Technical Report

Department of Computer Science
and Engineering
University of Minnesota
4-192 EECS Building
200 Union Street SE
Minneapolis, MN 55455-0159 USA

TR 00-051

Rivest-Vuillemin Conjecture Is True for Monotone Boolean Functions with Twelve Variables

Sui-xiang Gao, Ding-zhu Du, Xiao-dong Hu, and Xiaohua Jia

October 02, 2000

Rivest-Vuillemin Conjecture Is True for Monotone Boolean Functions with Twelve Variables

Sui-Xiang Gao[*§] Ding-Zhu Du[†‡§] Xiao-Dong Hu[‡§] Xiaohua Jia[§]

Abstract

A Boolean function $f(x_1, x_2, \cdots, x_n)$ is *elusive* if every decision tree computing f must examine all n variables in the worst case. It is a long-standing conjecture that every non-trivial monotone weakly symmetric Boolean function is elusive. In this paper, we prove this conjecture for Boolean functions with twelve variables.

Keywords. Monotone Boolean function, decision tree, elusive.

AMS(MOS) subject classifications. 05C25, 68Q05, 68R05

[*]Department of Mathematics, Graduate School at Beijing, University of Science and Technology of China, Beijing 100039, China.

[†]Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN 55455, USA.
Supported in part by NSF under grant CCR-9530306.
[‡]Institute of Applied Mathematics, Chinese Academy of Sciences, Beijing 100080, China.
Supported in part by 973 Information Technology and High-Performance Software Program of China.
[§]Department of Computer Science, City University of Hong Kong, Kowloon Tong, Hong Kong.

1 Introduction

An *assignment* for a Boolean function of n variables can be considered as a binary string of length n, i.e., a string in $\{0,1\}^n$. An assignment $\mathbf{x}$ of Boolean function $f(\mathbf{x})$ is called a *truth-assignment* if $f(\mathbf{x}) = 1$, and *false-assignment* if $f(\mathbf{x}) = 0$. We denote by *truth*($\mathbf{x}$) and *false*($\mathbf{x}$) respectively sets of variables with value 1 and with value 0 in the assignment $\mathbf{x}$.

For two assignments of a Boolean function $f(x_1, x_2, \cdots, x_n)$, say, $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n)$, if $x_i \le y_i$ for all i, then we write $\mathbf{x} \le \mathbf{y}$. A Boolean function $f(\mathbf{x})$ is *increasing* if $f(\mathbf{x}) = 1$ and $\mathbf{x} \le \mathbf{y}$ imply $f(\mathbf{y}) = 1$, and *decreasing* if $f(\mathbf{y}) = 1$ and $\mathbf{x} \le \mathbf{y}$ imply $f(\mathbf{x}) = 1$, *monotone* if it is either increasing or decreasing. $f(\mathbf{x})$ is *nontrivial* if it is not a constant function.

A *decision tree* of a Boolean function f is a rooted binary tree, whose nonleaf vertices are labeled by its variables, and leaves are labeled by 0 and 1. Edges of this binary tree are also labeled by 0 and 1 such that edges from an non-leaf vertex to its two children are labeled by 0 and 1 respectively, and every variable appears at most once in a path from the root to a leaf. Given an assignment to variables of a Boolean function $f(x_1, x_2, \cdots, x_n)$, we can compute the function value of f by its decision tree as follows: starting from the root, we look at its label. If its label is x_i, then we make a decision according to the value of x_i, to decide where we go. If $x_i = 0$, then we go to the next vertex along the edge with label 0; if $x_i = 1$, then we go to the next vertex along the edge with label 1. Once a leaf is reached, the function value for the given assignment is obtained from the label of the leaf.

Each decision tree of f gives an algorithm to compute the function value. The computation time depends on the length of root-leaf path that is the number of variables on the path. The *depth* of a decision tree is the maximum length of all paths from the root to leaves.

A Boolean function generally has many decision trees. We denote by $D(f)$ the minimum depth of all decision trees computing Boolean function f. $D(f)$ is called the *decision tree complexity* of f. Clearly, $D(f) \le n$ if f has n variables. $f(x_1, \cdots, x_n)$ is said to be *elusive* if $D(f) = n$.

The decision tree complexity is closely related to several other combinatorial and complexity issues, such as the certificate complexity (see [1]), the block sensitivity ([2]), the packing of graphs (see [3]), and the time-complexity of a CREW PRAM (see [2]).

A group G of permutations on $\{1, 2, \cdots, n\}$ is called *transitive* if for any $i, j \in \{1, 2, \cdots, n\}$, there exists $\sigma \in G$ such that $\sigma(i) = j$. Let $f(x_1, x_2, \cdots, x_n)$ be a Boolean function and G be a group of permutations on $\{1, 2, \cdots, n\}$. $f(x_1, x_2, \cdots, x_n)$ is said to be *invariant* under group G if for any $\sigma \in G$,

$$f(x_1, x_2, \cdots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}).$$

A Boolean function $f(x_1, x_2, \cdots, x_n)$ is said to be *weakly symmetric* if there exists a transitive permutation group G on $\{1, 2, \cdots, n\}$ such that $f(x_1, x_2, \cdots, x_n)$ is invariant under G. There is an interesting conjecture on monotone weakly symmetric Boolean functions.

Rivest-Vuillemin Conjecture (1975): Any nontrivial monotone weakly symmetric Boolean function $f(x_1, x_2, \cdots, x_n)$ is elusive.

Rivest and Vuillemin [11] proved that this conjecture is true when n is a prime power.[1] Gao *et al* [6, 7] showed that Rivest-Vuillemin conjecture is true for $n = 6, 10$. In this paper, we show that Rivest-Vuillemin Conjecture is true for $n = 12$. The proof involves some new techniques developed based on some facts on permutation groups.

2 Preliminary

An *abstract complex* Δ on a finite set X is a family of subsets of X, such that if A is a member of Δ, so is every subset of A. Each member of Δ is called a *face* of Δ. A *maximal face* of abstract complex Δ is a face that is not contained by another face. A *free face* is a non-maximal face that is contained by only one maximal face. An *elementary collapse* is an operation that deletes a free face together with all faces containing it. An abstract complex Δ is *collapsible* if it can be collapsed to the empty abstract complex through a sequence of elementary collapses.

