BULL. AUSTRAL. MATH. SOC. 11T06
VOL. 38 (1988) [325–327]

BINOMIAL PERMUTATIONS OF FINITE FIELDS

WUN-SENG CHOU

We discuss permutation properties of a specific kind of binomials over finite fields. As a result, we complete Cavior's classification of binomial octic permutation polynomials over F_q with q odd.

Let F_q be a finite field with q elements. A polynomial $f(x) \in F_q[x]$ is a permutation polynomial if the mapping $\alpha \mapsto f(\alpha)$, $\alpha \in F_q$, is a permutation of F_q. Cavior in [**1**] considered some specific octic polynomials of the form $x^8 + ax^j$, $j = 1, 3, 5, 7$, over F_q, and tried to determine if such polynomials are permutation polynomials over F_q with q odd. He raised three problems: Is $x^8 + ax^5$ a permutation polynomial over F_{7^n} for odd n? over F_{13^n} for n odd? Is $x^8 + ax^3$ a permutation polynomial over F_{11^n} for odd n? Recently, Mollin and Small [**3**] indicated that these problems were still open.

In fact, each of these polynomials is a binomial, that is, a polynomial of the form $bx^k + ax^j$. In this note we consider a specific kind of binomial, and thus answer all three of the above questions.

The method we use is the same as that used by Cavior. We will frequently use the following theorem and its corollary. Their proofs can be found in Lidl and Niederreiter [**2**, pp. 349–350].

Hermite's Criterion. Let F_q be of characteristic p. Then $f(x) \in F_q[x]$ is a permutation polynomial of F_q if and only if the following two conditions hold:

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

COROLLARY. *If $d > 1$ is a divisor of $q-1$, then there is no permutation polynomial of F_q of degree d.*

In the following theorem, we consider a specific kind of binomial which is a general form of the polynomials Cavior considered.

Received 5 January 1988
The author is grateful to Professor Gary L. Mullen for his suggestions and comments.

THEOREM. *Let $q = p^n$ with p an odd prime and n a positive integer. Let k, j be integers, with $1 \leqslant j < k$, such that $k \mid (p^2 - 1)$ and $(k-j) \mid (p-1)$. Write $(p^2-1)/k = lp + r$ with $1 \leqslant r \leqslant p-1$. If $(p-1)/(k-j) \leqslant l + r < p$, then for all $n \geqslant 2$, $f(x) = bx^k + ax^j$ is not a permutation polynomial of F_q for any $a, b \in F_q^*$.*

PROOF: If n is even, then $k|(p^2-1)$ implies $k|(q-1)$ and thus by the corollary to Hermite's Criterion, $f(x) = bx^k + ax^j$ is not a permutation polynomial of Fq for any $b \in F_q^*$.

From now on, we consider n odd and $n \geqslant 3$. For convenience, we write $m = k - j$.

Choose $t = p(1 + p^2 + p^4 + \ldots + p^{n-3})(p^2-1)/k + (p^2-1)/k$. Hence $t \not\equiv 0 \bmod p$, and moreover, $kt = p^n - 1 + p^2 - p < 2(p^n - 1)$ since $n \geqslant 3$. It follows that there is at most one term in the expansion of $[f(x)]^t$ which can be reduced to the term x^{q-1} mod $(x^q - x)$. In the reduction of $[f(x)]^t$ mod $(x^q - x)$, the coefficient of x^{q-1} is $\binom{t}{(p^2-p)/m}\left(b^{t-(p^2-p)/m}\right)\left(a^{(p^2-p)/m}\right)$.

We want to prove that $\binom{t}{(p^2-p)/m} \not\equiv 0 \bmod p$. It is easy to see that $p^{(p-1)/m} \|$ $((p^2-p)/m)!$ (where $p^e \| u$ means $p^e \mid u$ and $p^{e+1} \nmid u$). Let $p^\alpha \| t(t-1)\ldots(t+1-(p^2-p)/m)$. Since $\binom{t}{(p^2-p)/m}$ is always an integer, $(p-1)/m \leqslant \alpha$. To prove $\alpha = (p-1)/m$, it suffices to prove that $p^2 \nmid (t-i)$ for all $0 \leqslant i \leqslant (p^2-p)/m - 1$. When we write $(p^2-1)/k = lp + r$ with $1 \leqslant r \leqslant p-1$, we have $t = p(1 + p^2 + p^4 + \ldots + p^{n-3})(p^2-1)/k + (p^2-1)/k = sp^2 + (l+r)p + r$, where $s = l(1 + p^2 + p^4 + \ldots + p^{n-3}) + r(p + p^3 + \ldots + p^{n-4})$. Since $1 \leqslant l + r < p$ and $1 \leqslant r \leqslant p-1$, we have $(l+r)p + r < p^2$. This implies $p^2 \nmid (t-i)$ for all $0 \leqslant i < (l+r)p + r$. Since $(p-1)/m \leqslant l + r$, $p^2 \nmid (t-i)$ for all $0 \leqslant i < (p^2-p)/m$.

Since $\binom{t}{(p^2-p)/m} \not\equiv 0 \bmod p$, $\binom{t}{(p^2-p)/m}\left(b^{t-(p^2-p)/m}\right)\left(a^{(p^2-p)/m}\right) \neq 0$ in F_q whenever $a, b \in F_q^*$. So for all $a, b \in F_q^*$, the reduction of $[f(x)]^t$ mod $(x^q - x)$ has degree $q-1$. By Hermite's Criterion $f(x)$ is not a permutation polynomial of F_q, for all $a, b \in F_q^*$. This completes the proof. ∎

Now, we can answer Cavior's questions raised in [**1**, pp. 451–452]. We state them as the following corollaries.

COROLLARY 1. *Let $q = 7^n$. Then $f(x) = x^8 + ax^5 \in F_q[x]$ is a permutation polynomial of F_q if and only if $n = 1$ and $a = 3$ or 4.*

PROOF: If $a = 0$, then $f(1) = 1 = f(-1)$ and so $f(x) = x^8$ is not a permutation polynomial of F_{7^n} for any n.

If $n = 1$, then the reduction of $x^8 + ax^5$ mod $(x^7 - x)$ is $ax^5 + x^2$. Checking directly we have that $f(x) = x^8 + ax^5$ is a permutation polynomial of F_7 if and only if $a = 3$ or 4.

For $n > 1$ and $a \neq 0$, $k = 8$ and $j = 5$ satisfy the conditions of the Theorem and so $f(x) = x^8 + ax^5$ is not a permutation polynomial of F_{7^n} for all $n > 1$. This completes the proof. ∎

The following two corollaries have similar proofs which we omit.

COROLLARY 2. *Let* $q = 11^n$. *Then* $f(x) = x^8 + ax^3 \in F_q[x]$ *is a permutation polynomial of* F_q *if and only if* $n = 1$ *and* $a = 2, 4, 7$ or 9.

COROLLARY 3. *Let* $q = 13^n$. *Then for any* $a \in F_q$, $f(x) = x^8 + ax^5$ *is not a permutation polynomial of* F_q.

REFERENCES

[1] S.R. Cavior, 'A note on octic permutation polynomials', *Math. Comp.* **17** (1963), 450–452.

[2] R. Lidl and H. Niederreiter, *Finite Fields*, (Encyclopedia Math. Appl., Vol. 20) (Addison-Wesley, Reading, Mass., 1983).

[3] R.A. Mollin and C. Small, 'On permutation polynomial over finite fields', *Internat. J. Math. Sci.* **10** (1987), 535–543.

Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
United States of America

https://doi.org/10.1017/S0004972700027659 Published online by Cambridge University Press