International Journal of Algebra and Computation
Vol. 23, No. 3 (2013) 643–662
© World Scientific Publishing Company
DOI: 10.1142/S0218196713500136

World Scientific
www.worldscientific.com

ADDITIVE DECOMPOSABILITY OF FUNCTIONS OVER ABELIAN GROUPS

MIGUEL COUCEIRO*
Mathematics Research Unit, University of Luxembourg
6, rue Richard Coudenhove-Kalergi, L–1359 Luxembourg, Luxembourg
miguel.couceiro@uni.lu

ERKKO LEHTONEN
Computer Science and Communications Research Unit
University of Luxembourg, 6, rue Richard Coudenhove-Kalergi
L–1359 Luxembourg, Luxembourg
erkko.lehtonen@uni.lu

TAMÁS WALDHAUSER
Mathematics Research Unit, University of Luxembourg
6, rue Richard Coudenhove-Kalergi, L–1359 Luxembourg
Luxembourg, Bolyai Institute, University of Szeged
Aradi vértanúk tere 1, H–6720 Szeged, Hungary
twaldha@math.u-szeged.hu

Received 4 November 2011
Accepted 24 January 2013
Published 21 March 2013

Communicated by M. Volkov

Abelian groups are classified by the existence of certain additive decompositions of group-valued functions of several variables.

Keywords: Abelian group; Boolean group; group-valued function; arity gap; additive decomposition; discrete derivative.

Mathematics Subject Classification 2010: 08A40, 05E15

1. Introduction

The problem of expressing functions of several variables in terms of a finite number of functions with fewer variables has been addressed in various ways in the literature. Perhaps one of the most famous incarnations of this general problem

*Current address: Lamsade, Université Paris-Dauphine, Place du Maréchal de Lattre de Tassigny, 75775 Paris cedex 16, France, miguel.couceiro@dauphine.fr.

is Hilbert's 13th problem dealing with 7th-degree equations, which leads to the question whether continuous real functions of several variables can be expressed as a superposition of finitely many continuous functions with fewer variables. Affirmative answers were provided in the works by Kolmogorov [20] and Arnol'd [1, 2], which led into Kolmogorov's superposition theorem [21] that asserts, roughly speaking, that every continuous real function of two or more variables can be written as finite sums and superpositions of continuous real functions of just one variable.

In this paper, we consider yet another instance of this general problem. We study additive decompositions of functions $f: A^n \to B$ into sums of functions depending on fewer than n variables, assuming that A is an arbitrary set and B is an abelian group (not necessarily the real numbers). We show that such a decomposition exists for all functions $f: A^n \to B$ determined by oddsupp (see Sec. 2.2) if and only if A is finite and the exponent of B is a power of 2. In the case that the exponent of B is 2^e, every function $f: A^n \to B$ determined by oddsupp is decomposable into a sum of functions depending on at most $|A| + e - 2$ variables. (Note that this bound depends only on A and B.) Moreover, there exists such a decomposition where the summands are obtained from f by substitution of constants for variables. This generalizes and improves on [10, Theorem 5.2] whereby functions $f: A^n \to B$ determined by oddsupp and valued on a Boolean group B were decomposed into sums of functions depending on at most $n - 2$ variables. Functions determined by oddsupp arise in a natural way in the study of sequences $\langle p_n(C)\rangle_{n<\omega}$, where $p_n(C)$ denotes the number of n-ary operations of a clone C which depend on all of their variables (see [3, 18, 30]). Later, it was shown that determinability by oddsupp is also tightly related to the notion of arity gap, or the effect of identification of variables on the number of essential variables of functions of several variables (see Secs. 2.1 and 2.2).

2. Preliminaries

2.1. *Functions, essential variables, the arity gap*

Throughout this paper, let A and B be arbitrary sets with at least two elements. A *function* (*of several variables*) from A to B is a mapping $f: A^n \to B$, for some integer $n \geq 1$ called the *arity* of f. Functions of several variables from A to A are referred to as *operations* on A.

For an integer $n \geq 1$, let $[n] := \{1, \ldots, n\}$. Let $f: A^n \to B$, and let $i \in [n]$. We say that the ith variable is *essential* in f (or f *depends* on x_i), if there exist elements $a_1, \ldots, a_n, a_i' \in A$ such that

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

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

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

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

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

Observe that a function g is a simple minor of f, if g can be obtained from f by permutation of variables, addition and deletion of inessential variables and identification of variables. Similarly, two functions are equivalent, if one can be obtained from the other by permutation of variables and addition of inessential variables.

The *arity gap* of f is defined as

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

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

For general background and studies on the dependence of functions on their variables, see, e.g. [5, 6, 12–14, 25, 27, 29, 31]. For the simple minor relation and its variants, see, e.g. [4, 11, 15, 16, 19, 22–24, 28, 32]. The notion of arity gap was considered in [7–10, 25, 30], and a general classification of functions according to their arity gap was established in [8], given in terms of the notions of quasi-arity and determination by oddsupp. The following explicit complete classification of Boolean functions was established in [7].

Theorem 1. *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function with at least two essential variables. Then* $\operatorname{gap} f = 2$ *if and only if f is equivalent to one of the following polynomial functions over* GF(2):

- $x_1 + x_2 + \cdots + x_m + c$ *for some* $m \geq 2$,
- $x_1x_2 + x_1 + c$,
- $x_1x_2 + x_1x_3 + x_2x_3 + c$,
- $x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + c$,

where $c \in \{0,1\}$. *Otherwise* $\operatorname{gap} f = 1$.

2.2. *Functions determined by* oddsupp

We will denote tuples by boldface letters and their components by the corresponding italic letters with subscripts, e.g. $\mathbf{x} = (x_1, \ldots, x_n) \in A^n$. For $I \subseteq [n]$ and $\mathbf{x} \in A^n$, let $\mathbf{x}|_I \in A^I$ stand for the tuple that is obtained from $\mathbf{x}$ by deleting the ith component of $\mathbf{x}$ for every $i \notin I$. More precisely, if $I = \{i_1, \ldots, i_k\}$ and $i_1 < \ldots < i_k$, then $\mathbf{x}|_I = (x_{i_1}, \ldots, x_{i_k})$.

Berman and Kisielewicz [3] introduced the following notion of a function being determined by oddsupp. Denote by $\mathcal{P}(A)$ the power set of A, and define the function oddsupp : $\bigcup_{n \geq 1} A^n \to \mathcal{P}(A)$ by

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

For $\varphi : \mathcal{P}(A) \to B$, let $❄_\varphi : \bigcup_{n \geq 1} A^n \to B$ be the map defined by $❄_\varphi(\mathbf{x}) = \varphi(\operatorname{oddsupp}(\mathbf{x}))$. A function $f : A^n \to B$ is *determined by* oddsupp if $f(\mathbf{x})$ depends only on $\operatorname{oddsupp}(\mathbf{x})$, i.e. if there exists $\varphi : \mathcal{P}(A) \to B$ such that $❄_\varphi|_{A^n} = f$. When there is no risk of ambiguity, we will simply write $❄_\varphi$ instead of $❄_\varphi|_{A^n}$. Clearly, the restriction of φ to

$$\mathcal{P}'_n(A) = \{S \in \mathcal{P}(A) : |S| \in \{n, n-2, \ldots\}\}$$

uniquely determines f and vice versa. Thus, for finite sets A and B, the number of functions $f : A^n \to B$ that are determined by oddsupp is $|B|^{|\mathcal{P}'_n(A)|}$. The following facts are straightforward to verify.

Fact 2. The Boolean functions determined by oddsupp are exactly the affine functions (also known as linear functions in the theory of Boolean functions).

Fact 3. A function $f : A^n \to B$ is determined by oddsupp if and only if f is totally symmetric and $f_{2 \leftarrow 1}$ does not depend on x_1.

Fact 4. If $(B; +)$ is an abelian group, then $❄_{\varphi_1 + \varphi_2} = ❄_{\varphi_1} + ❄_{\varphi_2}$ holds for all maps $\varphi_1, \varphi_2 : \mathcal{P}(A) \to B$.

It was shown by Willard [30] that if the essential arity of a function $f : A^n \to B$ is sufficiently large, then $\operatorname{gap} f \leq 2$, and he also classified such functions according to their arity gap.

