DECOMPOSITIONS OF FUNCTIONS BASED ON ARITY GAP

MIGUEL COUCEIRO, ERKKO LEHTONEN, AND TAMÁS WALDHAUSER

ABSTRACT. We study the arity gap of functions of several variables defined on an arbitrary set A and valued in another set B. The arity gap of such a function is the minimum decrease in the number of essential variables when variables are identified. We establish a complete classification of functions according to their arity gap, extending existing results for finite functions. This classification is refined when the codomain B has a group structure, by providing unique decompositions into sums of functions of a prescribed form. As an application of the unique decompositions, in the case of finite sets we count, for each n and p, the number of n-ary functions that depend on all of their variables and have arity gap p.

1. INTRODUCTION

Essential variables of functions have been investigated in multiple-valued logic and computer science, especially, concerning the distribution of values of functions whose variables are all essential (see, e.g., [9, 16, 22]), the process of substituting constants for variables (see, e.g., [2, 3, 14, 16, 18]), and the process of substituting variables for variables (see, e.g., [5, 10, 16, 21]).

The latter line of study goes back to the 1963 paper by Salomaa [16] who considered the following problem: How does identification of variables affect the number of essential variables of a given function? The minimum decrease in the number of essential variables of a function $f: A^n \to B$ $(n \ge 2)$ which depends on all of its variables is called the arity gap of f. Salomaa [16] showed that the arity gap of any Boolean function is at most 2. This result was extended to functions defined on arbitrary finite domains by Willard [21], who showed that the same upper bound holds for the arity gap of any function $f: A^n \to B$, provided that n > |A|. In fact, he showed that if the arity gap of such a function f is 2, then f is totally symmetric. Salomaa's [16] result on the upper bound for the arity gap of Boolean functions was strengthened in [5], where Boolean functions were completely classified according to their arity gap. In [6], by making use of tools provided by Berman and Kisielewicz [1] and Willard [21], a similar explicit classification was obtained for all pseudo-Boolean functions, i.e., functions $f: \{0,1\}^n \to B$, where B is an arbitrary set. This line of study culminated in a complete classification of functions $f: A^n \to B$ with finite domains according to their arity gap in terms of so-called quasi-arity; see Theorem 3.6, first presented in [6].

Although Theorem 3.6 was originally stated in the setting of functions $f: A^n \to B$ with finite domains, it actually holds for functions with arbitrary, possibly infinite domains (see Remark 3.7 in Section 3). Alas, this classification is not quite explicit. However, as we will see in Section 4, provided that the codomain *B* has a group structure, this classification can be refined to a unique decomposition of functions as a sum of functions of a prescribed type (see Theorem 4.1). This result can be further strengthened by assuming that *B* is a Boolean group (see Section 5). As an application of the unique decomposition theorem, in Section 6, assuming that sets *A* and *B* are finite, we will count for each *n* and *p* the number of functions $f: A^n \to B$ that depend on all of their variables and have arity gap *p*.

The special case of operations $f: A^n \to A$ on finite sets A was considered earlier in the paper by Shtrakov and Koppitz [17], in which a decomposition scheme based

²⁰¹⁰ Mathematics Subject Classification. 08A40.

Key words and phrases. arity gap, variable identification minor, Boolean group.

on the arity gap was presented and the problem of counting the number of operations with a given arity gap was posed and upper bounds for these numbers were found. Our current work thus generalizes and strengthens the results obtained in [17].

2. Essential arity and quasi-arity

Throughout this paper, let A and B be arbitrary sets with at least two elements. A B-valued function (of several variables) on A is a mapping $f: A^n \to B$ for some positive integer n, called the *arity* of f. A-valued functions on A are called *operations* on A. Operations on $\{0,1\}$ are called *Boolean functions*. For an arbitrary B, we refer to B-valued functions on $\{0, 1\}$ as pseudo-Boolean functions.

A partial function from X to Y is a map $f: S \to Y$ for some $S \subseteq X$. In the case that S = X, we speak of total functions. Thus, an n-ary partial function from A to B is a map $f: S \to B$ for some $S \subseteq A^n$.

Let $f: S \to B$ be a partial function with $S \subseteq A^n$. We say that the *i*-th variable x_i is essential in f, or f depends on x_i , if there is a pair

$$((a_1,\ldots,a_{i-1},a_i,a_{i+1},\ldots,a_n),(a_1,\ldots,a_{i-1},b,a_{i+1},\ldots,a_n)) \in S^2,$$

called a witness of essentiality of x_i in f, such that

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

The number of essential variables in f is called the *essential arity* of f, and it is denoted by ess f. If ess f = m, we say that f is essentially m-ary. Note that the only essentially nullary total functions are the constant functions, but this does not hold in general for partial functions.

For $n \geq 2$, define

$$A_{=}^{n} := \{(a_{1}, \dots, a_{n}) \in A^{n} : a_{i} = a_{j} \text{ for some } i \neq j\}.$$

We also define $A^1_{\pm} := A$. Note that if A has less than n elements, then $A^n_{\pm} = A^n$.

Lemma 2.1. Let $f: A^n \to B$, $n \ge 3$, $\operatorname{ess} f < n$. Then for each essential variable x_i , there exists a pair of points $(\mathbf{a}, \mathbf{b}) \in (A^n_{\pm})^2$ that is a witness of essentiality of x_i in f.

Proof. Since ess f < n, f has an inessential variable. Assume, without loss of generality, that x_n is inessential in f. Assume that x_i is an essential variable in f, and let

 $((a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n), (a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n)) \in (A^n)^2$ be a witness of essentiality of x_i in f. Let $j \in \{1, \ldots, n-1\} \setminus \{i\}$. We have that

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}, a_j)$$

= $f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}, a_n)$
 $\neq f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_{n-1}, a_n)$
= $f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_{n-1}, a_j),$

where the two equalities hold by the assumption that x_n is inessential in f, and the inequality holds by our choice of a witness of essentiality of x_i in f. Thus,

$$((a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}, a_j), (a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_{n-1}, a_j)) \in (A_{=}^n)^2$$

a witness of essentiality of x_i in f .

is a witness of essentiality of x_i in f.

