Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 191 (2013)

Boolean functions with a vertex-transitive group of automorphisms

Petr Savicky
Institute of Computer Science,
Academy of Sciences of the Czech Republic,
Prague, Czech Republic
savicky@cs.cas.cz

Abstract

A Boolean function is called vertex-transitive, if the partition of the Boolean cube into the preimage of 0 and the preimage of 1 is invariant under a vertex-transitive group of isometric transformations of the Boolean cube. Although this is a very restrictive condition, there are non-trivial functions satisfying this property. The logarithm of the number of the vertex-transitive functions of n variables is $\Theta(n^2)$. There is a polynomial over GF(2) of any given degree, which defines a vertex-transitive function, and quadratic polynomials with this property can be characterized. There are vertex-transitive functions of n variables with sensitivity and block sensitivity $\Theta(\log n)$. For every vertex-transitive function, there is a representation of roughly quadratic size in n, which can be used to evaluate the function for a given input in time $O(n^2)$ on random access machine.

1 Introduction

One of the first classes of the Boolean functions, whose complexity was investigated, are the symmetric functions, see [18, 12]. A function is symmetric, if it is invariant under any permutation of its variables. A symmetric function of n variables is uniquely determined by a vector of values $c_0, \ldots, c_n \in \{0, 1\}$, such that for inputs x with i components equal to 1, we have $f(x) = c_i$. Hence, the number of the symmetric functions of n variables is 2^{n+1}.

A significantly larger class of Boolean functions defined by their symmetry are weakly symmetric functions, which are invariant under a transitive group of the permutations of the variables. Weakly symmetric functions were investigated, for example, in the context of decision tree complexity measures, see [12, 10].

Every graph property of the undirected graphs on k vertices can be understood as a Boolean function, whose $n = \binom{k}{2}$ variables are indicators of the presence of individual edges and are indexed by pairs of vertices. A graph property is invariant under any permutation of the k vertices. These permutations induce a transitive group of the permutations of the n pairs of the vertices and, hence, a transitive group of the permutations of the variables. Consequently, every graph property represents a weakly symmetric Boolean function.

ISSN 1433-8092

In [16], a lower bound $\Omega(n^{1/2})$ on the sensitivity of any non-trivial graph property is proven and the graph property "no vertex is isolated" with sensitivity $k-1=\Theta(n^{1/2})$ is presented. The lower bound of this magnitude does not hold for a general weakly symmetric function. An example of a weakly symmetric function of n variables and sensitivity $O(n^{1/3})$ was presented in [2] and [3]. The block sensitivity of a non-trivial weakly symmetric function is at least $\Omega(n^{1/3})$ by [15]. An example of a weakly symmetric function with block sensitivity $O(n^{3/7}\log n)$ is presented in [15] and an improved construction with block sensitivity $O(n^{3/7}\log^{1/7} n)$ is presented in [8]. Let us point out that the minimum sensitivity and block sensitivity of a general Boolean function, which depends on n variables, is $\Theta(\log n)$, see [12].

The purpose of this paper is to describe a class of Boolean functions, which are invariant under a more general type of transformations than the permutations of the variables and prove some of its properties. Several specific examples and infinite families of such functions are presented, including functions with logarithmic sensitivity.

The domain of the Boolean functions of n variables, the Boolean cube $\{0,1\}^n$, will be considered as a metric space with the Hamming distance as the metric. Isometric transformations of the Boolean cube are the permutations of its vertices, which preserve the Hamming distance. These transformations are exactly the transformations, which can be defined by a permutation of the n variables and the negation of a subset of the variables. We investigate non-constant Boolean functions f, for which the partition of the Boolean cube to the sets $f^{-1}(0)$ and $f^{-1}(1)$ is invariant under a vertex-transitive group of isometric transformations. Due to this property, the functions will be called vertex-transitive functions or, for simplicity, transitive functions.

Vertex-transitive functions are defined in Section 2 as functions satisfying a specific system of identities. Every linear function over the two-element field GF(2) is transitive for a simple reason and examples of non-linear transitive functions are presented. For every transitive function of n variables, there is an n-tuple of permutations and n additional bits, which represent the function. If a given n-tuple of permutations and bits represents a transitive function, then the function can be evaluated for any given input in time $O(n^2)$ on RAM (random access machine) with the unit cost measure. Section 2.4 presents a comparison of vertex-transitive functions and weakly symmetric functions.

Section 3 presents several constructions of non-linear transitive functions. In particular, quadratic polynomials over GF(2), which define a transitive function, are characterized in Corollary 3.10. There are polynomials over GF(2) of an arbitrary degree, which define a transitive function. An infinite sequence of transitive functions with sensitivity and block sensitivity $\Theta(\log n)$, where n is the number of their variables, is presented.

In Section 4, it is proved that for every transitive function, there is a transitive group G of its automorphisms, which is a 2-group. Since the groups are finite, this is equivalent to the condition that the size of G is a power of 2. These groups are easier to analyze than general groups, in particular, every finite 2-group is solvable. In Section 5 the representation by a 2-group is used to prove that the number of transitive functions of n variables is $2^{\Theta(n^2)}$. Section 6 discusses the existence of a simply transitive group of automorphisms of some transitive functions.

2 Vertex-transitive functions

2.1 Transformations of the Boolean cube

For a permutation $p \in S_n$ and $x = (x_1, \dots, x_n) \in \{0,1\}^n$, let x^p be the vector

$$x^p = (x_{p^{-1}(1)}, \dots, x_{p^{-1}(n)})$$

obtained from x by permuting its components according to p so that the i-th component of x is equal to the $p(i)$-th component of x^p. The composition p_1p_2 of the permutations p_1, p_2 is defined so that for every x, we have

$$(x^{p_1})^{p_2} = x^{p_1p_2} \ .$$

Isometric transformation of $\{0,1\}^n$ is a permutation of the vertices of the Boolean cube, which preserves the Hamming distance. The set of all such transformations is closed under composition and forms a group with this operation. One can verify that the isometric transformations are exactly the mappings of the form

$$x \mapsto x^p \oplus s \ ,$$

where $p \in S_n$ and $s \in \{0,1\}^n$, and will be denoted as $\tau(p, s)$. The group of all isometries $\tau(p, s)$ for $p \in S_n$ and $s \in \{0,1\}^n$ with composition as the operation will be denoted T_n. Similarly, if A is a set of indices of the variables, then T_A denotes the group of the isometric transformations of $\{0,1\}^A$. Clearly, $|T_n| = n!\,2^n$.

The composition of transformations $\tau_1, \tau_2 \in T_n$ is denoted $\tau_1\tau_2$ and satisfies $(\tau_1\tau_2)(x) = \tau_2(\tau_1(x))$. For every $p_1, p_2 \in S_n$ and every $s_1, s_2 \in \{0,1\}^n$, we have

$$(x^{p_1} \oplus s_1)^{p_2} \oplus s_2 = x^{p_1p_2} \oplus s_1^{p_2} \oplus s_2$$

and, hence,

$$\tau(p_1, s_1)\tau(p_2, s_2) = \tau(p_1p_2, s_1^{p_2} \oplus s_2) \ .$$

Let P_n be the subgroup of T_n consisting of the isometries defined by permutations of the variables, formally, $P_n = \{\tau(p, 0) \mid p \in S_n\}$. Note that P_n is the stabilizer in T_n of the point $0 \in \{0,1\}^n$. Let V_n be the subgroup of T_n consisting of the linear shifts, formally, $V_n = \{\tau(\mathrm{id}, s) \mid s \in \{0,1\}^n\}$. As an abstract group, P_n is isomorphic to S_n and V_n is isomorphic to the additive group of the linear space $\{0,1\}^n$ over GF(2). Let us remark that T_n is a semidirect product of P_n and V_n, since $T_n = P_nV_n$, $P_n \cap V_n$ is the trivial subgroup of T_n and V_n is a normal subgroup of T_n.

The elements of T_n can be represented as permutations of the literals, which keep the blocks $\{x_i, \neg x_i\}$, see also [6]. In particular, the elements of P_n permute the blocks, while keeping the order of the literals in each block. The elements of V_n keep the blocks as sets, but exchange the literals in some of them. This representation is isomorphic to the wreath product of Z_2 and S_n, where S_n acts on Z_2^n. For algorithmic purposes, this wreath product can be represented as a subgroup of S_{2n}, which will be denoted T_n^*, consisting of the permutations, which preserve the partition $\{1,2\},\{3,4\},\dots,\{2n-1,2n\}$. Let u be the vector of length $2n$ of the form $(0,1,0,1,\dots,0,1)$. The orbit of this vector under the permutation action of T_n^* has size 2^n and the action of T_n^* on this orbit is isomorphic to the action of T_n on $\{0,1\}^n$, where we can identify u with the zero vector in $\{0,1\}^n$. The subgroups of T_n^* corresponding to P_n and V_n in T_n will be denoted as P_n^* and V_n^*.

2.2 Definition and basic properties

If f is a Boolean function of n variables and $s \in \{0,1\}^n$, then $f(x \oplus s)$ is the function obtained from $f(x)$ by negating the variables corresponding to non-zero entries in s. This paper investigates functions f, for which any function of the form $f(x \oplus s)$ is either equal to $f(x)$ or to its negation $f(x) \oplus 1$ up to a permutation of the variables.

Definition 2.1 A non-constant Boolean function f of n variables is vertex-transitive, if for every $s \in \{0,1\}^n$, there is a permutation $q \in S_n$ and a constant $a \in \{0,1\}$, such that for every $x \in \{0,1\}^n$, we have

$$f(x \oplus s) = f(x^q) \oplus a \ . \tag{1}$$

Denoting $p = q^{-1}$ and substituting x^p for x in both sides of (1), we obtain

$$f(x^p \oplus s) = f(x) \oplus a \ ,$$

which can be written as

$$f(\tau(x)) = f(x) \oplus a \ , \tag{2}$$

where $\tau = \tau(p,s)$. The isometric transformation $\tau(p,s)$ will be called the transformation corresponding to (1).