Theorem 5 (Willard [30]). *Let A be a finite set and B be an arbitrary set, and assume that $f : A^n \to B$ depends on all of its variables and $n > \max(|A|, 3)$. If f is determined by* oddsupp *then* $\operatorname{gap} f = 2$. *Otherwise* $\operatorname{gap} f = 1$.

If B is a Boolean group (i.e. an abelian group of exponent 2), then functions f with $\operatorname{gap} f \geq 2$ can be characterized by the existence of certain additive decompositions. Here we present one of the main results of [10] in the case $n > |A|$.

Theorem 6 ([10]). *Let* $(B;+)$ *be a Boolean group, and let* $f\colon A^n \to B$ *be of essential arity* $n > |A|$. *If* f *is determined by* oddsupp, *then there exists a map* $\varphi\colon \mathcal{P}'_n(A) \to B$ *such that*

$$f(\mathbf{x}) = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{\substack{I \subseteq [n] \\ |I| = n-2i}} \text{❄}_{\varphi}(\mathbf{x}|_I). \tag{1}$$

From Theorems 5 and 6 it follows that every function $f\colon A^n \to B$ with large enough essential arity (i.e. ess $f > \max(|A|, 3)$) and gap $f = 2$ is decomposable into a sum of essentially at most $(n-2)$-ary functions. This fact is the starting point of this paper. We will prove in Sec. 3 that such decompositions exist not only when B is a Boolean group, but also whenever B is a group whose exponent is a power of 2. In fact, we will show that in this case there is a decomposition into functions with bounded essential arity, where the bound does not depend on n. We will also see that if the exponent of B is not a power of 2, then such a decomposition does not always exist, not even a decomposition into $(n-1)$-ary functions. In Sec. 4 we focus on Boolean groups B, and we provide a concrete decomposition of a very special symmetric form, which is also unique.

Any set B can be embedded into a Boolean group, e.g. into $\mathcal{P}(B)$ with the symmetric difference operation. Then we can regard any function $f\colon A^n \to B$ as a function from A^n to $\mathcal{P}(B)$, and we can apply the results of Sec. 4 to this function. We illustrate this for the case $A = B = \mathbb{Z}_3$ in Sec. 5. Here we obtain decompositions involving a strange mixture of the field operations on $\mathbb{Z}_3$ and the symmetric difference operation, but we will see that they can be always computed within B, without the need of working in the extension $\mathcal{P}(B)$.

2.3. *Binomial coefficients*

We shall make use of the following combinatorial results.

Theorem 7 (Shattuck and Waldhauser [26]). *For all non-negative integers* m, t *with* $0 \le t \le \frac{m}{2} - 1$, *the following identity holds*:

$$\sum_{i=t+1}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2i} \binom{i-1}{t} = 2^{m-2t-1} \sum_{k=0}^{\lfloor \frac{t}{2} \rfloor} \binom{m-3-t-2k}{t-2k} + (-1)^{t+1}.$$

Theorem 8. *For all non-negative integers* m, t *with* $0 \le t \le \frac{m-1}{2}$ *the following identity holds*:

$$\sum_{k=t+1}^{\lfloor \frac{m+1}{2} \rfloor} \binom{m}{2k-1} \binom{2k-1}{2t} = \binom{m}{2t} 2^{m-2t-1}.$$

Proof. Both sides of the identity count the number of pairs (A, B), where $A \subseteq B \subseteq [m]$, $|A| = 2t$ and $|B|$ is odd. □

3. The General Case

Throughout this section, unless mentioned otherwise, A is a finite set with a distinguished element 0_A and $(B;+)$ is an arbitrary, possibly infinite abelian group with neutral element 0_B. With no risk of ambiguity, we will omit the subscripts and will denote both 0_A and 0_B by 0. Recall that the *order* of $b \in B$, denoted by $\operatorname{ord}(b)$, is the smallest positive integer n such that $nb = \underbrace{b + \cdots + b}_{n \text{ times}} = 0$. If there is no such positive integer, then $\operatorname{ord}(b) = \infty$. If the orders of all elements of B have a finite common upper bound, then the *exponent* of B, denoted by $\exp(B)$, is the least common upper bound (equivalently, the least common multiple) of these orders. Otherwise let $\exp(B) = \infty$. Note that a Boolean group is a group of exponent 2.

We say that a function $f : A^n \to B$ is *k-decomposable* if it admits an additive decomposition $f = f_1 + \cdots + f_s$, where the essential arity of each $f_i : A^n \to B$ is at most k. Moreover, we say that f is *decomposable* if it is $(n-1)$-decomposable.

According to Fact 2, every Boolean function determined by oddsupp is 1-decomposable, while the functions described in Theorem 6 are $(n-2)$-decomposable. Our goal in this section is to extend these results by characterizing those abelian groups B which have the property that every function $f : A^n \to B$ determined by oddsupp is decomposable. As we will see, this is the case if and only if $\exp(B)$ is a power of 2. Moreover, we will determine, for each such abelian group B, the smallest number k such that every function $f : A^n \to B$ determined by oddsupp is k-decomposable.

The Taylor formula developed for finite functions by Gilezan [17] provides a tool to test decomposability of functions. Although in [17] the codomain B was assumed to be a ring, only multiplication by 0 and 1 was used in the Taylor formula; hence it is valid for abelian groups as well. For self-containedness, we present here the formula with a proof (see Proposition 10).

For a given $\mathbf{x} \in A^n$ and $i \in [n]$, $a \in A$, let $\mathbf{x}_i^a$ denote the n-tuple that is obtained from $\mathbf{x}$ by replacing its ith component by a. More generally, for $I \subseteq [n]$ and $\mathbf{a} \in A^n$, let $\mathbf{x}_I^{\mathbf{a}}$ denote the n-tuple that is obtained from $\mathbf{x}$ by replacing its ith component by a_i for every $i \in I$. (Observe that the components a_i of $\mathbf{a}$ with $i \notin I$ are irrelevant in determining $\mathbf{x}_I^{\mathbf{a}}$.)

For any $a \in A$ and $i \in [n]$ we define the *partial derivative* of $f : A^n \to B$ with respect to its ith variable with parameter a as the function $\Delta_i^a f : A^n \to B$ given by

$$\Delta_i^a f(\mathbf{x}) = f(\mathbf{x}_i^a) - f(\mathbf{x}).$$

Note that for each parameter $a \in A$ we have a different partial derivative of f with respect to its ith variable. We need the parameter a because A is just a set without any structure; hence we cannot define differences like $f(x+h) - f(x)$. It is easy to verify that the ith variable of f is inessential if and only if $\Delta_i^a f$ is identically 0 for some $a \in A$ (equivalently, for all $a \in A$).

Clearly, the partial derivatives are additive, i.e. $\Delta_i^a(f+g) = \Delta_i^a f + \Delta_i^a g$. Moreover, differentiations with respect to different variables commute with each other:

$$\Delta_i^a \Delta_j^b f(\mathbf{x}) = \Delta_j^b \Delta_i^a f(\mathbf{x}) = f(\mathbf{x}_{ij}^{ab}) - f(\mathbf{x}_i^a) - f(\mathbf{x}_j^b) + f(\mathbf{x}) \tag{2}$$

for all $a, b \in A$, $i \neq j \in [n]$. (Here $\mathbf{x}_{ij}^{ab}$ is a shorthand notation for $(\mathbf{x}_i^a)_j^b = (\mathbf{x}_j^b)_i^a$.) This property allows us to define higher-order derivatives: for $I = \{i_1, \ldots, i_k\} \subseteq [n]$ and $\mathbf{a} \in A^n$ let $\Delta_I^{\mathbf{a}} f = \Delta_{i_1}^{a_1} \cdots \Delta_{i_k}^{a_k} f$. (Again, the components a_i $(i \notin I)$ are irrelevant.) The following proposition generalizes formula (2) above.

Proposition 9. *For any function $f \colon A^n \to B$, $I \subseteq [n]$ and $\mathbf{a} \in A^n$, we have*

$$\Delta_I^{\mathbf{a}} f(\mathbf{x}) = \sum_{J \subseteq I} (-1)^{|I \setminus J|} f(\mathbf{x}_J^{\mathbf{a}}).$$

Proof. Easy induction on $|I|$. (For $|I| = 2$, the identity is just (2).) □

Now we are ready to state and prove the Taylor formula for functions $f \colon A^n \to B$, which is essentially the same as [**17**, Theorems 2 and 3]. (Let us note that in the following considerations any fixed n-tuple $\mathbf{a} \in A^n$ could be used instead of $\mathbf{0}$.)