The *complex* of a monotone Boolean function $f(x_1, x_2, \cdots, x_n)$ is an abstract complex defined by

$$\Delta_f = \begin{cases} \{false(\mathbf{x}) \mid f(\mathbf{x}) = 1\}, & \text{if } f \text{ is increasing} \\ \{truth(\mathbf{x}) \mid f(\mathbf{x}) = 1\}, & \text{if } f \text{ is decreasing.} \end{cases}$$

Each vertex of Δ_f is a variable of f. The following can be found in [9].

Lemma 2.1 *Let f be a nontrivial monotone Boolean function. If f is not elusive, then Δ_f is collapsible.*

For an abelian group G, an abstract complex Δ is G-acyclic if the homology groups of Δ under G are

$$H_0(\Delta, G) = G, \quad i = 0,$$
$$H_i(\Delta, G) = 0, \quad i > 0.$$

The following can be found in [9].

Lemma 2.2 *If Δ is collapsible, then Δ is Z_p-acyclic.*

The following follows immediately from Lemma 2.1 and Lemma 2.2.

Corollary 2.1 *Let f be a nontrivial monotone Boolean function. If f is not elusive, then Δ_f is Z_p-acyclic.*

[1] Actually, they proved that if $f(0, \cdots, 0) \neq f(1, \cdots, 1)$ and n is a prime power, then weakly symmetric Boolean function $f(x_1, \cdots, x_n)$ is elusive. They also made a conjecture for general n with condition $f(0, \cdots, 0) \neq f(1, \cdots, 1)$ instead of monotoneness. Illies in 1978 found a counterexample for Rivest-Vuillemin's original conjecture (see [5]). Current Rivest-Vuillemin conjecture is a modification suggested by this counterexample.

The *Euler characteristic* of an abstract complex Δ is defined by

$$\chi(\Delta) = \sum_{A\in\Delta, A\neq\emptyset} (-1)^{|A|-1} = \sum_{A\in\Delta} (-1)^{|A|-1} + 1,$$

in particular, $\chi(\{\emptyset\}) = 0$ and define $\chi(\emptyset) = 1$.

A permutation σ on the vertex set of an abstract complex Δ is called an *automorphism* of Δ, if for each face $A \in \Delta$, $\sigma(A) = \{\sigma(a) \mid a \in A\}$ is still a face of Δ. Every invariant permutation of Boolean function f induces an automorphism of Δ_f.

Let G be a group of automorphisms on Δ, an *orbit* of G is a minimal subset of vertices of Δ which is closed under actions of G. Clearly, G has only one orbit on Δ if and only if G is transitive on vertices of Δ.

Define

$$\Delta^G = \{\{H_1, \cdots, H_k\} \mid H_1, \cdots, H_k \text{ are orbits of } G, \text{ and } H_1 \cup \cdots \cup H_k \in \Delta\} \cup \{\emptyset\}.$$

Δ^G is an abstract complex (see [5]).

For p and q primes, denote by $\mathcal{Y}_p^q$ the class of finite groups G with normal subgroups $P \triangleleft H \triangleleft G$, such that P is of p-power order, the quotient group G/H is of q-power order, and the quotient group H/P is cyclic; denote by $\mathcal{Y}_p$ the class of finite groups G with normal p-subgroups $P \triangleleft G$ such that the quotient group G/P is cyclic. The following lemma comes from [10].

Lemma 2.3 *Let G be a group of automorphisms on a collapsible abstract complex Δ.*

(1) If G is a cyclic group or $G \in \mathcal{Y}_p$ for some prime p, then $\chi(\Delta^G) = 1$.

(2) If $G \in \mathcal{Y}_p^q$ for some primes p and q, then $\chi(\Delta^G) \equiv 1 \pmod q$.

The following lemma follows from previous ones.

Lemma 2.4 *If a nontrivial monotone Boolean function f has a transitive cyclic invariant group or has a transitive invariant group in $\mathcal{Y}_p$ or in $\mathcal{Y}_p^q$, then f is elusive.*

Proof. Let G be a group that meets the conditions of the current lemma, then G has only one orbit in Δ_f since it is transitive. This orbit cannot be a face of Δ_f. In fact, if it is a face, then the monotonicity of f forces that f must be a constant, contradicting the hypothesis that f is nontrivial. Thus, $\Delta_f^G = \{\emptyset\}$ and $\chi(\Delta_f^G) = 0$. By Lemma 2.3, Δ_f is not collapsible. By Lemma 2.1, f is elusive. $\square$

This lemma will be used extensively together with many facts on group theory in the next section, such as facts about block systems. For a transitive permutation group G on a set Ω, a partition $(\Omega_1, \cdots, \Omega_k)$ of Ω is called a *block system* of G if each Ω_i is transformed to some Ω_j under the action of any element of G. G is *primitive* if G has no nontrivial block system; otherwise, G is *imprimitive*.

For simplicity, all involved terminologies and concepts on group theory are employed from the same reference [4] while results come from different sources.

3 Main Result

In this section, we prove the following main result.

Main Theorem. *Every nontrivial monotone weakly symmetric Boolean function $f(x_1, x_2, \cdots, x_n)$ is elusive when $n = 12$.*

To prove it, we first show some lemmas.

Lemma 3.1 [13] *Any transitive permutation group of twelve degree contains one of following minimal transitive groups as its subgroup:*

