Additive decomposition schemes for polynomial functions over fields

Miguel Couceiro, Erkko Lehtonen, Tamas Waldhauser

This paper appeared in Novi Sad J. Math. **44** (2014), 89–105.

ADDITIVE DECOMPOSITION SCHEMES FOR POLYNOMIAL FUNCTIONS OVER FIELDS

MIGUEL COUCEIRO, ERKKO LEHTONEN, AND TAMÁS WALDHAUSER

Abstract. The authors' previous results on the arity gap of functions of several variables are refined by considering polynomial functions over arbitrary fields. We explicitly describe the polynomial functions with arity gap at least 3, as well as the polynomial functions with arity gap equal to 2 for fields of characteristic 0 or 2. These descriptions are given in the form of decomposition schemes of polynomial functions. Similar descriptions are given for arbitrary finite fields. However, we show that these descriptions do not extend to infinite fields of odd characteristic.

1. Introduction

The arity gap of a function $f\colon A^n \to B$ is a quantity that indicates the minimum number of variables that become inessential when a pair of essential variables is identified in f. This notion was first studied by Salomaa [8], who showed that the arity gap of any Boolean function is at most 2. Willard [10] showed that the same upper bound holds for any function $f\colon A^n \to B$ with a finite domain, provided that f depends on at least $\max(|A|, 3) + 1$ variables. A complete classification of functions in regard to the arity gap was presented in [3] and [5]; see Theorem 2.6.

A decomposition scheme of functions based on the arity gap was proposed by Shtrakov and Koppitz [9], and it was later refined in [5] as follows (here $\operatorname{ess} f$ denotes the number of essential variables of f, and $\operatorname{gap} f$ denotes the arity gap of f).

Theorem 1.1. *Assume that $(B; +)$ is a group with neutral element 0. Let $f\colon A^n \to B$, $n \geq 3$, and $3 \leq p \leq n$. Then the following two conditions are equivalent:*

(i) $\operatorname{ess} f = n$ *and* $\operatorname{gap} f = p$.

(ii) *There exist functions $g, h\colon A^n \to B$ such that $f = g + h$, $h|_{A^n_{\neq}} \equiv 0$, $h \not\equiv 0$, and* $\operatorname{ess} g = n - p$.

The decomposition $f = g + h$ given above is unique.

Theorem 1.1 does not extend as such into the case when $p = 2$. Namely, there exist functions $f\colon A^n \to B$ with $\operatorname{gap} f = 2$ that do not admit a decomposition of the form given in item (ii). These exceptional functions are determined by oddsupp (see Section 2). However, as shown in [5], if f is determined by oddsupp, then it can be decomposed as $f = g + h$ with $h|_{A^n_{\neq}} \equiv 0$, $h \not\equiv 0$, and g is a sum of functions of essential arity at most $n - 2$.

With these results as our starting point, we study in this paper polynomial functions over arbitrary fields. Our goal is to obtain further, more explicit and simpler decomposition schemes, especially for the case when $\operatorname{gap} f = 2$ and f is determined by oddsupp.

The paper is organised as follows. In Section 2, we recall the basic notions and introduce preliminary results which will be needed throughout the paper. In Section 3, we provide a general decomposition scheme for polynomial functions over arbitrary fields with arity gap at least 3. In subsequent sections we focus on functions with arity gap 2. More precisely, in Section 4, we describe the polynomial functions determined by oddsupp, and we obtain decomposition schemes for functions with arity gap 2 over finite fields and fields of characteristic 2. In Section 5, we consider the case of fields of characteristic 0. In this case, we show that if f is a polynomial function such that $f|_{A^n_{\neq}}$ is determined by oddsupp, then $f|_{A^n_{\neq}}$ is constant. Hence, simpler decomposition schemes are available for polynomial functions with arity gap 2. The question whether similar decomposition schemes exist over

2010 *Mathematics Subject Classification.* 08A40, 12E05.

Key words and phrases. function of several variables, arity gap, polynomial function, partial derivative.

infinite fields of odd characteristic is addressed in Section 6. We answer negatively to this question by means of an illustrative example.

2. Preliminaries

Let A and B be arbitrary sets with at least two elements. A *partial function of several variables* from A to B is a mapping $f\colon S \to B$, where $S \subseteq A^n$ for some integer $n \geq 1$, called the *arity* of f. If $S = A^n$, then we speak of (*total*) *functions of several variables.* Functions of several variables from A to A are referred to as *operations* on A.

For an integer $n \geq 1$, let $[n] := \{1, \dots, n\}$. Let $f\colon S \to B$ ($S \subseteq A^n$) be an n-ary partial function and let $i \in [n]$. We say that the i-th variable is *essential* in f (or f *depends* on x_i), if there exist tuples

$$(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n), (a_1, \dots, a_{i-1}, a_i', a_{i+1}, \dots, a_n) \in S$$

such that

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, a_i', a_{i+1}, \dots, a_n).$$

Variables that are not essential are called *inessential.* Let $\operatorname{Ess} f := \{i \in [n] : x_i \text{ is essential in } f\}$. The cardinality of $\operatorname{Ess} f$ is called the *essential arity* of f and denoted by $\operatorname{ess} f$.

Let $f\colon A^n \to B$, $g\colon A^m \to B$. We say that g is a *minor* of f, if there is a map $\sigma\colon [n] \to [m]$ such that $g(x_1, \dots, x_m) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. We say that f and g are *equivalent* if each one is a minor of the other.

For $i, j \in [n]$, $i \neq j$, define the *identification minor* of $f\colon A^n \to B$ obtained by identifying the i-th and the j-th variable, as the minor $f_{i \leftarrow j}\colon A^n \to B$ of f corresponding to the map $\sigma\colon [n] \to [n]$, $i \mapsto j$, $\ell \mapsto \ell$ for $\ell \neq i$, i.e., $f_{i \leftarrow j}$ is given by the rule

$$f_{i \leftarrow j}(x_1, \dots, x_n) := f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_n).$$

Remark 2.1. Note that for all $f\colon A^n \to B$ and for all $i, j \in [n]$ with $i \neq j$, it holds that $f_{i \leftarrow j}$ is equivalent to $f_{j \leftarrow i}$.

Remark 2.2. Loosely speaking, a function g is a minor of f, if g can be obtained from f by permutation of variables, addition of inessential variables and identification of variables. Similarly, two functions are equivalent, if each one can be obtained from the other by permutation of variables and addition or deletion of inessential variables.

The *arity gap* of f is defined as

$$\operatorname{gap} f := \min_{\substack{i,j \in \operatorname{Ess} f \\ i \neq j}} (\operatorname{ess} f - \operatorname{ess} f_{i \leftarrow j}).$$

Remark 2.3. Note that the definition of arity gap refers only to essential variables. Hence, in order to determine the arity gap of a function f, we may consider, instead of f, an equivalent function f' that is obtained from f by removing its inessential variables. It is easy to see that in this case $\operatorname{gap} f = \operatorname{gap} f'$. Therefore, whenever we consider the arity gap of a function f, we may assume without loss of generality that f depends on all of its variables.

