Partitions of the Boolean cube with a vertex-transitive automorphism group

Savický, Petr
2012

Institute of Computer Science
Academy of Sciences of the Czech Republic

Partitions of the Boolean cube with a vertex-transitive automorphism group

Petr Savicky

Technical report No. 1175

December 2012

Pod Vodárenskou věží 2, 182 07 Prague 8, phone: +420 266 051 111, fax: +420 286 585 789,
e-mail:ics@cs.cas.cz

Institute of Computer Science
Academy of Sciences of the Czech Republic

Partitions of the Boolean cube with a vertex-transitive automorphism group[1]

Petr Savicky[2]

Technical report No. 1175

December 2012

Abstract:

A Boolean function is called transitive, if there is a group of isometric mappings of the Boolean cube, which is transitive on the vertices of the cube, and the partition of the cube into two parts defined by the function as the preimage of 0 and the preimage of 1 is invariant under this group. Several constructions of transitive functions and an estimate of the number of these functions are presented.

Keywords:
Boolean function, partition of the Boolean cube, vertex-transitive group of automorphisms

[1]The author was supported by the Grant Agency of the Czech Republic under the grant number P202/10/1333 and by institutional support of the Institute of Computer Science (RVO:67985807).

[2]Institute of Computer Science, Academy of Sciences of Czech Republic Pod Vodarenskou Vezi 2, 182 07 Praha 8, Czech Republic, savicky@cs.cas.cz

Partitions of the Boolean cube with a vertex-transitive automorphism group

Petr Savicky

Abstract

A Boolean function is called transitive, if there is a group of isometric mappings of the Boolean cube, which is transitive on the vertices of the cube, and the partition of the cube into two parts defined by the function as the preimage of 0 and the preimage of 1 is invariant under this group. Several constructions of transitive functions and an estimate of the number of these functions are presented.

1 Introduction

Symmetry is an important tool to show simplicity of an object from some point of view. A standard notion of symmetry for Boolean functions is invariance under permutations of the variables. In this paper, we demonstrate a different type of symmetry, which is based on isometric mappings of the Boolean cube with the Hamming distance as a metric space.

A non-constant Boolean function represents a partition of its domain into two parts, the preimage of 0 and the preimage of 1. We investigate partitions of the Boolean cube defined in this way and their automorphism groups consisting of isometries of the cube. If σ is an automorphism of the partition defined by a function f, then we have either $f(\sigma(x)) = f(x)$ or $f(\sigma(x)) = \neg f(x)$ for every input x. In the former case, we say that σ preserves f and in the latter case, we say that σ reverses f. We investigate functions, which define a partition of the cube, whose automorphism group is transitive on the vertices of the cube. For simplicity, the functions, for which such a group exists, will be called transitive functions.

We demonstrate several constructions of non-linear transitive functions. The largest number of transitive functions of $2k$ variables is obtained using the Fourier transform of the functions, where the nonzero coefficients of the Fourier transform are given by an appropriate bent function of k variables, where k is even. In particular, we prove that any quadratic bent function may be used. Moreover, an example of a bent function of 6 variables and degree 3 over Z_2, which yields a transitive function of 12 variables in the same way, is presented. Since the number of quadratic bent functions of k variables is $2^{\Theta(k^2)}$, this implies a lower bound of magnitude $2^{\Omega(n^2)}$ on the number of the transitive functions of n variables. We also prove an upper bound on this number of magnitude $2^{O(n^2 \log^2 n)}$.

Related, but a different notion are Boolean functions, which are invariant under a transitive group of permutations of their variables. For example, the

functions studied in Section 5.4 Cyclically invariant function of [4] belong to this class.

The constructions of transitive functions in this paper generalize examples of these functions obtained by a computer search. The program generated small sets of random isometries of $\{0,1\}^n$ for even n up to 12. For the cases, when the chosen isometries generate a group with two orbits, the corresponding Boolean function was created and analyzed using Fourier transform. The formula (1) generalizes some of the non-linear functions obtained in this way. In most cases, the function h was a quadratic bent function with the exception of the functions equivalent to $h_{6,cub}$ presented in Section 10. In some cases, the function h was a symmetric bent function. Analysis of these cases lead to the general construction presented in Section 5.

2 Basic notions and a simple example

The addition in Z_2 will be denoted $\oplus$. The parity function is the sum of its input variables in Z_2. By $\mathrm{mod}(k,m)$, we denote the residue of k modulo m. For a logical condition C, let $[C]$ be 1, if C is satisfied and 0 otherwise.

Isometry of the Boolean cube is an automorphism of the Boolean cube considered as a metric space with respect to the Hamming distance. One can verify that isometric mappings of the Boolean cube of dimension n are exactly the mappings

$$\sigma(x) = (x_{p(1)} \oplus s_1, \ldots, x_{p(n)} \oplus s_n) \ ,$$

where $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, p is a permutation of the indices $\{1, \ldots, n\}$ and $s \in \{0,1\}^n$. An isometry σ preserves f, if $f(\sigma(x)) = f(x)$ for all $x \in \{0,1\}^n$ and reverses f, if $f(\sigma(x)) = \neg f(x)$ for all $x \in \{0,1\}^n$. Clearly, an isometry σ is an automorphism of the partition defined by a function f, if and only if σ either preserves f or reverses f.

Definition 2.1 The partition of the Boolean cube $\{0,1\}^n$ into two parts defined by a non-constant function $f : \{0,1\}^n \to \{0,1\}$ has a transitive group of automorphisms, if there is a group of isometries of the cube, which acts transitively on the vertices of the cube and the function f is either preserved or reversed by all its elements.

For simplicity, the automorphisms of the partition defined by a function f will also be called the automorphisms of f. A function with a transitive group of automorphisms will be called a transitive function for simplicity.