We say that a function $f: A^n \to B$ is obtained from $g: A^m \to B$ by simple variable substitution, or f is a simple minor of g, if there is a mapping $\sigma: \{1, \ldots, m\} \rightarrow$ $\{1,\ldots,n\}$ such that

$$f(x_1,\ldots,x_n)=g(x_{\sigma(1)},\ldots,x_{\sigma(m)}).$$

If σ is not injective, then we speak of *identification of variables*. If σ is not surjective, then we speak of addition of inessential variables. If σ is a bijection, then we speak of permutation of variables.

The simple minor relation constitutes a quasi-order \leq on the set of all *B*-valued functions of several variables on *A* which is given by the following rule: $f \leq g$ if and only if *f* is obtained from *g* by simple variable substitution. If $f \leq g$ and $g \leq f$, we say that *f* and *g* are *equivalent*, denoted $f \equiv g$. If $f \leq g$ but $g \not\leq f$, we denote f < g. It can be easily observed that if $f \leq g$ then $\operatorname{ess} f \leq \operatorname{ess} g$, with equality if and only if $f \equiv g$. For background, extensions and variants of the simple minor relation, see, e.g., [4, 8, 11, 12, 13, 15, 19, 23].

Consider $f: A^n \to B$. Any function $g: A^n \to B$ satisfying $f|_{A_{\pm}^n} = g|_{A_{\pm}^n}$ is called a *support* of f. The *quasi-arity* of f, denoted qa f, is defined as the minimum of the essential arities of the supports of f, i.e., qa $f = \min_g \operatorname{ess} g$, where g ranges over the set of all supports of f. If qa f = m, we say that f is *quasi-m-ary*.

The following two lemmas were proved in [6].

Lemma 2.2. For every function $f: A^n \to B$, $n \neq 2$, we have $\operatorname{qa} f = \operatorname{ess} f|_{A_n^n}$.

Lemma 2.3. If a quasi-m-ary function $f: A^n \to B$ has an inessential variable, then f is essentially m-ary.

Remark 2.4. If A is a finite set and n > |A|, then $A_{=}^{n} = A^{n}$, and hence for every $f: A^{n} \to B$ we have qa $f = \operatorname{ess} f$.

The following result will be used later on.

Proposition 2.5. Let $f: A^n \to B$, $n \ge 3$. If $\operatorname{ess} f = n > m = \operatorname{qa} f$, then f has a unique essentially m-ary support.

Proof. Let $g: A^n \to B$ be an essentially *m*-ary support of f, say, with x_1, \ldots, x_m essential. By Lemma 2.1, g and $f|_{A^n_{\pm}}$ have the same essential variables. Now if $h: A^n \to B$ is an essentially *m*-ary support of f, then x_1, \ldots, x_m are exactly the essential variables of h, and

$$h(x_1, \dots, x_n) = h(x_1, \dots, x_m, x_m, \dots, x_m) = f(x_1, \dots, x_m, x_m, \dots, x_m)$$

= $g(x_1, \dots, x_m, x_m, \dots, x_m) = g(x_1, \dots, x_n).$

Thus h and g coincide.

3. Arity gap

Recall that simple variable substitution induces a quasi-order on the set of *B*-valued functions on *A*, as described in Section 2. For a function $f: A^n \to B$ with at least two essential variables, we denote

$$\operatorname{ess}^{<} f = \max_{g < f} \operatorname{ess} g,$$

and we define the *arity gap* of f by gap $f = \text{ess } f - \text{ess}^{<} f$.

In the following, whenever we consider the arity gap of some function f, we will assume that all variables of f are essential. This is not a significant restriction, because every non-constant function is equivalent to a function with no inessential variables and equivalent functions have the same arity gap.

Salomaa [16] proved that the arity gap of every Boolean function with at least two essential variables is at most 2. This result was generalized by Willard [21, Lemma 1.2] in the following theorem.

Theorem 3.1. Let A be a finite set. Suppose $f: A^n \to B$ depends on all of its variables. If n > |A|, then gap $f \le 2$.

In [5], Salomaa's result was strengthened by completely classifying all Boolean functions in terms of arity gap: for $f: \{0,1\}^n \to \{0,1\}$, gap f = 2 if and only if f is equivalent to one of the following Boolean functions:

- $x_1 + x_2 + \cdots + x_m + c$,
- $x_1x_2 + x_1 + c$,
- $x_1x_2 + x_1x_3 + x_2x_3 + c$,
- $x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + c$,

where addition and multiplication are done modulo 2 and $c \in \{0, 1\}$. Otherwise gap f = 1.

Based on this, a complete classification of pseudo-Boolean functions according to their arity gap was presented in [6].

Theorem 3.2. For a pseudo-Boolean function $f: \{0,1\}^n \to B$ which depends on all of its variables, gap f = 2 if and only if f satisfies one of the following conditions:

- n = 2 and f is a nonconstant function satisfying f(0,0) = f(1,1),
- $f = g \circ h$, where $g: \{0,1\} \to B$ is injective and $h: \{0,1\}^n \to \{0,1\}$ is a Boolean function with gap h = 2, as listed above.

Otherwise gap f = 1.

The study of the arity gap of functions $A^n \to B$ culminated in the characterization presented in Theorem 3.6, originally proved in [6]. We need to introduce some terminology to state the result. Denote by $\mathcal{P}(A)$ the power set of A, and define the function oddsupp: $\bigcup_{n>1} A^n \to \mathcal{P}(A)$ by

$$oddsupp(a_1, \ldots, a_n) = \{a_i : |\{j \in \{1, \ldots, n\} : a_j = a_i\}| \text{ is odd}\}.$$

We say that a partial function $f: S \to B$, $S \subseteq A^n$, is determined by oddsupp if $f = f^* \circ \text{oddsupp}|_S$ for some function $f^*: \mathcal{P}(A) \to B$. In order to avoid cumbersome notation, if $f: S \to B$, $S \subseteq A^n$, is determined by oddsupp, then whenever we refer to the decomposition $f = f^* \circ \text{oddsupp}|_S$, we may write simply "oddsupp" in place of "oddsupp $|_S$ ", omitting the subscript indicating the domain restriction as it will be obvious from the context.