Proposition 10. *Any function $f \colon A^n \to B$ can be expressed as a sum of some of its partial derivatives at $\mathbf{0}$*:

$$f(\mathbf{x}) = \sum_{I \subseteq [n]} \Delta_I^{\mathbf{x}} f(\mathbf{0}). \tag{3}$$

Proof. Using Proposition 9, we can compute the right-hand side as follows:

$$\sum_{I \subseteq [n]} \Delta_I^{\mathbf{x}} f(\mathbf{0}) = \sum_{I \subseteq [n]} \sum_{J \subseteq I} (-1)^{|I \setminus J|} f(\mathbf{0}_J^{\mathbf{x}}).$$

Observe that $K := I \setminus J$ can be any subset of $[n] \setminus J$. Hence

$$\begin{aligned} \sum_{I \subseteq [n]} \sum_{J \subseteq I} (-1)^{|I \setminus J|} f(\mathbf{0}_J^{\mathbf{x}}) &= \sum_{J \subseteq [n]} \sum_{K \subseteq [n] \setminus J} (-1)^{|K|} f(\mathbf{0}_J^{\mathbf{x}}) \\ &= \sum_{J \subseteq [n]} \left(\sum_{K \subseteq [n] \setminus J} (-1)^{|K|} \right) f(\mathbf{0}_J^{\mathbf{x}}). \end{aligned}$$

Since a nonempty finite set has the same number of subsets of odd cardinality as subsets of even cardinality, the coefficient $\sum_{K \subseteq [n] \setminus J} (-1)^{|K|}$ of $f(\mathbf{0}_J^{\mathbf{x}})$ above is 0 unless $J = [n]$. Thus the sum reduces to $f(\mathbf{0}_{[n]}^{\mathbf{x}}) = f(\mathbf{x})$, and this completes the proof. □

The following proposition provides a useful criterion of decomposability.

Proposition 11. *A function $f \colon A^n \to B$ is k-decomposable if and only if $\Delta_I^{\mathbf{a}} f(\mathbf{0}) = 0$ for all $\mathbf{a} \in A^n$ and $I \subseteq [n]$ with more than k elements.*

Proof. Sufficiency follows directly from Proposition 10: clearly, the essential arity of the function $\mathbf{x} \mapsto \Delta_I^{\mathbf{x}} f(\mathbf{0})$ is at most $|I|$. Therefore, if $\Delta_I^{\mathbf{x}} f(\mathbf{0})$ vanishes whenever $|I| > k$, then (3) is a decomposition into a sum of essentially at most k-ary functions.

For necessity, let us suppose that $f = f_1 + \dots + f_s$, where $\operatorname{ess} f_i \leq k$ for $i \in [s]$. If $|I| > k$, then I contains (the index of) at least one of the inessential variables of f_i, hence $\Delta_I^{\mathbf{a}} f_i$ is constant 0 for every $\mathbf{a} \in A^n$ and $i \in [s]$. Since $\Delta_I^{\mathbf{a}} f = \Delta_I^{\mathbf{a}} f_1 + \dots + \Delta_I^{\mathbf{a}} f_s$, we can conclude that $\Delta_I^{\mathbf{a}} f$ is constant 0. In particular, we have $\Delta_I^{\mathbf{a}} f(\mathbf{0}) = 0$. □

The following two theorems constitute the main results of this section, and they show a strong dichotomy of abelian groups with respect to the decomposability of functions determined by oddsupp.

Theorem 12. *If A is a finite set and B is an abelian group of exponent 2^e, then every function $f : A^n \to B$ determined by* oddsupp *is $(|A| + e - 2)$-decomposable.*

Proof. Observe that if the essential arity of f is at most $|A|+e-2$, then the statement trivially holds (with a decomposition involving only one summand). Suppose now that $n = \operatorname{ess} f > |A| + e - 2$ and $f = ❄_\varphi$ for some $\varphi : \mathcal{P}'_n(A) \to B$. By Proposition 11, it suffices to verify that $\Delta_I^{\mathbf{a}} f(\mathbf{0}) = 0$ whenever $|I| \geq |A| + e - 1$. Let $\{a_i : i \in I\} =: \{b_1, \dots, b_t\}$ ($b_i \neq b_j$ whenever $i \neq j$), and let $B_j := \{i \in I : a_i = b_j\}$. Thus $|B_j|$ is the number of occurrences of b_j in $\mathbf{a}|_I$; hence $|B_1| + \dots + |B_t| = |I|$ and $t \leq |A|$. Using Proposition 9, we can expand $\Delta_I^{\mathbf{a}} f(\mathbf{0})$ as

$$\Delta_I^{\mathbf{a}} f(\mathbf{0}) = \sum_{J \subseteq I} (-1)^{|I \setminus J|} f(\mathbf{0}_J^{\mathbf{a}}) = \sum_{J \subseteq I} (-1)^{|I \setminus J|} \varphi(\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}})). \tag{4}$$

Let us fix a set $S \subseteq A$ that appears as $\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}})$ in the above sum.

Assume first that $0 \in \{b_1, \dots, b_t\}$, say $b_t = 0$. Then $\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}}) = S$ if and only if $|J \cap B_j|$ is odd whenever $b_j \in S$ and $|J \cap B_j|$ is even whenever $b_j \notin S$ for $j = 1, \dots, t-1$ (note that $J \cap B_t$ is irrelevant in determining $\mathbf{0}_J^{\mathbf{a}}$). Since the number of subsets of B_t of even cardinality equals the number of subsets of B_t of odd cardinality, it holds that the number of sets J satisfying $\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}}) = S$ that have an even cardinality equals the number of those that have an odd cardinality. Hence, the terms corresponding to such sets J will cancel each other in (4).

Assume now that $0 \notin \{b_1, \dots, b_t\}$. Then clearly $t \leq |A| - 1$. Similarly, as in the previous case, we have that $\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}}) = S$ if and only if $|J \cap B_j|$ is odd whenever $b_j \in S$ and $|J \cap B_j|$ is even whenever $b_j \notin S$ for $j = 1, \dots, t$. Therefore, the number of sets $J \subseteq I$ satisfying $\operatorname{oddsupp}(\mathbf{0}_J^{\mathbf{a}}) = S$ is

$$2^{|B_1|-1} \cdots 2^{|B_t|-1} = 2^{|B_1|+\dots+|B_t|-t} = 2^{|I|-t}.$$

Moreover, the parity of $|J|$ is determined by S. Therefore, all occurrences of $\varphi(S)$ in (4) have the same sign.

By the argument above, $\Delta_I^{\mathbf{a}} f(\mathbf{0})$ can be written as a sum of finitely many terms of the form $\pm 2^{|I|-t} \varphi(S)$, where $t \leq |A| - 1$. Since $|I| \geq |A| + e - 1$, the coefficient

$2^{|I|-t}$ is a multiple of 2^e; hence $\pm 2^{|I|-t}\varphi(S) = 0$ independently of the value of $\varphi(S)$. We conclude that $\Delta_I^{\mathbf{a}} f(\mathbf{0}) = 0$, as claimed. □

As the following example shows, Theorem 12 cannot be improved and the number $|A| + e - 2$ cannot be decreased. More precisely, for every finite set A with at least two elements, for every abelian group B of exponent 2^e, and for every $n > |A| + e - 3$, there exists a function $f : A^n \to B$ that is determined by oddsupp but is not $(|A| + e - 3)$-decomposable.

Example 13. Let $A = \{0, 1, \ldots, \ell\}$, and let B be an arbitrary abelian group of exponent 2^e. Fix an element $b \in B$ of order 2^e. Let $\varphi : \mathcal{P}(A) \to B$ be defined by

$$\varphi(T) = \begin{cases} b, & \text{if } T \supseteq A \setminus \{0\}, \\ 0, & \text{otherwise,} \end{cases}$$

let $n \geq \ell + e - 1$, and let $f : A^n \to B$ be given by $f(\mathbf{x}) = \text{❄}_{\varphi}(\mathbf{x})$.

