SOME CRITERIA FOR PERMUTATION BINOMIALS

PRE-PRINT (SEPT 1997)

Alberto Cáceres and Omar Colón-Reyes
University of Puerto Rico at Humacao
Mathematics Department
CUH Station, Humacao P.R. 00791

Abstract

We present necessary and sufficient conditions for a binomial $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ over a finite field F_q of odd characteristic to be a permutation function on $F_q^* = F - \{0\}$. When it is so, the "inverse" polynomial, in the sense of functions, is also a binomial of the same form, $x^{q-2} + Ax^{\frac{q-3}{2}}$. We also determine when f is self-invertible and otherrwise find the inverse. For prime fields Z_p we can express the criterion in terms of quadratic residues and make the complete classification for every B in Z_p.

Keywords - Finite Fields, Permutation Polynomials, Quadratic Residues.

§1. Introduction

Ever since Lidl and Mullen, in 1988, presented their AMM Unsolved Problems paper [L-M] asking when a polynomial permutes the elements of a finite field, there has been incresed interest in finding good algorithms, see [M-vzG], and new criteria, see [MAC] and [T], to determine whether a given polynomial $f(x)$ over a finite field F_q is a permutation polynomial. With this paper we intend to give criteria for particular binomials and thus make a contribution to [L-M]'s open problem P2.

The most simple criterion for permutation polynomials (PP) comes from group theory. Any power x^n determines a multiplicative group homomorphism $F_q \to F_q$, hence the monomial ax^n is a permutation polynomial if and only if $a \neq 0$ and $gcd(n, q-1) = 1$, see [L-M] and [L-N]. It is the Hermite-Dickson's (HD) the most general criterion to determine if a polynomial is a PP. However its application requires checking $q-1$ polynomial power sums which must be reduced modulo $x^q - x$, and whose number clearly increases according to the field size. Thus, although powerful, HD is not workable. even with appropriate computer software.

After monomials, binomials. Niederreiter and Robinson present a criterion for permutation binomials of the form $ax^k + bx$, see [N-R, Lemmas 2 and 4], which they essentially use to announce for which fields no permutation binomials of that type should be expected. Other binomials are presented by Small, [Sm] who under certain conditions proves that a binomial $ax^r + bx^s + c$ over F_q is a PP if and only if $b = 0$. The addition or deletion of an independent term c does not change the bijectitvity attribute of the polynomial, thus Small binomials are essentially monomials. However, in [Sm] a necessary condition for a binomial $ax^r + bx^s$ to be a PP appears hidden in the arguments, namely $gcd(r-s, q-1)$ must be $\neq 1$. For sake of completedness we will make it explicit.

A genuine binomial has the form $ax^r + bx^s$ with $ab \neq 0$ and $r \neq s$. It is a permutation polynomial if and only if $x^r + \frac{b}{a}x^s$ is so, see [L-N, Theorem 7.8]. Also as a direct consequence of HD a reduced PP must have degree $\leq q-2$, [L-M]. So, our binomials will be monic, $x^r + Bx^s$ with $B \neq 0$ and $0 < s < r < q-1$. More precisely we will use $r = q-2$ and $r - s = \frac{q-1}{2}$, hence $s = \frac{q-3}{2}$.

For those binomials, $x^{q-2} + Bx^{\frac{q-3}{2}}$, we prove that when they are permutation polynomials, their inverses, as mappings (polynomials, by the Lagrange interpolation, [L-N]) enjoy the same form $x^{q-2} + Ax^{\frac{q-3}{2}}$, and we obtain explicit formulae to calculate the coefficient A.

Furthermore we present necessary and sufficient conditions for a binomial of the form $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$, over a finite field $F_q = GF(q)$ to be a permutation binomial (PB). For any finite field F_q, of odd characteristic, we can make the complete classification of the binomials $x^{q-2} + Bx^{\frac{q-3}{2}}$, as not invertible, invertible and self invertible. For prime fields, the condition can be expressed in terms of quadratic residues.

Two ilustrative examples are $x^5 + 2x^2$ over $F = Z_7$ whose inverse is $x^5 + 5x^2$, and $x^{11} + 11x^2$ over Z_{13} which is its own inverse (self-invertible). Moreover we generate more permutation binomials using the Frobenius automorphism.

Finally we look at some famous primes for which our criterion will tell when to obtain or when not to expect certain permutation binomials.

§2. **Basic Results**

The Hermite-Dickson (H-D, c. 1908) is the best known criterion for permutation polynomials and we state it here for sake of completedness. However for our present analysis it is more appropriate to refer to the finite field characterization in the lemma which is key to the criterion. We present both as propositions.