The notion of arity gap has been studied by several authors [2, 3, 4, 5, 6, 7, 8, 9, 10]. In [3], a general classification of functions according to their arity gap was established. In order to state this result, we need to recall a few notions.

For $n \geq 2$, define

$$A^n_{=} := \{(a_1, \dots, a_n) \in A^n : a_i = a_j \text{ for some } i \neq j\}.$$

Furthermore, define $A^1_{=} := A$. Let $f\colon A^n \to B$. Any function $g\colon A^n \to B$ satisfying $f|_{A^n_{=}} = g|_{A^n_{=}}$ is called a *support* of f. The *quasi-arity* of f, denoted $\operatorname{qa} f$, is defined as the minimum of the essential arities of all supports of f, i.e., $\operatorname{qa} f := \min_g \operatorname{ess} g$ where g ranges over the set of all supports of f. If $\operatorname{qa} f = m$, then we say that f is *quasi-m-ary.* Note that if A is finite and $n > |A|$, then $A^n_{=} = A^n$; hence in this case $\operatorname{qa} f = \operatorname{ess} f$. Moreover, for an arbitrary A and $n \neq 2$, we have $\operatorname{qa} f = \operatorname{ess} f|_{A^n_{=}}$ (see Lemma 4 in [3]). The case $n = 2$ is excluded, because if $f\colon A^2 \to B$ is a function such that $f(a, a) \neq f(b, b)$ for some $a, b \in A$, then $\operatorname{qa} f = 1$ yet $\operatorname{ess} f|_{A^n_{=}} = 0$.

Example 2.4. Consider the polynomial function $f\colon \mathbb{R}^3 \to \mathbb{R}$ induced by the polynomial

$$x_1^2x_2^2x_3 - x_1^2x_2x_3^2 - x_1x_2^3x_3 + x_1x_2x_3^3 + x_1^3x_2^2 - x_2^2x_3^3 + x_2^3x_3^2.$$

Writing the above polynomial as

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)x_2x_3 + x_1^3x_2^2,$$

we see easily that

$$\begin{aligned} f_{1\leftarrow 2}(x_1, x_2, x_3) &= x_2^5, & f_{2\leftarrow 1}(x_1, x_2, x_3) &= x_1^5,\\ f_{1\leftarrow 3}(x_1, x_2, x_3) &= x_2^2x_3^3, & f_{3\leftarrow 1}(x_1, x_2, x_3) &= x_1^3x_2^2,\\ f_{2\leftarrow 3}(x_1, x_2, x_3) &= x_1^3x_3^2, & f_{3\leftarrow 2}(x_1, x_2, x_3) &= x_1^3x_2^2. \end{aligned}$$

Note that $f_{i\leftarrow j}$ is equivalent to $f_{j\leftarrow i}$ for all $i, j \in \{1, 2, 3\}$ with $i \neq j$, as pointed out in Remark 2.1. The function f clearly depends on all of its variables, and the essential arities of its identification minors are

$$\begin{aligned} &\operatorname{ess} f_{1\leftarrow 2} = \operatorname{ess} f_{2\leftarrow 1} = 1,\\ &\operatorname{ess} f_{1\leftarrow 3} = \operatorname{ess} f_{3\leftarrow 1} = \operatorname{ess} f_{2\leftarrow 3} = \operatorname{ess} f_{3\leftarrow 2} = 2. \end{aligned}$$

We conclude that $\operatorname{gap} f = 1$.

Let $g\colon \mathbb{R}^3 \to \mathbb{R}$ be the function induced by the polynomial $x_1^3x_2^2$. It is clear that g is a support of f of the smallest possible essential arity. Thus $\operatorname{qa} f = \operatorname{ess} g = 2$.

Denote by $\mathcal{P}(A)$ the power set of A. Following Berman and Kisielewicz [1], we define the function oddsupp$\colon \bigcup_{n\geq 1} A^n \to \mathcal{P}(A)$ by

$$\operatorname{oddsupp}(a_1, \dots, a_n) := \{a \in A : |\{j \in [n] : a_j = a\}| \text{ is odd}\}.$$

We say that a partial function $f\colon S \to B$ ($S \subseteq A^n$) is *determined by* oddsupp if there exists a function $f^*\colon \mathcal{P}(A) \to B$ such that

$$f = f^* \circ \operatorname{oddsupp}|_S. \tag{1}$$

Observe that only the restriction of f^* to the set

$$\mathcal{P}'_n(A) := \big\{T \in \mathcal{P}(A) : |T| \in \{n, n-2, n-4, \dots\}\big\},$$

is relevant in determining the values of f in (1). Moreover, the functions $f\colon A^n \to B$ determined by oddsupp are in one-to-one correspondence with the functions $f^*\colon \mathcal{P}'_n(A) \to B$.

Willard showed in [10] that if $f\colon A^n \to B$, where A is finite, $\operatorname{ess} f = n > \max(|A|, 3)$ and $\operatorname{gap} f \geq 2$, then f is determined by oddsupp. The following fact is easy to verify.

Fact 2.5. *A function $f\colon A^n \to B$ is determined by* oddsupp *if and only if f is totally symmetric and $f_{2\leftarrow 1}$ does not depend on x_1. Similarly, $f|_{A^n_{\neq}}$ is determined by* oddsupp *if and only if $f|_{A^n_{\neq}}$ is totally symmetric and $f_{2\leftarrow 1}$ does not depend on x_1.*

We can now state the general classification of functions according to the arity gap. This result was first obtained in [3] for functions with finite domains, and in [5] it was shown to still hold for functions with arbitrary, possibly infinite domains.

Theorem 2.6. *Let A and B be arbitrary sets with at least two elements. Suppose that $f\colon A^n \to B$, $n \geq 2$, depends on all of its variables.*

(i) *For $3 \leq p \leq n$, $\operatorname{gap} f = p$ if and only if $\operatorname{qa} f = n - p$.*

(ii) *For $n \neq 3$, $\operatorname{gap} f = 2$ if and only if*
- $\operatorname{qa} f = n - 2$ *or*
- $\operatorname{qa} f = n$ *and $f|_{A^n_{\neq}}$ is determined by* oddsupp.

(iii) *For $n = 3$, $\operatorname{gap} f = 2$ if and only if there is a nonconstant unary function $h\colon A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that*

$$\begin{aligned} f(x_1, x_0, x_0) &= h(x_{i_1}),\\ f(x_0, x_1, x_0) &= h(x_{i_2}),\\ f(x_0, x_0, x_1) &= h(x_{i_3}). \end{aligned}$$

(iv) *Otherwise* $\operatorname{gap} f = 1$.

