数理解析研究所講究録
第 482 巻 1983 年 49-72

EFFECTS OF PRACTICAL ASSUMPTIONS IN AREA COMPLEXITY OF VLSI COMPUTATION

Ken'ichi HAGIHARA ,

Kouichi WADA and

Nobuki TOKURA

Department of Information and Computer Sciences

Faculty of Engineering Science

Osaka University

Toyonaka, Osaka 560

JAPAN

1. Introduction

Brent, Kung and Thompson have presented suitable VLSI models [1, 10], and discussed area-time complexity of various computations such as discrete Fourier transform [10], and multiplication [1]. Following their pioneering works, several researchers have presented additional results [5, 9, 11, 12, 13].

Although the VLSI models by Brent-Kung and Thompson are suitable for analizing VLSI circuits theoretically, their models are not yet sufficiently practical from the viewpoint of the current VLSI technology. Thus, it is important to add new assumptions to their original models so that the modified model may become more suitable for the current technology, and it is also important to obtain better lower bounds on the new model. In this paper, effects of the following assumption on bounds of the area complexity are discussed.

Boundary Layout Assumption : all input/output (I/O) ports of a circuit must be located on its boundary.

The boundary layout assumption is one of the practical assumptions and technologically important. A VLSI circuit is hierarchically composed of several subcircuits called "blocks." These blocks communicate each other by the wires which connect the blocks through their boundaries. In this case, the inputs and the outputs of each block are performed on the boundary. The boundary layout assumption reflects such situation.

It has been shown that the boundary layout assumption affects lower and/or upper bounds of complexity [2, 14, 15]. For example, the area A necessary to embed the complete binary tree with n leaves under the present VLSI model satisfies

$A = \theta(n)$ without the boundary layout assumption, and

$A = \theta(n \cdot \log n)$ with the boundary layout assumption [2].

On of other examples is the area-time complexity AT^{α} for nontrivial n-input m-output functions, such as decoder and encoder. It has been shown that the lower bound on AT^{α} $(\alpha \geq 2)$ for these functions satisfies

$$AT^{\alpha} = \Omega(\max(n,m) \cdot [\max(\log N, \log M)]^{\alpha-1})$$

without the boundary layout assumption, and

$AT^{\alpha} = \Omega(\max(n,m)\cdot\max(\log^{\alpha}N/\log\log N,\ \log^{\alpha}M/\log\log M))$ with the boundary layout assumption [14], where N is the maximum of $N_1,\ldots,N_m$ (N_i $(1 \le i \le m)$ is the number of input variables on which the i-th output variable essentially depends), and where M is the maximum of $M_1,\ldots,M_n$ (M_j $(1 \le j \le n)$ is the number of output variables which essentially depend on the j-th input variable). In this case, the boundary layout assumption can reinforce the lower bound on AT^{α} measure by $\max(\log N/\log\log N,\ \log M/\log\log M)$.

In this paper, lower bounds on area of combinational circuits to perform addition, multiplication, division and sorting are derived on a VLSI model with the boundary layout assumption. In Section 3, a relationship between relative positions of I/O ports of a circuit and the circuit area is shown. By using the result, it is shown that a combinational circuit to compute the addition or the multiplication requires $\Omega(n^2)$ area, if some I/O port locations are specified, where n is the input bit-size. Similar result is shown by Savage [9]. But the result in this paper properly contains his result and is considered to be generalized one.

In Section 4, lower bounds on area of combinational circuits to perform the multiplication, the division or the sorting are derived. It is shown that the combinational circuits to perform these functions require $\Omega(n^2)$ area under the boundary layout assumption. These results are obtained by using the relationship between the I/O port locations and the circuit area shown in Section 3. It should be noted that the lower bound is independent of the I/O port locations and holds for any combinational circuit with the boundary layout assumption. These lower bounds are best possible for the multiplication and the division, and are optimal within a logarithmic factor for the sorting.

2. VLSI model

In this section, a model of VLSI circuits is described and is used as a basis for deriving area bounds.

VLSI model

(A-1) A VLSI circuit is constructed from processing elements (PEs for short) and wire segments. A PE corresponds to a gate, a (1-bit) storage element, an input/output port (I/O port for short). A VLSI circuit is embedded on a closed planar region R.

(A-2) Wires have width of λ (> 0). Separation and length of wires are at least λ. Each PE occupies area of at least λ^2.

(A-3) Wire and PE, or PE and PE cannot overlap each other. At most ν (≥ 2) wires can overlap at any point in the circuit.

(A-4) It takes minimum time $\tau > 0$ to transmit a bit along a wire w, where τ is a constant independent of geometry of a wire. It is assumed that the computation time of PE is included in τ.

(A-5) Each input value is available only once. It implies that if the same input value is required at different times it must be stored within the circuit.

(A-6) The time and location at which input and output values are available are fixed and independent of the contents of the input values.

(A-7) All I/O ports of a circuit C are located on the boundary of R. This assumption is called boundary layout assumption.

This model is essentially the same as the model by Brent and Kung [1] except the nonconvexity of a circuit region (A-1) and the boundary layout assumption (A-7). Although Brent, Kung and others assume the convexity of a circuit region [1, 8], the result in this paper does not require the convexity. The boundary layout is assumed by Chazelle-Monier [3] and Yasuura-Yajima [15].

In this paper, since area complexity of combinational circuits is discussed, all the assumptions in the VLSI model are not needed. The assumptions used in this paper are (A-1), (A-2), (A-3) and (A-7). In what follows, it is assumed that a combinational circuit is embedded on a closed region and satisfies the boundary layout assumption, unless otherwise stated. And through this paper, for a combinational circuit C, let A(C) denote the area of the circuit.

For a VLSI circuit C, let V be the set of PEs in C. Let W be the set of wires connecting PEs in C, and an element of W is represented by <a,b>, where a and b are PEs and data flow from a to b.

