$. Since $p_2=p_1$ we have $m_2=m_1=m$.

As in Case 1, let $l(x, y)=h(x^{-1}, y^{-1})$ where the degree of $l$ is $q$. Arguing as in Case 1, we can see that $q>m_2$. Hence $m_2=m_1=q$, which is a contradiction. Thus $f$ cannot be of the correct form and the proof of the theorem is complete.

We now prove a result analogous to Theorem 3.2 for the Dickson polynomials. In particular, we will prove

THEOREM 3.3. *Suppose $n\geqslant 2$ and the characteristic of $R$ does not divide $n$. If $f\in(R[x, y])^2$ is of degree $m\geqslant 1$, then $f$ commutes with $H_n$ if and only if $f$ is of the form*

$$f=(\alpha Q_m, \alpha^2 y^m) \tag{3.19}$$

*where $\alpha^{n-1}=1$.*

Proof. In Section 5 of [13] it was shown that $H_m$ commutes with $H_n$. If $f$ has the above form, then substituting into (2.4), we obtain

$$\begin{aligned}Q_n\circ f &= \sum e_i(\alpha Q_m)^{n-2i}(\alpha^2 y^m)^i=\sum e_i\alpha^n Q_m^{n-2i}y^{mi} \\ &= \alpha\sum e_i Q_m^{n-2i}y^{mi}=\alpha Q_n\circ H_m=\alpha Q_m\circ H_n.\end{aligned}$$

Hence $Q_n\circ f=f_1\circ H_n$ and $(\alpha^2 y^m)^n=\alpha^2(y^n)^m$ so that $f$ commutes with $H_n$.

Conversely suppose $f$ commutes with $H_n$ where the degree of $f$ is $m$. For simplicity of notation let $g=(g_1, g_2)=H_n$. Then we have

$$f\circ g\circ\theta=g\circ f\circ\theta. \tag{3.20}$$

Let $h = f \circ \theta$ where the degree of $h_i$ is $p_i$ for $i = 1, 2$. From (2.8) and (3.20) we have

$$h(x^n, y^n) = g \circ h(x, y). \tag{3.21}$$

From the second component of (3.21) we obtain

$$h_2(x^n, y^n) = g_2(h_1(x, y), h_2(x, y)) = [h_2(x, y)]^n \tag{3.22}$$

and from Lemma 3.1 we have

$$h_2(x, y) = \beta x^r y^{p_2 - r} + O(p_2 - p_2 m) = \beta x^r y^{p_2 - r} \tag{3.23}$$

where $\beta^{n-1} = 1$ and $r$ is an integer such that $0 \leqslant r \leqslant p_2$. Using (2.7) we see that $h_2(x, y) = h_2(y, x)$ so that $2r = p_2$. Substituting into (3.23) gives $h_2(x, y) = \beta x^r y^r$ so that $f_2(x, y) = \beta y^r$. Since the degree of $f_2$ is $m_2$ we have

$$f_2 = \beta y^{m_2} \tag{3.24}$$

where $\beta^{n-1} = 1$.

Let $y = 0$ in the first component of (3.21) so that

$$h_1(x^n, 0) = g_1(h_1(x, 0), h_2(x, 0)) = g_1(h_1(x, 0), 0). \tag{3.25}$$

Hence from [13], $g_1(x, y) = P_n^{-1/2}(x; y)$ and furthermore $g_1(x, 0) = x^n$. Substituting back into (3.25) yields

$$h_1(x^n, 0) = [h_1(x, 0)]^n. \tag{3.26}$$

If we let $y = 0$ in Lemma 3.1 we clearly have $h_1(x, 0) = \alpha x^r$ where $\alpha^{n-1} = 1$ and $0 \leqslant r \leqslant p_1$. Since $\theta$ is symmetric, $h_1$ is symmetric and thus $h_1$ has the form

$$h_1(x, y) = \alpha(x^r + y^r) + xyl(x, y) \tag{3.27}$$

for some $l \in R[x, y]$.

