Bull. Aust. Math. Soc. **89** (2014), 112–124
doi:10.1017/S0004972713000208

ON PERMUTATION BINOMIALS OVER FINITE FIELDS

MOHAMED AYAD, KACEM BELGHABA and OMAR KIHEL ✉

(Received 23 November 2012; accepted 29 November 2012; first published online 28 March 2013)

Abstract

Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements and $f(x) = ax^n + x^m$, a binomial with coefficients in this field. If some conditions on the greatest common divisor of $n - m$ and $q - 1$ are satisfied then this polynomial does not permute the elements of the field. We prove in particular that if $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in \mathbb{F}_p^*$, then $p - 1 \le (d - 1)d$, where $d = \gcd(n - m, p - 1)$, and that this bound of p, in terms of d only, is sharp. We show as well how to obtain in certain cases a permutation binomial over a subfield of $\mathbb{F}_q$ from a permutation binomial over $\mathbb{F}_q$.

2010 *Mathematics subject classification*: primary 11T06; secondary 12E20.
Keywords and phrases: finite fields, permutation polynomials, Hermite–Dickson theorem.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbb{F}_q$ is called a permutation polynomial of $\mathbb{F}_q$ if the induced map $f : \mathbb{F}_q \to \mathbb{F}_q$ is one-to-one. The study of permutation polynomials goes back to Hermite [3] for $\mathbb{F}_p$ and Dickson [1] for $\mathbb{F}_q$. Interest in permutation polynomials increased in part because of their application in cryptography and coding theory. Despite the widespread interest in the subject, characterising permutation polynomials and finding new families of permutation polynomials remain open questions. Carlitz conjectured that, given an even positive integer n, there exists a constant $C(n)$ such that, for $q > C(n)$, there are no permutation polynomials of degree n over $\mathbb{F}_q$. Fried *et al.* [2] proved Carlitz's conjecture. Permutation monomials are completely understood, but permutation binomials are not well understood. Niederreiter and Robinson [6] proved the following theorem.

THEOREM 1.1. *Given a positive integer n, there is a constant $C(n)$ such that, for $q > C(n)$, no polynomial of the form $ax^n + bx^m + c \in \mathbb{F}_q[x]$, with $n > m > 1$, $\gcd(n, m) = 1$, and $ab \neq 0$, permutes $\mathbb{F}_q$.*

The constant $C(n)$ in Theorem 1.1 is not explicit. Turnwald [9] improved Theorem 1.1 as follows.

THEOREM 1.2. *If $f(x) = ax^n + x^m$ permutes $\mathbb{F}_q$, where $n > m > 0$ and $a \in \mathbb{F}_q^*$, then either $q \leq (n-2)^4 + 4n - 4$ or $n = mp^i$.*

Turnwald's proof uses Weil's lower bound [11] for the number of points on the curve $(f(x) - f(y))/(x - y)$ over $\mathbb{F}_q$. For q a prime number, Turnwald [9] proved the following theorem.

THEOREM 1.3. *If $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in \mathbb{F}_p^*$, then $p < n \max\{m, n-m\}$.*

For $m = 1$, Wan [10] proved the following theorem.

THEOREM 1.4. *If $f(x) = ax^n + x$ permutes $\mathbb{F}_p$, where $n > 1$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (n-1) \cdot \gcd(n-1, p-1)$.*

The bounds in Theorems 1.3 and 1.4 are of different nature. The bound in Theorem 1.3 is given in terms of $\max\{m, n-m\}$, whereas the bound in Theorem 1.4 is given in term of $\gcd(n-1, p-1)$. Theorems 1.3 and 1.4 have been improved by Masuda and Zieve [5] as follows.

THEOREM 1.5. *If $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in \mathbb{F}_p^*$, and $d = \gcd(n-m, p-1)$, then $p - 1 \leq (n-1) \cdot \max\{m, d\}$.*

The bounds in the theorems above are not given in terms of d only, and one can ask whether the prime p can be bounded in terms of d only. The answer was given by Masuda and Zieve [5] who proved the following theorem.

THEOREM 1.6. *If $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (d+1)d$.*

Clearly, Theorem 1.6 improves Theorem 1.5 whenever $d - 1 \leq n - 1$, which is always the case except when $m = 1$ and $n - 1 \mid p - 1$. In Section 2, we prove the following theorem.

THEOREM 1.7. *If $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (d-1)d$.*

Clearly, Theorem 1.7 implies Theorems 1.6 and 1.5 in all cases. When $m = 1$ and $n - 1 \mid p - 1$, we will see in Corollary 3.5 that $p - 1 \leq (n-1)(n-3)$, which improves Theorem 1.5. It would be interesting to have a bound for p in terms of $d = \gcd(n-m, p-1)$ when $f(x) = ax^n + x^m$ permutes $\mathbb{F}_q$ and q is a power of the prime p. In Theorem 3.3, we will show how in certain cases, one can obtain from a permutation binomial $f(x) \in \mathbb{F}_q[x]$ a new permutation binomial $g(x) \in \mathbb{F}_p[x]$, and deduce in Corollary 3.6, a bound of p in terms of $d = \gcd(n-m, p-1)$. Some consequences of this theorem are stated in Sections 2 and 3.