Proposition 1. (HD criterion) Let F_q be of characteristic p. Then $f(x)$ is a permutation polynomial over F_q if and only if the following two conditions hold:

i) f has a unique root in F_q;

ii) For each integer t, $1 \leq t \leq q-2$, $t \not\equiv 0 (\text{mod } p)$ the reduction of $f(x)^t \pmod{x^q - x}$ has degree $\leq q-2$. ∎

Proposition 2. (Lemma) Let $S = \{a_0, a_1, \ldots, a_{q-1}\}$ be a set of q, not necessarily distinct elements in a finite filed F_q. Then $S = F_q$ if and only if:

i) $\sum_{i=0}^{q-1} a_i^k = 0$ for $k = 0, 1, \ldots, q-2$

ii) $\sum_{i=0}^{q-1} a_i^{q-1} = -1$ ∎

We will also make use of a known combinatorial fact which we present as Proposition 3. See [Sm, Exs. 2.9, pag. 45]

Proposition 3. If q is a power of an odd prime p then for $0 \leq j \leq q-1$

$$\binom{q-1}{j} \equiv (-1)^j \pmod{p}$$

If q is a power of 2, the same statement is true and simplifies to $\binom{q-1}{j} \equiv (-1)^j \equiv 1 \ (mod\ 2)$ for $0 \leq j \leq q-1$ ∎

As observed before, reduced permutation polynomials have degree $\leq q-2$. We will prove that a permutation polynomial and its inverse polynomial share the coefficient of degree $q-2$

Let us recall that for any finite field F_q, any mapping $\psi : F_q \to F_q$, by the Lagrange Interpolation Theorem. [L-N], can be written as a polynomial

$$\psi(x) = \sum_{a \in F} \psi(a)[1 - (x-a)^{q-1}]$$

which when applied to the inverse of a permutation polynomial, allows us to write:

$$\psi^{-1}(x) = \sum_{a \in F} a[1 - (x - \psi(a))^{q-1}]$$

and this is the formula we will expand to determine the coefficients of $f^{-1}(x)$.

Theorem 1. For every permutation polynomial f over a finite field F_q, $f(x)$ and $f^{(-1)}(x)$ share the coefficient of degree $q-2$

Proof: Let $F_q = \{a_0, a_1, \ldots, a_{q-1}\}$. If ψ is a permmutation polynomial, as a permutation it can be written:

$$\psi = \begin{pmatrix} a_0 & a_1 & \ldots & a_{q-1} \\ \psi(a_0) & \psi(a_1) & \ldots & \psi(a_{q-1}) \end{pmatrix}$$

and, of course, its inverse permutation ψ^{-1} can be written:

$$\psi = \begin{pmatrix} \psi(a_0) & \psi(a_1) & \ldots & \psi(a_{q-1}) \\ a_0 & a_1 & \ldots & a_{q-1} \end{pmatrix}.$$

Using the Lagrange Interpolation Theorem, we can write $\psi^(x)$ and $\psi^{-1}(x)$ as

$$\psi(x) = \sum_{i=0}^{q-1} \psi(a_i)[1 - (x-a_i)^{q-1}]$$

$$\psi^{-1}(x) = \sum_{i=0}^{q-1} a_i[1 - (x - \psi(a_i))^{q-1}]$$

Expanding $\psi(x)$ and $\psi^{-1}(x)$ by the Binomial Theorem as sums of powers of x and collecting terms we obtain the coefficient A_{q-2} of the polynomial $\psi(x)$ as:

$$A_{q-2} = \binom{q-1}{q-2} \sum_{i=0}^{q-1} a_i^1 \psi(a_i) = (q-1) \sum_{i=0}^{q-1} a_i \psi(a_i)$$

Analogously for $\psi^{-1}(x)$ we can write the coefficient B_{q-2} as:

$$B_{q-2} = \binom{q-1}{q-2} \sum_{i=0}^{q-1} \psi(a_i)^1 a_i = (q-1) \sum_{i=0}^{q-1} \psi(a_i) a_i$$

and they are equal, ending the proof. ∎

§3. **Binomials** $x^{q-2} + Bx^{\frac{q-3}{2}}$

Let us first state as a Theorem a necessary condition for a binomial to be a PP.

Theorem 2. If $f = x^r + Bx^s$, $0 < s < r < q-1$, $B \neq 0$, is a permutation polynomial over F_q, then $gcd(r-s, q-1) \neq 1$.

