Duke Math. J. 38 (1971), 659-665.

NOTE ON DICKSON'S PERMUTATION POLYNOMIALS

BY KENNETH S. WILLIAMS

1. Introduction. Let p be a prime and let m be an integer ≥ 1. The finite field with p^m elements is denoted by $GF(p^m)$ and its algebraic closure by $\overline{GF(p^m)}$. If X denotes an indeterminate, a polynomial $F(X) \in GF(p^m)[X]$ is called a permutation polynomial if the associated polynomial function is a bijection on $GF(p^m)$. Recently Hayes [5] has suggested an approach which might lead to a systematic theory of permutation polynomials, at least when $p^m > k(n)$, where $k(n)$ is a constant depending only on n, the degree of F. Appealing to a deep theorem of Lang and Weil [6] he notes (for $p^m > k(n)$) that

$$F^*(X, Y) = \frac{F(X) - F(Y)}{X - Y} \in GF(p^m)[X, Y]$$

must factor in $\overline{GF(p^m)}[X, Y]$ if $F(X) \in GF(p^m)[X]$ is to be a permutation polynomial. It is the purpose of this note to show that Hayes' approach works for Dickson's polynomials [3] [4]

$$D_{n,a}(X) = \sum_{s=0}^{n} (-1)^s \frac{2n+1}{2n+1-s} \binom{2n+1-s}{s} a^s X^{2n+1-2s}, \tag{1.1}$$

where $n \geq 1$ and $a(\neq 0) \in GF(p^m)$. We note that

$$\frac{2n+1}{2n+1-s} \binom{2n+1-s}{s}$$

is an integer for $s = 0, 1, 2, \cdots, n$ as it is just

$$2\binom{2n+1-s}{s} - \binom{2n-s}{s}.$$

It is shown by factoring $D^*_{n,a}(X, Y)$ in $\overline{GF(p^m)}[X, Y]$ that if G.C.D. $(p^{2m} - 1, 2n + 1) = 1$, then Dickson's polynomials $D_{n,a}(X)$ are permutation polynomials. This result is not new, in fact Dickson [3] [4] proved that the $D_{n,a}(X)$ are permutation polynomials under this condition by showing that the equation $D_{n,a}(x) = b$ has a unique solution $x \in GF(p^m)$ for any $b \in GF(p^m)$. (The equation $D_{n,a}(x) = b$ considered as an equation over the complex field is solvable algebraically by a generalization of Cardan's solution of the cubic $D_{1,a}(x) = b$—this has been rediscovered a number of times, see for example [7]—and Dickson's argument is just the finite field analogue of this.) What is new is the explicit form of the factorization of $D^*_{n,a}(X, Y)$ in $\overline{GF(p^m)}[X, Y]$. The author was led to the form of the factors through a study of a recent paper by Chowla [2].

Received November 8, 1969. Revision received August 4, 1970. This research was supported by a National Research Council of Canada Grant (No. A-7233).

2. The quantities α_i and β_i. We let $p^k(k \geq 0)$ denote the largest power of p dividing $2n + 1$ so that

(2.1) $$2n + 1 = p^k(2n_1 + 1), \qquad p \nmid (2n_1 + 1).$$

As G.C.D. $(p, 2n_1 + 1) = 1$ the quantity

$$q = \frac{p^{\phi(2n_1+1)} - 1}{2n_1 + 1},$$

where ϕ denotes Euler's function, is an integer. Hence if α is a primitive element of $GF(p^{\phi(2n_1+1)})$, that is a generator of the cyclic (multiplicative) group of $GF(p^{\phi(2n_1+1)})$, the quantity $\alpha^q \varepsilon GF(p^{\phi(2n_1+1)}) \subseteq GF(p^{m\phi(2n_1+1)}) \subset \overline{GF(p^m)}$ is a primitive $(2n_1 + 1)$-th root of unity over $GF(p^m)$. Denoting such a primitive root by θ, so that

(2.2) $$\theta^{2n_1+1} = 1, \qquad \theta^i \neq 1, \quad i = 1, 2, \cdots, 2n_1,$$

we set for $i = 1, 2, \cdots, n_1$

(2.3) $$\alpha_i = \theta^i + \theta^{2n_1+1-i}, \qquad \beta_i = \theta^i - \theta^{2n_1+1-i}.$$

We note that α_i and β_i are not independent as $\alpha_i^2 - \beta_i^2 = 4$. We require a number of simple results concerning the α_i and β_i so that for convenience we put them together in a lemma.

