INDEX BOUNDS FOR VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

GARY L. MULLEN, DAQING WAN, AND QIANG WANG

We dedicate this paper to the occasion of Harald Niederreiter's 70-th birthday. His work on permutation polynomials over finite fields, and more generally, his work in so many areas of finite fields and their applications, has been a huge and lasting inspiration to all of us.

Abstract. We provide an upper bound for the cardinality of the value set of a univariate polynomial over a finite field in terms of the index of the polynomial. Moreover, we study when a polynomial vector map in n variables is a permutation polynomial map, again using the index tuple of the map. This also provides an upper bound for the value set of a polynomial map in n variables.

1. introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. The *value set* of a polynomial g over $\mathbb{F}_q$ is the set V_g of images when we view g as a mapping from $\mathbb{F}_q$ to itself. Clearly g is a *permutation polynomial (PP)* of $\mathbb{F}_q$ if and only if the cardinality $|V_g|$ of the value set V_g of g is q. Asymptotic formulas such as $|V_g| = \lambda(g)q + O(q^{1/2})$, where $\lambda(g)$ is a constant depending only on certain Galois groups associated to g, can be found in Birch and Swinnerton-Dyer [7] and Cohen [16]. Later, Williams [39] proved that almost all polynomials f are polynomials satisfying $\lambda(g) = 1 - \frac{1}{2!} + \frac{1}{3!} + \cdots + (-1)^{d-1}\frac{1}{d!}$, where d is the degree of the polynomial g. There are also several results on explicit bounds for the cardinality of value sets if g is not a PP over $\mathbb{F}_q$; see for example [33, 34]. Perhaps the most well-known result is due to Wan [34] who proved that if g is not a PP then

$$|V_g| \leq q - \frac{q-1}{d}. \tag{1}$$

Using results from group theory, Guralnick and Wan [20] further proved that if $(d,q) = 1$ then $|V_g| \leq (47/63)q + O_d(\sqrt{q})$. Some progress on lower bounds of $|V_g|$ can be found in [17, 36]. The classification of *minimal value set polynomials* (polynomials satisfying $|V_g| = \lceil q/d \rceil$) can be found in [11, 19, 27], and in [8] for all the minimal

2000 *Mathematics Subject Classification.* 11T06.

Key words and phrases. polynomials, value sets, permutation polynomials, finite fields.

Research of Daqing Wan and Qiang Wang was partially supported by NSF, NSERC of Canada, and National Natural Science Foundation of China (Grant No. 61170289).

value set polynomials in $\mathbb{F}_q[x]$ whose set of values is a subfield of $\mathbb{F}_q$. More recently, algorithms and complexity in computing $|V_g|$ have been studied in [13]. All of these results relate $|V_g|$ to the degree d of g.

In this paper, we take a different approach to study value sets. We note that any non-constant polynomial $g \in \mathbb{F}_q[x]$ of degree $\leq q-1$ can be written *uniquely* as $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$ with index ℓ defined below. Namely, write

$$g(x) = a(x^n + a_{n-i_1}x^{n-i_1} + \cdots + a_{n-i_k}x^{n-i_k}) + b,$$

where $a,\ a_{n-i_j} \neq 0,\ j = 1, \ldots, k$. The case that $k = 0$ is trivial. Thus, we shall assume that $k \geq 1$. Write $n - i_k = r$, the vanishing order of x at 0 (i.e., the lowest degree of x in $g(x) - b$ is r). Then $g(x) = a\left(x^r f(x^{(q-1)/\ell})\right) + b$, where $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + \cdots + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$\ell = \frac{q-1}{\gcd(n-r, n-r-i_1, \ldots, n-r-i_{k-1}, q-1)} := \frac{q-1}{s},$$

and $\gcd(e_0, e_1, \ldots, e_{k-1}, \ell) = 1$. The integer $\ell = \frac{q-1}{s}$ is called the *index* of $h(x)$. The concept of the index of any polynomial was first introduced in [2] and is closely related to the concept of the least index of a cyclotomic mapping polynomial [14, 32]. Clearly, the study of the value set of $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$ over $\mathbb{F}_q$ is equivalent to studying the value set of $g(x) = x^r f(x^{(q-1)/\ell}) = x^r f(x^s)$ over $\mathbb{F}_q$. If $(r, (q-1)/\ell) = 1$, we say g is in *reduced form*. Otherwise, if $(r, (q-1)/\ell) = t$, then $g(x) = g'(x^t)$ where $g'(x) = x^{r/t} f(x^{s/t})$ is in reduced form. In fact a permutation polynomial g must be in reduced form. We note that permutation polynomials of the form $x^r f(x^s)$ were studied by Wan and Lidl [35] in 1991 and more recently by many others in [1, 2, 4, 5, 6, 15, 37, 43, 44, 45]. For more background material on permutation polynomials we refer to Chap. 7 of [24]. For a detailed survey see [22, 23, 28, 31] and recent results see [3, 9, 10, 12, 18, 21, 38, 40, 41, 42]. We refer to Section 8.1 of [29] for a detailed discussion of PPs and Section 8.3 of [29] for a discussion of value sets of polynomials over finite fields.

In Section 2, we study the value set problem in terms of the index of the polynomial g. In Theorem 2.1 we prove that if g is not a PP then

$$|V_g| \leq q - \frac{q-1}{\ell}. \tag{2}$$

Our result improves Wan's result when the index ℓ of a polynomial is strictly smaller than the degree d. We note that the index ℓ of a polynomial is always smaller than the degree d as long as $\ell \leq \sqrt{q} - 1$. For example, the index of any permutation binomial is always less than or equal to the degree. In fact, the index of polynomials is closely related to the concept of the least index of cyclotomic permutations. These permutations in terms of cyclotomic cosets were studied by Niederreiter and Winterhof in [32] and Wang [37, 38]. Also in Section 2 a generic formula for $|V_g|$ in terms of the number of certain distinct cyclotomic cosets is given in Proposition 2.3.

Let $g : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a polynomial map in n variables defined over $\mathbb{F}_q$, where n is a positive integer. Denote by $|V_g|$ the number of distinct values taken by $g(x_1, \ldots, x_n)$ as $(x_1, \ldots, x_n)$ runs over $\mathbb{F}_q^n$. It is clear that $|V_f| \leq q^n$. If $|V_f| = q^n$, then f is a *permutation polynomial vector*, see [24, Chapter 7]. Motivated by an open problem raised by Lipton [25] in his computer science blog, we extended Wan's result on upper bounds of value sets for univariate polynomials to polynomial maps in n variables in [30]. More specifically, we write g as a polynomial vector:

$$g(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)), \tag{3}$$

where each g_i $(1 \leq i \leq n)$ is a polynomial in n variables over $\mathbb{F}_q$. The polynomial vector g induces a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$. By reducing the polynomial vector g modulo the ideal $(x_1^q - x_1, \ldots, x_n^q - x_n)$, we may assume that the degree of g_i in each variable is at most $q-1$ and we may further assume that g is a non-constant map to avoid the trivial case. Let d_i denote the total degree of f_i in the n variables $x_1, \ldots, x_n$ and let $d = \max\{d_1, \ldots, d_n\}$. Then d satisfies $1 \leq d \leq n(q-1)$. In particular, we proved

