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

Boolean functions with a vertex-transitive group of automorphisms

Petr Savicky
Institute of Computer Science, Academy of Sciences of CR,
Prague, Czech Republic
e-mail: 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. Several constructions of vertex-transitive functions and some of their properties are presented.

1 Introduction

A Boolean function of n variables is a function $\{0,1\}^n \to \{0,1\}$. Its domain, the Boolean cube $\{0,1\}^n$, which is the set of the vertices of a hypercube of dimension n, is 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 Hammimg distance. These transformations are exactly those transformations, which may be defined by a permutation of the n variables and the negation of a set 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. For the purposes of this paper, vertex-transitive functions will also be called transitive functions, although this notion can have a different meaning in the literature, see Section 3.

Vertex-transitive functions are defined in Section 2 as solutions of a specific system of identities, which involve permutations and negations of the variables. This understanding is sufficient for most of the results of the first six sections of the paper. Vertex-transitive functions are also characterized using a suitably defined group of automorphisms. This is used for some of the results in Section 2 and further developed in Section 7.

Every linear function over the two-element field F_2 is transitive for trivial reasons and there is a simple quadratic transitive function on 4 variables, see Example 2.7. For every transitive function of n variables, there is a system of n identities, which uniquely determines the function. Moreover, this system allows to compute $f(x)$ for any $x \in \{0,1\}^n$ in time $O(n^2)$ on RAM machine, see Theorem 2.5. Section 3 presents a comparison of vertex-transitive functions and

ISSN 1433-8092

a related, but different, notion, which is sometimes called a transitive function in the literature. Section 4 presents a characterization of quadratic polynomials over F_2, which define a transitive function. Using this characterization and a result of Section 2, the number of transitive functions of n variables is proved to be at least $2^{\Omega(n^2)}$ and at most $2^{O(n^2 \log n)}$ in Theorem 4.5. Section 5 demonstrates for every integer d a transitive function defined by a polynomial of degree d over F_2. Section 6 demonstrates transitive functions of small sensitivity and with super-linear gap between sensitivity and block sensitivity.

The properties of the vertex-transitive groups of isometric transformations, which define a transitive function, are investigated in Section 7. In particular, it is proved that for every transitive function f, there is a transitive group G of automorphisms of f, which is a 2-group or, equivalently, the size of G is a power of 2. The minimum possible size of such G for a function of n variables is 2^n and the functions, which have a transitive group of automorphisms of this size, will be called uniquely transitive. See Section 8 for remarks concerning these functions.

2 Vertex-transitive functions

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

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

be the vector obtained from x by permuting its components according to p. Let the composition of the permutations p_1, p_2 be defined so that for every x, we have

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

Isometric transformation of $\{0,1\}^n$ is a permutation of the vertices of the hypercube, which preserves the Hamming distance. These mappings are exactly the mappings of the form

$$x \mapsto x^p \oplus s \ , \tag{1}$$

where $p \in S_n$ and $s \in \{0,1\}^n$. The mapping (1), will be denoted as $\tau(p,s)$. Hence, for every $p \in S_n$, every $s \in \{0,1\}^n$, and every $x \in \{0,1\}^n$, we have

$$\tau(p,s)(x) = x^p \oplus s \ .$$

The composition of transformations is denoted by $\circ$ and satisfies $(\tau_2 \circ \tau_1)(x) = \tau_2(\tau_1(x))$. Since

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

we have

$$\tau(p_2, s_2) \circ \tau(p_1, s_1) = \tau(p_1 p_2, s_1^{p_2} \oplus s_2) \ . \tag{2}$$

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

Definition 2.1 A Boolean function is vertex-transitive, if for every $s \in \{0,1\}^n$, there is a permutation p and a constant $a \in \{0,1\}$, such that the transformation $\tau = \tau(p,s)$ satisfies for every $x \in \{0,1\}^n$

$$f(\tau(x)) = f(x) \oplus a \ . \tag{3}$$

In this paper, the vertex-transitive functions will be called transitive for simplicity. However, in the literature, the notion of a transitive function can have a different meaning, see Section 3.

Clearly, a function f is transitive if and only if $\neg f$ is transitive. Due to this, we may, without loss of generality, restrict ourselves to the functions, which satisfy $f(0) = 0$. This restriction will be frequently used.

The identities of the form (3) may be composed, since $f(\tau_1(x)) = f(x) \oplus a_1$ and $f(\tau_2(x)) = f(x) \oplus a_2$ imply

$$f(\tau_2(\tau_1(x))) = f(\tau_1(x)) \oplus a_2 = f(x) \oplus a_1 \oplus a_2 \ . \tag{4}$$

In order to guarantee that a function is transitive, it is sufficient to find a set of identities (3), which generates, using the composition rule (4), a system of identities required by Definition 2.1. For a precise formulation, the following notion is useful.

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 (3) is satisfied.

Clearly, a transformation τ is an automorphisms of f, if and only if the partition of the Boolan cube into the sets $f^{-1}(0)$ and $f^{-1}(1)$ is invariant under τ.

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

Proof. If τ_1, τ_2 are autmorphisms, then also $\tau_2 \circ \tau_1$ is an automorphism due to (4). Hence, 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 group of automorphisms of f, which is transitive, then for every $s \in \{0,1\}^n$, there is an automorphism $\tau \in G$, which satisfies $\tau(0) = s$. Clearly, there is $p \in S_n$, such that $\tau = \tau(p,s)$. Since τ is an automorphism of f, there is $a \in \{0,1\}$, such that for all x, the identity (3) is satisfied. Hence, by Definition 2.1, the function f is transitive. □

The set of identities, which implies transitivity of a Boolean function using Lemma 2.3, may be relatively small. Example 2.8 demonstrates a function of 8 variables, for which, a transitive group of automorphisms can be generated by two identities. However, verification of the assumptions of the lemma includes verification of the transitivity of a group of automorphisms given by its generators. Verification of this condition may be avoided, if the system of generators

consists of n identities in the special form described in the next theorem. On the other hand, the existence of a function f satisfying identities (5) is not guaranteed. Hence, in order to apply the theorem, the function f has to be known in advance. The standard basis vector e_i is the vector, whose i-th component is 1 and all the remaining components are 0.

