BULL. AUSTRAL. MATH. SOC. 11T06
VOL. 56 (1997) [499–505]

A NOTE ON THE PERMUTATION BEHAVIOUR OF THE DICKSON POLYNOMIALS OF THE SECOND KIND

M. HENDERSON

In this note known factorisation results for the Dickson polynomials of the second kind, $f_k(X,a)$, are used to obtain simple restrictions on those k for which $f_k(X,a)$ is a permutation polynomial over $\mathbb{F}_q$.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field of order q where $q = p^e$ and p is a prime. Let $\mathbb{F}_q^*$ represent the non-zero elements of $\mathbb{F}_q$ and η denote the quadratic character on $\mathbb{F}_q^*$. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the mapping induced by f permutes $\mathbb{F}_q$. If $f \in \mathbb{F}_q[X]$ has no repeated roots over any extension of $\mathbb{F}_q$ then f will be called *simple*. Let $a \in \mathbb{F}_q^*$ and k be a positive integer. Every $x \in \mathbb{F}_q$ may be written as $x = u + au^{-1}$ where $u \in \mathbb{F}_{q^2}$ is a root of the quadratic $Z^2 - xZ + a$. Under these circumstances u will satisfy $u^{q-1} = 1$ or $u^{q+1} = a$. The Dickson polynomial of the second kind (DPSK), $f_k(X,a) \in \mathbb{F}_q[X]$, can be defined by

$$f_k(x,a) = \frac{u^{k+1} - a^{k+1}u^{-(k+1)}}{u - au^{-1}}$$

with the condition that $u \neq \pm b$ if $a = b^2$ for some $b \in \mathbb{F}_q$. The excluded values are calculated using $f_k(2b,a) = (k+1)b^k$ and $f_k(-2b,a) = (k+1)(-b)^k$. Other definitions of these polynomials can be found in the monograph [**5**] which is devoted to Dickson polynomials of the first and second kind. Some results on the permutation behaviour of the DPSK have been found, see [**7, 4**]. If $q = p$ or $q = p^2$ then the conditions given in [**7**] were shown to be both necessary and sufficient in [**2**] (case $q = p$) and [**3**] (case $q = p^2$).

Some factorisations of the Dickson polynomials of the first kind are contained in [**5**, Chapter 2]. In [**1**] the factorisation of both types of Dickson polynomials over a finite field was determined. The permutation properties of the Dickson polynomials of the first kind are well understood, see [**5**, Chapter 2]. Here we use results from [**1**] to obtain simple restrictions on those k for which $f_k(X,a)$ can be a permutation polynomial.

The factorisation of the DPSK over $\mathbb{F}_q$ is closely connected to the factorisation of the cyclotomic polynomials. We can use the formulas for the factorisation of $X^{k+1} - 1$ into cyclotomic polynomials, see [**6**], to obtain similar factorisations for the DPSK.

Received 17th March, 1997.

Lemma 1.1. *Suppose that $k+1$ is not divisible by p. Then the factorisation of $f_k(X,a)$ is given by*

$$f_k(x,a)=\prod_{\substack{d|(k+1)\\ d\neq 1}}\prod_{\substack{m=1\\ (m,d)=1}}^{d}(u-\zeta_d^m a u^{-1})$$

where ζ_d is a dth root of unity over $\mathbb{F}_q$.

Proof: From the definition of the DPSK we have

$$f_k(x,a)=\frac{u^{k+1}-a^{k+1}u^{-(k+1)}}{u-au^{-1}}=a^k u^k\left(\frac{(u^2a^{-1})^{(k+1)}-1}{u^2a^{-1}-1}\right).$$

By substituting y for u^2a^{-1} the problem of factorising $f_k(x,a)$ becomes the problem of determining the factors of the polynomial $(y^{k+1}-1)(y-1)$. By using the factorisation of the cyclotomic polynomials

$$\begin{aligned} f_k(x,a)&=\frac{a^{(k+1)}u^{-(k+1)}}{u-au^{-1}}\prod_{d|(k+1)}Q_d(a^{-1}u^2)\\ &=\frac{a^{(k+1)}u^{-(k+1)}}{u-au^{-1}}\prod_{d|(k+1)}\prod_{\substack{m=1\\ (m,d)=1}}^{d}(a^{-1}u^2-\zeta_d^m)\\ &=(u-au^{-1})^{-1}\prod_{d|(k+1)}\prod_{\substack{m=1\\ (m,d)=1}}^{d}(u-\zeta_d^m au^{-1})\\ &=\prod_{\substack{d|(k+1)\\ d\neq 1}}\prod_{\substack{m=1\\ (m,d)=1}}^{d}(u-\zeta_d^m au^{-1}). \end{aligned}$$

