# On the Monotone Circuit Complexity of Quadratic Boolean Functions*

Kazuyuki Amano[†‡] Akira Maruoka[†]

November 28, 2005

**Abstract**

Several results on the monotone circuit complexity and the conjunctive complexity, i.e., the minimal number of AND gates in monotone circuits, of quadratic Boolean functions are proved. We focus on the comparison between single level circuits, which have only one level of AND gates, and arbitrary monotone circuits, and show that there is an exponential gap between the conjunctive complexity of single level circuits and that of general monotone circuits for some explicit quadratic function. Nearly tight upper bounds on the largest gap between the single level conjunctive complexity and the general conjunctive complexity over all quadratic functions are also proved. Moreover, we describe the way of lower bounding the single level circuit complexity and give a set of quadratic functions whose monotone complexity is strictly smaller than its single level complexity.

**Keywords** computational complexity, Boolean circuit, monotone circuit, conjunctive complexity, quadratic functions, graph theory

## 1 Introduction

Deriving a superlinear lower bound on the Boolean circuit-size complexity for an explicit Boolean function is one of the most challenging problems in computational

*A preliminary version of this paper appeared in the *Proceedings of the 15th Annual International Symposium on Algorithms and Computation (ISAAC '04)*, Lecture Notes in Computer Science, 3341, pp. 28–40.

†Graduate School of Information Sciences, Tohoku University, Aoba 6-6-05, Aramaki, Sendai 980-8579, Japan. Email:{ama|maruoka}@ecei.tohoku.ac.jp

‡Corresponding Author.

complexity. In an attempt to solve the problem, the complexity of many types of restricted circuits have been investigated. The model of monotone Boolean circuits, i.e., circuits with only AND and OR gates, is one of the most well-studied models.

In this paper, we investigate the monotone circuit complexity of the class of quadratic Boolean functions, i.e., functions of the form $\bigvee_{i,j} a_{i,j} \wedge x_i \wedge x_j$ where $a_{i,j} \in \{0,1\}$. Although we have a series of strong lower bounds on the monotone circuit complexity of explicitly defined Boolean functions [2, 3, 4, 6, 8, 9, 10, 17, 18, 20], such as exponential lower bounds for the clique function, we believe that an investigation of the monotone complexity of quadratic functions is important for several reasons:

(i) The method of approximations and their many variants have been successfully used to obtain exponential lower bounds on the monotone circuit complexity [2, 3, 4, 6, 8, 9, 10, 17, 18, 20]. However, several researchers have pointed out that these methods are shown to be equivalent [4, 6, 9, 10, 20]. In addition, a simple analysis of the method shows that it cannot yield any non-trivial lower bounds on the *monotone* circuit complexity of a quadratic Boolean function. This is because the method is in fact lower bounding the *minimum* of the number of AND gates and that of OR gates needed to compute the function, and every quadratic Boolean function on $n$ variables can be computed by a monotone circuit including at most $n-1$ AND gates. So a superlinear lower bound for quadratic Boolean functions may imply an essentially different method for lower bounding the monotone circuit complexity. (ii) For a certain natural class of quadratic Boolean functions, which we will describe in Section 4, we can show that a superlinear lower bound on the monotone circuit complexity of a function $f$ in that class immediately implies a lower bound of the same order on the *general* circuit complexity of $f$. In addition, we hope that a lower bound proof that is highly specialized for a particular function may not fulfill the "largeness" condition in the notion of "natural proof" [19].

A quadratic Boolean function is naturally represented by a graph. Let $G = (V, E)$ be an undirected graph with vertex set $V = \{1, \ldots, n\}$ and edge set $E \subseteq \{(i,j) \mid 1 \leq i < j \leq n\}$. A quadratic (Boolean) function associated with $G$ is defined by $f_G(x_1, \ldots, x_n) = \bigvee_{(i,j)\in E} x_i x_j$.

There has been a series of research studies on the complexity of quadratic Boolean functions (sometimes under the name of graph complexity), which are mostly concerned with circuits of constant depth with unbound fan-in gates (e.g., [11, 14, 16]). In this paper, we restrict the fan-in of gates to two and mainly focus on the comparison between single level monotone circuits and general monotone circuits. A single level circuit is a circuit which has only one level of AND gates. Obviously, every quadratic function can be computed by a single level circuit of size $O(n^2)$. Not surprisingly, if we restrict ourselves to circuits of single level, we can easily derive a superlinear lower bound on the size. (We will describe this in more detail in Section 3.3.) However, it seems quite difficult to obtain a good lower bound on the general monotone circuit size for an explicit quadratic function.

One of the major differences between single level circuits and general circuits in a computation of quadratic functions relies on the use of the "absorption rule", i.e., $f \vee fg = f$ (and $f(f \vee g) = f$). We consider that an investigation on the efficiency of the absorption rule in a monotone computation may be a key to obtain a tighter/higher lower bound on the monotone complexity, and this was the initial motivation of our work.

The contributions of this paper are as follows: First, in Section 3, we consider the conjunctive complexity of quadratic Boolean functions. The conjunctive complexity of a quadratic function $f_G$ is the minimal number of AND gates in a monotone circuit that computes $f_G$. Such measures have been widely studied by, for example, Tuza [22], Lenz and Wegener [13]. In Section 3.2, we prove that there is an exponential gap between the conjunctive complexity of single level circuits and that of general monotone circuits for a certain explicit quadratic function (Theorem 2). Nearly tight upper bounds on the largest gap between the single level conjunctive complexity and the general conjunctive complexity over all quadratic functions are also proved (Theorem 3). Then, in Section 3.3, we describe the way of lower bounding the single level circuit complexity (Theorem 5) and give a set of quadratic functions whose monotone circuit complexity is strictly smaller than its single level complexity (Theorem 6). Finally, in Section 4, we discuss the relationship between the complexity of monotone circuits and of non-monotone circuits for quadratic functions based on the notion of pseudo complements (Theorem 7).