If A is a transitive group of automorphisms of a function f, then let A' be the subgroup consisting of the automorphisms, which preserve f. This subgroup has index 2, since it is the kernel of a nontrivial homomorphism $A \to Z_2$, which maps $\sigma \in A$ to 0, if σ preserves f, and to 1, if σ reverses f.

Clearly, every transitive function is balanced, which means that the size of the preimage of 0 and 1 have the same size. It is easy to see that the partition corresponding to any linear function is invariant, in particular, under isometries $\sigma(x) = x \oplus s$, which form a transitive group of automorphisms of the Boolean cube. Consequently, every non-constant linear function is transitive.

The smallest number of variables, for which there is a nonlinear transitive function is 4. An example of a nonlinear transitive function on 4 variables may be obtained as the function g defined either as

$$g(x) = \left[\left(\bigvee_{i=1}^{3} x_i < x_{i+1} \right) \wedge \left(\bigvee_{i=1}^{3} x_i > x_{i+1}) \right) \right]$$

or, equivalently, as the polynomial

$$g(x) = (x_1 \oplus x_3)(x_2 \oplus x_4) \oplus x_2 \oplus x_3$$

over Z_2. The group of automorphisms of this function is generated, for example, by $\sigma_1, \sigma_2, \sigma_3$, where

$$\sigma_1(x) = (x_2,\, x_3,\, x_4,\, x_1 \oplus 1) \ ,$$

$$\sigma_2(x) = (x_4,\, x_3,\, x_2,\, x_1) \ ,$$

and

$$\sigma_3(x) = (x_1,\, x_2 \oplus 1,\, x_3,\, x_4 \oplus 1) \ .$$

Note that σ_1 and σ_2 preserve the function g and σ_3 reverses g. In order to show that g is a transitive function, one can also use any subgroup, which is transitive, for example the subgroup generated by σ_1, σ_3.

A useful tool for the analysis of the transitive functions is the Fourier transform of the Boolean functions, which we use in the form of a polynomial in the domain $\{1, -1\}$. The polynomial, which represents the Fourier transform of a function $f(x)$ will be denoted $f^*(x^*)$. This polynomial represents f using the transformations $x_i^* = (-1)^{x_i}$ and $f^*(x^*) = (-1)^{f(x)}$. See [1] for more detail. The Fourier polynomial $f^* : \{1, -1\}^4 \to \{1, -1\}$ for f is given as

$$f^*(x^*) = \frac{1}{2}(x_1^* x_2^* - x_1^* x_4^* + x_2^* x_3^* + x_3^* x_4^*) \ .$$

3 Parity of independent transitive functions

In order to combine several transitive functions into a transitive function on a larger number of variables, one may use the following.

Theorem 3.1 *If f_1, f_2 are transitive functions on disjoint sets of variables, then $f_1 \oplus f_2$ is a transitive function.*

Proof. Denote the domain of f_i as X_i for $i = 1, 2$. Moreover, let f_i be invariant under a transitive group A_i of isometric maps of the cube X_i. Then $f_1 \oplus f_2$ is invariant under the direct product $A_1 \times A_2$, which acts transitively on $X_1 \times X_2$. □

Using this theorem, a non-linear transitive function may be constructed on any number of variables $n \geq 4$ by combining a non-linear transitive function on 4 variables and the parity of the remaining $n - 4$ variables. A larger number of non-linear transitive functions of n variables may be obtained by choosing any partition of the variables into $m \geq 1$ disjoint sets X_i, $i = 1, \ldots, m$ of size 4

and a possibly empty set X_{m+1} of the remaining variables. Then, a transitive function of n variables may be obtained in the form $\bigoplus_{i=1}^{m} g(X_i) \oplus par(X_{m+1})$, where $g(X_i)$ is the function g applied to the variables in X_i in any order and $par(X_{m+1})$ is the parity of the variables in X_{m+1}.

The number of transitive functions of n variables constructed in this way is $2^{\Theta(n \log n)}$. In Section 9, a construction of a larger number of transitive functions is described.

4 Isometric maps based on swapping variables

Let $n = 2k$, where $k \geq 1$ is an integer. The variables of the function will be denoted $x_1, \ldots, x_k, y_1, \ldots, y_k$ and an input vector will be denoted either as $\langle x, y \rangle$ or in the form of a 2 by k matrix of the form

$$\begin{pmatrix} x_1, & \ldots, & x_k \\ y_1, & \ldots, & y_k \end{pmatrix}$$

Let $d, r, s \in \{0,1\}^k$. Then, let $\delta_{d,r,s}$ be the mapping $\{0,1\}^{2k} \to \{0,1\}^{2k}$ such that $\langle x', y' \rangle = \delta_{d,r,s}(\langle x, y \rangle)$ satisfies for every $j = 1, \ldots, k$

$$\begin{pmatrix} x'_j \\ y'_j \end{pmatrix} = \begin{pmatrix} x_j \oplus r_j \\ y_j \oplus s_j \end{pmatrix} \text{ if } d_j = 0$$

and

$$\begin{pmatrix} x'_j \\ y'_j \end{pmatrix} = \begin{pmatrix} y_j \oplus s_j \\ x_j \oplus r_j \end{pmatrix} \text{ if } d_j = 1 \ .$$

Let D be a $0,1$-matrix of dimension k by k and let $c \in \{0,1\}^k$. The matrix D and vector c will be used as parameters of the group of isometries $A(D,c)$ of the Boolean cube $\{0,1\}^{2k}$. For $i = 1, \ldots, k$, consider the isometry $\sigma_{1,i} = \delta_{d,r,s}$, where d is i-th row od D, and the vectors r, s are given by

$$r = \begin{cases} e_i & \text{if } c_i = 0 \\ 0_k & \text{if } c_i = 1 \end{cases}$$

and

$$s = \begin{cases} 0_k & \text{if } c_i = 0 \\ e_i & \text{if } c_i = 1 \ . \end{cases}$$

Moreover, for $i = 1, \ldots, k$, let $\sigma_{2,i} = \delta_{d,r,s}$, where $d = 0_k$, and $r = s = e_i$. Note that $\sigma_{2,i}(\langle x, y \rangle) = (\langle x \oplus e_i, y \oplus e_i \rangle)$.