Theorem 2.4 *A function f of n variables is transitive, if and only if for every $i = 1, \ldots, n$, there is a permutation $p_i \in S_n$ and a constant $a_i \in \{0, 1\}$ such that*

$$f(x^{p_i} \oplus \mathrm{e}_i) = f(x) \oplus a_i \ , \tag{5}$$

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 p_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 exactly the set of n identities required by the statement of the theorem.

For the opposite direction, assume that f satisfies the n identities (5). For every $s \in \{0, 1\}^n$, we have to find $p \in S_n$ and $a \in \{0, 1\}$, such that $\tau = \tau(p, s)$ satisfies (3) for every $x \in \{0, 1\}^n$. Clearly, if $s = 0$, then $p = \mathrm{id}$ and $a = 0$ may be used. If $|s| = 1$, then $s = \mathrm{e}_i$ for some $i = 1, \ldots, n$ and using $p = p_i$ and $a = a_i$, the required identity follows from the assumption.

If $|s| \geq 2$, let $k = |s|$ and let $i_1, \ldots, i_k \in \{1, \ldots, n\}$ be indices such that $s = \mathrm{e}_{i_1} \oplus \ldots \oplus \mathrm{e}_{i_k}$. For every $l = 0, \ldots, k$, let $s_l = \mathrm{e}_{i_1} \oplus \ldots \oplus \mathrm{e}_{i_l}$. Hence, we have $|s_l| = l$ for $l = 0, \ldots, k$ and $s_k = s$. We prove by induction on $l = 0, \ldots, k$ that there is $r_l \in S_n$ and $b_l \in \{0, 1\}$ such that $\tau_l = \tau(r_l, s_l)$ satisfies (3) with $a = b_l$. Since $s_0 = 0$, we may choose $r_0 = \mathrm{id}$ and $b_0 = 0$, similarly as above.

Let $l \geq 1$ and assume that $\tau_{l-1} = \tau(r_{l-1}, s_{l-1})$ and b_{l-1} satisfy for all x

$$f(\tau_{l-1}(x)) = f(x) \oplus b_{l-1} \ . \tag{6}$$

Let $j = r_{l-1}^{(-1)}(i_l)$ and, hence, $\mathrm{e}_j^{r_{l-1}} = \mathrm{e}_{i_l}$. Let $\tau' = \tau(p_j, \mathrm{e}_j)$. By the assumption, we have

$$f(\tau'(x)) = f(x) \oplus a_j \ . \tag{7}$$

Combining (6) and (7), we obtain

$$f(\tau_{l-1}(\tau'(x))) = f(\tau'(x)) \oplus b_{l-1} = f(x) \oplus a_j \oplus b_{l-1} \ .$$

Moreover, using (2), we obtain

$$\tau_{l-1} \circ \tau' = \tau(p_j r_{l-1}, \mathrm{e}_j^{r_{l-1}} \oplus s_{l-1}) = \tau(p_j r_{l-1}, \mathrm{e}_{i_l} \oplus s_{l-1}) = \tau(p_j r_{l-1}, s_l) \ .$$

Consequently, setting $r_l = p_j r_{l-1}$ and $b_l = a_j \oplus b_{l-1}$ proves the induction hypothesis for l and, hence, also the first part of the theorem.

If f satisfies $f(0) = 0$, then it is uniquely determined by the 2^n identities from Definition 2.1. Since these identities may be derived from the identities (5), uniqueness of the solution f follows. □

The complexity of evaluating a transitive function on RAM (random access machine) with the unit cost measure may be bounded as follows.

Theorem 2.5 *Assume, f is a transitive function satisfying $f(0) = 0$ and let p_i, a_i for $i = 1, \ldots, n$ be as in Theorem 2.4. Then, for every $x \in \{0,1\}^n$, it is possible to compute $f(x)$ in time $O(n^2)$ on RAM, if p_i, a_i for $i = 1, \ldots, n$ are part of the input.*

Proof. Let x be fixed and let $s = x$. Since f is transitive, there is $p \in S_n$ and $a \in \{0,1\}$, such that for all $y \in \{0,1\}^n$

$$f(y^p \oplus s) = f(y) \oplus a \ .$$

Moreover, the proof of Theorem 2.4 demonstrates a procedure, which computes p and a for any given s using the parameters p_i and a_i. The procedure consists of $|s|$ steps, each of which may be performed in time $O(n)$ on RAM. Since $|s| \leq n$, the total complexity is $O(n^2)$. When p and a are computed, setting $y = 0$ in the identity above yields $f(x) = f(s) = f(0) \oplus a = a$. □

For an arbitrary set $A \subseteq \{1, \ldots, n\}$, let x_A denote the subset of the variables, whose indices belong to A. Let $\mathrm{par}(x_A)$ be the parity function of the variables from x_A.

Lemma 2.6 *If $A \subseteq \{1, \ldots, n\}$, then the linear function*

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

is transitive.

Proof. For any s, consider the transformation $\tau = \tau(\mathrm{id}, s)$. Clearly, for every x, we have

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

and, hence, (3) is satisfied with $a = f(s)$. □

An example of a quadratic transitive function may be described as follows.