# 2 Boolean Circuits

A *Boolean circuit* is a directed acyclic graph. Nodes with indegree zero are called *input* nodes and there are distinguished nodes with outdegree zero called *output* nodes. An input node is labeled by a Boolean variable or a constant 0 or 1. Each non-input node has indegree 2 or 1 and is called the *gate* node. A gate node of indegree 2 is labeled by a Boolean operation AND ($\wedge$) or OR ($\vee$). A gate node of indegree 1 is labeled by a Boolean operation NOT ($\neg$). A gate in a Boolean circuit computes a Boolean function in a natural way. If $g$ is a gate in a Boolean circuit, we will also use $g$ to denote the function computed by $g$. A Boolean circuit computes Boolean functions that are computed by the output gates. A *monotone Boolean circuit* is a Boolean circuit that contains no NOT gates. A Boolean function that can be computed by a monotone Boolean circuit is called a *monotone Boolean function.* Since we will not discuss any non-Boolean functions, we may drop the word "Boolean".

# 3 Single Level vs. Multi Level

## 3.1 Notations

Let $G = (V, E)$ be an undirected graph with vertex set $V = \{1, \ldots, n\}$ and edge set $E \subseteq \{(i,j) \mid 1 \le i < j \le n\}$. A quadratic (Boolean) function associated with $G$ is defined by $f_G(x_1, \ldots, x_n) = \bigvee_{(i,j)\in E} x_i x_j$.

For a monotone circuit $C$, the *level* of $C$ is defined as the maximal number of AND gates on a path from an input to an output in $C$. In particular, a circuit of level 1, i.e., a circuit such that no path combines AND gates, is called a *single level* circuit. Obviously, for every graph $G = (V, E)$ on $V = \{x_1, \ldots, x_n\}$, the function $f_G$ can be computed by a single level circuit including at most $|V| - 1$ AND gates and $|E|$ OR gates using the form $\bigvee_{1\le i<n} x_i \wedge (\vee_{j:(i,j)\in E} x_j)$.

Let $f$ be a monotone function. The *circuit complexity* (the *monotone circuit complexity*, resp.) of $f$, denoted by $size(f)$ ($size_{mon}(f)$, resp.), is the minimal number of gates in a Boolean circuit (a monotone circuit, resp.) for $f$, and the single level complexity of $f$, denoted by $size^1_{mon}(f)$, is the minimal number of gates in a single level monotone circuit for $f$.

In this paper, we also investigate the number of AND gates needed to compute a function, which is called as the *conjunctive complexity*. The conjunctive complexity (the single level conjunctive complexity, resp.) of $f$, denoted by $size_{mon,\wedge}(f)$ ($size^1_{mon,\wedge}(f)$, resp.), is the minimal number of AND gates in a monotone circuit (a single level monotone circuit, resp.) that computes $f$.

## 3.2 Conjunctive Complexity

If we restrict ourselves to circuits of single level, the conjunctive complexity of a quadratic function $f_G$ is equal to the minimal number of complete bipartite graphs whose union (of the edge sets) coincides with $G$.

Since the single level conjunctive complexity $size^1_{mon,\wedge}(f)$ is a purely graph theoretical complexity measure, it has been widely studied (see e.g., [13]). In contrast, little is known about the conjunctive complexity $size_{mon,\wedge}(f)$. In the following, we show that almost all quadratic functions have a conjunctive complexity $\Theta(n)$, which improves the $n/(c \log n)$ lower bound of Lenz and Wegener [13]. We remark that it was shown that almost all quadratic functions have a single level conjunctive complexity of larger than $n - c \log n$.

**Theorem 1** *For each $c < 1/13$, the conjunctive complexity of almost all quadratic functions is larger than $cn$.*

*Proof.* The proof of the theorem is analogous to the proof of the $n/(c \log n)$ lower bound by Lenz and Wegener [13]. The only difference is that we use the result of Zwick [26], which says that if $f$ can be computed by a monotone circuit that contains $k$ AND gates, then $f$ can also be computed by a monotone circuit that contains $k$ AND gates and $O(k(n+k)/\log k)$ OR gates, instead of the result of Alon and Boppana [2], which is slightly weaker than the result of Zwick.

Careful inspection of Zwick's proof reveals that the hidden constant in the Big-O notation of their upper bound is at most 3. The standard counting argument shows that, for each $d > 4$, the monotone circuit complexity of almost all quadratic functions is at least $n^2/(d \log n)$. Hence, for almost all graphs on $n$ vertices $G$, if we denote the conjunctive complexity of $f_G$ by $k$, then

$$\frac{n^2}{d \log n} \leq \frac{3k(n+k)}{\log k} + k$$

holds. A simple calculation shows that $k \geq cn$ for sufficiently large $n$. $\square$

One might conjecture that an optimal circuit for a quadratic function with respect to the conjunctive complexity is always given by a single level circuit. This was known as *the single level conjecture* (with respect to the conjunctive complexity) and was *disproved* by Lenz and Wegener [13]. They provided an explicit graph $H$ on 8 vertices such that $4 = size^1_{mon,\wedge}(f_H) > size_{mon,\wedge}(f_H) = 3$, and asked what the largest possible value of $size^1_{mon,\wedge}(f_G)/size_{mon,\wedge}(f_G)$ is (as open problem No. 7 in [13]).

In the following, we improve their result by giving an explicit construction of a graph $G$ on $n$ vertices such that $size^1_{mon,\wedge}(f_G)/size_{mon,\wedge}(f_G) = \Omega(n/\log n)$.