$$
\begin{aligned}
T_1 &= \langle (1,3,5,7,9,11,2,4,6,8,10,12) \rangle, \\
T_2 &= \langle (1,6,9,2,5,10)(3,8,11,4,7,12), (1,7)(2,8)(3,9)(4,10)(5,11)(6,12) \rangle, \\
T_3 &= \langle (1,10,5,2,9,6)(3,12,7,4,11,8), (1,3)(2,4)(5,11)(6,12)(7,9)(8,10) \rangle, \\
T_4 &= \langle (1,6,9,2,5,10)(3,8,11,4,7,12), (1,3,2,4)(5,11,6,12)(7,10,8,9) \rangle, \\
T_5 &= \langle (1,9,5)(2,10,6)(3,11,7)(4,12,8), (1,12,7)(2,11,8)(3,10,5)(4,9,6) \rangle, \\
T_6 &= \langle (1,8,11)(2,7,12)(3,5,10)(4,6,9), (1,9,7,4,11,5)(2,10,8,3,12,6) \rangle, \\
T_7 &= \langle (1,4)(2,3)(5,12)(6,11)(7,10)(8,9), (1,11,7)(2,12,8)(3,10,6)(4,9,5) \rangle, \\
T_8 &= \langle (1,8,4,10)(2,7,3,9)(5,12,6,11), (1,3,6)(2,4,5)(7,12,10)(8,11,9) \rangle, \\
T_9 &= \langle (1,2)(3,4)(5,7,6,8)(9,11,10,12), (1,11,6)(2,12,5)(3,10,8)(4,9,7) \rangle, \\
T_{10} &= \langle (1,7)(2,8)(3,9,5,11)(4,10,6,12), (1,6,3,2,5,4)(7,8)(9,10)(11,12) \rangle, \\
T_{11} &= \langle (1,9)(2,10)(3,11)(4,12)(5,7)(6,8), (1,6,3,2,5,4)(7,10)(8,9)(11,12) \rangle, \\
T_{12} &= \langle (1,11,3,10)(2,12)(4,7)(5,8,6,9), (1,4,10,7,2,6,11,9)(3,5,12,8) \rangle, \\
T_{13} &= \langle (1,5,3,4)(2,6)(7,12,9,11)(8,10), (1,8)(2,9,3,7)(4,11)(5,10,6,12) \rangle, \\
T_{14} &= \langle (1,5,12,2,6,11)(3,8,10,4,7,9), (1,7,11,2,8,12)(3,6,10,4,5,9) \rangle, \\
T_{15} &= \langle (1,9,6,12,2,10,5,11)(3,8,4,7), (1,2)(5,6)(7,12,10)(8,11,9) \rangle, \\
T_{16} &= \langle (1,12,5,3,11,6,2,10,7)(4,9,8), (1,3,2)(5,8,6)(9,11,12) \rangle, \\
T_{17} &= \langle (1,7)(2,9,3,8)(4,11,6,10,5,12), (1,4,2,6,3,5)(7,12,8,11)(9,10) \rangle,
\end{aligned}
$$

where $\langle \alpha, \beta \rangle$ denotes the group generated by permutations α and β. All of these groups are imprimitive groups and their orders are as follows:

group :	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}	T_{16}	T_{17}
order :	12	12	12	12	12	24	24	36	48	72	72	72	72	96	576	576	2592

Lemma 3.2 $T_2, T_3 \in \mathcal{Y}_2$.

Proof. For T_2, consider

$$
\begin{aligned}
H &= \langle (1,7)(2,8)(3,9)(4,10)(5,11)(6,12) \rangle \\
&= \{(1), (1,7)(2,8)(3,9)(4,10)(5,11)(6,12)\}.
\end{aligned}
$$

Note that H is a normal subgroup of T_2 and the quotient group

$$T_2/H \cong \langle(1,6,9,2,5,10)(3,8,11,4,7,12)\rangle.$$

Thus, $T_2 \in \mathcal{Y}_2$.

$T_3 \in \mathcal{Y}_2$ can be shown similarly. $\square$

Lemma 3.3 $T_4 \in \mathcal{Y}_3$.

Proof. Denote

$$\begin{aligned} a &= (1,6,9,2,5,10)(3,8,11,4,7,12) \\ b &= (1,3,2,4)(5,11,6,12)(7,10,8,9). \end{aligned}$$

Then

$$T_4 = \langle a, b\rangle = \{(1), a, a^2, a^3, a^4, a^5, b, b^3, ab, ba, a^{-1}b^{-1}, b^{-1}a^{-1}\}.$$

Consider

$$H = \langle a^2\rangle = \{(1), a^2, a^{-2}\}.$$

It is easy to verify that

(1) H is a normal subgroup of T_4,

(2) $|H| = 3$, and

(3) $T_4/H \cong \langle b\rangle$.

Therefore, $T_4 \in \mathcal{Y}_3$. $\square$

Lemma 3.4 $T_5 \in \mathcal{Y}_2$.

Proof. Denote

$$\begin{aligned} a &= (1,9,5)(2,10,6)(3,11,7)(4,12,8) \\ b &= (1,12,7)(2,11,8)(3,10,5)(4,9,6). \end{aligned}$$

Then

$$T_5 = \langle a, b\rangle = \{(1), a, b, a^2, b^2, ab, ba, a^2b, ab^2, a^2b^2, b^2a^2, a^2bab^2\}.$$

Consider

$$H = \{(1), a^2bab^2, a^2b, ab^2\}.$$

Note that $a^{-1} = a^2$, $b^{-1} = b$, $a^2b = b^2a$ and $ab^2 = ba^2$. It is easy to verify the following:

(1) H is a normal subgroup of T_5.

(2) $|H| = 4$.

(3) $T_5/H \cong \langle a\rangle$.

Thus, $T_5 \in \mathcal{Y}_2$. $\square$

Lemma 3.5 $T_6 \in \mathcal{Y}_2$.

Proof. Denote

$$\begin{aligned} a &= (1,8,11)(2,7,12)(3,5,10)(4,6,9) \\ b &= (1,9,7,4,11,5)(2,10,8,3,12,6). \end{aligned}$$

Then

$$\begin{aligned} T_6 &= \langle a, b\rangle \\ &= \{(1), a, a^2, b, b^2, b^3, b^4, b^5, ab, ab^2, ab^3, ab^4, ab^5, a^2b, a^2b^2, a^2b^3, a^2b^4, \\ &\quad ba, ba^2, b^2a^2, b^4a, b^4a^2, b^5a, ab^2a, ab^5a\} \end{aligned}$$

and the following equalities can be derived by simple computations:

$$a^{-1} = a, b^{-1} = b^5, ab^3 = b^3a, ab^4 = b^2a^2, b^4a = a^2b^2, a^2b^3 = b^3a^2,$$

$$a^2b^5 = ba, b^5a^2 = ab, (b^2a^2)(a^2b^2) = (a^2b^2)(b^2a^2) = (ab)(ba).$$

Consider

$$\begin{aligned} H &= \{(1), (1,2)(3,4)(5,6)(7,8), (1,2)(3,4)(9,10)(11,12), (5,6)(7,8)(9,10)(11,12)\} \\ &= \{(1), a^2b^2, b^2a^2, (a^2b^2)(b^2a^2)\} \end{aligned}$$

The following can be verified easily by using above equalities:

(1) H is a normal subgroup of T_6;

(2) $|H| = 4$;

(3) $T_6/H \cong \langle b\rangle$.