Definition 2.2 Let f be a Boolean function of n variables and $\tau \in T_n$ an isometric transformation of $\{0,1\}^n$. Then, τ is called an automorphism of f, if there is $a \in \{0,1\}$, such that for all x, the identity (2) is satisfied.

Composition of automorphisms of a function is again an automorphism, so the automorphisms of a function form a subgroup of T_n. The automorphism $\tau = \tau(p,s)$ corresponding to (1) maps 0 to s. Hence, if f is a vertex-transitive function, then the group of its automorphisms is transitive on the vertices of the Boolean cube.

Lemma 2.3 *A non-constant Boolean function f is vertex-transitive, if and only if there is a group of automorphisms of f, which is transitive on* $\{0,1\}^n$.

Proof. The closure of the set of isometries τ required by Definition 2.1 is a group of automorphisms of f, which is transitive.

If G is a transitive group of automorphisms of f, then for every $s \in \{0,1\}^n$, there is an automorphism $\tau \in G$, which satisfies $\tau(0) = s$. Since $\tau = \tau(p,s)$ for some $p \in S_n$, the identity (1) is satisfied for $q = p^{-1}$ and some $a \in \{0,1\}$. □

In this paper, the vertex-transitive functions will be called transitive for simplicity, although, in the literature, the notion of a transitive function can have a different meaning, see Section 2.4.

A function f is transitive, if and only if $\neg f = f \oplus 1$ is transitive. Due to this, we can, without loss of generality, restrict ourselves to the functions, which satisfy $f(0) = 0$.

Clearly, τ is an automorphism of f, if the partition of the Boolean cube to the sets $f^{-1}(0)$ and $f^{-1}(1)$ is invariant under τ. In other words, these two sets form a block system for the group of the automorphisms of f and each automorphism either keeps or exchanges the blocks depending on the constant a from (2). Properties of the groups of automorphisms of a transitive function, which can be derived using this block system, are investigated in Section 4.

The system of the generators of a transitive group of automorphisms can be small. The function α_3 in Example 2.10 is a function of 8 variables, for which a transitive group of automorphisms with two generators exists.

Verification of the transitivity of a group of automorphisms given by its generators can be avoided, if the system of generators consists of n identities in the special form described in Theorem 2.5. For the proof of this theorem, we use the following lemma. For groups H, K, let $HK = \{hk \mid h \in H, k \in K\}$.

Lemma 2.4 *A subgroup G of T_n is transitive, if and only if $P_n G = T_n$.*

Proof. Clearly, $P_n G \subseteq T_n$. If G is transitive and $\tau \in T_n$, then $g(0) = \tau(0)$ for some $g \in G$. Consequently, $\tau = (\tau g^{-1})g \in P_n G$, since P_n is the stabilizer of $0 \in \{0,1\}^n$. This implies $P_n G = T_n$.

If $P_n G = T_n$ and $s \in \{0,1\}^n$, then $\tau(0) = s$ for some $\tau \in T_n$ and $\tau = \pi g \in P_n G$, where $\pi \in P_n$ and $g \in G$. Since $\pi(0) = 0$, we have $g(0) = s$. Hence, G is transitive. □

The Boolean cube is a vertex-transitive graph, if two vertices are connected by an edge if and only if their Hamming distance is 1. The automorphism group of this graph is T_n. It is well-known that a set of automorphisms of a vertex-transitive graph, which map a given vertex to all its neighbours, generates a transitive subgroup of the automorphism group. The next theorem can be understood as a special case of this, since the standard basis vectors e_i, $i = 1, \ldots, n$ are the neighbours of the zero vertex of the Boolean cube. However, a self-contained proof is presented.

Theorem 2.5 *A function f of n variables is transitive, if and only if for every $i = 1, \ldots, n$, there is a permutation $q_i \in S_n$ and a constant $a_i \in \{0,1\}$, such that*

$$f(x \oplus \mathrm{e}_i) = f(x^{q_i}) \oplus a_i \ , \tag{3}$$

where e_i is the i-th standard basis vector. Moreover, if f satisfies $f(0) = 0$, then it is uniquely determined by the parameters q_i, a_i for $i = 1, \ldots, n$.

Proof. If f is transitive, then the subset of the identities from Definition 2.1 for the vectors s satisfying $|s| = 1$ is the set of n identities (3).

For the opposite direction, let us transform (3) to the equivalent form

$$f(x^{p_i} \oplus \mathrm{e}_i) = f(x) \oplus a_i \ , \tag{4}$$

where $p_i = q_i^{-1}$. If the identities (4) are satisfied, then the transformations $\tau_i = \tau(p_i, \mathrm{e}_i)$ for $i = 1, \ldots, n$ are automorphisms of f and let G be the group generated by them. In order to prove that G is transitive, let us first prove the following.

Lemma 2.6 *For every $\pi \in P_n$ and $i \in \{1, \ldots, n\}$, there is $\pi' \in P_n$ and $j \in \{1, \ldots, n\}$, such that*

$$\tau_i \pi = \pi' \tau_j \ . \tag{5}$$

Proof. If $\pi = \tau(r, 0)$ for $r \in S_n$, let $j = r(i)$ and $\pi' = \tau(p_i r p_j^{-1}, 0)$. Clearly, $\mathrm{e}_i^r = \mathrm{e}_j$. Using this, (5) can be verified by a simple calculation. □

Denoting $\pi_i = \tau(p_i^{-1}, 0)$ for $i = 1, \ldots, n$, we have $\tau(\mathrm{id}, \mathrm{e}_i) = \pi_i \tau_i \in \langle P_n, G \rangle$. Since the tranformations $\tau(\mathrm{id}, \mathrm{e}_i)$ generate V_n, we have $V_n \subseteq \langle P_n, G \rangle$. Every element of $\langle P_n, G \rangle$ is expressible as a word over the elements of P_n and the generators of G. By a repeated application of (5), this word can be transformed to a word expressing the same transformation as an element of $P_n G$. Hence, $\langle P_n, G \rangle = P_n G$ and we have $T_n = \langle P_n, V_n \rangle \subseteq \langle P_n, G \rangle = P_n G \subseteq T_n$. By Lemma 2.4, G is transitive and it follows that f is a transitive function.

Since f satisfies a system of identities (1), which is derived from identities (3), there is at most one function f satisfying (3). □

The existence of a function satisfying (3) for given parameters q_i, a_i is not guaranteed. However, if the parameters q_i, a_i define a transitive function f, it is possible to use them to compute $f(x)$ for any $x \in \{0,1\}^n$ in time polynomial in n.

Theorem 2.7 *Assume, f is a transitive function satisfying $f(0) = 0$ and let q_i, a_i for $i = 1, \ldots, n$ be as in Theorem 2.5. Then, for every $x \in \{0,1\}^n$, it is possible to compute $f(x)$ in time $O(n^2)$ on RAM (random access machine) with the unit cost measure, if q_i, a_i for $i = 1, \ldots, n$ are part of the input.*

Proof. The algorithm is obtained by reformulating the computation with the generators π_i and τ_i from the proof of Theorem 2.5 in an explicit form. Let $x \in \{0,1\}^n$, let $i_1, \ldots, i_k$ be indices such that $x = \mathrm{e}_{i_1} \oplus \ldots \oplus \mathrm{e}_{i_k}$, and let

$$\tau = \pi_{i_1} \tau_{i_1} \ldots \pi_{i_k} \tau_{i_k} \ .$$

Clearly, $\tau \in V_n$ and $\tau(0) = x$. The word for τ will be successively transformed into a word in $P_n G$. In a general step, the word has the form

$$\tau = \pi_{i_1} \tau_{i_1} \ldots \pi_{i_l} \tau_{i_l} \sigma \tau_{j_{l+1}} \ldots \tau_{j_k} \ ,$$

where $\sigma \in P_n$ and $j_{l+1}, \ldots, j_k \in \{1, \ldots, n\}$. The initial word has this form with $l = k-1$ and $\sigma = \pi_{i_k}$. Using (5), the product $\pi_{i_l}\tau_{i_l}\sigma$ can be transformed into $\sigma'\tau_{j_l}$, for appropriate j_l and $\sigma' \in P_n$. Repeating this with decreasing l up to $l = 1$, we obtain

$$\tau = \sigma\tau_{j_1} \ldots \tau_{j_k}$$

for an appropriate $\sigma \in P_n$ and $j_1, \ldots, j_k$. Since $\sigma(0) = 0$, we have

$$f(x) = f(\tau(0)) = f((\tau_{j_1} \ldots \tau_{j_k})(0)) = f(0) \oplus a_{j_1} \oplus \ldots \oplus a_{j_k} \ .$$

Computing the sequence $j_1, \ldots, j_k$ requires $O(n)$ operations with elements of T_n. Using the representation of T_n by T_n^*, the total complexity is $O(n^2)$. □

2.3 Examples of transitive functions

For a vector of variables x, let $\mathrm{par}(x)$ be the parity of the variables in x. For an arbitrary set $A \subseteq \{1, \ldots, n\}$, let x_A be the variables, whose indices belong to A.

Lemma 2.8 *If $A \subseteq \{1, \ldots, n\}$, then the linear function*

$$\mathrm{par}(x_A) = \bigoplus_{i \in A} x_i$$

is transitive.

Proof. Denote $f(x) = \mathrm{par}(x_A)$. The group V_n of the linear shifts is a group of automorphisms of f, since for any s and x, the transformation $\tau = \tau(\mathrm{id}, s)$ satisfies

$$f(\tau(x)) = f(x \oplus s) = f(x) \oplus f(s) \ .$$

□

The function α_2 from the following example is a quadratic function over GF(2), which is transitive. It will be used later to construct more complex transitive functions.