We fix some notation which will be used through this paper. The letter p always denotes a prime number, and $\mathbb{F}_q$ the finite field containing $q = p^r$ elements. For any polynomial $g(x) \in \mathbb{F}_q[x]$, we denote by $\overline{g(x)}$ the unique polynomial of degree at

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

most $q-1$, with coefficients in $\mathbb{F}_q$ such that $g(x) \equiv \overline{g(x)} \pmod{x^q - x}$. When we refer to a binomial $f(x)$ over $\mathbb{F}_q$, we always mean a polynomial $f(x) \in \mathbb{F}_q[x]$ of the form $f(x) = ax^n + x^m$ with the nonrestrictive condition $\gcd(m, n) = 1$ (see [7, Ex. 2.1]), $n > m$ and $a \neq 0$. The integer $d = \gcd(n-m, q-1)$ will play an important role. It is well known that if $-a \in (\mathbb{F}_q^\star)^d$, then the equation $f(x) = 0$ has $d+1$ distinct solutions in $\mathbb{F}_q$, so $f(x)$ is not a permutation of $\mathbb{F}_q$ [8]. In particular, this claim is true if $d = 1$.

2. Nonexistence of permutation binomials of certain shapes

An old result in the theory of permutation polynomials is the following theorem proved by Hermite for prime fields and Dickson in the general case.

THEOREM 2.1. *Let p be a prime number, $q = p^r$ and $g(x) \in \mathbb{F}_q[x]$. Then $g(x)$ is a permutation polynomial if and only if*

(i) *$g(x) = 0$ has a unique solution in $\mathbb{F}_q$;*

(ii) *for every $l \in \{1, \ldots, q-2\}$, $\deg \overline{g^l(x)} \leq q-2$.*

For binomials, we deduce from Theorem 2.1 the following corollary.

COROLLARY 2.2. *Let $f(x) = ax^n + x^m \in \mathbb{F}_q[x]$, such that $a \neq 0$ and $\gcd(m, n) = 1$. Let $d = \gcd(n-m, q-1)$. Suppose that $d \geq 2$. Then $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

(i) *$f(x) = 0$ has a unique solution in $\mathbb{F}_q$;*

(ii) *for every $l \in \{1, \ldots, q-2\}$ such that $d \mid l$, we have $\deg \overline{f^l(x)} \leq q-2$.*

PROOF. From Theorem 2.1, we have only to prove that if $l \in \{1, \ldots, q-2\}$ and $d \nmid l$, then $\deg \overline{f^l(x)} \leq q-2$. Let k be an integer and let $\overline{k}$ be the integer in $\{1, \ldots, q-1\}$ such that $k \equiv \overline{k} \pmod{q-1}$. Then, modulo $x^q - x$,

$$x^k \equiv \begin{cases} 1 & \text{if } k = 0 \\ x^{\overline{k}} & \text{if } k \neq 0. \end{cases}$$

It follows that if $k > 0$, then $x^k \equiv x^{q-1} \pmod{x^q - x}$ if and only if $k \equiv 0 \pmod{q-1}$. Suppose that there exists $l \in \{1, \ldots, q-2\}$ with $d \nmid l$ such that $\deg \overline{f^l(x)} = q-1$. We deduce from

$$(ax^n + x^m)^l = \sum_{j=0}^{l} \binom{l}{j} a^j x^{nj+m(l-j)} = \sum_{j=0}^{l} \binom{l}{j} a^j x^{(n-m)j+lm} \tag{2.1}$$

that there exists an integer $j \in \{0, \ldots, l\}$ such that

$$x^{(n-m)j+lm} \equiv x^{q-1} \pmod{x^q - x}.$$

Hence, $(n-m)j + lm > 0$ and $(n-m)j + lm \equiv 0 \pmod{q-1}$. Since $d = \gcd(n-m, q-1)$, it follows that $d \mid n-m$ and $d \mid q-1$. But $\gcd(n, m) = 1$ implies that $\gcd(d, m) = 1$. Then $d \mid l$, which is a contradiction. □

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

Corollary 2.2 reduces enormously the calculations when applying Theorem 2.1 to check whether a given binomial permutes $\mathbb{F}_q$ or not. One needs to check the degrees of only $\lfloor (q-2)/d \rfloor$ polynomials instead of $q-2$ polynomials as given by Theorem 2.1(ii).

For the proof of Theorem 1.7, we need the following lemma.

LEMMA 2.3. *Let $f(x)$ be a binomial such that $d > 1$. Let $l \in \{1, \ldots, q-2\}$ such that $d \mid l$. Then the following three assertions are equivalent:*

$$\deg f^l(x) \le q-2, \tag{2.2}$$

$$\sum_{\substack{j=0 \\ (n-m)j+lm \equiv 0 \pmod{q-1}}}^{l} \binom{l}{j} a^j = 0, \tag{2.3}$$

$$\sum_{\lambda=0}^{\gamma_l} \binom{l}{j_0 + \lambda(q-1)/d} (a^{(q-1)/d})^\lambda = 0, \tag{2.4}$$

where j_0 is the smallest nonnegative integer satisfying

$$j_0 \equiv \frac{-lm}{(n-m)} \pmod{\frac{q-1}{d}} \equiv \frac{-lm/d}{(n-m)/d} \pmod{\frac{q-1}{d}}$$

and γ_l is the largest integer λ such that

$$j_0 + \frac{\lambda(q-1)}{d} \le l.$$

PROOF. From (2.1), $\deg \overline{f^l(x)} \le q-2$ if and only if

$$\sum_{\substack{j=0 \\ (n-m)j+lm \equiv 0 \pmod{q-1}}}^{l} \binom{l}{j} a^j = 0. \tag{2.5}$$