Therefore, $T_6 \in \mathcal{Y}_2$. □

Lemma 3.6 $T_7 \in \mathcal{Y}_2^2$

Proof. Denote

$$\begin{aligned} a &= (1,4)(2,3)(5,12)(6,11)(7,10)(8,9) \\ b &= (1,11,7)(2,12,8)(3,10,6)(4,9,5). \end{aligned}$$

Then

$$\begin{aligned} T_7 &= \langle a, b\rangle \\ &= \{(1), a, b, b^2, ab, ab^2, ba, b^2a, (ab)^2, (ba)^2, (ab)(ba), aba, bab, b^2ab, bab^2, b^2ab^2, \\ &\quad b^2aba, abab^2, ab^2ab, bab^2a, ab^2aba, abab^2a, (ab)^2(ba)^2, a(ab)^2(ba)^2\} \end{aligned}$$

and the following equalities can be derived by simple computations:

$$\begin{aligned} &a^{-1} = a, b^{-1} = b^2, (ab)^{-1} = b^2a, (ba)^{-1} = ab^2, (ba)(ab) = b^2, \\ &ab = (b^2a)^3, (ab)^2 = (b^2a)^2, (ab)^3 = b^2a, ba = (ab^2)^3, (ba)^2 = (ab^2)^2, \\ &(ba)^3 = ab^2, babab = ab^2a, (bab)^2 = (ab)^2(ba)^2 = a(bab)^2a. \end{aligned}$$

Let

$$\begin{aligned} H &= \langle b, aba\rangle \\ &= \{(1), b, b^2, aba, (aba)^2, (aba)b, b(aba), b^2(aba), (aba)b^2, b(aba)^2, (aba)^2b, (aba)b^2(aba)\} \\ &= \{(1), (1,2)(3,4)(5,6)(7,8), (1,2)(3,4)(9,10)(11,12), (5,6)(7,8)(9,10)(11,12), \\ &\quad (1,11,7)(2,12,8)(3,10,6)(4,9,5), (1,7,11)(2,8,12)(3,6,10)(4,5,9), \\ &\quad (1,11,8)(2,12,7)(3,10,5)(4,9,6), (1,8,11)(2,7,12)(3,5,10)(4,6,9), \\ &\quad (1,12,7)(2,11,8)(3,9,6)(4,10,5), (1,7,12)(2,8,12)(3,6,9)(4,5,10), \\ &\quad (1,12,8)(2,11,7)(3,9,5)(4,10,6), (1,8,12)(2,7,11)(3,5,9)(4,6,10)\} \end{aligned}$$

and

$$\begin{aligned} P &= \{(1), abab, baba, (abab)(baba)\} \\ &= \{(1), (1,2)(3,4)(5,6)(7,8), (1,2)(3,4)(9,10)(11,12), (5,6)(7,8)(9,10)(11,12)\}. \end{aligned}$$

Using above equalities, we can verify the following :

(1) H is a normal subgroup of T_7 and P is a normal subgroup of H;

(2) $|P| = 4$;

(3) $|T_7/H| = 2$;

(4) $H/P \cong \langle b^2\rangle$.

Thus, $T_7 \in \mathcal{Y}_2^2$. □

Lemma 3.7 *$T_8 \in \mathcal{Y}_3$.*

Proof. Denote

$$\begin{aligned} a &= (1,8,4,10)(2,7,3,9)(5,12,6,11) \\ b &= (1,3,6)(2,4,5)(7,12,10)(8,11,9). \end{aligned}$$

Then

$$\begin{aligned} T_8 &= \langle a, b\rangle \\ &= \{(1), a, a^2, a^3, b, b^2, ab, a^2b, a^3b, ab^2, a^2b^2, a^3b^2, ba, ba^3, b^2a, b^2a^3, \\ &\quad bab, bab^2, ba^3b, b^2ab^2, b^2ab, b^2a^3b, (ab)^2, (a^3b)^2, (ab^2)^2, (a^3b^2)^2, \\ &\quad (a^2b^2)(ab)^2, (ab)(a^3b), (a^3b)(ab), a^3b^2ab^2, a^3ba, aba^3, ab^2a, aba, ba^3b^2, a^2bab^2\}, \end{aligned}$$

and the following equalities can be derived by simple computations:

$$a^{-1} = a^3, b^{-1} = b^2, a^2 = ba^2b = b^2a^2b^2, b = a^2b^2a^2, b^2 = a^2ba^2, a^2b^2 = ba^2,$$

$$b^2a^2 = a^2b, (ab)^{-1} = b^2a^3, (ba)^{-1} = a^3b^2, (ab^2)^{-1} = ba^3, (b^2a)^{-1} = a^3b.$$

Let

$$\begin{aligned} H &= \{(1), b, b^2, a^3ba, aba^3, aba^3b^3, a^3bab, aba^3b, a^3bab^2\} \\ &= \{(1), (1,3,6)(2,4,5)(7,12,10)(8,11,9), (1,6,3)(2,5,4)(7,10,12)(8,9,11), \\ &\quad (1,3,6)(2,4,5)(7,10,12)(8,9,11), (1,6,3)(2,5,4)(7,12,10)(8,11,9), \\ &\quad (1,3,6)(2,4,5), (1,6,3)(2,5,4), (7,10,12)(8,9,11), (7,12,10)(8,11,9)\}. \end{aligned}$$

Then one can verify the following with above equalities:

(1) H is a normal subgroup of T_8;

(2) $|H| = 9$;

(3) $T_8/H \cong \langle a \rangle$.

Thus, $T_8 \in \mathcal{Y}_3$. $\square$

The following two lemmas can be found in [14].

Lemma 3.8 *Let G be an imprimitive group. Suppose Ω_1, Ω_2, $\cdots$, Ω_s form a block system of G. Each element g of G induces a permutation on this block system:*

$$\theta_g = \begin{pmatrix} \Omega_1 & \Omega_2 & \cdots & \Omega_s \\ \Omega_1^g & \Omega_2^g & \cdots & \Omega_s^g \end{pmatrix}.$$

Denote $Q = \{\theta_g \mid g \in G\}$. Then Q is a group of permutations of degree s.

Lemma 3.9 *Let G be an imprimitive group. Suppose $\Omega_1, \Omega_2, \cdots, \Omega_s$ form a block system of G. Assume that Q is defined in Lemma 3.8 and $H = \{g \in G \mid \Omega_i^g = \Omega_i, i = 1, 2, \cdots, s\}$. Then $H \lhd G$ and $G/H \cong Q$.*

Lemma 3.10 $T_9 \in \mathcal{Y}_2$.