Example 2.9 *The function $\alpha_2(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_2 \oplus x_4$ is transitive.*

Proof. One can verify that the function $\alpha_2(x)$ satisfies

$$\begin{aligned} \alpha_2(x \oplus \mathrm{e}_1) &= \alpha_2(x_1, x_2, x_4, x_3) && (6)\\ \alpha_2(x \oplus \mathrm{e}_2) &= \alpha_2(x_1, x_2, x_4, x_3) \oplus 1 && (7)\\ \alpha_2(x \oplus \mathrm{e}_3) &= \alpha_2(x_2, x_1, x_3, x_4) && (8)\\ \alpha_2(x \oplus \mathrm{e}_4) &= \alpha_2(x_2, x_1, x_3, x_4) \oplus 1 \ , && (9) \end{aligned}$$

which are the identities (3). Hence, the function α_2 is transitive by Theorem 2.5. □

The next example demonstrates a transitive function α_3 of 8 variables defined by a polynomial of degree 3 over GF(2). The generators presented in the proof of its transitivity do not generate the full automorphism group of α_3, which requires three generators.

Example 2.10 *Let g be the function defined by*

$$g(y_1, \ldots, y_4) = y_1\, y_2\, y_3 \oplus y_1\, y_2\, y_4 \oplus y_1\, y_3\, y_4 \oplus y_2\, y_3\, y_4 \ .$$

Then, the function α_3 defined by the formula

$$\begin{array}{rcl} \alpha_3(x_1, \ldots, x_8) & = & g(x_1 \oplus x_2,\, x_3 \oplus x_4,\, x_5 \oplus x_6,\, x_7 \oplus x_8) \\ & & \oplus\, (x_1 \oplus x_3 \oplus x_5 \oplus x_7)(x_2 \oplus x_4 \oplus x_6 \oplus x_8) \\ & & \oplus\, (x_1 \oplus x_2)(x_3 \oplus x_4) \\ & & \oplus\, x_3 \oplus x_4 \oplus x_5 \oplus x_8 \ . \end{array}$$

is transitive.

Proof. One can verify that the function $\alpha_3(x)$ satisfies the identities

$$\begin{array}{rcl} \alpha_3(x \oplus \mathrm{e}_1) & = & \alpha_3(x^{p_1}) \\ \alpha_3(x \oplus \mathrm{e}_3) & = & \alpha_3(x^{p_2}) \oplus 1 \ , \end{array}$$

where the permutations p_1, p_2 in the cycle notation are

$$\begin{array}{l} p_1 = (1,7)(2,8)(3,6,4,5) \\ p_2 = (1,5,4,7,2,6,3,8) \ . \end{array}$$

The transformations $\tau(p_1^{-1}, \mathrm{e}_1)$ and $\tau(p_2^{-1}, \mathrm{e}_3)$ corresponding to these identities represent two automorphisms of α_3, which generate a group of size 2^8. Moreover, this group is transitive on $\{0,1\}^8$ and, hence, α_3 is a transitive function by Lemma 2.3. □

For small values of n, it is possible to use GAP computer algebra system [9] to construct all transitive subgroups of T_n up to conjugation and their intransitive subgroups of index 2. By Theorem 4.5, this allows to find all transitive functions up to a permutation of the variables. By Theorem 4.9, it is sufficient to perform this calculation in a Sylow 2-subgroup of T_n, which is more efficient.

Using this approach, one can verify that every transitive function of 4 variables is either linear or quadratic and in the latter case, it is equal to α_2 or $\alpha_2 \oplus 1$ up to a permutation of the variables. Similarly, one can verify that every transitive function of 8 variables has degree at most 3 and each such function of degree 3 is equal to α_3 or $\alpha_3 \oplus 1$ up to a permutation of the variables.

For every Boolean function, one can consider the induced subgraphs of the Boolean cube defined by the sets of vertices $f^{-1}(0)$ and $f^{-1}(1)$. For a transitive function, these graphs are vertex transitive and mutually isomorphic. In general, these graphs need not be connected. For example, for the parity of all variables, these graphs consist of isolated vertices. There are also transitive functions, for which these graphs are connected and not edge transitive.

For the function α_3, the graphs described above are connected graphs on 128 vertices of degree 4 and are isomorphic to the graph C4[128,37] in the census [19], see also [13]. This graph has 256 edges, is edge transitive, although not arc transitive, has girth 4, diameter 8 and the size of the vertex stabilizer is 2.

The function α_4 presented in the next example is a polynomial of degree 4 over GF(2) and is used in Section 6 as an example of a transitive function, which is not simply transitive.

Example 2.11 *There is a uniquely determined function α_4 of $n = 16$ variables satisfying for all $x \in \{0,1\}^n$ the identities*

$$\begin{aligned} \alpha_4(x \oplus \mathrm{e}_1) &= \alpha_4(x^{p_3}) \\ \alpha_4(x \oplus \mathrm{e}_5) &= \alpha_4(x^{p_4}) \\ \alpha_4(x \oplus \mathrm{e}_1 \oplus \mathrm{e}_2 \oplus \mathrm{e}_9 \oplus \mathrm{e}_{10}) &= \alpha_4(x) \oplus 1 \\ \alpha_4(0) &= 0\ , \end{aligned}$$

where the permutations p_3, p_4 in the cycle notation are

$$\begin{aligned} p_3 &= (5,6)(9,16)(10,15)(11,13)(12,14) \\ p_4 &= (1,10,8,15,3,11,5,13,2,9,7,16,4,12,6,14)\ . \end{aligned}$$

Proof. Let $\tau_1 = \tau(p_3^{-1}, \mathrm{e}_1)$, $\tau_2 = \tau(p_4^{-1}, \mathrm{e}_5)$ and $\tau_3 = \tau(\mathrm{id}, \mathrm{e}_1 \oplus \mathrm{e}_2 \oplus \mathrm{e}_9 \oplus \mathrm{e}_{10})$ be the transformations corresponding to the first three identities and let us consider the groups $G = \langle \tau_1, \tau_2, \tau_3 \rangle$ and $H = \langle \tau_1, \tau_2 \rangle$ generated by them. One can verify that G has size 2^{n+2} and is transitive on $\{0,1\}^n$. Group H is not transitive and has two orbits. The transformation τ_3 exchanges these two orbits. Every function satisfying the given identities is constant on the orbits of H and has different values on them. Together with the identity $f(0) = 0$, this implies that the function is the characteristic function of the orbit not containing 0. Hence, α_4 is uniquely determined. Since it has a transitive group of automorphisms, this function is transitive by Lemma 2.3. □

2.4 Weakly symmetric functions

A function f is weakly symmetric, if there is a transitive subgroup G of S_n, such that for every $p \in G$ and every $x \in \{0,1\}^n$, we have

$$f(x^p) = f(x)\ .$$

Although the definition of weakly symmetric and vertex-transitive functions use similar notions, the corresponding classes of the functions are very different. In particular, the number of the vertex-transitive functions is significantly smaller than the number of the weakly symmetric functions. The logarithm to base 2 of the number of the functions, which are invariant, for example, under the group of the cyclic shifts of the n variables, is at least $2^n/n$. On the other hand, the logarithm of the number of vertex-transitive functions is $O(n^2)$ by Theorem 5.1. Moreover, the classes are almost disjoint in the following sense.

Theorem 2.12 *If a non-constant function f satisfies $f(0) = 0$ and is simultaneously weakly symmetric and vertex-transitive, then f is the parity of all variables.*

Proof. For a weakly symmetric function, there is $a \in \{0, 1\}$ such that $f(\mathrm{e}_i) = a$ for all $i = 1, \ldots, n$. Hence, if $f(0) = 0$ and $x = 0$, then for every $i = 1, \ldots, n$, we get

$$f(x \oplus \mathrm{e}_i) = f(x) \oplus a \ .$$

For a vertex-transitive function, if there is a vertex x with this propery for all $i \in \{1, \ldots, n\}$, then all the vertices x of the Boolean cube have this property. If $a = 0$, this implies that the function is the zero function. If $a = 1$, this implies that the function is the parity of all variables. □

2.5 Combining transitive functions by parity

For an arbitrary set $A \subseteq \{1, \ldots, n\}$, let x_A denote the subset of the variables, whose indices belong to A.

Lemma 2.13 *If A and B are disjoint sets of indices of the variables and $f(x_A)$ and $g(x_B)$ are transitive functions, then also $f(x_A) \oplus g(x_B)$ is a transitive function.*

Proof. Let G_A, resp. G_B, be a transitive group of isometric transformations of $\{0, 1\}^A$, resp. $\{0, 1\}^B$, which are automorphisms of $f(x_A)$, resp. $g(x_B)$. Then, the direct product $G_A \times G_B$ considered as a group of isometries of $\{0, 1\}^{A \cup B} = \{0, 1\}^A \times \{0, 1\}^B$ is a transitive group of automorphisms of $f(x_A) \oplus g(x_B)$. □

For a proof of a partial converse of this statement, we use a relationship between the automorphisms of a function and its sensitivity on individual variables.

Definition 2.14 *For any function f of n variables and any i, $1 \leq i \leq n$, let $\sigma(f, i)$ be the sensitivity of the function f on the variable x_i, which is defined as the probability of $f(x \oplus \mathrm{e}_i) \neq f(x)$ or, equivalently, the expected value of $f(x \oplus \mathrm{e}_i) \oplus f(x)$ as a real number, where x is chosen at random from the uniform distribution on $\{0, 1\}^n$.*

For every f and i, $0 \leq \sigma(f, i) \leq 1$ and $\sigma(f, i) = 0$, if and only if f does not depend on x_i.

Lemma 2.15 *The function f satisfies $\sigma(f, i) = 1$, if and only if there is a function $g(x_A)$, where $i \notin A$, such that $f(x) = g(x_A) \oplus x_i$.*

Proof. The sensitivity of f on x_i is σ, if and only if the sensitivity of $g = f \oplus x_i$ on x_i is $1 - \sigma$. □

Lemma 2.16 *Let f be a function of n variables and let $\tau = \tau(p, s)$ for some $p \in S_n$, $s \in \{0,1\}^n$ be an automorphism of f. If $p(i) = j$, then the function f has the same sensitivity on the variables x_i and x_j.*

Proof. For some $a \in \{0,1\}$ and for all x, we have

$$f(x^p \oplus s) = f(x) \oplus a$$

and substituting $x \oplus \mathrm{e}_i$ for x in both sides of this identity yields

$$f(x^p \oplus s \oplus \mathrm{e}_j) = f(x \oplus \mathrm{e}_i) \oplus a \ .$$

Together, this implies

$$f(x^p \oplus s \oplus \mathrm{e}_j) \oplus f(x^p \oplus s) = f(x \oplus \mathrm{e}_i) \oplus f(x) \ .$$

Since the mapping $x \mapsto x^p \oplus s$ preserves the uniform distribution on $\{0,1\}^n$, the lemma follows. □

Assume, the variables of a transitive function f are splitted into the sets x_A and x_B and the sensitivity of every variable in x_A is different from the sensitivity of every variable in x_B. Then, for every automorphism $\tau = \tau(p, s)$ of f, the permutation p preserves the sets A and B. In other words, the automorphism group of f is a subgroup of the direct product $T_A \times T_B$.