Theorem 1.1. [30] *If $|V_g| < q^n$, then $|V_g| \leq q^n - \min\left\{\frac{n(q-1)}{d}, q\right\}$.*

In Section 3, we extend the concept of index of an univariate polynomial to index tuples for multivariate polynomials $g_i(x_1, \ldots, x_n)$ for $1 \leq i \leq n$ and the polynomial vector map $g(x_1, \ldots, x_n)$ respectively. We remark that any multivariate polynomial $g_i(x_1, \ldots, x_n)$ behaves as a monomial in each subset of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ that is partitioned by the cyclotomic cosets determined by the index tuple $(\ell_1^{(i)}, \ldots, \ell_n^{(i)})$. Similarly, each coordinate $g_i(x_1, \ldots, x_n)$ of any polynomial vector map $g(x_1, \ldots, x_n)$ behaves as a monomial when we view the vector map as a cyclotomic mapping. It turns out the index tuple $(\ell_1, \ldots, \ell_n)$ of $g(x_1, \ldots, x_n)$ can be obtained from index tuples $(\ell_1^{(i)}, \ldots, \ell_n^{(i)})$ of $g_i(x_1, \ldots, x_n)$'s. Namely, $\ell_i = lcm(\ell_i^{(1)}, \ldots, \ell_i^{(n)})$ for $1 \leq i \leq n$. Then we study the extreme cases for the value set problem for polynomial maps of n variables. Namely, we describe when a polynomial map g in n variables is a permutation polynomial map. Essentially, each coordinate polynomial of a permutation vector map behaves as a monomial in terms of only one variable in each subset of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ that is partitioned by the cyclotomic cosets determined by the index tuple $(\ell_1, \ldots, \ell_n)$, along with other explicit conditions as described in Theorem 3.5. In other words, each permutation vector map in n variables consists of n univariate cyclotomic monomial permutations together with another permutation on coordinate variables. As a corollary, we obtain

Theorem 1.2. *Let g be a polynomial vector map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ with the index tuple $(\ell_1, \ldots, \ell_n)$ and $\ell = \max\{\ell_1, \ldots, \ell_n\} > 1$. If $|V_g| < q^n$ then $|V_g| \leq q^n - \frac{q-1}{\ell}$.*

This also provides another answer to Lipton's problem on the existence of a Picard jump for polynomial maps (roughly, if g misses one value in $\mathbb{F}_q^n$ then g misses quite a few). An example meeting this upper bound is also provided. We also note that our new bound improves the bound in Theorem 1.1 when $\frac{d}{n} > \ell$.

2. Value sets of univariate polynomials

As explained in the introductory section, the value set problem for a univariate polynomial is equivalent to that for the polynomial $g(x) = x^r f(x^s)$. Here we want to emphasize the parameter index ℓ instead of the degree d. We note from [37] that $g(x) = x^r f(x^s)$ is a PP if and only if $\gcd(r, s) = 1$, and $f(\zeta^i) \neq 0$ for $0 \leq i \leq \ell - 1$ where ζ is a primitive ℓ-th root of unity, and $g(x)$ induces a permutation among all the ℓ cyclotomic cosets

$$\{C_0, C_1, \cdots, C_{\ell-1}\} = \mathbb{F}_q^*/(\mathbb{F}_q^*)^\ell.$$

In fact, we can always write $g(x)$ in terms of *cyclotomic mappings* $g(x) = c_i x^r$ if $x \in C_i$, where $c_i = f(\zeta^i)$; more details can be found in [14, 32, 37, 38]. In particular, a polynomial $g(x) \in \mathbb{F}_q[x]$ is called an orthomorphism if both $g(x)$ and $g(x) - x$ are permutation polynomials. Given a finite, nonempty set of positive integers R, a polynomial $g(x)$ is called an R-orthomorphism if $g^{(r)}(x)$ is an orthomorphism of $\mathbb{F}_q$ for all $r \in R$. (Here $g^{(r)}$ denotes the function g composed with itself r times.) We note that in [32] Niederreiter and Winterhof proved several existence results for cyclotomic orthomorphisms and cyclotomic R-orthomorphisms of finite fields. Here we only concentrate on the permutation behavior of $g(x)$.

Theorem 2.1. *Let $g(x) = ax^r f(x^s) + b$ ($a \neq 0$) be a polynomial in reduced form (i.e., $\gcd(r, s) = 1$) over $\mathbb{F}_q$ with index ℓ. Then $|V_g| > q - \frac{q-1}{\ell}$ if and only if g is a PP of $\mathbb{F}_q$.*

Proof. Without loss of generality, we can assume $a = 1$ and $b = 0$. Hence $g(0) = 0$. The conditions $\gcd(r, s) = 1$ and $f(\zeta^i) \neq 0$ guarantee that all the images of elements in each C_i are distinct nonzero elements. Because $|C_i| = s = \frac{q-1}{\ell}$, we conclude that $|V_g| > q - \frac{q-1}{\ell}$ if and only if there are more than $\ell - 1$ nonzero distinct image sets of cyclotomic cosets. Since there are exactly ℓ nonzero distinct image sets of cyclotomic cosets, we deduce that $|V_g| > q - \frac{q-1}{\ell}$ if and only if g is a PP of $\mathbb{F}_q$. □

This result improves Wan's result (i.e., Equation (1)) for arbitrary polynomials with index $\ell \leq \sqrt{q} - 1$. Indeed, if the index $\ell \leq \sqrt{q} - 1$, then $s \geq \sqrt{q} + 1$ and thus the degree $d \geq s + 1 > \ell$. Our result also works at least as good as Wan's result [34] if we want to verify an arbitrary binomial over a prime field is a permutation using the contrapositive lower bound. Indeed, let $g(x) = x^d + ax^m$ with $d > m > 0$, be an arbitrary permutation binomial over a prime field $\mathbb{F}_p$. It is proved by Masuda and Zieve in [26] that $\gcd(d - m, p - 1) \geq \sqrt{p - 3/4} - 1/2$ ($> \sqrt{p} - 1$). Here $\gcd(d - m, p - 1)$ turns out to be equal to s. So the index $\ell = \frac{p-1}{s} \leq \sqrt{p - 3/4} + 1/2$ ($< \sqrt{p} + 1$) and thus $s > \sqrt{p} - 1$. Then $d = m + es \geq 1 + s \geq \sqrt{p - 3/4} + 1/2 \geq \ell$.

Hence $p - \frac{p-1}{d} \geq p - \frac{p-1}{\ell}$. However, we note that d is strictly greater than ℓ for any $m > 1$ or $e > 1$ as above.

Corollary 2.2. *Let $g(x) = ax^r f(x^{\frac{q-1}{\ell}}) + b$ $(a \neq 0)$ be any polynomial over $\mathbb{F}_q$ with index $\ell > 1$ and $s = \frac{q-1}{\ell}$. Assume $|V_g| < q$. Then*
(a) If $\gcd(r, s) = 1$ then $|V_g| \leq q - \frac{q-1}{\ell}$.
(b) If $\gcd(r, s) = t > 1$ then $|V_g| \leq \frac{q-1}{t} + 1$.
Therefore we always have $|V_g| \leq q - \frac{q-1}{\ell}$.