LEMMA 1. *For $i = 1, 2, \cdots, n_1$ we have $\alpha_i \neq \pm 2$, $\beta_i \neq 0$, and for $i, j = 1, 2, \cdots, n_1$ with $i \neq j$ we have $\beta_i^2 \neq \beta_j^2$.*

Proof. If $\alpha_i = \pm 2$ then $\theta^i + \theta^{-i} = \pm 2$, that is, $\theta^i = \pm 1$, or $\theta^{2i} = 1$, which contradicts (2.2) as $1 < 2i \leq 2n_1$. Thus we have $\alpha_i \neq \pm 2$, and $\beta_i \neq 0$ follows from $\alpha_i^2 - \beta_i^2 = 4$.

Finally if $\beta_i^2 = \beta_j^2$, $i \neq j$, then $\theta^{2i} + \theta^{-2i} = \theta^{2j} + \theta^{-2j}$, so that on multiplying both sides of this by θ^{2i} we obtain $\theta^{4i} + 1 = \theta^{2i+2j} + \theta^{2i-2j}$, or equivalently $(\theta^{2i+2j} - 1)(\theta^{2i-2j} - 1) = 0$. Thus we have $\theta^{2(i \pm j)} = 1$. Hence there exists an integer t such that $2(i \pm j) = t(2n_1 + 1)$. Now $0 < |i \pm j| < 2n_1$, so that

$$0 < |t| < \frac{4n_1}{2n_1 + 1} < 2 \quad \text{giving} \quad t = \pm 1,$$

which is clearly impossible as $2(i \pm j)$ is even and $\pm(2n_1 + 1)$ is odd.

3. The factorization of $D_{n,a}(X)$. In this section we prove

THEOREM 1. *For $n \geq 1$ and $a(\neq 0) \varepsilon GF(p^m)$ we have*

$$D_{n,a}(X) = X^{p^k} \prod_{i=1}^{n_1} (X^2 + \beta_i^2 a)^{p^k}.$$

Proof. We write $\overline{GF(p^m)(X)}$ for the field of rational functions in the indeterminate X over the field $\overline{GF(p^m)}$. The algebraic extension field of $\overline{GF(p^m)}(X)$

formed by adjoining the element $\sqrt{X^2 - 4a}$ ($a(\neq 0) \in GF(p^m)$) is denoted by $\overline{GF(p^m)}(X, \sqrt{X^2 - 4a})$. Now if R is any commutative ring with identity and $\alpha, \beta \in R$, the following identity is readily established by induction on n

$$(3.1) \quad \alpha^{2n+1} + \beta^{2n+1} = \sum_{s=0}^{n} (-1)^s \frac{2n+1}{2n+1-s} \binom{2n+1-s}{s} (\alpha + \beta)^{2n+1-2s} (\alpha\beta)^s.$$

Applying (3.1) with

$$R = \overline{GF(p^m)}(X, \sqrt{X^2 - 4a}), \ \alpha = \frac{X + \sqrt{X^2 - 4a}}{2}, \ \beta = \frac{X - \sqrt{X^2 - 4a}}{2},$$

we obtain

$$(3.2) \qquad D_{n,a}(X) = \left(\frac{X + \sqrt{X^2 - 4a}}{2}\right)^{2n+1} + \left(\frac{X - \sqrt{X^2 - 4a}}{2}\right)^{2n+1}.$$

Now as $p \nmid (2n_1 + 1)$ we have seen that there exists a primitive $(2n_1 + 1)$-th root of unity over $GF(p^m)$, namely θ. Moreover θ^2 is also a primitive $(2n_1 + 1)$-th root of unity over $GF(p^m)$, so that if X_1, X_2 are indeterminates we have the following factorization in $\overline{GF(p^m)}[X_1, X_2]$

$$X_1^{2n_1+1} - X_2^{2n_1+1} = \prod_{i=0}^{2n_1} (X_1 - \theta^{2i} X_2).$$

Hence we have

$$\begin{aligned} X_1^{2n+1} - X_2^{2n+1} &= X_1^{p^k(2n_1+1)} - Y_1^{p^k(2n_1+1)} \\ &= (X_1^{2n_1+1} - Y_1^{2n_1+1})^{p^k} \\ &= \prod_{i=0}^{2n_1} (X_1 - \theta^{2i} X_2)^{p^k}. \end{aligned}$$