**Theorem 2** *There is a graph $G$ on $n$ vertices such that $size^1_{mon,\wedge}(f_G) = \Omega(n)$ and $size_{mon,\wedge}(f_G) = O(\log n)$.*

*Proof.* Let $\tilde{G} = (U \cup V, \tilde{E})$ be a bipartite graph with $U = \{u_1, \ldots, u_{n/2}\}$, $V = \{v_1, \ldots, v_{n/2}\}$ and $\tilde{E} = \{(u_i, v_i) \mid i = 1, \ldots, n/2\}$. For simplicity, we assume that $n = 2^t$ for some positive integer $t$. Let $G$ be a graph on $U \cup V$ such that $G = \tilde{G} \cup K_U \cup K_V$, where $K_U$ and $K_V$ are the complete graphs on $U$ and $V$, respectively. In the following, we show that $size^1_{mon,\wedge}(f_G) \geq n/4$ and $size_{mon,\wedge}(f_G) = O(\log n)$.

First, we show that $size^1_{mon,\wedge}(f_G) \geq n/4$. Let $C$ be a single level monotone circuit for $f_G$. For a function $g$, let $PI(g)$ denote the set of all prime implicants of $g$. Since $\tilde{G}$ contains $n/2$ edges, it is sufficient to show that for every $\wedge$ gate $g$ in $C$, if $PI(g)$ contains more than two edges in $\tilde{G}$, then $g$ can be eliminated without changing the output of $C$. Let $g_1$ and $g_2$ be two inputs of $g$. Note that $g_1$ and $g_2$ are OR's of variables. Suppose that $PI(g)$ contains three edges in $\tilde{G}$, say $(u_i, v_i)$,$(u_j, v_j)$ and $(u_k, v_k)$. Then, w.l.o.g., we can assume that for some distinct indices $i_1, i_2 \in \{i, j, k\}$, $u_{i_1}$ and $u_{i_2}$ appear in $g_1$, and $v_{i_1}$ and $v_{i_2}$ appear in $g_2$. This implies that $PI(g)$ contains $(u_{i_1}, v_{i_2})$, which is not included in $\tilde{G}$. Hence, $g$ cannot contribute to the output of $C$, and can be safely removed.

We now show that $size_{mon,\wedge}(f_G) = O(\log n)$. Let $d$ be a positive integer whose value will be chosen later. Let $l = 2^{d-1}$ and $r = (n/2)^{1/l}$. For simplicity, we assume that $r$ is an integer. For $1 \leq k \leq n/2$, we represent $k$ by a vector $k = (k_1, \ldots, k_l) \in \{1, \ldots, r\}^l$. It will be convenient to consider that $k$ is represented by an $r$-ary $l$-digits number. For $1 \leq i \leq l$ and $1 \leq j \leq r$, let $P_j^i$ ($Q_j^i$, resp.) be the set of $n/r$ variables which consists of all $u_k$ ($v_k$, resp.) such that $k = (r_1, \ldots, r_{i-1}, j, r_{i+1}, \ldots, r_l)$ for some $r_1, \ldots, r_l \in \{1, \ldots, r\}$, i.e., the $i$-th digit of the $r$-ary representation of $k$ is equal to $j$.

We claim that $f_G$ is equivalent to

$$\bigwedge_{1 \leq i \leq l} \left( \bigvee_{1 \leq j \leq r} \left( OR(P_j^i) \wedge OR(Q_j^i) \right) \right) \vee \left( Th_2^{n/2}(U) \vee Th_2^{n/2}(V) \right), \tag{1}$$

where $OR(X)$ denotes the disjunction of all variables of $X$ and $Th_k^n(X)$ denotes the $k$-threshold function on $n$ variables, i.e., it outputs 1 iff the number of ones in an input is greater than or equal to $k$.

Before we show the correctness of Eq. (1), we determine the value of $d$ and estimate the number of AND gates needed to compute Eq. (1). Since (i) the AND of $l$ functions can be computed by a circuit of level $\log l = d - 1$ with $l - 1$ AND gates, and (ii) the 2-threshold function on $n/2$ variables can be computed by a single level circuit that includes $\log(n/2) = \log n - 1$ AND gates[1], we can construct a $d$-level circuit including at most

$$lr + l - 1 + 2(\log n - 1) \quad < \quad 2^{d-1}((n/2)^{1/2^{d-1}} + 1) + 2\log n \tag{2}$$

AND gates. If we choose $d = \log\log n$, the RHS of Eq. (2) is upper bounded by $4.5 \log n$.

Now we proceed to the proof of the correctness of Eq. (1). Obviously, for an input with at most 1 one, both $f_G$ and Eq. (1) output 0. For an input with at least 3 ones, both $f_G$ and Eq. (1) output 1 because (at least) one of two sets $U$ and $V$ contains at least 2 variables that are assigned the value 1. Thus, the interesting cases are for an input with 2 ones.

(Case 1) $u_{k_1} = u_{k_2} = 1$ or $v_{k_1} = v_{k_2} = 1$ for some $k_1 \neq k_2$.

Obviously, both $f_G$ and Eq.(1) output 1 in this case.

(Case 2) $u_k = v_k = 1$ for some $k \in \{1, \ldots, n/2\}$.

By the definition of $G$, $f_G$ outputs 1 on such an input. For each $1 \leq i \leq l$, $OR(P_{k_i}^i) = OR(Q_{k_i}^i) = 1$ if $k_i$ is equal to the $i$-th digit of $r$-ary representation of $k$. This implies the output of Eq. (1) is also 1.

[1]Proof: Let $X = \{x_1, \ldots, x_n\}$ and consider that an integer $k = 1, \ldots, n$ is represented by a $\log n$-digits binary number. Let $X_{i,j}$ ($j \in \{0, 1\}$) be the OR of all $x_k$ such that the $i$-th digit of the binary representation of $k$ is equal to $j$. Then it is easy to confirm that $Th_2^n \equiv \vee_{1 \leq i \leq \log n}(X_{i,0} \wedge X_{i,1})$.

