Technical University of Denmark

On the difference between permutation poynomials over finite fields

Anbar Meidl, Nurdagül; Odzak, Almasa; Patel, Vandita; Quoos, Luciane; Somoza, Anna; Topuzoglu, Alev

Published in:
arXiv

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

On the difference between permutation polynomials over finite fields

Nurdagül Anbar[1], Almasa Odžak[2], Vandita Patel[3], Luciane Quoos[4], Anna Somoza[5,6], Alev Topuzoğlu[7]

[1] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria*
Email: `nurdagulanbar2@gmail.com`
[2] *University of Sarajevo, Zmaja od Bosne 35, 71000 Sarajevo, Bosnia and Herzegovina*
Email: `almasa.odzak@gmail.com`
[3] *University of Warwick, Coventry CV4 7AL, UK*
Email: `vandita.patel@warwick.ac.uk`
[4] *Universidade Federal do Rio de Janeiro, Cidade Universitária, Rio de Janeiro, RJ 21941-909, Brazil*
Email: `luciane@im.ufrj.br`
[5] *Universitat Politècnica de Catalunya, Calle Jordi Girona, 1-3, 08034 Barcelona, Spain*
[6] *Leiden University , Snellius building, Niels Bohrweg 1 2300 RA Leiden, Netherlands*
Email: `anna.somoza@upc.edu`
[7] *SabancıUniversity, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey*
Email: `alev@sabanciuniv.edu`

Abstract

The well-known Chowla and Zassenhaus conjecture, proven by Cohen in 1990, states that if $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial f in $\mathbb{F}_p[x]$ of degree $d \geq 2$. For arbitrary finite fields $\mathbb{F}_q$, a similar non-existence result is obtained recently by Işık, Topuzoğlu and Winterhof in terms of the Carlitz rank of f.

Cohen, Mullen and Shiue generalized the Chowla-Zassenhaus-Cohen Theorem significantly in 1995, by considering differences of permutation polynomials. More precisely, they showed that if f and $f+g$ are both permutation polynomials of degree $d \geq 2$ over $\mathbb{F}_p$, with $p > (d^2-3d+4)^2$, then the degree k of g satisfies $k \geq 3d/5$, unless g is constant. In this article, assuming f and $f+g$ are permutation polynomials in $\mathbb{F}_q[x]$, we give lower bounds for k in terms of the Carlitz rank of f and q. Our results generalize the above mentioned result of Işık et al. We also show for a special class of polynomials f of Carlitz rank $n \geq 1$ that if $f + x^k$ is a permutation over $\mathbb{F}_q$, with $\gcd(k+1, q-1) = 1$, then $k \geq (q-n)/(n+3)$.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where $r \geq 1$ and p is a prime. Throughout we assume $q \geq 3$. We recall that $f \in \mathbb{F}_q[x]$ is a *permutation polynomial* over $\mathbb{F}_q$ if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. If $f(x)$ and $f(x)+x$ are both permutation polynomials over $\mathbb{F}_q$, then f is called a *complete mapping*. We refer the reader to [11] for a detailed study of complete mapping polynomials over finite fields. Their use in the construction of mutually orthogonal Latin squares is described, for instance, in [9]. For various other applications, see [10, 12, 13, 14]. The paper [8] lists some recent work on complete mappings.

The Theorem 1 below was conjectured by Chowla and Zassenhaus [3] in 1968, and proven by Cohen [5] in 1990.

Theorem 1. If $d \geq 2$ and $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial of degree d over $\mathbb{F}_p$.

A significant generalization of this result was obtained by Cohen, Mullen and Shiue [6] in 1995, and gives a lower bound for the degree of the difference of two permutation polynomials in $\mathbb{F}_p[x]$ of the same degree d, when $p > (d^2 - 3d + 4)^2$.

