View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Kyoto University Research Information Repository

KURENAI 紅
Kyoto University Research Information Repository

KYOTO UNIVERSITY

Title	Circuit Complexity of An Explicity Defined First Slice Function
Author(s)	Tsukiji, Tatsuie
Citation	数理解析研究所講究録 (1995), 906: 81-88
Issue Date	1995-04
URL	http://hdl.handle.net/2433/59458
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

数理解析研究所講究録
906 巻 1995 年 81-88

Circuit Complexity of An Explicity Defined First Slice Function

Tatsuie Tsukiji
Dept. of Computer Science
Tokyo Institute of Technology
Meguro-ku Ookayama, Tokyo 152, Japan
Email: tsukiji@cs.titech.ac.jp

Abstract

We construct a family of subset $D_1, \ldots, D_n$ of $\{1, ..., n\}$ such that a first slice funciton defined by these $D_1, \ldots, D_n$ has superlinear lower bounds under some topological restrictions.

1 Introduction

In this paper, we consider the Boolean circuit complexity of a n collection of first slice functions, which we simply call a first slice function, $f = \{f_i\}_{i=1}^n$ with

$$f_i(x_1, ..., x_n) = \left(\bigvee_{j \in F_i} x_j\right) \vee T_2^n(x_1, ..., x_n), \quad F_i \subseteq [n] \qquad (1.1)$$

where $[n] = \{1, \ldots, n\}$. Here, our circuits are at most 2 fan-in of gates in $\{\vee, \wedge, \neg\}$, and the circuit complexity of a Boolean function f, denoted by $C_{\{\vee,\wedge,\neg\}}(f)$, is the minimum number of gates of a circuit computing f.

The main reason and difficulty for the investigation of the circuit complexity of an explicitly defined constant-slice function f is that their complexity are the same both on monotone circuits and on non-monotone circuits (see, e.g., [4]); that is,

$$C_{\{\vee,\wedge\}}(f) = \Theta(C_{\{\vee,\wedge,\neg\}}(f))$$

This relation, generally, does not hold for a *Boolean sum* (e.g., consider the Boolean sum defined by the family of $\binom{n}{2}$ sets $\{F_i \cap F_j\}_{i<j}$, where $\{F_i\}_{i=1}^n$ is the Brown's $(2,2)$-disjoint family [3]). Here, a Boolean sum is defined as (1.1) without T_2^n term, and some explicitly defined Boolean sums have nonlinear lower bounds on monotone circuit complexity (see, e.g., [6]). Every such lower bound of a Boolean sum f has been obtained by concerning the following combinatorial property of a family of sets $\mathbf{F} = \{F_i\}_{i=1}^n$ under f [5, 7] : $\mathbf{F}$ is (s,t)-disjoint iff, for any $I \subseteq [n]$ with $\|I\| = s+1$, $\|\bigcap_{i \in I} F_i\| \leq t$.

We consider the stronger property than (s,t)-disjointness : with the notations $F^0 = \neg F = [n] \setminus F$ and $F^1 = F$, a family of sets $\mathbf{F}$ is called to be strongly (s,t)-disjoint if for all $\mathbf{e} = (e_1, \ldots, e_n) \in \{0,1\}^n$ $\mathbf{F}^{\mathbf{e}} = \{F_i^{e_i}\}_{i=1}^n$ is (s,t)-disjoint. From definition, it is easily seen that $t \geq n/2^s$, if some $\mathbf{F}$ is strongly (s,t)-disjoint with $1 < s < \log n$.

On the other hand, we can show that a certain constructible family of sets **CSQ** do realize an optimal strong disjointness for $s = \Theta(\log n)$ without constant factor (see below). For any odd prime p, **CSQ** $= \{CSQ_i\}_{i=1}^{p}$ is defined to be a family of cyclic shifts of the quadratic numbers modulo p, namely, $CSQ_i = \{\, j^2 - i \bmod p \,:\, j \in [p] \,\}$. Roughly speaking, we can show its strong disjointness as follows. For any $S \subseteq [p]$ with $\|S\| = s \leq \sqrt{p}$ and any $\mathbf{e} \in \{0,1\}^p$, $2^s \cdot \| \bigcap_{i \in S} \mathbf{CSQ}^{e_i} \|$ is bounded from above by the number of rational points of a certain algebraic curve of a small genus over the finite field $\mathbf{F}_p$ (of order p), and this number is approximated by Weil's bound. In this way, we can prove the following theorem.

Theorem 1.1. For any $s \leq \log p/4$, **CSQ** is strongly $(s, (5/4)(p/2^s))$-disjoint.