The condition $(n-m)j + lm \equiv 0 \pmod{q-1}$ is equivalent to $((n-m)/d)j + (l/d)m \equiv 0 \pmod{(q-1)/d}$, which is equivalent to

$$j \equiv \frac{-lm}{n-m} \pmod{\frac{q-1}{d}}. \tag{2.6}$$

Let j_0 be the smallest integer satisfying (2.6). Then $j \equiv j_0 \pmod{(q-1)/d}$. Hence (2.5) is equivalent to

$$\sum_{\lambda=0}^{\alpha_l} \binom{l}{j_0 + \lambda(\frac{q-1}{d})} (a^{q-1/d})^\lambda = 0,$$

where γ_l is the largest integer λ such that $j_0 + \lambda(q-1)/d \le l$. □

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

PROOF OF THEOREM 1.7. In the following proof, we repeatedly use (2.4). The integer j_0 appearing in this equation depends on l, so it will be denoted by $j_0(l)$. Suppose that there exists a permutation binomial $f(x)$ over $\mathbb{F}_p$ such that $p-1 > d(d-1)$; then $(p-1)/d > d-1$, that is, $(p-1)/d \geq d$. Since $(p-1)/d \neq d$, then $(p-1)/d > d$. Set $(p-1)/d = \alpha d - z$ where $\alpha > 1$ and z are integers such that $z \in \{0, \ldots, d-1\}$. We may suppose that $z \in \{1, \ldots, d-1\}$. Let $j_0(d)$ be the unique integer determined by (2.4) for $l = d$. Set $j_0(d) = \beta d + \delta$ with $\delta \in \{0, \ldots, d-1\}$; then

$$j_0(d) < \frac{p-1}{d} < \alpha d. \tag{2.7}$$

Case 1: $j_0(d) \leq d$.

In this case, because $j_0(d) + \lambda(p-1)/d > d$ for $\lambda \geq 1$, (2.4) reduces to $\binom{d}{j_0(d)} = 0$. Since $j_0(d) \leq d < p$, it follows that $\binom{d}{j_0(d)} \neq 0$, which is a contradiction, and we can exclude this case.

Case 2: $j_0(d) > d$.

Clearly, $\beta \geq 1$, and from (2.7), we deduce that $\beta < \alpha$. Consider (2.4) for $l = \alpha d$. We have

$$\begin{aligned} \alpha j_0(d) &= \left(\frac{p-1}{d^2} + \frac{z}{d}\right) j_0(d) \\ &= \frac{p-1}{d}\beta + z\beta + \alpha\delta \\ &\equiv z\beta + \alpha\delta \pmod{\frac{p-1}{d}}. \end{aligned}$$

Case 2.1: $z\beta + \alpha\delta < (p-1)/d$.

In this case,

$$d < j_0(\alpha d) = z\beta + \alpha\delta < \frac{p-1}{d} < \alpha d = l. \tag{2.8}$$

Let λ be a positive integer. Then

$$\begin{aligned} j_0(\alpha d) + \frac{\lambda(p-1)}{d} &\geq j_0(\alpha d) + \frac{p-1}{d} \\ &= z\beta + \alpha\delta + \frac{p-1}{d} \\ &> d + \frac{p-1}{d} > z + \frac{p-1}{d} = \alpha d = l. \end{aligned}$$

Hence there is only one term in the left-hand side of (2.4) corresponding to $l = \alpha d$, namely $\binom{\alpha d}{j_0(\alpha d)} = \binom{\alpha d}{z\beta+\alpha\delta}$. Since $(p-1)/d \geq d$,

$$\alpha d < \frac{p-1}{d} + d < p.$$

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

Hence, from (2.8), we obtain that $j_0(\alpha d) = z\beta + \alpha\delta < \alpha d < p$. Then

$$\binom{\alpha d}{j_0(\alpha d)} = \binom{\alpha d}{z\beta + \alpha\delta} \neq 0,$$

and we reject this case.

Case 2.2: $z\beta + \alpha\delta \geq (p-1)/d$.

Suppose that $\delta = 0$. Then $z\beta + \alpha\delta = z\beta$ and since $\beta \leq \alpha - 1$, we deduce that $z\beta + \alpha\delta \leq (\alpha-1)z \leq (\alpha-1)(d-1)$. Hence

$$\begin{aligned} z\beta + \alpha\delta &\leq \alpha d - \alpha - d + 1 \\ &< \alpha d - z = \frac{p-1}{d}, \end{aligned}$$

which is a contradiction. We may suppose that δ is positive. Consider (2.4) for $l = (\alpha-1)d$. Then

$$\begin{aligned} (\alpha-1)j_0(d) &= \left(\frac{p-1}{d^2} + \frac{z-d}{d}\right) j_0(d) \\ &= \left(\frac{p-1}{d^2} + \frac{z-d}{d}\right)(\beta d + \delta) \\ &\equiv (z-d)\beta + (\alpha-1)\delta \pmod{\frac{p-1}{d}}. \end{aligned}$$

To prove that $(z-d)\beta + (\alpha-1)\delta = j_0((\alpha-1)d)$, we have to show that $0 \leq (z-d)\beta + (\alpha-1)\delta < (p-1)/d$. Since $z < d$, we have $(z-d)\beta < 0$. Hence

$$\begin{aligned} (z-d)\beta + (\alpha-1)\delta &< (\alpha-1)\delta \leq (\alpha-1)(d-1) \\ &= \alpha d - d - \alpha + 1 \\ &< \alpha d - z = \frac{p-1}{d}. \end{aligned}$$

We now look at the sign of $(z-d)\beta + (\alpha-1)\delta$. On the one hand, we have $\alpha > \beta \geq 1$, so $\alpha \geq 2$. Furthermore, since $z - d < 0$ and $\beta \leq \alpha - 1$, we have $(z-d)\beta \geq (z-d)(\alpha-1)$. Hence

$$\begin{aligned} (z-d)\beta + (\alpha-1)\delta &\geq (z-d)(\alpha-1) + (\alpha-1)\delta \\ &= (\alpha-1)(z-d+\delta) \\ &\geq z - d + \delta. \end{aligned}$$