Definition 4.1 Let D and c be as above. Then, let $A(D,c)$ be the group of the isometries of $\{0,1\}^{2k}$ generated by $\sigma_{1,i}$ and $\sigma_{2,i}$ for $i = 1, \ldots, k$.

In order to prove that $A(D,s)$ is transitive, we prove a slightly more general statement.

Lemma 4.2 *Let A be a group of isometries of $\{0,1\}^{2k}$ generated by δ_{d_i,r_i,s_i} for $i = 1, \ldots, m$ and by $\sigma_{2,i}$ for $i = 1, \ldots, k$. Then, A is transitive on the vertices of $\{0,1\}^{2k}$ if and only if the vectors $r_i \oplus s_i$ for $i = 1, \ldots, m$ generate the additive group Z_2^k.*

Proof. Consider the mapping $\omega : \{0,1\}^{2k} \to \{0,1\}^k$ defined by

$$\omega(\langle x, y\rangle) = x \oplus y \ .$$

Clearly, $\omega(\langle 0_k, 0_k\rangle) = 0_k$ and for every $i = 1, \ldots, m$ and every $\langle x, y\rangle$, we have

$$\omega(\delta_{d_i,r_i,s_i}(\langle x, y\rangle)) = \omega(\langle x, y\rangle) \oplus r_i \oplus s_i \ ,$$

and for every $i = 1, \ldots, k$, we have

$$\omega(\sigma_{2,i}(\langle x, y\rangle)) = \omega(\langle x, y\rangle) \ .$$

It follows that the range of $\omega(\sigma(\langle 0_k, 0_k\rangle))$ over $\sigma \in A$ is the closure of the vectors $r_i \oplus s_i$ for $i = 1, \ldots, m$ in Z_2^k. If this closure is not equal to Z_2^k, then A cannot be transitive on $\{0,1\}^{2k}$. In order to prove the opposite direction, assume that this closure is equal to Z_2^k and let $\langle a, b\rangle$ be an arbitrary element of $\{0,1\}^{2k}$. Hence, there is $\alpha \in A$ such that $\omega(\alpha(\langle 0_k, 0_k\rangle)) = a \oplus b$. Denote $\langle a', b'\rangle = \alpha(\langle 0_k, 0_k\rangle)$. For every $j = 1, \ldots, k$, we have $a'_j \oplus b'_j = a_j \oplus b_j$. It is easy to see that there is $\beta \in A$, more specifically an appropriate product of some of the generators $\sigma_{2,i}$, such that $\langle a, b\rangle = \beta(\langle a', b'\rangle) = \beta(\alpha(\langle 0_k, 0_k\rangle))$. Consequently, A is transitive as required. □

Theorem 4.3 *For every k, every matrix D and vector c, the group $A(D, c)$ is transitive on $\{0,1\}^{2k}$.*

Proof. The group $A(D, c)$ is generated by $\sigma_{1,i}$ and $\sigma_{2,i}$ for $i = 1, \ldots, k$. By construction of $\sigma_{1,i}$, we have $\sigma_{1,i} = \delta_{d_i,r_i,s_i}$, where $r_i \oplus s_i = e_i$. Since the vectors e_i generate Z_2^k, Lemma 4.2 implies the theorem. □

Definition 4.4 Let $A'(D, c)$ be the subgroup of $A(D, c)$ generated by $\sigma_{1,i}$ for $i = 1, \ldots, k$ and by the products $\sigma_{2,i_1} \circ \sigma_{2,i_2}$ for $i_1 \neq i_2$.

We are interested in cases, when $A'(D, c)$ has two orbits and each element of $A(D, c)$ either preserves the orbits of $A'(D, c)$ or exchanges them. Let f be a function of $n = 2k$ variables, which satisfies $f(\langle x, y\rangle) = 0$ if $\langle x, y\rangle$ belongs to the same orbit of $A'(D, c)$ as $\langle 0_k, 0_k\rangle$ and $f(\langle x, y\rangle) = 1$ otherwise. The function f defined in this way is a transitive function, since $A(D, c)$ is a transitive group of its automorphisms.

Since we do not have a characterization of D and c, for which the group $A'(D, c)$ defined above has two orbits, the examples of the transitive functions presented in this paper are demonstrated by describing a non-constant function f and by proving that f is preserved by $A'(D, c)$ and preserved or reversed by every element of $A(D, c)$ for an appropriate D and c. The properties of the groups $A'(D, c)$ and $A(D, c)$ for an arbitrary matrix D and a vector c remain an open question.

5 A transitive function which is symmetric on pairs of variables

In this section, we describe for any integer k a transitive function f_k of $2k$ variables. For this, we use the group $A(D,c)$ from Definition 4.1 with $D = N_k$ and $c = 0_k$, where $N_k = 1_{k\times k} - I_k$ is the complement of the identity matrix.

