4. The breakthrough of Razborov and Andreev

References

- Alexander E. Andreev, On a method for obtaining lower bounds for the complexity of individual monotone functions, Soviet Math. Dokl. 31 (1985), 530–534.
- Alexander A. Razborov, Lower bounds on the monotone complexity of some Boolean functions, Soviet Math. Dokl. 31 (1985), 354–357.
- Alexander A. Razborov, A lower bound on the monotone network complexity of the logical permanent, Math. Notes Acad. Sci. USSR 37 (1985), 485–493.
- Noga Alon, Ravi B. Boppana, The monotone circuit complexity of Boolean functions, Combinatorica 7 (1987), 1–22.

We shall present the approximation method as developed by Alexander Razborov.

$\mathcal{P}(\{0,1\}^n)$ denotes the power set of $\{0,1\}^n$.

Note that $\mathcal{P}(\{0,1\}^n)$ with the operations $\cap$ and $\cup$ is a lattice

For a function $f \in B_n$ let

$$\mathrm{at}(f) := \{ a \in \{0,1\}^n \mid f(a) = 1 \}.$$

Note that

$$\mathrm{at}(0) = \emptyset \quad \text{and} \quad \mathrm{at}(1) = \{0,1\}^n.$$

Furthermore, for $f, g \in B_n$

$$\mathrm{at}(f \vee g) = \mathrm{at}(f) \cup \mathrm{at}(g) \quad \text{and}$$

$$\mathrm{at}(f \wedge g) = \mathrm{at}(f) \cap \mathrm{at}(g).$$

Given any monotone Boolean network β for a function $f \in M_n$, we obtain a network β' which computes $\mathrm{at}(f)$ if we replace

- each input x_i, $1 \leq i \leq n$ by $\mathrm{at}(x_i)$,
- each $\wedge$-gate by an $\cap$-operation and
- each $\vee$-gate by an $\cup$-operation.

Exercise

Prove that the network β' constructed above computes the set $\mathrm{at}(f)$.

Idea (Razborov):

Replace in β' the operations $\cap$ and $\cup$ by two operations $\sqcap$ (meet) and $\sqcup$ (join) which have the property that $M \sqcap N \subseteq M \cap N$ and $M \cup N \subseteq M \sqcup N$.

After doing this, the network does not compute $\sigma(f)$ but an approximation of $\sigma(f)$.

$S \subseteq P(\{0,1\}^n)$ with two operations $\sqcap$ and $\sqcup$ is a <u>legitimate lattice</u> if the following hold:

i) $\sigma(0), \sigma(1), \sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n) \in S$ and

ii) S is a lattice with respect to set inclusion; i.e., $M, N \subseteq M \sqcup N$ and $M \sqcap N \subseteq M, N$ for all $M, N \in S$.

Note that the second property implies that

$$M \cup N \subseteq M \sqcup N \quad \text{and} \quad M \sqcap N \subseteq M \cap N.$$

For $M, N \in S$ let

$$\delta_{\sqcup}(M,N) := (M \sqcup N) \setminus (M \cup N) \quad \text{and}$$
$$\delta_{\sqcap}(M,N) := (M \sqcap N) \setminus (M \cap N)$$

<u>Interpretation</u>:

$\delta_{\sqcup}(M,N)$ and $\delta_{\sqcap}(M,N)$, respectively is a measure for the error introduced by the replacement of $\cup$ by $\sqcup$ and $\cap$ by $\sqcap$, respectively.

For $f \in M_n$ and the legitimate lattice S we define the <u>distance</u> $\rho(f,S)$ from f to S to be the minimal t such that there are

$$M, M_1, N_1, M_2, N_2, \ldots, M_t, N_t \in S \quad \text{such that}$$

$$q(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_{\sqcap}(M_i, N_i)$$

and

$$M \subseteq q(f) \cup \bigcup_{i=n}^{t} \delta_{\sqcup}(M_i, N_i)$$

Theorem 4.1

Let $f \in M_n$ and $(S, \sqcup, \sqcap)$ be a legitimate lattice. Then

$$\rho(f, S) \leq C_{\Omega_m}(f).$$

Proof:

Let β be an optimal monotone network for f. Let $g_1, g_2, \ldots, g_t$ be the gates in β numbered in any topological order.

Consider the network β' which we obtain from β by replacing each input variable x_i, $1 \leq i \leq n$ by $q(x_i)$, each $\vee$ by $\sqcup$ and each $\wedge$ by $\sqcap$.

The network β' computes elements of S. Let

$$M_i, N_i, \quad 1 \leq i \leq t$$

be the elements of S computed at the inputs of the gate g_i in β' and let M be the element of S computed at the output node of β'.

Claim.

$$\sigma(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_{\sqcap}(M_i, N_i) \quad \text{and}$$

$$M \subseteq \sigma(f) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i).$$

Note that the claim implies that the size of β is an upper bound for the distance $\rho(f, S)$ from f to S.

Proof of claim.

We prove the claim by induction on t.

$t = 0$:

This is obvious since f is constant or a variable such that $\sigma(f) \in S$.

$t > 0$:

Assume that the assertion holds for $\ell < t$.

Let f_t and h_t be the input functions of the gate g_t. We distinguish two cases.

Case 1: g_t is an $\vee$-gate.