To see that f is not $(|A| + e - 3)$-decomposable, by Proposition 11, it suffices to find $I \subseteq [n]$ and $\mathbf{a} \in A^n$ such that $|I| = |A| + e - 2 = \ell + e - 1$ and $\Delta_I^{\mathbf{a}} f(\mathbf{0}) \neq 0$. To this end, let

$$\mathbf{a} := (1, 2, \ldots, \ell - 1, \underbrace{\ell, \ldots, \ell}_{e}, \underbrace{0, \ldots, 0}_{n-\ell-e+1})$$

and let $I := \{1, 2, \ldots, \ell + e - 1\}$. Consider the expansion of $\Delta_I^{\mathbf{a}} f(\mathbf{0})$ as in (4). We can verify that for all $J \subseteq I$,

$$f(\mathbf{0}_J^{\mathbf{a}}) = \begin{cases} b, & \text{if } J \supseteq \{1, \ldots, \ell - 1\} \text{ and } |J \cap \{\ell, \ldots, \ell + e - 1\}| \text{ is odd,} \\ 0, & \text{otherwise.} \end{cases}$$

From this it follows that the number of sets $J \subseteq I$ satisfying $f(\mathbf{0}_J^{\mathbf{a}}) = b$ is 2^{e-1}. Therefore, we have

$$\Delta_I^{\mathbf{a}} f(\mathbf{0}) = (-1)^{e-1} 2^{e-1} b \neq 0,$$

where the inequality holds because the order of b is 2^e.

Theorem 14. *If A is a finite set with at least two elements and B is an abelian group whose exponent is not a power of 2, then for each n there exists a function $f : A^n \to B$ determined by* oddsupp *that is not decomposable.*

Proof. If the exponent of B is not a power of 2, then B has an element b whose order is not a power of 2 (possibly infinite). Let us consider first the special case $A = \{0, 1\}$. For any $\mathbf{x} \in A^n$ let $w(\mathbf{x})$ denote the *Hamming weight* of $\mathbf{x}$, i.e. the number of 1's appearing in $\mathbf{x}$. Let $f_0 : A^n \to B$ be the function defined by

$$f_0(\mathbf{x}) = \begin{cases} b, & \text{if } w(\mathbf{x}) \text{ is even,} \\ 0, & \text{if } w(\mathbf{x}) \text{ is odd.} \end{cases}$$

Let us compute $\Delta^{\mathbf{1}}_{[n]} f_0(\mathbf{0})$ with the help of Proposition 9:

$$\Delta^{\mathbf{1}}_{[n]} f_0(\mathbf{0}) = \sum_{J \subseteq [n]} (-1)^{|[n] \setminus J|} f_0(\mathbf{0}^{\mathbf{1}}_J) = (-1)^n \sum_{J \subseteq [n]} (-1)^{|J|} f_0(\mathbf{0}^{\mathbf{1}}_J).$$

Since $w(\mathbf{0}^{\mathbf{1}}_J) = |J|$, the above sum consists of 2^{n-1} many b's and 2^{n-1} many 0's. Thus $\Delta^{\mathbf{1}}_{[n]} f_0(\mathbf{0}) = (-1)^n 2^{n-1} b \neq 0$, as $\operatorname{ord}(b)$ does not divide $(-1)^n 2^{n-1}$. Now Proposition 11 shows that f_0 is not $(n-1)$-decomposable.

Considering the general case, let 0 and 1 be two distinguished elements of A, and let $f : A^n \to B$ be any function that is determined by oddsupp such that $f|_{\{0,1\}^n} = f_0$. Then f is not decomposable, since any decomposition of f would give rise to a decomposition of $f|_{\{0,1\}^n}$. □

Corollary 15. *Let A be a finite set with at least two elements, and B be an abelian group. All functions $f : A^n \to B$ determined by* oddsupp *are decomposable if and only if the exponent of B is a power of* 2.

As the following example shows, decomposability is not guaranteed when A is infinite, no matter what the exponent of B is.

Example 16. Let A be an infinite set, B be an abelian group and let $0 \neq b \in B$. Fix $n \geq 2$, and let $S := \{s_1, \ldots, s_n\} \subseteq A \setminus \{0\}$ with $|S| = n$. Define $f : A^n \to B$ by the rule

$$f(\mathbf{x}) = \begin{cases} b, & \text{if } \{x_1, \ldots, x_n\} = S, \\ 0, & \text{otherwise.} \end{cases}$$

It is clear that f is determined by oddsupp. Computing $\Delta^{\mathbf{a}}_{[n]} f(\mathbf{0})$ for $\mathbf{a} := (s_1, \ldots, s_n)$ as in (4), we obtain $\Delta^{\mathbf{a}}_{[n]} f(\mathbf{0}) = b \neq 0$. Hence f is not decomposable by Proposition 11.

Remark 17. Theorem 6 asserts that if B is a Boolean group and $n > |A|$, then every function $f : A^n \to B$ determined by oddsupp is $(n-2)$-decomposable. Theorem 12 gives a stronger result as it provides a decomposition into a sum of functions of essential arity at most $|A| - 1$. Note that here the bound does not depend on n, and in the case $n > |A|$ we have $|A| - 1 \leq n - 2$. Theorem 14 implies that if $\exp(B)$ is not a power of 2, then even the weakest kind of decomposability (namely, $(n-1)$-decomposability) fails to hold for all functions $f : A^n \to B$ determined by oddsupp.

4. The Case of Boolean Groups

In this section, we assume that A is a finite set with a distinguished element 0 and $(B; +)$ is a Boolean group with neutral element 0. Applying Theorem 12 to this case (with $e = 1$), we see that every function $f : A^n \to B$ determined by oddsupp is $(|A| - 1)$-decomposable. Here we will provide a canonical, highly symmetric decomposition of such functions and show that it is unique.

If $n > |A|$, then Theorem 6 provides a decomposition of f into a sum of functions of essential arity at most $n-2$. Each summand $\circledast_{\varphi}(\mathbf{x}|_I)$ is a function determined by oddsupp, and if $|I| > |A|$, then we can apply Theorem 6 to decompose $\circledast_{\varphi}(\mathbf{x}|_I)$ into a sum of functions of essential arity at most $|I|-2$. Repeating this process as long as we have summands of essential arity greater than $|A|$, we end up with an $|A|$-decomposition of f. If the parities of $|A|$ and n are different, then this is already an $(|A|-1)$-decomposition. By counting how many times a given summand $\circledast_{\varphi}(\mathbf{x}|_I)$ appears, we arrive at decomposition (5) given below in Theorem 18. If the parities of $|A|$ and n are equal, then we have to further decompose the summands of essential arity $|A|$. We then get the more refined decomposition (7) given below in Theorem 19. Note that in these theorems we assume that B is finite. However, as we will see in Remark 20, the general case can be easily reduced to the case of finite groups.

Theorem 18. *Let $f\colon A^n \to B$, where B is a finite Boolean group, A is a finite set and $n - |A| = 2t+1 > 0$. Then f is determined by* oddsupp *if and only if f is of the form*

$$f(\mathbf{x}) = \sum_{i=t+1}^{\lfloor \frac{n}{2} \rfloor} \sum_{\substack{I \subseteq [n] \\ |I| = n-2i}} \binom{i-1}{t} \circledast_{\varphi}(\mathbf{x}|_I), \tag{5}$$

for some map $\varphi\colon \mathcal{P}'_n(A) \to B$. Moreover, φ is uniquely determined by f.

Proof. Let $g_\varphi\colon A^n \to B$ denote the function given by the right-hand side of (5). Let us note that since $n > |A|$ and $n - |A|$ is odd, $\mathcal{P}'_n(A)$ contains all subsets of A whose complement has an odd number of elements. Observe also that in (5) I ranges over subsets of $[n]$ of size $|A|-1, |A|-3, \ldots$; hence (5) provides an $(|A|-1)$-decomposition of f. Clearly, for such sets I we have $\operatorname{oddsupp}(\mathbf{x}|_I) \in \mathcal{P}'_n(A)$.

To prove the theorem, it suffices to show that the following three statements hold:

(1) the number of functions $f\colon A^n \to B$ that are determined by oddsupp is the same as the number of maps $\varphi\colon \mathcal{P}'_n(A) \to B$;
(2) g_φ is determined by oddsupp for every $\varphi\colon \mathcal{P}'_n(A) \to B$;
(3) if $\varphi_1 \neq \varphi_2$ then $g_{\varphi_1} \neq g_{\varphi_2}$.