Theorem 2. Suppose f and $f + g$ are monic permutation polynomials over $\mathbb{F}_p$ of degree $d \geq 3$, where $p > (d^2 - 3d + 4)^2$. If $\deg(g) = k \geq 1$, then $k \geq 3d/5$.

An alternative invariant, the so-called Carlitz rank, attached to permutation polynomials, was used by Işık, Topuzoğlu and Winterhof [8] recently to obtain a non-existence result, similar to that in Theorem 1. The concept of Carlitz rank was first introduced in [1]. We describe it here briefly. The interested reader may see [16] for details.

By a well-known result of Carlitz [2] that any permutation polynomial over

$\mathbb{F}_q$, with $q \geq 3$ is a composition of linear polynomials $ax+b$, $a,b \in \mathbb{F}_q$, $a \neq 0$, and x^{q-2}, any permutation f over $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = \Big(\dots\big((a_0x+a_1)^{q-2}+a_2\big)^{q-2}\dots+a_n\Big)^{q-2}+a_{n+1}, \tag{1.1}$$

for some $n \geq 0$, where $a_i \neq 0$, for $i = 0, 2, \dots, n$. Note that $f(c) = P_n(c)$ holds for all $c \in \mathbb{F}_q$, however this representation is not unique, and n is not necessarily minimal. Accordingly the authors of [1] define the *Carlitz rank* of a permutation polynomial f over $\mathbb{F}_q$ to be the smallest integer $n \geq 0$ satisfying $f = P_n$ for a permutation P_n of the form (1.1), and denote it by $\mathrm{Crk}(f)$.

The representation of f as in (1.1) enables approximation of f by a fractional transformation in the following sense.

For $0 \leq k \leq n$, consider

$$R_k(x) = \frac{\alpha_{k+1}x+\beta_{k+1}}{\alpha_k x+\beta_k}\ , \tag{1.2}$$

where $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$, and

$$\alpha_k = a_k\alpha_{k-1}+\alpha_{k-2} \quad \text{and} \quad \beta_k = a_k\beta_{k-1}+\beta_{k-2} \tag{1.3}$$

for $k \geq 2$. The set

$$\mathcal{O}_n = \left\{x_k :\ x_k = \frac{-\beta_k}{\alpha_k}\ ,\ k = 1,\dots,n\right\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\} \tag{1.4}$$

is called the *set of poles* of f. The elements of $\mathcal{O}_n$ may not be distinct.

It can easily be verified that

$$f(c) = P_n(c) = R_n(c) \ \text{ for all } \ \mathrm{c} \in \mathbb{F}_q \setminus \mathcal{O}_n\ . \tag{1.5}$$

Obviously, this property is particularly useful when $\mathrm{Crk}(f)$ is small with respect to the field size. The values that f takes on $\mathcal{O}_n$ can also be expressed in terms of R_n, see [16]. In case $\alpha_n = 0$, i.e., the last *pole* $x_n = \infty$, R_n is linear. Following the terminology of [8], we define the *linearity* of $f \in \mathbb{F}_q[x]$ as $\mathcal{L}(f) = \max_{a,b\in\mathbb{F}_q} |\{c \in \mathbb{F}_q : f(c) = ac+b\}|$. Intuitively $\mathcal{L}(f)$ is large when f is a permutation polynomial of $\mathbb{F}_q$ of $\mathrm{Crk}(f) = n,\ R_n$ is linear, and n is small with respect to q.

Now we are ready to state the main result of [8]. We remark that the Theorems 1 and 2 hold over prime fields only, while the Theorem 3 is true for any finite field.

Theorem 3. If $f(x)$ is a complete mapping over $\mathbb{F}_q$ and $\mathcal{L}(f) < \lfloor (q+5)/2 \rfloor$, then $\mathrm{Crk}(f) \geq \lfloor q/2 \rfloor$.