Proof. Without loss of generality, we can assume $a = 1$ and $b = 0$. Hence $g(0) = 0$. The case of $\gcd(r, s) = 1$ follows from Theorem 2.1. If $\gcd(r, s) = t > 1$, then $g(x) = g_1(x^t)$ for some polynomial $g_1 \in \mathbb{F}_q[x]$. Thus, $|V_g| \leq |V_{x^t}| = \frac{q-1}{t} + 1$. We note that $\frac{q-1}{t} + 1 = q - \frac{(t-1)(q-1)}{t} = q - (q - 1 - \frac{q-1}{t})$. Because $t > 1$ and $\ell > 1$, we must have $q - 1 - \frac{q-1}{t} \geq q - 1 - \frac{q-1}{2} = \frac{q-1}{2} \geq \frac{q-1}{\ell}$. Thus we have $|V_g| \leq q - \frac{q-1}{\ell}$ in both cases. □

In fact, we can obtain the following formula for the cardinality of the value set.

Proposition 2.3. *Let $g(x) = ax^r f(x^s) + b$ $(a \neq 0)$ be any polynomial over $\mathbb{F}_q$ with index $\ell = \frac{q-1}{s}$ and let $\gcd(r, s) = t$. Let ξ be a fixed primitive element of $\mathbb{F}_q$. Then*

$$|V_g| = c\frac{s}{t} + 1, \text{ or } |V_g| = c\frac{s}{t},$$

where $c = |\{(\xi^{ir} f(\xi^{si}))^{\ell t} \mid i = 0, \ldots, \ell - 1\}|$.

Proof. Without loss of generality, we can assume $a = 1$ and $b = 0$. Hence $g(0) = 0$. Let C_0 be the subgroup of $\mathbb{F}_q^*$ consisting of all the ℓ-th powers of $\mathbb{F}_q^*$ and D_0 be the subgroup of $\mathbb{F}_q^*$ consisting of all the ℓt-th powers. Let $C_i = \xi^i C_0$ for $i = 0, \ldots, \ell - 1$ be cyclotomic cosets of $\mathbb{F}_q^*$ induced by C_0. Note that $g(x) = c_i x^r$ when $x \in C_i$, where $c_i = f(\xi^{si})$ for $i = 0, \ldots, \ell - 1$. We also note that x^r maps C_0 onto D_0 which contains $\frac{s}{t}$ distinct elements. So x^r maps each coset $C_i = \xi^i C_0$ onto $\xi^{ir} D_0$. Therefore g maps C_i onto $\xi^{ir} f(\xi^{si}) D_0$, which could be either the set $\{0\}$ or one of the nonzero cyclotomic cosets of index ℓt. We observe that c is the number of distinct cyclotomic cosets of the form $\xi^{ir} f(\xi^{si}) D_0$. Hence we have $|V_g| = c\frac{s}{t} + 1$ or $c\frac{s}{t}$, the latter happens when some of c_i's in $g(x) = c_i x^r$ equal $g(0) = 0$. □

From here it is straightforward to obtain a generic lower bound $\frac{s}{(r,s)}$ for any nonzero polynomial. However, this lower bound can be improved depending on how much information we know about the coefficients of g in order to say more about $\xi^{ir} f(\xi^{si})$. We also refer to [17] for a matrix method which can be used to obtain a lower bound for the cardinality $|V_g|$ of the value set of a univariate polynomial g over $\mathbb{F}_q$.

3. Permutation polynomial vectors

Let us first consider a multivariate polynomial $g(x_1,\dots,x_n)$ over $\mathbb{F}_q$. As in the univariate case, we can write $g(x_1,\dots,x_n) = x_1^{r_1}\cdots x_n^{r_n} f(x_1^{s_1},\dots,x_n^{s_n}) + b$ where $g(0,\dots,0)=b$, and $r_1,\dots,r_n$ are vanishing orders of $x_1,\dots,x_n$ in $g(x_1,\dots,x_n)-b$ at 0 respectively (i.e., the lowest degree of x_i in $g(x_1,\dots,x_n)-b$ is r_i), and each s_i is the greatest common divisor of all the exponents of x_i from all monomial terms after factoring $x_i^{r_i}$, together with $q-1$ for $1\le i\le n$ (i.e., s_i is the greatest common divisor of all the exponents of x_i in $f(x_1^{s_1},\dots,x_n^{s_n})$ together with $q-1$). We note that $r_i\ge 0$ in this case instead of $r\ge 1$ for univariate polynomials. Let $\ell_i = \frac{q-1}{s_i}$ with $1\le i\le n$. Then $(\ell_1,\dots,\ell_n)$ is called the *index tuple* of the multivariate polynomial $g(x_1,\dots,x_n)$.

Example 3.1. *Let $g(x_1,x_2) = x_1^4x_2^5 - x_1^2x_2^5 + 3x_2^5$ over $\mathbb{F}_7$. So $(r_1,r_2)=(0,5)$ is the pair of vanishing orders of x_1 and x_2 at 0 respectively. We can write $g(x_1,x_2) = x_2^5(x_1^4+x_1^2+3) = x_1^0x_2^5 f(x_1^2,x_2^6)$ with $f(x_1,x_2)=x_1^2+x_1+3$ because $s_1=\gcd(4,2,0,6)=2$ and $s_2=\gcd(0,0,0,6)=6$. Namely, $(\ell_1,\ell_2)=(3,1)$ is the index tuple of g.*

Similarly, $h(x_1,x_2)=3x_1x_2^3-2x_1$ over $\mathbb{F}_7$ can be written as $h(x_1,x_2)=x_1(3x_2^3-2) = x_1^1x_2^0 f(x_1^6,x_2^3)$ where $f(x_1,x_2)=3x_2-2$. Namely, $r_1=1$, $r_2=0$, $s_1=6$, $s_2=3$, $\ell_1=1$, and $\ell_2=2$.

Finally, $t(x_1,x_2) = 3x_1^2x_2^3 - 2x_1^3x_2 + 5$ over $\mathbb{F}_7$ can be written as $t(x_1,x_2) = x_1^2x_2(3x_2^2-2x_1)+5 = x_1x_2f(x_1,x_2^2)+5$ where $f(x_1,x_2)=3x_2-2x_1$. Namely, $r_1=1$, $r_2=1$, $s_1=1$, $s_2=2$, $\ell_1=6$, and $\ell_2=3$.

Definition 3.2. *The multivariate polynomial*

$$g(x_1,\dots,x_n) = x_1^{r_1}\cdots x_n^{r_n} f(x_1^{(q-1)/\ell_1},\dots,x_n^{(q-1)/\ell_n}) + b$$

is said to be in index form if $r_1,\dots,r_n$ are vanishing orders of $x_1,\dots,x_n$ at 0 respectively, $g(0,\dots,0)=b$, and $(\ell_1,\dots,\ell_n)$ is the index tuple of g.