Lemma 2.17 *Let A and B be disjoint sets of indices of the variables and let f, g_A and g_B be non-constant Boolean functions satisfying $f(x_A, x_B) = g_A(x_A) \oplus g_B(x_B)$. Let f be transitive and let G be a group of automorphisms of f, which is transitive on $\{0,1\}^{A \cup B}$. If G is a subgroup of $T_A \times T_B$, then $g_A(x_A)$ and $g_B(x_B)$ are transitive functions.*

Proof. By symmetry, it is sufficient to prove transitivity of g_A. Let G_A be the projection of G to the first component of the direct product $T_A \times T_B$. Since G is transitive on $\{0,1\}^{A \cup B}$, G_A is transitive on $\{0,1\}^A$.

Let $\tau \in G$ and let $\tau = (\tau_A, \tau_B)$, where $\tau_A \in T_A$ and $\tau_B \in T_B$. Since τ is an automorphism of f, there is $c \in \{0,1\}$, such that for every $x_A \in \{0,1\}^A$ and $x_B \in \{0,1\}^B$, we have

$$f(\tau(x_A, x_B)) = f(x_A, x_B) \oplus c$$

and, hence,

$$g_A(\tau_A(x_A)) \oplus g_B(\tau_B(x_B)) = g_A(x_A) \oplus g_B(x_B) \oplus c \ .$$

Let $u_B \in \{0,1\}^B$ be fixed and let $c' = g_B(\tau_B(u_B)) \oplus g_B(u_B) \oplus c$. Then, for every $x_A \in \{0,1\}^A$, we have

$$g_A(\tau_A(x_A)) = g_A(x_A) \oplus c' \ .$$

Consequently, τ_A is an automorphism of g_A. Since this is satisfied for every element of G, G_A consists of automorphisms of g_A and, hence, g_A is a transitive function. □

Theorem 2.18 *Let A and B be disjoint sets of indices of the variables and let $g(x_A)$ be an arbitrary Boolean function. Then, $g(x_A) \oplus \mathrm{par}(x_B)$ is transitive if and only if $g(x_A)$ is transitive.*

Proof. Without loss of generality, we can assume that g depends on all variables in x_A. If $g(x_A)$ is transitive, then the statement follows from Lemma 2.13. For the opposite direction, assume that $f(x_A, x_B) = g(x_A) \oplus \mathrm{par}(x_B)$ is transitive and consider two cases as follows.

For the first case, assume that the sensitivity of $g(x_A)$ on all x_i, $i \in A$, is less than 1. The sensitivity of $f(x_A, x_B)$ on the variables from x_A is the same as the sensitivity of $g(x_A)$ and the sensitivity on the variables in x_B is 1. Let G be a group of automorphisms of $f(x_A, x_B)$, which is transitive on $\{0,1\}^{A \cup B}$. If $\tau(p, s) \in G$, then by Lemma 2.16, the permutation p preserves each of the sets A and B. Hence, G is a subgroup of the direct product $T_A \times T_B$ and by Lemma 2.17, τ_A is an automorphism of $g(x_A)$, which finishes the first case of the proof.

If g has sensitivity 1 for some variables in x_A, let D be the set of their indices and let C be the set of the indices of the variables from A, for which the sensitivity of g is less than 1. Consider the decomposition

$$g(x_A) = g'(x_C) \oplus \mathrm{par}(x_D)$$

obtained by a repeated application of Lemma 2.15 to the function g. The function g' satisfies the assumption of the first case of the proof. It follows that g is transitive, if and only if g' is transitive and, similarly, the function

$$f(x_A, x_B) = g'(x_C) \oplus \mathrm{par}(x_D) \oplus \mathrm{par}(x_B)$$

is transitive, if and only if g' is transitive. Consequently, the theorem holds also in the general case. □

3 Further constructions of transitive functions

3.1 Characterization of quadratic transitive functions

Any multivariate quadratic polynomial $f(x)$ over GF(2), which satisfies $f(0) = 0$, can be written as

$$f(x) = x^t U x \oplus c^t x \ , \tag{10}$$

where U is an appropriate upper triangular matrix with zeros on the diagonal and c is a column vector. It is useful to consider also the matrix $Q = U \oplus U^t$, which is symmetric and represents the adjacency matrix of a graph, whose edges correspond to the products contained in the polynomial.

Lemma 3.1 *If f is a quadratic polynomial in the form (10), $Q = U \oplus U^t$ and $s \in \{0,1\}^n$, then for every x, we have*

$$f(x \oplus s) = f(x) \oplus s^t Q x \oplus f(s) \ .$$

Proof. Using (10), we obtain

$$f(x \oplus s) = (x \oplus s)^t U (x \oplus s) \oplus c^t (x \oplus s) \ .$$

Expanding the right hand side, we obtain 6 terms, which can be combined to the three expressions

$$\begin{aligned} x^t U x \oplus c^t x &= f(x) \\ s^t U x \oplus x^t U s = s^t U x \oplus s^t U^t x &= s^t Q x \\ s^t U s \oplus c^t s &= f(s) \ . \end{aligned}$$

The lemma follows. □

Definition 3.2 A quadratic polynomial f of $n = 2k$ variables is called special, if there is a homogeneous quadratic polynomial g of k variables, such that

$$f(x) = g(x_1 \oplus x_2,\, x_3 \oplus x_4,\, \ldots,\, x_{n-1} \oplus x_n) \oplus \bigoplus_{i=1}^{k} x_{2i} \ .$$

Special quadratic polynomials can also be characterized by the form of the corresponding matrix $Q = U \oplus U^t$. Let Π be the partition of the set of the indices of the n variables into k two-element blocks $\{1,2\}, \{3,4\}, \ldots, \{n-1, n\}$. Consider the matrix Q as a block matrix by partitioning both the rows and the columns according to Π into $k \times k$ blocks of size 2×2. Also, consider the vector c splitted to k blocks of length 2 according to Π. A quadratic polynomial in the form (10) is a special quadratic polynomial, if and only if the following conditions are satisfied

- the diagonal blocks of Q are zero,
- the components of every non-diagonal block of Q are either all 0 or all 1,
- the vector c consists of k blocks of the form $(0,1)$.

Lemma 3.3 *Every special quadratic polynomial is transitive.*

Proof. Let f be a special quadratic polynomial of $n = 2k$ variables, let U and c be as in (10) and let $Q = U \oplus U^t$.

In order to prove that f is a transitive function, we prove that for every $i = 1, \ldots, n$, the function $f(x \oplus \mathrm{e}_i)$ has the form (3). By Lemma 3.1, we have

$$f(x \oplus \mathrm{e}_i) = f(x) \oplus \mathrm{e}_i^t Q x \oplus f(\mathrm{e}_i) \ .$$

This implies that $f(x \oplus \mathrm{e}_i)$ has the same quadratic terms as f and possibly differs in the linear and constant terms. The linear part of $f(x \oplus \mathrm{e}_i)$ is $(c^t \oplus \mathrm{e}_i^t Q)x$. Since Q is a symmetric matrix, this is $(c \oplus Q\mathrm{e}_i)^t x$. Due to the block structure of Q and c described above, the vector $c' = (c \oplus Q\mathrm{e}_i)^t$ consists of k blocks, each of which is either $(0,1)$ or $(1,0)$. Let q_i be the permutation, which exchanges the indices in the blocks $\{2j-1, 2j\}$, $j \in \{1, \ldots, k\}$, where c' is equal to $(1, 0)$. Clearly, $c' = c^{q_i}$. Let us prove

$$f(x \oplus \mathrm{e}_i) = f(x^{q_i}) \oplus f(\mathrm{e}_i) \ .$$

Since f is a special quadratic polynomial, its quadratic part is invariant under the permutation q_i of the variables, so the quadratic terms are the same on both sides. Since $c' = c^{q_i}$, the coefficients of the linear terms are given by c' on both sides, so they are also equal. Since also the constant terms coincide, the function f is transitive by Theorem 2.5 and identities (3). □

Lemma 3.4 *The sensitivity of a quadratic polynomial on any variable is* 0*,* 1/2*, or* 1*.*

Proof. The sensitivity of f on the variable x_i is equal to the probability of $f(x \oplus \mathrm{e}_i) \oplus f(x) \neq 0$ for x chosen from the uniform distribution on $\{0,1\}^n$. If f is quadratic, then for every i, the function $f(x \oplus \mathrm{e}_i) \oplus f(x)$ is a linear function over GF(2). Hence, the probability of $f(x \oplus \mathrm{e}_i) \oplus f(x) \neq 0$ is 0, 1/2, or 1 as required. □

Recall that the sensitivity of f on the variable x_i is denoted $\sigma(f, i)$ for $i \in \{1, \ldots, n\}$. The sensitivity of a function in a vertex is defined as follows.

Definition 3.5 The sensitivity of a function f in a vertex $x \in \{0,1\}^n$ will be denoted $\sigma(f, x)$ and defined as the number of indices $i = 1, \ldots, n$, such that $f(x \oplus \mathrm{e}_i) \neq f(x)$.