Induction hypothesis $\Rightarrow$

$$M_t \subseteq \sigma(f_t) \cup \bigcup_{i=1}^{t-1} \delta_{\sqcup}(M_i, N_i)$$

and

$$N_t \subseteq \sigma(h_t) \cup \bigcup_{i=1}^{t-1} \delta_{\sqcup}(M_i, N_i).$$

Furthermore,

$$Q(f_t) \subseteq M_t \cup \bigcup_{i=1}^{t-1} \delta_\sqcap(M_i, N_i)$$

and

$$Q(h_t) \subseteq N_t \cup \bigcup_{i=1}^{t-1} \delta_\sqcap(M_i, N_i).$$

Hence we obtain

$$\begin{aligned} M = M_t \sqcup N_t &= M_t \cup N_t \cup \delta_\sqcup(M_t, N_t) \\ &\subseteq Q(f_t) \cup Q(h_t) \cup \bigcup_{i=1}^{t} \delta_\sqcup(M_i, N_i) \\ &= Q(f) \cup \bigcup_{i=1}^{t} \delta_\sqcup(M_i, N_i). \end{aligned}$$

and

$$\begin{aligned} Q(f) &= Q(f_t) \cup Q(h_t) \\ &\subseteq M_t \cup N_t \cup \bigcup_{i=1}^{t-1} \delta_\sqcap(M_i, N_i) \\ &\subseteq (M_t \sqcup N_t) \cup \bigcup_{i=1}^{t-1} \delta_\sqcap(M_i, N_i) \\ &\subseteq M \cup \bigcup_{i=1}^{t} \delta_\sqcap(M_i, N_i). \end{aligned}$$

Case 2: g_t is an $\wedge$-gate.

Can be proved similarly

Exercise. ∎

Theorem 4.1 gives us the following way to prove a lower bound for the monotone network

complexity of a monotone Boolean function f:

(1) Choose an appropriate legitimate lattice $(S, \sqcap, \sqcup)$.
(2) Prove a lower bound for the distance $\rho(f, S)$ from f to S.

How to choose a lattice $(S, \sqcap, \sqcup)$ such that for a given function f a large lower bound for $\rho(f, S)$ could be proved?

S should not contain a "good" approximation of $\sigma(f)$; i.e., S should only contain sets M such that $\sigma(f) \setminus M$ or $M \setminus \sigma(f)$ has to be "large". Furthermore, the δ-sets should be "small".

To get these properties, Razborov has defined a class of legitimate lattices which uses a new clever "closure" operation.

Let $r \geq 2$ and $\ell \geq 2$ be natural numbers. Consider not necessarily distinct sets $W, W_1, W_2, \ldots, W_r$. We say

- $W_1, W_2, \ldots, W_r$ imply W $(W_1, W_2, \ldots, W_r \vdash W)$ iff
  a) $|W|, |W_1|, |W_2|, \ldots, |W_r| \leq \ell$, and
  b) $W_i \cap W_j \subseteq W$ for all $1 \leq i < j \leq r$.

- Let A be a collection of sets. We say
  - A implies W $(A \vdash W)$ iff

$\exists W_1, W_2, \ldots, W_r \in A: W_1, W_2, \ldots, W_r \vdash W.$

- A is <u>closed</u> iff

  $\forall W: A \vdash W \Rightarrow W \in A.$

- A^* denotes the <u>closure</u> of A; i.e.,

  $A^* := \bigcap \{B \mid A \subseteq B \text{ and } B \text{ closed}\}.$

<u>Lemma 4.1</u>

Let A be a collection of sets. Then

a) A^* is closed,

b) $A \subseteq A^*$,

c) $(A^*)^* = A^*$, and

d) $A \subseteq B \Rightarrow A^* \subseteq B^*$.

<u>Proof</u>:

Exercise ■

Now we consider collections A of sets where each element $W \in A$ denotes a Boolean function in $\mathcal{B}_n$. We define

$$\lceil A \rceil := \bigcup_{W \in A} \sigma(W).$$

For a family $\mathcal{F}$ of such collections, we define $(S, \sqcap, \sqcup)$ in the following way:

- $S := S(n, r, e)$

  $:= \{\emptyset\} \cup \{\lceil A \rceil \mid A \in \mathcal{F} \text{ closed}\}$

- $\lceil A \rceil \sqcap \lceil B \rceil := \lceil A \cap B \rceil$ and
- $\lceil A \rceil \sqcup \lceil B \rceil := \lceil (A \cup B)^* \rceil$.

Given a monotone Boolean function $f \in B_n$, the goal is to define an appropriate family $\mathcal{K}$ such that $(S, \sqcap, \sqcup)$ is a legitimate lattice and $g(f, S)$ is large.

We shall give a very general definition of $\mathcal{K}$ such that $(S, \sqcap, \sqcup)$ is a legitimate lattice. Let

$$\mathcal{M}_{\ell,n} := \{ m \mid m : \{0,1\}^n \to \{0,1\} \text{ is a monomial with } |m| \leq \ell \}.$$

Note that the empty monomial 1 is contained in $\mathcal{M}_{\ell,n}$.

Lemma 4.2

Let $\mathcal{K} := \mathcal{P}(\mathcal{M}_{\ell,n})$. Then $(S, \sqcap, \sqcup)$ is a legitimate lattice.

Proof:

- By definition, $\sigma^{-1}(0) = \emptyset \in S$.
- Obviously, $\mathcal{M}_{\ell,n}$ is closed and $1 \in \mathcal{M}_{\ell,n}$. Hence,
$$\sigma^{-1}(1) = \{0,1\}^n = \lceil \mathcal{M}_{\ell,n} \rceil \in S.$$
- Let
$$A_i := \{ m \in \mathcal{M}_{\ell,n} \mid m \leq x_i \}.$$

Definition of $A_i \Rightarrow A_i$ is closed.
Furthermore, $\sigma_1(x_i) = \lceil A_i \rceil \in S$.
$\Rightarrow \quad \sigma_1(x_i) \in S$ for $1 \leq i \leq n$.