The purpose of this note is to obtain a lower bound for the degree of the difference between two permutation polynomials, analogous to Theorem 2, generalizing Theorem 3. In what follows we assume that f and $f+g$ are permutation polynomials over $\mathbb{F}_q$, where $g \in \mathbb{F}_q[x]$ has degree k with $1 \leq k < q-1$. We give lower bounds for k in terms of q and the Carlitz rank of f, see Theorems 2.1 and 3.1 below.

2 Degree of the difference of two permutation polynomials

Let f be a permutation polynomial over $\mathbb{F}_q$, $q \geq 3$, with $\mathrm{Crk}(f) = n \geq 1$. Suppose that f has a representation as in (1.1) and the fractional linear transformation R_n in (1.2), which is associated to f as in (1.5) is not linear, in other words α_n in (1.3) is not zero. We denote the set of all such permutations by $\mathcal{C}_{1,n}$, i.e., the set $\mathcal{C}_{1,n}$ consists of all permutation polynomials over $\mathbb{F}_q$, satisfying $\mathrm{Crk}(f) = n \geq 1$ and $\alpha_n \neq 0$. Clearly $\mathcal{L}(f) \leq n+2$, if $f \in \mathcal{C}_{1,n}$. We note that permutations $f \in \mathbb{F}_q[x]$ with $\alpha_n = 0$ behave very differently. For instance, there are examples of complete mappings over $\mathbb{F}_q$ of Carlitz rank 4 for infinitely many values of q. Indeed, the condition on the linearity of f in Theorem 3 corresponds to the case $\alpha_n = 0$. Therefore, we only consider permutations in $\mathcal{C}_{1,n}$.

We now prove our main theorem.

Theorem 2.1. *Let f and $f+g$ be permutation polynomials over $\mathbb{F}_q$, where $f \in \mathcal{C}_{1,n}$ and the degree k of $g \in \mathbb{F}_q[x]$ satisfies $1 \leq k < q-1$. Then*

$$nk + k(k-1)\sqrt{q} \geq q - \nu - n \ , \tag{2.1}$$

where $\nu = \gcd(k, q-1)$.

Proof. Since $f \in \mathcal{C}_{1,n}$, there exist $a, b, d \in \mathbb{F}_q$, such that $f(z) = R_n(z)$ for $z \in \mathbb{F}_q \setminus \mathcal{O}_n$, where

$$R_n(z) = \frac{az+b}{z+d} \ .$$

The fact that $ad - b \neq 0$ follows from (1.3).

The polynomial $f(z) + g(z)$ can be represented by $G_n(z) = R_n(z) + g(z)$ for $z \in \mathbb{F}_q \setminus \mathcal{O}_n$. Since $f+g$ is a permutation over $\mathbb{F}_q$, the map G_n is injective on $\mathbb{F}_q \setminus \mathcal{O}_n$.

For $u \in \mathbb{F}_q$ and

$$G_n(z) = \frac{az+b}{z+d} + g(z) = u \ , \tag{2.2}$$

we set

$$H_n(x) = G_n(x-d) = \frac{ax - \tilde{b}}{x} + h(x) = u \ .$$

where $\tilde{b} = ad - b \neq 0$ and $h(x) = g(x-d)$. Note that $H_n(x) = u$ for some nonzero $x \in \mathbb{F}_q$ if and only if $z \neq -d$ is a solution of Equation (2.2). Let S be the set of pairs $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ such that

$$S = \left\{ \, (x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \, : \, x \neq y \ \text{ and } \ H_n(x) = H_n(y) \, \right\} \ .$$

Denote the value set of H_n by V_{H_n}, i.e.,

$$V_{H_n} = \{ u \in \mathbb{F}_q : \exists \, x \in \mathbb{F}_q \ \text{ with } \ H_n(x) = u \} \ .$$