Theorem 2.6 can be refined to obtain more explicit classifications by assuming certain structures on the domain A or the codomain B of f. Examples of such refinements include the complete classification of Boolean functions [2], pseudo-Boolean functions [3], lattice polynomial functions [4], or more generally, order-preserving functions [6]. Moreover, in [5], B was assumed to be a group, and the following decomposition scheme based on the quasi-arity was obtained.

Theorem 2.7. *Assume that $(B;+)$ is a group with neutral element 0. Let $f\colon A^n \to B$, $n \geq 3$, and $1 \leq p \leq n$. Then the following two conditions are equivalent:*

(i) $\operatorname{ess} f = n$ *and* $\operatorname{qa} f = n - p$.

(ii) *There exist functions $g, h\colon A^n \to B$ such that $f = g + h$, $h|_{A^n_{=}} \equiv 0$, $h \not\equiv 0$, and* $\operatorname{ess} g = n - p$.

The decomposition $f = g + h$ given above is unique.

In the case when $p \geq 3$, condition (i) of Theorem 2.7 can be transformed into condition (i) of Theorem 1.1 by a straightforward application of Theorem 2.6(i). Thus, Theorem 1.1 is a special case of Theorem 2.7.

Remark 2.8. Note that if $h\colon A^n \to B$ satisfies $h|_{A^n_{=}} \equiv 0$ and $h \not\equiv 0$, then h depends on all of its variables. For, since h is not the constant 0 function, there exists a tuple $\mathbf{a} \in A^n \setminus A^n_{=}$ such that $h(\mathbf{a}) \neq 0$. For each $i \in [n]$, we may change the i-th component of $\mathbf{a}$ to obtain a tuple $\mathbf{b}$ belonging to $A^n_{=}$, and we have $g(\mathbf{b}) = 0 \neq g(\mathbf{a})$, showing that g depends on the i-th variable. Therefore, $\operatorname{ess} h = n$ for the function h of Theorem 2.7.

3. Polynomial functions over fields

In what follows, we will assume that the reader is familiar with the basic notions of algebra, such as rings, unique factorization domains, fields, vector spaces, polynomials and polynomial functions. However, we find it useful to recall the following well-known result.

Fact 3.1. *Every function $f\colon F^n \to F$ on a finite field F is a polynomial function over F.*

Polynomials over infinite fields are in one-to-one correspondence with polynomial functions. Fact 3.1 establishes a correspondence between polynomials and functions over finite fields, which is not bijective. This correspondence can be made bijective by assuming that we only consider polynomials over a given finite field, say $F = \mathrm{GF}(q)$, in which the exponent of every variable in every monomial is at most $q - 1$; we shall call such polynomials over finite fields *canonical*. In the case of infinite fields, every polynomial is *canonical*.

Given a polynomial function $f\colon F^n \to F$, we denote by P_f the unique canonical polynomial which induces f. Given a polynomial $p \in F[x_1, \ldots, x_n]$, we denote by $\overline{p}$ the function $f\colon F^n \to F$ induced by p. Note that $\overline{p+q} = \overline{p} + \overline{q}$ for all $p, q \in F[x_1, \ldots, x_n]$.

Fact 3.2. *A variable x_i is essential in a polynomial function $f\colon F^n \to F$ if and only if x_i occurs in P_f.*

Let F be a field, and let us apply the results of Section 2 in the case $A = B = F$ for polynomial functions $f\colon F^n \to F$.

Lemma 3.3. *If f is a polynomial function over F, then the functions g and h in the decomposition $f = g + h$ given in Theorem 1.1 and Theorem 2.7 are also polynomial functions.*

Proof. Since $\operatorname{ess} g = n - p \leq n - 1$, the function g has an inessential variable, say the i-th variable is inessential in g. Let $j \neq i$. We clearly have $g_{i \leftarrow j} = g$, and since $h|_{A^n_{=}} \equiv 0$, we have

$$f_{i \leftarrow j} = g_{i \leftarrow j} + h_{i \leftarrow j} = g + 0 = g.$$

Thus, g is a minor of f and hence a polynomial function. Then $h = f - g$ is a polynomial function as well. □

Lemma 3.4. *If h is an n-ary polynomial function over F, then $h|_{F^n_{=}} \equiv 0$ if and only if h is induced by a multiple of the polynomial*

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in F[x_1, \ldots, x_n].$$

Proof. It is clear that if h is induced by a multiple of Δ_n, then $h|_{F^n_{=}} \equiv 0$. For the converse implication, we need to distinguish between the cases of finite and infinite F. Assume first that F is infinite, and let us suppose that $h|_{F^n_{=}} \equiv 0$. Let us consider P_h as an element of $R[x_n]$, where R denotes the ring $F[x_1, \dots, x_{n-1}]$. Since $h|_{F^n_{=}} \equiv 0$, each one of the elements $x_1, \dots, x_{n-1} \in R$ is a root of the unary polynomial $P_h(x_n) \in R[x_n]$. Therefore P_h is divisible by $x_i - x_n$ for all $i = 1, \dots, n-1$. Repeating this argument with x_j in place of x_n, we can see that $x_i - x_j$ divides P_h for all $1 \leq i < j \leq n$. Since these divisors of P_h are relatively prime (and $R[x_n] = F[x_1, \dots, x_n]$ is a unique factorization domain), we can conclude that P_h is divisible by their product Δ_n.

Assume then that F is finite. Define the function $h' \colon F^n \to F$ by the rule

$$h'(\mathbf{a}) = \begin{cases} h(\mathbf{a}) \cdot (\overline{\Delta_n}(\mathbf{a}))^{-1}, & \text{if } \mathbf{a} \in F^n \setminus F^n_{=}, \\ 0, & \text{if } \mathbf{a} \in F^n_{=}. \end{cases}$$

Observe that $\overline{\Delta_n}(\mathbf{a}) \neq 0$ for every $\mathbf{a} \in F^n \setminus F^n_{=}$; hence h' is well defined. (In fact, h' could be defined in an arbitrary way on $F^n_{=}$.) Clearly $h = h' \cdot \overline{\Delta_n}$. By Fact 3.1, h' is a polynomial function. Thus h is induced by the polynomial $P_{h'} \cdot \Delta_n$. □

Combining the previous two lemmas with Theorem 1.1 we obtain the following description of polynomial functions over F with arity gap at least 3.