Consider $A, B \in \mathcal{M}_{e,n}$ closed. It remains to be proved

a) $\lceil A \rceil, \lceil B \rceil \subseteq \lceil A \rceil \sqcup \lceil B \rceil$ and
b) $\lceil A \rceil \sqcap \lceil B \rceil \in \lceil A \rceil$, $\lceil A \rceil \sqcap \lceil B \rceil \in B$.

To prove a) it suffices to show

$A \in (A \cup B)^*$ and $B \in (A \cup B)^*$.

Since $A, B \subseteq A \cup B$, this is obvious.

To prove b, it suffices to show

$A \cap B \subseteq A$ and $A \cap B \subseteq B$

This is obvious as well. ∎

Next we shall investigate the structure of closed sets. Let A be a collection of sets. $C \in A$ is called <u>minimal</u> iff for all $D \in A$ there holds $D \not\subset C$.

We shall show that closed systems contains only "few" minimal sets. This will be useful since we shall relate prime implicants in δ-sets and minimal sets in closed systems.

Lemma 4.3

In each closed system A, the number of minimal sets with at most k elements is bounded by $(r-1)^k$.

Proof:

A system $\mathcal{F}$ of sets of at most k elements has property $P(r,k)$ if

$\nexists\, W, W_1, W_2, \ldots, W_r \in \mathcal{F}$ and $U \subset W$ such that $W_i \cap W_j \subseteq U \;\forall\, 1 \le i < j \le r$ (i.e., $\mathcal{F} \vdash U$)

Note that the system of all minimal sets of A of cardinality $\le k$ has property $P(r,k)$. Otherwise, by the definition of closed sets, $U \in A$ and hence, W would not be minimal.

Claim 1:

Systems $\mathcal{F}$ having property $P(r,k)$ contains at most $(r-1)^k$ elements.

Proof (by induction on r)

$r = 2$: (then $(r-1)^k = 1$).

Assume that there are $W_1, W_2 \in \mathcal{F}$, $W_1 \neq W_2$.

Let

$$U := W_1 \cap W_2.$$

Then

$$U \subset W_1 \quad \text{or} \quad U \subset W_2.$$

Choose

$$W := \begin{cases} W_1 & \text{if } U \subset W_1 \\ W_2 & \text{otherwise} \end{cases}$$

$\Rightarrow$

$W, W_1, W_2 \in \mathcal{F}$, $U \subset W$ such that $W_1 \cap W_2 \subseteq U$.

Hence, $\mathcal{F}$ has not property $P(2,k)$, a contradiction.

$r-1 \rightsquigarrow r$:

Let $\mathcal{F}$ be a system having property $P(r,k)$ and $D \in \mathcal{F}$. For all $C \subseteq D$ define

$$\mathcal{F}_C := \{ W \setminus C \mid W \in \mathcal{F} \text{ and } W \cap D = C \}$$

Claim 2:

$\mathcal{F}_C$ has property $P(r-1, k-|C|)$.

Proof:

Assume that $\mathcal{F}_C$ has not property $P(r-1, k-|C|)$.
Choose

$$W', W_1', W_2', \ldots, W_{r-1}' \in \mathcal{F}_C, \quad U' \subset W'$$

such that

$$W_i' \cap W_j' \subseteq U' \quad \text{for } 1 \le i < j \le r-1.$$

Let

$$\begin{aligned} W &:= W' \cup C && \in \mathcal{F} \\ U &:= U' \cup C && \subset W \\ W_i &:= W_i' \cup C && \in \mathcal{F} \quad \text{for } 1 \le i \le r-1. \\ W_r &:= D && \in \mathcal{F} \end{aligned}$$

Note that

$$C \subseteq D \text{ and } W_i \cap W_j \subseteq U \text{ for } 1 \le i < j \le r.$$

$\Rightarrow$ $\mathcal{F}$ has not property $P(r,k)$, a contradiction.

□

By the induction hypothesis

$$|\mathcal{F}_C| \le (r-2)^{k-|C|}.$$

Since $D \in \mathcal{F}$ is chosen fixed, the condition

$$C = W \cap D$$

is fulfilled for only one set C.

Note that

$$(W \cap D = C = \tilde{W} \cap D \text{ and } W \neq \tilde{W}) \Rightarrow W|C \neq \tilde{W}|C$$

$\Rightarrow$

$$
\begin{aligned}
|\mathcal{F}| &= \sum_{C \in D} |\mathcal{F}_C| \\
&\leq \sum_{C \in D} (r-2)^{k-|C|} \\
&= \sum_{i=0}^{|D|} \binom{|D|}{i} (r-2)^{k-i} \\
&\underset{\text{since } |D| \leq k}{\leq} \sum_{i=0}^{k} \binom{k}{i} (r-2)^{k-i} \\
&\underset{\text{binomial Theorem}}{=} (r-1)^k
\end{aligned}
$$

□

11.06.

To estimate the $\delta_\sqcap$-sets in the case that $|M|$ is large, we shall use Lemma 4.3. If $|M|$ is not large enough, we need an estimation of the $\delta_\sqcup$-sets.