Proof: We factor f as $f = x^s(x^{r-s} + B)$ and if $gcd(r-s, q-1) = 1$, x^{r-s} is a PP. Hence $x^{r-s} + B$ has a non zero root, giving to f too many zeroes. This contradicts HD proposition 1 part i) ∎

So, for permutation polynomials $f = x^r + Bx^s$ which by Theorem 2 must satisfy $gcd(r-s, q-1) \neq 1$ we choose to explore the case $r = q-2$ and $r - s = \frac{q-1}{2}$, $s = \frac{q-3}{2}$ follows, and we prove that for a binomial of the form $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$, its inverse, as a function, is also a binomial sharing the same exponents. Permutation binomials of this form do exist for any field of odd characteristics $p \leq 7$, as is the case of $x^5 + 2x^2 \in F_7[x]$ whose inverse is $x^5 + 5x^2$, and $x^{11} + 3x^5 \in F_{13}[x]$, which is its own inverse.

Theorem 3. Let $F = F_q$ be a field of odd characteristic and $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ be a permutation binomial. Then its inverse (as a function) is also a binomial $f{-}1(x) = x^{q-2} + Ax^{\frac{q-3}{2}}$ for some $A \in F$.

Proof: The Binomial Theorem and Proposition 2 permit us to expand and suitably simplify the Lagrange forrmula (1) as:

$$\begin{aligned}
f^{-1}(x) &= \sum_{a\in F} a(1-(x-f(a))^{q-1}) \\
&= \sum_{a\in F} a - \sum_{a\in F} a(x-f(a))^{q-1}) \\
&= -\sum_{a\in F} a \sum_{k=0}^{q-1} \binom{q-1}{k} x^k f(a)^{q-1-k}) \\
&= \sum_{k=0}^{q-1} \left[(-1)^{k+1} \binom{q-1}{k} \sum_{a\in F} a f(a)^{q-1-k} \right] x^k \\
&= \sum_{k=0}^{q-1} \left[(-1)^{k+1} \binom{q-1}{k} \sum_{a\in F} a(a^r + Ba^s)^{q-1-k} \right] x^k \\
&= \sum_{k=0}^{q-1} \left[(-1)^{k+1} \binom{q-1}{k} \sum_{a\in F} a \sum_{i=0}^{q-1-k} \binom{q-1-k}{i} a^{ri} (Ba^s)^{q-1-k-i} \right] x^k \\
&= \sum_{k=0}^{q-1} \left[(-1)^{k+1} \binom{q-1}{k} \sum_{i=0}^{q-1-k} \binom{q-1-k}{i} a^{ri} B^{q-1-k-i} \sum_{a\in F} a^{1+ri-sk-si} \right] x^k
\end{aligned}$$

and applying Proposition 3 to the first binomial coefficient we can shorten the formula to

$$f^{-1}(x) = \sum_{k=0}^{q-1} \left[\sum_{i=0}^{q-1-k} \binom{q-1-k}{i} B^{q-1-k-i} \left(-\sum_{a\in F} a^{1+ri-sk-si} \right) \right] x^k \tag{2}$$

showing f^{-1} in the standard polynomial appearance $\sum_k c_k x^k$. In order to prove that it is indeed a binomial, we need to show that $c_k = 0$ except for the coefficients of degrees $q-2$ and $\frac{q-3}{2}$.

Remember that the inner sums $\sum_{a\in F} a^{1+ri-sk-si}$ are 0, except when

$$1 + ri - sk - si \equiv 0(mod\ q-1), \tag{3}$$

in which case it is -1. See [Se]. For the particular case $r = q-2$ and $s = \frac{q-3}{2}$ we have $r - s = \frac{q-1}{2}$ and hence the LHS of (3) can be written as

$$1 + (r-s)i - sk = 1 + \frac{q-1}{2}i - \frac{q-3}{2}k = 1 + k - \frac{q-1}{2}(k-i)$$

i.e., $1 + k \equiv \frac{q-1}{2}(k-i)(mod\ q-1)$. Multiplication by 2 in odd characteristic does not harm the congruence and we obtain $2(1+k) \equiv (q-1)(k-i)(mod\ q-1)$ and of course $2(1+k) \equiv 0(mod\ q-1)$.

