[28] Joseph B. Muskat, *On simultaneous representations of primes by binary quadratic forms*, Preprint.

[29] Joseph B. Muskat and Albert L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), pp. 185–216.

[30] Trygve Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York 1964.

[31] Bernard Oriat, *Groupe des classes des corps quadratiques imaginaires* $Q(\sqrt{-a})$, $a < 10000$, Faculté des Sciences de Besançon, France.

[32] Kenneth S. Williams, *Note on a result of Barrucand and Cohn*, J. Reine Angew. Math. 285 (1976), pp. 218–220.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, South Carolina, U.S.A.
29208

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada
K1S 5B6

Received on 18. 4. 1980
and in revised form on 2. 1. 1981 (1205)

ACTA ARITHMETICA
XLI (1982)

Some generalisations of Chebyshev polynomials and their induced group structure over a finite field

by

REX MATTHEWS (Hobart)

1. Introduction. If u, b are rational integers then the polynomial $f(z) = z^2 - uz + b$ has roots σ_1, σ_2 in the complex field, such that $u = \sigma_1 + \sigma_2$ and $b = \sigma_1\sigma_2$. The polynomial $g_k(u; b)$ may be defined by requiring $f_k(z) = z^2 - g_k(u; b)z + b^k$ to have roots σ_1^k, σ_2^k. Thus $g_k(u; b) = \sigma_1^k + \sigma_2^k = \sigma_1^k + b^k\sigma_1^{-k}$ and $b^k = \sigma_1^k\sigma_2^k$ and Waring's formula (see Lausch–Nöbauer [7], p. 297) allows the expression of $g_k(u; b)$ as a polynomial in u and b. These polynomials $g_k(u; b)$ are known as Dickson polynomials ([7], p. 209), the case $b = 1$ being the classical Chebyshev polynomials of the first kind. When these polynomials are considered as being defined over a finite field $\boldsymbol{F}_q$ (i.e. the coefficients are reduced modulo the field characteristic) it eventuates that some of them are so called *permutation polynomials*, i.e. the mapping of the field into itself induced by these polynomials is a permutation. The necessary and sufficient condition for $g_k(u; b)$ to be a permutation polynomial is that $(k, q^2-1) = 1$ where q is the order of the field (see [7], p. 209). Nöbauer [14] showed that the set $\{g_k(u; b), b \text{ fixed}\}$ is closed under composition of polynomials if and only if $b = 0$, 1, or -1, and determined the structure of the groups of permutations induced by polynomials of this type in these cases.

Lidl [10] extended this definition to an n-variable form of the Chebyshev polynomials and their algebraic properties were considered by Lidl and Wells [11]. In this formulation the quadratic $f(z)$ is replaced by a polynomial

$$r(u_1, \ldots, u_n, z) = z^{n+1} - u_1 z^n + \ldots + (-1)^n u_n z + (-1)^{n+1} b$$
$$= (z - \sigma_1) \ldots (z - \sigma_{n+1}),$$

where $u_i \in \boldsymbol{Z}$, $\sigma_i \in \boldsymbol{C}$. When taken over $\boldsymbol{F}_q$, r has $n+1$ not necessarily distinct roots in $\boldsymbol{F}_{q^{(n+1)!}}$.

If k is a positive integer, set

$$r^{(k)}(u_1, \ldots, u_n, z) = (z - \sigma_1^k) \ldots (z - \sigma_{n+1}^k).$$

The coefficients $g_i^{(k)}(u_1, \ldots, u_n)$ of $r^{(k)}$ are elementary symmetric functions of $(\sigma_1^k, \ldots, \sigma_{n+1}^k)$, and so are symmetric functions of $(\sigma_1, \ldots, \sigma_{n+1})$. Thus the coefficients of $r^{(k)}$ are all polynomials in $(u_1, \ldots, u_n)$ by the fundamental theorem on symmetric functions. In this way we obtain a polynomial vector $g(n, k, b) = \big(g_1^{(k)}(u_1, \ldots, u_n, b), \ldots, g_n^{(k)}(u_1, \ldots, u_n, b)\big)$. The explicit forms, recurrence relations, and generating functions of these polynomials are contained in [10]. Here we deal only with their algebraic properties. When considered as a polynomial vector over $\boldsymbol{F}_q$, $g(n, k, b)$ induces a permutation of $(\boldsymbol{F}_q)^n$ if and only if $(k, q^s-1) = 1$, $s = 1, \ldots, n+1$, for $b \neq 0$, $s = 1, \ldots, n$ for $b = 0$ (see [11], p. 106).

In the two variable case the corresponding group of permutations has been determined by Lidl ([8] and [9]). In this paper we begin by considering a more general construction. We take

$$r(u_1, \ldots, u_n, z) = z^n - u_1 z^{n-1} + \ldots + (-1)^n u_n = (z-\sigma_1) \ldots (z-\sigma_n).$$

If $f(z)$ is a fixed polynomial, define

$$r^{(f)}(u_1, \ldots, u_n, z) = \big(z-f(\sigma_1)\big) \ldots \big(z-f(\sigma_n)\big)$$
$$= z^n - g_1^{(f)}(u_1, \ldots, u_n) z^{n-1} + \ldots + (-1)^n g_n^{(f)}(u_1, \ldots, u_n).$$

Then, as before, each $g_n^{(f)}$ may be written as a polynomial in $u_1, \ldots, u_n$. When $f(z) = z^k$, this essentially corresponds to $g(n, k, 0)$ as given above. In the first section of this paper we examine the properties of the polynomials defined in this way. Then we consider the groups of permutations induced by Chebyshev polynomials in n variables over $\boldsymbol{F}_q$ and determine which of these groups are cyclic. (This generalises the results in [9], [10] and [12] to the n-dimensional case.) The general results are then applied to obtain a result of Brawley, Carlitz and Levine [2] on polynomials which permute the set of $n \times n$ matrices over $\boldsymbol{F}_q$.