Note that

$$\ulcorner A \urcorner \sqcup \ulcorner B \urcorner = \ulcorner (A \cup B)^* \urcorner .$$

Hence,

$$
\begin{aligned}
\delta_\sqcup(\ulcorner A \urcorner, \ulcorner B \urcorner) &= \ulcorner C_{A \cup B}{}^* \urcorner \setminus (\ulcorner A \urcorner \cup \ulcorner B \urcorner) \\
&= \ulcorner (A \cup B)^* \urcorner \setminus \ulcorner \underbrace{A \cup B}_{C} \urcorner \\
&= \ulcorner C^* \urcorner \setminus \ulcorner C \urcorner .
\end{aligned}
$$

Given C how to construct C^* ?

Let

$$C' := \{ W \notin C \mid C \vdash W \}.$$

Then

$$C^* = C \iff C' = \emptyset.$$

The following algorithm improves C with respect to C^*.

Algorithm IMPROVECLOSURE

Input: $C \subseteq C^*$.

Output: D such that $C \subseteq D \subseteq C^*$ and $D^* = C^*$.

Method:

(1) Choose a minimal set $W \in C'$.

(2) $D := C \cup \{ W' \in U_{\ell}(\mathcal{F}) \mid W \subseteq W' \}$.

This algorithm can be repeated until $C' = \emptyset$.

If $\mathcal{F} = P(M_{\ell,n})$ then the number of improvement steps is bounded by $|M_{\ell,n}| \leq n^{\ell}$.

The following lemma improves this upper bound.

Lemma 4.4

The maximal number of improvement steps applied to a set C until C^* is obtained is at most $2r^{\ell}$.

Proof:

Let $S = (W_1, W_2, \ldots, W_p)$ be a sequence of

distinct sets. We say that S has property $T(r,\ell)$ if

i) $|W_i| \leq \ell$ for $1 \leq i \leq p$, and

ii) $\nexists\ i_1 \leq i_2 \leq \dots \leq i_r < i_{r+m}$ and $U \subset W_{i_{r+m}}$ such that $W_{i_j} \cap W_{i_m} \subseteq U$ for all $1 \leq j < m \leq r$ (i.e., $W_{i_1}, W_{i_2}, \dots, W_{i_r} \vdash U$).

If $S = (W_1, W_2, \dots, W_p)$ is the sequence of minimal sets created by the sequence of improvement steps for obtaining C^* from C, then S has property $T(r,\ell)$. Otherwise, we get a contradiction to the minimality of $W_{i_{r+m}}$ at the moment when it has been chosen.

$\Rightarrow$ To prove the lemma, it suffices to prove:

Claim 1:
Let $r \geq 1$ and $\ell \geq 0$. If $S = (W_1, W_2, \dots, W_p)$ has property $T(r,\ell)$ then $p \leq 2r^\ell$.

Proof: (by induction on r).

$r = 1$: (then $2r^\ell = 1$).

Assume that S has property $T(1,\ell)$ and $p > 2$.

Since $r = 1$ makes $\vdash$ trivial there holds $W_1 \vdash \phi$. Since W_1, W_2, W_3 are pairwise distinct, either W_2 or W_3 is nonempty. We distinguish two cases.

a) $W_2 \neq \phi$.

But then $W_1 \vdash \phi \subset W_2$ contradicts the assumption that S has property $T(1,e)$.

b) $W_3 \neq \phi$.

Again, $W_1 \vdash \phi \subset W_3$ contradicts the assumption that S has property $T(1,e)$.

This proves the claim for $r=1$.

$r-1 \rightsquigarrow r$:

Assume that $S = (W_1, W_2, \ldots, W_p)$ has property $T(r,e)$. Let

$$D := W_1.$$

For each $C \subseteq D$ define:

S_C is the sequence of all sets $(W_i' :=) \; W_i \cap C$ such that $W_i \cap D = C$, appearing in the same order that the W_i appear in S.

Claim 2:

S_C has property $T(r-1, e-1|C|)$.

Proof:

Assume that S_C has not property $T(r-1, e-1|C|)$. Choose

$i_1 \leq i_2 \leq \ldots \leq i_{r-1} < i_r$ and $U' \subset W_{i_r}'$

such that

$W'_{i_j} \cap W'_{i_h} \subseteq U'$ for all $1 \leq j < h \leq r-1$.

To get a contradiction, we show that S has not property $T(r, \ell)$. For doing this, we choose

$$i'_1 \leq i'_2 \leq \ldots \leq i'_r < i'_{r+n} \text{ and } U \subseteq W_{i'_{r+n}}$$

where

$$i'_j := i_j \quad \text{for } 1 \leq j \leq r-1,$$
$$i'_r := i_{r-1},$$
$$i'_{r+1} := i_r, \text{ and}$$
$$U := U' \cup C.$$

Obviously, $W_{i'_j} \cap W_{i'_h} \subseteq U$ for $1 \leq j < h \leq r$.

$\Rightarrow$

S has not property $T(r, \ell)$, a contradiction. □

By the induction hypothesis

$$|S_C| \leq 2(r-1)^{\ell - |C|}.$$

Since D is chosen fixed, the condition

$$W_i \cap D = C$$

is fulfilled for exactly one set C.

$\Rightarrow$

$$|S| = \sum_{C \subseteq D} |S_C|$$
$$\leq 2 \cdot \sum_{i=0}^{|D|} \binom{|D|}{i} (r-1)^{\ell - i}$$

$$\leq \sum_{i=0}^{\ell} \binom{\ell}{i} (r-1)^{\ell-i}$$
$$|D| \leq \ell$$

$$= 2r^{\ell}$$

binomial Theorem

■

We shall use the approximation method to prove that the monotone complexity of the clique function is exponential.