Let $h_1(x, y) = \sum_{i+j<p_1} a_{ij} x^i y^j$ and let $q = \min\{i+j \mid a_{ij} \neq 0\}$. Assume that $q < m_2$ and that $p_1 > m_2$. Then

$$h_1(x, y) = \alpha_1 x^r y^{p_1 - r} + \sum a_{ij} x^i y^j + \alpha_2 x^s y^{q-s} \tag{3.28}$$

where $\alpha_1$ and $\alpha_2$ are non-zero and $r$ and $s$ are minimal among the non-zero terms of degree $p_1$ and $q$ respectively.

From the first component of (3.21) we have using (2.4) and (3.23)

$$h_1(x^n, y^n) = g_1(h_1, h_2) = \sum_{k=0}^{[n/2]} e_k h_1^{n-2k} (\beta x^r y^{m_2 - r})^k. \tag{3.29}$$

If we now substitute (3.28) we obtain

$$\begin{aligned} \alpha_1 x^{nr} y^{n(p_1 - r)} + \sum a_{ij} x^{ni} y^{nj} + \alpha_2 x^{ns} y^{n(q-s)} \\ = \sum e_i (\alpha_1 x^r y^{p_1 - r} + \sum a_{ij} x^i y^j + \alpha x^s y^{q-s})^{n-2k} (\beta x^r y^{m_2 - r})^k. \end{aligned} \tag{3.30}$$



Since $e_0 = 1$ and $p_1 > m_2$, the coefficient of $x^{rn} y^{(p_1 - r)n}$ is $\alpha_1 = \alpha_1^n$ so that $\alpha_1^{n-1} = 1$. Moreover since $q < m_2$, the term of smallest total degree is $x^{ns} y^{n(q-s)}$ whose coefficient in (3.30) is $\alpha_2 = \alpha_2^n$, whence $\alpha_2^{n-1} = 1$.

Assume that there exists a pair $(t, u) \neq (s, q-s)$ with $t+u \leqslant m$ and $a_{tu} \neq 0$. Then the coefficient of $[x^s y^{q-s}]^{n-1}(x^t y^u)$ in (3.30) is $0 = n\alpha_1^{n-1} a_{tu}$. Since each of these factors is non-zero, we have a contradiction.

Similarly there can be no pair $(t, u) \neq (r, p_1 - r)$ such that $t+u \geqslant m$ and $a_{tu} \neq 0$. Hence substituting into (3.28) gives

$$h_1(x, y) = \alpha_1 x^r y^{p_1 - r} + \alpha_2 x^s y^{q-s} \tag{3.31}$$

and by the symmetry of $h_1$, we have $r = p_1 - r$ and $s = q - s$.

Clearly $m_1 \neq 0$ so that $p_1 \neq 0$ and thus $r \neq 0$. Hence (3.31) contradicts (3.27) and therefore the assumption leading to (3.28) is incorrect. Hence $q \geqslant m_2$ and $p_1 \leqslant m_2$. But $p_2 \geqslant q$ so that $p_2 = q = m_2$, which combined with (3.27) yields

$$h_1(x, y) = \alpha x^{m_2} + \sum_{i=1}^{m_2 - 1} a_{i, m_2 - i} x^i y^{m_2 - i} + \alpha y^{m_2}. \tag{3.32}$$

Assume that there exists an integer $i$ with $1 \leqslant i \leqslant m_2 - 1$ such that $a_{i, m_2 - i} \neq 0$. Let $j = \min\{i \mid a_{i, m_2 - i} \neq 0\}$. Substituting the expression for $h_1$ given by (3.32) into (3.29) it can be seen that if, on the right-hand side, $k \neq 0$ then the power of $x$ is greater than or equal to $m$. Thus the coefficient of $y^{m_2(n-1)} x^j y^{m-j}$ is $0 = n\alpha_1^{n-1} a_{j, m-j}$, a contradiction since each factor is non-zero. Hence $h_1 = \alpha(x^{m_2} + y^{m_2})$ and thus $f_1 = \alpha Q_{m_2}$. We clearly have $m_2 = m_1 = m$, so that

$$f = (\alpha Q_m, \beta y^m) \tag{3.33}$$

where $\alpha^{n-1} = \beta^{n-1} = 1$.