∎

Suppose that p^n is the largest power of p dividing $k+1$. Then $k+1=mp^n$ for some $m\in\mathbb{Z}$ and it is a simple matter to show

$$f_{mp^n-1}(X,a)=f_{m-1}^{p^n}(X,a)(X^2-4a)^{(p^n-1)/2}. \tag{1}$$

We can completely factorise a DPSK over $\mathbb{F}_q$ using this identity and Lemma 1.1. We end this section with a simple but useful identity for the DPSK.

Lemma 1.2. *Let $a,a'\in\mathbb{F}_q^*$ satisfy $\eta(aa')=1$. Then $f_k(X,a)$ permutes $\mathbb{F}_q$ if and only if $f_k(X,a')$ permutes $\mathbb{F}_q$.*

Proof: As $\eta(aa')=1$ then there exists $b\in\mathbb{F}_q^*$ such that $a=ba'$. Then for $x=u+au^{-1}\in\mathbb{F}_q$

$$b^kf_k(x,a)=\frac{(bu)^{k+1}-(b^2a)^{k+1}(bu)^{-(k+1)}}{bu-b^2a(bu)^{-1}}=f_k(bx,b^2a).$$

It now follows that either both of the polynomials permute $\mathbb{F}_q$ or both do not permute $\mathbb{F}_q$. ∎

2. Linear factors of the DPSK where q is odd

In this section we assume q is odd. Lemma 1.1 leads to the next lemma concerned with linear factors of $f_k(X,a)$, or rather, their absence.

Lemma 2.1. *Let $\eta(a) = 1$. Then $f_k(X,a)$ has no roots in $\mathbb{F}_q$ if and only if $\big(k+1, p(q^2-1)\big) = 1$.*

Proof: Let $\eta(a) = 1$ and suppose $f_k(X,a)$ has no roots in $\mathbb{F}_q$. Let $b \in \mathbb{F}_q$ satisfy $b^2 = a$. If p did divide $k+1$ then from (1), $(X^2 - 4a) = (X-2b)(X+2b)$ are factors of $f_k(X,a)$. Suppose $(k+1, q-1) = d > 1$. Then d divides $q-1$ and there exist non-trivial dth roots of unity in $\mathbb{F}_q$. If d is even then -1 is a dth root over $\mathbb{F}_q$ and from Lemma 1.1 $x = u + au^{-1}$ divides $f_k(x,a)$. If d is odd then let m be an even integer satisfying $1 < m < d$ and $(m,d) = 1$. Let ζ_d be a primitive dth root of unity in $\mathbb{F}_q$. Then from Lemma 1.1

$$\begin{aligned}(u - \zeta_d^m au^{-1})(u - \zeta_d^{-m} au^{-1}) &= (u + au^{-1})^2 - a(\zeta_d^{m/2} + \zeta_d^{-m/2})^2 \\ &= \big(x + b(\zeta_d^{m/2} + \zeta_d^{-m/2})\big)\big(x - b(\zeta_d^{m/2} + \zeta_d^{-m/2})\big)\end{aligned}$$

divides $f_k(x,a)$ over $\mathbb{F}_{q^2}$. Hence $(k+1, q-1) = 1$. Suppose $(k+1, q+1) = d > 1$. As $(k+1, q-1) = 1$ then d must be odd. Since $d > 1$ there are non-trivial dth roots of unity in $\mathbb{F}_{q^2}$. Again let m be an even integer satisfying $1 < m < d$ and $(m,d) = 1$. Let ζ_d be primitive dth root of unity in $\mathbb{F}_{q^2}$. From Lemma 1.1

$$\big(u - \zeta_d^m au^{-1}\big)\big(u - \zeta_d^{-m} au^{-1}\big) = \big(x + b(\zeta_d^{m/2} + \zeta_d^{-m/2})\big)\big(x - b(\zeta_d^{m/2} + \zeta_d^{-m/2})\big)$$

divides $f_k(x,a)$. As d divides $q+1$ then

$$\big(\zeta_d^{m/2} + \zeta_d^{-m/2}\big)^q = \big(\zeta_d^{-1}\zeta_d^{q+1}\big)^{m/2} + \big(\zeta_d^{-1}\zeta_d^{q+1}\big)^{-m/2} = \zeta_d^{-m/2} + \zeta_d^{m/2}.$$