Let CLIQUE(m,s) be the Boolean function of $n := \binom{m}{2}$ variables representing the edges of an undirected graph $G = (V,E)$ on m nodes whose value is one iff G contains a clique of size s. In the subsequence, we use the node set $V = \{1,2,\ldots,m\}$. Furthermore, x_{ij} denotes the variable which corresponds to the edge (i,j). We shall identify the edge (i,j) and the variable x_{ij}.

Let

$$V(\ell) := \{ W \subseteq V \mid |W| \leq \ell \}.$$

Instead of thinking about n-tuples corresponding to certain graphs it is easier to consider these graphs directly. This yields the following definitions:

For $A \subseteq V(c)$ let $\lceil A \rceil$ be the set of all graphs with node set V which contain a clique on a set $W \in A$; i.e.,

$$\lceil A \rceil := \{ G = (V,E) \mid G \text{ contains a clique on some } W \in A \}.$$

Now, we use $\mathcal{F} := P(V(c))$ for the definition of the lattice $(\mathcal{F}, \sqcap, \sqcup)$.

Next, we shall characterize a subset of the set of graphs which do not contain any s-clique. This subset will be used in the lower bound proof.

An $(s-1)$-partite graph does not contain an s-clique. We are interested in complete $(s-1)$-partite graphs. Such a graph has the property that no edge can be added without destroying the property $(s-1)$-partite. We can describe such a graph $G = (V,E)$ by a colouring

$$h : V \to \{1, 2, \ldots, s-1\}$$

of the nodes such that the following is fulfilled:

$$(i,j) \in E \iff h(i) \neq h(j).$$

A complete $(s-1)$-partite graph $G = (V, E)$ is uniquely specified by the colouring h. Hence, we write $G(h)$ for this graph.

Note that $G(h)$ contains a clique on the node set $W \subseteq V$ iff the nodes in W are coloured with $|W|$ different colours. In that case, we say that W is <u>properly coloured</u>.

We consider complete g-partite graphs for an appropriate g. To prove the existence of such a graph having a certain property, we shall use a probabilistic argument. This means that we consider randomly chosen complete g-partite graphs or equivalently random colourings of the node set V with g colours. Assume that we have the uniform distribution on all g^n colourings of V.

<u>Lemma 4.5</u>

Let $g \geq \ell$, $A \subseteq V(G)$, $W, W_1, W_2, \ldots, W_r \subseteq A$ and $W_1, W_2, \ldots, W_r \not\subseteq W$. Let E and E_i, respectively be the event that W and W_i, respectively is properly coloured. Let $\overline{E_i}$ be the complementary event of E_i. Then

$$P_r\left(E \cap \bigcap_{i=1}^{r} \overline{E_i}\right) \leq \left[1 - \frac{g(g-1)\cdots(g-\ell+1)}{g^\ell}\right]^r.$$

<u>Proof</u>:

Note that $W_i \cap W_j \subseteq W$ for $1 \leq i < j \leq r$.

$\Rightarrow$

W properly coloured implies that the events $CE_1, CE_2, \ldots, CE_r$ are independent.

Furthermore, the sets $W_i \setminus W$, $1 \le i \le r$ are pairwise disjoint. Hence,

$$\begin{aligned} Pr\left(E \cap \bigcap_{i=1}^{r} CE_i\right) &\le Pr\left(\bigcap_{i=1}^{r} CE_i \mid E\right) \\ &= \prod_{i=1}^{r} Pr\left(CE_i \mid E\right) \\ &= \prod_{i=1}^{r} \left(1 - Pr\left(E_i \mid E\right)\right). \end{aligned}$$

Hence, it suffices to prove that for $1 \le i \le r$

$$Pr\left(E_i \mid E\right) \ge \frac{q(q-1)\cdots(q-\ell+1)}{q^\ell}.$$

For doing this let

$$p(i) := |W_i \cap W| \quad \text{and} \quad q(i) := |W_i \setminus W|.$$

Then

$$p(i) + q(i) = |W_i| \le \ell.$$

The event E implies for the set W_i that $W_i \cap W$ is coloured with $p(i)$ different colours. The probability that the $q(i)$ elements of $W_i \setminus W$ are coloured with $q(i)$ different other colours is

$$\prod_{0 \le j \le q(i)} \frac{q - p(i) - j}{q} \ge \prod_{0 \le j < \ell} \frac{q - j}{q}$$

$$= \frac{g(g-1)\cdots(g-\ell+1)}{g^\ell}.$$

This proves the lemma. ∎

Lemma 4.6

Let $C \subseteq V(e)$, $g \geq \ell$ and h be a random colouring of the node set V with g colours. Then

$$Pr\left(G(h) \in \lceil C^* \rceil \setminus \lceil C \rceil\right) \leq 2r^\ell \cdot \left[1 - \frac{g(g-1)\cdots(g-\ell+1)}{g^\ell}\right]^r.$$

Proof:

By Lemma 4.4, C^* is constructed from C by the application of $p \leq 2r^\ell$ improvement steps. Let

$$C = C_0, C_1, C_2, \ldots, C_p = C^*$$

be the results of the steps in this construction. It suffices to prove

$$Pr\left(G(h) \in \lceil C_i \rceil \setminus \lceil C_{i-1} \rceil\right) \leq \left(1 - \frac{g(g-1)\cdots(g-\ell+1)}{g^\ell}\right)^r.$$

Let W_i be the chosen set for the construction of C_i from C_{i-1}.

$G(h)$ contains a clique on a node set D iff D is properly coloured. Hence,

$G(h) \in \lceil C_i \rceil \Leftrightarrow$ A set in C_i is properly coloured.