2. The general construction. The construction outlined in the introduction defines a polynomial vector $(g_1^{(f)}, \ldots, g_n^{(f)})$ which induces a map $\boldsymbol{F}_q^n \to \boldsymbol{F}_q^n$. It is more convenient to consider this process as an operation on the set of monic polynomials of degree n over $\boldsymbol{F}_q$, denoted by $P(q, n)$. Thus if $f \in \boldsymbol{F}_q[x]$ is a fixed polynomial over $\boldsymbol{F}_q$, define the operator $\Delta_f : P(q, n) \to P(q, n)$ as follows: If $R(x) \in P(q, n)$ and $h(x) = \prod_{i=1}^{n} (x-\alpha_i)$, $\alpha_i \in \boldsymbol{F}_{q^n}$, is the factorization of $h(x)$ into linear factors in a suitable extension field of $\boldsymbol{F}_q$ then $\Delta_f h(x) = \prod \big(x-f(\alpha_i)\big)$.

Clearly the map induced by $(g_1^{(f)}, \ldots, g_n^{(f)})$ on $\boldsymbol{F}_q^n$ is a permutation if and only if Δ_f induces a permutation on $P(q, n)$. The following properties follow immediately from the definition:

LEMMA 1. $\Delta_f(hg) = \Delta_f h \Delta_f g$.

LEMMA 2. $\Delta_{f \circ g} h = \Delta_f(\Delta_g h)$.

We will need the following three elementary lemmas. For each divisor d of n, put

$$K_d = \{a \in \boldsymbol{F}_{q^n} \mid \deg a = d \text{ over } \boldsymbol{F}_q\}.$$

LEMMA 3. *$f(x) \in \boldsymbol{F}_q[x]$ is a permutation polynomial over $\boldsymbol{F}_{q^n}$, $n \in \boldsymbol{Z}$, if and only if $f(x)$ induces a permutation of K_d, for each $d \mid n$.*

Proof. Let $f(x)$ permute $\boldsymbol{F}_{q^n}$. Then $f(x)$ permutes $\boldsymbol{F}_q = K_1$. Let r be the smallest integer such that $f(x)$ does not permute K_r, $r \mid n$. If $\alpha \in K_r$, suppose that $f(\alpha) \notin K_r$. Then $f(\alpha) \in K_{r'}$ for some $r' \mid r$, $r' \neq r$. Since $f(x)$ permutes $K_{r'}$ there exists $\beta \in K_{r'}$ with $f(\alpha) = f(\beta)$. But $K_r \cap K_{r'} = \emptyset$, so $\alpha \neq \beta$. The reverse implication is trivial, as $\boldsymbol{F}_{q^n}$ is the disjoint union of the K_d, $d \mid n$.

LEMMA 4. *If $f(x) \in \boldsymbol{F}_q[x]$ and $f(a) = f(b)$ implies that a, b are conjugate over $\boldsymbol{F}_q$ when $a, b \in \boldsymbol{F}_{q^n}$, then $f(x)$ induces a permutation of K_r, for $r \mid n$.*

Proof. By induction on r.

If $r = 1$, let $f(a) = f(b)$, $a, b \in \boldsymbol{F}_q$. a, b conjugate implies a equals b. Hence $f(x)$ induces a permutation of $\boldsymbol{F}_q = K_1$. Now assume the proposition true for $r < k$. If $f(a) \in K_r$, $r < k$, where $a \in K_k$, then since $f(x)$ induces a permutation of K_r, there exists $b \in K_r$, with $f(a) = f(b)$. Thus a and b are conjugate over $\boldsymbol{F}_q$. But all the conjugates of a lie in K_k and $K_k \cap K_r = \emptyset$. Thus $f(a) \in K_k$. If $f(a) = f(b)$ with $a \neq b$, $a, b \in K_k$, then a, b conjugate implies $f(a) = f(a^{q^l}) = [f(a)]^{q^l}$, $l < k$. Thus $f(a) \in \boldsymbol{F}_{q^l}$ and so $f(a) \in K_{l'}$, $l' < k$, and we have already shown that $f(a) \in K_k$, a contradiction.

LEMMA 5. *Let $f(x) \in \boldsymbol{F}_q[x]$. The following conditions are equivalent,*

(i) *$f(a) = f(b)$, $a, b \in \boldsymbol{F}_{q^n}$, implies a, b are conjugate over $\boldsymbol{F}_q$.*

(ii) *If $a, b \in \boldsymbol{F}_{q^n}$, and $f(a)$, $f(b)$ are conjugate over $\boldsymbol{F}_q$, then a, b are conjugate over $\boldsymbol{F}_q$.*

(iii) *$f(x)$ is a permutation polynomial over $\boldsymbol{F}_{q^n}$.*

Proof. (ii) $\Rightarrow$ (i) trivial.

(iii) $\Rightarrow$ (i) trivial.

(i) $\Rightarrow$ (ii). Let $f(a)$, $f(b)$ be conjugate over $\boldsymbol{F}_q$. Then $f(b) = [f(a)]^{q^k} = f(a^{q^k})$, $k < n$. Thus b and a^{q^k} are conjugate over $\boldsymbol{F}_q$ and so a and b are conjugate over $\boldsymbol{F}_q$.

(i) $\Rightarrow$ (iii) by Lemmas 3 and 4.

We are now in a position to prove our main result.

THEOREM 1. *Δ_f induces a permutation of $P(q, n)$ if and only if $f(x)$ is a permutation polynomial over $\boldsymbol{F}_{q^r}$, for each $r \leqslant n$.*

Proof. (i) Sufficiency. We note that if $h(x)$ is irreducible of degree $r \leqslant n$ then $\Delta_f h$ is irreducible, for if $h = \prod_0^{r-1} (x-\sigma^{q^j})$, $\sigma \in \boldsymbol{F}_{q^r}$, then $\Delta_f h$

has as roots the conjugates over $\boldsymbol{F}_q$ of $f(\sigma)$, and these are all distinct since f is a permutation polynomial over $\boldsymbol{F}_{q^r}$.