Therefore the divisors of $f_k(x,a)$ found are divisors of $f_k(x,a)$ over $\mathbb{F}_q$. Hence $(k+1, q+1) = 1$. From these arguments we can conclude $\big(k+1, p(q^2-1)\big) = 1$.

Conversely, let $\big(k+1, p(q^2-1)\big) = 1$. Then for any d dividing $k+1$ there are no dth roots of unity in $\mathbb{F}_{q^2}$. Suppose that $f_k(X,a)$ has a linear factor. Then there is a solution $x \in \mathbb{F}_{q^2}$ to $f_k(x,a) = 0$. Therefore one of the factors in Lemma 1.1 must satisfy $u - \zeta_d^m au^{-1} = 0$ for some $u \in \mathbb{F}_{q^2}$. By rearranging, $u^2a^{-1} = \zeta_d^m$. Hence ζ_d^m is an element of $\mathbb{F}_{q^2}$. This contradicts the observation that there are no dth roots of unity in $\mathbb{F}_{q^2}$ for any divisor d of $k+1$. ∎

We have a similar result for non-square $a \in \mathbb{F}_q$.

Lemma 2.2. *Let $\eta(a) = -1$. Then $f_k(X, a)$ has no roots in $\mathbb{F}_q$ if and only if $k+1$ is odd.*

Proof: From the definition of the DPSK, X is a factor of $f_k(X,a)$ if and only if $k+1$ is even. Suppose $k+1$ is odd and $f_k(X,a)$ has a non-zero root in $\mathbb{F}_q$. Then there is a non-zero root $u \in \mathbb{F}_{q^2}$ to $u^{2(k+1)} = a^{k+1}$ where either $u^{q-1} = 1$ or $u^{q+1} = a$. If $u^{q-1} = 1$ then

$$(a^{k+1})^{(q-1)/2} = (u^{2(k+1)})^{(q-1)/2} = 1.$$

But as $k+1$ is odd then $(a^{k+1})^{(q-1)/2} = -1$. Hence $u^{q-1} \neq 1$. If $u^{q+1} = a$ then

$$(a^{k+1})^{(q+1)/2} = (u^{2(k+1)})^{(q+1)/2} = (u^{q+1})^{k+1} = a^{k+1}.$$

In this case, as $k+1$ is odd, $(a^{(q+1)/2})^{k+1} = (a^{(q-1)/2}a)^{k+1} = -a^{k+1}$ and we again have a contradiction. Hence $f_k(X,a)$ has no roots in $\mathbb{F}_q$. ∎

The next theorem is taken from [**1**].

Theorem 2.3. [Chou] *Let q be odd and k be a positive integer. Fix $a \in \mathbb{F}_q^*$ and let $b \in \mathbb{F}_{q^2}^*$ satisfy $b^2 = a$. Set $e = 1$ if $b \in \mathbb{F}_q$ and $e = 2$ if $b \notin \mathbb{F}_q$. Write $k+1 = p^r(m+1)$ with $(m+1, p) = 1$ and $r \geqslant 0$. For each divisor $d > 2$ of $2(m+1)$, let n_d be the smallest integer satisfying $q^{n_d} \equiv \pm 1 \bmod d$. Then,*

(1) *If $f \in \mathbb{F}_q[X]$ satisfies: if $e = 1$ then $f(X) \neq (X \pm 2b)$ and if $e = 2$ then $f(X) \neq (X^2 - 4a)$; then f is an irreducible factor of $f_m(X,a)$ if and only if $f(X)$ is an irreducible factor of $f_k(X,a)$ of multiplicity p^r.*

(2) *if $e = 1$ then $(X - 2b)$ and $(X + 2b)$ are irreducible factors of $f_k(X,a)$ of multiplicity $(p^r - 1)/2$, and if $e = 2$ then $(X^2 - 4a)$ is an irreducible factor of $f_k(X,a)$ of multiplicity $(p^r - 1)/2$,*