$G(h) \notin \lceil C_{i-1} \rceil \Leftrightarrow$ All sets in C_{i-1} are not properly coloured.

The event $G(h) \in \lceil C_i \rceil \setminus \lceil C_{i-1} \rceil$ implies that

- W_i is properly coloured.

and, since $C_{i-1} \vdash W_i$; i.e., $B_1, B_2, \dots, B_r \vdash W_i$ for sets $B_j \in C_{i-1}$, $1 \le j \le r$ that

- $B_1, B_2, \dots, B_r$ are not properly coloured.

$\Rightarrow$

The probability of this event has been upper bounded by Lemma 4.5.

∎

Lemma 4.6 gives us a useful bound for the probability that a random complete $(s-1)$-partite graph is in some S_L-set. Now we are prepared to prove the lower bound.

Theorem 4.2

Let $4 \le s \le \frac{1}{8}\left(\frac{m}{\log m}\right)^{2/3}$, $\ell = \lceil \frac{1}{2}\sqrt{s} \rceil$ and $r = \lceil 4\sqrt{s} \log m \rceil$. Then

$$C_{\Omega_m}(CLIQUE(m,s)) \ge \frac{1}{8} \cdot \left\lceil \frac{m}{s(r-1)} \right\rceil^{\left\lceil \frac{\ell+1}{2} \right\rceil}.$$

Proof:

By Theorem 4.1, it suffices to prove

$$\rho(\mathrm{CLIQUE}(m,s), S(m,r,\ell)) \geq \frac{1}{8}\left\lceil \frac{m}{s(r-1)} \right\rceil^{\left\lceil \frac{\ell+1}{2} \right\rceil}.$$

Let $f = \mathrm{CLIQUE}(m,s)$ and

$$t := \rho(f, S(m,r,\ell)).$$

$$\Sigma$$

Consider

$$M, M_1, N_1, M_2, N_2, \ldots, M_t, N_t \in \Sigma$$

such that

$$\sigma_1(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_r(M_i, N_i)$$

and

$$M \subseteq \sigma_1(f) \cup \bigcup_{i=1}^{t} \delta_u(M_i, N_i).$$

Again, instead of thinking about the elements of $\sigma_1(f)$ directly, we shall consider the corresponding graphs.

The definition of Σ implies that

$$\exists\, A, A_1, B_1, A_2, B_2, \ldots, A_t, B_t \in V(\ell) \text{ closed}$$

such that

$$M = \lceil A \rceil, \quad M_i = \lceil A_i \rceil \text{ and } N_i = \lceil B_i \rceil, \quad 1 \leq i \leq t.$$

We distinguish two cases.

Case 1: M is not the set of all graphs

We consider those $\binom{m}{s}$ graphs which contain exactly the edges of an s-clique. These are exactly those graphs which correspond to the prime implicants of the clique function. The assertion follows directly from the following two claims:

Claim 1:

M contains at most $\frac{1}{2} \cdot \binom{m}{s}$ of these graphs.

Claim 2:

Each $\delta_\Pi(M_i, N_i)$ contains at most

$$4 \cdot \left(\frac{s(r-1)}{m}\right)^{\left\lceil \frac{e+1}{2} \right\rceil} \cdot \binom{m}{s}$$

s-cliques.

Note that

$$\frac{\frac{1}{2}\binom{m}{s}}{4 \cdot \left(\frac{s(r-1)}{m}\right)^{\left\lceil \frac{e+1}{2} \right\rceil} \binom{m}{s}} = \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\left\lceil \frac{e+1}{2} \right\rceil}.$$

Proof of Claim 1:

Each graph contains all cliques on a single node. M is not the set of all graphs.

$\Rightarrow$

Each set $W \in A$ contains at least two elements.

Each s-clique in M contains a clique on a minimal element of A.

Lemma 4.3 $\Rightarrow$

Case 2: M is the set of all graphs.

Note that no complete $(s-1)$-partite graph is contained in $\sigma(f)$. Hence, all these graphs have to be contained in

$$\bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i).$$

Definition $\Rightarrow$

$$\begin{aligned}\delta_{\sqcup}(M_i, N_i) &= (M_i \sqcup N_i) \setminus (M_i \cup N_i) \\ &= \Gamma(A_i \cup B_i)^* \rceil \setminus \Gamma \underbrace{A_i \cup B_i}_{C_i} \rceil \\ &= \Gamma C_i^* \rceil \setminus \Gamma C_i \rceil.\end{aligned}$$

Let h be a random $(s-1)$ colouring of V.

Lemma 4.6 $\Rightarrow$

$$\begin{aligned}\Pr(G(h) \in \Gamma C_i^* \rceil \setminus \Gamma C_i \rceil) &\leq 2r^{\ell}\left(1 - \frac{(s-1)(s-2)\cdots(s-\ell)}{(s-1)^{\ell}}\right)^{r} \\ &< m^{\ell} \cdot \left(1 - \frac{(s-1)\cdot\ldots\cdot(s-\ell)}{(s-1)^{\ell}}\right)^{r} \\ &= m^{\ell}\left(1 - 1\left(1-\tfrac{1}{s-1}\right)\left(1-\tfrac{2}{s-1}\right)\cdot\ldots\cdot\left(1-\tfrac{\ell-1}{s-1}\right)\right)^{r} \\ &\leq m^{\ell}\left(1 - \left(1-\tfrac{\ell-1}{s-1}\right)^{\ell-1}\right)^{r} \\ &\overset{\text{Bernoulli inequality}}{\leq} m^{\ell}\left(1 - \left(1-(\ell-1)\tfrac{\ell-1}{s-1}\right)\right)^{r} \\ &= m^{\ell}\left(\frac{(\ell-1)^2}{s-1}\right)^{r}\end{aligned}$$

Since $\ell = \lceil \frac{1}{2}\sqrt{s} \rceil$, we obtain

$$(\ell-1)^2 < \tfrac{1}{4}(s-1).$$

If an s-clique on a node set Z is contained in $\delta_\Pi(M_i, N_i)$ then

- $\exists$ minimal set $U \in A_i$: $U \subseteq Z$,
- $\exists$ minimal set $W \in B_i$: $W \subseteq Z$, and
- no subset of Z is contained in $A_i \cap B_i$.