Example 2.7 *The function $\alpha(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_2 \oplus x_4$ is transitive.*

Proof. One can easily verify that the function $\alpha(x) = \alpha(x_1, x_2, x_3, x_4)$ satisfies

$$\begin{aligned}
\alpha(x_1 \oplus 1, x_2, x_4, x_3) &= \alpha(x) \\
\alpha(x_1, x_2 \oplus 1, x_4, x_3) &= \alpha(x) \oplus 1 \\
\alpha(x_2, x_1, x_3 \oplus 1, x_4) &= \alpha(x) \\
\alpha(x_2, x_1, x_3, x_4 \oplus 1) &= \alpha(x) \oplus 1 \ ,
\end{aligned}$$

which are the identities (5) for the function α. Hence, the function α is transitive by Theorem 2.4. □

The next example demonstrates a transitive function defined by a polynomial of degree 3 over F_2.

Example 2.8 *Let β_1 be the function of 4 variables defined by*

$$\beta_1(y_1, \ldots, y_4) = y_1\, y_2\, y_3 \oplus y_1\, y_2\, y_4 \oplus y_1\, y_3\, y_4 \oplus y_2\, y_3\, y_4$$

and let β_2 be the function of 8 variables defined by the formula (the symbol $+$ is used instead of $\oplus$ for simplicity of the notation)

$$\begin{aligned} \beta_2(x_1, \ldots, x_8) \;=\; & \beta_1(x_1 + x_2,\, x_3 + x_4,\, x_5 + x_6,\, x_7 + x_8) \\ & + (x_1 + x_3 + x_5 + x_7)(x_2 + x_4 + x_6 + x_8) \\ & + (x_1 + x_2)(x_3 + x_4) \\ & + x_3 + x_4 + x_5 + x_8\ . \end{aligned}$$

Then, the function β_2 is transitive.

Proof. Let $x = (x_1, \ldots, x_8)$. The function $\beta_2(x) = \beta_2(x_1, \ldots, x_8)$ satisfies the identities

$$\begin{aligned} \beta_2(x_5,\, x_6,\, x_7,\, x_8,\, x_1,\, x_2 \oplus 1,\, x_4,\, x_3) &= \beta_2(x) \\ \beta_2(x_1 \oplus 1,\, x_2,\, x_3,\, x_4 \oplus 1,\, x_8,\, x_7,\, x_6,\, x_5) &= \beta_2(x) \oplus 1\,. \end{aligned}$$

The arguments of β_2 in the left hand sides of these identities represent two automorphisms of β_2, which generate a transitive group of isometries. Verification of this is left to the reader. As a consequence, β_2 is transitive by Lemma 2.3. □

Lemma 2.9 *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. $g(x_B)$. A transitive group of automorphisms of $f(x_A) \oplus g(x_B)$ may be obtained as the direct product $G_A \times G_B$. □

In the next section, we will need a partial converse of this statement. For a proof of this converse, we need a relationship between the automorphisms of a function and its sensitivity on different variables.

Definition 2.10 *For any function f of n variables and any i, $1 \le i \le n$, let $\sigma(f, i)$ be the sensitivity of the function f on the variable x_i, which is defined as the probability of $f(x \oplus \mathrm{e}_i) \neq f(x)$, if x is chosen at random from the uniform distribution on $\{0,1\}^n$.*

Lemma 2.11 *Let f be a function of n variables and let $p \in S_n$, $s \in \{0,1\}^n$ be such that $\tau = \tau(p, s)$ is 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. Assume that for some $a \in \{0,1\}$ and for all x, we have

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

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

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

This implies that the probability of $f(x^p \oplus s \oplus \mathrm{e}_j) \neq f(x^p \oplus s)$ is the same as the probability of $f(x \oplus \mathrm{e}_i) \neq f(x)$. Since the mapping $x \mapsto x^p \oplus s$ preserves the uniform distribution on $\{0,1\}^n$, the lemma follows. □

Clearly, the sensitivity of f on x_i is 0, if and only if f does not depend on x_i. The other extreme is the sensitivity 1, which can also be characterized in simpler terms.

Lemma 2.12 *The sensitivity of a function f on a variable x_i is 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. Note that the sensitivity of f on x_i is r, if and only if the sensitivity of $g = f \oplus x_i$ on x_i is $1 - r$. □

Theorem 2.13 *Let A and B be disjoint sets of indices of the variables and let the functions $f(x_A, x_B)$ and $g(x_A)$ satisfy*

$$f(x_A, x_B) = g(x_A) \oplus \mathrm{par}(x_B) \ .$$

Then, f is transitive if and only if g is transitive.

Proof. The "if" part follows from Lemma 2.9. For the "only if" part, assume that $f(x_A, x_B)$ is transitive. Without loss of generality, we may assume that f depends on all the variables in x_A and x_B. Moreover, 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 in the open interval $(0,1)$. 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 2.11, the permutation p preserves each of the sets A and B. Hence, group G is a subgroup of the direct product $T_A \times T_B$, where T_A, resp. T_B, is the group of the isometric transformations of $\{0,1\}^A$, resp. $\{0,1\}^B$. Let id_A be the identity element of T_A. Since all elements of T_B are automorphisms of $\mathrm{par}(x_B)$, all elements of the group $\{\mathrm{id}_A\} \times T_B$ are automorphisms of $f(x_A, x_B)$.