Theorem 3.5. *Let F be a field and let $f \colon F^n \to F$ be a polynomial function of arity at least 3 that depends on all of its variables. Then $\operatorname{gap} f = p \geq 3$ if and only if there exist polynomials $P, Q \in F[x_1, \dots, x_n]$ such that $f = \overline{P} + \overline{Q}$, P is canonical, exactly $n-p$ variables occur in P, and Q is a nonzero multiple of the polynomial Δ_n such that $\overline{Q}$ is not identically 0. Moreover, if $f = \overline{P'} + \overline{Q'}$, where P' is canonical, $n-p$ variables occur in P' and Q' is a nonzero multiple of Δ_n such that $\overline{Q'}$ is not identically 0, then $P' = P$ and $\overline{Q'} = \overline{Q}$.*

4. Polynomial functions determined by oddsupp over fields of characteristic 2

We refine Fact 2.5 for polynomial functions over an arbitrary field F. For this purpose, we need some formalism. We use the following notation:

- If F is infinite, then N_F denotes the set $\mathbb{N}$ of nonnegative integers, M_F denotes the set of all nonnegative even integers, and $\oplus_F$ denotes the usual addition of nonnegative integers.
- If F has finite order q, then N_F denotes the set $\{0, 1, \dots, q-1\}$, $M_F := N_F$, and $\oplus_F$ is the operation on N_F given by the following rules:
  - $0 \oplus_F 0 = 0$.
  - If $a \neq 0$ or $b \neq 0$, then $a \oplus_F b = c$, where c is the unique number in $\{1, \dots, q-1\}$ such that $c \equiv a + b \pmod{q-1}$.

Define the map $\tau_F \colon N_F \to M_F$ by the rule $m \mapsto m \oplus_F m$.

Remark 4.1. If F is infinite or of even order, then τ_F is a bijection that has 0 as a fixed point.

Lemma 4.2. *Let F be an arbitrary field, and let $f \colon F^n \to F$ be a polynomial function with*

$$P_f = \sum_{\mathbf{k}=(k_1,\dots,k_n) \in N_F^n} c_{\mathbf{k}} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

Then $f_{2\leftarrow 1}$ does not depend on x_1 if and only if for all $(k, k_3, \dots, k_n) \in N_F^{n-1}$ with $k \neq 0$,

$$\sum_{\substack{(a_1,a_2) \in N_F^2 \\ a_1 \oplus_F a_2 = k}} c_{(a_1,a_2,k_3,\dots,k_n)} = 0.$$

Proof. The canonical polynomial for $f_{2\leftarrow 1}$ is

$$\sum_{(b_1,b_3,\dots,b_n) \in N_F^{n-1}} d_{(b_1,b_3,\dots,b_n)} x_1^{b_1} x_3^{b_3} \cdots x_n^{b_n},$$

where

$$d_{(b_1,b_3,\dots,b_n)} = \sum_{\substack{(a_1,a_2)\in N_F^2 \\ a_1\oplus a_2=b_1}} c_{(a_1,a_2,b_3,\dots,b_n)}.$$

By Fact 3.2, the condition that $f_{2\leftarrow 1}$ does not depend on x_1 is equivalent to the condition that $d_{(b_1,b_3,\dots,b_n)} = 0$ for all $(b_1, b_3, \dots, b_n) \in N_F^{n-1}$ such that $b_1 \neq 0$. □

Proposition 4.3. *Let F be an arbitrary field, and let $f\colon F^n \to F$ be a polynomial function with*

$$P_f = \sum_{\mathbf{k}=(k_1,\dots,k_n)\in N_F^n} c_{\mathbf{k}} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

Then f is determined by oddsupp *if and only if*

(A) *f is symmetric, i.e., $c_{(k_1,\dots,k_n)} = c_{(l_1,\dots,l_n)}$ whenever there is a permutation $\pi \in S_n$ such that $k_i = l_{\pi(i)}$ for all $i \in [n]$, and*

(B) *for all $(k, k_3, \dots, k_n) \in N_F^{n-1}$ with $k \neq 0$,*

$$\sum_{\substack{(a_1,a_2)\in N_F^2 \\ a_1\oplus_F a_2=k}} c_{(a_1,a_2,k_3,\dots,k_n)} = 0.$$

In particular, if the characteristic of F is 2, then f is determined by oddsupp *if and only if condition* (A) *above holds together with*

(B_2) *$c_{(k,k,k_3,\dots,k_n)} = 0$ for all $(k, k, k_3, \dots, k_n) \in N_F^n$ with $k \neq 0$.*

Proof. By Fact 2.5, f is determined by oddsupp if and only if f is totally symmetric (i.e., (A) holds) and $f_{2\leftarrow 1}$ does not depend on x_1 (i.e., (B) holds, by Lemma 4.2).

Assume then that the characteristic of F is 2. We need to prove that condition (B) is equivalent to (B_2) under the assumption that f is totally symmetric. Let us analyse more carefully the coefficient

$$\begin{aligned} d_{(b_1,b_3,\dots,b_n)} &= \sum_{\substack{(a_1,a_2)\in N_F^2 \\ a_1\oplus_F a_2=b_1}} c_{(a_1,a_2,b_3,\dots,b_n)} \\ &= \underbrace{\sum_{\substack{a_1\in N_F \\ a_1\oplus_F a_1=b_1}} c_{(a_1,a_1,b_3,\dots,b_n)}}_{\text{(I)}} + \\ &\qquad \underbrace{\sum_{\substack{(a_1,a_2)\in N_F^2 \\ a_1<a_2,\, a_1\oplus_F a_2=b_1}} \left(c_{(a_1,a_2,b_3,\dots,b_n)} + c_{(a_2,a_1,b_3,\dots,b_n)}\right)}_{\text{(II)}}. \end{aligned}$$

Assuming that f is totally symmetric, we have $c_{(a_1,a_2,b_3,\dots,b_n)} = c_{(a_2,a_1,b_3,\dots,b_n)}$. Hence summand (II) above equals $2{\cdot}C$ for some $C \in F$, which is equal to 0 since F has characteristic 2.

As for summand (I), observe first that if F is infinite and b_1 is odd, then there is no $a_1 \in N_F$ such that $a_1 \oplus_F a_1 = b_1$; hence the sum in (I) is empty and equals 0. Thus, in this case, we have $d_{(b_1,b_3,\dots,b_n)} = 0$. Otherwise, i.e., if F is finite or if F is infinite and b_1 is even, the sum in (I) has just one summand, namely the one indexed by $a_1 = \tau_F^{-1}(b_1)$ (τ_F is a bijection by Remark 4.1), and we have $d_{(b_1,b_3,\dots,b_n)} = c_{(\tau_F^{-1}(b_1),\tau_F^{-1}(b_1),b_3,\dots,b_n)}$.

By the above observations, we conclude that under the assumption that F has characteristic 2 and f is totally symmetric, condition (B) is equivalent to the condition that $c_{(k,k,k_3,\dots,k_n)} = 0$ for all $(k, k, k_3, \dots, k_n) \in N_F^n$ with $k \neq 0$. □

We reassemble in the following remark some facts that have been established in [5] (more specifically, in the second paragraph of Section 5 and in Theorem 5.2 of [5]).