(Case 3) $u_{k_1} = v_{k_2} = 1$ for some $k_1 \neq k_2$.

By the definition of $G$, $f_G$ outputs 0 on such an input. Since $k_1 \neq k_2$, there is $1 \leq i \leq l$ such that the $i$-th digit of the $r$-ary representation of $k_1$ and $k_2$ are different. For such $i$, the value of $\bigvee_{1 \leq j \leq l}(OR(P_j^i) \wedge OR(Q_j^i))$ is 0, and this implies the output of Eq. (1) is also 0. $\square$

**Remark 1** *The graph we defined in the proof of Theorem 2 consists of three subgraphs, $\tilde{G}$, $K_U$ and $K_V$. Interestingly, the single level conjunctive complexity and the conjunctive complexity of each subgraph are identical, i.e., $size^1_{mon,\wedge}(\tilde{G}) = size_{mon,\wedge}(\tilde{G}) = n/2$, $size^1_{mon,\wedge}(K_U) = size_{mon,\wedge}(K_U) = \log n - 1$ and $size^1_{mon,\wedge}(K_V) = size_{mon,\wedge}(K_V) = \log n - 1$.*

Let $Gap_\wedge(n) = \max\{size^1_{mon,\wedge}(f_G)/size_{mon,\wedge}(f_G) \mid G = (V,E), |V| = n\}$. Theorem 2 shows that $Gap_\wedge(n) = \Omega(n/\log n)$. Note that the upper bound of $O(n)$ is trivial since $size^1_{mon,\wedge}(f_G) \leq n-1$ for every $G$ on $n$ vertices. We conjecture that our lower bound is tight, i.e., $Gap_\wedge(n) = \Theta(n/\log n)$. Below we prove a slightly weaker upper bound of $Gap_\wedge(n) = O(n/\log\log n)$.

**Theorem 3** *Let $G$ be a graph on $n$ vertices. Suppose that $size^1_{mon,\wedge}(f_G) = \Omega(p(n))$ for some function $p(\cdot)$. Then $size_{mon,\wedge}(f_G) = \Omega(\log\log p(n))$.*

*Proof.* Let $G$ be a graph on $n$ vertices whose single level conjunctive complexity is $\Omega(p(n))$. Let $C$ be an arbitrary monotone circuit that computes $f_G$. Below we show that $C$ must contain $\Omega(\log\log p(n))$ AND gates.

For a monotone function $h$, let $PI_i(h)$ be the set of all prime implicants of $h$ whose length is $i$. The *covering number* of $h$, denoted by $cov(h)$, is defined as the minimal $m$ such that there are $m$ pairs of sets of variables $(A_i, B_i)$ $(i = 1, \ldots, m)$ that satisfy (i) $A_i \cap B_i = \emptyset$ $(\forall i)$, (ii) $A_i \times B_i \subseteq PI_2(h)$ $(\forall i)$, and (iii) $\bigcup_{i=1}^m A_i \times B_i = PI_2(h)$. In such a case, we say that a set of pairs $\{(A_i, B_i) \mid i = 1, \ldots, m\}$ *covers* $PI_2(h)$. Obviously, $cov(f_G) = size^1_{mon,\wedge}(f_G)$ for every $G$.

We define the operation $\wedge^*$ as follows: Suppose that $g = g_1 \wedge g_2$. Then $g_1 \wedge^* g_2$ is the disjunction of all prime implicants of $g$ whose length is at most 2. Let $C^*$ be a circuit obtained from $C$ by replacing each $\wedge$ gate in $C$ with $\wedge^*$ gate. The theorem known as the "replacement rule" (see e.g., [24, Theorem 5.1]) guarantees that the circuit $C^*$ also computes $f_G$. In the following, we assume that if $g_1$ and $g_2$ are two inputs of an $\wedge^*$ gate in $C^*$, then $PI_1(g_1)$ and $PI_1(g_2)$ are disjoint. (If $PI_1(g_1) \cap PI_1(g_2) = S \neq \emptyset$, then we replace $g_1 \wedge^* g_2$ by $(h_1 \wedge^* h_2) \vee OR(S)$ where $h_i$ is obtained from $g_i$ by removing all prime implicants in $S$. This does not affect the number of $\wedge^*$ gates in $C^*$ and the output of $C^*$. In addition, this replacement has no influence on the covering number of each gate.)

For an $\wedge^*$ gate $g$ in $C^*$, the *level* of $g$ is defined as the maximal number of $\wedge^*$ gates on a path from an input to (the output of) $g$. Note that the lowest $\wedge^*$ gate is of level 1. Let $d$ be the level of the circuit $C^*$, and for $i = 1, \ldots, d$, let $k_i$ be the number of $\wedge^*$ gates whose level is $i$. Note that the number of $\wedge^*$ gates in $C^*$, say $k$, is given by $k = \sum_{i=1}^{d} k_i$.

Let $g = g_1 \wedge^* g_2$ be an arbitrary $\wedge^*$ gate of level $l$ in $C^*$. We claim that

$$\begin{aligned} cov(g) &\leq 5 \cdot 6^{2^{l-1}-2} \max\{k_1, \ldots, k_{l-1}\}^{2^l-2}, && \text{(for } l \geq 2), && (3) \\ cov(g_i) &\leq 6^{2^{l-2}-1} \max\{k_1, \ldots, k_{l-1}\}^{2^{l-1}-1}, && \text{(for } l \geq 2 \text{ and } i = 1, 2). && (4) \end{aligned}$$

To prove these inequalities, we need the following lemma.