Now, since $0 \leq k \leq q-1$, the range of $2(k+1)$ is $2 \leq 2(k+1) \leq 2q$. Thus for $2(k+1)$ there are but two cases of congruence to 0 modulo $q-1$ and they are $2(k+1) = q-1$ and $2(k+1) = 2(q-1)$. The first one yields $k = \frac{q-3}{2}$ and the second, $k = q-2$. Only for these cases we have nonzero coefficientes in (2), and that proves that the inverse is indeed a binomial with terms of degrees $q-2$ and $\frac{q-3}{2}$. Now by Theorem 2 we know that $c_{q-2} = 1$. ∎

But we can follow the formulas and explicitly compute c_{q-2} and $c_{\frac{q-3}{2}}$.

For $k = q-2$, the range of i, the binomial coefficient index in (2), must be $0 \leq i \leq q-1-k = q-1-(q-2) = 1$, i.e., $i = 0$ or $i = 1$. From the same formula, the nonzero terms correspond to the solution of the congruence (3), which for the explicit values $r = k = q-2$ and $s = \frac{q-3}{2}$ becomes:

$$1 + (q-2)i - \frac{q-3}{2}(q-2) - \frac{q-3}{2}i \equiv 0(\text{mod } q-1)$$

which can be arranged as

$$1 + \frac{q-1}{2}i \equiv \frac{q+1}{2} + \frac{q-5}{2}(q-1)(\text{mod } q-1)$$

and since $q-5$ is even, it simplifies to

$$1 + \frac{q-1}{2}i \equiv \frac{q+1}{2}(\text{mod } q-1).$$

Clearly the congruence holds for $i = 1$ but fails for $i = 0$. Hence we compute in (2) the coefficient c_{q-2} with the sole summand for $i = 1$:

$$c_{q-2} = \binom{q-1-(q-2)}{1} B^{q-1-(q-2)-1}(-1) = 1,$$

as expected. For $k = \frac{q-3}{2}$ we invoke again the congruence (3) and obtain

$$1 + \frac{q-1}{2}i - \frac{q-3}{2} \cdot \frac{q-3}{2} \equiv 0(mod\ q-1)$$

and a suitable simplificacion produces $\frac{q-1}{2}i \equiv \left(\frac{q-3}{2}\right)^2 (mod\ q-1)$ or better $\frac{q-1}{2}\left(\frac{q-1}{2} - i\right) \equiv 0(mod\ q-1)$. The values of i solving this coongruence are clearly those making $\frac{q-1}{2} - i$ an even number, i.e., they must have the same parity as $\frac{q-1}{2}$ and that depends on whether $q \equiv 1(mod\ 4)$, in which case they must be even, or odd when $q \equiv 3(mod\ 4)$. Being i an index in the binomial coefficients of the formula (2) its range is determined by the binomial power, in this case $q-1-k = q-1-\frac{q-3}{2} = \frac{q+1}{2}$.

Now we have the form of the values of i and the range of them and are ready to compute the inverse of f. Unwilling to further annoy the reader with repeated calculations we present only the result of the complete computation of the inverse of a permutation binomial of the form $x^{q-2} + Bx^{\frac{q-3}{2}}$. We also present two examples.

Theorem 4. Let F_q be a finite field of odd characteristic and $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ a permutation binomial. Then the inverse of f, in the sense of mappings, is also a monic binomial of the form $f^{-1}(x) = x^{q-2} + Ax^{\frac{q-3}{2}}$ where

$$A = \begin{cases} \sum_{j=0}^{\frac{q-1}{4}} \binom{\frac{q+1}{2}}{2j} B^{\frac{q+1}{2}-2j}, & if\ q \equiv 1 (\text{mod } 4) \\ \sum_{j=0}^{\frac{q-1}{4}} \binom{\frac{q+1}{2}}{2j} B^{\frac{q-1}{2}-2j}, & if\ q \equiv 3 (\text{mod } 4) \end{cases}$$

■

Example 1. In F_{11}, $f(x) = x^9 + 8x^4$ is a permutation polynomial. So,

$$A = \binom{6}{1} B^5 + \binom{6}{3} B^3 + \binom{6}{5} B = 6 \times 8^5 + 20 \times 8^3 + 6 \times 8 (\text{mod } 11) = 8$$

showing f as its own inverse.