Remark 3.3. The notion of a function's being determined by oddsupp is due to Berman and Kisielewicz [1]. Willard [21] showed that if $f: A^n \to B$ where A is finite, $n > \max(|A|, 3)$ and gap f = 2, then f is determined by oddsupp.

Remark 3.4. It is easy to verify that for $n \ge 2$,

 $\operatorname{Im} \operatorname{oddsupp}|_{A^n_{-}} = \{ S \subseteq A : |S| \equiv n \pmod{2}, |S| \le n-2 \}.$

Thus, if $f: A_{=}^{n} \to B$ is determined by oddsupp, i.e., $f = f^* \circ \text{oddsupp}|_{A_{=}^{n}}$, then within the domain $\mathcal{P}(A)$ of f^* , only the subsets of A of cardinality at most n-2 with the same parity as n (odd or even) are relevant.

Remark 3.5. A function $f: A^n \to A$ is determined by oddsupp if and only if $f|_{A^n_{\underline{-}}}$ is determined by oddsupp and f is totally symmetric.

Theorem 3.6. Let A and B be arbitrary sets with at least two elements. Suppose that $f: A^n \to B, n \ge 2$, depends on all of its variables.

- (i) For $3 \le p \le n$, gap f = p if and only if qa f = n p.
- (ii) For $n \neq 3$, gap f = 2 if and only if qa f = n 2 or qa f = n and $f|_{A_{\pm}^n}$ is determined by oddsupp.
- (iii) For n = 3, gap f = 2 if and only if there is a nonconstant unary function $h: A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that

$$f(x_1, x_0, x_0) = h(x_{i_1}),$$

$$f(x_0, x_1, x_0) = h(x_{i_2}),$$

$$f(x_0, x_0, x_1) = h(x_{i_3}).$$

(iv) Otherwise gap f = 1.

Remark 3.7. While Theorem 3.6 was originally presented in the setting of functions $f: A^n \to B$ where A is a finite set, its proof does not make use of any assumption on the cardinality of A – except for A having at least two elements – so it immediately generalizes to functions with arbitrary domains.

4. A decomposition theorem for functions

In this section, we will establish the following classification of functions $f: A^n \to B$ $(n \ge 3)$ with arity gap $p \ge 3$, which also provides a decomposition of such functions into a sum of a quasi-nullary function and an essentially (n - p)-ary function.

Theorem 4.1. Assume that (B; +) is a group with neutral element 0. Let $f: A^n \to B$, $n \ge 3$, and $3 \le p \le n$. Then the following two conditions are equivalent:

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

The decomposition f = h + q given above, when it exists, is unique.

Remark 4.2. Theorem 4.1 generalizes and strengthens Shtrakov and Koppitz's Theorem 3.4 of [17]. While [17] deals only with operations on finite sets, Theorem 4.1 applies to functions $f : A^n \to B$, where A and B are arbitrary, possibly infinite sets. Also, [17] only deals with the additive group of integers modulo k, whereas any group structure on the codomain B is allowed here. Moreover, Theorem 4.1 establishes that the prescribed decompositions f = h + g are unique for each group structure on the codomain B, which will be a crucial property when the number of functions with a given arity gap is counted in Section 6. The uniqueness of decompositions is not proved in [17].

We will prove Theorem 4.1 using the following lemma.

Lemma 4.3. Assume that (B; +) is a group with neutral element 0. Let $f: A^n \to B$, $n \ge 3$, and $1 \le p \le n$. Then the following two conditions are equivalent:

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

The decomposition f = h + g given above, when it exists, is unique.

Proof. (a) \implies (b). Assume that ess f = n and qa f = n - p. By the definition of quasi-arity, there exists an essentially (n - p)-ary support $g: A^n \to B$ of f. Setting h := f - g, we have f = h + g. Since $g|_{A_{\pm}^n} = f|_{A_{\pm}^n}$ by the definition of support, we have that $h|_{A_{\pm}^n} \equiv 0$. Furthermore, h is not identically 0, because otherwise we would have that f = g, which constitutes a contradiction to ess g = n - p < n = ess f.

(b) \implies (a). Assume (b). By Lemma 2.2, qa $f = \operatorname{ess} f|_{A^n_{\pm}} = \operatorname{ess} g|_{A^n_{\pm}}$, and by Lemma 2.1, $\operatorname{ess} g|_{A^n_{\pm}} = \operatorname{ess} g = n - p$; hence qa f = n - p. Suppose for contradiction that $\operatorname{ess} f < n$, then $\operatorname{ess} f = \operatorname{qa} f = n - p$ by Lemma 2.3. Both f and g are essentially (qa f)-ary supports of f; therefore it follows from Proposition 2.5 that f = g. Thus $h \equiv 0$, which yields a contradiction.

For the uniqueness of the decomposition f = h + g, the function g in the decomposition f = h + g is clearly an essentially (qa f)-ary support of f. By the assumption that qa $f < \operatorname{ess} f$, Proposition 2.5 implies that g is uniquely determined, and therefore so is h.

Proof of Theorem 4.1. Observe that condition (2) is the same as condition (b) of Lemma 4.3. The latter is equivalent to (a) by Lemma 4.3, and (a) is equivalent to (1) by Theorem 3.6 (i). The uniqueness of the decomposition f = h + g follows from Lemma 4.3.