Proof. Let

$$\begin{aligned} a &= (1,2)(3,4)(5,7,6,8)(9,11,10,12) \\ b &= (1,11,6)(2,12,5)(3,10,8)(4,9,7). \end{aligned}$$

Then $T_9 = \langle a, b \rangle$. It can be easily verified that

$$\Omega_1 = \{1,2,3,4\}, \Omega_2 = \{5,6,7,8\}, \Omega_3 = \{9,10,11,12\}$$

form a block system of T_9. The generators a and b of T_9 induce respectively a permutation on $\{\Omega_1, \Omega_2, \Omega_3\}$:

$$\theta_a : \Omega_1 \to \Omega_1, \Omega_2 \to \Omega_2, \Omega_3 \to \Omega_3.$$

$$\theta_b : \Omega_1 \to \Omega_3, \Omega_2 \to \Omega_1, \Omega_3 \to \Omega_2.$$

Obviously, $\theta_a = (1)$ and $\theta_b = (1,3,2)$. Since every permutation g in T_9 can be written as a product of powers of a and b, the induced permutation θ_g on $\{\Omega_1, \Omega_2, \Omega_3\}$ can be written as a product of powers of θ_a and θ_b. Therefore, $Q = \{\theta_g | g \in T_9\} = \langle \theta_a, \theta_b \rangle = \langle \theta_b \rangle$.

By Lemma 3.1, T_9 is an imprimitive group. By Lemma 3.9, there exists a subgroup H such that $H \lhd T_9$ and $T_9/H \cong Q$. $|H| = |T_9|/|Q| = 2^4$ since $|T_9| = 48$ and $|Q| = 3$. Moreover, Q is a cyclic group. Thus, $T_9 \in \mathcal{Y}_2$. $\square$

The following two lemmas can be found in [12].

Lemma 3.11 *Any group of prime order is cyclic.*

Lemma 3.12 *Any subgroup with index 2 is a normal subgroup.*

Lemma 3.13 $T_{10}, T_{11}, T_{12}, T_{13} \in \mathcal{Y}_3^2$.

Let

$$\begin{aligned}
a_{10} &= (1,7)(2,8)(3,9,5,11)(4,10,6,12)\\
b_{10} &= (1,6,3,2,5,4)(7,8)(9,10)(11,12)\\
a_{11} &= (1,9)(2,10)(3,11)(4,12)(5,7)(6,8)\\
b_{11} &= (1,6,3,2,5,4)(7,10)(8,9)(11,12)\\
a_{12} &= (1,11,3,10)(2,12)(4,7)(5,8,6,9)\\
b_{12} &= (1,4,10,7,2,6,11,9)(3,5,12,8)\\
a_{13} &= (1,5,3,4)(2,6)(7,12,9,11)(8,10)\\
b_{13} &= (1,8)(2,9,3,7)(4,11)(5,10,6,12).
\end{aligned}$$

Then $T_{10} = \langle a_{10}, b_{10}\rangle$, $T_{11} = \langle a_{11}, b_{11}\rangle$, $T_{12} = \langle a_{12}, b_{12}\rangle$, and $T_{13} = \langle a_{13}, b_{13}\rangle$. It is easy to verify that

$$\Omega_1 = \{1,3,5\}, \Omega_2 = \{2,4,6\}, \Omega_3 = \{7,9,11\}, \Omega_4 = \{8,10,12\}$$

form a block system of T_{10} and T_{11}, and

$$\Omega_1' = \{1,2,3\}, \Omega_2' = \{4,5,6\}, \Omega_3' = \{7,8,9\}, \Omega_4' = \{10,11,12\}$$

form a block system of T_{12} and T_{13}.

The generators a_{10} and b_{10} of T_{10} induce following permutations on $\{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$ as follows:

$$\theta_{a_{10}} : \Omega_1 \to \Omega_3, \Omega_2 \to \Omega_4, \Omega_3 \to \Omega_1, \Omega_4 \to \Omega_2.$$

$$\theta_{b_{10}} : \Omega_1 \to \Omega_2, \Omega_2 \to \Omega_1, \Omega_3 \to \Omega_4, \Omega_4 \to \Omega_3.$$

That is, $\theta_{a_{10}} = (1,3)(2,4)$ and $\theta_{b_{10}} = (1,2)(3,4)$.

The generators a_{11} and b_{11} of T_{11} induce following permutations on $\{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$:

$$\theta_{a_{11}} : \Omega_1 \to \Omega_3, \Omega_2 \to \Omega_4, \Omega_3 \to \Omega_1, \Omega_4 \to \Omega_2.$$

$$\theta_{b_{11}} : \Omega_1 \to \Omega_2, \Omega_2 \to \Omega_1, \Omega_3 \to \Omega_4, \Omega_4 \to \Omega_3.$$

That is, $\theta_{a_{11}} = (1,3)(2,4)$ and $\theta_{b_{11}} = (1,2)(3,4)$.

The generators a_{12} and b_{12} of T_{12} induce the following permutations on $\{\Omega_1', \Omega_2', \Omega_3', \Omega_4'\}$:

$$\theta_{a_{12}} : \Omega_1' \to \Omega_4', \Omega_2' \to \Omega_3', \Omega_3' \to \Omega_2', \Omega_4' \to \Omega_1'.$$

$$\theta_{b_{12}}: \Omega_1' \to \Omega_2', \Omega_2' \to \Omega_4', \Omega_3' \to \Omega_1', \Omega_4' \to \Omega_3'.$$

That is, $\theta_{a_{12}} = (1,4)(2,3)$ and $\theta_{b_{12}} = (1,2,4,3)$.

The generators a_{13} and b_{13} of T_{13} induce the following permutations on $\{\Omega_1', \Omega_2', \Omega_3', \Omega_4'\}$:

$$\theta_{a_{13}}: \Omega_1' \to \Omega_2', \Omega_2' \to \Omega_1', \Omega_3' \to \Omega_4', \Omega_4' \to \Omega_3'.$$

$$\theta_{b_{13}}: \Omega_1' \to \Omega_3', \Omega_2' \to \Omega_4', \Omega_3' \to \Omega_1', \Omega_4' \to \Omega_2'.$$

That is, $\theta_{a_{13}} = (1,2)(3,4)$ and $\theta_{b_{13}} = (1,3)(2,4)$.