Without loss of generality, we assume $g(0,\dots,0)=0$ and $s_i=\frac{q-1}{\ell_i}$ for $1\le i\le n$. Hence

$$g(x_1,\cdots,x_n) = x_1^{r_1}\cdots x_n^{r_n} f(x_1^{s_1},\dots,x_n^{s_n}).$$

For each $1\le i\le n$, let $C_{i,0}$ be the multiplicative subgroup of $\mathbb{F}_q^*$ containing all the ℓ_i-th powers and let C_{i,j_i} be the j_i-th coset of $C_{i,0}$ in $\mathbb{F}_q^*$ where $1\le j_i\le \ell_i-1$. Let ξ be a fixed primitive element in $\mathbb{F}_q^*$ and $\zeta_i=\xi^{s_i}$ be a primitive ℓ_i-th root of unity where $1\le i\le n$. Hence $C_{i,j_i}=\xi^{j_i}C_{i,0}$. Moreover, if $x\in C_{i,j_i}$ then $x^{s_i}=\zeta_i^{j_i}$. If $r_i>0$, then $g(x_1,\dots,x_{i-1},0,x_{i+1},\dots,x_n)=0$. Otherwise, $g(x_1,\dots,x_{i-1},0,x_{i+1},\dots,x_n)$ may not be zero. Hence, for a given index tuple $(\ell_1,\dots,\ell_n)$, we can partition $\mathbb{F}_q\times\cdots\times\mathbb{F}_q$ as a union of $A_1\times\cdots\times A_n$ where A_i is either the set $\{0\}$ or one of the cosets C_{i,j_i} determined by the index ℓ_i. We define constants $a_1,\dots,a_n$ over these sets $A_1, \dots, A_n$ as follows:

$$a_i = \begin{cases} \zeta_i^{j_i} & \text{if } A_i = C_{i,j_i}, \\ 0 & \text{if } A_i = \{0\}. \end{cases}$$

Then $g(x_1, \dots, x_n) = x_1^{r_1} \cdots x_n^{r_n} f(x_1^{s_1}, \dots, x_n^{s_n})$ can be written as a *cyclotomic mapping* as follows:

$$g(x_1, \dots, x_n) = \begin{cases} 0 & \text{if } (x_1, \dots, x_n) = (0, \dots, 0), \\ f(a_1, \dots, a_n) x_1^{r_1} \cdots x_n^{r_n} & \text{if } (x_1, \dots, x_n) \in A_1 \times \cdots \times A_n. \end{cases} \tag{4}$$

Because $a_1, \dots, a_n$ are constants over $A_1 \times \cdots \times A_n$, we remark that any multivariate polynomial g behaves as a monomial $f(a_1, \dots, a_n) x_1^{r_1} \cdots x_n^{r_n}$ in the subset $A_1 \times \cdots \times A_n$, determined by the partition of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ according to the index tuple of g. We note that the similar concept for univariate polynomials can be found in [32, 37, 38].

Example 3.3. *Consider $g(x_1, x_2) = x_1^2 x_2 (4x_1^3 x_2^2 - 2x_2^4)$ over $\mathbb{F}_7$. We can write $g(x_1, x_2) = x_1^2 x_2 f(x_1^3, x_2^2)$ with the index tuple $(2, 3)$, where $f(x_1, x_2) = 4x_1 x_2 - 2x_2^2$. Let $\xi = 3$ be the fixed primitive element in $\mathbb{F}_7$. So $\zeta_1 = \xi^{6/2} = 6$ and $\zeta_2 = \xi^{6/3} = 2$. We can partition $\mathbb{F}_7^*$ into either $C_{1,0} = \{1, 2, 4\}$ and $C_{1,1} = \{3, 5, 6\}$ corresponding to $\ell_1 = 2$, or $C_{2,0} = \{1, 6\}$, $C_{2,1} = \{3, 4\}$, and $C_{2,2} = \{2, 5\}$ corresponding to $\ell_2 = 3$. Then $\mathbb{F}_7 \times \mathbb{F}_7$ can be partitioned into the union of all these $A_1 \times A_2$'s, where A_1 denotes any one of the sets $\{0\}$, $C_{1,0}$, and $C_{1,1}$, and A_2 denotes any one of the sets $\{0\}$, $C_{2,0}$, $C_{2,1}$ and $C_{2,2}$. Hence $g(x_1, x_2)$ can be represented by*

$$g(x_1, x_2) = \begin{cases} 0 & \textit{if } (x_1, x_2) = (0, 0), \\ 0 & \textit{if } (x_1, x_2) \in \{0\} \times C_{2,0}, \\ 0 & \textit{if } (x_1, x_2) \in \{0\} \times C_{2,1}, \\ 0 & \textit{if } (x_1, x_2) \in \{0\} \times C_{2,2}, \\ 0 & \textit{if } (x_1, x_2) \in C_{1,0} \times \{0\}, \\ 2x_1^2 x_2 & \textit{if } (x_1, x_2) \in C_{1,0} \times C_{2,0}, \\ 0 & \textit{if } (x_1, x_2) \in C_{1,0} \times C_{2,1}, \\ 5x_1^2 x_2 & \textit{if } (x_1, x_2) \in C_{1,0} \times C_{2,2}, \\ 0 & \textit{if } (x_1, x_2) \in C_{1,1} \times \{0\}, \\ x_1^2 x_2 & \textit{if } (x_1, x_2) \in C_{1,1} \times C_{2,0}, \\ 5x_1^2 x_2 & \textit{if } (x_1, x_2) \in C_{1,1} \times C_{2,1}, \\ x_1^2 x_2 & \textit{if } (x_1, x_2) \in C_{1,1} \times C_{2,2}, \end{cases} \tag{5}$$

where the coefficients of $x_1^2 x_2$ in all these branches are computed by using $f(a_1, a_2) = 4a_1 a_2 - 2a_2^2$ where $a_1 = 0, 1, -1$ and $a_2 = 0, 1, 2, 4$ respectively.

By an abuse of notation, let us now consider g as a polynomial vector map in n variables from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$:

$$g(x_1, \dots, x_n) = (g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)), \tag{6}$$

where each g_i $(1 \leq i \leq n)$ is a polynomial in n variables over $\mathbb{F}_q$. Using the previous definition of the index tuple and cyclotomic mappings, for each $1 \leq i \leq n$, we can write each g_i in the index form. Namely,

$$g_i(x_1,\ldots,x_n) = x_1^{r_1^{(i)}} \cdots x_n^{r_n^{(i)}} f_i(x_1^{s_1^{(i)}},\ldots,x_n^{s_n^{(i)}}) + b_i,$$

with the index tuple $(\ell_1^{(i)},\ldots,\ell_n^{(i)})$ and $b_i \in \mathbb{F}_q$. Without loss of generality, we assume further that $b_i = 0$ for all $1 \le i \le n$.

Hence

$$\begin{aligned} & g(x_1,\ldots,x_n) \\ = & \left(x_1^{r_1^{(1)}} \cdots x_n^{r_n^{(1)}} f_1(x_1^{s_1^{(1)}},\ldots,x_n^{s_n^{(1)}}),\ldots, x_1^{r_1^{(n)}} \cdots x_n^{r_n^{(n)}} f_n(x_1^{s_1^{(n)}},\ldots,x_n^{s_n^{(n)}})\right). \end{aligned}$$

For each $1 \le i \le n$, we let

$$s_i = \gcd(s_i^{(1)},\ldots,s_i^{(n)}) \text{ and } \ell_i = \frac{q-1}{s_i}.$$

Then we call $(\ell_1,\ldots,\ell_n)$ the *index tuple* of the polynomial vector map g in n variables.