The elements of D satisfy $d_{i,i} = 0$ and $d_{i,j} = 1$, if $i \neq j$. Hence, the isometries $\sigma_{1,i}$ and $\sigma_{2,i}$ generating $A(N_k, 0_k)$ have the form

$$\sigma_{1,i}(\langle x,y\rangle) = \begin{pmatrix} y_1, & \ldots, & y_{i-1}, & x_i \oplus 1, & y_{i+1}, & \ldots, & y_k \\ x_1, & \ldots, & x_{i-1}, & y_i, & x_{i+1}, & \ldots, & x_k \end{pmatrix}$$

and

$$\sigma_{2,i}(\langle x,y\rangle) = \begin{pmatrix} x_1, & \ldots, & x_{i-1}, & x_i \oplus 1, & x_{i+1}, & \ldots, & x_k \\ y_1, & \ldots, & y_{i-1}, & y_i \oplus 1, & y_{i+1}, & \ldots, & y_k \end{pmatrix} .$$

Let $\mu : \{0,1\}^2 \to Z_4$ be defined by the table

x	y	$\mu(x,y)$
0	0	0
1	0	1
1	1	2
0	1	3

Note that $\mu(y,x) = -\mu(x,y)$, $\mu(x\oplus 1, y) = 1 - \mu(x,y)$, and $\mu(x\oplus 1, y\oplus 1) = \mu(x,y) + 2$. Let us extend the mapping $\mu : \{0,1\}^2 \to Z_4$ to a mapping $\mu : \{0,1\}^{2k} \to Z_4$ by the formula

$$\mu(\langle x,y\rangle) = \sum_{j=1}^{k} \mu(x_j, y_j) .$$

Lemma 5.1 *For every $\langle x,y\rangle \in \{0,1\}^{2k}$ and $i = 1,\ldots,k$, we have*

$$\mu(\sigma_{1,i}(\langle x,y\rangle)) = 1 - \mu(\langle x,y\rangle) ,$$

$$\mu(\sigma_{2,i}(\langle x,y\rangle)) = \mu(\langle x,y\rangle) + 2 .$$

Proof. In order to prove the first identity, denote $\langle x',y'\rangle = \sigma_{1,i}(\langle x,y\rangle)$. By the definition of $\sigma_{1,i}$, we have

$$\mu(x'_i, y'_i) = \mu(x_i \oplus 1, y_i) = 1 - \mu(x_i, y_i)$$

and for every $j \neq i$ we have

$$\mu(x'_j, y'_j) = \mu(y_j, x_j) = -\mu(x_j, y_j)$$

By taking the sum of the contributions for all $j = 1,\ldots,k$, we get

$$\mu(x',y') = 1 - \mu(x,y)$$

as required.

In order to prove the second identity, let $\langle x', y' \rangle = \sigma_{2,i}(\langle x, y \rangle)$. For all $j \neq i$, we have $\mu(x'_j, y'_j) = \mu(x_j, y_j)$ and for the i-th coordinate, we have $\mu(x'_i, y'_i) = \mu(x_i \oplus 1, y_i \oplus 1) = \mu(x_i, y_i) + 2$. Consequently, we have

$$\mu(\langle x', y' \rangle) = \mu(\langle x, y \rangle) + 2$$

as required. □

Definition 5.2 *Let k be any integer and f_k be the Boolean function $f_k : \{0,1\}^{2k} \to \{0,1\}$ defined as*

$$f_k(\langle x, y \rangle) = [\ \mu(\langle x, y \rangle) \in \{2, 3\}\ ]\ .$$

Theorem 5.3 *For every k, the Boolean function f_k is preserved by $A'(N_k, 0_k)$ and the partition defined by f_k is invariant under $A(N_k, 0_k)$. In particular, f_k is a transitive function of $2k$ variables.*

Proof. By Theorem 4.3, the group $A(D, s)$ is a transitive group of automorphisms of the Boolean cube of dimension $2k$. Hence, it is sufficient to prove that f_k is preserved by the generators $\sigma_{1,i}$ and reversed by the generators $\sigma_{2,i}$.

Each of the subsets $\{0, 1\} \subseteq Z_4$ and $\{2, 3\} \subseteq Z_4$ is invariant under the transformation $Z_4 \to Z_4$ defined as $t \mapsto (1 - t)$. Hence, by Lemma 5.1, the generators $\sigma_{1,i}$ satisfy $f_k(\sigma_{1,i}(\langle x, y \rangle)) = f_k(\langle x, y \rangle)$ for every $\langle x, y \rangle \in \{0,1\}^{2k}$.

The transformation $Z_4 \to Z_4$ defined as $t \mapsto (t + 2)$ exchanges $\{0, 1\}$ with its complement $\{2, 3\}$. Hence, by Lemma 5.1, the generators $\sigma_{2,i}$ satisfy $f_k(\sigma_{2,i}(\langle x, y \rangle)) = \neg f_k(\langle x, y \rangle)$ for every $\langle x, y \rangle \in \{0,1\}^{2k}$. □

6 A Fourier polynomial invariant under swapping variables

In this section, we demonstrate a generalization of the function f_k from Theorem 5.3 for the cases, when k is even and, consequently, n is divisible by 4. Let us consider the Fourier polynomial

$$p^*_h(\langle x^*, y^* \rangle) = \frac{1}{2^{k/2}} \sum_{u \in \{0,1\}^k} (-1)^{h(u)} \prod_{u_j = 1} x^*_j \prod_{u_j = 0} y^*_j\ , \tag{1}$$

where h is a Boolean function of k variables. We are interested in cases, when p^*_h is the Fourier polynomial of a Boolean function. This condition is equivalent to the condition that the range of values of p^*_h is $\{1, -1\}$. In this case, the corresponding function $\{0,1\}^{2k} \to \{0,1\}$ is denoted p_h. All nonzero Fourier coefficients of such a function have the same absolute value and the structure of the corresponding monomials is restricted, since for each $j = 1, \ldots, k$, exactly one of the variables x^*_j and y^*_j is contained in each monomial with a nonzero coefficient.