Example 2. In $GF(3^2)$, we use the primitive element *alpha*, satisfying the equation $\alpha^2 = 2\alpha + 1$ and consider the binomial $f(x) = x^7 + \alpha^2 x^3$ which is a permutation binomial. Here the coefficient is $B = \alpha^2$. In order to calculate A we refer to Theorem 3 and identify $q = 9$, $\frac{q-1}{4} = 2$, $\frac{q+1}{4} = 5$, and of course we choose the formula for $q \equiv 1 \text{ mod } 4$. In that case the computation is

$$\begin{aligned} A &= \sum_{j=0}^{2} \binom{5}{2j} B^{5-2j} \\ &= \binom{5}{0} B^5 + \binom{5}{2} B^3 + \binom{5}{4} B \\ &= (\alpha^2)^5 + 10(\alpha^2)^3 + 5\alpha^2 \\ &= \alpha^{10} + \alpha^6 + 2\alpha^2 (\text{mod } 3) \\ &= 2\alpha + 1 + \alpha + 2 + \alpha + 2 = \alpha + 2 \end{aligned}$$

therefore, $f^{-1}(x) = x^7 + (\alpha + 2)x^3$.

Note: A successful computation of A from B is not sufficient to ensure that f is a permutation polynomial. However, simpler criteria for $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ to be a permutation binomial, in terms of B and quadratic residues, are presented below and are our main results.

§4. **Criteria for a Class of Permutation Binomials**

Let F_q be a field of odd characteristic. We suppose that the binomial $f(x) = x^r + Bx^s$ over F_q has an inverse $f^{-1}(x)$, which is also a binomial $f^{-1}(x) = x^r + Ax^s$. For f and f^{-1} to be mutual inverses as functions they must satisfy $f(f^{-1}(x))) = x$ and $f^{-1}(f(x))) = x$ for all x. By using the first equation we have:

$$(x^r + Ax^s)^r + (x^r + Bx^s)^s = x$$

$$[x^s(x^{r-s} + A)]^r + B[x^s(x^{r-s} + A)]^s = x$$

$$x^{sr}(x^{r-s}+A)^r + Bx^{s^2}(x^{r-s}+A)^s = x \tag{4}$$

and this last identity will be the basis of our proofs.

By Theorem 3, if $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ is a PP then $f^{-1}(x)$ is another binomial $f^{-1}(x) = x^{q-2} + Ax^{\frac{q-3}{2}}$. The relationship between A and B is now simpler and better stated in the following lemma which enormously improves Theorem 4. In what follows, B or A will be referred as "the coefficient".

Lemma 1. Let $r = q-2$ and $s = \frac{q-3}{2}$ and $B \neq 0$. If $f(x) = x^r + Bx^s$ over F_q is a permutation binomial then the coefficient A of $f^{-1}(x) = x^{q-2} + Ax^{\frac{q-3}{2}}$ is B or $-B$.

Proof: For any $x \in F_q$ equation (4) holds and in particular for $x = 1$ we have $(1+A)^r + B(1+A)^s = 1$ which we multiply by $(1+A)$ and obtain $(1+A)^{r+1} + B(1+A)^{s+1} = 1+A$. Observe that $r+1 = q+1$ and $s+1 = \frac{q+1}{2}$, hence $1 + B(1+A)^{\frac{q+1}{2}} = 1 + A$, i.e.,

$$(1+A)^{\frac{q+1}{2}} = \frac{A}{B} \tag{5}$$

The LHS of this equation is the square root of 1, thus for $1 + A \neq 0$ it is either 1 or -1, hence $A = B$ or $A = -B$. ∎

This lemma establishes that if $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ is a PP there are only two possibilities for $f^{-1}(x)$. It is either $f(x)$, in which case it is self invertible, or $f^{-1}(x) = x^{q-2} - Bx^{\frac{q-3}{2}}$.

Example 3: In F_{13}, $f(x) = x^{11} + 6x^5$ is PB and $f^{-1}(x) = x^{11} + 7x^5$. Also $f(x) = x^{11} + 2x^5$ is PB and self invertible.

Note that 13 is an odd prime of the form $4n+1$, and $B = 2$ determines that $f(x)$ is self invertible. Also with $B = 6$ the *coefficient* of the inverse polynomial is $-6 = 7 \in F_{13}$, according to Lemma 1. The following theorem presents these results for q of the form $4n + 1$