If $h = \prod h_i$, $g = \prod g_j$ are the factorizations of h and g into products of irreducibles over $\boldsymbol{F}_q$, and if $\Delta_f h = \Delta_f g$, then $\prod \Delta_f h_i$, $\prod \Delta_f g_j$ are factorizations of $\Delta_f h$ into a product of irreducibles over $\boldsymbol{F}_q$, and so for each i there is a j with $\Delta_f h_i = \Delta_f g_j$, degree h_i = degree $g_j = r$. If h_i has roots σ^{q^s}, and g_j has roots τ^{q^t}, then $f(\sigma) = f(\tau^{q^k})$, for some $k < n$. Since $f(x)$ is a permutation polynomial over $\boldsymbol{F}_{q^r}$, $\sigma = \tau^{q^k}$. Thus the conjugates of σ and τ coincide and $f_i = g_j$. Hence $h = g$.

(ii) Necessity. If $f(x)$ is not a permutation polynomial over $\boldsymbol{F}_{q^r}$, then by Lemma 5 there exist non-conjugate $\sigma, \tau \in \boldsymbol{F}_{q^r}$ with $f(\sigma) = f(\tau)$. The field polynomials of σ and τ, h_1, h_2 respectively, are distinct of degree r, but $\Delta_f h_1 = \Delta_f h_2$. Let $g_1(x) = x^{n-r} h_1$, $g_2(x) = x^{n-r} h_2$. Then $g_1(x) \neq g_2(x)$ but $\Delta_f g_1 = \Delta_f g_2$, and degree g_1 = degree $g_2 = n$.

LEMMA 6. *Let* $\lambda(x) = \mathrm{LCM}(x^q - x, \ldots, x^{q^n} - x)$. *If* $f(x) \equiv r(x) \bmod \lambda(x)$ *then* $\Delta_f h = \Delta_r h$, *for all* $h(x) \in P(q, t)$, $t \leqslant n$.

Proof. If $f(x) \equiv r(x) \bmod \lambda(x)$ then $f(x) \equiv r(x) \bmod (x^{q^k} - x)$, for $k \leqslant n$. Any root σ of $h(x)$ lies in $\boldsymbol{F}_{q^k}$ for some $k \leqslant n$, and so $f(\sigma) = r(\sigma)$. Thus $\Delta_f h = \Delta_r h$.

LEMMA 7. *The set* G_n *of polynomials* $f(x) \in \boldsymbol{F}_q[x]$ *such that*

(i) degree $f(x) <$ degree $\lambda(x)$,

(ii) $f(x)$ *induces a permutation of* $\boldsymbol{F}_{q^k}$, *for each* $k \leqslant n$, *forms a group under composition* mod $\lambda(x)$.

Proof. If $f(x) * r(x)$ is defined to be $(f \circ r)(x) = f\big(r(x)\big) \bmod \lambda(x)$ then $f \circ r - f * r = t\lambda$, for some $t \in \boldsymbol{F}_q[x]$. Since $\lambda(\sigma) = 0$ if $\sigma \in \boldsymbol{F}_{q^k}$, $(f \circ r)(\sigma) = (f * r)\sigma$. But $f \circ r$ induces a permutation of $\boldsymbol{F}_{q^k}$, and thus so does $f * r$. The identity of G_n is x and inverses exist since that system is finite and cancellative.

We now proceed to determine the group P_n of permutations of $P(q, n)$ induced by this process. By Lemma 6 it is sufficient to consider the action of Δ_f for $f \in G_n$.

The structure of G_n was determined by Carlitz and Hayes [3]. We now investigate the structure of P_n.

LEMMA 8. *The map* $\theta\colon f \to \Delta_f$ *is a homomorphism from* G_n *onto* P_n.

Proof. By Lemmas 2 and 7 and Theorem 1.

LEMMA 9. $\mathrm{Ker}\,\theta = \{f \in G_n\colon f(\sigma)$ *is a conjugate of* σ, *for all* $\sigma \in \boldsymbol{F}_{q^k}$, $k \leqslant n\}$.

Proof. If $\theta(f)$ induces the identity map on $P(q, n)$ then $\Delta_f h = h$, for all h of degree $\leqslant n$. Let $\sigma \in \boldsymbol{F}_{q^k}$, and h be the minimal polynomial of σ. Then $\Delta_f h = h \Rightarrow f(\sigma)$ is a conjugate of σ. Conversely, if $h \in P(q, n)$, then $h = \prod h_i$, where the h_i are irreducible over $\boldsymbol{F}_q$. h_i has roots $\sigma, \ldots, \sigma^{q^{k-1}}$,

$k = \deg h_i$, and so $f(\sigma)$ is a conjugate of σ. Since $f(\sigma^{q^l}) = [f(\sigma)]^{q^l}$, $f(\sigma^{q^l})$ runs through the set $\{\sigma^{q^m}\}$. Hence $\Delta_f h_i = h_i$, and $\Delta_f h = h$.

We denote by A_d the group of permutations of K_d which induce permutations on the set of equivalence classes of conjugate elements.

LEMMA 10. *If* $f \in G_n$, *then* f *induces a permutation of* K_d, *for each* $d \leqslant n$. *Denote this permutation by* p_d. *Define* $\psi\colon G_n \to A_1 \times A_2 \times \ldots \times A_n$ *by*

$$\psi\colon p \to (p_1, \ldots, p_n).$$

Then ψ *is a group isomorphism.*

Proof. To show that ψ is surjective, let $\pi_1, \ldots, \pi_n$ be arbitrary elements of $A_1, \ldots, A_n$. Consider $\boldsymbol{F}_{q^{n!}}$. Choose on each K_d, $n < d \leqslant n!$, any permutation π_d of K_d which induces a permutation on the conjugacy classes in K_d. Now consider the map π which is π_i on each K_i, $1 \leqslant i \leqslant n!$. Since π commutes with the Frobenius automorphism of $\boldsymbol{F}_{q^{n!}}$, there is a polynomial $f(x)$ of degree less than $q^{n!}$ with coefficients in $\boldsymbol{F}_q$ which induces π on $\boldsymbol{F}_{q^{n!}}$. The reduction of $f(x) \bmod \lambda(x)$ induces π_i on each A_i, since each $\boldsymbol{F}_{q^i}$ is a subfield of $\boldsymbol{F}_{q^{n!}}$, and so $f(x) \in G_n$. If $f \in \mathrm{Ker}\,\psi$, then $f(x)$ induces the identity on K_d for all $d \leqslant n$. Hence $f(x) \equiv x \bmod (x^{q^d} - x)$ for all $d \leqslant n$, and so $f(x) \equiv x \bmod \lambda(x)$. The other properties of ψ are obvious.