We shall prove in Section 8 that the Fourier polynomial of the function f_k from Definition 5.2 has the above form with h, which is a symmetric and quadratic bent function. In Section 9, we prove that for every quadratic bent function h, the polynomial (1) defines a transitive Boolean function of $2k$ variables. Additionally, in Section 10, we demonstrate a cubic bent function of 6 variables, for which the polynomial (1) defines a transitive function. On the other hand, not every bent function h yields a transitive function, since there are at least $2^{2^{k/2}}$ bent functions of k variables, which is much more than the number of transitive functions of $n = 2k$ variables, for which a bound $2^{O(n^2 \log^2 n)}$ is proven in Section 11.

In order to substitute into the Fourier polynomial, we use the isometries $\delta^*_{d,r,s}$ of $\{1,-1\}^{2k}$ induced by the original isometries $\delta_{d,r,s}$ of $\{0,1\}^{2k}$.

Theorem 6.1 *Let p^*_h be the polynomial (1) and let $d, r, s \in \{0,1\}^k$. Then, the Fourier polynomial obtained from p^*_h by substituting $\delta^*_{d,r,s}(\langle x^*, y^*\rangle)$ satisfies*

$$p^*_h(\delta^*_{d,r,s}(\langle x^*, y^*\rangle)) = p^*_{h'}(\langle x^*, y^*\rangle)$$

where

$$h'(u) = h(u \oplus d) \oplus \bigoplus_j (r_j \oplus s_j)u_j \oplus \bigoplus_j s_j \ . \tag{2}$$

Proof. We will substitute $\delta_{d,r,s}(\langle x, y\rangle)$ into (1) in two steps corresponding to the decomposition $\delta^*_{d,r,s}(\langle x, y\rangle) = \delta^*_{d,0_k,0_k}(\delta^*_{0_k,r,s}(\langle x, y\rangle))$. In the first step, we substitute $\delta^*_{d,0_k,0_k}(\langle x, y\rangle)$, which represents exchanging x^*_j and y^*_j, if $d_j = 1$ and keeping these variables otherwise. We obtain

$$p^*_h(\delta_{d,0_k,0_k}(\langle x^*, y^*\rangle)) = \frac{1}{2^{k/2}} \sum_{u\in\{0,1\}^k} (-1)^{h(u)} \prod_{u_j = 1\oplus d_j} x^*_j \prod_{u_j = d_j} y^*_j \ .$$

In the right hand side, substitute for u using the identity $u = v \oplus d$. This yields

$$p^*_h(\delta_{d,0_k,0_k}(\langle x^*, y^*\rangle)) = \frac{1}{2^{k/2}} \sum_{v\in\{0,1\}^k} (-1)^{h(v\oplus d)} \prod_{v_j = 1} x^*_j \prod_{v_j = 0} y^*_j \ , \tag{3}$$

In the second step, we substitute $\delta^*_{0_k,r,s}(\langle x, y\rangle)$ into both sides of (3). This represents replacing x^*_j by $(-1)^{r_j} x^*_j$ and y^*_j by $(-1)^{s_j} y^*_j$ and yields

$$p^*_h(\delta_{d,0_k,0_k}(\delta_{0_k,r,s}(\langle x^*, y^*\rangle)))$$

$$= \frac{1}{2^{k/2}} \sum_{v\in\{0,1\}^k} (-1)^{h(v\oplus d)} \prod_j (-1)^{r_j v_j \oplus s_j(v_j\oplus 1)} \prod_{v_j = 1} x^*_j \prod_{v_j = 0} y^*_j \ .$$

Since

$$\bigoplus_j (r_j v_j \oplus s_j(v_j \oplus 1)) = \bigoplus_j (r_j \oplus s_j)v_j \oplus \bigoplus_j s_j \ ,$$

the theorem follows. □

Theorem 6.1 implies that a Boolean function f, whose Fourier polynomial has the form (1), is preserved by $\delta_{d,r,s}$ if and only if $h' = h$, where h' is defined by (2). Similarly, f is reversed by $\delta_{d,r,s}$, if and only if $h' = h \oplus 1$.

7 Symmetric bent functions

Let $q_{k,l} : \{0,1\}^k \to \{0,1\}$ be the symmetric Boolean function defined as

$$q_{k,l}(u) = \left[\sum_{j=1}^{k} u_j + l \in \{2,3\} \pmod 4 \right] .$$

For every even k, these functions are bent functions and any symmetric bent function of k variables has this form, see [2]. Let m_1, m_0 be the last two digits of the binary expansion of $m = \sum_{j=1}^{k} u_j$. Clearly, $m \equiv 2m_1 + m_0 \pmod 4$ and by Lucas' theorem (see Wikipedia), we have

$$\binom{m}{2} \equiv m_1 \pmod 2$$

In particular, we have

$$m \in \{2,3\} \pmod 4 \Leftrightarrow \binom{m}{2} \equiv 1 \pmod 2 .$$

This implies the first of the following identities and the other may be derived using also the identity for m_0. We have

$$\begin{aligned}
q_{k,0}(u) &= \bigoplus_{i_1<i_2} u_{i_1} u_{i_2} , \\
q_{k,1}(u) &= \bigoplus_{i_1<i_2} u_{i_1} u_{i_2} \oplus \bigoplus_{i} u_i , \\
q_{k,2}(u) &= \bigoplus_{i_1<i_2} u_{i_1} u_{i_2} \oplus 1 , \\
q_{k,3}(u) &= \bigoplus_{i_1<i_2} u_{i_1} u_{i_2} \oplus \bigoplus_{i} u_i \oplus 1 .
\end{aligned}$$

It follows that the functions $q_{k,l}$ are quadratic over Z_2.