Theorem 5. Let $q = 4n + 1$, $r = q - 2$, $s = \frac{q-3}{2}$, $B \neq 0$

i) The binomial $x^r + Bx^s$ over F_q is a permutation binomial and self-invertible if and only if

$$(B+1)^{\frac{q-1}{2}} = (B-1)^{\frac{q-1}{2}} = 1$$

ii) The binomial $x^r + Bx^s$ over F_q is a permutation binomial with inverse $f^{-1}(x) = x^r - Bx^s$ if and only if

$$(B+1)^{\frac{q-1}{2}} = (B-1)^{\frac{q-1}{2}} = -1$$

Proof: i) Since q is odd, $rs = (q-2)\frac{q-3}{2} = (q-1)\frac{q-5}{2} + \frac{q-1}{2} + 1$, hence $rs \equiv \frac{q+1}{2} + 1 \bmod (q-1)$. Also, $s^2 = (\frac{q-3}{2})^2 = (\frac{q-1}{2} - 1)^2 = (2n-1)^2 = 4n^2 - 4n + 1 = 1 (\bmod\ q-1)$, hence $s^2 \equiv 1 (\bmod\ q-1)$. Then Eqn. (4) can be written as:

$$x^{\frac{q-1}{2}} \cdot x(x^{\frac{q-1}{2}} + B)^{q-2} + B \cdot x(x^{\frac{q-1}{2}} + B)^{\frac{q-3}{2}} = x \tag{6}$$

For $x \neq 0$, $x^{\frac{q-1}{2}} = \pm 1$, hence we have two alternatives. If $x^{\frac{q-1}{2}} = 1$ (e.g. $x = 1$), Eqn (6) reduces to $(B+1)^{\frac{q-1}{2}}$ as in Eqn 5. But if $x^{\frac{q-1}{2}} = -1$ the same simplification changes Eqn. (6) to $-x(B-1)^r + Bx(B-1)^s = x$, i.e.,$(B-1)^r + B(B-1)^s = 1$. Multiplying by $(B-1)$ we obtain $(B-1)^{\frac{q-1}{2}} = 1$

Conversly, if $(B-1)^{\frac{q-2}{2}} = (B+1)^{\frac{q-1}{2}} = 1$ we want to prove that f is self-invertible, i.e., $f(f(x)) = x$, So,

$$f(f(x)) = x^{\frac{q-1}{2}} \cdot x(x^{\frac{q-1}{2}} + B)^{q-2} + Bx(x^{\frac{q-1}{2}} + B)x^{\frac{q-3}{2}}.$$

For $x \in F_q$ such that $x^{\frac{q-1}{2}} = 1$ we have:

$$f(f(x)) = x(B+1)^{q-2} + Bx(B+1)^{\frac{q-3}{2}} = x(B+1)x^{\frac{q-3}{2}}[(B+1)^{\frac{q-1}{2}} + B]$$

but we know that $(B+1)^{\frac{q-1}{2}} = 1$ and hence we obtain $f(f(x)) = x(B+1)^{\frac{q-3}{2}}(B+1)$, which simplifies as:

$$f(f(x)) = x(B+1)^{\frac{q-3}{2}+1} = x(B+1)^{\frac{q-1}{2}} = x \cdot 1 = x$$

and for $x \in F_q$ such that when $x^{\frac{q-1}{2}} = -1$, doing the simplifying with $(B-1)^{\frac{q-1}{2}} = 1$ we obtain $f(f(x)) = x$ and that completes the proof of $i)$

$ii)$ By Lemma 1, we select $A = -B$ and we write:

$$f(f(x)) = x^{\frac{q-1}{2}} \cdot x(x^{\frac{q-1}{2}} + B)^{q-2} - Bx(x^{\frac{q-1}{2}} + B)^{\frac{q-3}{2}} = x \tag{7}$$

If $x^{\frac{q-1}{2}} = 1$, Eqn. (7) changes to $x(1+B)^{q-2} - Bx(1+B)^{\frac{q-3}{2}} = x$. Multiplying by $(1+B)$ on both sides and simplifying we obtain $(B+1)^{\frac{q-3}{2}} = -1$. Now when $x^{\frac{q-1}{2}} = -1$, Eqn. (7) changes to $-x(-1+B)^{q-2} - Bx(-1+B)^{\frac{q-3}{2}} = x$ and simplifies to $-x(-1+B)^{q-2} - B(-1+B)^{\frac{q-3}{2}} = 1$. Now if we multiply by $-(-1+B)$ both sides and simplify we obtain $(B-1)^{\frac{q-1}{2}} = -1$.

