RESEARCH ARTICLE

*ScienceAsia* 28 (2002) : **401-405**

# Some New Classes of Permutation Polynomials

**Suphawan Janphaisaeng[a, *], Vichian Laohakosol[b] and Ajchara Harnchoowong[c]**

[a] Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok 65000, Thailand.

[b] Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand.

[c] Department of Mathematics, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand.

Corresponding author, E-mail: ??????

*Received 24 May 2001*
*Accepted 19 Mar 2002*

**ABSTRACT** The problem of characterizing permutation polynomials over a finite field is considered. New classes of permutation polynomials are derived extending earlier works of Lidl-Niederreiter, Small and Mollin-Small.

KEYWORDS: permutation polynomials, finite fields.

## INTRODUCTION

Let $F_q$ be a finite field with $q = p^n$ elements, where $p$ is prime and $n$ is a fixed positive integer. A polynomial $f(x) \in F_q[x]$ is said to be a **permutation polynomial** of $F_q$ if and only if it is a bijection map from $F_q$ to itself. The general study of permutation polynomials started with Hermite[1-3] who considered the case of finite prime fields. For the case of arbitrary finite fields, permutation polynomials were first systematically studied by Dickson.[1-3] Very little is known concerning which polynomials are permutation polynomials, despite the attention of numerous authors. Recently, permutations of finite fields have become of considerable interest in the construction of cryptographic systems for the secure transmission of data (see Lidl and Mullen[1]). One of the open problems mentioned in Lidl and Mullen[1, 2] is to find new classes of permutation polynomials of $F_q$. The objective of this paper is to derive some new classes of permutation polynomials extending earlier works of Lidl and Niederreiter[3], Small[4] and Mollin and Small.[5]

## LEMMAS

The following criterion, proved first by Hermite for $F_p$ and later by Dickson for $F_q$, is frequently used and provides an essential tool in discovering most permutation polynomials. Its proof can be found in Lidl and Niederreiter.[3]

**Hermite-Dickson Criterion.** A polynomial $f(x) \in F_q[x]$ is a permutation polynomial of $F_q$ if and only if the following two conditions hold:

(1) $f$ has exactly one root in $F_q$ ;
(2) for each integer $t$ with $1 \le t \le q-2$ and $t \not\equiv 0 \pmod p$, the reduction of $(f(x))^t \bmod (x^q - x)$ has degree $\le q-2$.

We first collect here some other auxiliary results that will be later used.

**Lemma A.** For $f, g \in F_q[x]$ we have $f(c) = g(c)$ for all $c \in F_q$ if and only if $f(x) \equiv g(x) \bmod (x^q - x)$.

**Proof.** See Lidl and Niederreiter.[3]

**Lemma B.** Let $a_0, a_1, a_2, \ldots, a_{q-1}$ be elements of $F_q$. Then the following two conditions are equivalent:

*(1)* $a_0 , a_1 , a_2 , \ldots, a_{q-1}$ are distinct;

$$(2)\ \sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & for \quad t = 0, 1, 2, \ldots, q-2; \\ -1 & for \quad t = q-1. \end{cases}$$

**Proof.** See Lidl and Niederreiter.[3]

**Lemma C.**

(1) Every linear polynomial over $F_q$ is a permutation polynomial of $F_q$.
(2) The monomial $x^i$ is a permutation polynomial of $F_q$ if and only if $gcd\ (i\ ,\ q-1) = 1$, where gcd denotes the greatest common divisor.

**Proof.** See Lidl and Niederreiter.[3]

**Lemma D.** Let $f(x) \in F_q[x]$ , $a \in F_q$ and $b \in F_q^*$. Then the following conditions are equivalent:

(1) $f$ permutes $F_q$;
(2) $f(x) + a$ permutes $F_q$;
(3) $bf(x)$ permutes $F_q$.

**Proof.** See Small.[4]

**Lemma E.** Let $f(x) = \sum_{i=1}^{n} c_i x^{m_i} \in F_q[x]$, where $m_n > m_{n-1} > ... > m_1 \geq 1$, $\prod_{i=1}^{n} c_i \neq 0$, and let $e = gcd\ (m_1, m_2, ..., m_n)$. Then $f(x)$ is a permutation polynomial of $F_q$ if and only if $gcd\ (e, q-1) = 1$ and $\sum_{i=1}^{n} c_i x^{m_i/e}$ is a permutation polynomial of $F_q$.