For every even k, let h_k be the symmetric Boolean function

$$h_k = q_{k,1-k/2} .$$

By the definition of $q_{k,l}$, the value $l = 1-k/2$ is interpreted modulo 4. Moreover, for every even k, let h'_k be the symmetric bent function

$$h'_k = q_{k,\mathrm{mod}(1-k/2,2)} .$$

Lemma 7.1 *The function h_k achieves the value 0 on $2^{k-1} + 2^{k/2-1}$ inputs and the value 1 on $2^{k-1} - 2^{k/2-1}$ inputs.*

Proof. Since the total number of inputs is 2^k, the statement of the lemma is equivalent to the identity

$$s_h = \sum_u (-1)^{h_k(u)} = 2^{k/2} .$$

Denote

$$s_{k,l} = \sum_u (-1)^{q_{k,l}(u)}$$

and let ι denote the complex unit, in order to distinguish it from an index i. Use the binomial theorem to expand the power $z = (1+\iota)^k$. The coefficient of the term containing ι^i is the number of inputs satisfying $\sum_j u_j = i$. One may verify that the value $s_{k,l}$ for $l \in Z_4$ is as follows.

l	$s_{k,l}$
0	$\mathrm{Re}\, z + \mathrm{Im}\, z$
1	$\mathrm{Re}\, z - \mathrm{Im}\, z$
2	$-\mathrm{Re}\, z - \mathrm{Im}\, z$
3	$-\mathrm{Re}\, z + \mathrm{Im}\, z$

Since k is even, we have $z = (2\,\iota)^{k/2}$. Moreover, we have $s_h = s_{k,l}$ with l satisfying $l \equiv 1 - k/2 \pmod 4$. The following table presents the value of z under this assumption, so we can assume $k/2 \equiv 1 - l \pmod 4$.

l	z
0	$\iota\, 2^{k/2}$
1	$2^{k/2}$
2	$-\iota\, 2^{k/2}$
3	$-2^{k/2}$

In each of these cases, we have $s_h = s_{k,l} = 2^{k/2}$ as required. □

For the next lemma, recall that $N_k = 1_{k\times k} - I_k$.

Lemma 7.2 *For every $i = 1, \ldots, k$, every $d \in \{0,1\}^k$ and every $u \in \{0,1\}^k$, we have*

$$h_k(u \oplus d) = h_k(u) \oplus d^t\, N_k\, u \oplus h'_k(d)\ .$$

Proof. By substituting $u \oplus d$ to the quadratic polynomial representing $q_{k,0}$, we obtain for every even k

$$q_{k,0}(u \oplus d) = q_{k,0}(u) \oplus d^t N_k u \oplus q_{k,0}(d)\ .$$

Starting from this identity, we prove similar identities for $q_{k,l}$ for $l = 1, 2, 3$. Since the quadratic polynomial for $q_{k,1}$ differs from $q_{k,0}$ only in the linear terms, we have also

$$q_{k,1}(u \oplus d) = q_{k,1}(u) \oplus d^t N_k u \oplus q_{k,1}(d)\ .$$

Since $q_{k,2} = q_{k,0} \oplus 1$, we have

$$q_{k,2}(u \oplus d) = q_{k,2}(u) \oplus d^t N_k u \oplus q_{k,0}(d)\ .$$

Since $q_{k,3} = q_{k,1} \oplus 1$, we have

$$q_{k,3}(u \oplus d) = q_{k,3}(u) \oplus d^t N_k u \oplus q_{k,1}(d)\ .$$

In order to complete the proof of the lemma, note that the required identity for the functions h_k and h'_k is equivalent to the identity for $q_{k,l}$ and $q_{k,\mathrm{mod}(l,2)}$ proved above, since $h_k = q_{k,l}$ and $h'_k = q_{k,\mathrm{mod}(l,2)}$, where $l \equiv 1 - k/2 \pmod 4$. □

8 Fourier polynomial of the partially symmetric example

Let $D = N_k$ and for every $i = 1, \ldots, k$, let d_i be the i-th row of the matrix D.

Lemma 8.1 *For every $i = 1, \ldots, k$ and every $u \in \{0,1\}^k$, we have*

$$h_k(u \oplus d_i) \oplus u_i = h_k(u) \ .$$

Proof. Use Lemma 7.2 with $d = d_i$. Note that d_i contains $k-1$ ones. Since k is even, we have $d_i^t N_k u = e_i^t u = u_i$. Moreover, for every even k and $l \equiv 1 - k/2 \pmod 2$, we have $h'_k(d_i) = q_{k,l}(d_i) = 0$, since $k - 1 + l \notin \{2, 3\} \pmod 4$. □

Theorem 8.2 *For every even k, the Fourier polynomial for f_k is given by the formula (1), where $h = h_k$.*

Proof. By Theorem 5.3, function f_k is invariant under the group $A'(N_k, 0_k)$ and the partition defined by f_k is invariant under $A(N_k, 0_k)$. Since $A(N_k, 0_k)$ is transitive, the function f_k is the unique non-constant function, which satisfies $f_k(\langle 0_k, 0_k\rangle) = 0$, is invariant under the group $A'(N_k, 0_k)$, and its partition is invariant under $A(N_k, 0_k)$.

Consider the automorphisms $\sigma^*_{1,i}$ and $\sigma^*_{2,i}$ on $\{1,-1\}^{2k}$ induced by $\sigma_{1,i}$ and $\sigma_{2,i}$. In order to prove the theorem, it is sufficient to prove that the polynomial $p^*_{h_k}$ defined by (1) with $h = h_k$ satisfies

$$p^*_{h_k}(\langle 1_k, 1_k\rangle) = 1 \tag{4}$$

and for every $i = 1, \ldots, k$ satisfies

$$p^*_{h_k}(\sigma_{1,i}(\langle x^*, y^*\rangle)) = p^*_{h_k}(\langle x^*, y^*\rangle) \tag{5}$$

and

$$p^*_{h_k}(\sigma_{2,i}(\langle x^*, y^*\rangle)) = -p^*_{h_k}(\langle x^*, y^*\rangle) \ . \tag{6}$$

Let $A^*(N_k, 0_k)$ be the group of isometries of $\{1,-1\}^{2k}$ generated by $\sigma^*_{1,i}$ and $\sigma^*_{2,i}$. Since $A(N_k, 0_k)$ is transitive on its domain, so is $A^*(N_k, 0_k)$.