On the other hand, since $z\beta + \alpha\delta \geq (p-1)/d = \alpha d - z$,

$$\begin{aligned} (z-d)\beta + (\alpha-1)\delta &= z\beta + \alpha\delta - d\beta - \delta \\ &\geq \alpha d - z - d\beta - \delta \\ &= (\alpha-\beta)d - z - \delta \\ &\geq d - z - \delta. \end{aligned}$$

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

We have shown that $(z-d)\beta+(\alpha-1)\delta \geq |A|$, where $A = z-d-\delta$. Hence $(z-d)\beta+(\alpha-1)\delta \geq 0$ and then $j_0((\alpha-1)d) = (z-d)\beta+(\alpha-1)\delta$. As in the preceding cases we prove that on the left-hand side of (2.4), for $l=(\alpha-1)d$, there is only one term. For any integer $\lambda \geq 1$, we have $(z-d)\beta+(\alpha-1)\delta+\lambda(p-1)/d \geq (p-1)/d > l$. Equation (2.4) reads $\binom{(\alpha-1)d}{(z-d)\beta+(\alpha-1)\delta)} = 0$. But, since $(z-d)\beta < 0$, we have $(z-d)\beta+(\alpha-1)\delta < (\alpha-1)d$. Hence $\binom{(\alpha-1)d}{(z-d)\beta+(\alpha-1)\delta)} \neq 0$, and the proof of Theorem 1.7 is complete. □

Corollary 2.4. *Let $f(x)$ be a permutation binomial over $\mathbb{F}_p$. Then $p-1 \leq d(d-2)$ except possibly in the case $d \equiv 0 \pmod 3$, $p = d^2-d+1$ and one of the two possibilities $n \equiv 0 \pmod{(p-1)/d}$ or $m \equiv 0 \pmod{(p-1)/d}$.*

Proof. Since there are no permutation binomials over $\mathbb{F}_2$ and $\mathbb{F}_3$, we may suppose that $p \geq 5$. From Theorem 1.7, we have $(p-1)/d \leq d-1$. It remains to consider the case $(p-1)/d = d-1$, that is, $p = d^2-d+1$. Suppose that there exists a permutation binomial over $\mathbb{F}_p$, $f(x) = ax^n + x^m$ such that $p = d^2-d+1$. Consider (2.4) for $l=d$ and let j_0 be the integer appearing in this equation. Since $j_0 \in \{0, \ldots, (p-1)/d\}$, then $j_0 < d$. For any positive integer λ, we have $j_0+\lambda(p-1)/d \geq j_0+(p-1)/d > d$ except if $j_0 = 0$ or $j_0 = 1$. Beyond these exceptions, (2.4) reads $\binom{d}{j_0} = 0$. Since $j_0 < d < p$ this equation is impossible and we get a contradiction.

If $j_0 = 0$, (2.4) reads

$$\binom{d}{0} + \binom{d}{\frac{p-1}{d}}(a)^{(p-1)/d} = 0,$$

so $1+da^{d-1} \equiv 0 \pmod p$. We deduce that $d^d \equiv (-1)^d \pmod p$, so $(-d)^d \equiv 1 \pmod p$. We have $(-d)^2 \equiv d-1 \pmod p$ and $(-d)^3 \equiv 1 \pmod p$, so the order of $-d$ in $\mathbb{F}_p$ which is a divisor of d is equal to 1 or 3. Since $d(d-1) = p-1$, the first possibility is excluded, so $d \equiv 0 \pmod 3$. On the other hand, the condition $(n-m)j_0 + dm \equiv 0 \pmod{p-1}$ implies $dm \equiv 0 \pmod{p-1}$, that is, $m \equiv 0 \pmod{(p-1)/d}$.

If $j_0 = 1$, (2.4) reads

$$\binom{d}{1} + \binom{d}{1+\frac{p-1}{d}}(a)^{p-1/d} = 0,$$

so $d+a^d \equiv 0 \pmod p$. As in the preceding case we find $d^d \equiv (-1)^d \pmod p$, so $d \equiv 0 \pmod 3$. On the other hand, the condition $(n-m)j_0 + dm \equiv 0 \pmod{p-1}$ implies $(n-m)+dm \equiv 0 \pmod{p-1}$, that is, $n \equiv 0 \pmod{(p-1)/d}$. □

The condition $d \equiv 0 \pmod 3$, $p = d^2-d+1$ in Corollary 2.6 occurs, for instance, for $p=7$ and $d=3$ or $p=31$ and $d=6$ (see [5, Corollary 2. 5]). This shows that the bound of p in terms of d in Theorem 1.7 is sharp.

If $f(x) = ax^n + x$ permutes $\mathbb{F}_p$, where $n > 1$, $a \in \mathbb{F}_p^*$ and $n-1 \mid p-1$, then Theorem 1.6 does not generalise Theorem 1.5 which implies that $p-1 \leq (n-1)^2$. Theorem 1.7 proved above generalises Theorem 1.5 even in this case, as shown by the following corollary.

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

COROLLARY 2.5. *If $f(x) = ax^n + x$ permutes $\mathbb{F}_p$, where $n > 1$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (n-1)(n-3)$.*

PROOF. From Corollary 2.6, we have $p - 1 \leq d(d-2)$, which implies that $p - 1 \leq (n-1)(n-3)$, except if $d \equiv 0 \pmod 3$, $(p-1)/d = d - 1$, and $n \equiv 0 \pmod{(p-1)/d}$ (because $m = 1$). So we have only to consider the exceptional case. In this case, we have $n \equiv 0 \pmod{d-1}$ and $n - 1 \equiv 0 \pmod d$. Clearly $n \neq d - 1$. It follows that $n \geq 2(d-1)$. We conclude that $3 \leq d \leq n/2 + 1$. It is now easy to deduce the inequality $p - 1 \leq (n-1)(n-3)$. □

The following result is similar to [5, Corollary 2.4] except that the four polynomials arising for $d = 3$ and $p = 7$ were omitted.