Each $\pi \in A_i$ induces a permutation of the set of conjugacy classes of K_d. If there are $\pi(d)$ classes in K_d then this gives rise to a homomorphism from A_d to $S_{\pi(d)}$, the symmetric group on $\pi(d)$ elements. Thus there is a homomorphism $\varphi\colon A_1 \times \ldots \times A_n \to S_{\pi(1)} \times \ldots \times S_{\pi(n)}$. Define $\mu = \varphi \circ \psi\colon G_n \to S_{\pi(1)} \times \ldots \times S_{\pi(n)}$.

LEMMA 11. $\mathrm{Ker}\,\mu = \mathrm{Ker}\,\theta$.

Proof. If $f \in \mathrm{Ker}\,\mu$, then f induces the identity map on the set of conjugacy classes of K_d, $d \leqslant n$. This means that $f(\sigma)$ is a conjugate of σ, for all $\sigma \in \boldsymbol{F}_{q^k}$, $k \leqslant n$. Thus $f \in \mathrm{Ker}\,\theta$. Conversely, if $f \in \mathrm{Ker}\,\theta$, then $\psi(f)$ induces the identity on the set of conjugacy classes and so $f \in \mathrm{Ker}\,\mu$.

THEOREM 2. *The group* P_n *of maps of* $P(q, n) \to P(q, n)$ *induced by elements of* G_n *is isomorphic to the product of* n *symmetric groups of orders* $\pi(k)$, $k \leqslant n$, *where*

$$\pi(k) = k^{-1} \sum_{d \mid k} \mu\left(\frac{k}{d}\right) q^d, \quad \textit{where } \mu \textit{ is the Möbius } \mu\textit{-function}.$$

Proof. From Lemmas 8 and 11. The number of conjugacy classes in K_k is the number of monic irreducible polynomials of degree k in $\boldsymbol{F}_q[x]$, given by $\pi(k)$ above (see Blake and Mullin [1], p. 33, for this formula).

3. Chebyshev polynomials in several variables. As stated in Section 1, *the Chebyshev polynomial vector* $g(n, k, b)$ *is a permutation polynomial*

vector if and only if $(k, q^r-1) = 1$, $1 \leqslant r \leqslant n$, *for* $b = 0$, *and* $(k, q^r-1) = 1$, $1 \leqslant r \leqslant n+1$, *for* $b \neq 0$. The case $b = 0$ in fact follows directly from Theorem 1, as the polynomial x^k is a permutation polynomial over $\boldsymbol{F}_q$ if and only if $(k, q-1) = 1$. It was shown by Lidl and Wells [11] that the set $\{g(n, k, b)\}$, for b fixed, is closed under composition if and only if $b = 0, 1$, or -1, and for $n = 2$ the structure of the group of permutations induced by the $g(n, k, b)$ was determined in [8] and [9]. We now extend this to arbitrary n. The case $b = 0$ is treated first, then $b = 1$ and -1 are dealt with together.

The case $b = 0$.

THEOREM 3. *The group* G *of mappings of* $\boldsymbol{F}_q^n \to \boldsymbol{F}_q^n$ *induced by the permutation polynomial vectors among the vectors* $g(n, k, 0)$, *is isomorphic to the group* R *of reduced residues* $\bmod N = \mathrm{LCM}(q-1, \ldots, q^n-1)$ *factored by the cyclic subgroup* C *of order* $\mathrm{LCM}(1, \ldots, n)$, *generated by* q.

Proof. If $k \equiv k' \bmod N$, then $k \equiv k' \bmod (q^r-1)$, $1 \leqslant r \leqslant n$, and so the maps $f_k\colon x \to x^k$, $f_{k'}\colon x \to x^{k'}$ coincide on $\boldsymbol{F}_{q^r}$, $1 \leqslant r \leqslant n$, and so the maps Δ_{f_k}, $\Delta_{f_{k'}}$ are identical on $P(q, n)$. Thus the map $g_k \to k'$, where k' is the residue of $k \bmod N$, is a homomorphism of the semigroup of permutation vectors amongst the $g(n, k, 0)$ onto R. The map φ which sends k to the map which $g(n, k, 0)$ induces on $\boldsymbol{F}_q^n$ is then a homomorphism of R onto G. It remains to determine the kernel of this homomorphism. Suppose $k \equiv q^t \bmod N$.

If $f(x) = \prod f_i(x)$ is the decomposition of $f(x)$ into irreducible factors over $\boldsymbol{F}_q$, and $f_i(x) = \prod_{r=0}^{n-1} (x - \sigma^{q^r})$ is the factorization of f_i (where f_i has degree n), over its splitting field, then

$$\Delta_{x^k} f_i(x) = \prod_{r=0}^{n-1} (x - \sigma^{q^{r+\tau}}) = f_i(x).$$

Thus $\Delta_{x^k} f = f$.

Now suppose $k \in \mathrm{Ker}\varphi$. Then σ^k is a conjugate of σ for all $\sigma \in \boldsymbol{F}_{q^r}$, $1 \leqslant r \leqslant n$, by Lemma 9. If σ is a primitive element of $\boldsymbol{F}_{q^r}$, then $\sigma^k = \sigma^{q^l}$, since $0 \leqslant l \leqslant r$.