Let G_A be the projection of G to the component T_A. Since G is transitive on $\{0,1\}^{A \cup B}$, G_A is transitive on $\{0,1\}^A$. We have to prove that all elements of G_A are automorphisms of $g(x_A)$. Let $\tau_A \in G_A$ and let τ be an element of G, whose T_A component is τ_A. Hence, $\tau = (\tau_A, \tau_B)$ for some $\tau_B \in T_B$. Since $(\mathrm{id}_A, \tau_B^{-1})$ is an automorphism of f, also

$$(\tau_A, \mathrm{id}_B) = (\mathrm{id}_A, \tau_B^{-1}) \circ (\tau_A, \tau_B)$$

is an automorphism of f. This implies that τ_A is an automorphism of g, 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 in the open interval $(0, 1)$. Consider the decompositions

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

and

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

which may be obtained by a repeated application of Lemma 2.12 to the function g. The function g' satisfies the assumption of the first case of the proof, so we can use its conclusion for both these decompositions. It follows that g is transitive, if and only if g' is transitive and, similarly, f is transitive, if and only if g' is transitive. Consequently, the theorem holds also in the general case. □

3 Variable-transitive functions

A function f will be called variable-transitive, 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

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

These functions are called transitive functions and were investigated in relation to their sensitivity and decision tree complexity, see for example [6, 4, 2]. In particular, all graph properties are transitive functions in this sense.

Theorem 3.1 *If a function satisfies $f(0) = 0$ and is simultaneously variable-transitive and vertex-transitive, then it is either the parity of all variables or the zero function.*

Proof. For a variable-transitive function, there is $a \in \{0,1\}$ such that $f(\mathrm{e}_i) = a$ for all $i = 1, \ldots, n$. Hence, if $x = 0$, 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, then all vertices x of the hypercube 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. □

The number of variable-transitive and the number of vertex-transitive functions are very different. 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 at most $O(n^2 \log_2 n)$, see Theorem 4.5.

In the rest of this paper, a transitive function means a vertex-transitive function.

4 Characterization of quadratic transitive functions

In order to verify transitivity of quadratic polynomials, the following reformulation of Theorem 2.4 is useful.

Lemma 4.1 *A function f is transitive, if and only if for every $i = 1, \ldots, n$, there is a permutation q_i and a constant $a_i \in \{0, 1\}$ such that*

$$f(x \oplus \mathrm{e}_i) = f(x^{q_i}) \oplus a_i \ , \tag{8}$$

where e_i is the i-th standard basis vector.

Proof. If $q_i = p_i^{-1}$, then (8) is equivalent to (5). □

Later, we will use the following identities for α, which are obtained by the transformation of the first two identities from Example 2.7 to the form (8).

$$\begin{aligned} \alpha(x_1 \oplus 1, x_2, x_3, x_4) &= \alpha(x_1, x_2, x_4, x_3) & (9) \\ \alpha(x_1, x_2 \oplus 1, x_3, x_4) &= \alpha(x_1, x_2, x_4, x_3) \oplus 1 \ . & (10) \end{aligned}$$

Any quadratic polynomial $f(x)$ over F_2, which satisfies $f(0) = 0$, may be written as

$$f(x) = x^t U x \oplus c^t x \ , \tag{11}$$

where U is an appropriate upper triangular matrix with zeros on the diagonal and c is a column vector. In some contexts, it is useful to consider 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 4.2 *If f is a quadratic polynomial in the form (11), $Q = U \oplus U^t$ and $s \in \{0, 1\}^n$ is arbitrary, then for every x, we have*

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

Proof. Using (11), 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 may be combined to the following 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 4.3 A quadratic polynomial is called special, if the number of its variables is $n = 2k$ and there is a homogeneous quadratic polynomial g of k variables, such that

$$f(x) = g(u) \oplus \bigoplus_{i=1}^{k} x_{2i} \ ,$$

where $u = (x_1 \oplus x_2, x_3 \oplus x_4, \ldots, x_{n-1} \oplus x_n)$.

Special quadratic polynomials may also be characterized in the form (11). Let $n = 2k$ for some k and 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 obtained using Π for both the rows and columns. The matrix consists of $k \times k$ blocks, each of which has dimension 2×2. If the polynomial is a special quadratic polynomial, then all the diagonal blocks are zero and for each of the non-diagonal blocks, either all of the components are zero or all of them are equal to one. Moreover, if the vector c is splitted according to Π, it consists of k blocks of the form $(0,1)$.

The above block structure for special quadratic polynomials is, in fact, a characterization. A quadratic polynomial in the form (11) is a special quadratic polynomial, if and only if the matrix $Q = U \oplus U^t$ and the vector c have the block structure described in the previous paragraph.

Lemma 4.4 *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 (11) 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 (8). By Lemma 4.2, 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, 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 for every $j = 1, \ldots, k$ exchanges $2j-1$ and $2j$, whenever $\{2j-1, 2j\}$ is a block of Π, where the vector c' is equal to $(1,0)$ and does not move $2j-1$ and $2j$ otherwise. 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 Lemma 4.1. □

Using the special quadratic polynomials and a result of the previous section, it is now easy to obtain bounds on the number of transitive functions.

Theorem 4.5 *The number of transitive functions of n variables is at least $2^{\Omega(n^2)}$ and at most $2^{O(n^2 \log_2 n)}$.*

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 2.4, every transitive function of n variables satisfying $f(0) = 0$ may be uniquely described by n permutations and n additional bits. Hence the number of all transitive functions is at most

$$2\,(2 \cdot n!)^n = 2^{O(n^2 \log_2 n)} \ .$$

This implies the upper bound in the theorem. □

Lemma 4.6 *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 F_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 as $\sigma(f,i)$. We use also the sensitivity of a function in a vertex.

Definition 4.7 The sensitivity of a function f of n variables in any 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 not only the maximum, but also the average value of the sensitivity over all vertices. Due to this, we have

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

where the summation is over the real numbers. Since

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

we also have

$$\sigma(f) = \sum_{i=1}^{n} \sigma(f,i) \ . \tag{12}$$

Lemma 4.8 *If f is a quadratic transitive function (11) 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, (12) 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 the number of the linear terms of the polynomial $f(x \oplus s)$ considered as a function of x. By Lemma 4.2, 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 F_2. Under a general field, affine combinations are the linear combinations, whose sum of the coefficients is 1. Since M is a matrix over F_2, $\mathcal{A}(M)$ is the set of the sums of odd size subsets of the rows of M. Every affine subset A of a vector space may be obtained as $a + W$, where a is any 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 4.9 *If A is an affine subset of $\{0,1\}^n$, whose elements have $n/2$ non-zero components, then there is a permutation p of the n indices of the variables, such that the affine set A^p is a subset of the solutions of the system of the linear equations*

$$\begin{array}{lcl} x_1 \oplus x_2 & = & 1 \\ x_3 \oplus x_4 & = & 1 \\ \ldots & & \\ x_{n-1} \oplus x_n & = & 1 \ . \end{array} \tag{13}$$

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 the linear functions over the column 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.