Let $\sigma(f)$ be the maximum of $\sigma(f, x)$ over all $x \in \{0,1\}^n$. Clearly, for a transitive function f, the sensitivity $\sigma(f, x)$ is the same for all vertices x. Hence, $\sigma(f)$ is also the average value of the sensitivity over all vertices. Due to this, we have

$$\sigma(f) = \frac{1}{2^n} \sum_x \sigma(f, x) = \frac{1}{2^n} \sum_x \sum_i \mathrm{ind}(f(x \oplus \mathrm{e}_i) \neq f(x)) \ ,$$

where ind is the indicator function for a condition. Since

$$\sigma(f, i) = \frac{1}{2^n} \sum_x \mathrm{ind}(f(x \oplus \mathrm{e}_i) \neq f(x)) \ ,$$

we finally have

$$\sigma(f) = \sum_{i=1}^{n} \sigma(f, i) \ . \tag{11}$$

Lemma 3.6 *If f is a quadratic transitive function (10) of n variables, which has sensitivity* 1/2 *on every variable, then for every $s \in \{0,1\}^n$, the vector $c \oplus Qs$ contains $n/2$ non-zero components.*

Proof. By the assumption, for all $i = 1, \ldots, n$, $\sigma(f, i) = 1/2$. Hence, (11) implies $\sigma(f) = n/2$. Since f is transitive, we have $\sigma(f) = \sigma(f, s)$ for all $s \in \{0, 1\}^n$. In particular, $n/2$ is an integer. The sensitivity $\sigma(f, s)$ is equal to the sensitivity in the zero vertex of $f(x \oplus s)$ as a function of x. The sensitivity of a polynomial in the zero vertex is equal to the number of its nonzero linear terms. By Lemma 3.1, the linear part of $f(x \oplus s)$ is

$$c^t x \oplus s^t Q x = (c \oplus Qs)^t x \ .$$

Hence, the number of non-zero components of the vector $c \oplus Qs$ is $n/2$ as required. □

For every $0, 1$-matrix M, let $\mathcal{A}(M)$ be the affine set generated by the affine combinations of the rows of M over GF(2), which are the linear combinations, whose sum of the coefficients is 1. Equivalently, $\mathcal{A}(M)$ is the set of the sums of odd size subsets of the rows of M. Every affine subset A of a vector space can be obtained as $a + W$, where a is an element of A and W is the linear subspace formed by the differences of the elements of A. The dimension of W will be called the dimension of the affine set A. For a subset A of $\{0, 1\}^n$ and $p \in S_n$, let A^p be the set of x^p for $x \in A$.

Lemma 3.7 *If A is an affine subset of $\{0, 1\}^n$, whose elements have $n/2$ nonzero components, then there is a permutation $p \in S_n$, such that the affine set A^p is a subset of the solutions of the system of the linear equations*

$$\begin{array}{lcl} x_1 \oplus x_2 & = & 1 \\ x_3 \oplus x_4 & = & 1 \\ \cdots & & \\ x_{n-1} \oplus x_n & = & 1 \ . \end{array} \tag{12}$$

Proof. Let k be the smallest number of affine generators of A and let $B = \{b_{i,j}\}$, where $i = 1, \ldots, k$ and $j = 1, \ldots, n$, be a $k \times n$ matrix, whose rows form such a system of the generators. In particular, $A = \mathcal{A}(B)$. Moreover, let $b_1, \ldots, b_n \in \{0, 1\}^k$ be the columns of B.

Let $L = \{\ell_{I,y}\}$ be the $2^k \times 2^k$ matrix, such that the row indices I are subsets of $\{1, \ldots, k\}$ and the column indices y are vectors $y \in \{0, 1\}^k$. The rows are linear functions over the column index specified by the row index. More exactly, for every I and y, we have

$$\ell_{I,y} = \bigoplus_{i \in I} y_i \ .$$

Let $H = \{h_{I,y}\}$ be the matrix, whose elements are

$$h_{I,y} = (-1)^{\ell_{I,y}} \ .$$

The matrix H is a Hadamard matrix known as Sylvester's construction.

The set of the rows of L is a linear space over GF(2), whose elements are vectors of length 2^k with components indexed by $\{0, 1\}^k$. Let $\phi : L \to \{0, 1\}^n$ be defined for every row z of L as

$$\phi(z) = (z_{b_1}, \ldots, z_{b_n}) \ . \tag{13}$$

For every I, let ℓ_I be the row of L with index I. Let V be the set of k rows $\ell_{\{i\}}$ for $i = 1, \ldots, k$. The rows in V represent the linear functions depending on a single bit of the column index y. Using this, one can verify that $\phi(\ell_{\{i\}})$ is the i-th row of the matrix B, since

$$\phi(\ell_{\{i\}}) = (\ell_{\{i\},b_1}, \ldots, \ell_{\{i\},b_n}) = (b_{i,1}, \ldots, b_{i,n}) \ .$$

This implies that ϕ maps V to the rows of B and, hence, also maps the affine set $\mathcal{A}(V)$ onto the affine set $A = \mathcal{A}(B)$. Since the dimension of both these affine sets is $k-1$, the linear map ϕ is a bijection between $\mathcal{A}(V)$ and $A = \mathcal{A}(B)$.

By the assumption, for every $z \in \mathcal{A}(V)$, the vector $\phi(z) \in A$ has $n/2$ components equal to one. Since $\phi(z)$ is defined by (13) as a selection of some of the components of z, possibly with repetitions, the number of ones in $\phi(z)$, denoted as $|\phi(z)|$, can be expressed by the scalar product in the real numbers

$$|\phi(z)| = w \cdot z \ , \tag{14}$$

where w is an integer vector, whose components are given by

$$w_y = |\{j \in \{1, \ldots, n\};\ b_j = y\}| \ . \tag{15}$$

Clearly,

$$\sum_{y \in \{0,1\}^k} w_y = n \ . \tag{16}$$

Lemma 3.8 *For every $y \in \{0,1\}^k$, we have $w_{\overline{y}} = w_y$, where $\overline{y}$ is the componentwise complement of y.*

Proof. Since H has the full rank over the real numbers, the vector w is a linear combination of the rows of H. Consider any row z' of H and the corresponding row z of L, so we have in the real numbers

$$z' = 1 - 2z \ ,$$

where 1 denotes the vector of all ones. If $z \in \mathcal{A}(V) \subseteq L$, then $\phi(z) \in A$ and we have $|\phi(z)| = n/2$ by the assumption. Using (14) and (16), we obtain

$$w \cdot z' = n - 2\,(w \cdot z) = 0 \ .$$

Since H is an orthogonal matrix, this implies that w is a linear combination over the real numbers of the rows of H, which do not correspond to the rows $\mathcal{A}(V)$ of L. Since the rows in V are the linear functions over GF(2) of a single bit of y, the set $\mathcal{A}(V)$ consists exactly of the linear functions, which are the parity of an odd number of the bits of y. Hence, the rows of L, which do not belong to $\mathcal{A}(V)$, are the parities of an even number of the bits of y. The parity of an even number of the bits is the same for y and $\overline{y}$. Hence, if z is a row of L, which is not in $\mathcal{A}(V)$, then $z_{\overline{y}} = z_y$ for all $y \in \{0,1\}^k$. Clearly, the same is satisfied for the row $1 - 2z$ of H. Since all the rows of H, which contribute to the expression of w, satisfy this symmetry, the lemma follows. □

Lemma 3.8 and (15) imply that for every y, the number of the occurences of the column y in B is equal to the number of the occurences of the column $\overline{y}$. Hence, there is a permutation $p \in S_n$, such that the n columns of B^p form $n/2$ pairs of complementary consecutive columns. Hence, if x is a row of B^p, the equations (12) are satisfied. These identities clearly extend to the elements of $\mathcal{A}(B^p)$. Since $A^p = \mathcal{A}(B^p)$, the proof of Lemma 3.7 is completed. □

The main result of this section is the following theorem and its corollary.

Theorem 3.9 *If f is a transitive function defined by a quadratic polynomial (10) of n variables, which has sensitivity $1/2$ on each variable, then there is $p \in S_n$, such that $f(x) = g(x^p)$ for a special quadratic polynomial g.*

Proof. Let U be as in (10) and let $Q = U \oplus U^t$. By Lemma 3.6, the affine set

$$A = \{c \oplus Qs\,;\, s \in \{0,1\}^n\}$$

satisfies the assumptions of Lemma 3.7. Let p be the permutation guaranteed by Lemma 3.7. The elements of A^p satisfy (12). In particular, c^p satisfies these identities. Hence, if the vector c^p is splitted into blocks of size 2 according to Π, it consists of the blocks $(0,1)$ and $(1,0)$. Since the equations (12) are invariant under exchanging the variables in any block, we can choose p so that $c' = c^p$ has the form $(0,1,0,1,\ldots,0,1)$. Let Q' be the matrix obtained by reordering of both the columns and the rows of Q according to p. The matrix Q' is a symmetric matrix with zero diagonal, since Q has these properties. Let U' be the upper triangular part of Q' and let g be the function

$$g(x) = x^t U' x \oplus (c')^t x\ .$$

One can easily verify that $g(x^p) = f(x)$ for every x.

The sum in GF(2) of $c' = (0,1,\ldots,0,1)^t$ and any column of Q' belongs to A^p. Hence, if any column of Q' is splitted according to Π, it consists of the blocks $(0,0)$ and $(1,1)$. It follows that the matrix Q' consists of $n/2$ pairs of equal consecutive rows. Since it is symmetric, it consists of $n/2 \times n/2$ blocks of dimension 2×2, each of which contains either all ones or all zeros. Moreover, the diagonal blocks are zero, since the diagonal of the matrix is zero. Hence, Q', U' and c' have the form, which implies that g is a special quadratic polynomial as required. □

Corollary 3.10 *A quadratic polynomial defines a transitive function, if and only if it can be obtained from a special quadratic polynomial by a permutation of the variables and possibly removing irrelevant ones.*

Proof. A polynomial obtained in the specified way defines a transitive function by Lemma 3.3. For the opposite direction, let f be a transitive function defined by quadratic polynomial, which depends on all its variables. By a repeated application of Lemma 2.15, we can split the indices of the variables into disjoint sets A and B, such that $f(x) = g(x_A) \oplus \mathrm{par}(x_B)$ and g has sensitivity less than 1 on all its variables. By Lemma 3.4, g has sensitivity $1/2$ on all its variables. Moreover, by Theorem 2.18, the function $g(x_A)$ is transitive. Hence, by Theorem 3.9, g is a special quadratic polynomial up to a permutation of the variables. The function $\mathrm{par}(x_B)$ can be expressed as a special quadratic polynomial of $2|B|$ variables, which depends only on $|B|$ of them and contains no quadratic terms. Since the parity of two special quadratic polynomials on disjoint sets of variables is a special quadratic polynomial, the theorem follows. □

3.2 Transitive functions of an arbitrary degree

Let α_2 be the quadratic transitive function from Example 2.9.