Let $\zeta_i = \xi^{s_i}$ be a primitive ℓ_i-th root of unity and C_{i,j_i} be the j_i-th coset of $C_{i,0}$ in $\mathbb{F}_q^*$ where $1 \le j_i \le \ell_i$. We note again that $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ can be partitioned as a union of $A_1 \times \cdots \times A_n$ where A_i is either the set $\{0\}$ or one of the cosets C_{i,j_i} determined by the index tuple $(\ell_1,\ldots,\ell_n)$. Again, as defined before, we let

$$a_i = \begin{cases} \zeta_i^{j_i} & \text{if } A_i = C_{i,j_i}, \\ 0 & \text{if } A_i = \{0\}. \end{cases}$$

Hence, if $(x_1,\ldots,x_n) \in A_1 \times \cdots \times A_n$ then

$$\begin{aligned} & g(x_1,\ldots,x_n) \\ = & \left(x_1^{r_1^{(1)}} \cdots x_n^{r_n^{(1)}} f_1(a_1^{s_1^{(1)}/s_1},\ldots,a_n^{s_n^{(1)}/s_n}),\ldots, x_1^{r_1^{(n)}} \cdots x_n^{r_n^{(n)}} f_n(a_1^{s_1^{(n)}/s_1},\ldots,a_n^{s_n^{(n)}/s_n})\right). \end{aligned}$$

Let $c_i = f_i(a_1^{s_1^{(i)}/s_1},\ldots,a_n^{s_n^{(i)}/s_n})$. Then $g(x_1,\ldots,x_n)$ maps $(A_1,\ldots,A_n)$ to

$$\left(c_1 A_1^{r_1^{(1)}} \cdots A_n^{r_n^{(1)}},\ldots, c_n A_1^{r_1^{(n)}} \cdots A_n^{r_n^{(n)}}\right),$$

where we use the convention $0^0 = 1$ and $A^r = \{x^r \mid x \in A\}$.

Example 3.4. *Let $g(x_1,x_2) = (x_2(x_1^4 + 4x_1^2 + 4), x_1(3x_2^3 + 1))$ be a map from $\mathbb{F}_7 \times \mathbb{F}_7$ to itself. Using the previous definitions, we obtain $r_1^{(1)} = 0$, $r_2^{(1)} = 1$, $r_1^{(2)} = 1$, $r_2^{(2)} = 0$, $s_1^{(1)} = 2$, $s_2^{(1)} = 6$, $s_1^{(2)} = 6$, and $s_2^{(2)} = 3$. Moreover, $f_1(x_1^2, x_2^6) = x_1^4 + 4x_1^2 + 4$, $f_2(x_1^6, x_2^3) = 3x_2^3 + 1$. Hence $s_1 = \gcd(2,6) = 2$, $s_2 = \gcd(6,3) = 3$, $\ell_1 = 3$ and $\ell_2 = 2$. Therefore we use cyclotomic cosets of orders 3 and 2 respectively in the partition of $\mathbb{F}_7^*$. Namely, $C_{1,0} = \{1,6\}$, $C_{1,1} = \{3,4\}$ and $C_{1,2} = \{2,5\}$ are the cyclotomic cosets of order 3, $C_{2,0} = \{1,2,4\}$, and $C_{2,1} = \{3,5,6\}$ are cyclotomic cosets of order 2. Then $\mathbb{F}_7 \times \mathbb{F}_7$ is partitioned into $\{0\}\times\{0\}$, $\{0\}\times C_{2,0}$, $\{0\}\times C_{2,1}$, $C_{1,0}\times\{0\}$, $C_{1,1}\times\{0\}$, $C_{1,2}\times\{0\}$, $C_{1,0}\times C_{2,0}$, $C_{1,0} \times C_{2,1}$, $C_{1,1} \times C_{2,0}$, $C_{1,1} \times C_{2,1}$, $C_{1,2} \times C_{2,0}$, $C_{1,2} \times C_{2,1}$. Note that $a_1 \in \{0,1,2,4\}$ and $a_2 \in \{0,1,6\}$. We can check that $f_1(a_1, a_2^2) \neq 0$ and $f_2(a_1^3, a_2) \neq 0$. For example, $g(x_1,x_2) = (x_2(x_1^4 + 4x_1^2 + 4), x_1(3x_2^3 + 1))$ maps $C_{1,1} \times C_{2,1}$ into $C_{2,1} \times C_{1,0}$ because*

$g(x_1, x_2)$ behaves as the map $(2x_2, 5x_1)$ over $C_{1,1} \times C_{2,1}$. Indeed, $f_1(2, 6) = 2^2 + 8 + 4 = 2$ and $f_2(2, 6) = 18 + 1 = 5$.

Theorem 3.5. *Let g be a polynomial vector map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ defined by*

$$g(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n) + b_1, \ldots, g_n(x_1, \ldots, x_n) + b_n),$$

where $b_1, \ldots, b_n \in \mathbb{F}_q$ and g has index tuple $(\ell_1, \ldots, \ell_n)$ such that for each $1 \le i \le n$,

$$g_i(x_1, \cdots, x_n) = x_1^{r_1^{(i)}} \cdots x_n^{r_n^{(i)}} f_i(x_1^{s_1^{(i)}}, \ldots, x_n^{s_n^{(i)}})$$

is a polynomial in n variables over $\mathbb{F}_q$ in the index form with index tuple $(\ell_1^{(i)}, \ldots, \ell_n^{(i)})$ satisfying $g_i(0, \ldots, 0) = 0$ and $s_j^{(i)} = \frac{q-1}{\ell_j^{(i)}}$ for $1 \le j \le n$. Let $s_i = \gcd(s_i^{(1)}, \ldots, s_i^{(n)})$ and $\ell_i = \frac{q-1}{s_i}$ for $1 \le i \le n$. Then g is a permutation of $\mathbb{F}_q^n$ if and only if the following holds:

(1) For all $1 \le i \le n$, we must have $f_i(a_1^{s_1^{(i)}/s_1}, \ldots, a_n^{s_n^{(i)}/s_n}) \ne 0$ as long as not all a_i's are zero, where $a_i = 0$ or $a_i = \xi_i^{s_i j_i}$ with $0 \le j_i \le \ell_i - 1$ and ξ is a fixed primitive element of $\mathbb{F}_q$.

(2) The matrix $R := \begin{bmatrix} r_1^{(1)} & r_2^{(1)} & \cdots & r_n^{(1)} \\ r_1^{(2)} & r_2^{(2)} & \cdots & r_n^{(2)} \\ \vdots & \vdots & \cdots & \vdots \\ r_1^{(n)} & r_2^{(n)} & \cdots & r_n^{(n)} \end{bmatrix}$ *contains exactly one nonzero entry for each row and each column; Moreover, for each nonzero $r_i^{(k)}$ we must have* $\gcd(r_i^{(k)}, s_i^{(k)}) =$ 1.