COROLLARY 2.6. *If $f(x) = x^n + ax^m$ permutes $\mathbb{F}_p$, where $1 \leq m < n < p$ and $a \in \mathbb{F}_p^*$, then* $\gcd(n - m, p - 1) > 4$ *except if $d = 3$, $p = 7$ and $f(x)$ is one of the following:*

(i) $f(x) = x^4 + 3x$;
(ii) $f(x) = x^4 - 3x$;
(iii) $f(x) = x^5 + 2x^2$;
(iv) $f(x) = x^5 - 2x^2$.

PROOF. We conclude from Corollary 2.4 that if $d = 4$, then $p - 1 \leq 8$, that is, $p \leq 7$. We see from Table 7.1 of [4] that there are no permutation binomials in this case. When $d = 2$, we conclude from Corollary 2.4 that there are no permutation binomials in this case. When $d = 3$, Corollary 2.4 implies that $p = 7$. We see from Table 7.1 of [4] that the only possible cases are the ones listed above. □

3. Permutation binomials over a subfield of $\mathbb{F}_q$ arising from permutation binomials over $\mathbb{F}_q$

Before stating a result about the possibility of deducing, in some cases, a permutation binomial of a subfield of $\mathbb{F}_q$ from a given permutation binomial of $\mathbb{F}_q$, we make the following definition.

DEFINITION 3.1. Fix the integers m and n such that $1 \leq m < n \leq q - 1$ and let $d = \gcd(n - m, q - 1)$. We say that the polynomials $f(x) = ax^n + x^m$ and $g(x) = bx^n + x^m$, with coefficients in $\mathbb{F}_q$, are d-equivalent and we write $f \overset{d}{\sim} g$ if and only if there exists $\epsilon \in (\mathbb{F}_q)^d$ such that $b = \epsilon a$.

Obviously the above relation in the set of binomials over $\mathbb{F}_q$, of degree at most $q - 1$, where the pair (m, n) is fixed, is an equivalence relation and each equivalence class contains $(q-1)/d$ elements.

LEMMA 3.2. *Suppose that the polynomials $f(x) = ax^n + x^m$ and $g(x) = bx^n + x^m \in \mathbb{F}_q[x]$, are d-equivalent and that $f(x)$ permutes $\mathbb{F}_q$. Then so does $g(x)$.*

PROOF. Since $\gcd(n - m, q - 1) = d$, there exist two integers u and v such that

$$u(n - m) + v(q - 1) = d. \tag{3.1}$$

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

The binomials $f(x)$ and $g(x)$ being d-equivalent, there exists $\eta \in \mathbb{F}_q$ such that $b = \eta^d a$. Using (3.1), we obtain $b = \eta^{u(n-m)}a$. We deduce that

$$\begin{aligned} g(x) &= \eta^{u(n-m)}ax^n + x^m = \eta^{-um}(\eta^{un}ax^n + \eta^{um}x^m) \\ &= \eta^{-um}(a(\eta^u x)^n + (\eta^u x)^m) = \eta^{-um}f(\eta^u x)), \end{aligned}$$

and this proves our lemma. □

THEOREM 3.3. *Let $f(x) = ax^n + x^m$ be a permutation binomial of $\mathbb{F}_q$ with $q = p^r$ and s be a positive divisor of r. Let $d = \gcd(n-m, q-1)$.*

(1) *There exists a binomial $g(x) = bx^n + x^m \in \mathbb{F}_{p^s}[x]$ d-equivalent to $f(x)$ if and only if the order of a in $(\mathbb{F}_q)^\star$ divides $\operatorname{lcm}(p^s - 1, (q-1)/d)$.*

(2) *If these equivalent conditions hold, then the number of $g(x) = bx^n + x^m \in \mathbb{F}_{p^s}[x]$, d-equivalent to $f(x)$, is equal to $\gcd(p^s - 1, (q-1)/d)$ and they are all distinct as permutations of $\mathbb{F}_{p^s}$. Moreover, $g(x) \equiv bx^{n_1} + x^{m_1} \pmod{x^{p^s} - x}$ if $p^s - 1 \nmid d$ and $g(x) \equiv (b+1)x^k \pmod{x^{p^s} - x}$ if $p^s - 1 \mid d$ where k, m_1, n_1 are positive integers less than $p^s - 1$, $m_1 \neq n_1$, $\gcd(p^s - 1, k) = 1$.*

(3) *Let t be a positive integer (not necessarily dividing r). There exists a binomial $g(x) = bx^n + x^m \in (\mathbb{F}_{p^t} \cap \mathbb{F}_q)[x]$, d-equivalent to $f(x)$, if and only if the order of a in $(\mathbb{F}_q)^\star$ divides $\operatorname{lcm}(p^t - 1, (q-1)/d)$.*

PROOF. (1) Suppose first that the order of a in $(\mathbb{F}_q)^\star$ divides $\operatorname{lcm}(p^s - 1, (q-1)/d)$. We will use the following claim for which the proof is omitted.

Claim 1. Let δ, u, v be positive integers. Then $\delta \mid \operatorname{lcm}(u, v)$ if and only if there exist positive integers δ_1, δ_2 such that $\delta_1 \mid u$, $\delta_2 \mid v$ and $\delta = \operatorname{lcm}(\delta_1, \delta_2)$.