Replacing X_1, X_2 by the elements

$$\frac{X + \sqrt{X^2 - 4a}}{2}, \qquad \frac{\sqrt{X^2 - 4a} - X}{2}$$

(respectively) of the field $\overline{GF(p^m)}(X, \sqrt{X^2 - 4a})$ we obtain

$$\begin{aligned} &\left(\frac{X + \sqrt{X^2 - 4a}}{2}\right)^{2n+1} - \left(\frac{\sqrt{X^2 - 4a} - X}{2}\right)^{2n+1} \\ &= X^{p^k} \prod_{i=1}^{2n_1} \left\{\left(\frac{X + \sqrt{X^2 - 4a}}{2}\right) - \theta^{2i}\left(\frac{\sqrt{X^2 - 4a} - X}{2}\right)\right\}^{p^k} \\ &= X^{p^k} \prod_{i=1}^{n_1} \left\{\left[\left(\frac{X + \sqrt{X^2 - 4a}}{2}\right) - \theta^{2i}\left(\frac{\sqrt{X^2 - 4a} - X}{2}\right)\right]\right. \\ &\quad \left.\cdot\left[\left(\frac{X + \sqrt{X^2 - 4a}}{2}\right) - \theta^{2(2n_1+1)-2i}\left(\frac{\sqrt{X^2 - 4a} - X}{2}\right)\right]\right\}^{p^k} \end{aligned}$$

$$= X^{p^k} \prod_{i=1}^{n_1} \{X^2 - 2a + (\theta^{2i} + \theta^{2(2n_1+1)-2i})a\}^{p^k}$$
$$= X^{p^k} \prod_{i=1}^{n_1} \{X^2 + (\theta^i - \theta^{2n_1+1-i})^2 a\}^{p^k}$$
$$= X^{p^k} \prod_{i=1}^{n_1} (X^2 + \beta_i^2 a)^{p^k}.$$

The theorem now follows on appealing to (3.2).

As immediate consequences of Theorem 1 we have

COROLLARY 1. *For $n \geq 1$ and $a(\neq 0) \in GF(p^m)$ we have*

$$D_{n,a}(X) = \{D_{n_1,a}(X)\}^{p^k}.$$

COROLLARY 2. $\prod_{i=1}^{n_1} \beta_i^2 = (-1)^{n_1}(2n_1 + 1)$.

4. The factorization of $D^*_{n,a}(X, Y)$. We are now in a position to prove the main result of this paper, namely the factorization of $D^*_{n,a}(X, Y)$ in $\overline{GF(p^m)}[X, Y]$.

THEOREM 2. *For $n \geq 1$ and $a(\neq 0) \in GF(p^m)$ we have*

$$D^*_{n,a}(X, Y) = (X - Y)^{p^k - 1} \prod_{i=1}^{n_1} (X^2 - \alpha_i XY + Y^2 + \beta_i^2 a)^{p^k}, \tag{4.1}$$

where each quadratic factor is irreducible in $\overline{GF(p^m)}[X, Y]$.

Proof. Appealing to Corollary 1 we have

$$\begin{aligned}(X - Y)\, D^*_{n,a}(X, Y) &= D_{n,a}(X) - D_{n,a}(Y) \\ &= \{D_{n_1,a}(X)\}^{p^k} - \{D_{n_1,a}(Y)\}^{p^k} \\ &= \{D_{n_1,a}(X) - D_{n_1,a}(Y)\}^{p^k} \\ &= \{(X - Y)\, D^*_{n_1,a}(X, Y)\}^{p^k}\end{aligned}$$

giving

$$D^*_{n,a}(X, Y) = (X - Y)^{p^k - 1}\{D^*_{n_1,a}(X, Y)\}^{p^k}. \tag{4.2}$$

Thus it suffices to factor $D^*_{n_1,a}(X, Y)$. To do this we apply (3.1) with n_1 replacing n, $R = \overline{GF(p^m)}[X, Y]$,

$$\alpha = \frac{\theta^i X - Y}{\beta_i}, \qquad \beta = \frac{-\theta^{2n_1+1-i} X + Y}{\beta_i}$$