Next, let us turn to investigate combinatorial methods for obtaining lower bounds on circuit complexity of the first slice function f_{csq} defined by **CSQ**. For computing first slice functions, a combinatorially more tractable model of circuits, called set circuits, has introduced by Wegener [9] : A set circuit over $[n]$ (with n outputs) computes a family $\mathbf{F} = \{F_i\}_{i=1}^{n}$ of subsets of $[n]$; it is at most two fan-in, having gates in $\{\cup, \cap, \neg\}$, and inputs in $\{\{1\}, \ldots, \{n\}\}$. Thus, a set circuit is more static than a usual one in the sense that it does not have variables, hence niether assignments. It naturally computes a subset of $[n]$ at each gate, starting from one element sets. The complexity, i.e., the minimum number of required gates, on this model for computing $\mathbf{F}$ is denoted by $SC_{\{\cup,\cap,\neg\}}(\mathbf{F})$, and when $\mathbf{F}$ defines a first slice function f, we have

$$SC_{\{\cup,\cap,\neg\}}(\mathbf{F}) \;=\; C_{\{\vee,\wedge,\neg\}}(f) + \Theta(n) \;=\; \Theta(SC_{\{\cup,\cap\}}(\mathbf{F})) \;=\; \Theta(C_{\{\vee,\wedge\}}(f)).$$

The reason we do not remove $\neg$-gates in our model (even though it is possible from the above relation) is that we would like to consider the restriction on geometrical structure of circuits, rather than restricting gate types.

For making natural restrictions on topology of circuits, we define some natural messures on the structure of circuits. Let C be any set circuit and let g be any gate in C with child nodes g_1 and g_2 (let $g_1 = g_2$ if g has only one child node). Let us denote the set computed at g by $set(g)$. We first consider the following three amounts at g :

(1.a)

$$dec(g) \;=\; \min\{\, \|set(g)\| - \|set(g_1)\| \;,\; \|set(g)\| - \|set(g_2)\| \,\}.$$

(1.b)

$$overlap(g) \;=\; \begin{cases} \min\left\{\, \|set(g_1) \cap set(g_2)\| \;,\; \|\overline{set(g_1)} \cap \overline{set(g_2)}\| \,\right\} & \text{if } g \text{ is in } \{\cup, \cap\}, \\ 0 & \text{if } g = \neg. \end{cases}$$

Thus, $overlap(g) = \|set(g_1) \cap set(g_2)\|$ if $g = \cup$, and $= \|set(\neg g_1) \cap set(\neg g_2)\|$ if $g = \cap$.

(1.c) $alt(g)$ is the maximum number of alternations of gate types on any path from an input to g.

The amounts $dec(g)$, $overlap(g)$ and $alt(g)$ are called *decrement*, *overpapping-volume*, *alternating-size*, respectively, at g. Then, the *decrement of* C (written as $dec(C)$), is defined to be the maximum of $dec(g)$ of all gate g in C, and similar definitions are given for $overlap(C)$ and $alt(C)$.
From definition, if we added one extra gate g with decrement $> dec(C)$, then the decrement of C would increase to be eqal to $dec(g)$. In order to avoid this phenomenon and make the restriction on dec more robust, we consider a new mesure dec^* on C: $dec^*(C)$ of a set circuit C is the minimum natural number k such that $dec(g) \leq k$ for all gates g but k exceptions in C. $overlap^*(C)$ is similarly defined. Finally, $size(C)$ is defined to be the number of gates in C.
We first consider to restrict decrement. For example, consider any circuit C with 0 decrement. Then it is easy to show that all $\cup$-gates are meaningless; that is, they can be removed from the circuit without changing its output. Also, an occurrence of $\neg$-gates can be restricted only at output nodes. Hence, computing **CSQ** (i.e., f_{csq}), restricting the decrement $= 0$ requires $\Omega(n^{1.25/(\log n)^2})$ size [5]. We can relax the bound of decrement without losing nontrivial lower bound.

Theorem 1.2. Let C be any circuit computing **CSQ** such that $dec^*(C) = o(n/(\log n)^3)$. Then $size(C) = \omega(n)$.

The proof is a simple modification of the known method for obtaining monotone lower bounds of Boolean sums, and here we omit the proof of Theorem 1.2.

Next, we bound both overlapping-volume and alternating-depth. In fact, we first prepare a technical lemma for obtaining a lower bound on the union size of sets of sets, and then apply the lemma to obtain the following theorem.