Since $U \cup W \subseteq Z$ and A_i, B_i closed, there holds

$$|U \cup W| > \ell.$$

Otherwise, $U \cup W \in A_i$ and $U \cup W \in B_i$.

Hence, at least one of U and W contains

$$\geq \left\lceil \frac{\ell+1}{2} \right\rceil$$

elements.

Therefore, we obtain for the total number TN of s-cliques in $\delta_\Pi(M_i, N_i)$

$$\begin{aligned} TN &\leq 2 \cdot \sum_{k=\lceil \frac{\ell+1}{2} \rceil}^{\ell} (r-1)^k \binom{m-k}{s-k} \\ &\leq 2 \cdot \binom{m}{s} \cdot \sum_{k=\lceil \frac{\ell+1}{2} \rceil}^{\ell} \left(\frac{s(r-1)}{m} \right)^k \\ &< 2 \binom{m}{s} \left(\frac{s(r-1)}{m} \right)^{\lceil \frac{\ell+1}{2} \rceil} \cdot \sum_{j=0}^{\infty} \left(\frac{1}{2} \right)^j \\ &= 4 \cdot \left(\frac{s(r-1)}{m} \right)^{\lceil \frac{\ell+1}{2} \rceil} \binom{m}{s}. \end{aligned}$$

□

For $2 \le k \le \ell$, the number of minimal elements of cardinality k is

$$\le (r-1)^k.$$

Each of these elements is contained in exact

$$\binom{m-k}{s-k}$$

s-cliques.

Hence, the total number of s-cliques in M is bounded by

$$\sum_{k=2}^{\ell} (r-1)^k \cdot \binom{m-k}{s-k}$$

$$\le \sum_{k=2}^{\ell} (r-1)^k \binom{m}{s} \cdot \left(\frac{s}{m}\right)^k$$

$$= \binom{m}{s} \cdot \sum_{k=2}^{\ell} \left(\frac{s(r-1)}{m}\right)^k$$

$$\le \binom{m}{s} \cdot \sum_{k=2}^{\ell} \left(\frac{1}{2}\right)^k$$

$$< \frac{1}{2} \binom{m}{s}.$$

□

Proof of Claim 2:

Definition $\Rightarrow$

$$\delta_\Pi(M_i, N_i) = (M_i \cap N_i) \setminus (M_i \sqcap N_i)$$

$$= (\lceil A_i \rceil \cap \lceil B_i \rceil) \setminus \lceil A_i \cap B_i \rceil.$$

Hence, we obtain

$$< m^{s}\left(\frac{1}{4}\right)^{r}$$

$$= m^{\lceil \frac{1}{2}\sqrt{s} \rceil} \cdot 2^{-2\lceil 4\sqrt{s} \log m \rceil}$$

$$< m^{-\sqrt{s}}$$

Therefore, we obtain

$$Pr\left(G(n) \in \bigcup_{i=1}^{t} \left(\lceil C_i^* \rceil \setminus \lceil C_i \rceil\right)\right) \leq t \cdot m^{-\sqrt{s}}$$

For $t < \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\lceil \frac{e+1}{2} \rceil} < m^{\sqrt{s}}$ there holds

$$Pr\left(G(n) \in \bigcup_{i=1}^{t} \left(\lceil C_i^* \rceil \setminus \lceil C_i \rceil\right)\right) < 1$$

$\Rightarrow$

There exists at least one complete $(s-1)$-partite graph which is not contained in

$$\bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i),$$

a contradiction.

$\Rightarrow$

$$t \geq \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\lceil \frac{e+1}{2} \rceil}$$

■

<u>Corollary 4.1</u>

Let $s = \frac{1}{8}\left(\frac{m}{\log m}\right)^{2/3}$. Then

$$C_{\Omega_m}(\mathrm{CLIQUE}(m,s)) = \exp\left(\Omega\left(\left(\frac{m}{\log m}\right)^{1/3}\right)\right).$$

<u>Remark</u>: The structure of an optimal Ω_m-network is not used in the lower bound proof.

Alexander Andreev was the first who could prove an exponential lower bound for the monotone complexity of a Boolean function in NP. His methods are different, though very similar, to those of of Razborov. Using Razborov's approximation method, Alon and Boppana have improved Andreev's lower bound

from $2^{\Omega(n^{1/8}/\sqrt{\ln n})}$ to $2^{\Omega(n^{1/4}\cdot\sqrt{\ln n})}$.

We shall present this proof.

Andreev's function is the characteristic function is the characteristic function POLY(q,s) of the following problem:

For a prime power $q \geq 2$ let GF(q) denote the finite field with q elements. Let $G = (A, B, E)$ be a bipartite graph where $A := GF(q)$ and $B := GF(q)$. For given q and s, the problem is to decide whether there exists a polynomial p over GF(q) of degree at most s-1 such that for all $i \in A$ there hold $(i, p(i)) \in E$.