5. Functions with arity gap 2

We prove an analogue of Theorem 4.1 for the case gap f = 2. If qa f = n - 2, then Lemma 4.3 can be applied, so we only consider the case when $f|_{A_{\pm}^n}$ is determined by oddsupp (see Theorem 3.6 (ii)). In this case we cannot expect f to have a support of arity n - 2, but we may look for a support which is a sum of (n - 2)-ary functions. We will prove that such a support exists if B is a *Boolean group*, i.e., it is an abelian group such that x + x = 0 holds identically. (However, this is not true for arbitrary groups; this will be discussed in a forthcoming paper [7].)

First we need to introduce a notation. Let $\varphi: A^{n-2} \to B$ be a function that is determined by oddsupp, i.e., $\varphi = \varphi^* \circ \text{oddsupp}$, for some function $\varphi^*: \mathcal{P}(A) \to B$. Let $\tilde{\varphi}$ be the *n*-ary function defined by

(1)
$$\widetilde{\varphi}(x_1,\ldots,x_n) = \sum_{\substack{k < n \\ 2|n-k}} \sum_{1 \le i_1 < \cdots < i_k \le n} \varphi^*(\text{oddsupp}(x_{i_1},\ldots,x_{i_k})).$$

Observe that each summand is a variable identification minor of φ , namely

 $\varphi^*(\text{oddsupp}(x_{i_1},\ldots,x_{i_k})) = \varphi(x_{i_1},\ldots,x_{i_k},y,\ldots,y),$

where the number of occurrences of y is n-2-k, which is an even number; therefore y is indeed an inessential variable of the function on the right-hand side; moreover, the order of the variables is irrelevant. The function $\tilde{\varphi}$ is obviously totally symmetric, and according to the following lemma, $\tilde{\varphi}|_{A_{\underline{n}}^{\underline{n}}}$ is determined by oddsupp; hence $\tilde{\varphi}$ is determined by oddsupp as well by Remark 3.5.

Lemma 5.1. Assume that (B; +) is a Boolean group with neutral element 0. Let $\varphi: A^{n-2} \to B$ be a function determined by oddsupp. Then for all $(x_1, \ldots, x_n) \in A^n_{\pm}$ we have

$$\widetilde{\varphi}(x_1,\ldots,x_n) = \varphi^*(\text{oddsupp}(x_1,\ldots,x_n)).$$

Proof. We have to show that $\tilde{\varphi}(x_1, \ldots, x_n) + \varphi^*(\text{oddsupp}(x_1, \ldots, x_n)) = 0$ holds identically on A^n_{\pm} . This function differs from the right-hand side of (1) only by a summand corresponding to k = n:

$$\widetilde{\varphi}(x_1, \dots, x_n) + \varphi^*(\text{oddsupp}(x_1, \dots, x_n)) = \sum_{\substack{k \le n \\ 2|n-k}} \sum_{1 \le i_1 < \dots < i_k \le n} \varphi^*(\text{oddsupp}(x_{i_1}, \dots, x_{i_k})).$$

Let us fix a set $\{a_1, \ldots, a_r\} \subseteq A$ and $(x_1, \ldots, x_n) \in A^n_{=}$. We count how many summands there are in the above sum with $\operatorname{oddsupp}(x_{i_1},\ldots,x_{i_k}) = \{a_1,\ldots,a_r\}$. If this set occurs at all, then a_1, \ldots, a_r can be found among the components of (x_1,\ldots,x_n) . Let us denote the rest of the elements appearing in (x_1,\ldots,x_n) by a_{r+1},\ldots,a_t , and for $j=1,\ldots,t$ let s_j stand for the number of occurrences of a_j in (x_1, \ldots, x_n) . Thus $\{x_1, \ldots, x_n\} = \{a_1, \ldots, a_t\}$ and $s_1 + \cdots + s_t = n$; moreover, t < n, because $(x_1, \ldots, x_n) \in A^n_{=}$. If we want to choose i_1, \ldots, i_k such that $\operatorname{oddsupp}(x_{i_1},\ldots,x_{i_k}) = \{a_1,\ldots,a_r\}$, then we have to choose an odd number of the s_j places occupied by a_j in (x_1, \ldots, x_n) for $j = 1, \ldots, r$, and an even number of the s_j places occupied by a_j for j = r + 1, ..., t. A set of s_j elements has 2^{s_j-1} subsets with odd cardinality, and likewise 2^{s_j-1} subsets with even cardinality, so the number of possibilities is 2^{s_j-1} in both cases. Thus there are altogether $2^{s_1-1} \cdot \ldots \cdot 2^{s_t-1} = 2^{n-t}$ summands with the same oddsupp $(x_{i_1}, \ldots, x_{i_k})$. This number is even since t < n; therefore the terms will cancel each other. This holds for any set $\{a_1, \ldots, a_r\}$ and any $(x_1,\ldots,x_n) \in A^n_{=}$; hence $\widetilde{\varphi}(x_1,\ldots,x_n) + \varphi^*(\text{oddsupp}(x_1,\ldots,x_n))$ is identically zero on $A^n_{=}$.

Theorem 5.2. Assume that (B; +) is a Boolean group with neutral element 0. Let $f: A^n \to B$ be a function such that $f|_{A^n_{\underline{n}}}$ is determined by oddsupp. Then f has a support that is a sum of functions of arity at most n - 2.

Proof. Since $f|_{A^n_{\pm}}$ is determined by oddsupp, there is a function $f^* \colon \mathcal{P}(A) \to B$ such that $f|_{A^n_{\pm}} = f^* \circ \text{oddsupp}$. The function $\varphi(x_1, \ldots, x_{n-2}) := f(x_1, \ldots, x_{n-2}, y, y)$ is determined by oddsupp, and we can suppose that the corresponding function φ^* coincides with f^* , since

$$\varphi(x_1, \dots, x_{n-2}) = f(x_1, \dots, x_{n-2}, y, y) = f^*(\text{oddsupp}(x_1, \dots, x_{n-2}))$$

7

for all $(x_1, \ldots, x_{n-2}) \in A^{n-2}$. Applying Lemma 5.1 we get the following equality for every $(x_1, \ldots, x_n) \in A^n_-$:

$$\widetilde{\varphi}(x_1, \dots, x_n) = \varphi^*(\text{oddsupp}(x_1, \dots, x_n))$$
$$= f^*(\text{oddsupp}(x_1, \dots, x_n)) = f(x_1, \dots, x_n).$$

This shows that $\tilde{\varphi}$ is a support of f, and from (1) it is clear that $\tilde{\varphi}$ is a sum of at most (n-2)-ary functions.