**Lemma 1** *Let $h = h_1 \wedge^* h_2$. Suppose that $cov(h_1), cov(h_2) \geq 1$ and $PI_1(h_1) \cap PI_1(h_2) = \emptyset$. Then $cov(h) \leq 5 \cdot cov(h_1)cov(h_2)$.*

*Proof.* Let $m_1 = cov(h_1)$ and $m_2 = cov(h_2)$. We can express $h_1$ and $h_2$ as

$$h_1 = t_1 \vee \bigvee_{i=1}^{m_1} a_{i,1}b_{i,1}, \qquad h_2 = t_2 \vee \bigvee_{i=1}^{m_2} a_{i,2}b_{i,2},$$

where the $t_j$, $a_{i,j}$ and $b_{i,j}$ are disjunctions of variables such that $Var(a_{i,j}) \cap Var(b_{i,j}) = \emptyset$ $(\forall i, j)$ and $Var(t_1) \cap Var(t_2) = \emptyset$. We have

$$\begin{aligned} PI_2(h_1 \wedge^* h_2) &= \bigvee_{i_1,i_2} PI_2(a_{i_1,1}a_{i_2,1}b_{i_1,1}b_{i_2,2}) \\ &\quad \vee \bigvee_{i_2} PI_2(t_1 a_{i_2,2}b_{i_2,2}) \vee \bigvee_{i_1} PI_2(t_2 a_{i_1,1}b_{i_1,1}) \vee PI_2(t_1 t_2). \end{aligned}$$

It is easy to check that, for each pair $(i_1, i_2)$, $PI_2(a_{i_1,1}a_{i_2,1}b_{i_1,1}b_{i_2,2})$ can be covered by two pairs, namely, $(a_{i_1,1} \cap a_{i_2,2}, b_{i_1,1} \cap b_{i_2,2})$ and $(a_{i_1,1} \cap b_{i_2,2}, a_{i_2,2} \cap b_{i_1,1})$. Similarly, each $PI_2(t_1 a_{i_2,2}b_{i_2,2})$ ($PI_2(t_2 a_{i_1,1}b_{i_1,1})$, resp.) can be covered by a pair $(t_1 \cap a_{i_2,2}, t_1 \cap b_{i_2,2})$ ($(t_2 \cap a_{i_1,1}, t_2 \cap b_{i_1,1})$, resp.). Altogether, $PI_2(h_1 \wedge^* h_2)$ can be covered by a set of at most $2m_1m_2 + m_1 + m_2 + 1 \leq 5m_1m_2$ pairs. □

*Proof of Theorem 3(continued)* By Lemma 1, Eq. (4) immediately implies Eq. (3) for each $l$. Hence, we only need to show Eq. (4). We show this by induction on $l$.

The base case, $l = 2$, is obvious since RHS of Eq. (4) is $k_1$ and the covering number of an input of an $\wedge^*$ gate of level 2 is shown to be at most $k_1$.

The induction step is as follows: Since the function computed by an input of an $\wedge^*$ gate of level $l$ can be represented by the disjunction of variables and outputs of $\wedge^*$ gates at a level of at most $l - 1$, the covering number of it is upper bounded by

$$\begin{aligned} &5k_{l-1}6^{2^{l-2}-2} \max\{k_1, \ldots, k_{l-2}\}^{2^{l-1}-2} + 6^{2^{l-3}-1} \max\{k_1, \ldots, k_{l-2}\}^{2^{l-2}-1} \\ &\leq 6^{2^{l-2}-1} \max\{k_1, \ldots, k_{l-1}\}^{2^{l-1}-1}, \end{aligned}$$

which completes the proof of the induction step.

The assumption $size^1_{mon,\wedge}(f_G) = \Omega(p(n))$ in the statement of the theorem implies that $k$ times the value of Eq. (3) for $l = d$ is $\Omega(p(n))$, and this implies $(6k)^{2^k} \geq (6k)^{2^d} = \Omega(p(n))$ (since $k \geq d$). Hence we have $k = \Omega(\log\log p(n))$, which completes the proof of the theorem. $\Box$

## 3.3 Disproving Single Level Conjecture for Multi-Output Functions

Again, if we restrict ourselves to circuits of single level, a good lower bound on $size^1_{mon}(f)$ can easily be derived by combining the graph theoretic arguments and the results that have been developed for obtaining a lower bound on the monotone complexity of the *Boolean sums*, which we state below.

**Definition 1** *Let $X = \{x_1, \ldots, x_n\}$. $F(X) \equiv (f_1, \ldots, f_m) : \{0,1\}^n \to \{0,1\}^m$ is a set of Boolean sums if each function $f_i$ is a disjunction of variables in $X$. For a disjunction $f$ of variables in $X$, we use $Var(f)$, which denotes the subset of $X$ on which $f$ essentially depends. A set of Boolean sums $F$ is called $(h,k)$-disjoint if for every $\{i_0, \ldots, i_h\} \subseteq \{1, \ldots, m\}$, $|\bigcup_{i=0}^h Var(f_i)| \leq k$ holds.*

**Theorem 4 ([15])** *Let $F = (f_1, \ldots, f_m)$ be a set of Boolean sums. If $F$ is $(h,k)$-disjoint, then the size of an optimal monotone circuit for $F$ is at least*

$$\sum_{1 \leq i \leq m} \frac{\lceil |Var(f_i)|/k \rceil - 1}{h \max\{1, h-1\}}.$$

By using the above theorem, we can show the following.

**Theorem 5** *Let $G = (V, E)$ be a graph that does not contain a copy of $K_{2,2}$. Then $size^1_{mon}(f_G) \geq |E|$.*

*Proof.* Let $C$ be an optimal single level monotone circuit for $f_G$. We represent $f_G = \vee_{i=1}^k g_{i,1} g_{i,2}$, where $k$ is the number of AND gates in $C$, and $g_{i,1}$ and $g_{i,2}$ are disjunctions of variables computed by the inputs of the $i$-th AND gate.