**Proof.** See Mollin and Small.[5]

**Lemma F.** Let $r$ be a positive integer with $gcd\ (r, q-1) = 1$ and let $s$ be a positive divisor of $q-1$. Assume $g \in F_q[x]$ is such that $g(x^s)$ has no nonzero root in $F_q$. Then $f(x) = x^r(g(x^s))^{(q-1)/s}$ is a permutation polynomial of $F_q$.

**Proof.** See Lidl and Niederreiter.[3]

**Lemma G.** Let $f(x) = x^{p^s} - ax^{p^r}$ where $s > r \geq 0$ and $a \in F_q^*$. Then

(i) $f$ permutes $F_q$ if and only if $a$ is not a $(p^s - p^r)^{th}$ power in $F_q$;
(ii) If $a$ is a primitive element in $F_q$ (ie, a generator for the multiplicative group $F_q^*$), then $f$ permutes $F_q$, unless $p = 2$ and $gcd\ (s-r, n) = 1$ where $q = p^n$.

**Proof.** See Small.[4]

## Results

The next two theorems are modifications of Theorem 7.10 in Lidl and Niederreiter[3], derived through further analyses of the original proof.

**Theorem 1.** Let $r$ be a positive integer and $s$ be a positive divisor of $q-1$. Let $h, g \in F_q[x]$ be such that $h(0) = 0$, $h(x^r)$ and $g(x^s)$ have no nonzero root in $F_q$. If for each integer $t$, $1 \leq t \leq q-2$, the degree of each term in $h(x^r)^t$ is not divisible by $s$, then $f(x) = h(x^r)(g(x^s))^{(q-1)/s}$ is a permutation polynomial of $F_q$.

**Proof.** We first show that $f$ has exactly one root in $F_q$. Consider $f(x) = 0$. Then $h(x^r) = 0$ or $(g(x^s))^{(q-1)/s} = 0$. Since $g(x^s)$ and $h(x^r)$ has no nonzero root in $F_q$, $x = 0$ is the only root of $f$. We next show that for each integer $t$, $1 \leq t \leq q-2$, the reduction of $(f(x))^t$ mod $(x^q - x)$ has degree $\leq q-2$.

*Case* 1. $s \mid t$, say $t = ks$ with integral $k$. Then $(f(x))^t = (h(x^r))^t(g(x^s))^{(q-1)k}$. Let $c \in F_q^*$.

Since $c^s \neq 0$ and $g(x^s)$ has no nonzero root in $F_q$, then $(g(c^s))^{q-1} = 1$. Thus $(f(c))^t = (h(c^r))^t$. Also $(f(0))^t = 0 = (h(0^r))^t$. By Lemma A, $(f(x))^t \equiv (h(x^r))^t \bmod (x^q - x)$. By assumption, each term in $(h(x^r))^t$ is of the form $ax^{ru}$ where $s \nmid ru$ and $a$ is a constant. Since $s \nmid ru$ and $s \mid (q-1)$, then $ru = (q-1)A + \beta$, where $A$ is integral and $0 < \beta \leq q-2$. Thus $x^{ru} = x^{(q-1)A+\beta} \equiv x^\beta \bmod (x^q - x)$.

*Case* 2. $s \nmid t$. Each term in $(h(x^r))^t$ is of the form $ax^{ru}$. Since $s \nmid ru$, then $(q-1) \nmid ru$. Thus $(f(x))^t$ is a sum of terms whose exponents are of the form $ru + sm$ where $m$ is a nonnegative integer. Since $s \nmid ru$ and $s \mid sm$, then $ru + sm = (q-1)A + \beta$ where $A$ is integral and $0 < \beta \leq q-2$. Thus $x^{ru+sm} = x^{(q-1)A+\beta} \equiv x^\beta \bmod (x^q - x)$.

In either case, the reduction of $(f(x))^t$ mod $(x^q - x)$ has degree $\leq q-2$. Hence, $f(x)$ is a permutation polynomial of $F_q$ by Hermite-Dickson criterion.

**Theorem 2.** Let $r$ be a positive integer and $s$ be a positive divisor of $q-1$ such that $gcd(\frac{r(q-1)}{s}, s) = 1$. Let $g \in F_q[x]$ be such that $g(x^s)$ has root only at 0 in $F_q$. Assume that for each integer $t$, $1 \leq t \leq q-2$, if $s \mid t$, then the reduction of $(g(x^s))^t$ mod $(x^q - x)$ has degree $\leq q-2$. Then $f(x) = g(x^s)x^{r(q-1)/s}$ is a permutation polynomial of $F_q$.