Remark 4.4. Assume that B is a set with a Boolean group structure (i.e., an abelian group such that $x+x=0$ holds identically). Let $n \geq 3$, and assume that $f\colon A^n \to B$ is a function such that $f|_{A^n_{=}}$ is determined by oddsupp. Fix an element $a \in A$, and let $\varphi\colon A^{n-2} \to B$ be the function given by $\varphi(a_1,\dots,a_{n-2}) := f(a_1,\dots,a_{n-2},a,a)$ for all $a_1,\dots,a_{n-2} \in A$. (Since $f|_{A^n_{=}}$ is determined by oddsupp, the definition of φ is independent of the choice of a.) Then φ is determined by oddsupp, i.e., $\varphi = \varphi^* \circ \mathrm{oddsupp}|_{A^{n-2}}$ for some function $\varphi^*\colon \mathcal{P}(A) \to B$. Let $\widetilde{\varphi}\colon A^n \to B$ be the function given by

$$\widetilde{\varphi}(a_1,\dots,a_n) = \sum_{\substack{k<n \\ 2|n-k}} \sum_{1\leq i_1<\dots<i_k\leq n} \varphi^*(\mathrm{oddsupp}(a_{i_1},\dots,a_{i_k})),$$

for all $a_1,\dots,a_n \in A$. Each summand $\varphi^*(\mathrm{oddsupp}(a_{i_1},\dots,a_{i_k}))$ on the right side is an identification minor of φ. The function $\widetilde{\varphi}$ is determined by oddsupp and $\widetilde{\varphi}|_{A^n_{=}} = f|_{A^n_{=}}$.

Proposition 4.5. *Let F be a field, and let $f\colon F^n \to F$ be a polynomial function. If F is finite or the characteristic of F is 2, then $f|_{F^n_{=}}$ is determined by* oddsupp *if and only if there exist polynomials $P, Q \in F[x_1,\dots,x_n]$ such that $f = \overline{P} + \overline{Q}$, $\overline{P}$ is determined by* oddsupp*, and Q is a multiple of the polynomial Δ_n.*

Proof. For sufficiency, let us assume that $f = \overline{P}+\overline{Q}$, where P and Q are as in the statement of the proposition. Since $\overline{P}$ is determined by oddsupp, the restriction $\overline{P}|_{F^n_{=}}$ is obviously determined by oddsupp as well. Moreover, $\overline{Q}|_{F^n_{=}} \equiv 0$ by Lemma 3.4. Thus, $f|_{F^n_{=}} = \overline{P}|_{F^n_{=}} + \overline{Q}|_{F^n_{=}} = \overline{P}|_{F^n_{=}}$ is determined by oddsupp.

For necessity, assume first that F is finite. If $f|_{F^n_{=}}$ is determined by oddsupp, then there is a (not necessarily unique) function g such that g is determined by oddsupp and $f|_{F^n_{=}} = g|_{F^n_{=}}$. By Fact 3.1, g is a polynomial function; hence so is $h = f - g$. By Lemma 3.4, P_h is a multiple of the polynomial Δ_n.

Assume then that F is a field of characteristic 2. Since the additive group of any field of characteristic 2 is a Boolean group, Remark 4.4 applies to operations on F. Assume that $f\colon F^n \to F$ is a polynomial function such that $f|_{F^n_{=}}$ is determined by oddsupp, and let φ, φ^*, and $\widetilde{\varphi}$ be as defined in Remark 4.4. Then φ is also a polynomial function. The functions $\varphi^*(\mathrm{oddsupp}(a_{i_1},\dots,a_{i_k}))$, being identification minors of φ, are polynomial functions. Therefore, Remark 4.4 implies that $\widetilde{\varphi}$ is a polynomial function and $\widetilde{\varphi}|_{F^n_{=}} = f|_{F^n_{=}}$. Letting $g := \widetilde{\varphi}$ and $h := f - g$, and arguing as in the previous paragraph, we conclude that P_h is a multiple of the polynomial Δ_n. □

Theorem 4.6. *Let F be a field of characteristic 2, possibly infinite, and let $f\colon F^n \to F$ be a polynomial function of arity at least 4 which depends on all of its variables. Then $\operatorname{gap} f = p \geq 2$ if and only if there exist polynomials $P, Q \in F[x_1,\dots,x_n]$ such that $f = \overline{P}+\overline{Q}$, P is canonical, Q is a multiple of the polynomial Δ_n, and either*

(a) *exactly $n-p$ variables occur in P and $\overline{Q} \neq 0$, or*
(b) *P is not a constant polynomial and $\overline{P}$ satisfies conditions* (A) *and* (B_2) *of Proposition 4.3.*

Otherwise $\operatorname{gap} f = 1$.

Proof. Combine Theorem 2.6, Theorem 2.7, Lemma 3.3, Lemma 3.4, Proposition 4.3, and Proposition 4.5, and observe that if $f|_{F^n_{=}}$ is determined by oddsupp then $\operatorname{qa} f = n$ if and only if $f|_{F^n_{=}}$ is not constant. □

Corollary 4.7. *Let $F = \mathrm{GF}(q)$, where q is a power of 2, and let $f\colon F^n \to F$ be a polynomial function of essential arity $n > \max(q,3)$. If $\operatorname{gap} f = 2$, then f can be decomposed into a sum of polynomial functions of essential arity at most $q-1$.*

Proof. If $n > q$, then $F^n_{=} = F^n$; hence case (a) in Theorem 4.6 cannot occur, while in case (b) we have $\overline{Q} \equiv 0$; thus $f = \overline{P}$. Moreover, in case (b), every monomial of P involves at most $q-1$ variables, by conditions (A) and (B_2) of Proposition 4.3. This implies that f can be written as a sum of polynomial functions of essential arity at most $q-1$, namely the polynomial functions corresponding to the monomials of f. □

Remark 4.8. Applying Corollary 4.7 in the case $q = 2$, we see that any function $f\colon \{0,1\}^n \to \{0,1\}$ with essential arity $n \geq 4$ and $\operatorname{gap} f = 2$ can be written as a sum of at most unary functions, i.e., that f is a linear function.

Remark 4.9. From the results of [5] it follows that if A is a finite set and B is a Boolean group, then every function $f\colon A^n \to B$ with essential arity $n > \max(|A|, 3)$ and $\operatorname{gap} f = 2$ can be decomposed into a sum of functions of essential arity at most $n-2$ (cf. Remark 4.4). Corollary 4.7 shows that the bound $n-2$ on the essential arity of the summands can be improved to $q-1$ (which is independent of n) if $A = B = \mathrm{GF}(q)$, where q is a power of 2 (for further results in this direction see also [7]). In the example below, we will construct a polynomial function $f\colon F^n \to F$ over $F = \mathrm{GF}(q)$ for any odd prime power q and any $n \geq 2$, such that $\operatorname{gap} f = 2$ but f cannot be written as a sum of $(n-1)$-ary functions. This shows that Corollary 4.7 does not hold for finite fields with odd characteristic and that the condition of B's being a Boolean group cannot be dropped in the aforementioned result of [5].