Remark 5.3. Let us note that if A is finite and n > |A|, then $A^n = A_{=}^n$; hence the only support of f is f itself. In this case the above theorem implies that f itself can be expressed as a sum of functions of arity at most n - 2.

Next we prove a uniqueness companion to the above theorem. Here we do not need the assumption that B is a Boolean group: if there exists a support that is a sum of at most (n-2)-ary functions, then it is unique for any abelian group B. Note that this does not exclude the possibility that this unique support can be written in more than one way as a sum of at most (n-2)-ary functions. Observe also that the following theorem generalizes Proposition 2.5 in the case m = n - 2.

Theorem 5.4. Assume that (B; +) is an abelian group with neutral element 0. Then a function $f: A^n \to B$ can have at most one support that is a sum of functions of arity at most n - 2.

Proof. Suppose that g_1 and g_2 are supports of f and both of them can be expressed as sums of at most (n-2)-ary functions. Then $g = g_1 - g_2$ is also a sum of at most (n-2)-ary functions, and $g|_{A_{\pm}^n}$ is constant zero. Let us choose the smallest k such that g can be written as a sum of functions of arity at most k. If k = 0, then g is constant; hence g = 0 and then we can conclude that $g_1 = g_2$. To complete the proof, we just have to show that the assumption $1 \le k \le n-2$ leads to a contradiction.

In the expression of g as a sum of at most k-ary functions we can combine functions depending on the same set of variables to a single function, and by introducing dummy variables we can make all of the summands n-ary functions. Then g takes the following form:

(2)
$$g(x_1,\ldots,x_n) = \sum_I g_I(x_1,\ldots,x_n),$$

where I ranges over the k-element subsets of $\{1, 2, ..., n\}$, and $g_I: A^n \to B$ is a function which only depends on some of the variables x_i $(i \in I)$. Let us choose a constant $c \in A$ and substitute this into the last n - k variables. Since $n - k \ge 2$, the resulting vector will lie in A^n_{\pm} ; hence the value of g will be zero:

$$0 = g(x_1, \ldots, x_k, c, \ldots, c) = \sum_I g_I(x_1, \ldots, x_k, c, \ldots, c).$$

Let $J = \{1, ..., k\}$, and let us express g_J from the above equation:

$$g_J(x_1,\ldots,x_n) = g_J(x_1,\ldots,x_k,c,\ldots,c) = -\sum_{I \neq J} g_I(x_1,\ldots,x_k,c,\ldots,c).$$

For each k-element subset I of $\{1, 2, ..., n\}$, the function $g_I(x_1, ..., x_k, c, ..., c)$ depends only on the variables x_i $(i \in I \cap J)$; thus its essential arity is at most k - 1 whenever I is different from J. This means that the above expression for g_J can be regarded as a sum of at most (k - 1)-ary functions (after getting rid of the dummy variables). We can get a similar expression for g_J for any k-element subset J of $\{1, 2, ..., n\}$, and substituting these into (2) we see that g is a sum of at most (k - 1)-ary functions. This contradicts the minimality of k, which shows that $k \ge 1$ is indeed impossible.

Combining the above results with Theorem 3.6 and Lemma 4.3 we get the characterization of functions $f: A^n \to B$ with gap f = 2 for the case when B is a Boolean group.

Theorem 5.5. Assume that (B; +) is a Boolean group with neutral element 0. Let $f: A^n \to B$ be a function of arity at least 4. Then the following two conditions are equivalent:

- (1) $\operatorname{ess} f = n \ and \operatorname{gap} f = 2.$
- (2) There exist functions g, h: Aⁿ → B such that f = h + g, h|_{Aⁿ₌} ≡ 0, and either
 (a) ess g = n 2 and h ≠ 0, or
 - (b) $g = \widetilde{\varphi}$ for some nonconstant (n-2)-ary function φ that is determined by oddsupp.

The decomposition f = h + g given above, when it exists, is unique.

Proof. The uniqueness follows immediately from Theorem 5.4, so we just need to show that (1) and (2) are equivalent.

(1) \implies (2). By Theorem 3.6 (ii) we have two cases: either qa f = n - 2, or qa f = n and $f|_{A_{\underline{n}}^{n}}$ is determined by oddsupp. In the first case Lemma 4.3 shows that (2a) holds. In the second case we apply Theorem 5.2 to find an (n-2)-ary function φ such that $g = \tilde{\varphi}$ is a support of f, and we let h = f + g. If φ is constant, then so is $\tilde{\varphi}$, and then $f|_{A_{\underline{n}}^{n}}$ is constant as well, contradicting that qa f = n.

 $(2) \Longrightarrow (1)$. The case (2a) is settled by Lemma 4.3 and Theorem 3.6 (ii), so let us assume that (2b) holds. It is clear that $f|_{A_{\underline{n}}^{n}}$ is determined by oddsupp, so according to Theorem 3.6 it suffices to show that qa $f = \operatorname{ess} f = n$. The function $f|_{A_{\underline{n}}^{n}} = \widetilde{\varphi}|_{A_{\underline{n}}^{n}}$ is totally symmetric, hence it either depends on all of its variables, or on none of them, i.e., either qa f = n or qa f = 0. In the first case we are done, since ess f cannot be less than qa f. In the second case Lemma 5.1 implies that φ^* takes on the same value for every subset of A of size $n-2, n-4, \ldots$. Since only these values of φ^* are relevant for determining $\varphi = \varphi^* \circ \operatorname{oddsupp}$, we can conclude that φ is constant, contrary to our assumption.