The existence and uniqueness of the decomposition then follows by a simple counting argument: the functions $f\colon A^n \to B$ determined by oddsupp are in a one-to-one correspondence with the functions g_φ. (Alternatively, the existence could be proved by repeated applications of Theorem 6, as explained above.)

Statement (1) is clear: the number of functions $f\colon A^n \to B$ that are determined by oddsupp is $|B|^{|\mathcal{P}'_n(A)|}$, the same as the number of maps $\varphi\colon \mathcal{P}'_n(A) \to B$.

To see that (2) holds, observe that each g_φ is a totally symmetric function. Hence, by Fact 3, it suffices to prove that $g_\varphi(x_1, x_1, x_3, \ldots, x_n)$ does not depend on x_1. Let $\mathbf{x} = (x_1, x_1, x_3, \ldots, x_n)$ and let I be a set appearing in the summation in (5) such that $1 \in I$ and $2 \notin I$. Then $I' := I \triangle \{1, 2\} = (I \backslash \{1\}) \cup \{2\}$ ($\triangle$ denotes the symmetric difference) appears as well, since it has the same cardinality as I. As $\operatorname{oddsupp}(\mathbf{x}|_I) = \operatorname{oddsupp}(\mathbf{x}|_{I'})$, we have $\text{❄}_\varphi(\mathbf{x}|_I) = \text{❄}_\varphi(\mathbf{x}|_{I'})$, thus these two summands will cancel each other. The remaining sets I either contain both 1 and 2 or neither of them. In the first case, $\operatorname{oddsupp}(\mathbf{x}|_I) = \operatorname{oddsupp}(\mathbf{x}|_{I \backslash \{1,2\}})$, and hence $\text{❄}_\varphi(\mathbf{x}|_I)$ does not depend on x_1, whereas in the second case x_1 does not appear in $\text{❄}_\varphi(\mathbf{x}|_I)$ at all. Thus $g_\varphi(x_1, x_1, x_3, \ldots, x_n)$ does not depend on x_1, which shows that (2) holds.

To prove statement (3), suppose on the contrary that there exist maps $\varphi_1, \varphi_2 \colon \mathcal{P}'_n(A) \to B$ such that $\varphi_1 \neq \varphi_2$ but $g_{\varphi_1} = g_{\varphi_2}$. Then for $\varphi = \varphi_1 + \varphi_2$ we have $g_\varphi = g_{\varphi_1} + g_{\varphi_2} \equiv 0$ by Fact 4, that is,

$$\sum_{i=t+1}^{\lfloor \frac{n}{2} \rfloor} \sum_{\substack{I \subseteq [n] \\ |I| = n-2i}} \binom{i-1}{t} \text{❄}_\varphi(\mathbf{x}|_I) = 0 \tag{6}$$

for all $\mathbf{x} \in A^n$. Moreover, since $\varphi_1 \neq \varphi_2$, there exists an $S \in \mathcal{P}'_n(A)$ with $\varphi(S) \neq 0$. Let us choose S to be minimal with respect to this property, i.e. $\varphi(S) \neq 0$, but φ vanishes on all proper subsets of S.

Suppose first that S is nonempty, say $S = \{s_1, \ldots, s_{n-2r}\}$. Since $n - |A| = 2t+1$, we have that $t \leq r - 1$. Let us examine the left-hand side of (6) for

$$\mathbf{x} := (\underbrace{s_1, \ldots, s_1}_{2r+1}, s_2, \ldots, s_{n-2r}) \in A^n.$$

Observe that $\operatorname{oddsupp}(\mathbf{x}|_I) \subseteq S$. If $\operatorname{oddsupp}(\mathbf{x}|_I) \subset S$, then $\text{❄}_\varphi(\mathbf{x}|_I) = 0$ by the minimality of S. If $\operatorname{oddsupp}(\mathbf{x}|_I) = S$, then $\text{❄}_\varphi(\mathbf{x}|_I) = \varphi(S) \neq 0$. The latter is the case if and only if I is a proper superset of $\{2r+2, \ldots, n\}$ of cardinality $n - 2i$ for some i. The number of sets $I \subseteq [n]$ with $|I| = n - 2i$ and $I \supset \{2r+2, \ldots, n\}$ is $\binom{2r+1}{2i}$. Hence the left-hand side of (6) equals

$$\sum_{i=t+1}^{r} \binom{2r+1}{2i} \binom{i-1}{t} \varphi(S).$$

Since $r \geq t+1$, the coefficient $\sum_{i=t+1}^{r} \binom{2r+1}{2i} \binom{i-1}{t}$ of $\varphi(S)$ is odd according to Theorem 7 (for $m = 2r+1$). Therefore, taking into account that B is a Boolean group, we can conclude that the left-hand side of (6) is $\varphi(S) \neq 0$, which is a contradiction.

Suppose then that S is empty. Choose $\mathbf{x} := (s_1, \ldots, s_1)$ for an arbitrary $s_1 \in A$. Since $S \in \mathcal{P}'_n(A)$, n is even and hence each I occurring in (6) is of even cardinality. Whenever $|I|$ is even, $\operatorname{oddsupp}(\mathbf{x}|_I) = \emptyset = S$ and $\text{❄}_\varphi(\mathbf{x}|_I) = \varphi(S)$. Therefore, the left-hand side of (6) becomes

$$\sum_{i=t+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} \binom{i-1}{t} \varphi(S),$$

which equals $\varphi(S)$ by Theorem 7 (for $m = n$). This yields the desired contradiction, and the proof of (3) is now complete. □

Theorem 19. *Let $f : A^n \to B$, where B is a finite Boolean group, A is a finite set and $n - |A| = 2t > 0$. Then f is determined by* oddsupp *if and only if f is of the form*

$$f(\mathbf{x}) = \sum_{i=t+1}^{\lfloor \frac{n}{2} \rfloor} \sum_{\substack{I \subseteq [n] \\ |I| = n-2i}} \binom{i-1}{t} \text{❉}_\varphi(\mathbf{x}|_I) + \sum_{k=t+1}^{\lfloor \frac{n+1}{2} \rfloor} \sum_{\substack{K \subseteq [n] \\ |K| = n-2k+1}} \binom{2k-1}{2t} \text{❉}_\varphi(\mathbf{x}|_K) \qquad (7)$$

for some map $\varphi : \mathcal{P}(A) \to B$ satisfying $\varphi(S) = \varphi(S \triangle \{0\})$ for every $S \in \mathcal{P}(A)$. Moreover, φ is uniquely determined by f.

Proof. Let us note first that since $n > |A|$ and $n - |A|$ is even, $\mathcal{P}'_n(A)$ contains all subsets of A whose complement has an even number of elements. The number of maps $\varphi : \mathcal{P}(A) \to B$ satisfying $\varphi(S) = \varphi(S \triangle \{0\})$ for every $S \in \mathcal{P}(A)$ is $|B|^{|\mathcal{P}'_n(A)|}$, since $\varphi|_{\mathcal{P}'_n(A)}$ can be chosen arbitrarily, and this uniquely determines $\varphi|_{\mathcal{P}(A) \setminus \mathcal{P}'_n(A)}$. The number of functions $f : A^n \to B$ that are determined by oddsupp is $|B|^{|\mathcal{P}'_n(A)|}$ as well, and we can use the same counting argument as in the proof of Theorem 18. The fact that the right-hand side of (7) is determined by oddsupp can be proven in a similar way, and for the uniqueness it suffices to prove that if

$$\sum_{i=t+1}^{\lfloor \frac{n}{2} \rfloor} \sum_{\substack{I \subseteq [n] \\ |I| = n-2i}} \binom{i-1}{t} \text{❉}_\varphi(\mathbf{x}|_I) + \sum_{k=t+1}^{\lfloor \frac{n+1}{2} \rfloor} \sum_{\substack{K \subseteq [n] \\ |K| = n-2k+1}} \binom{2k-1}{2t} \text{❉}_\varphi(\mathbf{x}|_K) = 0 \qquad (8)$$

for all $\mathbf{x} \in A^n$, then $\varphi|_{\mathcal{P}'_n(A)}$ is identically 0.