Using (3.29) and the fact that $(Q_m, y^m)$ commutes with $g$, we have

$$\alpha \sum e_k Q_m^{n-2k} (x^m y^m)^k = \sum e_k (\alpha Q_m)^{n-2k} (\beta x^m y^m)^k$$

and thus

$$\alpha \sum e_k Q_m^{n-2k} (x^m y^m)^k = \sum \alpha^{n-2k} \beta^k e_k Q_m^{n-2k} (x^m y^m)^k.$$

Since $e_1 = -n \neq 0$ we have $\alpha^{n-2} \beta = \alpha$. But also $\alpha^{n-1} = 1$ so that $\beta = \alpha^2$ which completes the proof.

**4.** In this section we determine all linear commuting polynomial vectors in two variables over $R = \mathrm{GF}(q)$ the finite field of order $q$. Suppose that

$$g = (g_1, g_2) \quad \text{where} \quad g_i = a_{i1} x_1 + a_{i2} x_2 + c_i \quad \text{for} \quad i = 1, 2$$

where we assume for simplicity, that each $a_{ij} \neq 0$. We wish to determine all

$$f = (f_1, f_2) \quad \text{where} \quad f_i = b_{i1} x_1 + b_{i2} x_2 + d_i \quad \text{for } i = 1, 2$$

such that

$$f\circ g = g\circ f.$$

To this end, let

$$D = (a_{11}-1)(a_{22}-1)-a_{12}a_{21}.$$

We now prove

THEOREM 4.1. (A) *If $D \neq 0$ then $f\circ g = g\circ f$ if and only if the $b_{ij}$ $(i, j = 1, 2)$ satisfy*

$$b_{11}+[(a_{22}-a_{11})/a_{21}]b_{21}-b_{22} = 0, \tag{4.1}$$

$$b_{12}-(a_{12}/a_{21})b_{21} = 0 \tag{4.2}$$

*and*

$$d_1 = [(a_{22}-1)x-a_{12}y]/D, \qquad d_2 = [(a_{11}-1)y-a_{21}x]/D$$

*where*

$$x = (b_{11}-1)c_1+b_{12}c_2 \quad \text{and} \quad y = b_{21}c_1+(b_{22}-1)c_2.$$

(B) *If $D = 0$ then $f\circ g = g\circ f$ if and only if the $b_{ij}$ $(i, j = 1, 2)$ satisfy* (4.1), (4.2), *the equation*

$$a_{21}x = (a_{11}-1)y \tag{4.3}$$

*and $d_1$ and $d_2$ satisfy*

$$(a_{11}-1)d_1+a_{12}d_2 = x. \tag{4.4}$$

Proof. The vector equation $f\circ g = g\circ f$ is equivalent to the following system of equations in the unknowns $b_{11}$, $b_{12}$, $b_{21}$, $b_{22}$, $d_1$, and $d_2$.

$$\begin{array}{rrrrrrl}
 & -a_{21}b_{12} & +a_{12}b_{21} & & & & = 0,\\
-a_{12}b_{11} & +(a_{11}-a_{22})b_{12} & & +a_{12}b_{22} & & & = 0,\\
-c_1b_{11} & -c_2b_{12} & & & +(a_{11}-1)d_1 & +a_{12}d_2 & = -c_1,\\
a_{21}b_{11} & & +(a_{22}-a_{11})b_{21} & -a_{21}b_{22} & & & = 0,\\
 & a_{21}b_{12} & -a_{12}b_{21} & & & & = 0,\\
 & & -c_1b_{21} & -c_2b_{22} & +a_{21}d_1 & +(a_{22}-1)d_2 & = -c_2.
\end{array}$$

The theorem follows upon row reduction of the above system.