6. The number of finite functions with a given arity gap

The classification of functions according to their arity gap (Theorem 3.6) and the unique decompositions of functions provided by Theorem 4.1 can be applied to count, for finite sets A and B, and for each n and p the number of functions $f: A^n \to B$ with gap f = p. This problem was first considered by Shtrakov and Koppitz [17], who found upper bounds for these numbers.

For positive integers m, i, we will denote by $(m)_i$ the falling factorial

$$(m)_i := m(m-1)\cdots(m-(i-1)).$$

Note that if i > m, then $(m)_i = 0$, because one of the factors in the above expression is 0.

Let A and B be finite sets with |A| = k, $|B| = \ell$. Let us denote by $G_{np}^{k\ell}$ the number of functions $f: A^n \to B$ with $\operatorname{ess} f = n$ and $\operatorname{gap} f = p$, and let us denote by $Q_{nm}^{k\ell}$ the number of functions $f: A^n \to B$ with $\operatorname{ess} f = n$ and $\operatorname{qa} f = m$.

It is well known (see Wernick [20]) that the number of functions $g: A^n \to B$ that depend on exactly r variables $(0 \le r \le n)$ is

$$U_{nr}^{k\ell} := \binom{n}{r} \sum_{i=0}^r (-1)^i \binom{r}{i} \ell^{k^{r-i}}.$$

The number of functions $h: A^n \to B$ such that $h|_{A^n} \equiv 0, h \neq 0$ is

$$V_n^{k\ell} := \ell^{(k)_n} - 1$$

Lemma 6.1. For $k \ge 2, \ \ell \ge 2, \ n \ge 3$,

(3)
$$Q_{nm}^{k\ell} = \begin{cases} U_{nm}^{k\ell} V_n^{k\ell}, & \text{if } m < n, \\ U_{nn}^{k\ell} \ell^{(k)_n} - V_n^{k\ell} \ell^{k^n}, & \text{if } m = n. \end{cases}$$

Proof. By Lemma 4.3, for $3\leq n\leq k$ and m< n, $Q_{nm}^{k\ell}=U_{nm}^{k\ell}V_n^{k\ell}.$

If n > k, then $V_n^{k\ell} = 0$ and hence the right-hand side of the above equation is 0 as well. Indeed, $Q_{nm}^{k\ell} = 0$ in this case, because for $f: A^n \to B$, $\operatorname{qa} f = \operatorname{ess} f$ whenever n > k.

Consider then the case when m = n. By the above formula, we have

(4)
$$Q_{nn}^{k\ell} = U_{nn}^{k\ell} - \sum_{i=0}^{n-1} Q_{ni}^{k\ell} = U_{nn}^{k\ell} - \sum_{i=0}^{n-1} U_{ni}^{k\ell} V_n^{k\ell} = U_{nn}^{k\ell} - V_n^{k\ell} \sum_{i=0}^{n-1} U_{ni}^{k\ell}.$$

The sum $\sum_{i=0}^{n-1} U_{ni}^{k\ell}$ counts the number of functions $f: A^n \to B$ with ess f < n; hence

$$\sum_{i=0}^{n-1} U_{ni}^{k\ell} = \ell^{k^n} - U_{nn}^{k\ell}.$$

Substituting this back to (4), we have

$$Q_{nn}^{k\ell} = U_{nn}^{k\ell} - V_n^{k\ell}(\ell^{k^n} - U_{nn}^{k\ell}) = U_{nn}^{k\ell}(1 + V_n^{k\ell}) - V_n^{k\ell}\ell^{k^n} = U_{nn}^{k\ell}\ell^{(k)_n} - V_n^{k\ell}\ell^{k^n}. \quad \Box$$

Let us denote by $O_n^{k\ell}$ the number of functions $f: A^n \to B$ such that $\operatorname{ess} f = n$, $\operatorname{qa} f = n$ and $f|_{A_{\underline{n}}}$ is determined by oddsupp.

Lemma 6.2. For $k \ge 2, \ \ell \ge 2, \ n \ge 2$,

$$O_n^{k\ell} = \begin{cases} \ell^{2^{k-1}} - \ell, & \text{if } n > k, \\ \ell^{(k)_n} (\ell^{S_n^k} - \ell), & \text{if } n \le k, \end{cases}$$

where

(5)
$$S_n^k = \begin{cases} \sum_{i=0}^{\frac{n}{2}-1} \binom{k}{2i}, & \text{if } n \text{ is even,} \\ \sum_{i=0}^{\frac{n-1}{2}-1} \binom{k}{2i+1}, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Let $f: A^n \to B$ be a map such that $f|_{A^n_{\pm}}$ is determined by oddsupp. It is clear that then $f|_{A^n_{\pm}}$ is totally symmetric; hence, either all variables are essential in $f|_{A^n_{\pm}}$ or none of them is. In the former case, qa f = n, and in the latter case qa f = 0 (i.e., $f|_{A^n_{\pm}}$ is constant). Therefore $O_n^{k\ell}$ equals the number of nonconstant maps Im oddsupp $|_{A^n_{\pm}} \to B$ multiplied by the number of maps $A^n \setminus A^n_{\pm} \to B$. By Remark 3.4,

$$\operatorname{Im} \operatorname{oddsupp}|_{A_{\underline{n}}} = \{ S \subseteq A : |S| \equiv n \pmod{2}, |S| \le n-2 \}.$$

Consider first the case that n > k. Then $A^n_{=} = A^n$ and there is only one map $A^n \setminus A^n_{=} \to B$, namely the empty map. In this case, Im oddsupp $|_{A^n_{=}}$ equals the set of odd subsets of A or the set of even subsets of A, depending on the parity of n. It is well known that the number of odd subsets of A equals the number of even subsets of A, and this number is 2^{k-1} . Thus $O_n^{k\ell}$ equals the number of nonconstant functions from the set of even (or odd) subsets of A to B, which is $\ell^{2^{k-1}} - \ell$. Note that this number does not depend on n.