Suppose that the cardinality $|S|$ of S is μ. For $u \in V_{H_n}$, we consider the inverse image; $H_n^{-1}(u) = \{x \in \mathbb{F}_q : \ H_n(x) = u\}$ and put $n_u = |H_n^{-1}(u)|$. We remark that $0 \notin H_n^{-1}(u)$ and that $x \in H_n^{-1}(u)$ if and only if x is a root of the polynomial

$$xh(x) + (a-u)x - \tilde{b} \ . \tag{2.3}$$

This shows that for any $u \in V_{H_n}$ we have $n_u \leq k+1$ as the polynomial in Equation (2.3) has degree $k+1$. We then conclude that

$$\mu = \sum_{u \in V_{H_n}} n_u(n_u - 1) \leq (k+1) \sum_{u \in V_{H_n}} (n_u - 1) \ . \tag{2.4}$$

If there exist n_u distinct elements x with $H_n(x) = u$, then there exist n_u distinct elements z with $G_n(z) = u$. Since $G_n(z)$ is injective on $\mathbb{F}_q \setminus \mathcal{O}_n$, this shows that $n_u - 1$ distinct elements z lie in the set of poles $\mathcal{O}_n$. In particular, by Equation (2.4) and the fact that $-d \in \mathcal{O}_n$ we conclude that

$$n \geq |\mathcal{O}_n| \geq 1 + \sum_{u \in V_{H_n}} (n_u - 1) \geq 1 + \frac{\mu}{k+1} \ . \tag{2.5}$$

Therefore in order to obtain a lower bound for k in terms of q and n, it is sufficient to determine μ in relation to q and k.

We can re-write the equation $H_n(x) = H_n(y)$ as

$$y(xh(x) - \tilde{b}) - x(yh(y) - \tilde{b}) = 0 \ .$$

Note that $x-y$ is a factor of $y(xh(x)-\tilde{b})-x(yh(y)-\tilde{b})$. We want to find an absolutely irreducible factor over $\mathbb{F}_q$ of the polynomial in two variables of degree $k+1$ defined by

$$\frac{y(xh(x)-\tilde{b})-x(yh(y)-\tilde{b})}{x-y} \ ,$$

or equivalently defined by

$$xy\frac{h(x)-h(y)}{x-y}+\tilde{b} \ . \tag{2.6}$$

We recall that a rational function $\ell(x)/t(x) \in \mathbb{F}_q(x)$ is called *exceptional* over $\mathbb{F}_q$ if the polynomial $\Theta_{\ell/t}$, defined by

$$\Theta_{\ell/t} = \frac{t(Y)\ell(X)-t(X)\ell(Y)}{X-Y}$$

has no absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. By Theorem 5 of [4], ℓ/t is a permutation over $\mathbb{F}_q$ if it is an exceptional function over $\mathbb{F}_q$. In particular, $t(\alpha) \neq 0$ for all $\alpha \in \mathbb{F}_q$. Now we put $\ell/t = (xh(x)-\tilde{b})/x$, and conclude that the rational function in (2.6) has an absolutely irreducible factor $p(x,y)$ over $\mathbb{F}_q$. We note that $\tilde{b}$ is not zero and hence $p(x,y)$ is a factor different from $x-y$. Moreover we assume without loss of generality that $p(x,y)$ is separable; otherwise we can replace $p(x,y)$ with a separable polynomial of smaller degree.

Consider the curve $\mathcal{X}$ whose affine equation is given by $p(x,y)$ of degree $\varrho \leq k+1$. Then by [7, Theorem 9.57] the number of rational points $N(\mathcal{X})$ in $PG(2,q)$ of $\mathcal{X}$ is bounded by

$$N(\mathcal{X}) \geq q+1-(\varrho-1)(\varrho-2)\sqrt{q} \geq q+1-k(k-1)\sqrt{q} \ .$$

We denote by $P(X,Y,Z)$ the homogenized polynomial of $p(x,y)$, i.e.,

$$P(X,Y,Z) = Z^{\varrho} p\left(\frac{X}{Z},\frac{Y}{Z}\right) \ .$$

In order to find the number of affine solutions $(x:y:1)$ such that $xy \neq 0$ and $x \neq y$, we proceed as follows. From Equation (2.6) we have that $P(X,Y,Z)$ is a divisor of the homogeneous polynomial

$$XYZ^{k-1}\left(\frac{h(X/Z)-h(Y/Z)}{X-Y}\right)+\tilde{b}Z^{k+1} \ . \tag{2.7}$$