We note that if $D \neq 0$ then there are $q^2$ such pairs $f = (f_1, f_2)$.

**5.** In this section we extend some results of Wells [17] and Mullen [14] concerning polynomials over finite fields which commute with linear permutations of the field. We restrict our attention to the case where $R$ is the finite field $GF(q)$ of order $q = p^n$ where $p$ is a prime and $n \geq 1$.

In [14] Mullen characterized and enumerated those polynomials over $GF(q)$ which commute with linear permutations, i.e., he characterized those



polynomials $f(x)$ over $GF(q)$ for which $f(bx+a) = bf(x)+a$. There are several ways to extend these ideas to commuting polynomials in several variables. The Lagrange Interpolation Formula for a finite field states that every function from $GF(q)$ into itself can be represented as a polynomial over $GF(q)$ of degree less than $q$. The above enumeration was obtained by using the Lagrange Interpolation Formula and the following combinatorial result. If $\theta$ is a permutation of a finite set $D$ where $\theta$ has type $(d_1, d_2, \ldots)$, then the number of functions $f\colon D\to D$ for which $f(\theta) = \theta(f)$ is given by

$$\prod_i \big(\sum_{j\mid i} jd_j\big)^{d_i}. \tag{5.1}$$

We first consider the case where the commutivity is coordinatewise. In particular, if $f_i\colon R\to R$ and $\theta_i(x) = b_ix+a_i$ for $i = 1, \ldots, m$, let $f = (f_1, \ldots, f_m)$ and $\theta = (\theta_1, \ldots, \theta_m)$. Then we say that $f$ commutes with $\theta$, written $f\theta = \theta f$, if $f_i\theta_i = \theta_i f_i$ for $i = 1, \ldots, m$. Suppose

$$f_i(x) = c_0^{(i)}+c_1^{(i)}x+ \ldots +c_{q-1}^{(i)}x^{q-1}$$

for $i = 1, \ldots, m$. Using an argument similar to that in [14], we may state

THEOREM 5.1. *The polynomial vector $f$ satisfies $f\theta = \theta f$ if and only if for $i = 1, \ldots, m$*

$$c_0^{(i)}(b_i-1) = -a_i+\sum_{t=1}^{q-1} c_t^{(i)}a_i^t,$$

$$c_s^{(i)}(1-b_i^{s-1}) = b_i^{s-1}\sum_{t=s+1}^{q-1}\binom{t}{s}c_t^{(i)}a_i^{t-s} \qquad (1 \leqslant s \leqslant q-1).$$

Suppose $b_i \neq 1$ for the subscripts $i_1, \ldots, i_e$ while for the remaining $m-e$ subscripts, $b_i = 1$. For $j = 1, \ldots, e$ let $k_{i_j}$ be the multiplicative order of $b_{i_j}$. Then using (5.1) we have

COROLLARY 5.2. *The number of polynomial vectors $f$ satisfying $f\theta = \theta f$ is given by*

$$q^{(m-e)q/p}\prod_{j=1}^{e} q^{(q-1)/k_{i_j}}. \tag{5.2}$$

It should be pointed out that (5.2) counts the number of polynomial vectors

$$f = (f_1, \ldots, f_m)\colon R^m \to R^m$$

where $f_i\colon R\to R$ and $f_i\theta_i = \theta_i f_i$ for $i = 1, \ldots, m$; not the total number of functions $g\colon R^m\to R^m$ such that $g\theta = \theta g$. To count this total number of functions $g$ one might proceed as follows.