(3) *$f_m(X,a)$ is simple,*

(4) *$f_m(X,a)$ has the linear factor X whenever m is odd,*

(5) *for any divisor $d > 4$ of $2(m+1)$ with $d \equiv 0 \bmod 4$,*

   (a) *if n_d is even, $n_d/2$ is odd, $e = 2$ and either $(d, q^{n_d/2} - 1) = d/2$ or $(d, q^{n_d/2} + 1) = d/2$ then there are exactly $\phi(d)/n_d$ irreducible factors of $f_m(X,a)$ over $\mathbb{F}_q$ with degree $n_d/2$ where every such factor is of the form*

$$f(x) = \prod_{i=0}^{n_d/2-1} \left(x - b^{q^i}(\zeta_d + \zeta_d^{-1})^{q^i}\right)$$

   where ζ_d is a primitive dth root of unity,

   (b) *otherwise, there are exactly $\phi(d)/(2\,\mathrm{lcm}\,(e, n_d))$ irreducible factors over $\mathbb{F}_q$ of $f_m(X,a)$ with degree $\mathrm{lcm}\,(e, n_d)$ and any such factor is of the form*

$$f(x) = \prod_{i=0}^{\mathrm{lcm}\,(e,n_d)-1} \left(x - b^{q^i}(\zeta_d + \zeta_d^{-1})^{q^i}\right), \tag{2}$$

   where ζ_d is a primitive dth root of unity,

(6) *for any divisor* $d > 2$ *of* $2(m+1)$ *with* $d \not\equiv 0 \bmod 4$, *if* d *is even put* $t = \phi(d)/(2\,\mathrm{lcm}\,(e, n_d))$ *and if* d *is odd put* $t = (\phi(d) + \phi(2d))/(2\,\mathrm{lcm}\,(e, n_d))$. *Then there are exactly* t *irreducible factors of* $f_m(X,a)$ *of degree* $\mathrm{lcm}\,(e, n_d)$ *so that any such factor is of the form (2). Moreover, if* $d > 2$ *is an odd divisor of* $2(m+1)$, *the set of all irreducible factors of* $f_m(X,a)$ *over* $\mathbb{F}_q$ *corresponding to* d *equals the set of all irreducible factors of* $f_m(X,a)$ *over* $\mathbb{F}_q$ *corresponding to* $2d$.

We note that the next lemma is an extension of [**2**, Lemma 3] as it includes all square $a \in \mathbb{F}_q$.

Lemma 2.4. *Let* $\eta(a) = 1$. *If* $f_k(X,a)$ *permutes* $\mathbb{F}_q$ *then either*

(i) $q \equiv \pm 3 \bmod 8$ *and* $(2(k+1), p(q^2-1)) = 8$, *or*

(ii) $(k+1, p(q^2-1)) = 2$.

Proof: As $f_k(X,a)$ permutes $\mathbb{F}_q$ then it has one linear factor. If p divides $k+1$ then $(x^2 - 4a) = (x + 2\sqrt{a})(x - 2\sqrt{a})$ divides $f_k(x,a)$. Therefore $(k+1, p) = 1$ and in Theorem 2.3 $k = m$. From (3) of Theorem 2.3 $f_k(X,a)$ is simple so each of its factors has multiplicity one.

Put $D = (2(k+1), q^2-1)$. If $D = 2$ then $(k+1, q^2-1) = 1$ and from Lemma 2.1 $f_k(X,a)$ has no linear factors. Let $d > 1$ be an odd prime divisor of D. As $(q-1, q+1) = 2$ then d divides one of $q-1$ or $q+1$ and $q \equiv \pm 1 \bmod d$. In Theorem 2.3 $n_d = 1$. From (6) of Theorem 2.3 $f_k(X,a)$ has $(\phi(d) + \phi(2d))/2 > 1$ linear factors over $\mathbb{F}_q$. This contradicts that $f_k(X,a)$ permutes $\mathbb{F}_q$, so $D = 2^r$ where $r > 1$.

Suppose that $d = 2^s$, where $s > 2$ is a divisor of D and $q \equiv \pm 1 \bmod d$. Then from (5b) of Theorem 2.3 $f_k(X,a)$ has $\phi(d)/2 > 1$ distinct linear factors over $\mathbb{F}_q$. Again this contradicts the permutation property of $f_k(X,a)$, so $D = 4$ and $(k+1, q^2-1) = 2$ which establishes (ii).