Theorem 1.3. Let C be any circuit computing **CSQ** such that $alt(C) = O(1)$ and $overlap^*(C) = o(n)$. Then $size(C) = \omega(n)$.

We can prove a similar result for the unbounded alternation depth (see Section 3 for the detail).
The paper is organized as follows. In Section 2, the general technical lemma mentioned above is prepared, and in section 3, Theorem 1.3 and related results are proved.

2 Discrepancies

In this section, we develop some combinatorial methods for obtaining lower bounds on the union size of sets of sets. Our method uses the following value defined for any two sets A, B, called the *discrepancy* of A on B:

$$disc\ (A, B) = |\ \|A \cap B\| \ - \ \|A \cap \neg B\|\ |.$$

In addition, for a set $A \subseteq [n]$, we define $vol(A) = \min\ \{\|A\|\ ,\ \|\neg A\|\}$, and call it the *volume* of A.

The following properties with respect to these two measures for sets are easily checked : For any $A, A_1, A_2, B \subseteq [n]$,

(2.a): if $A = A_1 g A_2$ with $g \in \{\cup, \cap\}$, $disc(A, B) \leq disc(A_1, B) + disc(A_2, B) + overlap(g)$.

(2.b): $vol(A) = vol(\neg A)$, and furthermore, if $\|B\| = n/2$, then $disc(A, B) = disc(\neg A, B)$.

(2.c): $disc(A, B) \leq vol(A)$.

Given a set $A \subseteq [n]$, and we first consider the discrepancies of A on sets in the following family $\mathbf{F}$: for sufficiently large $s \leq \log n$, and a constant $c_1 \geq 1$, $\mathbf{F} = (F_1, \ldots, F_s)$ is a strong $(s, c_1 n/2^s)$-disjoint family of halves of $[n]$. Since $F_1, \ldots, F_s$ are well separated, it seems impossible to make $disc_i(A) := disc(A, F_i)$ large for all F_i. In fact, the following lemma can be proved.

Lemma 2.1. Let $\overline{disc}(A) = (1/s) \cdot \sum_{i=1}^{s} disc_i(A)$. Then, for any constant c_2 with $2 < c_2 < 6$ and sufficiently large s, either $100(vol(A)/\overline{disc}(A))^{c_2}$ or $(2\ln(n/\overline{disc}(A)))^{c_2/(c_2-2)}$ is greater than s.

Proof of Lemma 2.1. By the property (2.b) of vol and $disc$, we may assume, without loss of generality, that $vol(A) = \|A\|$ and $disc(A) = \|A \cap F_i\| - \|A \cap \neg F_i\|$ for all F_i. We then have

$$\begin{aligned}
\textstyle\sum_{i=1}^{s} disc_i(A) &= \textstyle\sum_{j \in A} (\| \{i : j \in F_i\} \| - \| \{i : j \notin F_i\} \|) \\
&= \textstyle\sum_{\mathbf{e} \in \{0,1\}^s} (\# \text{ of 1's in } \mathbf{e} - \# \text{ of 0's in } \mathbf{e}) \cdot \|A \cap (\bigcap \mathbf{F}^{\mathbf{e}})\|, \quad \textit{and} \\
\|A\| &= \textstyle\sum_{\mathbf{e} \in \{0,1\}^s} \|A \cap (\bigcap \mathbf{F}^{\mathbf{e}})\|,
\end{aligned}$$

where $\bigcap \mathbf{F}^{\mathbf{e}} = \bigcap_{i=1}^{s} F_i^{e_i}$. The last summantion part in the first equality becomes largest when $\|A \cap (\bigcap \mathbf{F}^{\mathbf{e}})\|$ for $\mathbf{e} \in \{0,1\}^s$ are as much large as possible in propotion as # of 1's in $\mathbf{e}$ are large. Set $t = c_1 n/2^s$ for brevity. From the (s,t)-disjointness of $\mathbf{F}$, we have $\|A \cap (\bigcap \mathbf{F}^{\mathbf{e}})\| \leq t$. Thus, the extremal case on the above two equalities derives

$$\sum_{i=1}^{s} disc_i(A) \leq \sum_{i=0}^{k} (s - 2i) \binom{s}{i} \cdot t = t(s-k) \binom{s}{k},$$

where k ($\leq s/2$) is the integer such that

$$\sum_{i=0}^{k-1} t \cdot \binom{s}{i} < \|A\| \leq \sum_{i=0}^{k} t \cdot \binom{s}{i}.$$