The circuit graph corresponding to C (denoted by G(C)) is a directed graph $(G_p(V), G_w(W))$, satisfying the following conditions:

(1) The node in G(C) corresponds to each PE in C. The set of nodes in G(C) is denoted by $G_p(V)$, where G_p is a bijective mapping from the set of PEs to the set of nodes.

(2) The directed edge in G(C) corresponds to each wire connecting PEs in C. The set of directed edges in G(C) is denoted by $G_w(W)$, where G_w is a bijective mapping from the set of wires to the set of directed edges. When a wire <a,b> is in W, the directed edge $<G_p(a), G_p(b)>$ is included in $G_w(W)$, that is, the direction of the edge corresponds to the flow of data in C.

The circuit graph G(C) is used to analyze topological or graph theoretical properties for C.

3. Relationship between Circuit Area and I/O Port Location Restriction

In this section, a lower bound of the area complexity of a combinational circuit is discussed, which is embedded on a closed region and has some I/O port location restrictions.

The situations with I/O port location restriction are often encountered. For example, n input ports (or output ports) corresponding to an n-bit integer are usually located with preserving the bit order (Fig. 1). One of other examples is that the location of an operand X, the location of another operand W and the location of a result Y are separated one another (Fig. 2).

The results in this section insist that such constraints about the order of I/O port location possiblly requires larger area than the complexity of the function itself. For example, a combinational adder circuit of two n-bit integers can be

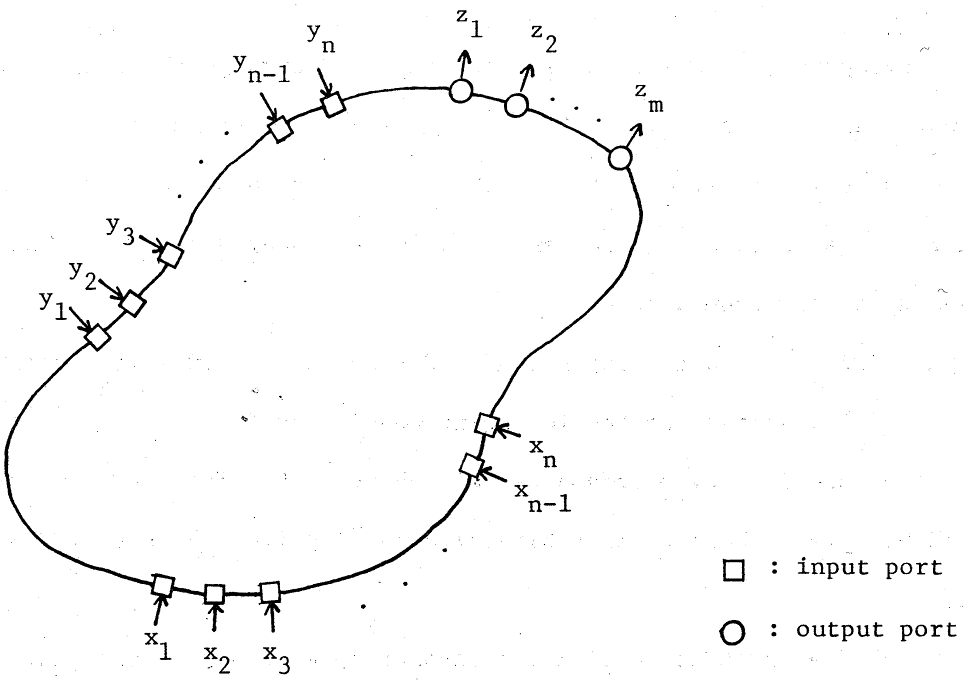


Fig. 1. I/O port locations with preserving the bit order.

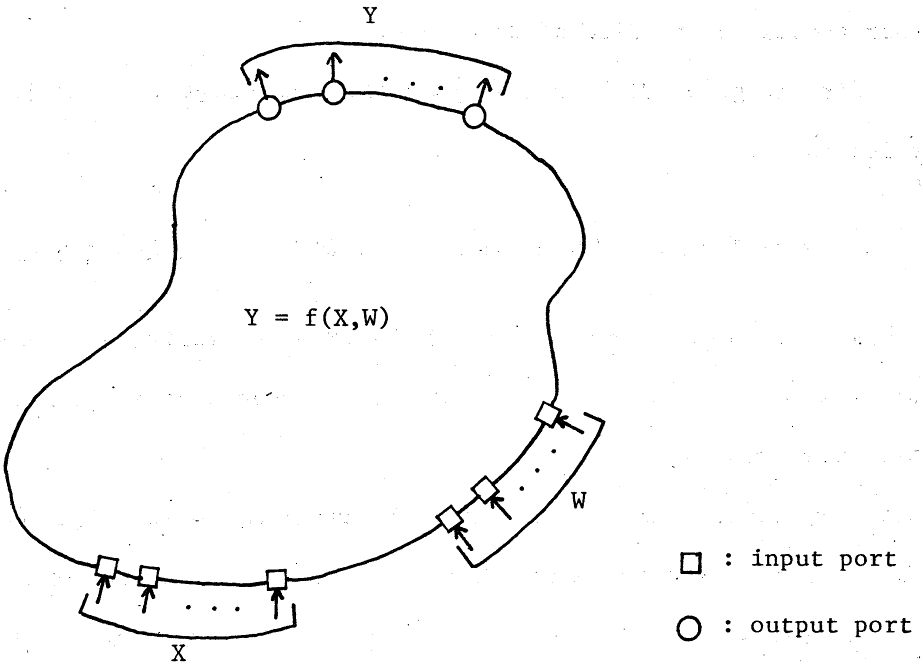


Fig. 2. Separated I/O ports.

constructed with O(n) area by locating input ports of the addend and the augend alternatively on the boundary. However, separated I/O ports as shown in Fig. 2 must require $\Omega(n^2)$ area to perform the addition itself. And it is shown that usual restrictions on the location of I/O ports (e.g., Fig. 1 or Fig. 2) require large area say $\Omega(n^2)$, when the multiplication or the division are computed by combinational circuits.