Thus $k \equiv q^l \bmod (q^r-1)$ and k is a solution of the system of congruences

$$\begin{aligned} &k \equiv 1 \bmod (q-1),\\ &k \equiv 1, q \bmod (q^2-1),\\ &\ldots\ldots\ldots\ldots\ldots\\ &k \equiv 1, q, \ldots, q^{n-2} \bmod (q^{n-1}-1),\\ &k \equiv 1, q, \ldots, q^{n-1} \bmod (q^n-1). \end{aligned} \tag{1}$$

We now show that this system is equivalent to the single congruence

$$k \equiv 1, q, \ldots, q^t \bmod N, \quad \text{where} \quad t = \mathrm{LCM}(1, \ldots, n). \tag{2}$$

Firstly it is clear that any solution to (2) is also a solution to (1). We now wish to determine the order m of $q \bmod N$. If $s = \mathrm{LCM}(1, \ldots, n)$, then $q^s \equiv 1 \bmod N$, since $(q^t-1) \mid (q^s-1)$ for all t with $1 \leqslant t \leqslant n$. Thus $m \mid s$. Since $q^m \equiv 1 \bmod N$, $N \mid (q^m-1)$, and so $(q^t-1) \mid (q^m-1)$, $1 \leqslant t \leqslant n$. This holds only if $t \mid m$. Thus $s \mid m$, and so $s = m$, implying that the number of solutions of (2) is $s = \mathrm{LCM}(1, \ldots, n)$. We next show that the number of solutions of (1) is also s, thus proving that every solution of (1) is a solution of (2). We do this by induction on n. When $n = 1$ there is nothing to prove, as $N = q-1$. By the induction hypothesis, the number of solutions of the first $(n-1)$ congruences is $\mathrm{LCM}(1, \ldots, n-1)$, and by the earlier arguments this system is equivalent to $k \equiv 1, q, \ldots, q^{\mathrm{LCM}(1, \ldots, n-1)} \bmod \mathrm{LCM}(q-1, \ldots, q^{n-1}-1)$. Let $N' = \mathrm{LCM}(q-1, \ldots, q^{n-1}-1)$. Suppose $k \equiv q^t \bmod N'$, $k \equiv q^s \bmod (q^n-1)$. Then $k = q^t + aN' \equiv q^s \bmod (q^n-1)$, for some $a \in \boldsymbol{Z}$. $aN' = q^t(q^{s-t}-1) \bmod (q^n-1)$, where $(s-t)$ is taken mod n. This has a solution if and only if $\gcd(N', q^n-1) \mid q^t(q^{s-t}-1)$. Now suppose that n is not of the form p^α, p a prime. Then

$$n = \prod_{i=1}^{m} p_i^{\alpha_i}, \quad m \geqslant 2, \quad \text{and} \quad p_i^{\alpha_i} < n.$$

Thus

$$k \equiv q^t \bmod N' \Rightarrow k \equiv q^t \bmod (q^{p_i^{\alpha_i}}-1)$$

and so

$$(q^{p_i^{\alpha_i}}-1) \mid (q^{s-t}-1) \quad \text{for each } p_i^{\alpha_i}.$$

Thus $s \equiv t \bmod p_i^{\alpha_i}$, and so $s \equiv t \bmod n$. Hence the choice of s is already determined and so the number of solutions remains the same, namely $\mathrm{LCM}(1, \ldots, n-1) = \mathrm{LCM}(1, \ldots, n)$. If $n = p$, then the condition for a solution is $(q-1) \mid (q^{s-t}-1)$, which always holds, and so s is arbitrary, and for each choice of s there is a unique solution $\bmod \mathrm{LCM}(N', q^n-1) = N$. Thus the number of solutions is $n\,\mathrm{LCM}(1, \ldots, n-1) = \mathrm{LCM}(1, \ldots, n)$. Now suppose $n = p^\alpha$, $\alpha > 1$. The condition reduces to $s \equiv t \bmod p^{\alpha-1}$, which has p solutions modulo p^α, each giving a unique solution $\bmod N$. Thus the number of solutions is $p\,\mathrm{LCM}(1, \ldots, n-1) = \mathrm{LCM}(1, \ldots, n)$.

The cases $b = 1$ or -1. In this section, let $f(x) = x^k$, with $b = 1$ for characteristic 2, otherwise k odd, $b = \pm 1$. We use the notation of Sections 1 and 2.

LEMMA 12. *If* Δ_f *induces the identity map on the set* P_b^n *of polynomials of degree* n *with constant term* $(-1)^n b$, *then* f *induces the identity map on* $\boldsymbol{F}_q$, *and* Δ_f *induces the identity map on all polynomials of degree less than* n, *for* $n > 2$.

Proof. Let ω be a primitive element of $\boldsymbol{F}_q$ and let

$$h(x) = (x-1)^{n-3}(x-\omega)^2(x-\omega^{-2}), \quad b = 1;$$
$$h(x) = (x-1)^{n-3}(x-\omega)^2(x+\omega^{-2}), \quad b = -1.$$

Then

$$\Delta_f h = (x-1)^{n-3}(x-\omega^k)^2(x-\omega^{-2k}), \quad b = 1;$$
$$\Delta_f h = (x-1)^{n-3}(x-\omega^k)^2(x+\omega^{-2k}), \quad b = -1,$$

since k is assumed to be odd. If the characteristic is 2, consider only the case $b = 1$.

In each case, $h \in P_b^n$, and so $\Delta_f h = h$ by hypothesis. Thus $\omega = \omega^k$, by unique factorization, and ω primitive implies $k \equiv 1\,(q-1)$. Hence $f(x)$ induces the identity map on $\boldsymbol{F}_q$. (Note that if $n = 2$, $\omega = \omega^{-k}$ is also possible, and we can only deduce $k \equiv \pm 1\,(q-1)$.) Now let $g(x) \in \boldsymbol{F}_q[x]$, with degree $g(x) = m < n$. Let $g(x)$ have constant term β. Clearly we may assume $\beta \neq 0$. Define

$$h(x) = \left(x - \frac{(-1)^m b}{\beta}\right)(x-1)^{n-m-1} g(x).$$

$h(x)$ has degree n, and has constant term $(-1)^n b$, and so $\Delta_f h = h$. But

$$\Delta_f h = \left(x - \frac{(-1)^m b}{\beta}\right)(x-1)^{n-m-1} \Delta_f g,$$

since $\beta \in \boldsymbol{F}_q$, and $\beta^k = \beta$. Thus $\Delta_f g = g$.