so that

$$\alpha + \beta = X, \qquad \alpha\beta = \frac{-(X^2 - \alpha_i XY + Y^2)}{\beta_i^2},$$

obtaining

$$(4.3) \qquad \frac{1}{\beta_i^{2n_1+1}} \{(\theta^i X - Y)^{2n_1+1} + (-\theta^{2n_1+1-i} X + Y)^{2n_1+1}\}$$
$$= \sum_{s=0}^{n_1} \frac{2n_1+1}{2n_1+1-s} \binom{2n_1+1-s}{s} X^{2n_1+1-2s} \left(\frac{X^2 - \alpha_i XY + Y^2}{\beta_i^2}\right)^s.$$

Similarly choosing

$$\alpha = \frac{-X + \theta^i Y}{\beta_i}, \qquad \beta = \frac{X - \theta^{2n_1+1-i} Y}{\beta_i},$$

so that

$$\alpha + \beta = Y, \qquad \alpha\beta = -\frac{(X^2 - \alpha_i XY + Y^2)}{\beta_i^2}$$

we obtain

$$(4.4) \qquad \frac{1}{\beta_i^{2n_1+1}} \{(-X + \theta^i Y)^{2n_1+1} + (X - \theta^{2n_1+1-i} Y)^{2n_1+1}\}$$
$$= \sum_{s=0}^{n_1} \frac{2n_1+1}{2n_1+1-s} \binom{2n_1+1-s}{s} Y^{2n_1+1-2s} \left(\frac{X^2 - \alpha_i XY + Y^2}{\beta_i^2}\right)^s.$$

Now

$$(-X + \theta^i Y)^{2n_1+1} = (-\theta^{2n_1+1-i} X + Y)^{2n_1+1},$$
$$(X - \theta^{2n_1+1-i} Y)^{2n_1+1} = (\theta^i X - Y)^{2n_1+1}$$

so that from (4.3) and (4.4) we have

$$\sum_{s=0}^{n_1} \frac{2n_1+1}{2n_1+1-s} \binom{2n_1+1-s}{s} (X^{2n_1+1-2s} - Y^{2n_1+1-2s}) \left(\frac{X^2 - \alpha_i XY + Y^2}{\beta_i^2}\right)^s = 0.$$

Hence the equation

$$\sum_{s=0}^{n_1} \frac{2n_1+1}{2n_1+1-s} \binom{2n_1+1-s}{s} (X^{2n_1+1-2s} - Y^{2n_1+1-2s}) t^s = 0$$

has the n_1 distinct roots

$$t = \frac{X^2 - \alpha_i XY + Y^2}{\beta_i^2} \qquad (i = 1, 2, \cdots, n_1) \quad \text{in} \quad \overline{GF(p^m)}[X, Y].$$

Thus

$$\sum_{s=0}^{n_1} \frac{2n_1+1}{2n_1+1-s} \binom{2n_1+1-s}{s} (X^{2n_1+1-2s} - Y^{2n_1+1-2s}) t^s$$
$$= (2n_1+1)(X - Y) \prod_{i=1}^{n_1} \left(t - \frac{(X^2 - \alpha_i XY + Y^2)}{\beta_i^2}\right)$$
$$= (X - Y) \prod_{i=1}^{n_1} (X^2 - \alpha_i XY + Y^2 - \beta_i^2 t),$$

appealing to Corollary 2. Taking $t = -a$ we have

$$D^*_{n_1,a}(X, Y) = \sum_{s=0}^{n_1} (-1)^s \frac{2n_1+1}{2n_1+1-s}\binom{2n_1+1-s}{s} \frac{X^{2n_1+1-2s} - Y^{2n_1+1-2s}}{X-Y} a^s$$

$$= \prod_{i=1}^{n_1} (X^2 - \alpha_i XY + Y^2 + \beta_i^2 a),$$

and the required factorization of $D^*_{n,a}(X, Y)$ follows from (4.2).