Let δ be the order of a in $(\mathbb{F}_q)^\star$. Then $\delta = \operatorname{lcm}(\delta_1, \delta_2)$, where δ_1 and δ_2 are positive integers such that $\delta_1 \mid p^s - 1$ and $\delta_2 \mid (q-1)/d$. Let ξ be a generator of $(\mathbb{F}_q)^\star$. Then $a = (\xi^{(q-1)/\delta_1})^i(\xi^{(q-1)/\delta_2})^j$ for some nonnegative integers i and j. Let $\epsilon = \xi^{-j(q-1)/\delta_2}$, $b = \epsilon a$ and $g(x) = bx^n + x^m$. Then $\epsilon^{(q-1)/d} = (\xi^{-j(q-1)/d\delta_2})^{q-1} = 1$ and $b^{p^s-1} = (\xi^{i(p^s-1)/\delta_1})^{q-1} = 1$, so $\epsilon \in \mathbb{F}_q)^d$, $b \in \mathbb{F}_{p^s}$ and $g(x) \overset{d}{\sim} f(x)$.

Conversely, suppose that there exists $g(x) = bx^n + x^m \in \mathbb{F}_{p^s}$, d-equivalent to $f(x)$. Then we may find a $(q-1)/d$th root of unity ϵ such that $a = \epsilon b$. Hence $a^{\operatorname{lcm}(p^s-1,(q-1)/d)} = (\epsilon b)^{(p^s-1)(q-1)/d/\delta_s} = 1$, where $\delta_s = \gcd(p^s - 1, (q-1)/d)$. It follows that the order of a in $(\mathbb{F}_q)^\star$ divides $\operatorname{lcm}(p^s - 1, (q-1)/d)$.

(2) Let $\delta_s = \gcd(p^s - 1, (q-1)/d)$. By (1), there exists at least one permutation binomial of $\mathbb{F}_q$, $g(x) = c_s x^n + x^m$ with $c_s \in \mathbb{F}_{p^s}$, d-equivalent to $f(x)$. Let $h(x) = b_s x^n + x^m$ be any permutation binomial of $\mathbb{F}_q$ with $b_s \in \mathbb{F}_{p^s}$, d-equivalent to $f(x)$. Then $g(x) \overset{d}{\sim} h(x)$, so there exists $\epsilon \in \mathbb{F}_q^d$ such that $b_s = \epsilon c_s$. We deduce that $\epsilon = b_s/c_s \in \mathbb{F}_{p^s}$. It follows that $\epsilon^{p^s-1} = 1 = \epsilon^{(q-1)/d}$ and then $\epsilon^{\delta_s} = 1$. We conclude that $h(x)$ has the form $h(x) = \epsilon c_s x^n + x^m$ with ϵ satisfying the condition $\epsilon^{\delta_s} = 1$. On the other hand, any polynomial $h(x)$ of this form is d-equivalent to $g(x)$ and then to $f(x)$. Clearly all these $h(x)$, as permutations of $\mathbb{F}_q$, are distinct. Because they all take different values at the argument $x = 1$, they are distinct as permutations of $\mathbb{F}_{p^s}$. We conclude that the number of these h is equal to δ_s.

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

To prove the last part of the theorem we reduce $g(x)$ modulo $x^{p^s} - x$. Denote by $\overline{g(x)}$ the unique polynomial over $\mathbb{F}_{p^s}$ of degree at most $p^s - 1$ such that $g(x) \equiv \overline{g(x)} \pmod{x^{p^s} - x}$. Set $n = (p^s - 1)\lambda + n_1$ and $m = (p^s - 1)\mu + m_1$ with $0 \le m_1, n_1 \le p^s - 2$. If $m_1 = 0$ or $n_1 = 0$, then the degree of $\overline{g(x)}$ is equal to $p^s - 1$, which is excluded by the fact that $g(x)$ is a permutation polynomial of $\mathbb{F}_{p^s}$. If $m_1 = n_1$, then clearly $p^s - 1 \mid d$ and $\overline{g(x)} = (b+1)x^k$, where $k = n_1 = m_1$ and $\gcd(k, p^s - 1) = 1$. Suppose now that $m_1 \neq 0$, $n_1 \neq 0$ and $m_1 \neq n_1$. Then $p^s - 1 \nmid d$ and $\overline{g(x)} = bx^{n_1} + x^{m_1}$. Let $k = \gcd(m_1, n_1)$; then the polynomial $g_1(x) = bx^{n_1/k} + x^{m_1/k}$ is a permutation binomial of $\mathbb{F}_{p^s}$.

(3) We will use the following well-known claim.

Claim 2. Let a, b, c be nonzero integers. Then $\gcd(\mathrm{lcm}(a,b), \mathrm{lcm}(a,c)) = \mathrm{lcm}\,(a, \gcd(b,c))$.