Conversly, if $(B-1)^{\frac{q-1}{2}} = (B+1)^{\frac{q-1}{2}} = -1$, lets call $g(x) = x^{q-2} - Bx^{\frac{q-3}{2}}$. we want to prove that $g(f(x)) = x$. Hence

$$g(f(x)) = x^{\frac{q-1}{2}} \cdot x(x^{\frac{q-1}{2}} + B)^{q-2} - Bx(x^{\frac{q-1}{2}} + B)^{\frac{q-3}{2}} \tag{8}$$

when $x^{\frac{q-1}{2}} = 1$ the RHS of Eqn. (8) simplifies as: $g(f(x)) = x(B+1)^{q-2} - Bx(B+1)^{\frac{q-3}{2}} = -x(B+1)^{\frac{q-3}{2}}[-(B+1)^{\frac{q-1}{2}} + B)]$ but we know that $(B+1)^{\frac{q-1}{2}} = -1$, hence, $g(f(x)) = -x(B+1)^{\frac{q-1}{2}} = -x \cdot -1 = x$. On the other hand when $x^{\frac{q-1}{2}} = -1$ and using the same approach we conclude that $g(f(x)) = x$. ∎

We recall that by *Euler Theorem*, see [Le], a necessary and sufficient condition for an integer a to be a quadratic residue modulo the odd prime p is that $a^{\frac{p-1}{2}} \equiv 1 \bmod (p)$. Hence we can state that a necessary and sufficient condition for a binomial $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ over a prime field of the form $4n+1$ to be a permutation binomial and self-invertible is that $B+1$ and $B-1$ are quadratic residues. We can also say that a binomial $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ is a permutation binomial with inverse $f^{-1}(x) = x^{q-2} - Bx^{\frac{q-3}{2}}$ if and only if $B+1$ and $B-1$ are quadratic non residues.

The case of $q = 4n+3$ is similar to the previous one except for some signs and the interpretation. So we present it as Theorem 6. Its proof is similar to Theorem 5.

Theorem 6. Let $q = 4n+3$, $r = q-2$, $s = \frac{q-3}{2}$, $B \neq 0$

i) The binomial $x^r + Bx^s$ over F_q is a permutation binomial and self-invertible if and only if

$$(B+1)^{\frac{q-1}{2}} = 1 \quad \text{and} \quad (B-1)^{\frac{q-1}{2}} = -1$$

ii) The binomial $x^r + Bx^s$ over F_q is a permutation binomial with inverse $f^{-1}(x) = x^r - Bx^s$ if and only if

$$(B+1)^{\frac{q-1}{2}} = -1 \quad \text{and} \quad (B-1)^{\frac{q-1}{2}} = -1 \qquad \blacksquare$$

Again by the Euler criterion we can state that a necessary and sufficient condition for $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ to be a PP and self-invertible over a prime field Z_p with p of the form $4n+3$, is that $B+1$ is a quadratic residue and $B-1$ is a quadratic non residue. Also a necessary and sufficient condition for $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ to be a PP with $f^{-1}(x) = x^{q-2} - Bx^{\frac{q-3}{2}}$ is that $B-1$ is a quadratic residue and $B+1$ is a quadratic non residue.

For every $B \in F_q$ we can now say whether a binomial $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$ is or not a permutation binomial and when it is self-invertible. Otherwise we find its inverse. Just look at $B+1$ and $B-1$ and apply Theorems 5 and 6.

Example 4 F_{27} or $GF(3^3)$. A permutation polynomial over F_{27} with α the primitive element satisfying $\alpha^3 + 2\alpha + 1$, is $f(x) = x^{25} + \alpha x^{11}$ with inverse $f^{-1}(x) = x^{25} - \alpha^2 x^{11}$. $q = 27$ has the form $4n+3$ and one can check that $(\alpha^2 - 1)^{13} = 1$ and $(\alpha^2 + 1)^{13} = -1$. All according to Theorem 6.

Table 1 shows an example of a finite field F_q where $q = 4n+1$, F_{13}, and its distribution of quadratic residues, with their relation to binomials of the form $f(x) = x^{q-2} + Bx^{\frac{q-3}{2}}$. Notations are : NPB=non-Permutation Binomial, SPB=self-invertible Binomial, PB=Permutation Binomial, PM=Permutation Monomial.

TABLE 1

QUADRATIC RESIDUES AND BINOMIALS FOR f_{13}

Elements in F_{13}	$x^{q-2} + Bx^{\frac{q-3}{2}}$
B	
0	PM
1QR	NPB
2	SPB
3-QR	NPB
4-QR	NPB
5	NPB
6	NPB
7	PB
8	NPB
9-QR	NPB
10-QR	NPB
11	SPB
12-QR	NPB

Remark. Since the characteristic p of a field $GF(p^n)$ satisfies $\gcd(p^k, q-1) = 1$, for $k = 1, \ldots, n-1$, the monomials x^{p^k} are PP and by the Frobenius automorphism, see [Fr], the polynomials $(x^{q-2} +$

$Bx^{\frac{q-3}{2}})^{p^k}$ are also permmutation binomials, and they do have exponents different than $q-2$ and $\frac{q-3}{2}$. So, this is a source of new permutation binomials.