It should be noted that the result in this paper is based on the following assumption: the amount of information which each logic gate can output is only one bit. That is, a logic gate may have some fanouts, but the values on them are identical.

Definition 1 Let G = (V, E) be a directed graph. A path in the graph is represented by the sequence $v_1,\ldots,v_n$ of the nodes. A pair of paths $p = (v_1,\ldots,v_n)$ and $q = (u_1,\ldots,u_m)$ is called node-disjoint if p and q have no common nodes. A set P of paths is called node-disjoint if each pair of paths in P is node-disjoint.

Let V_1 and V_2 be subsets of the node set V such that $V_1 \cap V_2 = \phi$. A directed path $v_1,\ldots v_n$ is called (V_1, V_2)-connecting, if it has the following properties:

1) $(v_1 \in V_1$ and $v_n \in V_2)$ or $(v_1 \in V_2$ and $v_n \in V_1)$.

2) for each i $(2 \le i \le n-1)$, $v_i \in (V - V_1 - V_2)$. □

The following two lemmas demonstrate the relationship between a restriction of I/O port locations and the circuit area. Let R be a closed region on which a circuit is embedded. The boundary B of R forms a closed curve. A segment of the closed curve is called a contiguous subboundary of B.

Lemma 1 For a combinational circuit C, let G(C) = (V, E) be the circuit graph of C, and let IO denote the set of I/O nodes of G(C). If there exist subsets V_1, V_2 and V_3 of IO which satisfy the following conditions.

1) $V_i \cap V_j = \phi$ $(1 \le i < j \le 3)$.

2) G(C) has a node-disjoint set P_1 of (V_1, V_3)-connecting paths.

3) G(C) has a node-disjoint set P_2 of (V_2, V_3)-connecting paths.

4) $|P_1| = |P_2| = |V_3|$.

5) There exist three contiguous subboundaries B_1, B_2 and B_3 such that

$V_i \subseteq IO_i \quad (i = 1\text{-}3)$,

where IO_i (i=1-3) denotes the set of I/O nodes located on B_i.

Then, it follows that

$$A(C) = \Omega(|V_3|^2).$$

(proof) For the nodes of V_3 on B_3, number the nodes from v_1 to v_k in the order of the location on B_3, where $k = |V_3|$. For each v_i ($1 \le i \le k$), let p_i and q_i be the paths in P_1 and P_2 which have v_i as an endpoint respectively.

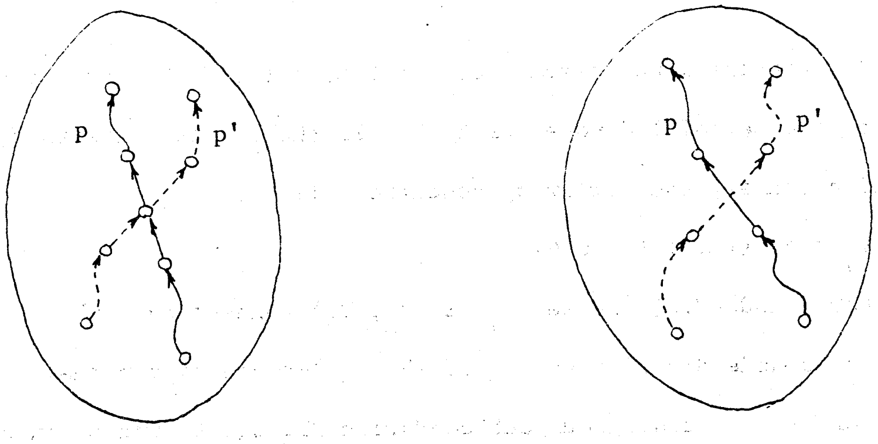
Since the endpoint of q_i, which is not v_i, is located on neither B_1 nor B_3 by the condition 5), each q_i crosses each p_j ($j < i$) on R at least once, or crosses each p_h ($h > i$) on R at least once. Therefore, each q_i must cross at least min(i-1, k-i) paths in P_1 on R. Note that the expression "a path p crosses a path p' " has two meanings. One is that p and p' join at a common node and branch from the node. Another is that an edge in p and an edge in p' cross each other (Fig. 3).

Since a unit of area has at most ν crossing wires, a unit of area has at most $\binom{\nu}{2}$ crossing points. Thus A(C) has at least $(1/\binom{\nu}{2})\cdot\Sigma \min(i-1, k-i)$ units. So we have

$$A(C) \ge (1/\binom{\nu}{2})\cdot\sum_{i=1}^{k}\min(i-1, k-i)$$

$$= \begin{cases} (1/4\cdot\binom{\nu}{2})\cdot k(k-2) & \text{(if k is even)} \\ (1/4\cdot\binom{\nu}{2})\cdot(k-1)^2 & \text{(if k is odd)} \end{cases}$$

$$= \Omega(|V_3|^2). \quad \square$$



crossing with a common vertex

multi-level crossing

Fig. 3 Two kind of crossings.

The next lemma is proved similarly to Lemma 1.

Lemma 2 For a combinational circuit C, let $G(C) = (V, E)$ be the circuit graph of C, and IO denote the set of I/O nodes of G(C). If there exist subsets V_1, V_2, V_3 and V_4 of IO which satisfy the following conditions 1)-4).

1) $V_i \cap V_j = \phi$ $(1 \le i < j \le 4)$.

2) G(C) has a node-disjoint set P_1 of (V_1, V_3)-connecting paths.

3) G(C) has a node-disjoint set P_2 of (V_2, V_4)-connecting paths.

4) There exist four contiguous subboundaries B_1, B_2, B_3 and B_4 in clockwise order such that $V_i \subseteq IO_i$ $(i = 1\text{-}4)$, where IO_i denotes the set of I/O nodes located on B_i.