If $X^2 - \alpha_i XY + Y^2 + \beta_i^2 a$ is reducible in $\overline{GF(p^m)}[X, Y]$, then there exist $r, s, t, u \in \overline{GF(p^m)}$ such that

$$X^2 - \alpha_i XY + Y^2 + \beta_i^2 a = (X + rY + s)(X + tY + u).$$

As $\beta_i \neq 0$ (Lemma 1) and $a \neq 0$ we have $s \neq 0$, $u \neq 0$. Thus equating coefficients of X and Y we obtain $u = -s$ and $t = r$. Next equating coefficients of Y^2 and XY we have $r^2 = 1$ and $2r = -\alpha_i$, that is, $\alpha_i = \pm 2$, which contradicts Lemma 1. Hence $X^2 - \alpha_i XY + Y^2 + \beta_i^2 a$ is irreducible in $\overline{GF(p^m)}[X, Y]$.

5. Dickson's theorem. We show how Dickson's theorem [3], [4] can be deduced from Theorem 1 if G.C.D. $(p^{2m} - 1, 2n + 1) = 1$. We first prove a lemma concerning the non-vanishing of the quadratic factors of $D^*_{n,a}(X, Y)$ in $GF(p^m)$.

LEMMA 2. *If G.C.D.* $(p^{2m} - 1, 2n + 1) = 1$ *and* $a(\neq 0) \in GF(p^m)$, *then for* $i = 1, 2, \cdots, n_1$ *there do not exist* $x, y \in GF(p^m)$ *such that*

$$x^2 - \alpha_i xy + y^2 + \beta_i^2 a = 0. \tag{5.1}$$

Proof. Writing ϕ for $\theta^i (1 \leq i \leq n_1)$ (5.1) becomes

$$x^2 - \left(\phi + \frac{1}{\phi}\right)xy + y^2 + \left(\phi - \frac{1}{\phi}\right)^2 a = 0,$$

that is,

$$\phi^4 - \frac{xy}{a}\phi^3 + \left(\frac{x^2+y^2}{a} - 2\right)\phi^2 - \frac{xy}{a}\phi + 1 = 0. \tag{5.2}$$

Now it can be deduced immediately from the work of Carlitz [1] that the reciprocal quartic $X^4 + AX^3 + BX^2 + AX + 1 \in GF(p^m)[X]$, where $p > 2$, is irreducible in $GF(p^m)[X]$ if and only if both of $A^2 - 4B + 8$ and $(B + 2)^2 - 4A^2$ are non-squares in $GF(p^m)$. It is easy to check that if $X^4 + AX^3 + BX^2 + AX + 1$ is reducible, it has only linear or quadratic factors. We have $A = -xy/a$ and

$$B = \frac{x^2+y^2}{a} - 2 \quad \text{so that} \quad (B+2)^2 - 4A^2 = \left(\frac{x^2-y^2}{a}\right)^2.$$

Hence the quartic (5.2) is reducible into linear and/or quadratic factors over $GF(p^m)$. This implies that $\phi \in GF(p^{2m})$. Thus, as $\phi \neq 0$, $\phi^{p^{2m}-1} = 1$. As

G.C.D. $(p^{2m} - 1, 2n + 1) = 1$ there exist integers a and b such that $a(p^{2m} - 1) + b(2n + 1) = 1$. Hence

$$\phi = \phi^{a(p^{2m}-1)+b(2n+1)} = 1,$$

which is the required contradiction.

Hence from Theorem 2 and Lemma 2 we have

THEOREM 3 (Dickson). *If G.C.D.* $(p^{2m} - 1, 2n + 1) = 1$ *then* $D_{n,a}(X)$, *where* $a(\neq 0) \in GF(p^m)$, *is a permutation polynomial in* $GF(p^m)[X]$.

REFERENCES

1. L. CARLITZ, *A special quartic congruence*, Math. Scand., 4(1956), pp. 243–246.
2. S. CHOWLA, *On substitution polynomials (mod p)*, Norske Vid. Selsk. Forh., Trondhjem, vol. 41(1968), pp. 4–6.
3. L. E. DICKSON, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, I, Ann. of Math., vol. 11(1896/7), pp. 161–183; II, Ann. of Math., vol. 11(1896/7), pp. 65–120.
4. L. E. DICKSON, *Linear Groups*, New York, 1958, pp. 57–58.
5. D. R. HAYES, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J., vol. 34(1967), pp. 293–306.
6. S. LANG AND A. WEIL, *Number of points of varieties in finite fields*, Amer. J. Math., vol. 76(1953), pp. 819–827.
7. K. S. WILLIAMS, *A generalization of Cardan's solution of the cubic*, Math. Gaz., vol. 46(1962), pp. 221–223.

CARLETON UNIVERSITY