(3) g induces a bijection between the set of all the parts $A_1 \times \cdots \times A_n$ of the partition of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ corresponding to the index tuple $(\ell_1, \ldots, \ell_n)$, and the set of all the parts $A'_{i_1} \times \cdots \times A'_{i_n}$ of the partition of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ corresponding to the index tuple $(\ell_{i_1}, \ldots, \ell_{i_n})$, where $(i_1, \ldots, i_n)^T = P(1, \ldots, n)^T$ and the permutation matrix P is associated with R defined by $p_{ij} = 1$ if $r_j^{(i)} \ne 0$.

Proof. Without loss of generality, we can assume that $b_1 = b_2 = \cdots = b_n = 0$. Assume that g is a permutation polynomial vector from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$. It is easy to see that condition (1) holds. Otherwise, at least two elements in $\mathbb{F}_q^n$ are mapped into the tuple consisting of all 0's.

We now prove condition (2). First, each row of R must contain at least one nonzero entry. Otherwise, suppose the i-th row is the zero row, all the tuples $(x_1, \ldots, x_n)$ satisfying that the i-th entry $x_i \in A_i$ must be mapped into tuples with the same i-th entry, contradicting that g is a permutation. Moreover, each row contains exactly one nonzero entry. Indeed, without loss of generality, suppose the first row contains two nonzero entries $r_1^{(1)}$ and $r_2^{(1)}$. Then tuples of the form $\{0\} \times A_2 \times \cdots \times A_n$ and $A_1 \times \{0\} \times \cdots \times A_n$ are both mapped into $\{0\} \times A_2 \times \cdots \times A_n$, which is a contradiction.

Similarly, each column of R should also contain exactly one nonzero entry. Indeed, if one column is a zero column, for example the first column, then $g(x_1, x_2, \ldots, x_n) = g(x'_1, x_2, \ldots, x_n)$ for any $x_1, x'_1 \in C_{1,j_1}$, contradicting that g is a permutation map of $\mathbb{F}_q^n$. If one column contains at least two nonzero entries, for example $r_1^{(1)}, r_1^{(2)}$, then tuples of the form $\{0\} \times A_2 \times \cdots \times A_n$ are mapped to tuples of the form $\{0\} \times \{0\} \times \cdots \times A_n$, contradicting that g is a permutation map. Moreover, if $r_i^{(k)} > 0$ then we consider two distinct tuples which differ only in the coordinate x_i but both values in coordinate x_i are in the same coset C_{i,j_i}. These tuples must be mapped to different images, this forces that $\gcd(r_i^{(k)}, s_i^{(k)}) = 1$.

Using condition (2), we write

$$g(x_1, \ldots, x_n) = \left(x_{i_1}^{r_{i_1}^{(1)}} f_1(x_1^{s_1^{(1)}}, \ldots, x_n^{s_n^{(1)}}), \ldots, x_{i_n}^{r_{i_n}^{(n)}} f_n(x_1^{s_1^{(n)}}, \ldots, x_n^{s_n^{(n)}}) \right)$$

so that $i_1, \ldots, i_n$ is a permutation of $1, \ldots, n$ induced by the permutation matrix P. Let $A_1 \times \cdots \times A_n$ be a part in the partition of $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ determined by the index tuple $(\ell_1, \ldots, \ell_n)$. Recall that $c_i = f_i(a_1^{s_1^{(i)}/s_1}, \ldots, a_n^{s_n^{(i)}/s_n})$. Then $g(x_1, \ldots, x_n)$ maps $(A_1, \ldots, A_n)$ to $\left(c_1 A_{i_1}^{r_{i_1}^{(1)}}, \ldots, c_n A_{i_n}^{r_{i_n}^{(n)}} \right)$. Because $\gcd(r_i^{(i)}, s_i^{(i)}) = 1$ for each i, the image becomes $(A'_{i_1}, \ldots, A'_{i_n})$, which gives one part $A'_{i_1} \times \cdots \times A'_{i_n}$ of the partition of $\mathbb{F}_q^n$ corresponding to the index tuple $(\ell_{i_1}, \ldots, \ell_{i_n})$. Hence condition (3) holds. The converse also holds using the same arguments as above. □

We now consider the following examples to illustrate Theorem 3.5.

Example 3.6. *Let* $g(x_1, x_2) = (x_2(x_1^4 + 4x_1^2 + 4), x_1(3x_2^3 + 1))$ *be a map from* $\mathbb{F}_7 \times \mathbb{F}_7$ *to itself as shown in Example 3.4. Obviously* $f_1(a_1, a_2^2) = a_1^2 + 4a_1 + 4 \neq 0$ *and* $f_2(a_1^3, a_2) = 3a_2 + 1 \neq 0$ *where* $a_1 \in \{0, 1, 2, 4\}$ *and* $a_2 \in \{0, 1, 6\}$*. Here,* $P = R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ *is a permutation matrix. Moreover,* $\gcd(r_2^{(1)}, s_2^{(1)}) = 1$ *and* $\gcd(r_1^{(2)}, s_1^{(2)}) = 1$*. Furthermore,* g *maps a part* $A_1 \times A_2$ *of the partition* $\mathbb{F}_7 \times \mathbb{F}_7$ *corresponding to the index tuple* $(3, 2)$ *into a part* $A'_2 \times A'_1$ *of the same size corresponding to the index tuple* $(2, 3)$*. Indeed,* g *maps*

$$\begin{array}{lcl}
\{0\} \times \{0\} & \longmapsto & \{0\} \times \{0\} \\
\{0\} \times C_{2,0} & \overset{(4x_2,0)}{\longmapsto} & C_{2,0} \times \{0\} \\
\{0\} \times C_{2,1} & \overset{(4x_2,0)}{\longmapsto} & C_{2,1} \times \{0\} \\
C_{1,0} \times \{0\} & \overset{(0,x_1)}{\longmapsto} & \{0\} \times C_{1,0} \\
C_{1,1} \times \{0\} & \overset{(0,x_1)}{\longmapsto} & \{0\} \times C_{1,1} \\
C_{1,2} \times \{0\} & \overset{(0,x_1)}{\longmapsto} & \{0\} \times C_{1,2} \\
C_{1,0} \times C_{2,0} & \overset{(2x_2,4x_1)}{\longmapsto} & C_{2,0} \times C_{1,1} \\
C_{1,0} \times C_{2,1} & \overset{(2x_2,5x_1)}{\longmapsto} & C_{2,1} \times C_{1,2} \\
C_{1,1} \times C_{2,0} & \overset{(2x_2,4x_1)}{\longmapsto} & C_{2,0} \times C_{1,2} \\
C_{1,1} \times C_{2,1} & \overset{(2x_2,5x_1)}{\longmapsto} & C_{2,1} \times C_{1,0} \\
C_{1,2} \times C_{2,0} & \overset{(x_2,4x_1)}{\longmapsto} & C_{2,0} \times C_{1,0} \\
C_{1,2} \times C_{2,1} & \overset{(x_2,5x_1)}{\longmapsto} & C_{2,1} \times C_{1,1}
\end{array}$$