Hence we conclude that there is no affine solution $(x : y : 1)$ of $P(X, Y, Z)$ with $xy = 0$. We now estimate the number of rational points of $\mathcal{X}$ at infinity, i.e., the points of the form $(x : y : 0)$ for $x, y \in \mathbb{F}_q$. By Equation (2.7) the point $(x : y : 0)$ is on $\mathcal{X}$ only if

$$xy\frac{x^k - y^k}{x - y} = 0 \ .$$

This holds only if $(x : y : 0) = (0 : 1 : 0), (1 : 0 : 0)$ or $x^k = y^k$ for some $x, y \in \mathbb{F}_q^*$. Since $\nu = \gcd(k, q-1)$, the equality $x^k = y^k$ is satisfied if and only if x/y is an ν-th root of unity in $\mathbb{F}_q$. Hence there exist at most $\nu + 2$ rational points of $\mathcal{X}$ lying at infinity.

Bezout's theorem implies that there are at most $k + 1$ rational points $(x : y : z)$ of $\mathcal{X}$ with $x = y$, since the degree of $\mathcal{X}$ is at most $k + 1$.

This shows that the cardinality μ of the set S satisfies

$$\mu \geq q + 1 - k(k-1)\sqrt{q} - (\nu + k + 2) \ .$$

Note that we subtract $\nu + k + 2$ instead of $\nu + k + 3$. This is because of the point $(1 : 1 : 0)$. If $(1 : 1 : 0)$ is on $\mathcal{X}$ then it is taken into account twice. If it is not on $\mathcal{X}$ then we do not have to exclude it as a point at infinity. Therefore, $\mathrm{Crk}(f) = n$ satisfies

$$\begin{aligned} n &\geq 1 + \frac{1}{k+1}(q + 1 - k(k-1)\sqrt{q} - (\nu + k + 2)) \\ &= \frac{1}{k+1}(q - k(k-1)\sqrt{q} - \nu) \ , \end{aligned}$$

by (2.5), which implies the desired result. □

For $k = 1$ (and hence $\nu = 1$) we obtain Theorem 3, i.e., the main result in [8].

Corollary 2.2. *Let $f \in \mathcal{C}_{1,n}$. If $n < (q-1)/2$, then f is not a complete mapping.*

Remark 2.3. We note that the bound given in (2.1) is non-trivial only when $q \geq k(k-1)\sqrt{q} + k + \nu + 1$.

3 The case $g(x) = cx^k$

Throughout this section we focus on the monomials $g(x) = cx^k \in \mathbb{F}_q[x]$ and $f \in \mathcal{C}_{1,n}$, where $x_n \in \mathcal{O}_n$ in (1.4) satisfies $x_n = 0$. In this particular case, the lower bound in (2.1) can be simplified significantly when $\gcd(k+1, q-1) = 1$. Let $\mathcal{C}_{2,n}$ be the set of $f \in \mathcal{C}_{1,n}$ such that the last pole x_n of f is zero.

Theorem 3.1. *Let $f(x)$ and $f(x) + cx^k$ be permutation polynomials over $\mathbb{F}_q$, where $f \in \mathcal{C}_{2,n},\ 1 \leq k < q-1,\ c \in \mathbb{F}_q^*$. Put $m = \gcd(k+1, q-1)$. Then*

$$k(n+3) + (k-1)(m-1)\sqrt{q} \geq q - n \ .$$

In particular, if $m = 1$, then $k \geq (q-n)/(n+3)$.