Consider then the case that $n \leq k$. If n = 2q, then

$$\left|\operatorname{Im} \operatorname{oddsupp}\right|_{A^n_{\pm}}\right| = \sum_{i=0}^{q-1} \binom{k}{2i}.$$

If n = 2q + 1, then

$$\left|\operatorname{Im} \operatorname{oddsupp}\right|_{A_{\pm}^{n}}\right| = \sum_{i=0}^{q-1} \binom{k}{2i+1}.$$

The number of maps $A^n \setminus A^n_{=} \to B$ is $\ell^{(k)_n}$. Thus,

$$O_n^{k\ell} = \ell^{(k)_n} (\ell^{S_n^k} - \ell),$$

where S_n^k is as given in equation (5).

Theorem 6.3. Let $k \ge 2, \ \ell \ge 2, \ n \ge 2$.

- (i) If n > k and $3 \le p \le n$, then $G_{np}^{k\ell} = 0$.
- (ii) If n > k and $n \ge 4$, then

$$G_{n2}^{k\ell} = O_n^{k\ell} = \ell^{2^{k-1}} - \ell, \qquad G_{n1}^{k\ell} = U_{nn}^{k\ell} - G_{n2}^{k\ell}.$$

(iii) If $3 \le n \le k$ and $3 \le p \le n$, then $G_{np}^{k\ell} = U_{n(n-p)}^{k\ell} V_n^{k\ell}$.

(iv) If
$$4 \le n \le k$$
, then
 $G_{n2}^{k\ell} = U_{n(n-2)}^{k\ell} V_n^{k\ell} + O_n^{k\ell}$, $G_{n1}^{k\ell} = U_{n(n-1)}^{k\ell} V_n^{k\ell} + U_{nn}^{k\ell} \ell^{(k)_n} - V_n^{k\ell} \ell^{k^n} - O_n^{k\ell}$
(v) $G_{32}^{k\ell} = (8\ell^{(k)_3} - 3)(\ell^k - \ell), G_{31}^{k\ell} = U_{33}^{k\ell} - G_{33}^{k\ell} - G_{32}^{k\ell}$.

(vi) $G_{22}^{k\ell} = \ell^{(k)_2+1} - \ell, \ G_{21}^{k\ell} = U_{22}^{k\ell} - G_{22}^{k\ell}.$

Proof. (i) Follows from Theorem 3.1.

(ii) If $f: A^n \to B$ depends on all of its variables and n > k, then by Remark 2.4 qa $f = \operatorname{ess} f = n$. Thus gap f = 2 if and only if $f|_{A_{\pm}^n} = f$ is determined by oddsupp. Thus, $G_{n2}^{k\ell} = O_n^{k\ell} = \ell^{2^{k-1}} - \ell$ by Lemma 6.2. The equality for $G_{n1}^{k\ell}$ follows immediately from (i) and the equality for $G_{n2}^{k\ell}$. (iii) By Theorem 3.6 (i), for $3 \le n \le k$ and $3 \le p \le n$, we have $G_{np}^{k\ell} = Q_{n(n-p)}^{k\ell}$,

and $Q_{n(n-p)}^{k\ell} = U_{n(n-p)}^{k\ell} V_n^{k\ell}$ by Lemma 6.1.

(iv) By Theorem 3.6, and Lemma 6.1, for $n \ge 4$, we have

$$G_{n2}^{k\ell} = Q_{n(n-2)}^{k\ell} + O_n^{k\ell} = U_{n(n-2)}^{k\ell} V_n^{k\ell} + O_n^{k\ell}$$

and

$$G_{n1}^{k\ell} = Q_{n(n-1)}^{k\ell} + Q_{nn}^{k\ell} - O_n^{k\ell} = U_{n(n-1)}^{k\ell} V_n^{k\ell} + U_{nn}^{k\ell} \ell^{(k)_n} - V_n^{k\ell} \ell^{k^n} - O_n^{k\ell}$$

(v) We apply Theorem 3.6 (iii) in order to determine $G_{32}^{k\ell}$. It is easy to verify that given nonconstant functions $h, h': A \to B$, elements $i_1, i_2, i_3, i'_1, i'_2, i'_3 \in \{0, 1\}$ and functions $f, f': A^3 \to B$ such that

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

it holds that $f|_{A_{\pm}^3} = f'|_{A_{\pm}^3}$ if and only if h = h', $i_1 = i'_1$, $i_2 = i'_2$, $i_3 = i'_3$.

There are $2^3 = 8$ choices for (i_1, i_2, i_3) , there are $\ell^k - \ell$ nonconstant maps $h: A \to B$, and there are $\ell^{(k)_3}$ ways to choose values for a function on $A^3 \setminus A_{=}^3$. Thus the number of functions of the form given in Theorem 3.6 (iii) is

$$8(\ell^k - \ell)\ell^{(k)_3}.$$

However, some of the functions corresponding to Theorem 3.6 (iii) are not essentially ternary, and we have to subtract the number of these functions from the above number. We claim that $f: A^3 \to B$ satisfies the condition of Theorem 3.6 (iii) and ess f < 3 if and only if ess f = 1. Indeed, every essentially unary function $f: A^3 \to B$ satisfies the condition of Theorem 3.6 (iii) with $(i_1, i_2, i_3) \in \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ and h(x) =f(x, x, x). Conversely, suppose that f satisfies the condition of Theorem 3.6 (iii) and ess f < 3, say, the last variable of f is inessential. Then we have

$$f(x_0, x_1, x_2) = f(x_0, x_1, x_0) = h(x_{i_2}),$$

i.e., f is equivalent to the nonconstant unary function h.