**Proof.** We first show that $f$ has exactly one root in $F_q$. Since $g(x^s)$ has no nonzero root in $F_q$, then 0 is the only root of $f$. We next show that for each integer $t$, $1 \leq t \leq q-2$, the reduction of $(f(x))^t$ mod $(x^q - x)$ has degree $\leq q-2$.

*Case* 1. $s \mid t$, say $t = ks$ with integral $k$. Then $(f(x))^t = (g(x^s))^t x^{(q-1)rk}$. Let $c \in F_q^*$. Then $(f(c))^t = (g(c^s))^t$ and $(f(0))^t = 0 = (g(0^s))^t$. By Lemma A, $(f(x))^t \equiv (g(x^s))^t \bmod (x^q - x)$.

*Case* 2. $s \nmid t$. Since each term in $(g(x^s))^t$ is of the form $ax^{su}$, then $(f(x))^t$ is a sum of terms whose exponents are of the form $su+\frac{rt(q-1)}{s}$. If $(q-1)/su+\frac{rt(q-1)}{s}$, then $s/\frac{rt(q-1)}{s}$, a contradiction.

Thus $su+\frac{rt(q-1)}{s}=(q-1)A+\beta$ where $A$ is integral and $0<\beta\le q-2$, and so $x^{su+rt(q-1)/s}=x^{(q-1)A+\beta}\equiv x^{\beta} \bmod (x^q-x)$.

In either case, the reduction of $(f(x))^t \bmod (x^q-x)$ has degree $\le q-2$. By Hermite-Dickson criterion, $f(x)$ is a permutation polynomial of $F_q$.

The next theorem gives a new class of permutation polynomials by removing an assumption on the coefficients in Theorem 2.5 of Mollin and Small.[5]

**Theorem 3.** Let $f(x) = ax^i + bx^j + c \in F_q[x]$, $a \neq 0$, $i > j \geq 1$. Assume that $-ba^{-1}$ is not an $(i-j)^{th}$ power in $F_q$. If $i-j = q-1$ and $gcd\ (j, q-1) = 1$, then $f(x)$ is a permutation polynomial of $F_q$.

**Proof.** By Lemma D we know that $f$ permutes $F_q \Leftrightarrow x^i + ba^{-1}x^j = x^j(x^{i-j} + ba^{-1})$ permutes $F_q$. Since $gcd\ (j, q-1) = 1$, $i-j = q-1$ and $-ba^{-1}$ is not an $(i-j)^{th}$ power in $F_q$, by Lemma F, $x^j(x^{i-j} + ba^{-1})$ is a permutation polynomial of $F_q$, and so is $f(x)$.

Since the hypothesis on $-ba^{-1}\beta^{-1}$ in Theorem 2.7 of Mollin and Small[5] is difficult to check, simplifying this condition, we get the following result.

**Theorem 4.** Let $f(x) = ax^i + bx^j + c \in F_q[x]$, $a \neq 0$, $i > j \geq 1$, $j \mid i$ and $gcd\ (j, q-1) = 1$.

(1) If $b = 0$, then $f$ permutes $F_q \Leftrightarrow gcd\ (i, q-1) = 1$;

(2) If $b \neq 0$, then $f(x)$ is not a permutation polynomial of $F_q$ provided that $x^{(i/j)-1} + ba^{-1}$ has a nonzero root in $F_q$.

**Proof.**

(1) Assume that $b = 0$. Then $f(x) = ax^i + c$. By Lemmas C and D, $f$ permutes $F_q \Leftrightarrow x^i$ permutes $F_q \Leftrightarrow gcd\ (i, q-1) = 1$.

(2) Assume that $b \neq 0$. Then $-ba^{-1} \neq 0$. By Lemma E, $x^i + ba^{-1}x^j$ permutes $F_q \Leftrightarrow x^{i/j} + ba^{-1}x = x(x^{(i/j)-1} + ba^{-1})$ permutes $F_q$. If $x^{(i/j)-1} + ba^{-1}$ has a nonzero root $\beta$ in $F_q$, then $x(x^{(i/j)-1} + ba^{-1})$ has both 0 and $\beta \neq 0$ as roots in $F_q$, so it is not a permutation polynomial of $F_q$.

The following theorem is an extension of Theorem 2.8 in Mollin and Small.[5]

**Theorem 5.** Let $f(x) = ax^k + bx^{k-2} + c \in F_q[x]$ with $k \geq 2$ and $a \neq 0$.

(1) For $q = 2$, $f$ permutes $F_q \Leftrightarrow b = 0$ or $k = 2$.