In order to determine the action of $\sigma^*_{1,i}$ and $\sigma^*_{2,i}$ on $p^*_{h_k}$, we use Theorem 6.1. For all $i = 1, \ldots, k$, $\sigma_{1,i} = \delta_{d_i, e_i, 0_k}$. In this case, the function h' defined by (2) is

$$h'(u) = h_k(u \oplus d_i) \oplus u_i \ .$$

By Lemma 8.1, we have $h' = h_k$, which implies (5). For all $i = 1, \ldots, k$, $\sigma_{2,i} = \delta_{0_k, e_i, e_i}$. In this case, the function h' defined by (2) is $h'(u) = h_k(u) \oplus 1$, which implies (6).

Since all elements of $A^*(N_k, 0_k)$ either preserve p^*_h or change its sign, we have that the range of values of $p^*_h(\langle x^*, y^*\rangle)$ is $\{p^*_h(\langle 1_k, 1_k\rangle), -p^*_h(\langle 1_k, 1_k\rangle)\}$. By Lemma 7.1, we have

$$p^*_{h_k}(\langle 1_k, 1_k\rangle) = \frac{1}{2^{k/2}} \sum_u (-1)^{h_k(u)} = \frac{1}{2^{k/2}}\, 2^{k/2} = 1 \ ,$$

which is (4).

Consequently, $p^*_{h_k}(\langle x^*, y^*\rangle)$ is the Fourier polynomial for f_k. □

9 Generalization for an arbitrary quadratic bent function

The function h_k used in Theorem 8.2 is one of the symmetric bent functions, which are known to be quadratic over Z_2, see [2]. In this section, we demonstrate that the polynomial (1) defines a transitive function of $2k$ variables for every quadratic bent function of k variables $h : \{0,1\}^k \to \{0,1\}$, where k is even. All quadratic bent functions of k variables may be obtained from any of them by applying an affine transform to $u_1, \ldots, u_k$, see [3]. As a consequence, every quadratic bent function $h(u)$ may be obtained in the form

$$h(u) = h_k(Lu) \oplus \bigoplus_i a_i u_i \oplus b$$

for an appropriate non-singular k by k matrix L over Z_2 and some constants $a_1, \ldots, a_k, b \in Z_2$. The main part of the proof is to show that (1) is a transitive function for every function $h(u) = h_k(Lu)$, where L is an appropriate matrix as specified above. Then, a simpler argument is needed to see that (1) is a transitive function also if h contains nonzero linear and constant terms.

Let L be a fixed non-singular matrix over Z_2 and let

$$h(u) = h_k(Lu) \ . \tag{7}$$

Moreover, let

$$D = (L^t N_k L)^{-1} \ . \tag{8}$$

Note that D is symmetric. Since for an even k, we have $N_k N_k = I_k$, D is non-singular. For every $i = 1, \ldots, k$, let d_i be the i-th row of D considered as a column vector. Let $c \in \{0,1\}^k$ be defined by

$$c_i = h'_k(Ld_i) \ . \tag{9}$$

Lemma 9.1 *For every $i = 1, \ldots, k$ and $u \in \{0,1\}^k$, we have*

$$h(u \oplus d_i) = h(u) \oplus u_i \oplus c_i \ .$$

Proof. By Lemma 7.2, we have

$$h(u \oplus d_i) = h_k(Lu \oplus Ld_i) = h_k(Lu) \oplus (Ld_i)^t N_k Lu \oplus h'_k(Ld_i)$$

$$= h(u) \oplus (L^t N_k L d_i)^t u \oplus c_i \ .$$

Since

$$(L^t N_k L d_i)^t u = (D^{-1} d_i)^t u = e_i^t u = u_i \ ,$$

where e_i is the i-th standard basis vector, the lemma follows. □

Theorem 9.2 *For every L, the polynomial (1) with h given by (7) is the Fourier polynomial of a transitive Boolean function.*

Proof. Let $\sigma_{1,i}, \sigma_{2,i}$ be the isometries used to define the group $A(D,c)$ from Definition 4.1 with D given by (8) and c given by (9). Let $\sigma^*_{1,i}, \sigma^*_{2,i}$ be the isometries of $\{1,-1\}^{2k}$ induced by $\sigma_{1,i}, \sigma_{2,i}$. Similarly as in the proof of Theorem 8.2, Theorem 6.1 and Lemma 9.1 imply for every $i = 1, \ldots, k$

$$p^*_h(\sigma_{1,i}(\langle x^*, y^*\rangle)) = p^*_h(\langle x^*, y^*\rangle) \tag{10}$$

and

$$p^*_h(\sigma_{2,i}(\langle x^*, y^*\rangle)) = -p^*_h(\langle x^*, y^*\rangle) \ . \tag{11}$$

Let $A^*_2(D,c)$ be the group induced on $\{1,-1\}^{2k}$ by $A(D,c)$, where D is given by (8) and c is given by (9). Since $A(D,c)$ is transitive on its domain, so is $A^*_2(D,c)$. Since all elements of $A^*_2(D,c)$ either preserve p^*_h or change its sign, we have that the range of values of $p^*_h(\langle x^*, y^*\rangle)$ is $\{p^*_h(\langle 1_k, 1_k\rangle), -p^*_h(\langle 1_k, 1_k\rangle)\}$. Since $h(u) = h_k(Lu)$ is a bent function of k variables with the same number of values 0 and 1 as the function h_k, the same argument as in the proof Theorem 8.2 yields

$$p^*_h(\langle 1_k, 1_k\rangle) = 1 \ .$$

Consequently, $p^*_h(\langle x^*, y^*\rangle)$ is a Fourier polynomial for a Boolean function. Let us denote this function $p_h(\langle x, y\rangle)$. We have $p_h(\langle 0_k, 0_k\rangle) = 0$. By (10), this function is preserved by the automorphisms $\sigma_{1,i}$ and by (11), it is reversed by the automorphisms $\sigma_{2,i}$. By Theorem 4.3, the group $A(D,c)$ generated by these isometries is transitive. □