Lemma 3.11 *For $i = 1, 2$, let g_i be a transitive function of k_i variables and degree d_i. For $i = 1, 2$ and $j = 1, 2$, let $x_{i,j}$ be a vector of k_i variables, such that the sets of variables in the four vectors $x_{i,j}$ are mutually disjoint. Then, $\alpha_2(g_1(x_{1,1}), g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2}))$ is a transitive function of $2(k_1+k_2)$ variables and degree $d_1 + d_2$.*

Proof. The concatenation of all the blocks $x_{i,j}$ will be denoted as x. Let f be the considered function, so we have

$$f(x) = f(x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}) = \alpha_2(g_1(x_{1,1}), g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2})) \ .$$

Let $\mathrm{e}_{i,j,l}$ be the standard basis vector of length $2(k_1 + k_2)$, which contains 1 at the l-th position of the block corresponding to $x_{i,j}$. In order to prove transitivity of f using Theorem 2.5 and identities (3), we show that for every i, j, l, there is a permutation $p \in S_{2(k_1+k_2)}$ and $a \in \{0, 1\}$ such that

$$f(x \oplus \mathrm{e}_{i,j,l}) = f(x^p) \oplus a \ . \tag{17}$$

If $(i, j) = (1, 1)$, then we consider $\mathrm{e}_{1,1,l}$, which has 1 at the l-th position of the block $x_{1,1}$ and is zero in all other blocks. Hence, we have

$$f(x \oplus \mathrm{e}_{1,1,l}) = \alpha_2(g_1(x_{1,1} \oplus \mathrm{e}_l), g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2})) \ .$$

Since g_1 is a transitive function, there are $q \in S_{k_1}$ and $b \in \{0, 1\}$, such that

$$g_1(x_{1,1} \oplus \mathrm{e}_l) = g_1(x^q_{1,1}) \oplus b \ ,$$

which implies

$$f(x \oplus \mathrm{e}_{1,1,l}) = \alpha_2(g_1(x^q_{1,1}) \oplus b, g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2})) \ .$$

If $b = 0$, this implies

$$f(x \oplus \mathrm{e}_{1,1,l}) = f(x^q_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}) \ ,$$

which has the required form (17). If $b = 1$, we additionally use (6) to obtain

$$f(x \oplus \mathrm{e}_{1,1,l}) = \alpha_2(g_1(x^q_{1,1}), g_1(x_{1,2}), g_2(x_{2,2}), g_2(x_{2,1}))$$

and, finally,

$$f(x \oplus \mathrm{e}_{1,1,l}) = f(x_{1,1}^{q}, x_{1,2}, x_{2,2}, x_{2,1}) \ ,$$

which has the form (17).

If $(i,j) = (1,2)$, then we consider $\mathrm{e}_{1,2,l}$, which has 1 at the l-th position of the block $x_{1,2}$ and is zero in all other blocks. Similarly as in the previous case, we obtain

$$f(x \oplus \mathrm{e}_{1,2,l}) = \alpha_2(g_1(x_{1,1}), g_1(x_{1,2}^{q}) \oplus b, g_2(x_{2,1}), g_2(x_{2,2}))$$

with $q \in S_{k_1}$ and $b \in \{0,1\}$ guaranteed by identities (3) for g_1. If $b = 0$, this can be rewritten to the form (17) as in the previous case. If $b = 1$, we use (7) to obtain

$$f(x \oplus \mathrm{e}_{1,2,l}) = \alpha_2(g_1(x_{1,1}), g_1(x_{1,2}^{q}), g_2(x_{2,2}), g_2(x_{2,1})) \oplus 1 \ ,$$

and, finally,

$$f(x \oplus \mathrm{e}_{1,2,l}) = f(x_{1,1}, x_{1,2}^{q}, x_{2,2}, x_{2,1}) \oplus 1 \ ,$$

which has the form (17).

The cases $(i,j) = (2,1)$ and $(i,j) = (2,2)$ are similar and left to the reader. □

Theorem 3.12 *For every integer $d \geq 1$, there is a transitive function of at most $2d^2$ variables represented by a polynomial over* GF(2) *of degree d.*

Proof. Consider a binary tree with d leaves and the depth $k = \lceil \log_2 d \rceil$. We assign a transitive function to every node in the tree as follows. The leaves are assigned to different variables. An internal node, both successors of which are already assigned, is assigned to the function obtained by the previous lemma from the functions in the two successors. This is repeated until the function assigned to the root of the tree is obtained. It is easy to see that the degree of this function is d and the number of the variables of this function is at most $d2^k \leq 2d^2$. □

3.3 Transitive functions with small sensitivity

Let us consider the sensitivity and the block sensitivity of Boolean functions. Both these sensitivities are first defined in every vertex of the Boolean cube and the sensitivity of the function is the maximum of the corresponding sensitivity over all vertices, see [12], Chapter 14.3 or, for example, [1]. For the sensitivity of f in a vertex x see also Definition 3.5.

The block sensitivity of f in a vertex x is the maximum number m, such that there are vectors v_j, $j = 1, \ldots, m$, such that the sets of indices of non-zero components in these vectors are pairwise disjoint and for every $j = 1, \ldots, m$, we have $f(x \oplus v_j) \neq f(x)$. The sets of non-zero positions in the vectors v_j will be called the sensitive blocks for f in x. Clearly, the block sensitivity in a vertex is at least the sensitivity in the vertex, since the vectors v_j can be the vectors e_i, for which $f(x \oplus \mathrm{e}_i) \neq f(x)$. For a transitive function, the block sensitivity is the same in all the vertices, so the maximum is also the common value, similarly as for the sensitivity.

A certificate for the value $f(x)$ in an input x is any set C of indices of the components of x, such that every vector y satisfying $f(y) \neq f(x)$ differs from x in at least one position with index in C. The certificate complexity of f in the input x is the smallest size of a certificate for the value $f(x)$, see [12, 1]. For a transitive function, the certificate complexity is the same for all $x \in \{0,1\}^n$ and this common value will be called the certificate complexity of the function.

In order to present a transitive function with sensitivity and block sensitivity logarithmic in the number of the variables, let us prove additional properties of the construction from Lemma 3.11.

Lemma 3.13 *For $i = 1, 2$, let g_i be a transitive function of k_i variables, sensitivity s_i, block sensitivity b_i and certificate complexity c_i. Let g be the combined function of $2(k_1 + k_2)$ variables as in Lemma 3.11 and let s, b and c denote its sensitivity, block sensitivity and certificate complexity in this order. Then, we have*

$$\begin{array}{rcl} s & = & s_1 + s_2 \\ b & \geq & b_1 + b_2 + \min\{b_1, b_2\} \\ c & \leq & c_1 + c_2 + \min\{c_1, c_2\} \ . \end{array}$$

Proof. Since g_1, g_2 and g are transitive functions, it is sufficient to consider their sensitivity, block sensitivity and certificate complexity in the zero vector. Consider the value of

$$g(x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}) = \alpha_2(g_1(x_{1,1}), g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2}))$$

in the zero vector and in a vector obtained from the zero vector by changing a single bit to 1. These values differ, if and only if the change of the bit changes either the value of $g_1(x_{1,2})$ or the value of $g_2(x_{2,2})$. There are $s_1 + s_2$ bit positions, whose change has this effect.

In order to prove the required bound on b, choose $b_1 + b_2$ disjoint sensitive blocks for the functions $g_1(x_{1,2})$ and $g_2(x_{2,2})$ in the zero vector. These blocks are disjoint sensitive blocks also for g. Moreover, consider some collection of $\min\{b_1, b_2\}$ disjoint sensitive blocks for $g_1(x_{1,1})$ and a collection of the same number of disjoint sensitive blocks for $g_2(x_{2,1})$. Take the unions of pairs of these blocks, one for $g_1(x_{1,1})$ and the other for $g_2(x_{2,1})$, so that each block from the two collections is used exactly once. This yields additional $\min\{b_1, b_2\}$ disjoint sensitive blocks for g.

In order to prove the required bound on c, consider a certificate for the 0 value in the zero vector for each of the functions $g_1(x_{1,2})$ and $g_2(x_{2,2})$. Moreover, consider the shorter of the certificates for the value 0 for $g_1(x_{1,1})$ and $g_2(x_{2,1})$. The union of these three certificates is a certificate for $g(0) = 0$ of total size $c_1 + c_2 + \min\{c_1, c_2\}$. □

Let β_i and γ_i be the sequences of functions defined by the recursions

$$\begin{array}{rcl} \beta_0 & = & x \\ \beta_{i+1} & = & \alpha_2(\beta_i^{(1)}, \beta_i^{(2)}, \beta_i^{(3)}, \beta_i^{(4)}) \end{array}$$

and

$$\begin{aligned}\gamma_0 &= x\\ \gamma_{i+1} &= \alpha_2(\gamma_i^{(1)}, \gamma_i^{(2)}, x^{(1)}, x^{(2)})\ ,\end{aligned}$$

where x denotes a single variable and the upper indices distinguish distinct variables or copies of a function depending on disjoint sets of variables. Note that $\beta_1 = \gamma_1 = \alpha_2$.