(2) Let $q = 3$. When $b = 0$, $f$ permutes $F_q \Leftrightarrow k$ is odd.
When b 0, $f$ permutes $F_q \Leftrightarrow k$ is odd and $ba^{-1} = 1$.

(3) Let $q > 3$.

(3.1) If $f$ permutes $F_q$, then either $b = 0$ or $q \not\equiv \pm 1 \pmod{k}$.

(3.2) Assume that $x^2 + ba^{-1}$ has a root in $F_q$.

(i) If $b = 0$, then $f$ permutes $F_q \Leftrightarrow gcd\ (k, q-1) = 1$.

(ii) If $b \neq 0$, then k > 2 implies $f(x)$ is not a permutation polynomial of $F_q$ while for $k = 2$, $F_q$ has characteristic 2 $\Leftrightarrow f$ permutes $F_q$.

**Proof.**

(1) Let $q = 2$.
Then $f$ permutes $F_q \Leftrightarrow x^{k-2}(x^2 + ba^{-1})$ permutes $F_q \Leftrightarrow$ either $b = 0$ or $k = 2$.

(2) Let $q = 3$. We have $f$ permutes $F_q \Leftrightarrow x^{k-2}(x^2 + ba^{-1})$ permutes $F_q$.

*Case* 2.1 $b = 0$.
Then $f$ permutes $F_q \Leftrightarrow x^k$ permutes $F_q$
$\Leftrightarrow gcd\ (k, 2) = 1$ (by Lemma C), ie $k$ is odd.

*Case* 2.2 $b \neq 0$. If $ba^{-1} = 2$, then $h(x) = x^{k-2}(x^2 + 2)$ is not a permutation polynomial of $F_q$ as $h(1) = 0 = h(0)$, which implies that $f$ is not a permutation polynomial of $F_q$. Assume that $ba^{-1} = 1$. If $k = 2$, then $f(x) = ax^2 + b + c$ and $f(x)$ is not a permutation polynomial of $F_q$ since $gcd\ (2, 3-1)\ 1$. Consider $k > 2$. Let $g(x) = x^{k-2}(x^2 + 2) \in F_q[x]$. Then $g(0) = 0$, $g(1) = 2$, $g(2) = 2^{k-1}$, so $g(x)$ is a permutation polynomial of $F_q$ if and only if $2^{k-1} \equiv 1 \pmod 3$, ie $k$ is odd. Hence $f$ permutes $F_q$ if and only if $k$ is odd.

(3) Let $q > 3$.

(3.1) By Lemma D, $f$ permutes $F_q \Leftrightarrow$ permutes $F_q$ where $\alpha = -ba^{-1}$. Assume that $f$ permutes $F_q$. Suppose that $q \equiv \pm 1 \pmod{k}$ and $b \neq 0$. Then $\alpha \neq 0$. Let

$$n = \frac{q \pm 1}{k}.$$

Then $n \neq q-1$. By Lemma

B and the fact that $f$ is a permutation polynomial of $F_q$, we have

$$0 = \sum_{w\in F_q} (w^k - \alpha w^{k-2})^n =$$

$$\sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{w\in F_q} w^{kn-2i}.$$

By Lemma B, if $kn - 2i \neq q - 1$, then $\sum_{w\in F_q} w^{kn-2i} = 0$. Assume that $kn - 2i = q - 1$. Either $kn = q - 1$ which implies $i = 0$, or $kn = q + 1$ which implies $i = 1$.Then either $kn = q - 1$, which yields

$$0 = \sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{w\in F_q} w^{kn-2i} = \sum_{w\in F_q} w^{q-1} = -1,$$

a contradiction, or $kn = q + 1$, which yields

$$0 = \sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{w\in F_q} w^{kn-2i} = n(-\alpha) \sum_{w\in F_q} w^{q-1},$$

so $0 = \sum_{w\in F_q} w^{q-1}$, a contradiction. Hence either $q \not\equiv \pm 1 \pmod{k}$ or $b = 0$.

(3.2) Assume that $x^2 + ba^{-1}$ has a root in $F_q$. We have that $f$ permutes $F_q \Leftrightarrow x^{k-2}(x^2 + ba^{-1})$ permutes $F_q$. By Lemma C, (i) is trivial. To show that (ii) holds, assume b ≠ 0. Then $ba^{-1} \neq 0$, so the root of $x^2 + ba^{-1}$ is not zero.