Hence, by putting $v = vol(A)$ and $d = 1/s \cdot \sum_{i=1}^{s} disc_i(A)$

$$d < t\binom{s}{k} \quad \text{and} \quad \sum_{i=0}^{k-1} t \cdot \binom{s}{i} < v \leq \sum_{i=0}^{k} t \cdot \binom{s}{i}.$$

Since $t = c_1 n/2^s$, they can be seen as the following inequalities on the binomial distribution.

$$\frac{d}{c_1 n} < \binom{s}{k} \cdot 2^{-s} \quad \text{and} \quad \sum_{i=0}^{k-1} \binom{s}{i} \cdot 2^{-s} < \frac{v}{c_1 n} \leq \sum_{i=0}^{k} \binom{s}{i} \cdot 2^{-s}.$$

Let $x = (s - 2k)/\sqrt{s}$, the normalization of $s - k$ ($\geq s/2$) with mean $s/2$ and variance $s/4$. The following inequalities can be derived by using the Starling's formula and some known inequality on the standard distribution function (see [2]): For any constant $c_3 > 1$ and sufficiently large s,

$$\binom{s}{k} \cdot 2^{-s} < c_3 \sqrt{\frac{2}{\pi s}} \cdot e^{-\frac{x^2}{2}} \quad \text{and} \quad \frac{e^{-\frac{x^2}{2} - \frac{x^3}{s}}}{c_3 (x+1)\sqrt{2\pi}} < \sum_{i=0}^{k-1} \binom{s}{i} \cdot 2^{-s}.$$

Plugging these inequalities to the aboves, we obtain

$$\frac{\sqrt{s}e^{-x^3/s}}{2c_3^2(x+1)} < \frac{v}{d} \text{ and } \frac{d}{c_1 n} < c_3 \cdot \sqrt{\frac{2}{\pi s}} \cdot e^{-x^2/2}.$$

Choose a constant c_4 with $0 < c_4 < 1/3$, and take s sufficiently large. If $x \leq s^{c_4}$, then the first inequality derives $x < 100(v/d)^{2/(1-2c_4)}$; Otherwise, $x > s^{c_4}$, and the second one derives $s < (2\ln(n/d))^{1/(2c_4)}$. Finally by changing the parameter c_4 to $c_2 = \frac{2}{1-2c_4}$, we have the required inequality. □ Lemma 2.1

This lemma can be applied to derive lower bounds on the union size of sets of sets. Here we increase number of sets in $\mathbf{F}$ to m ($\geq s$) and consider a family $\mathbf{F} = \{F_i\}_{i=1}^m$ such that all F_i are halves of $[n]$ and, for any $s \leq s_0$ ($= s_0(n) \leq \log n$), $\mathbf{F}$ is strongly $(s, c_1 n/2^s)$-disjoint. Then we can prove the following lemma.

Lemma 2.2. Fix c_2 in $2 < c_2 < 6$. Suppose we are given $\mathcal{A} = \{\mathbf{A}_1, \ldots, \mathbf{A}_m\}$, $\mathbf{A}_i \subseteq \mathcal{P}([n])$, a family of sets of sets in $[n]$. For any A in $\bigcup \mathcal{A} = \bigcup_{i=1}^m \mathbf{A}_i$, let $\overline{disc}(A)$ = the average of $disc(A, F_i)$ for all i with $A \in \mathbf{A}_i$, and let $\rho(A) = \max\{\, 100(vol(A)/\overline{disc}(A))^{c_2}, (2\ln(n/\overline{disc}(A))^{(c_2/(c_2-2))}\,\}$. Then, if $\rho(A) \leq s_0$ for any $A \in \bigcup \mathcal{A}$ then $\|\bigcup \mathcal{A}\| > \sum_{i=1}^m \sum_{A \in \mathbf{A}_i} 1/\rho(A)$.

Proof of Lemma 2.2. For $A \subseteq [n]$, let $I(A)$ be the set of indices such that $A \in \mathbf{A}_i$. Then, obviously, $\|\bigcup \mathcal{A}\| = \sum_{i=1}^m \sum_{A \in \mathbf{A}_i} 1/\|I(A)\|$. It is thus sufficient to show that $\|I(A)\| < \rho(A)$ for any A in some $\mathbf{A}_i$. Let us fix one such A. In case $\|I(A)\| \leq s_0$, Lemma 2.1 can be applied to A and $\{F_i\}_{i \in I(A)}$, since the latter is strongly $(\|I(A)\|, c_1 n/2^{\|I(A)\|})$-disjoint, deriving $\|I(A)\| < \rho(A)$. Otherwise, we have $\|I(A)\| > s_0$, and in this case a contradiction is derived as follows. We can take a subset $I \subseteq I(A)$ with $\|I\| = s_0$ such that $\overline{disc}'(A)$, the average of $disc_i(A)$ over $i \in I$, is $\geq \overline{disc}(A)$. Let $\rho'(A)$ be defined similarly as $\rho(A)$ by using $\overline{disc}'(A)$. Then, applying the Lemma to $(F_i)_{i \in I}$ derives $s_0 < \rho'(A) \leq \rho(A)$, which conflicts the assumption that $s_0 \geq \rho(A)$. □ Lemma 2.2