Now suppose $q \not\equiv \pm 1 \bmod d$ for any $d = 2^s$ dividing D where $s > 2$. In particular, $q \equiv \pm 3 \bmod 8$, so 8 is the highest power of 2 dividing $q^2 - 1$ and $(2(k+1), q^2-1) = 8$. This is the condition in (i). ∎

We could also have proven this lemma by combining [**2**, Lemma 3] and Lemma 1.2. [**2**, Lemma 4] can also be extended to all square $a \in \mathbb{F}_q$ by applying Lemma 1.2.

Lemma 2.5. *If* $f_k(X,a)$ *permutes* $\mathbb{F}_q$ *and* $\eta(a) = 1$ *then* $(k(k+2), q^2-1) = 1$ *if* $p = 3$ *and* $(k(k+2), q^2-1) = 3$ *otherwise.*

We have a result similar to Lemma 2.4 for non-square $a \in \mathbb{F}_q$.

Lemma 2.6. *Let* $\eta(a) = -1$. *If* $f_k(X,a)$ *permutes* $\mathbb{F}_q$ *then either*

(i) $q \equiv \pm 1 \bmod d$ *for all* $d > 4$ *dividing* $(2(k+1), q^2-1)$ *with* $d \equiv 0 \bmod 4$, *or*

(ii) $(k+1, q^2-1) = 2$.

Proof: As $f_k(x,a)$ permutes $\mathbb{F}_q$, it has exactly one linear factor. If $k+1$ is odd then from Lemma 2.2 $f_k(X,a)$ has no roots in $\mathbb{F}_q$. Therefore $k+1$ is even and X must be the

https://doi.org/10.1017/S0004972700031300 Published online by Cambridge University Press

only linear factor of $f_k(X,a)$ over $\mathbb{F}_q$. Put $k+1 = p^r(m+1)$ where $(m+1,p)=1$. From (1) $f_k(X,a) = f_m^{p^r}(X,a)(X^2-4a)^{(p^r-1)/2}$ and we can consider linear factors of $f_m(X,a)$ instead. From Theorem 2.3 part (3) $f_m(X,a)$ is simple so each factor has multiplicity one.

Let $D = \big(2(m+1), q^2-1\big)$. We have $D \equiv 0 \bmod 4$. Let d be a divisor of D such that $d \equiv 0 \bmod 4$ and $d > 4$. If $q \equiv \pm 1 \bmod d$ then in Theorem 2.3 $n_d = 1$ and there are no linear factors to be found, other then X. Part (i) now follows. If $q \not\equiv \pm 1 \bmod d$ then $n_d = 2$ (as d divides q^2-1) and there are $\phi(d)/2$ linear factors over $\mathbb{F}_q$ of $f_k(X,a)$. But this contradicts the permutation property of $f_k(X,a)$ as $d > 4$ so $\phi(d)/2 > 1$. Therefore $D = 4$ and $(k+1, q^2-1) = 2$, establishing part (ii). ∎

3. Linear factors of the DPSK where q is even

Throughout this section we assume q is even. We have the following result which is analogous to Lemma 2.1. The proof is omitted as it is similar to the proof of Lemma 2.1.

Lemma 3.1. *Let q be even. Then $f_k(X,a)$ has no roots in $\mathbb{F}_q$ if and only if* $\big(k+1, 2(q^2-1)\big) = 1$.

The following theorem is taken from [**1**].

Theorem 3.2. [Chou] *Let q be even and k be a positive integer. Fix $a \in \mathbb{F}_q$ and let $b \in \mathbb{F}_q$ satisfy $b^2 = a$. Write $k+1 = 2^r(m+1)$ where m is even and $r \geqslant 0$. For each divisor $d > 1$ of $m+1$ let n_d be the smallest integer satisfying $q^{n_d} \equiv \pm 1$ mod d. Then,*

(1) if $f \in \mathbb{F}_q[X]$ and $f(X) \neq X$, then f is an irreducible factor of $f_m(X,a)$ if and only if f is an irreducible factor of $f_k(X,a)$,

(2) for $m > 0$, $f_m(X,a) = h(X)^2$ where $h(X)$ is simple and $h(0) \neq 0$,

(3) X^{2^r-1} is a factor of $f_k(X,a)$ and any other irreducible factor of $f_k(X,a)$ has multiplicity 2^{r+1},

(4) for any divisor $d > 1$ of $m+1$ there are exactly $\phi(d)/(2n_d)$ irreducible factors of $f_m(X,a)$ over $\mathbb{F}_q$ with degree n_d so that any such factor is of the form

$$f(X) = \prod_{i=0}^{n_d-1} \left(x - b^{q^i}(\zeta_d + \zeta_d^{-1})^{q^i}\right)$$

where ζ_d is a primitive dth root of unity.