If $k > 2$, then $x^{k-2}(x^2 + ba^{-1})$ has at least two distinct roots, so $x^{k-2}(x^2 + ba^{-1})$ is not a permutation polynomials of $F_q$ and neither is $f$.

If $k = 2$, then $f$ permutes

$F_q \Leftrightarrow x^2 + ba^{-1}$ permutes $F_q$

$\Leftrightarrow gcd\,(2, q - 1) = 1$

$\Leftrightarrow q$ is even

$\Leftrightarrow F_q$ has characteristic 2.

Our next theorem gives an analysis of some classes larger than those in Proposition 6 of Small.[4]

**Theorem 6**. Let $f(x) = x^i - ax^j$, $i > j \geq 1$, $a$, and put $k = i - j$.

(1) For $i < q - 1$ and $k \geq 2$, if $i \mid (q - 1 + k)$ but $p \nmid \frac{q-1+k}{i}$, then $f(x)$ is not a permutation polynomial of $F_q$.

(2) Assume that $(q - 1) \mid k$ and $(q - 1)$ does not divide $i$, $i - k$, $2i$, $2i - k$, $2i - 2k$, ..., $(q - 2)i$, $(q - 2)i - k$, $(q - 2)i - 2k$, ..., $(q - 2)i - (q - 2)k$. Then $f(x)$ is a permutation polynomial of $F_q$ if and only if $a \neq 1$.

(3) If $(q - 1)$ does not divide $(q - 1)i - k$, $(q - 1)i - 2k$, $(q - 1)i - 3k$, ..., $(q - 1)i - (q - 2)k$, then $f(x)$ is not a permutation polynomial of $F_q$.

**Proof.** (1) Let $i < q - 1$ and $k \geq 2$. Since $2 \leq k < i < q - 1$, then $q > 3$. Assume that $i \mid (q - 1 + k)$ and $p \nmid \frac{q-1+k}{i}$, say $ir = q - 1 + k$. If $r = 1$, then $i = q - 1 + k \geq q - 1$ which contradicts $i < q - 1$.Thus $r > 1$. Now $r \leq k(r - 1) = kr - k > ir - k = q - 1$. Suppose that $f(x)$ is a permutation polynomial of $F_q$. By Lemma B,

$$0 = \sum_{w\in F_q} (w^j - aw^j)^r = \sum_{t=0}^{r} \binom{r}{t} (-a)^t \sum_{w\in F_q} w^{i(r-t)+jt}.$$

Since $i(r - t) + jt = ir - kt = q - 1 + (1 - t)k$, the $w$-exponents in the sum, for $t = 0, 1, \ldots\ldots, r$, are $q - 1 + k, q - 1, q - 1 - k, q - 1 - 2k, \ldots, q - 1 - (r - 1)k$. Thus

$$0 = \sum_{t=0}^{r} \binom{r}{t} (-a)^t \sum_{w\in F_q} w^{i(r-t)+jt} = ra, \text{ so } p \mid r, \text{ a contradiction.}$$

(2) Assume that $(q - 1) \mid k$ and $(q - 1)$ does not divide $i$, $i - k$, $2i$, $2i - k$, $2i - 2k$, ..., $(q - 2)i$, $(q - 2)i - k$, $(q - 2)i - 2k$, ..., $(q - 2)i - (q - 2)k$. By Lemma B we have that $f$ permutes

$$F_q \Leftrightarrow \sum_{w\in F_q} (w^j - aw^j)^t = \begin{cases} 0 & for \quad t = 0, 1, \ldots, q-2, \\ -1 & for \quad t = q-1. \end{cases}$$

Analyzing each separate case, we have

$$t = 0: \quad \sum_{w\in F_q} (w^j - aw^j)^t = \sum_{w\in F_q} 1 = 0.$$

$$t = 1: \quad \sum_{w\in F_q} (w^j - aw^j)^t = \binom{1}{0} \sum_{w\in F_q} w^j + \binom{1}{1} (a) \sum_{w\in F_q} w^{j-k} = 0.$$

$$\vdots$$

$$t = q - 2: \quad \sum_{w\in F_q} (w^j - aw^j)^t = \binom{q-2}{0} \sum_{w\in F_q} w^{(q-2)i} +$$

$$\binom{q-2}{1}(-a)\sum_{w\in F_q} w^{(q-2)i-k}+\ldots$$

$$+\binom{q-2}{q-2}(-a)^{q-2}\sum_{w\in F_q} w^{(q-2)i-(q-2)k}=0.$$

$$t=q-1:\quad \sum_{w\in F_q}(w^i-aw^j)^t=\binom{q-1}{0}\sum_{w\in F_q} w^{(q-1)i}+$$

$$\cdot\binom{q-1}{1}(-a)\sum_{w\in F_q} w^{(q-1)i-k}+\ldots$$

$$+\binom{q-1}{q-1}(-a)^{q-1}\sum_{w\in F_q} w^{(q-1)i-(q-1)k}=(-1)(1-a)^{q-1}.$$