3 Small Overlapping-Volume and Small Alternating-Depth Circuits

In this section, we apply the method developed in Section 2 to obtain lower bounds on set circuit size of strongly disjoint family, e.g. **CSQ**, by restricting both alternating-depth and overlapping-volume. We are give a strongly disjoint family $\mathbf{F} = \{F_1, \ldots, F_n\}$ as before in Section 2 (with $m = n$). Let C be a set circuit computing $\mathbf{F}$.

Lemma 3.1. Let k and l be any natural numbers such that $4^{l+10} \leq \log(\min\{s_0, n/k\})$. Then, for any a with $4^{l+5} \leq \log a \leq \log(\min\{s_0, n/k\})/4^{l+5}$, we have $size(C) > a^2 n$, if $overlap^*(C) \leq k$ and $alt(C) \leq l$.

Proof. It is sufficient to show that $size^*(C) \leq (a^2+1)n$, under the assumption that $overlap(C) \leq k$ and $alt(C) \leq l$, where $size^*(C)$ is the number of gates g in C with $\|set(g)\| > k$. We would like to apply Lemma 2.2 by finding a family of sets of gates $\{\mathcal{A}_i\}_{i=1}^n$, such that, for any g in some $\mathcal{A}_i$, $\rho(g) := \rho(set(g))$ (defined in Lemma 2.2) is small, implying $disc_i(g)$ would be large.

We will find the desired $\mathcal{A}_i$ in the following steps. First, for some appropriate $l+2$ parameters r_j with $1/2 = r_0 > r_1 > r_2 > \cdots > r_{l+1} > 0$, let us define a maximal sequence of gates $g_{i,0}, \ldots, g_{i,l(i)}$ such that

(i): $g_{i,0} = F_i$, the i-th output of C (thus, $disc_i(g_{i,0}) = nr_0$),

and for any $j > 0$,

(ii): $disc_i(g_{i,j}) \geq nr_j$,

(iii): $g_{i,j}$ is not a $\neg$-gate, and there is a path from $g_{i,j}$ to $g_{i,j-1}$ through some (possibly 0) of only $\neg$-gates at first and after then only the same type of gates as $g_{i,j-1}$, until reaching to $g_{i,j-1}$.

Let us fix i, and set $r = r_{l_i}$ and $r' = r_{l_i+1}$ for brevity. Now we define $\mathcal{T}_i$ to be the maximal subcircuit under $g_i := g_{i,l_i}$ such that any gate $g \in \mathcal{T}_i$ has the same type with g_i and $disc_i(g) \geq nr'$. Because of the maximality of l_i, $\mathcal{T}_i$ consists of a single type of gates, either $\cup$ or $\cap$. From definition, $disc_i(g)$ is large, i.e., (3.1) : $disc_i(g) \geq r'$ for any $g \in \mathcal{T}_i$, hence Lemma 2.2 would derive a good lower bound on the size of $\bigcup_{i=1}^n \mathcal{T}_i$ (we sometimes see $\mathcal{T}_i$ as the set of gates), if $\|\mathcal{T}_i\|$ is large for many i, e.g., for at least $n/2$ of $i \in [n]$. Therefore, we define $\mathcal{A}_i = \mathcal{T}_i$ for any $i \in I = \{i \ : \ \|\mathcal{T}_i\| \geq 1/r'^3\}$. From definition, (3.2) : $\|\mathcal{A}_i\| \geq 1/r'^3$ for $i \in I$.
However, in case $\|I\|$ is small, $\|\bigcup_{i \in I} \mathcal{A}_i\|$ would be small, and in this case, we count $\mathcal{L}_i$, the set of the leaves of $\mathcal{T}_i$ (it will be shown later that $\mathcal{T}_i$ is in fact a tree). More explicitly, let $\mathcal{L}_i$ be the set of edges whose top ends are in $\mathcal{T}_i$, and the bottom ends are not. *disc* and *vol* of an edge e in C are defined to be those of the bottom-end node of e, respectively. Notice that, since C is at most 2 fan-in, if we find, say, N edges in C, C should contain at least $N/2$ gates. However, $\mathcal{L}_i$ is not enough as defined to be $\mathcal{A}_i$, since $disc_i(e)$ of $e \in \mathcal{L}_i$ might be very small. Thus, by preparing further l appropriate parameters q_j (> 0), $0 \leq j \leq l$, we define subsets $\mathcal{L}'_i$ of $\mathcal{L}_i$ to be $\{e \in \mathcal{L}_i \ : \ disc_i(e) \geq nq\}$ with $q = q_{l_i}$, and define $\mathcal{A}_i = \mathcal{L}'_i$ for $i \notin I$. Notice that (3.3) : $nq \leq disc_i(e) < nr'$ for any $e \in \mathcal{L}'_i$.