By Theorem 3.5, g *is a permutation of* $\mathbb{F}_7^2$*.*

Example 3.7. *Let* $g(x_1, x_2) = (x_2, x_1(2 + x_2^3(x_1^4 - 2x_2^3)))$ *be a map from* $\mathbb{F}_7 \times \mathbb{F}_7$ *to itself. So* $s_1^{(1)} = 6$*,* $s_2^{(1)} = 6$*,* $s_1^{(2)} = 2$*, and* $s_2^{(2)} = 3$*. Hence* $s_1 = \gcd(6, 2) = 2$ *and* $s_2 = \gcd(6, 3) = 3$*.*

Thus $\ell_1 = 3$ and $\ell_2 = 2$. So $C_{1,0} = \{1, 6\}$, $C_{1,1} = \{3, 4\}$, and $C_{1,2} = \{2, 5\}$ are the cyclotomic cosets of order 3, $C_{2,0} = \{1, 2, 4\}$, and $C_{2,1} = \{3, 5, 6\}$ are cyclotomic cosets of order 2. Then $\mathbb{F}_7 \times \mathbb{F}_7$ is partitioned into $\{0\} \times \{0\}$, $\{0\} \times C_{2,0}$, $\{0\} \times C_{2,1}$, $C_{1,0} \times \{0\}$, $C_{1,1} \times \{0\}$, $C_{1,2} \times \{0\}$, $C_{1,0} \times C_{2,0}$, $C_{1,0} \times C_{2,1}$, $C_{1,1} \times C_{2,0}$, $C_{1,1} \times C_{2,1}$, $C_{1,2} \times C_{2,0}$, $C_{1,2} \times C_{2,1}$. Moreover, $f_1(x_1^6, x_2^6) = 1$ and $f_2(x_1^2, x_2^3) = 2 + x_2^3(x_1^4 - 2x_2^3)$. Note that $a_1 \in \{0, 1, 2, 4\}$ and $a_2 \in \{0, 1, 2\}$. We can easily check that $f_1(a_1^3, a_2^2) \neq 0$ and $f_2(a_1, a_2) \neq 0$ as long as one of a_1 and a_2 is nonzero. Furthermore, $R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. In fact, g maps

$$\begin{array}{ccc}
\{0\} \times \{0\} & \longmapsto & \{0\} \times \{0\} \\
\{0\} \times C_{2,0} & \overset{(x_2,0)}{\longmapsto} & C_{2,0} \times \{0\} \\
\{0\} \times C_{2,1} & \overset{(x_2,0)}{\longmapsto} & C_{2,1} \times \{0\} \\
C_{1,0} \times \{0\} & \overset{(0,2x_1)}{\longmapsto} & \{0\} \times C_{1,2} \\
C_{1,1} \times \{0\} & \overset{(0,2x_1)}{\longmapsto} & \{0\} \times C_{1,0} \\
C_{1,2} \times \{0\} & \overset{(0,2x_1)}{\longmapsto} & \{0\} \times C_{1,1}
\end{array}$$

$$\begin{array}{ccc}
C_{1,0} \times C_{2,0} & \overset{(x_2,x_1)}{\longmapsto} & C_{2,0} \times C_{1,0} \\
C_{1,0} \times C_{2,1} & \overset{(x_2,6x_1)}{\longmapsto} & C_{2,1} \times C_{1,0} \\
C_{1,1} \times C_{2,0} & \overset{(x_2,4x_1)}{\longmapsto} & C_{2,0} \times C_{1,2} \\
C_{1,1} \times C_{2,1} & \overset{(x_2,3x_1)}{\longmapsto} & C_{2,1} \times C_{1,2} \\
C_{1,2} \times C_{2,0} & \overset{(x_2,2x_1)}{\longmapsto} & C_{2,0} \times C_{1,1} \\
C_{1,2} \times C_{2,1} & \overset{(x_2,5x_1)}{\longmapsto} & C_{2,1} \times C_{1,1}
\end{array}$$

By Theorem 3.5, g is a permutation of $\mathbb{F}_7^2$.

We remark that from the proof of Theorem 3.5, each coordinate polynomial of the permutation vector map is a multivariate cyclotomic mapping, which in turn behaves as a monomial (in one variable) on every individual coset. In other words, each permutation vector map in n variables consists of n univariate cyclotomic permutations together with another permutation on coordinate variables. This fact may help us to construct permutation maps in n variables from these simpler coordinate polynomials.

Also from the proof of Theorem 3.5, it is easy to see that if one element in a part of the partition of $\mathbb{F}_q^n$ belongs to the value set then the whole part of the partition belongs to the value set. Hence we also obtain

Corollary 3.8. *Let g be a polynomial vector map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ with the index tuple $(\ell_1, \ldots, \ell_n)$ and $\ell = \max\{\ell_1, \ldots, \ell_n\} > 1$. If $|V_g| < q^n$ then $|V_g| \leq q^n - \frac{q-1}{\ell}$.*

Proof. Under the assumptions (1) and (2) in Theorem 3.5, the cardinality of the value set of g satisfies $|V_g| > q^n - \frac{q-1}{\ell}$ if and only if g induces a permutation of $\mathbb{F}_q^n$.

Also from the proof of Theorem 3.5, if assumption (1) fails, then at least two cosets corresponding to one coordinate, say i, are collapsed into the same image set, therefore $|V_g| \leq q^n - \frac{q-1}{\ell_i} \leq q^n - \frac{q-1}{\ell}$. When assumption (2) fails, the matrix R contains a zero row or a zero column, or at least two entries in one row or column. Hence the same discussion shows that at least two cosets are collapsed into one image set. This implies again that $|V_g| \leq q^n - \frac{q-1}{\ell_j}$ for some j and thus $|V_g| \leq q^n - \frac{q-1}{\ell}$. Finally, if the matrix R

contains exactly one entry in each row and column, but $(r_i^{(k)}, s_i^{(k)}) = t_i > 1$ for some i, we miss at least $\frac{(t_i-1)(q-1)}{t_i} = (q-1) - \frac{q-1}{t_i} \geq \frac{q-1}{2} \geq \frac{q-1}{\ell}$ values in the value set. Hence $|V_g| \leq q^n - \frac{q-1}{\ell}$. □

As the next simple example shows, the upper bound for non permutations can be achieved.