Consider the matrix L as the set of its rows. In this sense, L is a linear space over F_2. Its elements are vectors, whose components are indexed by $\{0,1\}^k$. Let $\phi : L \to \{0,1\}^n$ be defined for every row z of L as

$$\phi(z) = (z_{b_1}, \ldots, z_{b_n}) \ . \tag{14}$$

For every I, let ℓ_I be the row of L with index I. Let V be the set of $\ell_{\{i\}}$ for $i = 1, \ldots, k$. The rows of L, which belong to 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 (14) as a selection of some of the components of z, possibly with repetitions, the number of ones in $\phi(z)$, denoted as $|\phi(z)|$, may be expressed by the scalar product in the real numbers

$$|\phi(z)| = w \cdot z \ , \tag{15}$$

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

$$w_y = |\{j \in \{1, \ldots, n\};\ b_j = y\}| \ . \tag{16}$$

Clearly,

$$\sum_{y \in \{0,1\}^k} w_y = n \ . \tag{17}$$

Lemma 4.10 *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 (15) and (17), we obtain

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

Since H is an orthogonal matrix, this implies that the rows of H, which correspond to the rows $\mathcal{A}(V)$ of L, do not contribute to the linear combination of the rows of H, which expresses w over the real numbers. Hence, w is the linear combination of the remaining rows of H. Since the rows in V are the linear functions over F_2 of a single bit of y, the set $\mathcal{A}(V)$ consists exactly of

those 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. A parity of an even number of the bits of y 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, if $z' = 1 - 2z$ is the row of H corresponding to z, then $z'_{\overline{y}} = z'_y$ for all $y \in \{0,1\}^k$. Since this property is satisfied for all rows of H, which contribute to the linear combination over the real numbers, which expresses w, the lemma follows. □

Lemma 4.10 and (16) imply that for every y, the number of the occurrences of the column y in B is equal to the number of the occurrences 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 (13) 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 4.9 is completed. □

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

Theorem 4.11 *If f is a transitive function defined by a quadratic polynomial (11) of n variables, which has sensitivity $1/2$ on each variable, then there is $p \in S_n$, such that the function $f(x^p)$ is a special quadratic polynomial.*

Proof. Let U be as in (11) and let $Q = U \oplus U^t$. By Lemma 4.8, the affine set

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

satisfies the assumptions of Lemma 4.9, if this lemma is understood in terms of the column vectors. Let q be the permutation guaranteed by Lemma 4.9. The elements of A^q satisfy (13). In particular, c^q satisfies these identities. Hence, if the vector c^q is splitted into blocks of size 2 according to Π, it consists of the blocks $(0,1)$ and $(1,0)$. Since the equations (13) are invariant under exchanging the variables in any block, we may choose q so that $c' = c^q$ 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 q. The matrix Q' is a symmetric matrix with zero diagonal, since these properties are preserved, if the columns and the rows are permuted in the same way. Let U' be the upper triangular part of Q' and let f' be the function

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

One can easily verify that $f'(x^q) = f(x)$ for every x.

The sum in F_2 of $c' = (0,1,\ldots,0,1)^t$ and any column of Q' belongs to A^q. 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 f' is a special quadratic polynomial. Since $f'(x) = f(x^p)$ for $p = q^{-1}$, the proof is finished. □

Corollary 4.12 *A quadratic polynomial defines a transitive function, if and only if it may be obtained from a special quadratic polynomial by a permutation of the variables and possibly removing irrelevant ones.*

Proof. The "if" direction follows from Lemma 4.4. For the "only if" direction, let f be a quadratic transitive polynomial, which depends on all its variables. By a repeated application of Lemma 2.12, 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 4.6, g has sensitivity $1/2$ on all its variables. Moreover, by Theorem 2.13, the function $g(x_A)$ is transitive. Hence, by Theorem 4.11, g is a special quadratic polynomial up to a permutation of the variables. The function $\mathrm{par}(x_B)$ may 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. □

5 Transitive functions of an arbitrary degree

Let α be the quadratic transitive function from Example 2.7.

Lemma 5.1 *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, $\alpha(g_1(x_{1,1}), g_1(x_{1,2}), g_2(x_{2,1}), g_2(x_{2,2}))$ 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

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

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 Lemma 4.1, we need to 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

$$f(x \oplus \mathrm{e}_{i,j,l}) = f(x^p) \oplus a \ . \tag{18}$$

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

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

By Lemma 4.1, there are $q \in S_{k_1}$ and $b \in \{0, 1\}$, such that

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

which implies

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

If $b = 0$, this implies

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

which is the identity (18) for a suitable permutation p and $a = 0$. If $b = 1$, we additionally use (9) to obtain

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

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 is the identity (18) for a suitable permutation p.

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

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

with $q \in S_{k_1}$ and $b \in \{0, 1\}$ guaranteed by Lemma 4.1 for g_1. If $b = 0$, this is the identity (18) as in the previous case. If $b = 1$, we use (10) to obtain

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

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 is the identity (18) for a suitable permutation p and $a = 1$.