For each $i = 1, \ldots, k$, at least one of $Var(g_{i,1})$ or $Var(g_{i,2})$ contains at most one variable. This is because if $|Var(g_{i,1})| \geq 2$ and $|Var(g_{i,2})| \geq 2$, then $G$ must contain $K_{2,2}$ (if two sets are disjoint), or $f_G$ must contain a prime implicant of length 1 (if two sets are not disjoint). Hence, without loss of generality, we can assume that

$|Var(g_{i,1})| = 1$ for every $i = 1, \dots, k$ (by exchanging $g_{i,1}$ and $g_{i,2}$ if necessary). Let $X = \bigcup_i Var(g_{i,1})$. Now we convert $C$ to a circuit $C'$ by the following construction:

$$\bigvee_{x \in X} x \wedge \left( \bigvee_{j:Var(g_{j,1})=\{x\}} g_{j,2} \right).$$

Since we can save $k - |X|$ AND gates and the number of additional OR gates we need is shown to be at most $k - |X|$, the size of $C'$ is not greater than that of $C$.

For each $x \in X$, let $h_x = \bigvee_{j:Var(g_{j,1})=\{x\}} g_{j,2}$. It is obvious that $Var(h_x)$ is a subset of the set of neighbors of $x$. Since $G$ does not contain $K_{2,2}$, $|Var(h_{x_1}) \cap Var(h_{x_2})| \leq 1$ for every distinct $x_1, x_2 \in X$. Hence the set of functions $H = \{h_x \mid x \in X\}$ can be viewed as the $(1,1)$-disjoint Boolean sums. Therefore, the size of $C'$ is at least

$$size_{mon}(H) + |X| + |X| - 1 \quad \geq \quad |E| - |X| + 2|X| - 1 \geq |E|.$$

The first inequality follows from Lemma 4. $\square$

An explicit construction of the graph on $n$ vertices that does not contain $K_{2,2}$ and has $\Omega(n^{3/2})$ edges based on the notion of the "projective plane" is known (e.g., [1]). The above theorem yields $size^1_{mon}(f_G) = \Omega(n^{3/2})$ for such $G$. We remark that we can extend the arguments of the proof of Theorem 5 for a graph that does not contain a copy of $K_{r,r}$ for $r > 2$. Thus, an explicit construction for such a graph (see e.g., [5]) may yield higher lower bounds on the size of single level circuits.

The following question then arises: "Is there a quadratic function $f$ such that $size_{mon}(f_G)$ is strictly smaller than $size^1_{mon}(f_G)$?"

The problem of answering this question was stated as an open problem in [13]. We have shown in the previous section that the answer is "yes" if we only count the number of AND gates. In the following, we show that the answer is also "yes" if we consider *a set of* quadratic functions.

For a set of $m$ graphs $\mathcal{G} = (G_1, \dots, G_m)$, a set of quadratic functions associated with $\mathcal{G}$, denoted by $f_{\mathcal{G}}$, is defined by the set of $m$ functions $(f_{G_1}, \dots, f_{G_m})$.

**Lemma 2** *Let $H = (h_1, \dots, h_m)$ be a set of Boolean sums on $\{x_1, \dots, x_n\}$. Let $F = (f_1, \dots, f_m)$ be a set of quadratic functions on $U \cup V = \{u_1, \dots, u_n\} \cup \{v_1, \dots, v_n\}$ where each $f_i$ is obtained from $h_i$ by replacing each variable $x_k$ in $h_i$ with the conjunction $u_k v_k$. Then an optimal single level monotone circuit for $F$ is a circuit obtained from an optimal monotone circuit for $H$ that consists of OR gates only by replacing each input node $x_k$ with an AND gate $u_k \wedge v_k$.*

*Proof.* Let $C$ be an optimal single level monotone circuit for $F$. Let $g$ be an AND gate in $C$. Since $C$ is a single level circuit, we can represent $g = g_1 \wedge g_2$ where $g_1$ and

$g_2$ are disjunctions of variables. Suppose that $g$ contains a prime implicant not of the form $u_k v_k$ for some $k$. In such a case, there is an assignment to the input variables that contains at most 2 ones such that $g$ outputs 1 and $f_i$ outputs 0 for every $i$. This implies that there are no paths from an input to an output of $C$ that lead through $g$ (since $C$ is a single level circuit), and this contradicts the assumption that $C$ is optimal. Hence we can conclude that every AND gate computes the conjunction of the form $u_k v_k$ for some $k$. □

**Theorem 6** *There is a set of graphs $\mathcal{G} = (G_1, \ldots, G_{14})$ such that $size_{mon}(f_{\mathcal{G}})$ is strictly smaller than $size^1_{mon}(f_{\mathcal{G}})$.*

*Proof.* To prove this theorem, we use the construction of Boolean sums given by Tarjan [21] (or [24, p.164]), which was used for disproving that AND gates are powerless for computing Boolean sums. Let $H = (h_1, \ldots, h_{14})$ be a set of Boolean functions on $\{x_1, \ldots, x_{11}\}$ defined as follows: Let

$$\begin{array}{llll} H_1 = \{1,5\}, \quad H_2 = \{2,6\}, & H_3 = \{3,5\}, \quad H_4 = \{4,6\}, & \\ H_5 = \{5,9\}, & H_6 = \{5,9,10\}, & H_7 = \{5,9,10,11\}, \\ H_8 = \{6,9\}, & H_9 = \{6,9,10\}, & H_{10} = \{6,9,10,11\}, \\ H_{11} = H_1 \cup \{7,9,10,11\}, & H_{12} = H_2 \cup \{8,9,10,11\}, & \\ H_{13} = H_3 \cup \{7,9,10,11\}, & H_{14} = H_4 \cup \{8,9,10,11\}, & \end{array}$$

and define $h_i = \bigvee_{k \in H_i} x_k$ for $i = 1, \ldots, 14$. It was shown that 18 OR gates are necessary to compute $H$ if no AND gates are used. On the other hand, we can compute $H$ by a circuit that contains 16 OR gates and one AND gate (an AND gate that computes $h_7 \wedge h_{10}$ can save two OR gates.)