Lemma 13. *Let ω be a primitive element of $\boldsymbol{F}_{q^n}$, and put $\lambda = \omega^{q-1}$, q even or odd, $\mu = \omega^{\frac{1}{2}(q-1)}$, q odd. Then $\lambda, \mu \in K_n$.*

Proof. λ has order $(q^n-1)/(q-1)$. If $\lambda \in \boldsymbol{F}_{q^r}$, $r < n$, then $\operatorname{ord}\lambda \leqslant q^r - 1$. But $(q^n-1)/(q-1) > q^r - 1$, $r < n$, and so $\lambda \in K_n$. If $\mu \in \boldsymbol{F}_{q^r}$, $r < n$, then $\lambda = \mu^2 \in \boldsymbol{F}_{q^r}$. Since $K_n \cap \boldsymbol{F}_{q^r} = \emptyset$, this is impossible.

Theorem 4. *Δ_f induces the identity map on P_b^{n+1}, $b = \pm 1$ if and only if k satisfies the system*

$$\begin{aligned}
&k \equiv 1 \bmod (q-1),\\
&\cdots\cdots\cdots\cdots\cdots\\
&k \equiv 1, q, \ldots, q^{n-1} \bmod (q^n-1),\\
&k \equiv 1, q, \ldots, q^n \bmod \frac{q^{n+1}-1}{q-1} \quad \textit{in case } b = 1,\\
\textit{or}\quad &k \equiv 1, q, \ldots, q^n \bmod 2\left(\frac{q^{n+1}-1}{q-1}\right) \quad \textit{in case } b = -1.
\end{aligned} \tag{3}$$

Proof. Assume firstly that k satisfies the system. Then if $g(x)$ is irreducible over $\boldsymbol{F}_q$, and degree $g(x) \leqslant n$, $\Delta_f g = g$. If g is irreducible

of degree $(n+1)$ and has constant term $(-1)^{n+1}b$, then

$$g(x) = (x-\sigma)\ldots(x-\sigma^{q^n}), \quad \sigma \in \boldsymbol{F}_{q^{n+1}}$$

where

$$(-1)^{n+1}\sigma^{1+q+\ldots+q^n} = (-1)^{n+1}b, \quad \text{or} \quad \sigma^{(q^{n+1}-1)/(q-1)} = b.$$

In the case $b = 1$, this implies that

$$\sigma^k = \sigma^{q^t} \quad \text{for some } 1 \leqslant t \leqslant n,$$

and so

$$\Delta_f g = g.$$

If $b = -1$, then $\sigma^{(q^{n+1}-1)/(q-1)} = -1$, and $\sigma^{2(q^{n+1}-1)/(q-1)} = 1$, and (3) again gives $\Delta_f g = g$.

Conversely, if $\Delta_f g = g$ for all $g \in P_b^{n+1}$, then by Lemma 12, Δ_f induces the identity map on all polynomials of degree $\leqslant n$. Hence k satisfies the first n equations of the system, as in the case $b = 0$.

Now let ω be a primitive element of $\boldsymbol{F}_{q^{n+1}}$, and take $\lambda = \omega^{q-1}$, $\mu = \omega^{\frac{1}{2}(q-1)}$ for q odd. If q is even consider just the first case, since $1 = -1$. By Lemma 13, $\lambda, \mu \in K_n$, and so their minimal polynomials h, g respectively, have degree $(n+1)$.

The constant terms of h, g are

$$\lambda^{(q^{n+1}-1)/(q-1)} \quad \text{and} \quad \mu^{(q^{n+1}-1)/(q-1)},$$

which equal 1 and -1, respectively.

In the case $b = 1$, it follows that $\Delta_f h = h$ and so

$$\lambda^k = \lambda^{q^t}, \quad 0 \leqslant t \leqslant n.$$
$$\Rightarrow \omega^{(q-1)k} = \omega^{(q-1)q^t}$$
$$\Rightarrow (q-1)k \equiv (q-1)q^t \bmod (q^{n+1}-1)$$
$$\Rightarrow k \equiv q^t \bmod \left(\frac{q^{n+1}-1}{q-1}\right).$$

In the case $b = -1$, $\Delta_f g = g$ implies

$$\mu^k = \mu^{q^t}, \quad 0 \leqslant t \leqslant n.$$
$$\Rightarrow \omega^{\frac{1}{2}(q-1)k} = \omega^{\frac{1}{2}(q-1)q^t}$$
$$\Rightarrow \tfrac{1}{2}(q-1)k \equiv \tfrac{1}{2}(q-1)q^t \bmod (q^{n+1}-1)$$
$$\Rightarrow k \equiv q^t \bmod 2(q^{n+1}-1)/(q-1).$$

Corollary. *The group G of mappings $\boldsymbol{F}_q^n \to \boldsymbol{F}_q^n$ induced by permutation polynomial vectors $g(n, k, b)$, where $b = 1$ [resp. $b = -1$], is isomorphic to the group of reduced residues* mod LCM $(q-1, \ldots, q^n-1, (q^{n+1}-1)/(q-1))$ [*resp.* mod LCM $(q-1, \ldots, q^n-1, 2(q^{n+1}-1)/(q-1))$] *factored by the cyclic subgroup generated by q of order* LCM $(1, \ldots, n+1)$.

Proof. The proof is essentially the same as for Theorem 3, with the following modification. We treat the case $b = 1$, the case $b = -1$ is similar. Let $N = \mathrm{LCM}\,(q-1, \ldots, q^n-1, (q^{n+1}-1)/(q-1))$. We note firstly that the order of $q \bmod ((q^{n+1}-1)/(q-1))$ is $(n+1)$, since clearly $q^{n+1} \equiv 1 \bmod ((q^{n+1}-1)/(q-1))$, and if q has order $t \mid (n+1)$, then $(q^{n+1}-1) \mid (q^t-1)(q-1)$.

But

$$(q-1)(q^t-1) = (q^{t+1}-1)-(q^t+q-2).$$

Since $q \geqslant 2$, and as $n+1 \geqslant 2$, $t \leqslant (n+1)/2 \leqslant n$, and so $(q^{n+1}-1) > (q-1)(q^t-1)$, a contradiction.