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

Theorem 5.2 *For every integer $d \geq 1$, there is a transitive function of at most $2d^2$ variables represented by a polynomial over F_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. Every leaf will be assigned to an arbitrary transitive function of degree 1. An internal node, both successors of which are already assigned, will be 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 the function in the root is d and the number of the variables of this function is at most $d2^k \leq 2d^2$. □

6 Transitive functions with small sensitivity

Let ϕ_i be a formula in the form of a balanced 4-ary tree of depth i, whose internal nodes compute the connective α from Example 2.7 and the leaves are different variables. Let g_i be the function of 4^i variables, which is represented by ϕ_i. In particular, g_1 is the function α and the function g_2 is defined as

$$g_2(x_1, \ldots, x_{16}) = \alpha(\alpha(x_1, \ldots, x_4), \ldots, \alpha(x_{13}, \ldots, x_{16})) \ .$$

We consider the sensitivity and the block sensitivity of g_i. For a general function f, both these sensitivities are first defined in every vertex of the hypercube and the sensitivity of the function is the maximum of the corresponding sensitivity over all vertices, see, for example, [2], [1]. The sensitivity of f in a vertex x is denoted as $\sigma(f, x)$, see Definition 4.7.

The block sensitivity of f in 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 $f(x \oplus v_j) \neq f(x)$. Clearly, the block sensitivity in a vertex is at least the sensitivity in the same vertex, since the vectors v_j may be chosen to be those 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.

Since α is transitive, its sensitivity is equal to its sensitivity in the zero vertex, which is 2, since $\alpha(\mathrm{e}_2) = \alpha(\mathrm{e}_4) = 1$ and $\alpha(0) = \alpha(\mathrm{e}_1) = \alpha(\mathrm{e}_3) = 0$. The block sensitivity of α in the zero vertex is at least 3, since $\alpha(\mathrm{e}_2) = \alpha(\mathrm{e}_4) = \alpha(\mathrm{e}_1 \oplus \mathrm{e}_3) = 1$. Moreover, the set of the indices of non-zero components of every vector v, which satisfies $\alpha(v) \neq \alpha(0)$, contains at least one of the sets $\{2\}$, $\{4\}$, and $\{1, 3\}$. This implies that the block sensitivity of α in the zero vertex is at most 3. Altogether, the block sensitivity of α is 3. Moreover, the same argument proves the implication

$$\alpha(x_1, x_2, x_3, x_4) = 1 \ \Rightarrow \ \frac{1}{2}x_1 + x_2 + \frac{1}{2}x_3 + x_4 \geq 1 \ , \tag{19}$$

which will be used later.

Theorem 6.1 *For every $i \geq 0$, g_i is a transitive funtion of 4^i variables, whose sensitivity is 2^i and block sensitivity is 3^i.*

Proof. For every $i \geq 0$, the function g_i is transitive by an induction argument using Lemma 5.1. As mentioned above, this implies that the sensitivity and block sensitivity of g_i is equal to the corresponding sensitivity in the zero vertex, which is the assignment of all 4^i variables to 0. Consider the tree structure of the formula ϕ_i, which defines g_i. Every internal node of the tree computes the connective α, whose arguments correspond to the 4 successors of the node in the tree. In this sense, every edge in the tree corresponds to one of the arguments of α and we will refer to these arguments using their indices.

The value of g_i for the zero input is 0. There are 2^i variables of g_i, such that the path from the root of the formula to the considered variable consists

only of edges, which correspond to arguments 2 and 4 of α. Clearly, changing any of these variables to 1 leads to an assignment, for which the value of g_i is 1. Hence, the sensitivity of g_i in the zero vertex is at least 2^i. One can also verify that changing any other variable to 1 in the zero assignment does not change the value of the whole formula. Hence, the sensitivity of g_i in the zero vertex is at most 2^i. Altogether, the sensitivity of g_i is 2^i.

In the rest of the proof, we use the following notation. For any set of variables V of g_i, let a_V be the assignment, which assigns 1 to the variables in V and 0 to the remaining variables.

In order to get a lower bound on the block sensitivity of g_i in the zero vertex, consider the subtrees of the formula, which contain the root of the formula, the leaves of the subtree are leaves of the formula and the following is satisfied. For every internal node of the subtree, the set of the indices of the successors, which are contained in the subtree, is precisely one of the sets $\{2\}$, $\{4\}$, and $\{1,3\}$. Moreover, the choice of the set of the successors is the same for all nodes at the same level of the tree. Since there are i levels in the tree and for each of them, we choose one of the three sets, there are 3^i such subtrees and the sets of the leaves of these subtrees are disjoint. Hence, the sets of the leaves of the subtrees define 3^i different sets of variables, which are disjoint. If V is one of these sets, then $g_i(a_V) = 1$. Hence, the block sensitivity of g_i in the zero vertex is at least 3^i.

For an upper bound on the block sensitivity of g_i in the zero vertex, consider the weights of the arguments of α, which appear as coefficients in (19). Every edge of the tree ϕ_i corresponds to an argument of α, so, we may assign these weights also to the edges of the tree. Moreover, we assign to every variable of g_i the weight, which is the product of the weights of the edges, which form the path from the root of ϕ_i to the leaf with the considered variable. Since the sum of the weights of the edges from any given vertex is 3, the sum of the weights of all variables is 3^i. Consider the sets of variables V, such that $g_i(a_V) = 1$. In the next paragraph, we prove that the sum of the weights of the variables in every such V is at least 1. Since the total sum over all variables is 3^i, this implies that there are at most 3^i disjoint sets V satisfying $g_i(a_V) = 1$. This implies the upper bound 3^i on the block sensitivity of g_i.