Example 3.9. *Let $g(x_1, x_2) = (x_1, x_2(-x_2^3(x_1^3+2)^2+4)^2)$ be a map from $\mathbb{F}_7 \times \mathbb{F}_7$ to itself. So $s_1^{(1)} = 6$, $s_2^{(1)} = 6$, $s_1^{(2)} = 3$, and $s_2^{(2)} = 3$. Hence $s_1 = \gcd(6,3) = 3$ and $s_2 = \gcd(6,3) = 3$. Thus $\ell_1 = 2$ and $\ell_2 = 2$. Here we use cyclotomic cosets of order 2: $C_{1,0} = C_{2,0} = \{1,2,4\}$, and $C_{1,1} = C_{2,1} = \{3,5,6\}$ to partition $\mathbb{F}_7 \times \mathbb{F}_7$ into $\{0\}\times\{0\}$, $\{0\}\times C_{2,0}$, $\{0\}\times C_{2,1}$, $C_{1,0}\times\{0\}$, $C_{1,1}\times\{0\}$, $C_{1,0}\times C_{2,0}$, $C_{1,0}\times C_{2,1}$, $C_{1,1}\times C_{2,0}$, $C_{1,1}\times C_{2,1}$. Moreover, $f_1(x_1^6, x_2^6) = 1$ and $f_2(x_1^3, x_2^3) = (-x_2^3(x_1^3+2)^2+4)^2$. Note that $f_2(a_1,a_2) = (-a_2(a_1+2)^2+4)^2 \in \{0,2,4\}$ where $a_1 \in \{0,1,6\}$ and $a_2 \in \{0,1,6\}$. In fact, g maps*

$$\begin{array}{lcl}
\{0\}\times\{0\} & \longmapsto & \{0\}\times\{0\} \\
\{0\}\times C_{2,0} & \xmapsto{(0,0)} & \{0\}\times\{0\} \\
\{0\}\times C_{2,1} & \xmapsto{(0,x_2)} & \{0\}\times C_{2,1} \\
C_{1,0}\times\{0\} & \xmapsto{(x_1,2x_2)} & C_{1,0}\times\{0\} \\
C_{1,1}\times\{0\} & \xmapsto{(x_1,2x_2)} & C_{1,1}\times\{0\} \\
C_{1,0}\times C_{2,0} & \xmapsto{(x_1,4x_2)} & C_{1,0}\times C_{2,0} \\
C_{1,0}\times C_{2,1} & \xmapsto{(x_1,x_2)} & C_{1,0}\times C_{2,1} \\
C_{1,1}\times C_{2,0} & \xmapsto{(x_1,2x_2)} & C_{1,1}\times C_{2,0} \\
C_{1,1}\times C_{2,1} & \xmapsto{(x_1,4x_2)} & C_{1,1}\times C_{2,1}
\end{array}$$

Here g maps the $\{0\}\times C_{2,1}$ into $\{0\}\times\{0\}$, and all other parts of the partition corresponding to the index tuple $(2,2)$ to distinct parts of the partition corresponding to the index tuple $(2,2)$. Therefore $|V_g| = 46 = q^2 - \frac{q-1}{2}$.

Acknowledgements

We thank the referee and Arne Winterhof for their helpful suggestions.

References

[1] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory* 4 (2008), no. 1, 121-133.

[2] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* 15 (2009), 195-206.

[3] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2011), no. 1, 51-67.

[4] A. Akbary and Q. Wang, On some permutation polynomials, *Int. J. Math. Math. Sci.* 16 (2005), 2631–2640.

[5] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.* 134 (2006), no 1, 15-22.

[6] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.*, Volume 2007 (2007), Article ID 23408, 7 pages.

[7] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith. 5 (1959), 417-423.

[8] H. Borges and R. Conceicao, On the characterization of minimal value set polynomials, *J. Number Theory* 133 (2013), 2021-2035.

[9] X. Cao and L. Hu, New methods for generating permutation polynomials over finite fields, *Finite Fields Appl.* 17 (2011), 493-503.

[10] X. Cao, L. Hu, and Z. Zha, Constructing permutation polynomials from piecewise permutations, *Finite Fields Appl.* 26 (2014), 162-174.

[11] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961), 121-130.

[12] P. Charpin and G. Kyureghyan, When does $F(x) + Tr(H(x))$ permute $\mathbb{F}_{p^n}$?, *Finite Fields Appl.* 15 (2009), no. 5, 615-632.

[13] Q. Cheng, J. Hill and D. Wan, Counting value sets: algorithms and complexity, Tenth Algorithmic Number Theory Symposium ANTS-X, 2012, University of California at San Deigo.

[14] A. B. Evans, Orthomorphism Graphs of Groups, Lecture Notes in Mathematics, Vol. 1535, Springer, Berlin, 1992.

[15] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* 13 (2007), 58-70.

[16] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970), 255-271.

[17] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, in *Finite Fields with Applications in Coding Theory, Cryptography and Related Areas*, G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, Eds., Springer, 2002, 80-85.

[18] N. Fernando and X. Hou, A piecewise construction of permutation polynomial over finite fields, *Finite Fields Appl.* 18 (2012), 1184-1194.

[19] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988), no. 2, 167-188.

[20] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101 (1997), 255-287.

[21] X. Hou, Two classes of permutation polynomials over finite fields, *J. Combin. Theory Ser. A* 118 (2011), no. 2, 448-454.

[22] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* 95 (1988), 243-246.

[23] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* 100 (1993), 71-74.

[24] R. Lidl and H. Niederreiter, Finite Fields, Sec. Ed., Cambridge University Press, Cambridge, 1997.

[25] R. Lipton, Claiming Picard's math may have gaps, http://rjlipton.wordpress.com/2011/09/26/claiming-picards-math-may-have-gaps/.

[26] A. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* 361 (2009), no. 8, 4169-4180.

[27] W. H. Mills, Polynomials with minimal value sets, *Pacific J. Math* 14 (1964), 225-241.

[28] G. L. Mullen, Permutation polynomials over finite fields, Lecture Notes in Pure and Appl. Math., Vol. 141, Marcel Dekker, New York, 1992, 131-151.

[29] G. L. Mullen and D. Panario, Handbook of Finite Fields, CRC Press, Boca Raton, FL, 2013.

[30] G. L. Mullen, D. Wan, and Q. Wang, Value sets of polynomial maps over finite fields, *Quart. J. Math.* 64 (2013), no. 4, 1191-1196.

[31] G. L. Mullen and Q. Wang, Permutation polynomials of one variable, Section 8.1 in Handbook of Finite Fields, CRC Press, Boca Raton, FL, 2013.

[32] H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, *Discrete Math.* 295 (2005), 161-171.

[33] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1 (1995), 64-82.

[34] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, Lecture Notes in Pure and Appl. Math., Marcel Dekker, New York, Vol. 141, 1992, 209-216.

[35] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991), 149–163.

[36] D. Wan, P. J. S. Shiue and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* 119 (1993), 711-717.

[37] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Sequences, Subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), 119-128, Lecture Notes in Comput. Sci. Vol. 4893, Springer, Berlin, 2007.

[38] Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* 22 (2013), 57-69.

[39] K. S. Williams, On general polynomials, *Canad. Math. Bull.* 10 (1967), no. 4, 579-583.

[40] P. Yuan and C. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.* 17 (2011), no. 6, 560 - 574.

[41] P. Yuan and C. Ding, Further results on permutation polynomials over finite fields, *Finite Fields Appl.*, to appear.

[42] Z. Zha and L. Hu, Two classes of permutation polynomials over finite fields, *Finite Fields Appl.* 18 (2012), no. 4, 781-790.

[43] M. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory* 4 (2008), 851–857.

[44] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* 137 (2009), no. 7, 2209-2216.

[45] M. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, Additive Number Theory, 355-361, Springer, New York, 2010.

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802
E-mail address: mullen@math.psu.edu

Department of Mathematics, University of California, Irvine, CA 92697-3875
E-mail address: dwan@math.uci.edu

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada
E-mail address: wang@math.carleton.ca