We now determine the order of $q \bmod N$. Let $s = \mathrm{LCM}(1, \ldots, n+1)$. Then $q^s \equiv 1 \bmod N$. If $q^m \equiv 1 \bmod N$, then $t \mid m$, $1 \leqslant t \leqslant n$. To show $(n+1) \mid m$, we have

$$\left(\frac{q^{n+1}-1}{q-1}\right) \mid (q^m-1).$$

Let $\gamma = \gcd(q^{n+1}-1, q^m-1) = q^{\gcd(n+1, m)}-1$ then

$$\frac{q^{n+1}-1}{\gamma} \mid (q-1)\frac{q^m-1}{\gamma}$$

thus

$$\frac{q^{n+1}-1}{\gamma} \mid (q-1)$$

or

$$(q^{n+1}-1) \mid (q-1)(q^{\gcd(n+1,m)}-1).$$

As before, this is impossible unless $n+1 = \gcd(n+1, m)$, i.e. $(n+1) \mid m$. Now suppose

$$k \equiv q^t \bmod N', \quad N' = \mathrm{LCM}(q-1, \ldots, q^n-1), \quad k \equiv q^s \bmod \left(\frac{q^{n+1}-1}{q-1}\right).$$

Then

$$k = q^t + aN' \equiv q^s \bmod \left(\frac{q^{n+1}-1}{q-1}\right),$$

hence

$$aN' = q^t(q^{s-t}-1)\left(\frac{q^{n+1}-1}{q-1}\right).$$

Thus

$$\left(\frac{q^m-1}{q-1}\right) \mid (q^{s-t}-1), \quad \text{for} \quad m \mid n+1.$$

As before this implies $m \mid (s-t)$, or $s \equiv t \bmod m$. The rest of the proof goes through as before, noting that we already know the nature and number of the solutions to the first n congruences.

Lidl and Müller [12] examined the question of when the group induced by the permutation polynomial vectors $g(n, k, b)$ is cyclic for $n = 2$. The case $n = 1$ was settled earlier by Hule and Müller [6]. We now extend this to the general case.

THEOREM 5. *The group G induced by the permutation polynomial vectors amongst the $g(n, k, b)$ is cyclic if $q = 2$, $n = 2$ and $b = 1$, or if $q = 2$ or 3, $n = 2$ and $b = 0$. G is not cyclic if $n > 2$.*

Proof. The fact that G is cyclic in the cases given was established in [12]. The following argument was suggested, in the case $n = 2$, by W. Narkiewicz [13]. If an Abelian group A contains a subgroup isomorphic to the direct sum of three or more copies of C_2, then, when A is factored by a cyclic group, the resulting group cannot be cyclic. If N is the appropriate modulus ($\mathrm{LCM}(q-1, \ldots, q^n-1)$ for $b = 0$, etc.), and q is odd then $8 \mid (q^2-1)$, and (q^3-1) (resp. $\left(\frac{q^3-1}{q-1}\right)$) is divisible by an odd prime. Thus the prime decomposition of N is of the form $N = 2^\beta p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, $p_i \neq 2$, $\beta \geqslant 3$, $\alpha_i \geqslant 1$. The group G of reduced residues mod N is isomorphic to the direct sum of the groups $Z/(2^\beta)$, $Z/(p_i^{\alpha_i})$. $Z/(2^\beta) \simeq C_2 \oplus C_{2^{\beta-1}}$, where C_i denotes a cyclic group of order i.

$$Z/(p_1^{\alpha_1}) \simeq C_{p_1^{\alpha_1-1}} \oplus C_{p_1-1}.$$

Thus G contains a subgroup isomorphic to C_2^3.

If q is even, $q \neq 2$, then $\gcd(q^2-1, q^3-1) = (q-1)$, and so there are prime factors of (q^2-1) not dividing (q^3-1). If $q-1$, q^2+q+1 have a common prime factor k, then $q \equiv 1 \bmod k$, and so $q^2+q+1 \equiv 3 \bmod k$. Thus unless 3 is the only prime dividing $(q-1)$, there is a prime dividing $(q-1)$ and not (q^2+q+1). If $q-1 = 3^t$, then

$$q^2+q+1 = (q-1)^2+3(q-1)+3 = 3[3^{2t-1}+3^t+1]$$

and the second factor is not divisible by 3. Thus there are at least three odd primes dividing N, and so G contains C_2^3. If $q = 2$, $n \geqslant 3$, $N = \gcd(1, 3, 7, 15, \ldots)$ and so N is divisible by at least three odd primes as before.

4. Matrix permutation polynomials. Brawley, Carlitz, and Levine [2] have determined the polynomials $f(x) \in \boldsymbol{F}_q[x]$ which permute the set of $n \times n$ matrices over $\boldsymbol{F}_q$ under substitution. In this section we give a different proof of their result using Theorem 1.

THEOREM 6 (Brawley, Carlitz and Levine). *Let $f(x) \in \boldsymbol{F}_q[x]$. Then $f(x)$ is a permutation polynomial on $F_{n\times n}$, the set of $n \times n$ matrices with entries in $\boldsymbol{F}_q$ if and only if*

(i) *$f(x)$ is a permutation polynomial over $\boldsymbol{F}_{q^r}$, $1 \leqslant r \leqslant n$,*

(ii) *$f'(x)$ does not vanish on any of the fields $\boldsymbol{F}_q, \ldots, \boldsymbol{F}_{q^{[n/2]}}$.*

We first prove the following lemma.