In order to prove a lower bound on the sum of the weigths of the variables in V satisfying $g_i(a_V) = 1$, we may assume that V is an inclusion minimal set with this property. Consider the subtree, which is the union of the paths from the root to the variables in V. Since V is inclusion minimal, every node of the subtree evaluates to 1 for the assignment a_V. Using (19), we obtain that for every node of the subtree, the sum of the weights of the edges to the successors of the node, which also belong to the subtree, is at least 1. Hence, the sum of the weights of the variables in V is at least 1. $\square$

7 Groups of isometries

In Section 2, a vertex-transitive or, simply, a transitive function was defined as a Boolean function, which satisfies a system of identities. These identities gen-

erate a group of automorphisms of the function. In this section, we investigate the properties of these groups. For this purpose, the isometries are understood as permutations of the vertices of the hypercube and the transitive functions are characterized using the notion of a block system of a permutation group.

Recall that a block for a group G of permutations of a domain Ω is a 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 permutations in 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 among them forms a partition of Ω. Moreover, this partition is preserved by G and, hence, is a block system. These considerations are the basis for the statement (i) of Lemma 7.1 below. For more information, see, for example, [5], [8].

Lemma 7.1 ([5], [8]) *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 subgroup of G, which contains $\mathrm{Stab}_G(u)$, then the orbits of H form a block system of G. In particular, all the orbits of H have the same size.

Lemma 7.2 *A non-constant function f of n variables is transitive, if and only if there is a transitive group G of isometries of $\{0,1\}^n$, 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 and let $s \in \{0,1\}^n$. By Definition 2.1, there is a permutation $p \in S_n$ and $a \in \{0,1\}$, such that the isometry $\tau = \tau(p,s)$ satisfies for every x

$$f(\tau(x)) = f(x) \oplus a \ . \tag{20}$$

Let G be the group generated by the isometries, which appear as τ in (20) for some s. Clearly, G is transitive on the vertices of the hypercube, since for every s, there is $\tau \in G$ such that $\tau(0) = s$.

Consider the partition $\{f^{-1}(0), f^{-1}(1)\}$. If $a = 0$, then the identity (20) is equivalent to the condition that x and $\tau(x)$ belong to the same block of the partition. On the other hand, if $a = 1$, then (20) is equivalent to the condition that x and $\tau(x)$ belong to different blocks of the partition. Hence, the considered partition is invariant under the generators of G and, consequently, is a block system for G.

For the opposite direction, let f be any non-constant function of n variables and G a transitive group of isometries of $\{0,1\}^n$, 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 $\tau(0) = s$ and, hence, $\tau = \tau(p, s)$ for some $p \in S_n$. Clearly, τ either preserves the blocks of the partition or exchanges them. Using the same analysis as in the previous paragraph, this implies that there is $a \in \{0,1\}$, such that (20) holds for all x. Hence, the requirement of Definition 2.1 is satisfied. □

A transitive group G may have several two-element block systems. In this case, G does not define a transitive function uniquely. In fact, the parity of all variables represents a block system of any transitive group of isometries of $\{0,1\}^n$. Hence, no other function can be determined uniquely only by the group G. In order to specify a unique transitive function, we can use a pair of groups as follows.

Definition 7.3 Let u be any vertex of the Boolean cube $\{0,1\}^n$ and f a non-constant Boolean function of n variables, which satisfies $f(u) = 0$. Let the groups G and H of isometries of $\{0,1\}^n$ be such that

- G is transitive,
- $H \leq G$, $|G : H| = 2$,
- H is not transitive and its orbits are equal to $f^{-1}(0)$ and $f^{-1}(1)$.

Then, we say that G, H and u define f.

Before we prove that this definition characterizes transitive functions, we prove a simple lemma.

Lemma 7.4 *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 x, we have $|\mathrm{Orbit}_H(x)| = 2^{n-1}$ and $\mathrm{Stab}_G(x) \leq H$.

Proof. Let G and H be groups satisfying the assumptions and let x be any vertex of the hypercube. By the orbit-stabilizer theorem, we have

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

and

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

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

Theorem 7.5 *A non-constant Boolean function f is transitive, if and only if there are groups G and H of isometries of $\{0,1\}^n$ and a vertex u, which define f.*

Proof. Let G, H and u define f. By Lemma 7.4, H contains $\mathrm{Stab}_G(u)$. Hence, Lemma 7.1(ii) implies that $\mathrm{Orbit}_H(u)$ is a block of G. Since G is transitive, the partition into the orbits of H is a block system by Lemma 7.1(iii). Hence, the complement of $\mathrm{Orbit}_H(u)$ is also an orbit of H and a block of G. The assumption implies that the blocks are equal to the sets $f^{-1}(0)$ and $f^{-1}(1)$. Hence, by Lemma 7.2, the function f is transitive. This implies the "if" part of the theorem.

Let f be a non-constant transitive function. By Lemma 7.2, the partition $\{f^{-1}(0), f^{-1}(1)\}$ is a block system of a transitive group G of isometries. Let $B = f^{-1}(0)$ and let u be any element of B. By Lemma 7.1(ii), there is a subgroup H of G, which contains $\mathrm{Stab}_G(u)$, and such that $B = \mathrm{Orbit}_H(u)$. Since $|B| = 2^{n-1}$ and $\mathrm{Stab}_H(u) = \mathrm{Stab}_G(u)$, we have $|G : H| = 2$ and the blocks $f^{-1}(0)$, $f^{-1}(1)$ are orbits of H. Hence, the groups G, H and vertex u define f. This implies the "only if" part of the theorem. □

In order to verify that groups G and H define f, it is not necessary to verify that H is transitive on each of the sets $f^{-1}(0)$, $f^{-1}(1)$.

Lemma 7.6 *Let u be any vertex of $\{0,1\}^n$ and f a non-constant Boolean function of n variables, which satisfies $f(u) = 0$. Let the groups G and H of isometries of $\{0,1\}^n$ be such that*

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

Then G, H and u define f.