Next, we determine the parameters $r_1, \ldots, r_{l+1}$ and $q_0, \ldots, q_l$. First of all, choose any real a satisfying the asserted conditions, and also take any ε with $10 \ln\ln a / \ln a < \varepsilon < 1/10$ (such an ε does exists, since a is fairly large, namely $\geq 2^{4^{l+5}} \geq 2^{2^{10}}$), and fix them. Notice that, from our choice, (3.4) : $\log a \geq 4^{l+5}$, (3.5) : $a^{2^{2l+10}} \leq s_0$, (3.6) : $a^{2^{2l+10}} \leq n/k$, and (3.7) : $a > (\ln a)^{10/\varepsilon}$.
In the discussion we will require the following inequalities to hold : For all considerable i,

$$(P) : 10nr_i \geq k. \quad (Q) : 10nq_i \geq k. \quad (R) : s_0 r_i^{2+\varepsilon} \geq 100. \quad (S) : \ln r_i \geq -(\ln a)^2.$$
$$(T) : r_{i+1} \leq r_1. \quad (U) : a^{2-4\varepsilon} - 1 \geq 200(l+1)(2\ln a)^{2(2+\varepsilon)^2/\varepsilon}. \quad (V) : r_i r_{i+1}^3 \geq 10q_i.$$
$$(W) : s_0 q_i^{2+\varepsilon} \geq 100. \quad (X) : \ln q_i \geq -(\ln a)^2.$$
$$(Y) : r_i^{3+\varepsilon}/r_{i+1} \geq r_1^{3+\varepsilon}/r_2. \quad (Z) : a^{2-4\varepsilon} - 1 \geq 10^4(l+1)(2\ln a)^{2(2+\varepsilon)^2/\varepsilon}.$$

These inequalities are all satisfied, if we set, for example, $r_i = a^{-4^i}$ and $q_i = r_i r_{i+1}^3/10$, in virtue of (3.4)–(3.7).

Now we return to show that our setting is sufficient to derive $size^*(C) \geq (a^2+1)n$. Notice that, any gate g in $\mathcal{T}_i$ has $\|set(g)\| > k$ by (3.1) and (P), hence counted on the measure $size^*$, and similar with any edge in $\mathcal{L}_i$ in virtue of (3.3) and (Q).

First of all, we claim that $\mathcal{T}_i$ is a tree. Suppose otherwise. Then, there must be an (indirected) loop in $\mathcal{T}_i$, or more explicitly, two gates g and g' in $\mathcal{T}_i$, so that g' has two paths to g such that they get into g through different child nodes of g, implying $set(g') \subseteq set(g)$ if the gate type of T is $\cup$, and $\neg set(g') \subseteq \neg set(g)$ if it is $\cap$. In either case, we have $vol(g) \leq overlap(g) \leq k$. On the other hand, by (3.c), $vol(g) \geq disc_i(g) > k$, conflicting the last inequality.

Thus, in special, (3.8) : $\|\mathcal{L}_i\| = \|\mathcal{T}_i\| + 1$. Now, as mentioned when we defined $\mathcal{A}_i$, we apply Lemma 2.2 by dividing into the following two cases.

<u>Case : $\|I\| \geq n/2$</u> l_i changes in the range from 0 to l depending on $i \in I$, and in order to fix it, we further take a subset I_1 of I with the maximum cardinality such that all l_i is equal to some constant l_c for any $i \in I_1$. Clearly, $\|I_1\| \geq n/2(l+1)$. Let us set $r = r_{l_c}$, $r' = r_{l_c+1}$ and $q = q_{l_c}$.