Theorem 3.14 *For every $i \geq 0$, the function β_i is a transitive function of $n = 4^i$ variables with sensitivity $2^i = n^{1/2}$ and block sensitivity $3^i \approx n^{0.7925}$.*

Proof. Transitivity of β_i and the number of the variables of this function follow by induction using Lemma 3.11. The remaining properties can be easily verified for β_0 and β_1. For $i \geq 2$, the sensitivity of β_i can be obtained by a straightforward induction using Lemma 3.13 with $g_1 = g_2 = \beta_i$. In order to obtain the block sensitivity of β_i, let us consider also its certificate complexity, which is known to be an upper bound on block sensitivity. Using this and Lemma 3.13, we get by induction $3^i \leq b_i \leq c_i \leq 3^i$. □

Theorem 3.15 *For every $i \geq 0$, the function γ_i is a transitive function of $n = 3 \cdot 2^i - 2$ variables with sensitivity $i + 1 = \Theta(\log n)$ and block sensitivity $2i + 1 = \Theta(\log n)$.*

Proof. Transitivity of γ_i and the number of the variables of this function follow by induction using Lemma 3.11. The remaining properties can be easily verified for γ_0 and γ_1. For $i \geq 2$, a similar approach as in the proof of the previous theorem can be used. In this case, Lemma 3.13 is used with $g_1 = \gamma_i$ and g_2 equal to a single variable. □

4 Groups of automorphisms

In Section 2.2, a transitive function was defined as a Boolean function, which satisfies a system of identities corresponding to a transitive group of automorphisms of the function. In this section, we investigate the properties of these groups themselves. As already mentioned, an isometry $\tau \in T_n$ is an automorphism of f, if the partition of the vertices of the Boolean cube into the sets $f^{-1}(0)$ and $f^{-1}(1)$ is invariant under τ.

A block for a group G of permutations of a domain Ω is a non-empty subset $B \subseteq \Omega$, such that for every $\pi \in G$, we have either $B^\pi = B$ or $B^\pi \cap B = \emptyset$, where $B^\pi = \{b^\pi\, ;\, b \in B\}$. A block system for G is a partition of Ω, which is preserved by G. Clearly, the elements of a block system are blocks in the sense above. If G is transitive on Ω and B is a block, then the sets B^π for $\pi \in G$ are blocks and the set of the different blocks of this form is a partition of Ω. Moreover, this partition is preserved by G and, hence, is a block system. These considerations are the basis for part (i) of Lemma 4.1, which summarizes well-known facts used later. Part (iii) is used only for groups satisfying $|G : H| = 2$. For more information on block systems for the permutation groups, see, for example, [5, 11, 7].

Lemma 4.1 *Let G be a transitive group of permutations of a domain Ω and $u \in \Omega$. Then, the following three statements hold.*

(i) Every block system for G is uniquely specified by the block in it, which contains u.

(ii) A subset B of Ω containing u is a block of G, if and only if $B = \mathrm{Orbit}_H(u)$ for a subgroup H, which contains $\mathrm{Stab}_G(u)$. Moreover, there is a bijection between the blocks of G, which contain u, and the subgroups H of G, which contain $\mathrm{Stab}_G(u)$.

(iii) If H is a normal subgroup of G, then the orbits of H form a block system of G. In particular, the orbits of H have the same size.

Lemma 4.2 *A non-constant function f of n variables is transitive, if and only if there is a transitive group $G \leq T_n$, such that the partition of $\{0,1\}^n$ to the sets $\{f^{-1}(0), f^{-1}(1)\}$ is a block system of G.*

Proof. Let f be transitive. Clearly, the group generated by the isometries, which appear as τ in (2), is a transitive subgroup of T_n satisfying the requirement.

For the opposite direction, let f be any non-constant function of n variables and G a transitive subgroup of T_n, for which the partition $\{f^{-1}(0), f^{-1}(1)\}$ is a block system. Let $s \in \{0,1\}^n$ be arbitrary. Since G is transitive, there is $\tau \in G$, such that $\tau(0) = s$. Since τ satisfies (2) for some $a \in \{0,1\}$, f is transitive by Definition 2.1. □

A transitive group can have several two-element block systems and they define different transitive functions. The parity of all variables represents a block system for T_n and, clearly, also for any of its subgroups. Hence, a transitive group of automorphisms of any function except of the parity of all variables admits at least two different two element block systems. A unique block system can be specified by considering the subgroup H of G, which is the set-wise stabilizer of the blocks. Clearly, H is not transitive and for every $\tau \in H$ and $x \in \{0,1\}^n$, we have $f(\tau(x)) = f(x)$.

Lemma 4.3 *Let G and H be groups of isometries of $\{0,1\}^n$ such that*

- *G is transitive,*
- *$H \leq G$, $|G : H| = 2$,*
- *H is not transitive.*

Then, for every vertex u, we have $|\mathrm{Orbit}_H(u)| = 2^{n-1}$ and $\mathrm{Stab}_G(u) \leq H$. Consequently, H has two orbits and they form a block system of G.

Proof. Let G and H be groups satisfying the assumptions and let $u \in \{0,1\}^n$. Since $|G : H| = 2$, H is normal in G and by Lemma 4.1(iii), the orbits of H form a block system of G. The orbit-stabilizer theorem implies

$$|\mathrm{Orbit}_G(u)| = \frac{|G|}{|\mathrm{Stab}_G(u)|} = 2^n$$

and

$$|\mathrm{Orbit}_H(u)| = \frac{|H|}{|\mathrm{Stab}_H(u)|} = \frac{|G|}{2\,|\mathrm{Stab}_H(u)|}\ .$$

Since $\mathrm{Stab}_H(u) = H \cap \mathrm{Stab}_G(u)$, we have either $\mathrm{Stab}_H(u) = \mathrm{Stab}_G(u)$ or $|\mathrm{Stab}_H(u)| \le \frac{1}{2}|\mathrm{Stab}_G(u)|$. In the latter case, we would have $|\mathrm{Orbit}_H(u)| = 2^n$, which is not possible, since H is intransitive. Hence, $\mathrm{Stab}_H(u) = \mathrm{Stab}_G(u)$, which implies $|\mathrm{Orbit}_H(u)| = 2^{n-1}$ and $\mathrm{Stab}_G(u) \le H$. □

This lemma implies correctness of the following definition.

Definition 4.4 Let f be a non-constant Boolean function of n variables and let G and H be subgroups of T_n such that

- G is transitive,
- $H \le G$, $|G : H| = 2$,
- for every $\tau \in H$ and $x \in \{0,1\}^n$, we have $f(\tau(x)) = f(x)$.

Moreover, if $u \in \{0,1\}^n$, such that $f(u) = 0$, then, we say that G, H and u define f.

By Lemma 4.3, H has two orbits and the function is constant on each of them. Hence, the function is uniquely determined. Moreover, the functions, which can be defined in this way, are exactly the transitive functions.

Theorem 4.5 *A non-constant Boolean function is transitive, if and only if it is defined by some subgroups G and H of T_n and a vertex $u \in \{0,1\}^n$.*

Proof. Assume, G, H, and u define a function f. By Lemma 4.3, H has two orbits and they form a block system of G. Since f is constant on each of these blocks, it is transitive by Lemma 4.2.

Let f be a non-constant transitive function. By Lemma 4.2, the partition $\{f^{-1}(0), f^{-1}(1)\}$ is a block system for a transitive group G of isometries. Let H be the set-wise stabilizer of $f^{-1}(0)$ and let u be any element of $f^{-1}(0)$. One can easily verify that the groups G, H, and vertex u define f. □

A minimally transitive group is a permutation group, which is transitive, but no its proper subgroup is transitive.

Lemma 4.6 *For every non-constant transitive function f, there are groups G and H and a vertex u, which define f, and G is minimally transitive.*

Proof. If f is transitive, then Theorem 4.5 guarantees the existence of groups G and H and a vertex u, which define f. If G is not minimally transitive, let G' be a minimally transitive subgroup of G and $H' = H \cap G'$. Since H' is intransitive, it follows that $|G' : H'| > 1$. Moreover, since $|G' : H'| \le |G : H|$, we have $|G' : H'| = 2$. Clearly, $f(\tau(x)) = f(x)$ for every $\tau \in H'$. Hence, the groups G' and H' define the same function as the groups G and H. □

The minimally transitive groups G satisfy further conditions, which are based on the following consequence of a more general Theorem 3.4 from [17].

Theorem 4.7 (Wielandt, 1964) *If G is a transitive group of permutations of a domain Ω, such that $|\Omega| = p^n$, where p is a prime, then every Sylow p-subgroup of G is also transitive on Ω.*

Specifically, we use the following consequence of this theorem.

Corollary 4.8 *Every minimally transitive subgroup of T_n is a 2-group.*

Proof. Let G be a minimally transitive subgroup of T_n. If G is not a 2-group, then every its Sylow 2-subgroup is a proper subgroup, which is also transitive by Theorem 4.7. This contradicts the assumptions, hence G is a 2-group. □

This allows to strengthen the characterization of the transitive functions.

Theorem 4.9 *A Boolean function f is transitive if and only if there are groups G and H and a vertex u, which define f, and such that G is a minimally transitive 2-group.*

Proof. Let u be any vertex satisfying $f(u) = 0$. By Lemma 4.6, the function f is defined by G, H and u, such that G is minimally transitive and, hence, a 2-group. □

For a minimally transitive group G of isometries of $\{0, 1\}^n$, the characterization of the subgroups H of G, which define a transitive function, can be simplified, since every maximal proper subgroup H of G is intransitive and has index 2 in G. The intersection of all the maximal subgroups of G is the Frattini subgroup $\Phi(G)$. Using the properties of the Frattini subgroup of a p-group, see for example [14, 4], we obtain the following theorem.

Theorem 4.10 *Let G be a minimally transitive subgroup of T_n. If k is the minimal number of its generators, then there are $2^k - 1$ maximal proper subgroups of G. If u is a vertex, then there are $2^k - 1$ different transitive functions defined by G, some of its maximal subgroups H, and u.*

Proof. Let u be a vertex. Since G is a minimally transitive 2-group, every maximal proper subgroup H of G has index $|G : H| = 2$ and is intransitive. Hence, by Lemma 4.3, every maximal proper subgroup H of G defines, together with G and u, a transitive function. Moreover, different subgroups H define different transitive functions by Lemma 4.1(ii).