§4. **Applications to Famous Primes**

Lemma 2. If $q > 5$ is a *Mersenne prime* or a *Fermat prime*, then 2 is a Quadratic Residue (QR) modulo q.

Proof: Mersenne primes q are of the form $2^p - 1$, where p is a prime number. From the identity $2(2^p - 1) + 2 = 2^{p+1}$ we obtain

$$2 \equiv 2^{p+1} \bmod (2^p + 1)$$

and since $q > 5$ is prime, p must be odd, so, 2^{p+1} is a square. Hence 2 is QR modulo q.

Fermat primes have the form $2^k + 1$, where $k = 2^\alpha$. From the identity $(2^{\frac{n}{2}} - 2)(2^n + 1) + 2 = (2^{\frac{3n}{4}} - 2^{\frac{n}{3}})^2$ we obtain:

$$2 \equiv (2^{\frac{3}{4}n} - 2^{\frac{n}{4}})^2 \bmod (2^n + 1)$$

which says that 2 is QR modulo q. ∎

This lemma establishes that 2 s a QR over F_q be q a Mersenne or a Fermat prime. But note that a Mersenne prime is of the form $4n + 3$ and a Fermat prime s $4n + 1$. Also note that 4 is always a QR in F_q $q > 5$. Then 3 is between QRs. By Theorem 6 if q is a Mersenne prime the binomial $x^{q-2}+3x^{\frac{q-3}{2}}$ over F_q is never a permutation binomal. On the other hand using Theorem 5 the binomal $x^{q-2} + 3x^{\frac{q-3}{2}}$ is always a permutation binomal in any F_q, q a Fermat prime. Moreover, this binomial is self-invertible. So we state:

Theorem 7. Let q be a prme number and $f(x) = x^{q-2} + 3x^{\frac{q-3}{2}}$ over F_q then

i) If q is a Fermat prime then f is always a self-invertible permutation binomial.

ii) If q is a Mersenne prime and f is never a permutation binomial. ∎

More generally it is known that if p is an odd prime $x^2 \equiv 2 \bmod (p)$ is solvable in x if and only if $p \equiv \pm 1 \bmod (8)$, see [Co, Theorem 9, p.191]. Also it is known that in a prime field of the form $4n + 1$ the distribution of quadratic residues is symmetric, i.e., x is QR if and only if $-x$ is QR. As a consequence of this and according to Theorems 5 and 6 we can state the following Theorem.

Theorem 8. Let $p > 5$ and $f(x) = x^{p-2} \pm 3x^{\frac{p-3}{2}}$ over Z_p then

i) If $p \equiv -1 \bmod (8)$ then the binomals $f(x)$ are never permutation binomials.

ii) If $p \equiv 1 \bmod (8)$ then the binomls $f(x)$ are always self-invertible permutation binomials. ∎

REFERENCES

[Co] H. Cohn *Advanced Number Theory* Dover Books 1962

[Fr] J.B.Fraleigh *A First course in Abstract Algebra.* Addison Wesley. 1968

[Le] J. LeVeque *Elementary Theory of Numbers.* Dover Books 1990

[L-M] R. Lidl and G. L. Mullen *When does a polynomila over a finite field permutes the elements of the field?, American Mathematical Society, March 1988, 242-246*

[L-N] R. Lidl and J Niederreiter *Finite Fields.* Addison Wesley Reading Mass 193

[MAC] O. Moreno M. Alonso and A. Cáceres *A Characterizaton of Chevalley Warning Solvabiltiy* UPRRP Gauss Lab. Internal Report, 1994.

[M-vzG] k. Ma and J.van zur Gathen. *Test for permutation functions* Finite Fields and their Applicatons, Vol I, No. 1, 1995.

[N-R] Niederreiter H. and Robinson k. *Complete Mappings over Finite Fields.* Australian Mathematical Society (Series A) 33 (1982) 197-212.

[Se] J.P. Serre. *Course d'Arithmetique.* Presses Unversitaires de France Paris 1970.

[Sm] Small.*Arithmetc of Finite Fields.* Marcel Dekker Inc, 1991

[T] G. Turnwald *A New Criteron for Permutation Polynomials*, Finite Fields and Their Appilcations. Vol 1 No. 1 1995