Example 4.10. Let q be an odd prime power, and let f be the polynomial function

$$f(x_1, \dots, x_n) = \prod_{i=1}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big) \tag{2}$$

over $\mathrm{GF}(q)$, where $\frac{1}{2}$ stands for the multiplicative inverse of $2 = 1+1$ (it exists, since $\mathrm{GF}(q)$ is of odd characteristic). Let us identify the first two variables of f:

$$\begin{aligned} f(x_1, x_1, x_3, \dots, x_n) &= \Big(x_1^{q-1} - \frac{1}{2} \Big)^2 \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big) \\ &= \Big(x_1^{2q-2} - x_1^{q-1} + \frac{1}{4} \Big) \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big) \\ &= \frac{1}{4} \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big), \end{aligned}$$

since $x_1^q = x_1$ holds identically in $\mathrm{GF}(q)$. We see that x_1 becomes an inessential variable, and $\operatorname{ess} f_{2 \leftarrow 1} = n-2$. This together with the total symmetry of f shows that $\operatorname{gap} f = 2$.

Suppose that f is a sum of functions of arity at most $n-1$. By Fact 3.1, these functions are polynomial. This implies that every monomial of P_f involves at most $n-1$ variables. However, this is clearly not possible, as the expansion of the right side of (2) is a canonical polynomial that involves the monomial $x_1^{q-1} \cdots x_n^{q-1}$, which will not be cancelled by any other monomial. This contradiction shows that f cannot be expressed as a sum of functions of arity at most $n-1$.

5. Polynomial functions over fields of characteristic 0

We now consider the case of polynomial functions over fields of characteristic 0. Unlike polynomial functions over fields of characteristic 2 (see Proposition 4.5), it turns out that in the current case there is no polynomial function $f\colon F^n \to F$ whose restriction $f|_{F^n_{\neq}}$ is nonconstant and determined by oddsupp.

We first recall the notion of partial derivative in the case of polynomial functions. We denote the *partial derivative* of a polynomial $p \in F[x_1, \dots, x_n]$ with respect to its i-th variable by $\partial_i p$, and we define it by the following rules. The i-th partial derivative of a monomial is defined by the rule

$$\partial_i c x_1^{a_1} \cdots x_n^{a_n} = \begin{cases} c a_i x_1^{a_1} \cdots x_{i-1}^{a_{i-1}} x_i^{a_i - 1} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}, & \text{if } a_i \neq 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Moreover, partial derivatives are additive, i.e.,

$$\partial_i \sum_{j \in J} f_j = \sum_{j \in J} \partial_i f_j. \tag{4}$$

The partial derivatives of arbitrary polynomials can then be determined by application of (3) and (4). The partial derivative of a polynomial function $f\colon F^n \to F$ with respect to its i-th variable is denoted by $\partial_i f$, and it is given by $\partial_i f := \overline{\partial_i P_f}$.

Observe that for fields of characteristic 0, $\partial_i f = 0$ if and only if the i-th variable is inessential in f. Also, let us note the difference between

$$\partial_1 f(x_1, x_1, x_2) = \partial_1(f(x_1, x_1, x_2)) \quad \text{and} \quad (\partial_1 f)(x_1, x_1, x_2),$$

where $f\colon F^3 \to F$ is a polynomial function. The first one is a partial derivative of an identification minor of f, while the second one is an identification minor of a partial derivative of f. The chain rule gives the following relationship between these polynomials functions:

$$\partial_1 f(x_1, x_1, x_2) = (\partial_1 f)(x_1, x_1, x_2) + (\partial_2 f)(x_1, x_1, x_2).$$

Since we will often consider derivatives of minors, it is worth formulating a generalization of the above formula.

Fact 5.1. *Let F be a field of characteristic 0, let $f\colon F^n \to F$ be a polynomial function, let $\sigma\colon [n] \to [m]$, and let $g \in F^m \to F$ be the minor of f defined by $g(x_1, \dots, x_m) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. Then the j-th partial derivative of g is*

$$\partial_j g = \sum_{\sigma(i)=j} (\partial_i f)(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Lemma 5.2. *Let F be a field of characteristic 0 and let $f\colon F^n \to F$ be a polynomial function of arity at least 2. Then $f|_{F^n_{\neq}}$ is determined by* oddsupp *if and only if $f|_{F^n_{\neq}}$ is constant, i.e.,* $\operatorname{qa} f = 0$.

Proof. Sufficiency is obvious. We will prove necessity. For $n = 2$, the claim is trivial, so we will assume that $n \geq 3$. Let us suppose that $f|_{F^n_{\neq}}$ is determined by oddsupp. Then $f(x_1, x_1, x_3, \dots, x_n)$ does not depend on x_1 by Fact 2.5; hence we have

$$(\partial_1 f)(x_1, x_1, x_3, \dots, x_n) + (\partial_2 f)(x_1, x_1, x_3, \dots, x_n) = 0$$

by Fact 5.1. Let $\mathbf{u} = (x_1, x_1, x_1, x_4, \dots, x_n) \in F^n$. From the above equality it follows that

$$(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) = 0,$$

and a similar argument shows that

$$(\partial_1 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0 \quad \text{and} \quad (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0.$$

Since the characteristic of F is different from 2, by adding these three equalities we can conclude that

$$(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0.$$

However, according to Fact 5.1, $(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u})$ is nothing else but the derivative of $f(x_1, x_1, x_1, x_4, \dots, x_n)$ with respect to x_1. This implies that $f(x_1, x_1, x_1, x_4, \dots, x_n)$ does not depend on x_1, i.e.,

$$f(a, a, a, x_4, \dots, x_n) = f(b, b, b, x_4, \dots, x_n) \tag{5}$$

for any $a, b, x_4, \dots, x_n \in F$.