Then, it follows that

$$A(C) = \Omega(|P_1| \cdot |P_2|). \quad \square$$

Lemma 1 and 2 state a relationship between a circuit graph G(C) and the circuit area A(C). In order to obtain lower bounds on area of combinational circuits which compute a function f by using these lemmas, we examine some properties of the circuit graph for that function.

For a sequence $Z = (z_1, \ldots, z_k)$, a sequence $(z_{i_1}, \ldots, z_{i_j})$, where $1 \le i_1 < \ldots < i_j \le k$, is called a subsequence of Z. For a sequence $Z = (z_1, \ldots, z_k)$, let $\overline{Z}$ denote the set $\{z_1, \ldots, z_k\}$.

Let Z_1 and Z_2 be subsequences of Z. If it holds that $\overline{Z}_1 \cap \overline{Z}_2 = \phi$ and $\overline{Z}_1 \cup \overline{Z}_2 = \overline{Z}$ then Z_2 is denoted by $Z - Z_1$.

Definition 2 Let $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_m)$, and let $Y = f(X)$ be a function. Let $X_1 = (x_{i_1}, \ldots, x_{i_h})$ denote a subsequence of X and let $X - X_1 = (x_{j_1}, \ldots, x_{j_{n-h}})$. Let $Y_1 = (y_{k_1}, \ldots, y_{k_\ell})$ be a subsequence of Y. Let $Q = (q_1, \ldots, q_{n-h}) \in \{0, 1\}^{n-h}$

$Y_1 = h(X_1)$ is a subfunction obtained from f, if it is obtained by assigning q_r to each input variable x_{j_r} of $X - X_1$ for f $(1 \le r \le n-h)$, and by restricting output variables to Y_1 of f. The subfunction h is denoted by $Y|Y_1 = f(X, Q)|X_1$.

A function $(y_1,\ldots y_k) = g(x_1,\ldots,x_k)$ is a k-identity function, if it holds that $y_i = x_{p(i)}$ for each i $(1 \le i \le k)$, where $(p(1),\ldots,p(k))$ is a permutation of $(1,\ldots,k)$. □

Let C be a combinational circuit which computes a function f. In order to combine the function f with the circuit graph G(C), the following proposition and lemmas are needed. In what follows, a combinational circuit which computes f is denoted by C_f, unless otherwise stated.

Proposition 1 (Menger's theorem) [7]

Let G = (V, E) be a directed graph. Let a be a node of G whose indegree is zero, and let b be a node of G whose outdegree is zero.

Let U be a subset of V − {a, b} satisfying the following conditions:

1) Every directed path from a to b goes through a certain node in U,
2) U is minimal; i.e., for every $U' \subsetneq U$, U' does not satisfy 1).

Then, the maximum number of node-disjoint ({a}, {b})-connecting paths is equal to the number of nodes in U. □

In order to use Proposition 1, the following directed graph is constructed from a circuit graph and special nodes a and b.

For a circuit graph G(C) = (V, E), define the directed graph $\hat{G}(C)$ obtained from G(C) to be

$$\hat{G}(C) = (V \cup \{a, b\} , E \cup \{<a,p>|\ p \in I\} \cup \{<q, b>|\ q \in O\}).$$

where $a, b \notin V$, and I and O denote the set of input nodes of G(C) and the set of output nodes of G(C) respectively.

Lemma 3 Let $(y_1,\ldots y_k) = g(x_1,\ldots,x_k)$ be a k-identity function. For the directed graph $\hat{G}(C_g)$ obtained from $G(C_g) = (V, E)$, let U be a subset of V such that every path from a to b goes through a certain node in U. Then,

$$|U| \ge k.$$

(proof) Let $U = \{v_1,\ldots,v_j\}$ and assume $j \leq k-1$. Since C_g is a combinational circuit, the output value of each logic gate corresponding to v_i ($\in U$) is uniquely determined by the input values, and the output values of g are also uniquely determined by the output values of the logic gates corresponding to $v_1,\ldots,v_j$. By the assumption that each logic gate can output only one bit amount of information, the number of possible values of the logic gates corresponding to $v_1,\ldots,v_j$ is at most 2^j ($\leq 2^{k-1}$). On the other hand, since g is a k-identity function, the number of possible output values of g must be equal to 2^k. This implies that C_g cannot compute g correctly. Thus, $|U| \geq k$. □

Let $(y_1,\ldots,y_m) = f(x_1,\ldots,x_n)$ be a function, and let $G(C_f)$ be the circuit graph. Let IO denote the set of I/O nodes of $G(C_f)$. For $G(C_f)$, the I/O node mapping

$$P : \{x_1,\ldots x_n\} \cup \{y_1,\ldots,y_m\} \rightarrow IO$$

is defined as the bijective mapping that indicates which I/O node an input or output variable corresponds to.

The following lemma combines a function f with the circuit graph $G(C_f)$.

Lemma 4 Let f be a function whose subfunction contains a k-identity function $Y = g(X)$. Then, the circuit graph $G(C_f)$ has k node-disjoint (V_1, V_2)-connecting paths, where $V_1 = P(X)$ and $V_2 = P(Y)$.

(proof) Let $\hat{G}(C_f)$ be the directed graph obtained from $G(C_f)$. Since C_f computes a k-identity function, Lemma 3 implies that

$$|U| \geq k$$

for $\hat{G}(C_f)$. Therefore, by Proposition 1 the maximum number of node-disjoint $(\{a\}, \{b\})$-connecting paths in $\hat{G}(C_f)$ is at least k. From the construction of $\hat{G}(C_f)$, $G(C_f)$ must have k node-disjoint $(P(X), P(Y))$-connecting paths. □

By Lemma 1 and 4, the following theorem holds, Theorem 1 Let $Y = f(X)$ be a function. Assume that there exist subsequences X_1 and X_2 of X, and a subsequence Y_1 of Y which satisfy the following condition 1)-3).

1) $\overline{X}_1 \cap \overline{X}_2 = \phi$.