Let $\theta$ be a linear permutation on $R^m$ defined by

$$\theta(x_1, \ldots, x_m) = b(x_1, \ldots, x_m)+(a_1, \ldots, a_m)$$

where $0 \neq b \in R$ has multiplicative order $k$. We note that this is a special case of the previous situation where $b = b_1 = \ldots = b_m$. We now count the total number of functions $g\colon R^m \to R^m$ such that $g\theta \doteq \theta g$. The cycles of $\theta$ consists of $m$-tuples and $\theta$ has type $(d_1, d_2, \ldots)$ given by

$$\begin{array}{llll} d_p = q^m/p & \text{and} \quad d_i = 0 \quad \text{for} \quad i \neq p & \text{if} & b = 1, \\ d_1 = 1 & \text{and} \quad d_k = (q^m-1)/k & \text{if} & b \neq 1. \end{array}$$

Thus using (5.1) again we may prove

THEOREM 5.3. *The number of functions* $g\colon R^m \to R^m$ *such that* $g\theta = \theta g$ *is given by*

$$\begin{array}{ll} q^{mq^m/p} & \textit{if} \quad b = 1, \\ q^{m(q^m-1)/k} & \textit{if} \quad b \neq 1. \end{array}$$

We note that if $m = 1$ the results of this section reduce to those of Mullen [14].

**Acknowledgement.** The first author acknowledges the assistance of K. B. Dunn in the preparation of parts of this paper.

**References**

[1] E. A. Bertram, *Polynomials which commute with a Tschebyscheff polynomial*, Amer. Math. Monthly 68 (1971), pp. 650–653.
[2] H. D. Block and H. P. Thielman, *Commuting polynomials*, Quart. J. Math., Oxford Series, 2 (1951), pp. 241–243.
[3] W. M. Boyce, *On polynomials which commute with a given polynomial*, Proc. Amer. Math. Soc. 33 (1972), pp. 229–234.
[4] K. B. Dunn and R. Lidl, *Multi-dimensional Chebyshev polynomials, I, II*, Proc. Japan Acad., Series A, 56 (1980), pp. 154–159, and 160–165.
[5] — — *Generalizations of the classical Chebyshev polynomials to polynomials in two variables*, Czechoslovak Math. J. 32 (1982), pp. 516–528.
[6] R. Eier and R. Lidl, *Tschebyscheffpolynome in einer und zwei Variablen*, Abh. Math. Sem. Univ. Hamburg 41 (1974), pp. 17–27.
[7] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. 63 (1941), pp. 249–255.
[8] E. J. Jacobsthal, *Über vertauschbare Polynome*, Math. Zeitschr. 63 (1955), pp. 243–276.
[9] H. Kautschitsch, *Kommutative Teilhalbgruppen der Kompositions-halbgruppe von Polynomen und formalen Potenzreihen*, Monats. Math. 74 (1970), pp. 421–436.
[10] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North Holland, Amsterdam 1973.
[11] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. 64 (1942), pp. 389–400.
[12] R. Lidl, *Tschebyscheffpolynome in mehreren Variablen*, J. Reine Angew. Math. 273 (1975), pp. 178–198.
[13] R. Lidl and C. Wells, *Chebyshev polynomials in several variables*, ibid. 255 (1972), pp. 104–111.
[14] G. L. Mullen, *Polynomials over finite fields which commute with linear permutations*, Proc. Amer. Math. Soc. 84 (1982), pp. 315–317.



[15] J. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. 25 (1923), pp. 399–448.
[16] T. J. Rivlin, *The Chebyshev Polynomials*, J. Wiley, New York 1974.
[17] C. Wells, *Polynomials over finite fields which commute with translation*, Proc. Amer. Math. Soc. 46 (1974), pp. 347–350.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TASMANIA
(7001) HOBART
AUSTRALIA

DEPARTMENT OF MATHEMATICS
230 McALLISTER BUILDING
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802
U.S.A.

*Received on 13. 8. 1984* (1444)