Since every permutation g in T_i can be generated by a_i and b_i, the induced permutation θ_g can be generated by θ_{a_i} and θ_{b_i} ($i = 10, 11, 12, 13$). Thus,

$$Q_{10} = \{\theta_g \mid g \in T_{10}\} = \langle \theta_{a_{10}}, \theta_{b_{10}} \rangle = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

$$Q_{11} = \{\theta_g \mid g \in T_{11}\} = \langle \theta_{a_{11}}, \theta_{b_{11}} \rangle = \{(1), (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\},$$

$$Q_{12} = \{\theta_g \mid g \in T_{12}\} = \langle \theta_{a_{12}}, \theta_{b_{12}} \rangle = \{(1), (1,4)(2,3), (1,2,4,3), (1,3,2,4)\},$$

$$Q_{13} = \{\theta_g \mid g \in T_{13}\} = \langle \theta_{a_{13}}, \theta_{b_{13}} \rangle = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

All Q_i for $i = 10, 11, 12, 13$ are groups of order 4.

For $i = 10, 11, 12, 13$, T_i is imprimitive by Lemma 3.1. By Lemma 3.9, there exists an normal subgroup $H_i \lhd T_i$ such that $T_i/H_i \cong Q_i$. Moreover, the facts that $|T_i| = 72$ and $|Q_i| = 4$ imply that $|H_i| = 18$. Since $18 = 2 \cdot 3^2$, H_i has a Sylow subgroup K_i of order 3^2. By Lemma 3.12, K_i is a normal subgroup of H_i. Since $|H_i/K_i| = 2$, H_i/K_i is a cyclic group by Lemma 3.11. Therefore, $T_i \in \mathcal{Y}_3^2$ for $i = 10, 11, 12, 13$. □

Lemma 3.14 $T_{14} \in \mathcal{Y}_2$.

Proof. Let

$$\begin{aligned} a &= (1,5,12,2,6,11)(3,8,10,4,7,9) \\ b &= (1,7,11,2,8,12)(3,6,10,4,5,9) \end{aligned}$$

Then $T_{14} = \langle a, b \rangle$. It is easy to verify that

$$\Omega_1 = \{1,2,3,4\}, \Omega_2 = \{5,6,7,8\}, \Omega_3 = \{9,10,11,12\}$$

form a block system of T_{14}. The generators a and b of T_{14} induce following permutations on $\{\Omega_1, \Omega_2, \Omega_3\}$:

$$\theta_a: \Omega_1 \to \Omega_2, \Omega_2 \to \Omega_3, \Omega_3 \to \Omega_1.$$

$$\theta_b: \Omega_1 \to \Omega_2, \Omega_2 \to \Omega_3, \Omega_3 \to \Omega_1.$$

That is, $\theta_a = \theta_b = (1,2,3)$. Since every permutation g of T_{14} can be generated by a and b, the induced permutation θ_g can be generated by θ_a and θ_b.

$$Q = \{\theta_g \mid g \in T_{14}\} = \langle \theta_a, \theta_b \rangle = \langle \theta_a \rangle,$$

which is a cyclic group of order 3.

Since T_{14} is imprimitive, by Lemma 3.9 there exists an normal subgroup $H \triangleleft T_{14}$ such that $T_{14}/H \cong Q$. Moreover, $|T_{14}| = 96$ and $|Q| = 3$ imply that $|H| = 2^5$. Therefore, $T_{14} \in \mathcal{Y}_2$. $\square$

The following two lemmas can be found in [10].

Lemma 3.15 *If a p-group P acts on the finite complex Δ, then $\chi(\Delta^P) \equiv \chi(\Delta) \pmod p$, and if Δ is Z_p-acyclic, so is Δ^P.*

Lemma 3.16 *Suppose Z_n acts on the finite Q-acyclic complex Δ. Then $\chi(\Delta^{Z_n}) = 1$.*

Lemma 3.17 *Let $f(x_1, x_2, \cdots, x_{12})$ be a nontrivial monotone Boolean function, invariant under the action of T_{15}. If f is not elusive, then $\chi(\Delta_f^{T_{15}}) \equiv 1 \pmod 3$.*

Proof. Let

$$\begin{aligned} a &= (1,9,6,12,2,10,5,11)(3,8,4,7) \\ b &= (1,2)(5,6)(7,12,10)(8,11,9). \end{aligned}$$

Then $T_{15} = \langle a, b \rangle$. It is easy to verify that

$$\Omega_1 = \{1,2,\}, \Omega_2 = \{3,4\}, \Omega_3 = \{5,6\}, \Omega_4 = \{7,8\}, \Omega_5 = \{9,10\}, \Omega_6 = \{11,12\}$$

form a block system of T_{15}. The generators a and b of T_{15} induce following permutations on $\{\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5, \Omega_6\}$:

$$\theta_a : \Omega_1 \to \Omega_5, \Omega_2 \to \Omega_4, \Omega_3 \to \Omega_6, \Omega_4 \to \Omega_2, \Omega_5 \to \Omega_3, \Omega_6 \to \Omega_1.$$

$$\theta_b : \Omega_1 \to \Omega_1, \Omega_2 \to \Omega_2, \Omega_3 \to \Omega_3, \Omega_4 \to \Omega_6, \Omega_5 \to \Omega_4, \Omega_6 \to \Omega_5.$$

That is, $\theta_a = (1,5,3,6)(2,4)$ and $\theta_b = (4,6,5)$. Since every permutation g of T_{15} can be generated by a and b, θ_g can be generated by θ_a and θ_b. Hence,

$$\begin{aligned} Q &= \{\theta_g | g \in T_{15}\} \\ &= \langle \theta_a, \theta_b \rangle \\ &= \{(1), (12)(45), (12)(46), (12)(56), (13)(45), (13)(46), (13)(56), (23)(45), (23)(46), (23)(56), \\ &\quad (123), (132), (456), (465), (1,2,3)(456), (123)(465), (132)(456), (132)(465), \\ &\quad (1425)(36), (1524)(36), (1426)(35), (1624)(35), (1435)(26), (1534)(26), (1436)(25), \\ &\quad (1634)(25), (1526)(34), (1625)(34), (1536)(24), (1635)(24), (14)(2536), (14)(2635), \\ &\quad (15)(2436), (15)(2634), (16)(2435), (16)(2534)\}, \end{aligned}$$

which is a group of order 36.