2) There exist assignments Q_1 and Q_2 to $X - X_1$ and $X - X_2$ respectively, such that subfunctions $Y|Y_1 = f(X,Q_1)|X_1$ and $Y|Y_1 = f(X,Q_2)|X_2$ are $|\overline{Y}_1|$-identity functions.

3) There exist two contiguous subboundaries B_1 and B_2 of the boundary of C_f such that

i) $P(\overline{X}_1) \subseteq IO_1$ and $(P(\overline{X}_2) \cup P(\overline{Y}_1)) \cap IO_1 = \phi$,

ii) $P(\overline{Y}_1) \subseteq IO_2$ and $(P(\overline{X}_1) \cup P(\overline{X}_2)) \cap IO_2 = \phi$,

where IO_i $(i = 1, 2)$ denotes the set of all I/O nodes located on B_i.

Then, it holds that

$$A(C_f) = \Omega(|\overline{Y}_1|^2).$$

(proof) By the condition 2) and Lemma 4, the circuit graph $G(C_f)$ has $|\overline{Y}_1|$ node-disjoint $(P(\overline{X}_1), P(\overline{Y}_1))$-connecting paths, and $|\overline{Y}_1|$ node-disjoint $(P(\overline{X}_2), P(\overline{Y}_1))$-connecting paths. And by the condition 1), it holds that

$$P(\overline{X}_1) \cap P(\overline{X}_2) = \phi.$$

Thus, the conditions 1)-4) of Lemma 1 are satisfied. Since the condition 3) satisfies the condition 5) of Lemma 1, we have

$$A(C_f) = \Omega(|Y_1|^2). \square$$

Remark: If the relationship between input variables and output variables of f is exchanged, similar result holds. This is shown by the next theorem.

Theorem 2 Let $Y = f(X)$ be a function. Assume that there exist a subsequence X_1 of X, and subsequences Y_1 and Y_2 of Y which satisfy the following conditions 1)-3).

1) $\overline{Y}_1 \cap \overline{Y}_2 = \phi$.

2) There exist assignments Q_1 and Q_2 to $X - X_1$ such that $Y|Y_1 = f(X,Q_1)|X_1$ and $Y|Y_2 = f(X, Q_2)|X_1$ are $|\overline{X}_1|$-identity functions.

3) There exist two contiguous subboundaries B_1 and B_2 of the boundary of C_f such that

i) $P(\overline{Y}_1) \subseteq IO_1$ and $(P(\overline{X}_1) \cup P(\overline{Y}_2)) \cap IO_1 = \phi$,

ii) $P(\overline{Y}_2) \subseteq IO_2$ and $(P(\overline{X}_1) \cup P(\overline{Y}_1)) \cap IO_2 = \phi$,

where IO_i $(i = 1, 2)$ denotes the set of all I/O ports located on B_i. Then, it holds that

$$A(C_f) = \Omega(|\overline{X}_1|^2). \square$$

From Theorem 1, it can be concluded that combinational circuits which compute the addition, the multiplication, the maximum operation or the minimum operation require $\Omega(n^2)$ area, if the circuits have the separated I/O port locations, where n is the bit-size of the operand. Generally the following corollary can be obtained from Theorem 1.

A binary algebra $[S, \beta]$ is a set S with a binary operation $\beta: S\times S \rightarrow S$. It is assumed that the binary operation β is expressed as

$$(y_1,\dots,y_m) = \beta(x_1,\dots,x_n, w_1,\dots,w_k),$$

where the operands $(x_1,\dots,x_n)$, $(w_1,\dots,w_k)$ and the result $(y_1,\dots,y_m)$ are represented in the same coding system.

Let $n = k$, and $m \geq n$ for the binary operation β. An element $(s_1,\dots,s_n)$ in S is called an identity of β, if it holds that $(a_1,\dots,a_n, 0,\dots,0) = \beta(s_1,\dots,s_n, a_1,\dots,a_n)$ for any element $(a_1,\dots,a_n)$ in S.

Corollary 1 Let $(y_1,\dots,y_m) = f_b(x_1,\dots,x_n, w_1,\dots,w_n)$ be a binary operation which has an identity, where $m \geq n$. If the input ports corresponding to two operands and the output ports corresponding to the result are separated one another, then it follows that

$$A(C_{f_b}) = \Omega(n^2). \square$$

A combinational circuit to compute the addition of two n-bit integers requires $\Omega(n^2)$ area if the input ports of the addend and the augend and the output ports are separated one another. However, there exists a construction of the n-bit addition with O(n) by locating the input ports of the addend and the augend alternatively on the boundary. For the multiplication of two n-bit integers, Theorem 2 implies that even if the input ports of the multiplier and the multiplicand are located alternatively on the boundary, the circuit requires $\Omega(n^2)$ area by locating the output ports corresponding to the result while preserving the bit order. Then, does there exist a combinational circuit to compute the multiplication with smaller area, if some I/O port locations are properly specified? It will be shown in the following section that it is impossible to construct these circuits. That is, if combinational multiplication circuits satisfy the boundary layout assumption, the circuits would require $\Omega(n^2)$ area independent of the I/O port locations. It is also shown that similar results hold for the division and the sorting.

4. A Lower Bound on Area of Combinational Circuits

4.1 Multiplication and Division

Consider the following N-bit shift function with selectors $s_0, \ldots, s_{N-1}$

$(y_1, \ldots, y_N) = f_s(x_1, \ldots, x_N, s_0, \ldots, s_{N-1})$;

i) one and only one s_i is set to 1 among the selectors $s_0, \ldots, s_{N-1}$,

ii) the i-th selector s_i is equal to 1 if and only if

$y_{j+i} = x_j$ for $1 \le j \le N-j$, and

y_j is undefined for $j < i$.

Since the multiplication and the division contain the shift function as a subfunction, obtaining lower bounds for the multiplication and the division is reduced to deriving a lower bound for the shift function. In the following, a lower bound on area of combinational circuits to compute the shift function is considered. In order to derive the lower bound, some definitions are needed.