10 A transitive function derived from a cubic bent function

Let $k = 6$ and let $h_{6,cub} : \{0,1\}^k \to \{0,1\}$ be the function defined by the polynomial over Z_2

$$h_{6,cub}(u) = (u_1 \oplus u_4)(u_2 \oplus u_5)(u_3 \oplus u_6)$$
$$\oplus (u_1 \oplus u_4)u_2 \oplus (u_2 \oplus u_5)u_3 \oplus (u_3 \oplus u_6)u_1 \ .$$

The polynomial (1) with $h = h_{6,cub}$ defines a transitive function of $2k = 12$ variables, which will be called $f_{6,cub}$. In order to describe a transitive group of its automorphisms, the isometries $\delta_{d,r,s}$ described in Section 4 are not sufficient.

Let p be a permutation of $1, \ldots, k$. Then, let δ_p be the mapping $\{0,1\}^{2k} \to \{0,1\}^{2k}$ such that $\langle x', y'\rangle = \delta_p(\langle x, y\rangle)$ satisfies $x'_j = x_{p(j)}$ and $y'_j = y_{p(j)}$ for every $j = 1, \ldots, k$.

Let $\alpha_1(\langle x, y\rangle) = \delta_p(\langle x, y\rangle)$, where $p = (2,3,1,5,6,4)$, and let $\alpha_2(\langle x, y\rangle) = \delta_{d,r,s}(\delta_p(\langle x, y\rangle))$ where $p = (1,2,6,4,5,3)$, $d = e_4$, $r = e_2$, and $s = 0_k$. Using the matrix notation, these isometries are

$$\alpha_1(\langle x, y\rangle) = \begin{pmatrix} x_2, & x_3, & x_1, & x_5, & x_6, & x_4 \\ y_2, & y_3, & y_1, & y_5, & y_6, & y_4 \end{pmatrix}$$

and

$$\alpha_2(\langle x, y\rangle) = \begin{pmatrix} x_1, & x_2 \oplus 1, & x_6, & y_4, & x_5, & x_3 \\ y_1, & y_2, & y_6, & x_4, & y_5, & y_3 \end{pmatrix} \ .$$

These isometries were found by a computer search, as well as the function $h_{6,cub}$ itself. It may be verified that the group generated by α_1 and α_2 has two orbits. Together with the generator $\sigma_{2,1}$ for $k = 6$, we get a group, which is transitive on the vertices of the cube $\{0,1\}^{12}$. Moreover, one can verify that α_1 and α_2 preserve the function $f_{6,cub}$ and $\sigma_{2,1}$ reverses this function. Hence, the group generated by α_1, α_2, and $\sigma_{2,1}$ is a transitive group of automorphisms of the partition defined by $f_{6,cub}$. Hence, we have the following.

Theorem 10.1 *The function $f_{6,cub}$ is a transitive function.*

11 An upper bound on the number of transitive functions

In order to have a transitive function uniquely determined by the partition, which is induced by the function, we consider only functions, which satisfy $f(\langle 0_k, 0_k \rangle) = 0$. Using this, every transitive function f is uniquely determined by the group of the automorphisms of the cube, which preserve f. Hence, the number of groups of isometries of the Boolean cube is an upper bound on the number of transitive functions.

Lemma 11.1 *Every finite group G is generated by at most $\log_2 |G|$ of its elements.*

Proof. Let G_0 be the trivial subgroup of G containing only the identity element. If $G_i \neq G$, let G_{i+1} be obtained as a subgroup of G containing G_i and an element $g_{i+1} \in G \backslash G_i$. Since $|G_{i+1}| \geq 2\,|G_i|$, this process selects at most $\log_2 |G|$ elements g_i and these elements generate G. □

Theorem 11.2 *The number of transitive functions of n variables is at most*

$$\binom{m}{\lceil \log_2 m \rceil},$$

where $m = 2^n n!$, which is at most $m^{\log_2 m} = 2^{O(n^2 \log^2 n)}$.

Proof. The number of isometries of the Boolean cube $\{0,1\}^n$ is $m = 2^n n!$ and every group of such isometries is generated by at most $\log_2 m$ of its elements. Hence, the number of subgroups is at most the number of subsets of isometries of size $\lceil \log_2 m \rceil$. Due to the considerations above, this is an upper bound also to the number of transitive functions.

For every $m \geq 9$, we have $\lceil \log_2 m \rceil ! \geq m$, which implies

$$\binom{m}{\lceil \log_2 m \rceil} \leq m^{\lceil \log_2 m \rceil - 1} \leq m^{\log_2 m}\ . \tag{12}$$

It is easy to verify that (12) holds also for $m = 8$. The asymptotic estimate follows from $m = 2^{O(n \log_2 n)}$. □

Acknowledgements. The autor was supported by the Grant Agency of the Czech Republic under the grant 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] R. O'Donnell. Some Topics in Analysis of Boolean Functions. TR08-055, ECCC, 2008.

[2] P. Savicky. On the Bent Boolean Functions That are Symmetric. European J. of Combinatorics 15 (1994), pp. 407-410.

[3] F. J. MacWilliams and N. J. Sloane. The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.

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