Informally, equality (5) expresses the fact that whenever the first three entries of an n-tuple are the same, then replacing these three entries with another element of F, the value of f does not change. (By symmetry, this is certainly true for any three entries, not only the first three.) From the definition of being determined by oddsupp it follows immediately that we can also change any two identical entries:

$$f(\cdots a \cdots a \cdots) = f(\cdots b \cdots b \cdots). \tag{6}$$

Let $\mathbf{x} = (x_1, \dots, x_n)$ be any vector in $F^n_{\neq}$. We may suppose without loss of generality that $x_1 = x_2$. With the help of (5) and (6) we can replace the entries of $\mathbf{x}$ in triples and

pairs, until all of them are the same:

$$\begin{aligned} f(\mathbf{x}) &= f(\underline{x_1, x_1}, x_3, x_4, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_3, x_3, x_3}, x_4, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_4, x_4}, \underline{x_4, x_4}, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_5, x_5, x_5}, \underline{x_5, x_5}, x_6, \dots, x_n) \\ &= f(\underline{x_6, x_6}, \underline{x_6, x_6}, \underline{x_6, x_6}, \dots, x_n) = \cdots \\ &= f(x_n, x_n, x_n, x_n, x_n, x_n, \dots, x_n). \end{aligned}$$

If n is even, then (6) shows that $f(\mathbf{x}) = f(\mathbf{0})$:

$$f(\mathbf{x}) = f(\underline{x_n, x_n}, \underline{x_n, x_n}, \dots, \underline{x_n, x_n}) = f(0, 0, 0, 0, \dots, 0, 0);$$

while if n is odd, then we use both (5) and (6):

$$f(\mathbf{x}) = f(\underline{x_n, x_n, x_n}, \underline{x_n, x_n}, \dots, \underline{x_n, x_n}) = f(0, 0, 0, 0, 0, \dots, 0, 0).$$

We have shown that $f(\mathbf{x}) = f(\mathbf{0})$ for all $\mathbf{x} \in F^n_{=}$; hence $f|_{F^n_{=}}$ is indeed constant. □

Remark 5.3. It follows from Lemma 3.4 that a function $f\colon A^n \to B$ satisfies the condition of Lemma 5.2, i.e., $f|_{F^n_{=}}$ is constant, if and only if f is induced by a polynomial of the form $P \cdot \Delta_n + c$, where $P \in F[x_1, \dots, x_n]$ and $c \in F$.

Lemma 5.4. *Let F be a field of characteristic 0 and let $f\colon F^3 \to F$ be a polynomial function. If* $\operatorname{gap} f = 2$, *then* $\operatorname{qa} f = 1$.

Proof. By case (iii) of Theorem 2.6, there exist a nonconstant map $h\colon A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that

$$\begin{aligned} f(x_1, x_0, x_0) &= h(x_{i_1}), \\ f(x_0, x_1, x_0) &= h(x_{i_2}), \\ f(x_0, x_0, x_1) &= h(x_{i_3}). \end{aligned}$$

Up to permutation of variables there are four possibilities for (i_1, i_2, i_3), namely $(1, 1, 1)$, $(0, 0, 0)$, $(1, 1, 0)$ and $(1, 0, 0)$. We will show that the first three cases cannot occur.

If $(i_1, i_2, i_3) = (1, 1, 1)$ then $f|_{F^3_{=}}$ is determined by oddsupp, and Lemma 5.2 shows that h is constant, a contradiction.

If $(i_1, i_2, i_3) = (0, 0, 0)$ then $f(x_2, x_1, x_1) = f(x_1, x_2, x_1) = f(x_1, x_1, x_2) = h(x_1)$; hence $f(x_2, x_1, x_1)$ does not depend on x_2. By Fact 5.1 this means that $(\partial_1 f)(x_2, x_1, x_1) = 0$, in particular, $(\partial_1 f)(x_1, x_1, x_1) = 0$ for all $x_1 \in F$. Similarly, we have $(\partial_2 f)(x_1, x_1, x_1) = (\partial_3 f)(x_1, x_1, x_1) = 0$. Another application of Fact 5.1 yields

$$\begin{aligned} \partial_1 h(x_1) &= \partial_1 f(x_1, x_1, x_1) \\ &= (\partial_1 f)(x_1, x_1, x_1) + (\partial_2 f)(x_1, x_1, x_1) + (\partial_3 f)(x_1, x_1, x_1) = 0, \end{aligned}$$

and this means that h is constant, a contradiction.

If $(i_1, i_2, i_3) = (1, 1, 0)$, then $f(x_1, x_2, x_2) = f(x_2, x_1, x_2) = f(x_1, x_1, x_2) = h(x_1)$, which does not depend on x_2. Again, by Fact 5.1 we see that

$$\begin{aligned} (\partial_2 f)(x_1, x_2, x_2) + (\partial_3 f)(x_1, x_2, x_2) &= 0, \\ (\partial_1 f)(x_2, x_1, x_2) + (\partial_3 f)(x_2, x_1, x_2) &= 0, \\ (\partial_3 f)(x_1, x_1, x_2) &= 0. \end{aligned}$$

From these equalities it follows that

$$(\partial_1 f)(x_1, x_1, x_1) = (\partial_2 f)(x_1, x_1, x_1) = (\partial_3 f)(x_1, x_1, x_1) = 0,$$

which is again a contradiction.

We are left with the case that $(i_1, i_2, i_3) = (1, 0, 0)$ (up to permutation). This implies that $f|_{F^3_{=}} = h(x_1)|_{F^3_{=}}$, i.e., $\operatorname{qa} f = 1$. □

Theorem 5.5. *Let F be a field of characteristic 0, let $n \geq 3$, and let $P \in F[x_1, \ldots, x_n]$ be a polynomial such that all n variables occur in P. Then* $\operatorname{gap} \overline{P} = p \geq 2$ *if and only if there exist polynomials $Q, R \in F[x_1, \ldots, x_n]$ such that $P = Q + R$, exactly $n - p$ variables occur in Q, and R is a nonzero multiple of the polynomial Δ_n. Otherwise* $\operatorname{gap} \overline{P} = 1$. *Moreover, the decomposition $P = Q + R$ is unique.*

Proof. For necessity, assume that $\operatorname{gap} \overline{P} = p \geq 2$. By Lemma 5.2, if $\overline{P}|_{F^n_=}$ is determined by oddsupp, then $\operatorname{qa} \overline{P} = 0$. Theorem 2.6 and Lemma 5.4 then imply that if $\operatorname{gap} \overline{P} = p \geq 2$, then $\operatorname{qa} \overline{P} = n - p$. By Theorem 2.7, there exist unique functions $g, h \colon F^n \to F$ such that $\overline{P} = g + h$, $h|_{F^n_=} \equiv 0$, $h \not\equiv 0$ and $\operatorname{ess} g = n - p$. By Lemma 3.3, g and h are polynomial functions. Since F is infinite, each one of g and h is induced by a unique polynomial over F, namely P_g and P_h, respectively. Thus, $P = P_g + P_h$. By Fact 3.2, exactly $n - p$ variables occur in P_g, and by Lemma 3.4, P_h is a nonzero multiple of $\Delta(x_1, \ldots, x_n)$.