Definition 3 Let $[k, k'] = \{i \in \mathbb{Z} \mid k \le i \le k'\}$, where $\mathbb{Z}$ is the set of integers. For an integer r and nonnegative integers a and b, let $L_r(a, b)$ denote the set of all the subsets of exactly b elements of $[r+1, r+a]$.

For a subset $p = \{\ell_1, \ldots, \ell_b\}$ of $\mathbb{Z}$, define the i-shift of p, $s_i(p)$ as $s_i(p) = \{\ell_1 + i, \ldots, \ell_b + i\}$. For two subsets $p = \{\ell_1, \ldots, \ell_b\}$ and $q = \{m_1, \ldots, m_b\}$, define the number of meets $m(p, q)$ between p and q to be $m(p, q) = |p \cap q|$, where $|p \cap q|$ denotes the number of elements in $p \cap q$. □

For two elements p and q in $L_r(a, b)$, the following property holds. This property plays an important role for deriving the lower bound of the shift function.

Lemma 5 For any p, q in $L_r(a, b)$, there exists an integer i $(-a \leq i \leq a)$ such that

$$m(p, s_i(q)) \geq \lfloor b^2/2a \rfloor .$$

(proof) For an element ℓ in p and an element m in q, it holds that

$$r + 1 \leq \ell \leq r + a, \text{ and}$$

$$r + 1 \leq m \leq r + a.$$

Since the following inequality is satisfied

$$-(a - 1) \leq \ell - m \leq (a - 1),$$

there exists exactly one integer i $(-(a-1) \leq i \leq a-1)$ such that $\ell = m+i$ for every pair (ℓ, m). Thus,

$$\begin{aligned} \sum_{i=-(a-1)}^{a-1} m(p, s_i(q)) &= \sum_{i=-(a-1)}^{a-1} |p \cap s_i(q)| \\ &= \sum_{i=-(a-1)}^{a-1} \sum_{\ell \in p} \sum_{m \in q} |\{\ell\} \quad \{m+i\}| \\ &= \sum_{\ell \in p} \sum_{m \in q} \sum_{i=-(a-1)}^{a-1} |\{\ell\} \quad \{m+i\}| \\ &= \sum_{\ell \in p} \sum_{m \in q} 1 \quad = b^2 \end{aligned}$$

If Lemma 5 does not hold, for every i $(-a < i < a)$ it follows that

$$m(p, s_i(q)) < \lfloor b^2/2a \rfloor .$$

Therefore, we have

$$\sum_{i=-(a-1)}^{a-1} m(p, s_i(q)) < (2a - 1) \cdot \lfloor b^2/2a \rfloor \leq b^2 .$$

This is a contradiction. □

The following lemma enables us to use the result in preceding section.

Lemma 6 Let $(y_1,\ldots,y_{3N}) = f_s(x_1,\ldots,x_{3N}, s_0,\ldots,s_{3N-1})$ be the 3N-bit shift function. Let X be an arbitrary subsequence of $(x_1,\ldots,x_N)$ and Y be an arbitrary subsequence of $(y_{N+1},\ldots,y_{2N})$ such that $|\overline{X}| = |\overline{Y}| = k \le N$. Then, the shift function f_s contains an ℓ-identity function $Y_1 = f(X_1)$ as a subfunction which satisfies the following conditions.

1) $\overline{X}_1 \subseteq \overline{X}$ and $\overline{Y}_1 \subseteq \overline{Y}$, and
2) $\ell \ge \lfloor k^2/2N \rfloor$.

(proof) Let $p = \{i+N \mid x_i \in \overline{X}\}$ and $q = \{i \mid y_i \in \overline{Y}\}$. By definition, it holds that

$$p,\ q \in L_N(N,\ k).$$

By Lemma 5, we have

$$m(p,\ s_i(q)) \ge \lfloor k^2/2N \rfloor,$$

for an integer i such that $-N \le i \le N$.

By letting $\overline{X}_1 = \{x_{j-N} \mid j \in p \cap s_i(q)\}$ and $\overline{Y}_1 = \{y_j \mid j \in p \cap s_i(q)\}$, we have $m(p,\ s_i(q))$-identity function

$$Y|Y_1 = f_s'(X,\ Q)|X_1,$$

where $Y = f_s'(X)$ is a subfunction of f_s, and where Q is the assignment of $(s_0,\ldots,s_{3N-1})$ such that $s_{N+i} = 1$ and $s_h = 0$ $(h \ne N+i)$. □

The following theorem is a main result in this subsection and is obtained from Lemma 2 and 6.

Theorem 3 Let $(y_1,\ldots,y_{3N}) = f_s(x_1,\ldots,x_{3N}, s_0,\ldots,s_{3N-1})$ be the 3N-bit shift function. Let C be a combinational circuit to compute a function which contains f_s as a subfunction. Then,

$$A(C) = \Omega(N^2).$$

(proof) Consider the subset IO of I/O nodes corresponding to $x_1,\ldots,x_N$ and $y_{N+1},\ldots,y_{2N}$, that is,

$$IO = P(\{x_1,\ldots,x_N\} \cup \{y_{N+1},\ldots,y_{2N}\}).$$

Let $N = 4t + \delta$ $(0 \le \delta \le 3)$. Let B be the boundary of C. Since each node in IO is located on B, we can divide B into two contiguous subboundaries B_1 and B_2 such that each B_i ($i = 1, 2$) contains at least 2t input nodes in IO. And either B_1 or B_2 contains at least 2t output nodes in IO. Without loss of generality, it is assumed that subboundary B_2 contains at least 2t output nodes in IO.

The subboundary B_1 is divided into two contiguous subboundaries D_1 and D_2 such that both D_1 and D_2 contain at least t input nodes in IO, and the subboundary B_2 is also divided into two contiguous subboundaries F_1 and F_2 such that both F_1 and F_2 contain at least t output nodes in IO

Consider the exactly t input nodes in IO located on D_1 and D_2 respectively, and let I_1 and I_2 denote the set of such nodes. And consider the exactly t output nodes in IO located on F_1 and F_2 respectively, and let O_1 and O_2 denote the set of such nodes.