Define a set of the quadratic functions $F = (f_1, \ldots, f_{14})$ as in the statement of Lemma 2. By the above argument, we have $size_{mon}(F) \leq 17 + 11 = 28$. On the other hand, by Lemma 2, we have $size^1_{mon}(F) = 18 + 11 = 29$, which completes the proof of the theorem. □

As for the case of the conjunctive complexity, to determine the largest possible value of $size^1_{mon}(F)/size_{mon}(F)$ seems to be an interesting subject. The construction in the proof of Theorem 6 gives the lower bound of 29/28. More sophisticated constructions may yield a slightly better constant. The authors do not know whether there is a set of quadratic functions $F$ such that the ratio is more than a constant.

# 4 Monotone vs. Non-Monotone

The graph $G$ that we defined in the proof of Theorem 2 has the form of $G = \tilde{G} \cup K_U \cup K_V$ where $\tilde{G} \subseteq U \times V$ is a bipartite graph, and $K_U$ and $K_V$ are the complete graphs on $U$ and $V$, respectively. Interestingly, it is shown that NOT gates are almost powerless for quadratic functions associated with graphs of such form.

**Theorem 7** *(implicitly in [23]) Let $G$ be a graph on $\{1,\ldots,n\}$ such that $G=\tilde{G}\cup K_U\cup K_V$ where $\tilde{G}\subseteq U\times V$ for some partition $U,V\subseteq\{1,\ldots,n\}$. Then*

$$size_{mon}(f_G)\le 2size(f_G)+6n+o(n).$$

*Proof.* In fact, the result by Wegener [23, Theorem 4.4] is of the form $size_{mon}(f_G)\le O(size(f_G))+O(n)$. For the purpose of completeness and in order to determine the hidden constants, we describe the outline of the proof of the theorem here.

Given an optimal circuit $C$ which computes $f_G$, by using DeMorgan's law, we can convert $C$ to a so-called standard circuit $C'$ for $f_G$, that is a Boolean circuit in which the permitted gate operations are $\{\wedge,\vee\}$ and whose input nodes are labeled by literals, whose size is at most twice of the size of $C$.

Let $U=\{u_1,\ldots,u_k\}$ and $V=\{v_1,\ldots,v_{n-k}\}$. Let $u'_i=u_i\wedge OR(V)$, $v'_i=v_i\wedge OR(U)$, $\tilde{u}_i=\vee_{j\ne i}u'_j$ and $\tilde{v}_i=\vee_{j\ne i}v'_j$. Let $f'$ be a function computed by a circuit obtained from $C'$ by replacing each $u_i$ ($v_i$, resp.) with $u'_i$ ($v'_i$, resp.) and each $\bar{u}_i$ ($\bar{v}_i$, resp.) with $\tilde{u}_i$ ($\tilde{v}_i$, resp.). The key to the proof is the observation that $f_G$ can be computed by $f'\vee Th_2^{|U|}(U)\vee Th_2^{|V|}(V)$. (In other words, we can use $u'_i$ and $v'_i$ as *pseudoinputs* and $\tilde{u}_i$ and $\tilde{v}_i$ as *pseudocomplements* for $u_i$ and $v_i$, respectively. See [23] for the proof of the correctness of this replacement.)

Using the following equation,

$$Th_2^n(X)=\bigvee_{q=1}^{2}Th_2^{\sqrt{n}}\left(OR(B_1^q),\ldots,OR(B_{\sqrt{n}}^q)\right),$$

where $X=\{x_{r_1r_2}\mid 1\le r_1,r_2\le\sqrt{n}\}$ and $B_i^q=\{x_{s_1s_2}\mid s_q=i\}$, we can compute $Th_2^{|U|}$ and $Th_2^{|V|}$ with at most $2(|U|+|V|)+o(n)=2n+o(n)$ gates. Clearly, $\sqrt{|U|}+\sqrt{|V|}=o(n)$ additional gates are sufficient to compute $OR(U)$ and $OR(V)$. All $u'_i$ and $v'_i$ can be computed with $n$ gates. Moreover, $3|U|+3|V|=3n$ gates are sufficient to compute all $\tilde{u}_i$ and $\tilde{v}_i$. Altogether we use $6n+o(n)$ gates at most. $\square$

It should be noted that the standard counting argument shows that the circuit complexity of almost all quadratic functions associated with graphs of the form $G\cup K_U\cup K_V$, where $\tilde{G}\subseteq U\times V$, is $\Omega(n^2/\log n)$.

For a bipartite graph $G\subseteq U\times V$, let $G^+$ be the graph $G\cup K_U\cup K_V$. The relationship between the monotone complexity of $f_G$ and of $f_{G^+}$ seems to be interesting. Since $size_{mon}(Th_2^n)$ is known to be $2n+o(n)$, we have $size_{mon}(f_{G^+})\le size_{mon}(f_G)+2n+o(n)$. On the other hand, we do not know whether $size_{mon}(f_{G^+})=\Omega(size_{mon}(f_G))$ or not. However, if we consider multi-output functions, computing a set of functions $f_{G_1^+},\ldots,f_{G_m^+}$ may be significantly easier than computing a set of functions $f_{G_1},\ldots,f_{G_m}$.