Since T_{15} is imprimitive, by Lemma 3.9 there exists a normal subgroup $H \triangleleft T_{15}$ such that $T_{15}/H \cong Q$. Moreover, $|T_{15}| = 576$ and $|Q| = 36$ imply $|H| = 2^4$. Let

$$\begin{aligned} K &= \langle (123), (456) \rangle \\ &= \{(1), (123), (132), (456), (123)(456), (123)(465), (132)(456), (132)(465)\}. \end{aligned}$$

Then $K \triangleleft Q$, $|K| = 9$, $|Q/K| = 4$, and $Q/K \cong \langle(1536)(24)\rangle$.

If f is not elusive, then Δ is Z_2-acyclic by Corollary 2.1. Since H and Q/K are of 2-power order, Δ^H and thus $(\Delta^H)^{Q/K}$ are Z_2-acyclic by Lemma 3.15. By Lemmas 3.15 and 3.16, we have

$$\chi(\Delta^{T_{15}}) = \chi((\Delta^H)^{T_{15}/H}) = \chi((\Delta^H)^Q) = \chi(((\Delta^H)^{Q/K})^K) \equiv \chi((\Delta^H)^{Q/K}) = 1 \pmod 3.$$

□

The next lemma can be found in [8].

Lemma 3.18 *Suppose that G is a group of order pq^t, where p and q are primes, then G has either a normal subgroup of order q^t or a normal subgroup of order pq^{t-1}.*

Lemma 3.19 *Let $f(x_1, x_2, \cdots, x_{12})$ be a nontrivial monotone Boolean function, invariant under the action of T_{16}. If f is not elusive, then $\chi(\Delta_f^{T_{16}}) \equiv 1 \pmod 3$.*

Proof. Let

$$\begin{aligned} a &= (1, 12, 5, 3, 11, 6, 2, 10, 7)(4, 9, 8) \\ b &= (1, 3, 2)(5, 8, 6)(9, 11, 12). \end{aligned}$$

Then $T_{16} = \langle a, b\rangle$. It is easy to verify that

$$\Omega_1 = \{1, 2, 3, 4\}, \Omega_2 = \{5, 6, 7, 8\}, \Omega_3 = \{9, 10, 11, 12\}$$

form a block system of T_{16}. The generators a and b of T_{16} induce following permutations on $\{\Omega_1, \Omega_2, \Omega_3\}$:

$$\theta_a : \Omega_1 \to \Omega_3, \Omega_2 \to \Omega_1, \Omega_3 \to \Omega_2.$$

$$\theta_b : \Omega_1 \to \Omega_1, \Omega_2 \to \Omega_2, \Omega_3 \to \Omega_3.$$

That is, $\theta_a = (1, 2, 3)$ and $\theta_b = (1)$. Since every permutation g of T_{16} can be generated by a and b, θ_g can be generated by θ_a and θ_b. Thus,

$$Q = \{\theta_g | g \in T_{16}\} = \langle\theta_a, \theta_b\rangle = \langle\theta_a\rangle,$$

which is a cyclic group of order 3.

Since T_{16} is imprimitive, by Lemma 3.9 there exists a normal subgroup $H_1 \triangleleft T_{16}$ such that $T_{16}/H_1 \cong Q$. Moreover, $|T_{16}| = 576$ and $|Q| = 3$ imply that $|H_1| = 192 = 3 \times 2^6$. By Lemma 3.18, there exists a normal subgroup H_2 of H_1 such that either $|H_2| = 2^6$ and $|H_1/H_2| = 3$ or $|H_2| = 3 \times 2^5$ and $|H_1/H_2| = 2$. In the former case, $T_{16} \in \mathcal{Y}_2^3$, and by Lemmas 2.1 and 2.3, $\chi(\Delta_f^{T_{16}}) \equiv 1 \pmod 3$. In the latter case, applying Lemma 3.19 to H_2, we can find there exists a normal subgroup H_3 of H_2 such that either $|H_3| = 2^5$ and $|H_2/H_3| = 3$ or $|H_3| = 3 \times 2^4$ and $|H_2/H_3| = 2$. Repeating this process, we can finally reach one of the following cases:

(1) For some integer k with $7 > k > 2$, there exists a normal subgroup chain

$$T_{16} \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_{k-1} \triangleright H_k$$

such that

$$|T_{16}/H_1| = 3, |H_i/H_{i+1}| = 2(i = 1, 2, \cdots, k-2), |H_{k-1}/H_k| = 3 \text{ and } |H_k| = 2^{8-k}$$

(2) there exists a normal subgroup chain

$$T_{16} \triangleright H_1 \triangleright H_2 \triangleright H_3 \triangleright H_4 \triangleright H_5 \triangleright H_6 \triangleright H_7$$

such that $|T_{16}/H_1| = 3$, $|H_i/H_{i+1}| = 2$ $(i = 1, 2, \cdots, 6)$ and $|H_7| = 3$.

In the former case, $\chi(\Delta_f^{T_{16}}) = \chi((\Delta_f^{H_1})^{T_{16}/H_1}) \equiv \chi(\Delta_f^{H_1}) \pmod 3$ by Lemma 3.15. Moreover, since f is not elusive, Δ_f is Z_2-acyclic by Corollary 2.1. Denote

$$\Delta_1 = ((\Delta_f^{H_1/H_2})^{H_2/H_3} \cdots)^{H_{k-2}/H_{k-1}}.$$

Then Δ_1 is Z_2-acyclic by Lemma 3.15, and

$$\chi(\Delta_f^{H_1}) = \chi((((\Delta_f^{H_1/H_2})^{H_2/H_3} \cdots)^{H_{k-2}/H_{k-1}})^{H_{k-1}}) = \chi(\Delta_1^{H_{k-1}}).$$

Furthermore, $\chi(\Delta_f^{H_{k-1}}) = 1$ by Lemma 2.3 since H_k is a normal 2-subgroup of H_{k-1} and H_{k-1}/H_k is a cyclic group of order 3. Thus, $\chi(\Delta_f^{T_{16}}) \equiv 1 \pmod 3$.