We would like to apply Lemma 2.2 to $\{\mathcal{A}_i\}_{i \in I_1}$ and $(F_i)_{i \in I_1}$ with $c_2 = 2 + \varepsilon$, and for which it is sufficient to show that $\rho(g)$, the maximum of $\phi(g)$ and $\psi(g)$, is at most s_0 for any $g \in A := \bigcup_{i \in I_1} \mathcal{A}_i$, where we set $\phi(g) := 100(vol(g)/\overline{disc}(g))^{(2+\varepsilon)}$ and $\psi(g) := (\ln(n/\overline{disc}(g)))^{(2+\varepsilon)/\varepsilon}$. Notice that, here, the average $\overline{disc}(g)$ of $disc_i(g)$ ranges over all those $i \in I_1$ with $g \in \mathcal{A}_i$. Fix any $g \in A$. By (3.1) and $vol(g) \leq n$, $\phi(g) \leq M := 100r'^{-2-\varepsilon}$, and hence $< s_0$ by (R). Similarly, we can prove that $\psi(g) \leq N := (2 \ln a)^{2(2+\varepsilon)/\varepsilon} < s_0$ by (3.1),(S),(3.5) and (3.7).

Now, Lemma 2.2 derives $\|A\| > \sum_{i \in I_1} \sum_{g \in \mathcal{A}_i} 1/\rho(g)$, and since $\rho(g) \leq MN$ for any $g \in A$, we have $\|A\| > \sum_{i \in I_1} \|\mathcal{T}_i\|/MN$, hence by (3.2) and the definition of M, $\|A\| > nr'^{\varepsilon-1}/(10(l+1)N)$. Finally, by (T) and (U), we obtain $\|A\| > (a^2+1)n$, as required.

<u>Case : $\|I\| < n/2$</u> Fix $i \notin I$, and let $r = r_{l_i}$, $r' = r_{l_i+1}$ and $q = q_{l_i}$ within this and the next paragraphs. In this case we do not have a lower bound of $\|\mathcal{A}_i\|$. However, we can see that (3.9) : $\sum_{e \in \mathcal{A}_i} disc_i(e) > nr/2$, if we could show that $\|\mathcal{T}_i\| < 1/r'^3$ implies (3.9). We prove the contraposition of this. Suppose $\sum_{e \in \mathcal{L}'_i} disc_i(e) \leq nr/2$. Then we have $\sum_{e \in \mathcal{L}_i} disc_i(e) = \sum_{e \in \mathcal{L}'_i} disc_i(e) + \sum_{e \in \mathcal{L}_i - \mathcal{L}'_i} disc_i(e) \leq nr/2 + nq_i\|\mathcal{L}_i - \mathcal{L}'_i\|$. On the other hand, since $\mathcal{T}_i$ consists of a single type of gates, (3.a) derives $\sum_{e \in \mathcal{L}_i} disc_i(e) \geq nr - k\|\mathcal{T}_i\|$. Plugging the above two inequalities, we have $r/(2\|\mathcal{T}_i\|) \leq q \cdot \|\mathcal{L}_i - \mathcal{L}'_i\|/\|\mathcal{T}_i\| + \frac{k}{n} < 5q$ by (3.8) and (Q). Hence by (V) we have $\|\mathcal{T}_i\| > 1/r'^3$, as desired.

We can also evaluate the sum of $vol(e)$ over $e \in \mathcal{L}_i$ by (3.10) : $\sum_{e \in L} vol(g) \leq 2n$. In fact, in case T is a $\cup$-tree, we have $\sum_{e \in L} \|set(e)\| \leq \|set(g_{i,l_i})\| + k\|\mathcal{T}_i\|$, by $overlap(C) \leq k$. On this inequality, the left-hand is $\geq \sum_{e \in L} vol(e)$, and the right-hand is $\leq n(1 + k/(nr'^3)) < 2n$ by (3.6). The case that T is a $\cap$-tree is similar, where we estimate $\sum_{e \in L} \|\neg set(e)\|$.

As before, we take $I_2 \subseteq [n] - I$ such that $\|I_2\| \geq n/2(l+1)$ and $l_i = l'_c$ for all $i \in I_2$, and apply Lemma 2.2 with $(\mathcal{A}_i)_{i \in I_2}$ and $(F_i)_{i \in I_2}$. Here we reset $r = r_{l'_c}$, $r' = r_{l'_c+1}$ and $q = q_{l'_c}$.

Choose $g \in A' = \bigcup_{i \in I_2} \mathcal{A}_i$. $\overline{disc}(g)$, $\rho(g)$, $\phi(g)$ and $\psi(g)$ are similarly defined as the previous case, using $(\mathcal{A}_i)_{i \in I_2}$. We can check that $\rho(g) \leq s_0$, and also $\psi(g) \leq N := (2 \ln a)^{2(2+\varepsilon)/\varepsilon}$ by using (3.3),(W) and (X).