The $n$-point Boolean convolution $\mathrm{CONV}_n(x_0,\ldots,x_{n-1}, \quad y_0,\ldots,y_{n-1})$: $\{0,1\}^{2n} \to \{0,1\}^{2n-1}$ is the function with output $(S_0,\ldots,S_{2n-2})$ defined by

$$S_k(x_0,\ldots,x_{n-1},y_0,\ldots,y_{n-1}) = \bigvee_{i+j=k} x_i y_i.$$

Each $S_k$ is naturally represented by a bipartite graph $\tilde{G}_k \subseteq U \times V$, where $U = \{x_0,\ldots,x_{n-1}\}$ and $V = \{y_0,\ldots,y_{n-1}\}$. Let $\mathrm{CONV}_n^+$ denote the function with output $(f_{G_0^+},\ldots,f_{G_{2n-2}^+})$. It is known that the monotone complexity of the $n$-point Boolean convolution is $\Omega(n^{1.5})$ [25] and that its (general) circuit complexity is $O(n\log^2 n\log\log n)$ [24, p.168]. These facts imply that $size_{mon}(\mathrm{CONV}_n) = \Omega(n^{1.5})$ whereas $size_{mon}(\mathrm{CONV}_n^+) = O(size(\mathrm{CONV}_n^+)) + O(n) = O(size(\mathrm{CONV}_n)) + O(n) = O(n\log^2 n\log\log n)$.

# 5 Concluding Remarks

We have shown several results on the conjunctive complexity and the monotone circuit complexity of quadratic Boolean functions. There are many interesting open problems suggested by our work, some of which are described herein. Is there a single output quadratic function whose monotone complexity is strictly smaller than its single level complexity? If such a function exists, what is the largest gap between these complexities? Can we find a characterization of graphs that does not have a linear size $d$-layer circuit when $d \geq 2$?

Note Added: After the submission of this paper, Jukna [12] showed that there are single output quadratic functions whose monotone complexity is $O(n)$ and their single level complexity is $\Omega(n^{2-\epsilon})$. This solves the first of three problems addressed above.

**Acknowledgments**

The authors would like to thank anonymous referees for their remarks. We would also like to thank anonymous reviewers of the conference ISAAC 2004 for their helpful suggestions which helped in improving the quality of this paper.

# References

[1] N. Alon, Eigenvalues, Geometric Expanders, Sorting in Rounds, and Ramsey Theory, *Combinatorica* **6** (1986), 207–219

[2] N. Alon and R. Boppana, The Monotone Circuit Complexity of Boolean Functions, *Combinatorica* **7(1)** (1987), 1–22

[3] A. Andreev, On a Method for Obtaining Lower Bounds for the Complexity of Individual Monotone Functions, *Soviet Math. Dokl.* **31(3)** (1985), 530–534

[4] K. Amano and A. Maruoka, The Potential of the Approximation Method, *SIAM J. Comput.* **33(2)** (2004), 433–447. (Preliminary version in : *Proc. of 37th FOCS* (1996) 431–440)

[5] L. Babai, A. Gál, J. Kollár, L. Rónyai, T. Szabó and A. Wigderson, Extremal Bipartite Graphs and Superpolynomial Lower Bounds for Monotone Span Programs, *Proc of 28th STOC* (1996), 603–611.

[6] C. Berg, S. Ulfberg, Symmetric Approximation Arguments for Monotone Lower Bounds Without Sunflowers, *Computational Complexity* **8(1)** (1999), 1–20.

[7] P.E. Dunne, The Complexity of Boolean Networks, Academic Press, San Diego, CA, 1988.

[8] A. Haken, Counting Bottlenecks to Show Monotone P≠NP, *Proc. of 36th FOCS* (1995), 36–40.

[9] D. Harnik, R. Raz, Higher Lower Bounds for Monotone Size, *Proc. of 32nd STOC* (2000), 191–201.

[10] S. Jukna, Combinatorics of Monotone Computations, *Combinatorica* **19(1)** (1999), 65–85.

[11] S. Jukna, On Graph Complexity, *Electronic Colloquium on Computational Complexity*, ECCC TR04-004 (2004) (Journal version to appear in : *Combinatorics, Probability and Computing*)

[12] S. Jukna, Disproving the Single Level Conjecture, *Electronic Colloquium on Computational Complexity*, ECCC TR05-021 (2005)

[13] K. Lenz and I. Wegener, The Conjunctive Complexity of Quadratic Boolean Functions, *Theoret. Comput. Sci.* **81** (1991), 257–268.

[14] S.V. Lokam, Graph Complexity and Slice Functions, *Theory Comput. Syst.* **36** (2003), 71–88.

[15] K. Mehlhorn, Some Remarks on Boolean Sums, *Acta Inf.* **12** (1979), 371–375.

[16] P. Pudlák, V.Rődl and P.Savický, Graph Complexity, *Acta Inf.* **25** (1988), 515–535.

[17] A. Razborov, Lower Bounds on the Monotone Complexity of Some Boolean Function, *Soviet Math. Dokl.* **31** (1985), 354–357.

[18] A. Razborov, On the Method of Approximation, *Proc. 21th STOC* (1989), 167–176.

[19] A. Razborov, S. Rudich, Natural Proofs, *J. Comput. Syst. Sci.* **55(1)** (1997), 24–35.

[20] J. Simon and S.C. Tsai, On the Bottleneck Counting Argument, *Theoret. Comput. Sci.* **237(1-2)** (2000), 429–437.

[21] R. Tarjan, Complexity of Monotone Networks for Computing Conjunctions, *Ann. Disc. Math.* **2** (1978), 121–133.

[22] Z. Tuza, Covering of Graphs by Complete Bipartite Subgraphs, Complexity of 0-1 Martix, *Combinatorica* **4** (1984), 111–116.

[23] I. Wegener, More on the Complexity of Slice Functions, *Theoret. Comput. Sci.* **43** (1986), 201–211.

[24] I. Wegener, The Complexity of Boolean Functions, Wiley-Teubner, Stuttgart, 1987.

[25] J. Weiss, An $\Omega(n^{3/2})$ Lower Bound on the Complexity of Boolean Convolution, *Info. and Cont.* **59** (1983), 84–88.

[26] U. Zwick, On the Number of ANDs versus the Number of ORs in Monotone Boolean Circuits, *Inf. Process. Let.* **59** (1996), 29–30.