If $a = 1$, then $\sum_{w\in F_q}(w^i-aw^j)^{q-1}=0$, implying that $f(x)$ is not a permutation polynomial of $F_q$. If $a \neq 1$, then $\sum_{w\in F_q}(w^i-aw^j)^{q-1}=-1$, so $f(x)$ is a permutation polynomial of $F_q$.

(3) Assume that $(q-1)$ does not divide $(q-1)i-k$, $(q-1)i-2k$, $(q-1)i-3k$, ..., $(q-1)i-(q-2)k$. From the proof of (2), $\sum_{w\in F_q}(w^i-aw^j)^{q-1}=(-1)+(-a)^{q-1}(-1)\neq 1$, so $f(x)$ is not a permutation polynomial of $F_q$.

Our last theorem is an extension of Proposition 8(b) in Small.[4]

**Theorem 7.** Let $a$ be a primitive element in $F_q$, $q = p^n$ and $f(x)=x^{p^s}-ax^{p^r}$, where $s > r \geq 0$. Then $f$ permutes $F_q \Leftrightarrow$ one of the following conditions holds:

(1) $p > 2$;
(2) $p = 2$ and $gcd(s-r, n) > 1$.

**Proof.** From Lemma G(i), $f$ permutes $F_q \Leftrightarrow a$ is not a $(p^s-p^r)^{th}$ power in $F_q$. We claim that $a$ is not a $k^{th}$ power in $F_q \Leftrightarrow gcd(k, q-1) = d > 1$. Assume $d = 1$. Then $uk + v(q-1) = 1$ for some integers $u$, $v$. Thus $a = a^{uk+(q-1)v} = a^{uk}$. Since $a$ is a primitive element, $a^u = w$ for some $w \in F_q$, yielding $a = w^k$, a $k^{th}$ power. Assume that $a = w^k$ for some $w \in F_q$. Since $a(\neq 0)$ is a primitive element, $w = a^u$ for some integer $u$, $1 \leq u \leq q-1$. Then $a^{uk-1} = 1$. Thus $uk - 1 = (q-1)v$ for some integer $v$. Since $d \mid k$ and $d \mid (q-1)$, then $d = 1$, and the claim is proved. From this claim we deduce that

$f$ permutes $F_q \Leftrightarrow gcd(p^s-p^r, q-1) > 1$.

*Case* 1. $p = 2$. Then

$gcd(p^s-p^r, q-1) = gcd(2^r(2^{s-r}-1), 2^n-1) = gcd(2^{s-r}-1, 2^n-1) = 2^{gcd(s-r,n)}-1$.

Thus $gcd(p^s-p^r, q-1) = 1 \Leftrightarrow gcd(s-r, n) = 1$.

*Case* 2. $p \neq 2$. Then

$gcd(p^s-p^r, q-1) = gcd(p^r(p^{s-r}-1), p^n-1) = gcd(p^{s-r}-1, p^n-1)$.

Since $p \neq 2$, then $gcd(p^s-p^r, q-1) \geq 2 > 1$, and the result follows.

## Conclusion

Seven classes of permutation polynomials are derived. The first two classes, which are products of two polynomials, are modifications of those due to Lidl and Niederreiter in 1983. The next three classes, which are polynomials with three terms, are extensions of those due to Mollin and Small in 1987. The last two classes, which are polynomials with two terms, are extensions of those due to Small in 1990.

## References


1. Lidl R and Mullen GL (1988) When does a polynomial over a finite field permute the elements of the field?. *Amer Math Monthly* **95**, 243-6.
2. Lidl R and Mullen GL (1993) When does a polynomial over a finite field permute the elements of the field?, II *Amer Math Monthly* **100**, 71-4.
3. Lidl R and Niederreiter H (1993) *Finite Fields*, pp 347-393. Addison-Wesley, Reading, MA.
4. Small C (1990) Permutation binomials. *Internat J Math and Math Sci* **13**, 337-42.
5. Mollin RA and Small C (1987) On permutation polynomials over finite fields. *Internat J Math and Math Sci* **10**, 535-44.