Suppose, for the sake of contradiction, that there exists an $S \in \mathcal{P}'_n(A)$ such that $\varphi(S) \neq 0$, and let $n - 2r$ be the cardinality of the smallest such S. If $r = t$, then $\varphi(A) = \varphi(A \setminus \{0\}) \neq 0$, and φ is zero on all other subsets of A. Let $A = \{0, a_1, \ldots, a_\ell\}$, where $\ell = n - 2t - 1$, and let $\mathbf{x} = (0, \ldots, 0, a_1, \ldots, a_\ell) \in A^n$, where the number of 0's is $2t + 1$. Then, for any set I appearing in the first summation of (8), we have $A \setminus \{0\} \nsubseteq \operatorname{oddsupp}(\mathbf{x}|_I)$; hence $\text{❉}_\varphi(\mathbf{x}|_I) = 0$. Similarly, $\text{❉}_\varphi(\mathbf{x}|_K) = 0$ for all sets K appearing in (8), except for $K = \{2t+2, \ldots, n\}$, where $\text{❉}_\varphi(\mathbf{x}|_K) = \varphi(A \setminus \{0\})$. Thus the left-hand side of (8) equals $\varphi(A \setminus \{0\}) \neq 0$, contrary to our assumption.

Let us now consider the case $r > t$, and let us suppose first that there exists a set $S \in \mathcal{P}'_n(A)$ of cardinality $n - 2r$ such that $\varphi(S) \neq 0$ and $0 \in S$, say $S = \{s_1, \ldots, s_{n-2r}\}$ with $s_1 = 0$. Let T be a subset of S. By the minimality of $|S|$, if $T \in \mathcal{P}'_n(A)$ then we have $\varphi(T) \neq 0$ if and only if $T = S$. Similarly, if $T \notin \mathcal{P}'_n(A)$ then we have $\varphi(T) \neq 0$ if and only if $T = S \setminus \{0\}$. (Indeed, if $T \neq S \setminus \{0\}$, then $T \triangle \{0\} \in \mathcal{P}'_n(A)$ is a proper subset of S. Hence $\varphi(T) = \varphi(T \triangle \{0\}) = 0$.)

Let us examine the left-hand side of (8) for

$$\mathbf{x} := (\underbrace{s_1, \ldots, s_1}_{2r+1}, s_2, \ldots, s_{n-2r}) \in A^n.$$

The same argument as in the proof of Theorem 18 shows that the first sum of (8) equals

$$\sum_{i=t+1}^{r} \binom{2r+1}{2i} \binom{i-1}{t} \varphi(S),$$

which is $\varphi(S)$ by Theorem 7, since $r \geq t+1$. If K is a set of size $n-2k+1$ appearing in the second sum of (8), then $\text{❉}_{\varphi}(\mathbf{x}|_K) = \varphi(S \backslash \{0\}) = \varphi(S)$ if $K \supseteq \{2r+2, \ldots, n\}$, and $\text{❉}_{\varphi}(\mathbf{x}|_K) = 0$ otherwise. The number of such sets K is $\binom{2r+1}{2k-1}$, thus the second sum on the left-hand side of (8) equals

$$\sum_{k=t+1}^{r+1} \binom{2r+1}{2k-1} \binom{2k-1}{2t} \varphi(S).$$

By Theorem 8, the coefficient of $\varphi(S)$ here is $\binom{2r+1}{2t} 2^{2r-2t}$, which is even since $r > t$. Thus the left-hand side of (8) reduces to $\varphi(S)$, contradicting our assumption.

In the remaining case we have $r > t$ and for all $S \in \mathcal{P}'_n(A)$ of cardinality $n-2r$ we have $0 \notin S$ whenever $\varphi(S) \neq 0$. Let $S = \{s_1, \ldots, s_{n-2r}\}$ be such a set, and let $T \subseteq S$. If $T \in \mathcal{P}'_n(A)$, then we have $\varphi(T) \neq 0$ if and only if $T = S$ by the minimality of $|S|$. Similarly, if $T \notin \mathcal{P}'_n(A)$, then we have $\varphi(T) = 0$. (Indeed, if $T \notin \mathcal{P}'_n(A)$ then $T \cup \{0\} = T \triangle \{0\} \in \mathcal{P}'_n(A)$ and $|T \triangle \{0\}| \leq |S|$. On the other hand, if $\varphi(T \triangle \{0\}) = \varphi(T) \neq 0$ then $|T \triangle \{0\}| \geq |S|$ by the minimality of $|S|$. Thus we have $|T \triangle \{0\}| = |S| = n - 2r$, hence $T \triangle \{0\}$ is a set in $\mathcal{P}'_n(A)$ with cardinality $n - 2r$ such that $\varphi(T \triangle \{0\}) \neq 0$ and $0 \in T \triangle \{0\}$, and then replacing S by $T \triangle \{0\}$ we come back to the previous case.)

Let us choose $\mathbf{x} := (s_1, \ldots, s_1, s_2, \ldots, s_{n-2r}) \in A^n$ as before, and examine the summands in (8). For each K appearing in the second sum, $\operatorname{oddsupp}(\mathbf{x}|_K) \subseteq S$ and $\operatorname{oddsupp}(\mathbf{x}|_K) \notin \mathcal{P}'_n(A)$, thus $\text{❉}_{\varphi}(\mathbf{x}|_K) = 0$. For each I appearing in the first sum, we have $\text{❉}_{\varphi}(\mathbf{x}|_I) = \varphi(S) \neq 0$ if I is a proper superset of $\{2r+2, \ldots, n\}$; otherwise $\operatorname{oddsupp}(\mathbf{x}|_I) \subset S$, and so $\text{❉}_{\varphi}(\mathbf{x}|_I) = 0$. Therefore, using Theorem 7 as before, we can conclude that the left-hand side of (8) equals $\varphi(S)$, and this contradiction finishes the proof of the theorem. □

Remark 20. Theorems 18 and 19 still hold for infinite Boolean groups B. To see this, let $f : A^n \to B$ be a function that is determined by oddsupp, where A is a finite set and B is a possibly infinite Boolean group, and let $R \subseteq B$ be the range of f. Since R is finite, the subgroup $[R] \leq B$ generated by R is also finite. (The free Boolean group on r generators has cardinality 2^r.) Applying Theorems 18 and 19 to $f : A^n \to [R]$, we obtain the desired decomposition of f. To show the uniqueness, suppose that $\varphi_1, \varphi_2 : \mathcal{P}(A) \to B$ both yield the function f. Then we can replace B by its subgroup generated by the union of the ranges of φ_1 and φ_2, and apply the uniqueness parts of Theorems 18 and 19.

5. Illustration: Operations Over the Three-Element Set

We saw in Theorem 1 that a Boolean function of essential arity at least 4 has arity gap 2 if and only if it is a sum of essentially at most unary functions. Alternatively, this fact follows from the results of Sec. 4 together with Willard's Theorem 5. More generally, Theorems 18 and 19 can be applied to describe polynomial functions over finite fields of characteristic 2 with arity gap 2. In this section we show how Theorems 18 and 19 can be used to describe functions $f : \mathbb{Z}_3^n \to \mathbb{Z}_3$ of arity at least 4 with gap $f = 2$. Since $\mathbb{Z}_3$ is not a Boolean group, we cannot apply these theorems directly. First we need to embed $\mathbb{Z}_3$ into a Boolean group. To this extent, let $A := \mathbb{Z}_3 = \{0, 1, 2\}$ with the usual field operations $+$ and $\cdot$, and $B := \mathcal{P}(A)$ with the symmetric difference operation $\oplus$. We use the notation $\oplus$ instead of the more common $\triangle$ in order to emphasize that this is a Boolean group operation on B (which was denoted by $+$ before). The neutral element of $(A; +)$ is 0, and the neutral element of $(B; \oplus)$ is the empty set $\emptyset$. We identify the elements of A with the corresponding one-element sets, i.e. we simply write a instead of $\{a\}$ for $a \in A$. In this way, A becomes a subset (but, of course, not a subgroup) of B.