The number of essentially unary ternary functions is $3(\ell^k - \ell)$; hence

$$G_{32}^{k\ell} = 8(\ell^k - \ell)\ell^{(k)_3} - 3(\ell^k - \ell) = (8\ell^{(k)_3} - 3)(\ell^k - \ell).$$

It is clear that

$$G_{31}^{k\ell} = U_{33}^{k\ell} - G_{33}^{k\ell} - G_{32}^{k\ell}.$$

(vi) For $f: A^2 \to B$, gap f = 2 if and only if $f|_{A^2_{=}}$ is constant (but f itself is not constant). Thus $G_{22}^{k\ell} = \ell^{(k)_2+1} - \ell$. It is clear that $G_{21}^{k\ell} = U_{22}^{k\ell} - G_{22}^{k\ell}$. \square

We have evaluated $G_{np}^{k\ell}$ for some values of k, ℓ, n, p in Table 1.

10

DECOMPOSITIONS OF FUNCTIONS BASED ON ARITY GAP

| k | l | n | $U^{k\ell}_{nn}$ | $G_{n1}^{k\ell}$ | $G_{n2}^{k\ell}$ | $G_{n3}^{k\ell}$ | $G_{n4}^{k\ell}$ | $G_{n5}^{k\ell}$ |
|---|---|---|----------------------|----------------------|-------------------|--------------------|--------------------|------------------|
| 2 | 2 | 2 | 10 | 4 | 6 | | | |
| | | 3 | 218 | 208 | 10 | 0 | | |
| | | 4 | 64594 | 64592 | 2 | 0 | 0 | |
| | | 5 | 4294642034 | 4294642032 | 2 | 0 | 0 | 0 |
| 3 | 3 | 2 | 19632 | 17448 | 2184 | | | |
| | | 3 | 7625597426016 | 7625597283936 | 139896 | 2184 | | |
| | | 4 | $4.4\cdot 10^{38}$ | $4.4 \cdot 10^{38}$ | 78 | 0 | 0 | |
| | | 5 | $8.7 \cdot 10^{115}$ | $8.7 \cdot 10^{115}$ | 78 | 0 | 0 | 0 |
| 4 | 4 | 2 | 4294966788 | 4227857928 | 67108860 | | | |
| | | 3 | $3.4\cdot10^{38}$ | $3.4\cdot10^{38}$ | $5.7\cdot10^{17}$ | $1.1\cdot 10^{15}$ | | |
| | | 4 | $1.3\cdot 10^{154}$ | $1.3\cdot10^{154}$ | $7.3\cdot10^{24}$ | $2.8\cdot 10^{17}$ | $1.1\cdot 10^{15}$ | — |
| | | 5 | $3.2\cdot10^{616}$ | $3.2\cdot10^{616}$ | 65532 | 0 | 0 | 0 |

TABLE 1. $G_{np}^{k\ell}$ for small values of k, ℓ, n, p .

Acknowledgements

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

References

- J. Berman, A. Kisielewicz, On the number of operations in a clone, Proc. Amer. Math. Soc. 122 (1994) 359–369.
- [2] K.N. Čimev, On some properties of functions. In: B. Csákány, I. Rosenberg (eds.), Finite Algebra and Multiple-Valued Logic, Abstracts of lectures of the colloquium on finite algebra and multiplevalued logic (Szeged, 1979), North-Holland, 1981, pp. 38–40.
- [3] K.N. Čimev, Separable Sets of Arguments of Functions, Studies 180/1986, Computer and Automation Institute, Hungarian Academy of Sciences, Budapest, 1986.
- M. Couceiro, On the lattice of equational classes of Boolean functions and its closed intervals, J. Mult.-Valued Logic Soft Comput. 18 (2008) 81–104.
- [5] M. Couceiro, 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.
- [6] M. Couceiro, E. Lehtonen, Generalizations of Świerczkowski's lemma and the arity gap of finite functions, Discrete Math. 309 (2009) 5905–5912.
- [7] M. Couceiro, E. Lehtonen, T. Waldhauser, On the arity gap of polynomial functions, arXiv:1104.0595.
- [8] M. Couceiro, M. Pouzet, On a quasi-ordering on Boolean functions, Theoret. Comput. Sci. 396 (2008) 71–87.
- [9] R.O. Davies, Two theorems on essential variables, J. London Math. Soc. 41 (1966) 333–335.
- [10] K. Denecke, J. Koppitz, Essential variables in hypersubstitutions, Algebra Universalis 46 (2001) 443–454.
- [11] A. Feigelson, L. Hellerstein, The forbidden projections of unate functions, Discrete Appl. Math. 77 (1997) 221–236.
- [12] E. Lehtonen, Descending chains and antichains of the unary, linear, and monotone subfunction relations, Order 23 (2006) 129–142.
- [13] E. Lehtonen, A. Szendrei, Equivalence of operations with respect to discriminator clones, Discrete Math. 309 (2009) 673–685.
- [14] O.B. Lupanov, On a class of schemes of functional elements, Problemy Kibernetiki 7 (1962) 61–114 (in Russian).
- [15] N. Pippenger, Galois theory for minors of finite functions, Discrete Math. 254 (2002) 405–419.
- [16] 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.
- [17] S. Shtrakov, J. Koppitz, On finite functions with non-trivial arity gap, Discuss. Math. Gen. Algebra Appl. 30 (2010) 217–245.
- [18] 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).
- [19] C. Wang, Boolean minors, Discrete Math. 141 (1991) 237–258.

- [20] W. Wernick, An enumeration of logical functions, Bull. Amer. Math. Soc. 45 (1939) 885–887.
- [21] R. Willard, Essential arities of term operations in finite algebras, Discrete Math. 149 (1996) 239–259.
- [22] S.V. Yablonski, Functional constructions in a k-valued logic, Tr. Mat. Inst. Steklova 51 (1958) 5–142 (in Russian).
- [23] 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.

(M. Couceiro) MATHEMATICS RESEARCH UNIT, UNIVERSITY OF LUXEMBOURG, 6, RUE RICHARD COUDENHOVE-KALERGI, L-1359 LUXEMBOURG, LUXEMBOURG *E-mail address:* miguel.couceiro@uni.lu

(E. Lehtonen) Computer Science and Communications Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: erkko.lehtonen@uni.lu

(T. Waldhauser) 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

 $E\text{-}mail\ address: \texttt{twaldha@math.u-szeged.hu}$