By Lemma 4, 6, there exist ℓ_1 node-disjoint (I_1,O_1)-connecting paths, and ℓ_2 node-disjoint (I_2,O_2)-connecting paths, where $\ell_1, \ell_2 \geq \lfloor t^2/2N \rfloor$ and $t = \lfloor N/4 \rfloor$. Therefore, Lemma 2 implies that, for constant $c > 0$,

$$\begin{aligned} A(C) &\geq c \cdot \ell_1 \cdot \ell_2 \\ &\geq c \cdot (\lfloor 1/2N(\lfloor N/4 \rfloor) \rfloor)^2)^2 \\ &= \Omega(N^2). \quad \square \end{aligned}$$

Remark: The shift function f_s considered here is slightly different from usual one. A usual shift function has an encoded selector, that is, shift by i-bit ($0 \leq i \leq N-1$ is specified by a binary number $a_{\log N} \ldots a_1$. However, Theorem 3 holds for shift functions with selectors of any form.

The n-bit multiplication and the n-bit division contain the shift function f_s as a subfunction. Thus the following corollaries are directly obtained from Theorem 3.

Corollary 2 Let C be a combinational circuit to compute the multiplication of two n-bit integers. Then,

$$A(C) = \Omega(n^2). \quad \square$$

Corollary 3 Let C be a combinational circuit to compute the division of 2n-bit integer by n-bit integer. Then,

$A(C) = \Omega(n^2)$. □

Remark 1: Lower bounds on area of combinational circuits to compute the multiplication and the division have not been known without trivial ones. Although our lower bounds on area of these functions assume the boundary layout, it is considered that the lower bounds are fairly good in the sence that the multiplication and the division are both constructed with $O(n^2)$ area [4].

Remark 2: In the derivation of the lower bound on area for the shift function, the convexity of a circuit region is not assumed. If the convexity is assumed, the same lower bound on area for the shift function (thus, the multiplication and the division) can be proved without the boundary layout assumption. The next theorem is shown by using Lemma 6 and the relationship between the area of convex region and the length of a chord perpendicular to the diameter [1].

Theorem 4 Let $(y_1,\ldots,y_n) = f_s(x_1,\ldots,x_n, s_0,\ldots,s_{n-1})$ be the n-bit shift function. Let C be a combinational circuit to compute a function which contains f_s as a subfunction. Assume that C is embedded on a convex region. Then,

$A(C) = \Omega(n^2)$. □

(proof) Let R be a convex region on which C is embedded. Let D be a diameter of R, and L be a chord perpendicular to D.

Consider the input nodes corresponding to $x_1,\ldots x_N$, and let I denote the set of such input nodes ($I = P(\{x_1,\ldots,x_N\})$). The chord L divides R into two parts R_1 and R_2 such that R_1 contains i input nodes in I, and R_2 contains N-i input nodes in I. We can assume that the input nodes in I are shrunk to infinitesimal size and that L does not intersect any input nodes in I, because the area of the input ports is not used in the proof. By sliding the intersection of L and D along D, we can arrange that both R_1 and R_2 contain at least $\lfloor N/2 \rfloor$ input nodes in I.

Since either R_1 or R_2 contains at least $\lfloor N/2 \rfloor$ output nodes in $P(\{y_{N+1},\ldots,y_{2N}\})$ (denoted by O), without loss of generality, R_2 contains at least $\lfloor N/2 \rfloor$ output nodes in O.

Consider the exactly $\lfloor N/2 \rfloor$ input nodes in I located on R_1, and let I_1 denote such input nodes. Similarly, consider the exactly $\lfloor N/2 \rfloor$ output nodes in O located on R_2, and let O_2 denote such output nodes. By Lemma 4 and 6, there exists ℓ node-disjoint (I_1, O_2)-connecting paths, where $\ell \geq \lfloor \lfloor N/2 \rfloor^2/2N \rfloor$. Then, since ℓ edges cross the chord L, it follows that

$$L \geq \ell \geq \lfloor \lfloor N/2 \rfloor^2/2N \rfloor .$$

By the relationship between A(C) and L [1], it holds that

$$A(C) \geq L^2 \geq \lfloor \lfloor N/2 \rfloor^2/2N \rfloor = \Omega(N^2). \quad \square$$

4.2 Sorting

When a sorting is computed by a combinational circuit, a lower bound on area can be also shown by using the result in the preceding section.

Definition 4 [11] A boolean function $(y_1,\ldots,y_N) = f(x_1,\ldots,x_N, s_1,\ldots,s_b)$ computes a permutation group G, if for each permutation $g \in G$, there exist values for $s_1,\ldots,s_b$ such that $y_i = x_{g(i)}$ $(1 \leq i \leq N)$, where $(g(1),\ldots,g(N))$ denotes the permutation of $(1,\ldots,N)$ by g. $\square$

It has been known that a function to sort a list of n k-bit words $(k \geq \log_2 n)$ contains a boolean function which computes the symmetric group $S_{\lfloor n/2 \rfloor}$ as a subfunction [3]. Whereas, a lower bound on area for the boolean function which computes the symmetric group S_N is considered more generally. The lower bound for the sorting is obtained from the result.

Theorem 5 Let $(y_1,\ldots,y_N) = f(x_1,\ldots,x_N, s_1,\ldots,s_b)$ be a boolean function which computes the symmetric group S_N. Then it follows that

$$A(C_f) = \Omega(N^2).$$

(proof) Let I and O denote the input nodes and the output nodes corresponding to $x_1,\ldots,x_N$ and $y_1,\ldots,y_N$ respectively, that is,

$I = P(\{x_1,\dots,x_N\})$ and $O = P(\{y_1,\dots,y_N\})$.