Let $f : A^n \to B$, where $n \geq 4$ is even. Then we have $n = 2t + 4$ in Theorem 18, and the summation in (5) runs over the subsets of $[n]$ of size 2 (for $i = t + 1$) and of size 0 (for $i = t + 2$). The corresponding coefficients $\binom{i-1}{t}$ are $\binom{t}{t} = 1$ and $\binom{t+1}{t} = t + 1$, respectively. Thus $\binom{i-1}{t} ❈_{\varphi}(\mathbf{x}|_I) = ❈_{\varphi}(\mathbf{x}|_I)$ whenever $|I| = 2$ or $I = \emptyset$ and t is even (i.e. n is divisible by 4); on the other hand, if $I = \emptyset$ and t is odd, then $\binom{i-1}{t} ❈_{\varphi}(\mathbf{x}|_I) = 0$. Therefore, (5) takes one of the following two forms, depending on the residue of n modulo 4 (the summation indices i and j always run from 1 to n, unless otherwise indicated):

$$f(\mathbf{x}) = \bigoplus_{i<j} \varphi(\operatorname{oddsupp}(x_i, x_j)) \oplus \varphi(\emptyset) \quad \text{if } n \equiv 0 \pmod 4,$$

$$f(\mathbf{x}) = \bigoplus_{i<j} \varphi(\operatorname{oddsupp}(x_i, x_j)) \qquad\qquad \text{if } n \equiv 2 \pmod 4.$$

(Note that $\varphi(\operatorname{oddsupp}(x_i, x_j)) = \varphi(\{x_i, x_j\})$ if $x_i \neq x_j$, and $\varphi(\operatorname{oddsupp}(x_i, x_j)) = \varphi(\emptyset)$ if $x_i = x_j$.)

If n is odd, then we can apply Theorem 19. In this case we have $n = 2t + 3$, and in the first summation of (7) I is a one-element set ($i = t + 1$) and the corresponding coefficient is $\binom{i-1}{t} = \binom{t}{t} = 1$. In the second summation, K is either a two-element set ($k = t + 1$) or the empty set ($k = t + 2$). The corresponding coefficients $\binom{2k-1}{2t}$ are $\binom{2t+1}{2t} = 2t + 1$ and $\binom{2t+3}{2t} = \frac{(2t+3)(2t+1)(t+1)}{3} \equiv t + 1 \pmod 2$. Thus, (7) takes one of the following two forms:

$$f(\mathbf{x}) = \bigoplus_{i<j} \varphi(\operatorname{oddsupp}(x_i, x_j)) \oplus \bigoplus_{i} \varphi(\{x_i\}) \qquad \text{if } n \equiv 1 \pmod{4},$$

$$f(\mathbf{x}) = \bigoplus_{i<j} \varphi(\operatorname{oddsupp}(x_i, x_j)) \oplus \bigoplus_{i} \varphi(\{x_i\}) \oplus \varphi(\emptyset) \quad \text{if } n \equiv 3 \pmod{4}.$$

(Note that $\varphi(\operatorname{oddsupp}(x_i)) = \varphi(\{x_i\})$.)

The above formulas are valid for any function $f\colon A^n \to B$, but we are interested only in functions whose range lies within A, i.e. whose values are one-element sets in B. In this case, we can give more concrete expressions for the above decompositions.

Theorem 21. *Let $f\colon \mathbb{Z}_3^n \to \mathbb{Z}_3$ be a function of arity at least 4. Then* gap $f = 2$ *if and only if there exists a unary polynomial $p = ax^2 + bx + c \in \mathbb{Z}_3[x]$ and a constant $d \in \mathbb{Z}_3$, which are uniquely determined by f, such that*

$$f(\mathbf{x}) = \bigoplus_{i<j} ((x_i - x_j)^2 p(x_i + x_j) + d) \oplus d \qquad \text{if } n \equiv 0 \pmod{4},$$

$$f(\mathbf{x}) = \bigoplus_{i<j} ((x_i - x_j)^2 p(x_i + x_j) + d) \oplus \bigoplus_{i} (p(x_i) + d) \qquad \text{if } n \equiv 1 \pmod{4},$$

$$f(\mathbf{x}) = \bigoplus_{i<j} ((x_i - x_j)^2 p(x_i + x_j) + d) \qquad \text{if } n \equiv 2 \pmod{4},$$

$$f(\mathbf{x}) = \bigoplus_{i<j} ((x_i - x_j)^2 p(x_i + x_j) + d) \oplus \bigoplus_{i} (p(x_i) + d) \oplus d \quad \text{if } n \equiv 3 \pmod{4}.$$

Otherwise we have gap $f = 1$.

Proof. Let $A := \mathbb{Z}_3$ and $B := \mathcal{P}(\mathbb{Z}_3)$ as explained above. We work out the details only for the case $n \equiv 3 \pmod{4}$, the other cases are similar. First let us consider the function

$$f_1(\mathbf{x}) = \bigoplus_{i} (p(x_i) + d).$$

It is clear that this function is totally symmetric, and $f_1(x_1, x_1, x_3, \dots, x_n)$ does not depend on x_1, since

$$\begin{aligned} f_1(x_1, x_1, x_3, \dots, x_n) &= (p(x_1) + d) \oplus (p(x_1) + d) \oplus \bigoplus_{i=3}^{n} (p(x_i) + d) \\ &= \bigoplus_{i=3}^{n} (p(x_i) + d). \end{aligned}$$

Therefore, f_1 is determined by oddsupp by Fact 3. Hence, it holds that $f_1(\mathbf{x}) = \varphi_1(\operatorname{oddsupp}(\mathbf{x}))$ for some map $\varphi_1\colon \mathcal{P}'_n(A) \to B$. Observe that $\mathcal{P}'_n(A) =$

$\{\{0\},\{1\},\{2\},\{0,1,2\}\}$. Thus, in order to determine φ_1, it suffices to compute the following four values of f_1:

$$\varphi_1(\{0\}) = f_1(0,\dots,0) = \bigoplus_{i=1}^{n}(p(0)+d) = p(0)+d = c+d,$$

$$\varphi_1(\{1\}) = f_1(1,\dots,1) = \bigoplus_{i=1}^{n}(p(1)+d) = p(1)+d = a+b+c+d,$$

$$\varphi_1(\{2\}) = f_1(2,\dots,2) = \bigoplus_{i=1}^{n}(p(2)+d) = p(2)+d = a+2b+c+d,$$

$$\begin{aligned}\varphi_1(\{0,1,2\}) &= f_1(0,\dots,0,1,2) = \bigoplus_{i=1}^{n-2}(p(0)+d) \oplus (p(1)+d) \oplus (p(2)+d)\\ &= (p(0)+d) \oplus (p(1)+d) \oplus (p(2)+d)\\ &= (c+d) \oplus (a+b+c+d) \oplus (a+2b+c+d).\end{aligned}$$

We now analyze the function

$$f_2(\mathbf{x}) = \bigoplus_{i<j}((x_i-x_j)^2 p(x_i+x_j)+d)$$

in a similar manner. Examining $f_2(x_1,x_1,x_3,\dots,x_n)$ we can see that the summands corresponding to $i=1, j\geq 3$ cancel the summands corresponding to $i=2, j\geq 3$, while the summand corresponding to $i=1$, $j=2$ is $(x_1-x_1)^2p(x_1+x_1)+d=d$. Hence

$$f_2(x_1,x_1,x_3,\dots,x_n) = d \oplus \bigoplus_{3\leq i<j}((x_i-x_j)^2p(x_i+x_j)+d),$$

which clearly does not depend on x_1. Since f_2 is totally symmetric, we can conclude that f_2 is determined by oddsupp. Therefore, there is a map $\varphi_2 : \mathcal{P}'_n(A) \to B$ such that $f_2(\mathbf{x}) = \varphi_2(\mathrm{oddsupp}(\mathbf{x}))$. For any $a \in A$ we have

$$\varphi_2(\{a\}) = f_2(a,\dots,a) = \bigoplus_{i<j}((a-a)^2p(a+a)+d) = \binom{n}{2}d = d,$$

where the last equality holds, because $\binom{n}{2}$ is an odd number by the assumption that $n \equiv 3 \pmod 4$. To find $\varphi_2(\{0,1,2\})$, we can proceed as follows:

$$\begin{aligned}\varphi_2(\{0,1,2\}) &= f_2(0,\dots,0,1,2)\\ &= \bigoplus_{i<j\leq n-2}((0-0)^2p(0+0)+d) \oplus \bigoplus_{i=1}^{n-2}((0-1)^2p(0+1)+d)\\ &\qquad \oplus \bigoplus_{i=1}^{n-2}((0-2)^2p(0+2)+d) \oplus ((1-2)^2p(1+2)+d)\\ &= (a+b+c+d) \oplus (a+2b+c+d) \oplus (c+d).\end{aligned}$$

(Here we made use of the fact that $\binom{n-2}{2}$ is even and $n-2$ is odd.)