Proof. The assumptions imply that H is not transitive. By Lemma 7.4, the size of the orbits of H is 2^{n-1}. This implies that H has two orbits and, hence, the third requirement of Definition 7.3 is satisfied. □

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

Lemma 7.7 *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 7.5 guarantees the existence of groups G and H and a vertex u, which define f. If G is not minimally transitive, let G' be any minimally transitive subgroup of G and $H' = H \cap G'$. Since H' is intransitive, it follows that $|G' : H'| > 1$. Moreover, since $|G' : H'| \leq |G : H|$, we have $|G' : H'| = 2$. Clearly, $f(x^h) = f(x)$ for every $h \in H'$. 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 [7].

Theorem 7.8 (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.

Lemma 7.9 *Every minimally transitive group of isometries of $\{0,1\}^n$ is a 2-group.*

Proof. Let G be a minimally transitive group of isometries. If G is not a 2-group, then every its Sylow 2-subgroup is a proper subgroup, which is also transitive by Theorem 7.8. Since this is in contradiction with the assumptions, G is a 2-group. □

This allows to strengthen the characterization of the transitive functions.

Theorem 7.10 *A non-constant 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 7.7, the function f is defined by G, H and u, such that G is minimally transitive. By Lemma 7.9, G is a 2-group. □

Minimally transitive groups of isometries of $\{0,1\}^n$ can be characterized as follows.

Theorem 7.11 *A transitive group G of isometries of $\{0,1\}^n$ is minimally transitive, if and only if G is a 2-group and for some vertex u, every maximal proper subgroup of G contains* $\mathrm{Stab}_G(u)$.

Proof. Due to Lemma 7.9, in order to characterize the minimally transitive groups of isometries, it is sufficient to consider 2-groups.

Assume, G is a transitive 2-group and u is a vertex. Group G is minimally transitive, if and only if there is no maximal proper subgroup K, which is transitive. Since G is a 2-group, the maximal proper subgroups of G are exactly the subgroups K, for which $|G : K| = 2$. A subgroup K of G is transitive, if and only if $\mathrm{Orbit}_G(u)$ and $\mathrm{Orbit}_K(u)$ have the same size. By the orbit-stabilizer theorem, this is equivalent to $|\mathrm{Stab}_G(u) : \mathrm{Stab}_K(u)| = |G : K|$. On the other hand, for every subgroup K, we have $|\mathrm{Stab}_G(u) : \mathrm{Stab}_K(u)| \leq |G : K|$. Altogether, G is minimally transitive, if and only if for every subgroup K such that $|G : K| = 2$, we have $|\mathrm{Stab}_G(u) : \mathrm{Stab}_K(u)| < 2$.

Since the index $|\mathrm{Stab}_G(u) : \mathrm{Stab}_K(u)|$ is an integer power of 2, the condition from the previous paragraph is equivalent to the condition that for all subgroups K, such that $|G : K| = 2$, we have $|\mathrm{Stab}_G(u) : \mathrm{Stab}_K(u)| = 1$ or, equivalently, $\mathrm{Stab}_G(u) \leq K$. This implies the theorem. □

For a minimally transitive group G of isometries of $\{0,1\}^n$, the characterization of the set of 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 2-group from [3], we obtain the following theorem.

Theorem 7.12 *If G is a minimally transitive 2-group of isometries, such that k is the minimal number of its generators, then there are 2^k-1 maximal proper subgroups H of G. If u is a vertex, then there are 2^k-1 different transitive functions satisfying $f(u)=0$ and defined by G and some of its maximal subgroups.*

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 7.4, every maximal proper subgroup H of G defines, together with G and u, a transitive function. Moreover, every such subgroup H of G contains $\mathrm{Stab}_G(u)$. Hence, Lemma 7.1(ii) implies that the transitive functions obtained for different subgroups H are different.

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 [3]. There is a bijection between the maximal subgroups of Z_2^k and the subspaces of F_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. Each of these groups defines a transitive function satisfying $f(u)=0$ and these functions are different. □

8 Uniquely transitive functions

If G is a transitive group of isometric transformations of $\{0,1\}^n$, 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 hypercube. Some of the transitive functions are defined by a transitive group G of size equal to 2^n.

Definition 8.1 A Boolean function is uniquely transitive, if it is defined by groups G and H and a vertex u, such that G has size 2^n, or, equivalently, if G is a regular group of permutations of the vertices of the hypercube.

It is easy to prove that every linear and quadratic transitive function is uniquely transitive. In fact, the groups of isometries used to verify transitivity of these functions in the previous sections have size 2^n. Using computer search, it was possible to find about 60 non-isomorphic transitive functions of at most 12 variables and degree 3. Each of these functions appeared to be uniquely transitive.

Question. Is there a transitive function, which is not uniquely 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 stimulating discussions concerning vertex-transitive Boolean functions.

References

[1] Andris Ambainis, Yihan Gao, Jieming Mao, Xiaoming Sun, Song Zuo. New upper bound on block sensitivity and certificate complexity in terms of sensitivity.
http://arxiv.org/abs/1306.4466

[2] Sourav Chakraborty. Sensitivity, Block Sensitivity and Certificate Complexity of Boolean Functions. Masters Thesis, 2005.
http://www.cmi.ac.in/~sourav/papers/mastersthesis.pdf

[3] David A. Craven. The Theory of p-Groups. Hilary Term, 2008.
https://people.maths.ox.ac.uk/craven/pgroups.html

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

[5] Alexander Hulpke. Constructing Transitive Permutation Groups.
http://www.math.colostate.edu/~hulpke/paper/ctg.pdf

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

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

[8] The Wikipedia article "Block (permutation group theory)",
http://en.wikipedia.org/wiki/Block_(permutation_group_theory)

ECCC ISSN 1433-8092

http://eccc.hpi-web.de