For sufficiency, assume that $P = Q + R$, where Q and R are as in the statement of the theorem. Then $\operatorname{ess} \overline{Q} = n - p$ by Fact 3.2, and $\overline{R} \not\equiv 0$ and $\overline{R}|_{F^n_=} \equiv 0$ by Lemma 3.4. From Theorem 2.7 it follows that $\operatorname{qa} \overline{P} = n - p$, and then Theorem 2.6 implies that $\operatorname{gap} \overline{P} = p$.

The uniqueness of the decomposition $P = Q + R$ follows from Theorem 2.7 and from the fact that polynomials and polynomial functions over infinite fields are in one-to-one correspondence. □

Let us note that in the proof of the above theorem we did not really make use of the fact that the function $\overline{P}$ is polynomial; we only used the basic properties of the derivative. Therefore the theorem remains valid for differentiable real functions.

Theorem 5.6. *Let $f \colon \mathbb{R}^n \to \mathbb{R}$ be a differentiable function of arity at least 2. Then* $\operatorname{gap} f = p \geq 2$ *if and only if there exist differentiable functions $g, h \colon \mathbb{R}^n \to \mathbb{R}$ such that $f = g + h$, $h|_{\mathbb{R}^n_=} \equiv 0$, $h \not\equiv 0$, and $\operatorname{ess} g = n - p$. Otherwise* $\operatorname{gap} f = 1$. *Moreover, the decomposition $f = g + h$ is unique.*

6. Some remarks on polynomial functions over infinite fields of odd characteristic

As the following example illustrates, Proposition 4.5 and Lemma 5.2 do not extend to infinite fields of odd characteristic.

Example 6.1. Let F be an arbitrary field of characteristic 3, and let $f \colon F^3 \to F$ be the polynomial function induced by

$$2x^3 + 2y^3 + 2z^3 + yz^2 - xy^2 - xz^2 + y^2z + 2xyz. \tag{7}$$

It is straightforward to verify that

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = 2y^3.$$

Hence $f|_{F^3_=}$ is determined by oddsupp but $f|_{F^3_=}$ is not constant. This shows that Lemma 5.2 does not hold if F has characteristic 3.

Next we show that Proposition 4.5 does not hold for infinite fields of characteristic 3. Assume now that F is infinite, and let f be induced by (7). Suppose that $g \colon F^3 \to F$ is a polynomial function determined by oddsupp induced by the canonical polynomial

$$\sum_{(k_1,k_2,k_3) \in \mathbb{N}^3} c_{(k_1,k_2,k_3)} x_1^{k_1} x_2^{k_2} x_3^{k_3}.$$

Condition (B) of Proposition 4.3 yields the following equalities:

$$\begin{aligned} c_{(3,0,0)} + c_{(2,1,0)} + c_{(1,2,0)} + c_{(0,3,0)} &= 0, \\ c_{(2,0,1)} + c_{(1,1,1)} + c_{(0,2,1)} &= 0, \\ c_{(1,0,2)} + c_{(0,1,2)} &= 0. \end{aligned}$$

Taking into account the total symmetry of g (condition (A)) and the fact that the characteristic of F is not 2, the only solution to this system of equations is $c_{(k_1,k_2,k_3)} = 0$ for all $(k_1, k_2, k_3) \in \mathbb{N}^3$ such that $k_1 + k_2 + k_3 = 3$. Thus, the canonical polynomial of $g(x, x, x)$ does not contain any cubic term; therefore it cannot coincide with $f(x, x, x) = 2x^3$, and we conclude that $f|_{F^3_=} \neq g|_{F^3_=}$.

Acknowledgments

The authors are grateful to Ágnes Szendrei for her valuable comments on an early version of this manuscript.

The first named author is supported by the internal research project F1R-MTH-PUL-12RDO2 of the University of Luxembourg.

The third named author acknowledges that the present project is supported by the Hungarian National Foundation for Scientific Research under grants no. K77409 and K83219, by the National Research Fund of Luxembourg, and cofunded under the Marie Curie Actions of the European Commission (FP7-COFUND).

The present project is supported by the European Union and co-funded by the European Social Fund under the project "Telemedicine-focused research activities on the field of Mathematics, Informatics and Medical sciences" of project number "TÁMOP-4.2.2.A-11/1/KONV-2012-0073". This work was developed within the FCT Project PEst-OE/MAT/UI0143/2014 of CAUL, FCUL.

References

[1] Berman, J., Kisielewicz, A., On the number of operations in a clone. Proc. Amer. Math. Soc. 122 (1994), 359–369.

[2] Couceiro, M., Lehtonen, E., On the effect of variable identification on the essential arity of functions on finite sets. Int. J. Found. Comput. Sci. 18 (2007), 975–986.

[3] Couceiro, M., Lehtonen, E., Generalizations of Świerczkowski's lemma and the arity gap of finite functions. Discrete Math. 309 (2009), 5905–5912.

[4] Couceiro, M., Lehtonen, E., The arity gap of polynomial functions over bounded distributive lattices. In: 40th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2010), pp. 113–116. Los Alamitos: IEEE Computer Society 2010.

[5] Couceiro, M., Lehtonen, E., Waldhauser, T., Decompositions of functions based on arity gap. Discrete Math. 312 (2012), 238–247.

[6] Couceiro, M., Lehtonen, E., Waldhauser, T., The arity gap of order-preserving functions and extensions of pseudo-Boolean functions. Discrete Appl. Math. 160 (2012), 383–390.

[7] Couceiro, M., Lehtonen, E., Waldhauser, T., Additive decomposability of functions over abelian groups. Internat. J. Algebra Comput. 23 (2013), 643–662.

[8] Salomaa, A., On essential variables of functions, especially in the algebra of logic. Ann. Acad. Sci. Fenn. Ser. A I. Math. 339 (1963), 3–11.

[9] Shtrakov, S., Koppitz, J., On finite functions with non-trivial arity gap. Discuss. Math. Gen. Algebra Appl. 30 (2010), 217–245.

[10] Willard, R., Essential arities of term operations in finite algebras. Discrete Math. 149 (1996), 239–259.

(M. Couceiro) LAMSADE, Université Paris-Dauphine, Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France and LORIA (CNRS – Inria Nancy Grand Est – Université de Lorraine), BP239, 54506 Vandœuvre lès Nancy, France

E-mail address: miguel.couceiro@inria.fr

(E. Lehtonen) Computer Science and Communications Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg and Centro de Álgebra da Universidade de Lisboa, Avenida Professor Gama Pinto 2, 1649-003 Lisbon, Portugal; Departamento de Matemática, Faculdade de Ciências, Universidade de Lisboa, 1749-016 Lisbon, Portugal

E-mail address: erkko@campus.ul.pt

(T. Waldhauser) Mathematics Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L–1359 Luxembourg, Luxembourg and Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H–6720 Szeged, Hungary

E-mail address: twaldha@math.u-szeged.hu