Proof. The condition $x_n = 0$ implies that β_n in (1.3) is zero. Hence we have $R_n(x) = \frac{ax+b}{x}$ for some $a, b \in \mathbb{F}_q$, with $b \neq 0$. That is, for $x \in \mathbb{F}_q \setminus \mathcal{O}_n$ we can represent $f + cx^k$ by $G_n(x) = R_n(x) + cx^k$.

We proceed as in the proof of Theorem 2.1. The equation $G_n(x) = u$ for some $u \in \mathbb{F}_q$ becomes

$$\frac{ax+b}{x} + cx^k = u \ .$$

Then for some $x, y \in \mathbb{F}_q^*$, we have $G_n(x) = G_n(y)$ if and only if the equation

$$cx^k + \frac{b}{x} = cy^k + \frac{b}{y} \ ,$$

or equivalently the equation

$$x^k - y^k = \frac{b}{c}\left(\frac{x-y}{xy}\right) \tag{3.1}$$

holds.

We again consider the set S of pairs $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*,\ x \neq y$, where (x, y) is a solution of (3.1), and denote the cardinality of S by μ. By using the argument given in the proof of Theorem 2.1, we have $n \geq 1 + \mu/(k+1)$. Hence our aim now is to express μ in terms of q and k.

Applying the change of variable $(x, y) \to (xy, y)$, Equation (3.1) becomes

$$y^k(x^k - 1) = \frac{b(x-1)}{cxy} \ .$$

Hence we are looking for the affine points $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of the curve

$$\mathcal{X} :\ y^{k+1} = \frac{b(x-1)}{cx(x^k-1)} \ . \tag{3.2}$$

Note that in this case the solutions should not lie in the set $\{(\gamma^2,\gamma)\,|\,\gamma\in\mathbb{F}_q\}$. Recall that $m=\gcd(k+1,q-1)$, hence the monomial $y^{(k+1)/m}$ gives rise to a permutation over $\mathbb{F}_q^*$. Therefore, there is one-to-one correspondence between the affine solutions $(x,y)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$ of the curves

$$\mathcal{Y}:\; y^m=\frac{b(x-1)}{cx(x^k-1)}\;, \tag{3.3}$$

and $\mathcal{X}$ in (3.2). Equation (3.3) defines a Kummer extension. Then by using arithmetic of function fields, see [15, Proposition 3.7.3], we can estimate the number of $\mathbb{F}_q$-rational points of $\mathcal{Y}$ as follows.

For the rational function field $\mathbb{F}_q(x)$ and $\alpha\in\mathbb{F}_q$, we denote by $(x=\alpha)$ and $(x=\infty)$ the places corresponding to the zero and the pole of $x-\alpha$, respectively. Let $F=\mathbb{F}_q(x,y)$ be the function field of $\mathcal{Y}$ defined by Equation (3.3), and let $k=p^\ell t$ with $\gcd(p,t)=1$. It is clear that the places $(x=0)$ and $(x=\alpha)$, with $\alpha^t=1$ and $\alpha\neq 1$, are totally ramified in F. In particular, this shows that the full constant field of F is $\mathbb{F}_q$. For the place $(x=\infty)$ we have the ramification index $e_\infty=m/\gcd(m,k)=m$, since m is a divisor of $k+1$. Moreover, for $(x=1)$ the ramification index is given by $e_1=m/\gcd(m,p^\ell-1)$. Hence we conclude that the number of ramified places of $\mathbb{F}_q(x)$ in F is at most $k/p^\ell+2$ if $\ell>0$ and is exactly $k+1$ if $\ell=0$. That is, the place $(x=1)$ can be ramified only if $\ell>0$. We consider the case $\ell=0$, i.e. $\gcd(k,p)=1$, where the genus of F is the largest. In this case, the ramified places are exactly

$$(x=0),\quad (x=\infty)\quad\text{and}\quad (x=\alpha)\quad\text{with}\quad \alpha^k=1\text{ and }\alpha\neq 1\;.$$