Suppose that there exists a binomial $g(x) = bx^n + x^m \in (\mathbb{F}_{p^t} \cap \mathbb{F}_q)[x]$, d-equivalent to $f(x)$. Let $s = \gcd(r,t)$. Then $\mathbb{F}_q \cap \mathbb{F}_{p^t} = \mathbb{F}_{p^s}$ and, by (1), the order of a in $\mathbb{F}_q$ divides $\mathrm{lcm}(p^s - 1, (q-1)/d)$. Therefore this order divides $\mathrm{lcm}(p^t - 1, (q-1)/d)$. Suppose now that the order of a in $(\mathbb{F}_q)^\star$ divides $\mathrm{lcm}(p^t - 1, (q-1)/d)$. Then applying Claim 2 with $a = (q-1)/d$, $b = p^t - 1$ and $c = p^r - 1$, we conclude that this order divides $\mathrm{lcm}(p^s - 1, (q-1)/d)$ and then by (1) there exists a binomial $g(x) = bx^n + x^m \in (\mathbb{F}_{p^t} \cap \mathbb{F}_q)[x]$, d-equivalent to $f(x)$. □

Remark 3.4. Suppose that p is odd. Then under hypothesis (1) of the above theorem, $\gcd(d, p^s - 1) \neq 1$. Indeed if this greatest common divisor is equal to 1, then $\mathrm{lcm}(p^s - 1, (q-1)/d) = (q-1)/d$. But it is known that if $(-1/a)^{(q-1)/d} = 1$, then the corresponding binomial is not a permutation binomial of $\mathbb{F}_q$ (see [8]).

Corollary 3.5. *Let $f(x) = ax^n + x^m$ be a permutation binomial of $\mathbb{F}_q$. Suppose that the order of a in $(\mathbb{F}_q)^\star$ divides* $\mathrm{lcm}(p-1, (q-1)/d)$. *Then $p - 1 \le d(d-1)$.*

Proof. If $p - 1 \mid d$, the corollary is clear. If not, the proof is a direct consequence of Theorems 1.7 and 3.3. □

Corollary 3.6. *Suppose that there exists a permutation binomial $f(x) = ax^n + x^m$ of $\mathbb{F}_q$ with $q = p^r$ such that for any prime number l, where $l \mid d$, $\gcd(l(l-1), r) = 1$. Then $d = p - 1$ or there exists a permutation binomial of $\mathbb{F}_p$, $g_1(x) = cx^{n_1} + x^{m_1}$, such that $n \equiv kn_1 \pmod{p-1}$, $m \equiv km_1 \pmod{p-1}$, $0 < km_1 < kn_1 < p - 1$, where k is a positive integer coprime with $p - 1$, and $p - 1 \le d(d-1)$. Moreover, the two possibilities exclude each other.*

Proof. Let l be any prime factor of d. We have $p^r \equiv 1 \pmod{l}$ by assumption, and $p^{l-1} \equiv 1 \pmod{l}$ by Fermat's little theorem. Since r and $l - 1$ are coprime, $p \equiv 1 \pmod{l}$. It is easy to see that $p \equiv 1 \pmod{d}$ and $\mathrm{lcm}(p-1, (q-1)/d) = q - 1$ so that Theorem 3.3 may be applied to any permutation binomial of $\mathbb{F}_q$. Let $g(x)$ be the permutation binomial of $\mathbb{F}_q$ with coefficients in $\mathbb{F}_p$ deduced from $f(x)$, using Theorem 3.3. Let $g_1(x)$ be the reduced polynomial of $g(x)$ modulo $x^p - x$. Then $g_1(x)$ is a monomial or $g_1(x)$ is a sum of two monomials of degree n' and m' respectively

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

satisfying $0 < m' < n' < p-1$. Moreover, the first case holds if and only if $p-1 \mid d$. Since $p \equiv 1 \pmod{d}$, the first case holds if and only if $d = p-1$. To complete the proof let $k = \gcd(m', n')$, $m_1 = m'/k$ and $n_1 = n'/k$; by applying Corollary 3.6, we have $p - 1 \leq d(d-1)$. □

The following result is a generalisation of [5, Corollaries 2.4 and 2.5].

COROLLARY 3.7. *There does not exist a permutation binomial of $\mathbb{F}_q$ with $q = p^r$ if one of the following conditions holds:*

(i) *r odd, $d = 2$, $p \neq 3$;*
(ii) *r odd, $d = 4$, $p \neq 5$;*
(iii) $\gcd(r, 6) = 1$, *$d = 3$, $p \neq 7$;*
(iv) $\gcd(r, 10) = 1$, *$d = 5$, $p \neq 11$;*
(v) $\gcd(r, 6) = 1$, *$d = 6$, $p \neq 7, 13, 19, 31$;*
(vi) $\gcd(r, 42) = 1$, *$d = 7$, $p \neq 29$;*
(vii) *r odd, $d = 8$, $p \neq 17$.*

PROOF. We prove case (v) using Corollaries 3.5 and 3.6 and [5, Corollary 2.5]. The proof of the other statements will be omitted. Suppose that there exists a permutation binomial of $\mathbb{F}_q$ with $d = 6$ and $\gcd(r, 6) = 1$. Then the hypotheses of the above corollary hold. We deduce that $p = d + 1 = 7$ or there exists some permutation binomial $g_1(x) = cx^{n_1} + x^{m_1}$ of $\mathbb{F}_p$. It is evident that $\gcd(n_1 - m_1, p-1)$ divides $d = 6$ and is not trivial. The possible values of this greatest common denominator are 2 or 3 or 6. According to [5, Corollary 2. 5], the possible values of p are $p = 7, 13, 19, 31$. □

REMARK 3.8. It is of interest to improve the conditions on r and p in the above corollary. We use the results of [4, Table 7.1] to make some observations in this direction. Since $ax^3 + x$ is a permutation polynomial of $\mathbb{F}_q$ for $q \equiv 0 \pmod{3}$ and $-a$ is not a square, the condition $p \neq 3$ is necessary for $d = 2$. The polynomial $ax^5 + x$ is a permutation of $\mathbb{F}_q$ for $q \equiv 0 \pmod{5}$ and $-a$ is not a fourth power, so the condition $p \neq 5$ is necessary for $d = 4$. Let $a \in \mathbb{F}_9$ such that $a^2 = -1$; then $ax^5 + x$ permutes $\mathbb{F}_9$, so the condition r odd is necessary for $d = 4$.