There is a bijection between the maximal subgroups of G and the maximal subgroups of $G/\Phi(G)$. Since G is a 2-group, the factor group $G/\Phi(G)$ is isomorphic to Z_2^k, see [14, 4]. There is a bijection between the maximal subgroups of Z_2^k and the subspaces of $\mathrm{GF}(2)^k$ of dimension $k - 1$. The number of these subspaces is $2^k - 1$. Hence, also the number of the maximal subgroups of G is $2^k - 1$. □

The following theorem allows to obtain a transitive function from a group in a straightforward way.

Theorem 4.11 *A Boolean function f of n variables is transitive, if and only if the set $f^{-1}(0)$ is an orbit of a subgroup of T_n and $|f^{-1}(0)| = 2^{n-1}$.*

Proof. Let $B = f^{-1}(0)$ and $u \in B$. By assumption, there is a subgroup H of T_n, such that $B = \mathrm{Orbit}_H(u)$. Since $|B|$ is a power of 2, there is a 2-group H with this property by Theorem 3.4 from [17]. Assume, H is a maximal 2-subgroup of T_n satisfying $B = \mathrm{Orbit}_H(u)$. By Sylow theorems, there is a Sylow 2-subgroup K_1 of T_n, such that $H \leq K_1$. Since K_1 is transitive on $\{0,1\}^n$, we actually have $H < K_1$. Since K_1 is a finite 2-group, it satisfies the normalizer condition and, hence, the normalizer K_2 of H in K_1 satisfies $H < K_2$. Let $g \in K_2$ be such that gH is an element of K_2/H of order 2. Let $G = H \cup gH$ be the group generated by H and g.

Since H is a maximal 2-group satisfying the property above and G is a larger 2-group, we have $2^{n-1} < |\mathrm{Orbit}_G(u)|$. The size of the orbit is a power of 2, hence, G is transitive on the vertices of the Boolean cube. The groups G and H satisfy the assumptions of Lemma 4.3 and hence, B is a block of G. It follows that f is transitive by Lemma 4.2. □

5 The number of transitive functions

The number of the special quadratic polynomials defined in Section 3.1 is a lower bound on the number of the transitive functions of n variables. For an upper bound on this number, one can use the representation of a transitive function from Theorem 2.5. This immediately implies an upper bound $2^{O(n^2 \log_2 n)}$ and is improved to $2^{O(n^2)}$ by restricting the permutations used in the representation to any fixed Sylow 2-subgroup of T_n in Theorem 5.1.

In order to get a bound on the size of a Sylow 2-subgroup of T_n, let us consider an example of such a subgroup in the representation T_n^* described in Section 2.1. Let m be the smallest power of 2, such that $2n \leq m$. Let M be a balanced binary tree with m leaves numbered by integers from 1 to m in the natural order. The automorphisms of this tree can be identified with the permutations of the leaves. Let U_n^* be the subgroup of S_{2n} defined by the action on $\{1, \ldots, 2n\}$ of those automorphisms of M, which fix all the leaves with index larger than $2n$. Since every automorphism of M preserves the partition $\{1,2\}, \{3,4\}, \ldots, \{2n-1, 2n\}$, U_n^* is a subgroup of T_n^*.

If the binary representation of $2n$ has non-zero bits at positions $i_1, \ldots, i_r$ or, equivalently, $2n = 2^{i_1} + \ldots + 2^{i_r}$ and $i_1 > i_2 > \ldots > i_r$, then U_n^* is the direct product of the groups of the automorphisms of r balanced binary trees, whose depths are $i_1, \ldots, i_r$, and the set of the leaves of each of these trees is an orbit of U_n^*. One can verify that the size of U_n^* is 2^{2n-r}, which is the largest power of 2 dividing $(2n)!$. Hence, U_n^* is a Sylow 2-subgroup of S_{2n} and, hence, also of T_n^*. Since U_n^* is a subgroup of T_n^*, it can be identified with a Sylow 2-subgroup U_n of T_n of the same size.

Theorem 5.1 *The number of transitive functions of n variables is $2^{\Theta(n^2)}$.*

Proof. The number of quadratic transitive functions of n variables is at least the number of the special quadratic polynomials of $2k$ variables, where $k = \lfloor n/2 \rfloor$. This number is equal to the number of the homogeneous quadratic polynomials of k variables, which is

$$2^{\binom{k}{2}} = 2^{n^2/8+O(n)} .$$

This implies the lower bound.

By Theorem 4.9, there are 2-groups G and H, which define f together with a vertex u, which can be chosen to be the zero vertex. For each $i = 1\ldots, n$, let $\tau_i \in G$, such that $\tau_i(0) = \mathrm{e}_i$. Moreover, let $a_i = 0$, if $\tau_i \in H$ and $a_i = 1$ otherwise. By Theorem 2.5, transformations τ_i and the constants a_i uniquely determine f. Let us represent G and H as subgroups of T_n^* and let U be any fixed Sylow 2-subgroup of T_n^*. The size of U is $2^{2n-r} \leq 2^{2n-1}$, where r is the number of the non-zero bits in the binary representation of $2n$. By Sylow theorems, G is a subgroup of U^g, which is conjugated to U by an appropriate element $g \in T_n^*$. Since U is fixed, the number of the possible choices of $\tau_i \in G$ is at most $|U|^n|T_n^*| \leq 2^{2n^2+O(n\log n)} = 2^{O(n^2)}$. Since there are at most 2^n choices of the constants a_i, the upper bound of the theorem follows. □

6 Simply transitive functions

If G is a transitive subgroup of T_n, then its size is a multiple of 2^n, since G is a transitive group of permutations of $\{0,1\}^n$ and, hence, its size is $|\mathrm{Stab}_G(u)|2^n$ for any vertex u of the Boolean cube. Some of the transitive functions of n variables have a transitive group of automorphisms of size equal to 2^n or, equivalently, the group is simply transitive on $\{0,1\}^n$.

Definition 6.1 A Boolean function is simply transitive, if it is defined by groups G and H and a vertex u, such that G is simply transitive or, equivalently, is a regular group of the permutations of the vertices of the Boolean cube.

Regular subgroups of T_n are precisely the groups, whose Cayley graph with an appropriate generating set is the Boolean cube. See [6] for the details and for a classification of such groups for $n \leq 6$.

It is easy to prove that every linear and quadratic transitive function is simply transitive. In fact, the groups of isometries used to verify transitivity of these functions described in the previous sections have size 2^n, where n is the number of the variables.

GAP computer algebra system [9] was used for a random search of small subgroups of T_n^*, $n = 16$, whose action on $\{0,1\}^n$ is transitive. This search identified several transitive functions, which are not simply transitive. In particular, the function α_4 from Example 2.10 has this property and was obtained in this way. The automorphism group of α_4 has size 2^{n+2} and is transitive on $\{0,1\}^n$, however, no proper subgroup of this group is transitive. Hence, α_4 is not a simply transitive function. This function is a polynomial of degree 4 over $GF(2)$. There are also polynomials of 16 variables and degree 3, which define a transitive function, which is not simply transitive.

Acknowledgements. The autor was supported by the Grant Agency of the Czech Republic under the grant NoSCoM number P202/10/1333 and by institutional support of the Institute of Computer Science (RVO:67985807). The author is grateful to Petr Gregor for helpful discussions concerning vertex-transitive Boolean functions and for providing the reference [19].

References

[1] Harry Buhrman and Ronald de Wolf. Complexity Measures and Decision Tree Complexity: A Survey. In Theoretical Computer Science, 288(1):21–43, 2002.

[2] Sourav Chakraborty. Sensitivity, Block Sensitivity and Certificate Complexity of Boolean Functions. Masters Thesis, 2005.

[3] Sourav Chakraborty. On the Sensitivity of Cyclically-Invariant Functions. In IEEE Conference on Computational Complexity, pages 163–167, 2005.

[4] David A. Craven. The Theory of p-Groups. Lecture notes, 2008.

[5] John D. Dixon and Brian Mortimer. Permutation Groups, volume 163 of Graduate Texts in Mathematics. Springer, 1996.

[6] John D. Dixon. Groups with a Cayley graph isomorphic to a hypercube. Bull. Austral. Math. Soc. Vol. 55 (1997), pp 385–393.

[7] Edward Dobson. Imprimitive Permutation Groups. Lecture notes.

[8] Andrew Drucker. Block Sensitivity of Minterm-Transitive Functions. Computing Research Repository, report number 1001.2052, 2010.

[9] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.6; 2014, (`http://www.gap-system.org`).

[10] Péter Hajnal. Decision tree complexity of Boolean functions. Coll. Math. Soc. János Bolyai 60, Sets, graphs and numbers, Budapest (Hungary), 1991, (1992), 365–389.

[11] Alexander Hulpke. Constructing Transitive Permutation Groups. J. Symb. Comp. 39 (2005), 1–30.

[12] Stasys Jukna. Boolean Function Complexity: Advances and Frontiers. Springer-Verlag, 2012, Series: Algorithms and Combinatorics, Vol. 27.

[13] Primož Potočnik, Pablo Spiga, Gabriel Verret. A census of 4-valent half-arc-transitive graphs and arc-transitive digraphs of valence two. ArXiv 1310.6543, 2013.

[14] Joseph J. Rotman. An Introduction to the Theory of Groups, Fourth Edition, Graduate Texts in Mathematics, Springer, 1999.

[15] Xiaoming Sun. Block sensitivity of weakly symmetric functions. Theor. Comput. Sci., 384(1):87–91, 2007.

[16] György Turán. The critical complexity of graph properties. Inform. Process. Lett. 18 (1984), 151–153.

[17] Helmut Wielandt. Finite Permutation groups. Acad. Press. N.Y., 1964.

[18] Ingo Wegener. The complexity of boolean functions. Wiley-Teubner series in computer science, 1987.

[19] Steve Wilson, Primož Potočnik, A Census of edge-transitive tetravalent graphs, `http://jan.ucc.nau.edu/~swilson/C4Site/` .

ECCC ISSN 1433-8092

http://eccc.hpi-web.de