LEMMA 14. *$f(x) \in \boldsymbol{F}_q[x]$ is a permutation polynomial on $F_{n\times n}$ if and only if $f(x)$ permutes the similarity classes of $F_{n\times n}$, where the similarity class of $B \in F_{n\times n}$ is $C_B = \{A^{-1}BA \mid A \in F_{n\times n}, A \text{ invertible}\}$.*

Proof. Suppose $f(x)$ is a permutation polynomial on $F_{n\times n}$. Then f acts on the similarity classes, by defining

$$f(C_B) = C_{f(B)}.$$

If $Y \in C_B$, then $Y = A^{-1}BA$, and $f(Y) = A^{-1}f(B)A \in C_{f(B)}$. The map $C_B \to C_{f(B)}$ is surjective on the set of similarity classes, as otherwise there would be a class with no preimage, and any matrix Y in this class would have no preimage under f, contradicting the fact that f is a permutation polynomial on $F_{n\times n}$. Thus f permutes the similarity classes, as there are a finite number of them.

Now suppose f permutes the similarity classes in $F_{n\times n}$. Then since $|C_{f(B)}| \leqslant |C_B|$ for all $B \in F_{n\times n}$, each C_B can only be mapped to a class whose order is less than or equal to that of C_B. If $|C_B| = |C_{f(B)}|$ then f induces a one-to-one map of C_B onto $C_{f(B)}$. Thus f can fail to permute $F_{n\times n}$ only if $|C_B| > |C_{f(B)}|$ for some C_B. Let M be the set of classes which are of maximal order n with respect to this property.

Then since all the classes of order greater than n are mapped onto classes of their own cardinality, the set of preimages of the classes of M must be M itself.

Thus $f(x)$ preserves the cardinality of the classes of M, a contradiction. Thus $f(x)$ preserves the cardinality of all classes and so is a permutation polynomial over $F_{n\times n}$.

Proof of Theorem 6. Suppose $f(x)$ permutes $F_{n\times n}$. Let $A(x) \in \boldsymbol{F}_q[x]$, and let C_A be its companion matrix. The minimal polynomial of C_A is $A(y)$. Hence the algebra $J(A)$ generated by C_A over $\boldsymbol{F}_q$ is isomorphic to $\boldsymbol{F}_q[y]/(A(y))$. Since $f(x)$ is a permutation polynomial on $F_{n\times n}$, it is so on $J(A)$, and *via* the isomorphism is so on $\boldsymbol{F}_q[y]/(A(y))$. Now if $A(y) = \prod p_i^{a_i}(y)$, then $\boldsymbol{F}_q[y]/(A(y)) \simeq \oplus\sum \boldsymbol{F}_q[y]/(p_i^{a_i}(y))$, and $f(x)$ permutes each of the $\boldsymbol{F}_q[y]/(p_i^{a_i}(y))$. Taking $A(y)$ to have an irreducible factor of degree r and multiplicity one, we see that $f(x)$ permutes $\boldsymbol{F}_{q^r}$. Now if $A(y)$ has a factor of multiplicity greater than one (and the degree of any such must be less than or equal to $[n/2]$), $f(x)$ must permute $\boldsymbol{F}_q[y]/(p_i^{a_i}(y))$, $a_i > 1$, $\deg p_i(y) > r$. Such an $f(x)$ is called regular over $\boldsymbol{F}_q$, and it is known that regularity of f is equivalent to $f'(u) \neq 0$ for $u \in \boldsymbol{F}_{q^r}$. [See Lausch and Nöbauer [7], prop. 4.31, p. 163].

Now assume $f(x)$ satisfies the given conditions. The similarity classes are determined by their invariant factors, which are polynomials in $\boldsymbol{F}_q[x]$.

A result from Gantmacher ([5], p. 158, note 2) ensures that the invariant factors of $f(A)$ are $\Delta_f g$, where g are the invariant factors of A, and Δ_f is the mapping defined in Section 1. If $f(A) = f(B)$, where A, B are in different similarity classes, then if $\{g_i\}$ are the invariant factors of A, $\{h_j\}$ of B, the invariant factors of $f(A)$, $f(B)$ are $\{\Delta_f g_i\}$, $\{\Delta_f h_j\}$ respectively. Since the degrees of g_i, h_j are $\leqslant n$, and as by Theorem 1 Δ_f permutes the polynomials in $\boldsymbol{F}_q$ of each degree $\leqslant n$, $\{g_i\} = \{h_j\}$ and so A is similar to B, a contradiction. Thus f permutes the similarity classes, and so permutes $F_{n\times n}$ by Lemma 14.

References

[1] I. Blake and C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York 1975.

[2] J. Brawley, L. Carlitz and J. Levine, *Scalar polynomial functions on the $n \times n$ matrices over a finite field*, Linear Algebra Appl. 10 (1975), pp. 199–217.

[3] L. Carlitz and J. Hayes, *Permutations with coefficients in a subfield*, Acta Arith. 21 (1972), pp. 131–135.

[4] R. Eier and R. Lidl, *Tschebyscheffpolynome in einer und zwei Variablen*, Abh. Math. Sem. Univ. Hamburg 41 (1973), pp. 17–27.

[5] G. Gantmacher, *The Theory of Matrices*, Chelsea, New York 1959.

[6] H. Hule and W. B. Müller, *Grupos ciclicos de permutaciones inducidas por polinomios sobre campos de Galois*, Anais da Academia Brasileira de Ciencias 44.

[7] H. Lausch and W. Nöbauer, *Algebra of polynomials*, North-Holland, Amsterdam 1973.

[8] R. Lidl, *Tschebyscheffpolynome und die dadurch dargestellten Gruppen*, Monatsh. Math. 77 (1973), pp. 132–147.

[9] — *Über die Struktur einer durch Tschebyscheffpolynome in 2 Variablen dargestellten Permutationsgruppe*, Beit. Algebra Geom. 3 (1974), pp. 41–48.

[10] — *Tschebyscheffpolynome in mehreren Variablen*, J. Reine Angew. Math. 273 (1975), pp. 178–198.

[11] R. Lidl and C. Wells, *Chebyshev polynomials in several variables*, ibid. 255 (1972), pp. 104–111.

[12] R. Lidl and W. Müller, *Über Permutationsgruppen die durch Tschebyscheffpolynome erzeugt werden*, Acta Arith. 30 (1976), pp. 19–25.

[13] W. Narkiewicz, private communication, 1977.

[14] W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. 231 (1968), pp. 215–219.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TASMANIA
Hobart, Australia

Received on 17. 6. 1980 (1211)