In the latter case, $\chi(\Delta_f^{T_{16}}) = \chi((\Delta_f^{H_1})^{T_{16}/H_1}) \equiv \chi(\Delta_f^{H_1}) \pmod 3$ by Lemma 3.15. If f is not elusive, then Δ_f is Z_2-acyclic by Corollary 2.1. Denote

$$\Delta_1 = (((((\Delta_f^{H_1/H_2})^{H_2/H_3})^{H_3/H_4})^{H_4/H_5})^{H_5/H_6})^{H_6/H_7}.$$

Then Δ_1 is Z_2-acyclic by Lemma 3.15 since $|H_i/H_{i+1}| = 2$ $(i = 1, 2, \cdots, 6)$. Thus,

$$\chi(\Delta_f^{H_1}) = \chi((((((((\Delta_f^{H_1/H_2})^{H_2/H_3})^{H_3/H_4})^{H_4/H_5})^{H_5/H_6})^{H_6/H_7})^{H_7}) = \chi(\Delta_1^{H_7}).$$

Moreover, $\chi(\Delta_1^{H_7}) = 1$ by Lemma 3.16 since H_7 is cyclic. This implies $\chi(\Delta_f^{T_{16}}) \equiv 1 \pmod 3$. □

Lemma 3.20 *Suppose G acts on the finite Z_p-acyclic complex Δ. If there exists a sequence of subgroups $P \triangleleft H \triangleleft G$ such that*

(1) G/H is of q-power order,

(2) H/P is of p-power order, and

(3) P is cyclic,

then $\chi(\Delta^G) \equiv 1 \pmod q$.

Proof. Since Δ is Z_p-acyclic and H/P is of p-power order, $\Delta^{H/P}$ is Z_p-acyclic by Lemma 3.15. Denote $\Delta_1 = \Delta^{H/P}$, then Δ_1 is Z_p-acyclic and hence Q-acyclic. By Lemma 3.16, $\chi(\Delta_1^P) = 1$. This, combined with Lemma 3.15, shows that

$$\chi(\Delta^G) = \chi((\Delta^H)^{G/H}) \equiv \chi(\Delta^H) = \chi((\Delta^{H/P})^P) = \chi(\Delta_1^P) = 1 \pmod q.$$

$\square$

Lemma 3.21 *Let $f(x_1, x_2, \cdots, x_{12})$ be a nontrivial monotone Boolean function, invariant under the action of T_{17}. If f is not elusive, then $\chi(\Delta_f^{T_{17}}) \equiv 1 \pmod 2$.*

Proof. Let

$$H = \langle (1,2,3), (4,5,6), (7,8,9), (10,11,12) \rangle.$$

It is easy to verify that $H \triangleleft T_{17}$ and $|H| = 3^4$. Moreover, $|T_{17}| = 2^5 \times 3^4$. Thus, $|T_{17}/H| = 2^5$. Denote $P = \langle (123) \rangle$. Clearly, $P \triangleleft H$, $|P| = 3$, and $|H/P| = 3^3$. Furthermore, P is cyclic by Lemma 3.11. By Corollary 2.1 and Lemma 3.21, $\chi(\Delta_f^{T_{17}}) \equiv 1 \pmod 2$. $\square$

Now we can prove our main theorem as follows.

Proof of Main Theorem. Let $f(x_1, x_2, \cdots, x_{12})$ be a nontrivial monotone weakly symmetric Boolean function. By the definition of weakly symmetry, there exists a transitive permutation group G on $\{1, 2, \cdots, 12\}$ such that f is invariant under G. By Lemma 3.1, G contains a transitive subgroup isomorphic to one of T_i for $i = 1, 2, \cdots, 17$, denoted by T. Note that T_1 is cyclic. When $T = T_i$ for $i = 1, \cdots, 14$, by Lemma 2.4 and Lemmas 3.2-3.14, f is elusive.

When $T = T_i$ ($i = 15, 16, 17$), T has only one orbit on Δ_f since it is transitive. This orbit cannot be a face of Δ_f. Otherwise, the monotonicity of f forces f being a constant, contradicting that f is nontrivial. Thus, $\Delta_f^T = \{\emptyset\}$ and $\chi(\Delta_f^T) = 0$. On the other hand, if f is not elusive, then by Lemmas 3.17, 3.19, and 3.21, $\chi(\Delta_f^T) \equiv 1 \pmod p$ where $p = 2$ or 3, a contradiction. $\square$

4 Discussion

Rivest-Vuillemin conjecture is showed to be true for nontrivial monotone Boolean functions of 12 variables. The proof involves many facts about permutation groups. With those facts, we established two new techniques which are used in dealing with groups T_i for $i = 9, \cdots, 17$.

References

[1] I. Wegener, *The Complexity of Boolean Functions,* Wcley-Teubner Series in Comp. Sci., (New York–Stuttgart, 1987).

[2] N. Nisan, CREW PRAM's and decision trees, *SIAM J. Computing,* 6 (1991) 999-1007.

[3] B. Bollobas, *Extremal Graph Theory*, (Academic Press, New York, 1978).

[4] J.D. Dixon and B. Mortimer, *Permutation Groups*, (Springer, New York, 1996).

[5] D.-Z. Du and K.-I Ko, *Theory of Computational Complexity*, (John-Wiley, New York, 2000) pp.147-192.

[6] S.-X. Gao, X.-D. Hu, and W. Wu, Nontrivial monotone weakly symmetric Boolean functions of six variables are elusive, *Theoretical Computer Science*, 223 (1999) 193-197.

[7] S.-X. Gao, W. Wu, D.-Z. Du, and X.-D. Hu, Rivest-Vuillemin conjecture on monotone Boolean functions is true for ten variables, *Journal of Complexity*, 15 (1999) 526-536.

[8] J. Greever, Stationary points for finite transformation groups, *Duke Math. J.*, 27 (1960) 163-170.

[9] J. Kahn, M. Saks and D. Strutevant, A topological approach to evasiveness, *Combinatorica*, 4 (1984) 297-306.

[10] R. Oliver, Fixed-point sets of group actions on finite acyclic complexes, *Comment. Math. Helvetici*, 50 (1975) 155-177.

[11] R. L. Rivest and S. Vuillemin, A generalization and proof of the Aanderaa-Rosenberg conjecture, in *Proc. of 7th ACM Symp. Theory of Computing,* (Albuquerque, 1975) 6-11.

[12] J.J. Rotman, *An Introduction to the Theory of Groups (4th edition)* (Springer-Verlag, New York, 1994)

[13] G.F. Royle, The transitive groups of degree twelve, *J. Symbolic Computation*, 4 (1987) 255-268.

[14] E.-F. Wang, *Basic of Finite Group Theory*, (Beijing University Press, 1987, in Chinese).