We have the following result which relies on the above theorem and is similar to Lemmas 2.4 and 2.6.

Lemma 3.3. *If q is even and $f_k(X,a)$ permutes $\mathbb{F}_q$ then $(k+1, q^2-1) = 3$ if $k+1$ is odd and $(k+1, q^2-1) = 1$ if $k+1$ is even.*

PROOF: As $f_k(X,a)$ permutes $\mathbb{F}_q$ it must have one linear factor over $\mathbb{F}_q$. Put $D = (k+1, q^2-1)$ and suppose $D > 1$. From part (3) of the previous theorem, X is a factor of $f_k(X,a)$ if and only if $k+1$ is even. Suppose that $k+1$ is odd. Put $d_1 = (k+1, q-1)$ and $d_2 = (k+1, q+1)$. At least one of d_1 or d_2 must be greater then 1. Now $q \equiv 1 \bmod d_1$ and $q \equiv -1 \bmod d_2$ which means $n_{d_1} = n_{d_2} = 1$ in Theorem 3.2.

Suppose that $d_1 > 1$. Using part (4) of Theorem 3.2 we obtain $\phi(d_1)/2$ distinct linear factors of $f_k(X,a)$ over $\mathbb{F}_q$. As $f_k(X,a)$ is a permutation polynomial of $\mathbb{F}_q$ then $\phi(d_1) = 2$ which means $d_1 = 3, 4$ or 6. As $k+1$ and $q-1$ are odd then $d_1 = 3$. Similarly, if $d_2 > 1$ then $d_2 = 3$. As 3 may only divide one of $q-1$ or $q+1$ then we deduce exactly one of d_1 or d_2 must be 3. Hence $D = 3$.

If $k+1$ is even then X is a factor of $f_k(X,a)$. Put $k+1 = 2^r(m+1)$ where $(m+1, 2) = 1$. From (1) $f_k(X,a) = X^{2^r-1} f_m^{2^r}(X,a)$. As $f_k(X,a)$ is a permutation polynomial $f_m(X,a)$ can have no linear factors, so from Lemma 3.1 $(m+1, q^2-1) = 1$. □

We do not include a proof of our final result as it can be established in much the same way as Lemma 2.5, see [**2**, Lemma 4].

LEMMA 3.4. *Let q be even and $f_k(X,a)$ permute $\mathbb{F}_q$. Then $\big(k(k+2), q^2-1\big) = 1$ if $k+1$ is odd and $\big(k(k+2), q^2-1\big) = 3$ if $k+1$ is even.*

REFERENCES

[1] W.S. Chou, 'The factorization of Dickson polynomials over finite fields', *Finite Fields Appl.* **3** (1997), 84–96.

[2] S.D. Cohen, 'Dickson polynomials of the second kind that are permutations', *Canad. J. Math* **46** (1994), 225–238.

[3] S.D. Cohen, 'Dickson permutations', in *Number-theoretic and algebraic methods in Computer Science (Moscow 1993)* (World Scientific Publishing, River Edge, NJ, 1995), pp. 29–51.

[4] M. Henderson and R. Matthews, 'Permutation properties of Chebyshev polynomials of the second kind over a finite field', *Finite Fields Appl.* **1** (1995), 115–125.

[5] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Maths **65** (Longman Scientific and Technical, Essex, England, 1993).

[6] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl. **20** (Addison-Wesley, Reading, 1983), (now distributed by Cambridge University Press).

[7] R. Matthews, *Permutation polynomials in one and several variables*, Ph.D. Thesis (University of Tasmania, Tasmania, Australia, 1982).

School of Information Technology
The University of Queensland
Queensland 4072 Australia
e-mail: marie@it.uq.edu.au