Let B be the boundary of C_f. Since each node in $I \cup O$ is located on B, we can divide B into three contiguous subboundaries B_1, B_2 and B_3 such that each B_i ($i = 1, 2, 3$) contains at least $\lfloor N/3 \rfloor$ output nodes in O. Then, there exists contiguous subboundary among B_1, B_2 and B_3, on which at least $\lfloor N/3 \rfloor$ input nodes of I are located. Without loss of generality, it is assumed that the subboundary B_1 contains at least $\lfloor N/3 \rfloor$ input nodes in I (Fig. 11).

Consider the exactly $\lfloor N/3 \rfloor$ input nodes in I located on B_1, and the exactly $\lfloor N/3 \rfloor$ output nodes in O located on B_2 and B_3, respectively. Let I_1, O_2 and O_3 denote the sets of such nodes, i.e.,

$$I_1 = P(\{x_{i_1},\dots,x_{i_k}\}),$$
$$O_2 = P(\{y_{j_1},\dots,y_{j_k}\}), \text{ and}$$
$$O_3 = P(\{y_{h_1},\dots,y_{h_k}\}),$$

where $k = \lfloor N/3 \rfloor$ and $I_1 \subseteq I$, O_2, $O_3 \subseteq O$ and $O_2 \cap O_3 = \phi$.

Since the function f computes the symmetric group S_N, there exist permutations $g_1, g_2 \in S_N$ such that $y_{j_p} = x_{g_1(i_p)}$ $(1 \le p \le k)$ and $y_{h_q} = x_{g_2(i_q)}$ $(1 \le q \le k)$. By setting $X_1 = (x_{i_1},\dots,x_{i_k})$, $Y_1 = (y_{j_1},\dots,y_{j_k})$ and $Y_2 = (y_{h_1},\dots,y_{h_k})$, the conditions 1)-3) in Theorem 2 are satisfied and $|\overline{X}_1| = k$ $(= \lfloor N/3 \rfloor)$. Thus, it follows that

$$A(C_f) = \Omega(N^2). \quad \square$$

Corollary 4 Let C be a combinational circuit to sort a list of n k-bit words ($k \ge \log_2 n$). Then

$$A(C) = \Omega(n^2). \quad \square$$

Remark: Sorting a list of n $\log_2 n$-bit words is constructed by a combinational circuit with $O(n^2 \cdot \log n)$ area [6], so the lower bound shown here is optimal within a logarithmic factor.

5. Conclusion

It is important to discuss the area complexity or the area-time complexity on the model more suitable for the current VLSI technology. In this paper, it has been shown that the practical restrictions such as the boundary layout assumption, and the restricted I/O port location assumption, possibly requires larger area than the functional complexity.

A lower bound on area of combinational circuits to compute the multiplication, and the division is little known. It is still open whether or not any combinational circuit to compute the multiplication requires $\Omega(n^2)$ area. However, from the results of this paper, if the combinational circuit is embedded on a convex region, or it satisfies the boundary layout assumption, then the multiplication must have the area complexity quadratic in the bit-size of its input.

References

[1] R.P.Brent and H.T.Kung, "The Chip Complexity of Binary Arithmetic," Proc. 12th Annu. ACM Symp. on Theory of Comput.,ACM, pp.190-200,April 1980.

[2] R.P.Brent and H.T.Kung, "On the Area of Binary Tree Layouts," Information Processing Letters,Vol.11,No.1,pp.46-48,Aug. 1980.

[3] B.Chazelle and L.Monier, "A Model of Computation for VLSI with Related Complexity Results," Dept. of Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, Pa., Tech. Rep. CMU-CS-81-107,Feb. 1981.

[4] I.Deegan, "Concise Cellular Array for Multiplication and Division," Electronics Letters, Vol.7,No.23,Nov. 1971.

[5] R.B.Johnson Jr.,"The Complexity of a VLSI Adder," Information Processing Letters,Vol.11,No.2,pp.92-93,Oct. 1980.

[6] D.E.Knuth, The Art of Computer Programming, Vol.3: Sorting and Searching, Addison-Wesley, Reading, Massachusetts, 1973.

[7] K.Menger, " Zur Allgemeinen Kurventheorie," Fund. Math.,Vol.10,pp.96-115, 1927.

[8] J.E.Savage, "Area-Time Tradeoffs for Matrix Multiplication and Related Problems in VLSI Models," Dept. of Comput. Sci., Brown Univ., Providence, R.I., Tech. Rep. CS-50,Aug. 1979.

[9] J.E.Savage, "Planar Circuit Complexity and the Performance of VLSI Algorithms," INRIA Papports de Recherche,No.77,April 1981.

[10] C.D.Thompson, "A Complexity Theory for VLSI," Dept. of Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, Pa., Tech. Rep. CMU-CS-80-140,Aug. 1980.

[11] J.Vuilemin, "A Combinational Limit to the Computing Power of V.L.S.I. Circuits," IEEE 21st Annu. Symp. on FOCS,pp.294-300,Oct. 1980.

[12] K.Wada, K.Hagihara and N.Tokura, "The Area-Time Complexity of n Variables Logical Functions," Trans. IECE Japan, Vol.J64-D, No.8,pp.676-681,Aug 1981 (in Japanese).

[13] K.Wada, K.Hagihara and N.Tokura, "The Area Complexity on a VLSI Model," Trans. IECE Japan, Vol.J65-D, No.4,pp.478-485,April 1982 (in Japanese).

[14] K.Wada, K.Hagihara and N.Tokura, "Area and Time Complexities of VLSI Computations," Proc. of the 7th IBM Symp. on Math. Foundations of Comput. Sci., Math. Thoeory of Computations, IBM Japan,June 1982.

[15] H.Yasuura and S.Yajima, "On Embedding Problems of Logic Circuits in a VLSI Model," Papers of Tech. Group on Automat. and Lang., AL81-49, IECE Japan, Sept. 1981 (in Japanese).