The expression given for f in the theorem is $f_1(\mathbf{x}) \oplus f_2(\mathbf{x}) \oplus d$, and from the above calculations it follows that this function is determined by oddsupp, namely, $f_1(\mathbf{x}) \oplus f_2(\mathbf{x}) \oplus d = \varphi(\text{oddsupp}(\mathbf{x}))$, where

$$\begin{aligned}
\varphi(\{0\}) &= \varphi_1(\{0\}) \oplus \varphi_2(\{0\}) \oplus d = (c+d) \oplus d \oplus d = c+d, \\
\varphi(\{1\}) &= \varphi_1(\{1\}) \oplus \varphi_2(\{1\}) \oplus d = (a+b+c+d) \oplus d \oplus d = a+b+c+d, \\
\varphi(\{2\}) &= \varphi_1(\{2\}) \oplus \varphi_2(\{2\}) \oplus d = (a+2b+c+d) \oplus d \oplus d = a+2b+c+d, \\
\varphi(\{0,1,2\}) &= \varphi_1(\{0,1,2\}) \oplus \varphi_2(\{0,1,2\}) \oplus d \\
&= (c+d) \oplus (a+b+c+d) \oplus (a+2b+c+d) \\
&\qquad \oplus (a+b+c+d) \oplus (a+2b+c+d) \oplus (c+d) \oplus d = d.
\end{aligned}$$

Observe that the range of φ is a subset of A. Hence $f_1(\mathbf{x}) \oplus f_2(\mathbf{x}) \oplus d$ is a function from A^n to A.

Let us consider the linear transformation

$$L : \mathbb{Z}_3^4 \to \mathbb{Z}_3^4, \quad (a,b,c,d) \mapsto (c+d, a+b+c+d, a+2b+c+d, d).$$

The determinant of L is 1; hence L is a bijection. This means that the maps $\varphi : \mathcal{P}_n'(A) \to B$ that are of the above form are in a one-to-one correspondence with the 4-tuples over A, i.e. there are $3^4 = 81$ such maps. The number of functions $f : A^n \to A$ that are determined by oddsupp is also 81. Hence we can conclude by a simple counting argument that for any such f there exists a unique tuple $(a,b,c,d) \in A^4$ such that $f(\mathbf{x}) = f_1(\mathbf{x}) \oplus f_2(\mathbf{x}) \oplus d$. □

Let us observe that when computing the value of a function of the form given in Theorem 21, we do not have to "leave" $\mathbb{Z}_3$: using the fact that $\oplus$ is commutative and associative and it satisfies $u \oplus u \oplus v = v$ for any $u, v \in \mathbb{Z}_3$, we can always perform the calculations in such a way that we work only with singleton elements of B. It is not even necessary to know that B is the power set of $\mathbb{Z}_3$, it could be any Boolean group that contains $\mathbb{Z}_3$ as a subset. To illustrate this point, let us compute $f(0,0,1,2)$ for the function

$$f(x_1,x_2,x_3,x_4) = \bigoplus_{i<j} ((x_i - x_j)^2 p(x_i + x_j) + d) \oplus d$$

that corresponds to the case $n = 4$ with $a = 1$, $b = c = d = 2$ in Theorem 21:

$$f(0,0,1,2) = 2 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 2 = (0 \oplus 0) \oplus (1 \oplus 1) \oplus (2 \oplus 2) \oplus 1 = 1.$$

Acknowledgments

The authors would like to thank the editor and the anonymous referee for their insightful comments and suggestions. The third named author acknowledges that this project was supported by the TÁMOP-4.2.1/B-09/1/KONV-2010-0005 program of National Development Agency of Hungary, 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).

References

[1] V. I. Arnol'd, On functions of three variables, *Dokl. Akad. Nauk SSSR* **114** (1957) 679–681 (in Russian); *Amer. Math. Soc. Transl.* (*2*) **28** (1963) 51–54 (in English).

[2] V. I. Arnol'd, On the representation of continuous functions of three variables by superpositions of continuous functions of two variables, *Mat. Sb.* (*N.S.*) **48**(90) (1959) 3–74 (in Russian); *Amer. Math. Soc. Transl.* (*2*) **28** (1963) 61–147 (in English).

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

[4] M. Bouaziz, M. Couceiro and M. Pouzet, Join-irreducible Boolean functions, *Order* **27** (2010) 261–282.

[5] K. N. Čimev, On some properties of functions, in *Finite Algebra and Multiple-Valued Logic, Abstracts of Lectures of the Colloquium on Finite Algebra and Multiple-Valued Logic*, eds. B. Csákány and I. Rosenberg (North-Holland, 1981), pp. 38–40.

[6] K. N. Čimev, *Separable Sets of Arguments of Functions,* Studies 180/1986 (Computer and Automation Institute, Hungarian Academy of Sciences, Budapest, 1986).

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

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

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

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

[11] M. Couceiro and M. Pouzet, On a quasi-ordering on Boolean functions, *Theoret. Comput. Sci.* **396** (2008) 71–87.

[12] R. O. Davies, Two theorems on essential variables, *J. London Math. Soc.* **41** (1966) 333–335.

[13] K. Denecke and J. Koppitz, Essential variables in hypersubstitutions, *Algebra Universalis* **46** (2001) 443–454.

[14] A. Ehrenfeucht, J. Kahn, R. Maddux and J. Mycielski, On the dependence of functions on their variables, *J. Combin. Theory Ser. A* **33** (1982) 106–108.

[15] O. Ekin, S. Foldes, P. L. Hammer and L. Hellerstein, Equational characterizations of Boolean function classes, *Discrete Math.* **211** (2000) 27–51.

[16] A. Feigelson and L. Hellerstein, The forbidden projections of unate functions, *Discrete Appl. Math.* **77** (1997) 221–236.

[17] K. Gilezan, Taylor formula of Boolean and pseudo-Boolean function, *Zb. Rad. Prirod.-Mat. Fak. Ser. Mat.* **25**(2) (1995) 141–149.

[18] G. Grätzer and A. Kisielewicz, A survey of some open problems on p_n-sequences and free spectra of algebras and varieties, in *Universal Algebra and Quasigroup Theory*, eds. A. Romanowska and J. D. H. Smith (Heldermann, Berlin, 1992), pp. 57–88.

[19] L. Hellerstein, On generalized constraints and certificates, *Discrete Math.* **226** (2001) 211–232.

[20] A. N. Kolmogorov, On the representation of continuous functions of several variables by superpositions of continuous functions of a smaller number of variables, *Dokl.*

Akad. Nauk SSSR **108** (1956) 179–182 (in Russian); *Amer. Math. Soc. Transl. (2)* **17** (1961) 369–373 (in English).

[21] A. N. Kolmogorov, On the representation of continuous functions of many variables by superposition of continuous functions of one variable and addition, *Dokl. Akad. Nauk SSSR* **114** (1957) 953–956 (in Russian); *Amer. Math. Soc. Transl. (2)* **28** (1963) 55–59 (in English).

[22] E. Lehtonen, Descending chains and antichains of the unary, linear, and monotone subfunction relations, *Order* **23** (2006) 129–142.

[23] E. Lehtonen and Á. Szendrei, Clones with finitely many relative $\mathcal{R}$-classes, *Algebra Universalis* **65** (2011) 109–159.

[24] N. Pippenger, Galois theory for minors of finite functions, *Discrete Math.* **254** (2002) 405–419.

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

[26] M. Shattuck and T. Waldhauser, Proofs of some binomial identities using the method of last squares, *Fibonacci Quart.* **48**(4) (2010) 290–297.

[27] N. A. Solovjev, On the question of the essential dependence of functions of the algebra of logic, *Problemy Kibernetiki* **9** (1963) 333–335 (in Russian).

[28] C. Wang, Boolean minors, *Discrete Math.* **141** (1991) 237–258.

[29] W. Wernick, An enumeration of logical functions, *Bull. Amer. Math. Soc.* **45** (1939) 885–887.

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

[31] S. V. Yablonski, Functional constructions in a k-valued logic, *Tr. Mat. Inst. Steklova* **51** (1958) 5–142 (in Russian).

[32] I. E. Zverovich, Characterizations of closed classes of Boolean functions in terms of forbidden subfunctions and Post classes, *Discrete Appl. Math.* **149** (2005) 200–218.