Thus, we can apply Lemma 2.2. In this case, we cannot bound $\phi(g)$ directly, however $\rho(g) \leq N\phi(g)$, since $\phi(g) > 1$ by (3.c), and we have $\|A\| > (1/100N) \cdot \sum_{i \in I_1} \sum_{g \in \mathcal{A}_i} (\overline{disc}(g)/vol(g))^{2+\varepsilon}$. Here, we use the following inequality, which is checked, e.g., by considering the extreme points of the left-hand function : given $L > 0$ and $c_5 \geq 1$. For any reals $x_1, \ldots, x_k$ with $0 \leq \forall x_i \leq L$ and also any positive reals $y_1, \cdots, y_k$, it holds that $\sum_{i=1}^k (x_i/y_i)^{c_5} \geq (\sum_{i=1}^k x_i)^{c+1}/L(\sum_{i=1}^k y_i)^{c_5}$. Setting $c_5 = 2 + \varepsilon$, $L = nr'$

(by (3.3)), $k = \sum_{i \in I_2} \|\mathcal{A}_i\|$, $x_i = \overline{disc}(g)$, and $y_i = vol(g)$, we get $\|A'\| > S^{3+\varepsilon}/(100Nnr'T^{2+\varepsilon})$, where $S = \sum_{i \in I_2} \sum_{g \in \mathcal{A}_i} \overline{disc}(g) = \sum_{i \in I_2} \sum_{g \in \mathcal{A}_i} disc_i(g)$ and $T = \sum_{i \in I_2} \sum_{g \in \mathcal{A}_i} vol(g)$. Here, in virtue of (3.9) and (3.10), $S \geq \|I_2\| \cdot nr/2$ and $T \leq \|I_2\| \cdot 2n$. Thus we obtain $\|A'\| > nr^{3+\varepsilon}/(100 \cdot 2^{5+2\varepsilon}(l+1)Nr')$, and finally by (Y) and (Z), $\|A'\| > (2a^2+2)n$. Here we counted the number of edges, thus actually, $size^*(C) > (a^2+1)n$, as required. □

Now by using the fact that **CSQ** is strongly $(s, (5/4)n/2^s)$-disjoint for any $s \leq \log n/4$, the following lower bound is derived from the above lemma.

Theorem 3.2. Let C be any set circuit computing **CSQ** such that $alt(C) = O(1)$ and $overlap^*(C) = \omega(n)$, then $size(C) = \omega(n)$.

Corollary 3.3. Let C be any $\{\vee, \wedge, \neg\}$-circuit computing f_{csq} such that $alt(S(C)) = O(1)$ and $overlap^*(S(C)) = \omega(n)$. Then $size(C) = \omega(n)$.

We also have the following bound.

Theorem 3.4. Let C be any $\{\vee, \wedge, \neg\}$-circuit computing f_{csq} such that $alt(S(C)) \leq (\ln\ln\ln n)/2$ and $overlap^*(SC(C)) \leq n/\ln n$. Then for some $c > 0$, $size(C) = \Omega\left(ne^{(\ln\ln n)^c}\right)$.

References

[1] Berkowitz, S., On some relationships between monotone and non-monotone circuit complexity, Technical Report, Univ. of Tront. (1982).

[2] Bollobás, B., *Random Graphs*, Academic Press (1985).

[3] Brown, W.G., On graphs that do not contain a Thompson graph, *Can. Math. Bull.* **9** (1966), 281–285.

[4] Dunne, P.E., Relations beween monotone and non-monotone network complexity, *London Math. Soc. Lecture Note* **169** (1992), 1–25.

[5] Mehlhorn, K., Some remarks on Boolean sums, *Acta Informatica* **12** (1979), 371–375.

[6] Nečhiporuk, E.I., On a Boolean matrix, *Problemy Kibernet.* **21** (1969), 237–241 (in Russian); *Systems Theory Research* **21** (1971), 236–239 (in English).

[7] Pippenger, N., *On Another Boolean Matrix*, Theoret. Comput. Sci. **11** (1980) 49–56.

[8] Savage, J.E., An algorithm for the computation of linear forms, *SIAM J. Comput.* **3** (1974) 150–158.

[9] Wegener, I., *The Complexity of Boolean Functions*, Wiley-Teubner Series in Comput. Sci. (1987).

[10] Wegener, I., A new lower bound on the monotone network complexity of Boolean sums, *Acta Informatica* **15** (1980), 109–144.