Therefore, the degree of the different divisor of $F/\mathbb{F}_q(x)$ is $(k+1)(m-1)$. Then by the Hurwitz genus formula the genus $g(F)$ of F satisfies

$$2g(F)-2=-2m+(k+1)(m-1)\;,$$

which implies that $g(F)=(k-1)(m-1)/2$. By the Hasse–Weil theorem the number $N(F)$ of $\mathbb{F}_q$-rational places of F is bounded by

$$N(F)\geq q+1-2g(F)\sqrt{q}=q+1-(k-1)(m-1)\sqrt{q}\;. \tag{3.4}$$

We observe that the pole divisors $(x)_\infty$, $(y)_\infty$ of x,y are

$$(x)_\infty=mP_\infty\quad\text{and}\quad (y)_\infty=P_0+\sum_{\alpha^k=1,\alpha\neq1}P_\alpha\;,$$

where P_∞, P_0, P_α are the unique places of F lying over $(x=\infty), (x=0), (x=\alpha)$, respectively.

We remark that the curve $\mathcal{Y}$ defined by Equation (3.3) is of degree $k+m$ and has two points at infinity; namely $Q_1 = (1:0:0)$ and $Q_2 = (0:1:0)$. These are the only singular points of $\mathcal{Y}$ and Q_1 has intersection multiplicity m while Q_2 is an ordinary point of multiplicity k. Moreover, P_∞ is the unique place corresponding to Q_1, and there are k places corresponding to Q_2, which correspond to the places lying in the support of $(y)_\infty$. All the affine points in the curve $\mathcal{Y}$ defined by Equation (3.3) are non-singular and there is a one to one correspondence between these points and the places in the function field F of $\mathcal{Y}$ which do not lie in the support of pole divisors of x and y. Moreover, the fact that the zero divisors of x and y are $(x)_0 = mP_0$ and $(y)_0 = kP_\infty$, respectively, implies that the rational places not lying in the pole divisors correspond to points $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Therefore, Equation (3.4) implies that the number of affine points $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of $\mathcal{Y}$ is at least $q-(k-1)(m-1)\sqrt{q}-k$.

Now we turn our attention to the curve $\mathcal{X}$ in Equation (3.2). We have seen that $\mathcal{X}$ has at least $q-(k-1)(m-1)\sqrt{q}-k$ affine points $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Next we estimate the number of affine points (x,y) of $\mathcal{X}$ such that (x,y) is not of the form (γ^2,γ) for some $\gamma \in \mathbb{F}_q$. By Equation (3.2), the affine point (γ^2,γ) lies on $\mathcal{X}$ if and only if γ is a root of

$$T^{k+1}\sum_{i=1}^{k} T^{2i} - \frac{b}{c} \ . \tag{3.5}$$

Since the polynomial in Equation (3.5) has degree $3k+1$, there can be at most $3k+1$ such points. Hence the number μ of affine solutions $(x,y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of Equation (3.2), which do not lie on the curve $x = y^2$ satisfies

$$\mu \geq q-(k-1)(m-1)\sqrt{q}-(4k+1) \ .$$

Therefore $\mathrm{Crk}(f) = n$ satisfies

$$n \geq 1 + \frac{1}{k+1}(q-(k-1)(m-1)\sqrt{q}-(4k+1)) \ .$$

□

Example 3.2. For $q=9$, $n=3$ and $m=1$, the bound in Theorem 3.1 gives $k \geq 1$. Combining with Corollary 2.2 we get $k \geq 2$ as $q > 2n+1$. Let ζ be a primitive element of $\mathbb{F}_9$ and consider the permutation polynomial $f(x) = (((x+a)^7)+b)^7+c)^7 \in \mathbb{F}_9[x]$ of Carlitz rank 3, where $a=\zeta^5$, $b=\zeta^6$ and $c=\zeta^3$. It can be checked easily that $f(x)+x^2$ is a permutation polynomial of $\mathbb{F}_9$.