PROPOSITION 3.9. *Let $q = p^r$ and $f(x) = ax^n + x^m \in \mathbb{F}_q[x]$ be a permutation binomial. Let $\mathbb{F}_{p^{s_1}}, \ldots, \mathbb{F}_{p^{s_u}}$ be subfields of $\mathbb{F}_q$ such that for each i, $\mathbb{F}_{p^{s_i}}$ contains the coefficients of some binomial $g_i(x)$, d-equivalent to $f(x)$. Then $\bigcap_{i=1}^{u} \mathbb{F}_{p^{s_i}}$ contains the coefficients of some binomial $g(x)$, d-equivalent to $f(x)$.*

PROOF. We prove the result for $u = 2$. The proposition may be completed easily by induction. By Theorem 3.3(1), the order of a divides both $\operatorname{lcm}(p^{s_1} - 1, (q-1)/d)$ and $\operatorname{lcm}(p^{s_2} - 1, (q-1)/d)$, so by Claim 2, this order divides $\operatorname{lcm}((q-1)/d, \gcd(p^{s_1} - 1, p^{s_2} - 1))$. It is well known that $\gcd(p^{s_1} - 1, p^{s_2} - 1) = p^{\gcd(s_1, s_2)} - 1$ and that $\mathbb{F}_{p^{s_1}} \cap \mathbb{F}_{p^{s_2}} = \mathbb{F}_{p^{\gcd(s_1, s_2)}}$. By Theorem 3.3 again this last field contains the coefficients of some binomial $g(x)$, d-equivalent to $f(x)$. □

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

If we consider all the subfields $\mathbb{F}_{p^{s_i}}$ of $\mathbb{F}_q$ satisfying the given property in the preceding proposition we may conclude that the field $F_0 = \bigcap_i \mathbb{F}_{p^{s_i}}$ contains the coefficients of some binomial $g(x)$, d-equivalent to $f(x)$. We call this field *the smallest field containing the coefficients of some d-equivalent to $f(x)$.*

The next proposition shows that binomials that are conjugate over $\mathbb{F}_q$ or in the same d-class have the same smallest field.

PROPOSITION 3.10. *Let $f(x) = ax^n + x^m \in \mathbb{F}_q[x]$ be a permutation binomial of $\mathbb{F}_q$ and let F_0 be the smallest field containing the coefficients of some d-equivalent to $f(x)$.*

(1) *Let $g(x) \in \mathbb{F}_q[x]$. If $f \overset{d}{\sim} g$, then F_0 is the smallest field containing the coefficients of some d-equivalent to $g(x)$.*
(2) *If $\tilde{f}(x) = a^{p^e}x^n + x^m$, then F_0 is the smallest field containing the coefficients of some d-equivalent to $\tilde{f}(x)$.*

PROOF. (1) Let F_1 be the smallest field corresponding to $g(x)$. For the proof of (1) and by symmetry it is sufficient to prove that $F_0 \subset F_1$. Let $g_1(x)$ be a d-equivalent of $g(x)$ with coefficients in F_1; then $g_1 \overset{d}{\sim} g \overset{d}{\sim} f$, so F_1 contains the coefficients of some d-equivalent to $f(x)$. Therefore $F_0 \subset F_1$.

(2) The result follows from Theorem 3.3, (1) and the observation that a and a^{p^e} have the same order. □

References

[1] L. E. Dickson, 'The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group', *Ann. of Math.* **11**(16) (1896/97), 161–183.
[2] M. Fried, R. Guralnick and J. Saxl, 'Schur covers and Carlitz's conjecture', *Israel J. Math.* **82** (1993), 157–225.
[3] C. Hermite, 'Sur les fonctions de sept lettres', *C. R. Acad. Sci. Paris* **57**(1863)750–757.
[4] R. Lidl and H. Niedereiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications (Cambridge University Press, Cambridge, 2008).
[5] A. Masuda and M. Zieve, 'Permutation binomials over finite fields', *Trans. Amer. Math. Soc.* **361** (2009), 4169–4180.
[6] H. Niederreiter and K. H. Robinson, 'Complete mappings of finite fields', *J. Aust. Math. Soc. (Ser. A)* **33** (1982), 197–212.
[7] C. Small, *Arithmetic of Finite Fields* (Marcel Dekker, New York, 1991).
[8] C. Small, 'Permutation binomials', *Internat. J. Math. Math. Sci.* **13** (1990), 337–342.
[9] G. Turnwald, *Permutation polynomials of binomial type*, Contributions to General Algebra 6 (Holder-Pichler-Tempsky, Vienna, 1988), pp. 281–286.
[10] D. Q. Wan, 'Permutation polynomials over finite fields', *Acta Math. Sinica (N. S.)* **3** (1987), 1–5.
[11] A. Weil, 'Sur les courbes algébriques et les variétés qui s'en déduisent', Actualités Sci. Ind., 1041 (Hermann, Paris, 1948).

MOHAMED AYAD, Laboratoire de Mathématiques Pures et Appliquées,
Université du Littoral, F-62228 Calais, France
e-mail: ayad@lmpa.univ-littoral.fr

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press

KACEM BELGHABA, Laboratoire de Mathématiques et ses Applications,
Université d'Oran, BP 15 24, Algeria
e-mail: belghaba.kacem@univ-oran.dz

OMAR KIHEL, Department of Mathematics, Brock University,
Ontario, Canada L2S 3A1
e-mail: okihel@brocku.ca, okihel@brocku.ca

https://doi.org/10.1017/S0004972713000208 Published online by Cambridge University Press