Remark 3.3. As we have seen in Example 3.2, the bound in Theorem 3.1 is weaker than the one in Theorem 2.1 for $k = 1$. The reason is the change of variable $(x, y) \to (xy, y)$ in the proof of Theorem 3.1. However, a direct calculation in this specific case is possible, and gives an alternative proof for Theorem 3, which was proven in [8]. In fact, the change of variable is not needed when $k = 1$ as Equation (3.1) becomes $xy = b$. In this case, each non-zero x uniquely determines y, i.e., there exists $q-1$ distinct solutions (x, y) of $xy = b$. We also leave out the solutions (x, y) with $x = y$. We therefore obtain $\mu = q-2$ if q is even, and $\mu = q-3$ or $q-1$ (depending on b being square or not) if q is odd. Then the fact that $n \geq 1 + \mu/2$ implies Corollary 2.2.

Acknowledgement

The initial work on this project began during “Women in Numbers Europe 2 (WIN-E2)” workshop, held in the Lorentz Centre, Leiden in September 2016. The authors are grateful to the Lorentz Centre and all supporting institutions for making this conference and collaboration possible. They would especially like to thank the organisers of WIN-E2, Irene Bouw, Rachel Newton and Ekin Özman for all of their hard work, as this resulted in an extremely fruitful and enjoyable meeting.

The authors N.A.; A.O.; V.P.; L.Q. and A.T. are partially supported by H.C. Ørsted COFUND Post-doc Fellowship from the project “Algebraic curves with many rational points”; Federal Ministry of Education and Science, grant No.05-39-3663-1/14; an EPSRC studentship; CNPq, PDE grant number 200434/2015-2 and TUBİTAK project number 114F432, respectively.

References

[1] E. Aksoy, A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *On the Carlitz rank of a permutation polynomial*, Finite Fields Appl. 15 (2009), 428–440.

[2] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc. 4 (1953), 538.

[3] S. Chowla, H. Zassenhaus, *Some conjectures concerning finite fields*, Nor. Vidensk. Selsk. Forh. (Trondheim) 41 (1968), 34–35.

[4] S.D. Cohen, *The distribution of polynomials over finite fields*, Acta Arithmetica 17 (1970), 255–271.

[5] S.D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, Can. Math. Bull. 33 (1990), 230–234.

[6] S.D. Cohen, G.L. Mullen, P.J.-S. Shiue, *The difference between permutation polynomials over finite fields*, Proc. Amer. Math. Soc. 123 (1995), 2011–2015.

[7] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic curves over a finite field*, Princeton University Press, 2013.

[8] L. Işık, A. Topuzoğlu and A. Winterhof, *Complete mappings and Carlitz rank*, Des. Codes Cryptogr., DOI 10.1007/s10623-016-0293-5.

[9] C.F. Laywine, G. Mullen, *Discrete mathematics using Latin squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.

[10] A. Muratovic-Ribic, E. Pasalic, *A note on complete mapping polynomials over finite fields and their applications in cryptography*, Finite Fields Appl. 25 (2014), 306–315.

[11] H. Niederreiter, K.H. Robinson, *Complete mappings of finite fields*, J. Aust. Math. Soc. A 33 (1982), 197–212.

[12] R.-H. Schulz, *On check digit systems using anti-symmetric mappings*, in: Numbers, Information and Complexity (Bielefeld, 1998), 295–310, Kluwer Acad. Publ., Boston, MA, 2000.

[13] R. Shaheen, A. Winterhof, *Permutations of finite fields for check digit systems*, Des. Codes Cryptogr. 57 (2010), 361–371.

[14] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inf. Theory 58 (2012), 4064–4072.

[15] H. Stichtenoth, *Algebraic function fields and codes*, 2$^{\text{nd}}$ Edition, Graduate Texts in Mathematics 254, Springer Verlag, 2009.

[16] A. Topuzoğlu, *Carlitz rank of permutations of finite fields: A survey*, J. Symb. Comput. 64 (2014), 53–66.