POLY(q,s) is a monotone Boolean function of $n := q^2$ variables. Given any polynomial p over GF(q) of degree $\leq s-1$, it is easy to check if for all $i \in A$, $(i, p(i)) \in E$. Hence, POLY(q,s) $\in$ NP.

The prime implicants of POLY(q,s) are the monomials corresponding exactly to a polynomial p over

$GF(q)$ of degree $\leq s-1$, i.e. $\wedge\{x_{i,p(i)} \mid 0 \leq i \leq q-1\}$.

We shall use Razborov's legitimate lattice defined for the function $POLY(q,s)$. First, we shall prove some combinatorial lemmas used in the lower bound proof.

Lemma 4.7

Let $G = (A, B, E)$ be a random bipartite graph, in which each edge appears independently with probability $1-\varepsilon$. Suppose $A \subseteq U_\ell(POLY(q,s))$ and $A \vdash W$. Then

$$Pr(W \subseteq E \text{ and no set in } A \text{ is contained in } E) \leq (1-(1-\varepsilon)^\ell)^r \leq (\varepsilon\ell)^r.$$

Proof:

$$A \vdash W \Rightarrow$$

$$\exists W_1, W_2, \ldots, W_r \in A : W_1, W_2, \ldots, W_r \vdash W.$$

Hence,

$$Pr(W \subseteq E \text{ and no set in } A \text{ is contained in } E) \leq Pr(W_i \not\subseteq E, 1 \leq i \leq r \mid W \subseteq E) = \prod_{i=1}^{r} Pr(W_i \not\subseteq E \mid W \subseteq E)$$

Note that by the definition of $\vdash$, the events $\{W_i \subseteq E \mid W \subseteq E\}$ are independent.

Furthermore,

$$\Pr(W_i \subseteq E \mid W \subseteq E) = 1-(1-\varepsilon)^{|W_i \setminus W|} \leq 1-(1-\varepsilon)^{\ell}.$$

Hence,

$$\Pr(W \subseteq E \text{ and no set in } A \text{ is contained in } E) \leq (1-(1-\varepsilon)^{\ell})^{r}.$$

Bernoulli's inequality $\Rightarrow$

$$(1-\varepsilon)^{\ell} = (1+(-\varepsilon)^{\ell}) \geqslant 1-\varepsilon\ell$$

$\Rightarrow$

$$-(1-\varepsilon)^{\ell} \leq -1+\varepsilon\ell$$

and hence,

$$(1-(1-\varepsilon)^{\ell})^{r} \leq (\varepsilon\ell)^{r}.$$

■

<u>Lemma 4.8</u>

Let $G = (A, B, E)$ be a random bipartite graph, in which each edge appears independently with probability $1-\varepsilon$. Suppose $C \in U_\ell(\text{POLY}(q,s))$. Then

$$\Pr(G \in \Gamma C^* \urcorner \setminus \Gamma C \urcorner) \leq 2r^{\ell}(1-(1-\varepsilon)^{\ell})^{r} \leq 2r^{\ell}\cdot(\varepsilon\ell)^{r}.$$

Proof:

Starting with C, we apply the algorithm ImproveClosure until C^* is obtained.

Lemma 4.4 $\Rightarrow$

The number of improvement steps is $\leq 2r^2$.

Let

$$C = C_0, C_1, C_2, \ldots, C_p = C^*$$

be the results of the improvement steps in this construction. It suffices to prove

$$\Pr(G \in \Gamma C_i \rceil \setminus \Gamma C_{i-1} \rceil) \leq (\varepsilon \ell)^r.$$

Let $W_i \in \{W \notin C_{i-1} \mid C_{i-1} \vdash W\}$ be the chosen set for the construction of C_i from C_{i-1}.

Lemma 4.7 $\Rightarrow$

$$\Pr(W_i \subseteq E \mid \text{no set of } C_{i-1} \text{ is contained in } E) \leq (\varepsilon \ell)^r$$

Altogether,

$$\Pr(G \in \Gamma C^* \rceil \setminus \Gamma C \rceil) \leq \sum_{i=1}^{p} \Pr(G \in \Gamma C_i \rceil \setminus \Gamma C_{i-1} \rceil)$$

$$\leq p \cdot (\varepsilon \ell)^r \leq 2r^2 (\varepsilon \ell)^r.$$

■

Now we are prepared to prove the lower bound for the monotone complexity for $f := \text{POLY}(q,S)$.

Theorem 4.3

Let $S = S(q^2, r, \ell)$, where $\ell = s$ and $2 \le r \le \frac{q}{3} + 1$. Then

$$\rho(f,S) \ge \min\left\{ \tfrac{1}{2}\left(\tfrac{q}{r-1}\right)^{s/2}, \tfrac{1}{4r^2}\left(\tfrac{q}{2s^2 \ln q}\right)^r \right\}.$$

Proof:

Let $t := \rho(f,S)$. Consider

$$M, M_1, N_1, M_2, N_2, \ldots, M_t, N_t \in S$$

such that

$$\sigma(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_\sqcap(M_i, N_i)$$

and

$$M \subseteq \sigma(f) \cup \bigcup_{i=1}^{t} \delta_\sqcup(M_i, N_i)$$

The definition of S implies that

$\exists A, A_1, B_1, A_2, B_2, \ldots, A_t, B_t \in \mathcal{U}_\ell(f)$ closed such that

$$M = \lceil A \rceil, \quad M_i = \lceil A_i \rceil \text{ and } N_i = \lceil B_i \rceil, \quad 1 \le i \le t.$$

Depending of the structure of M, we distinguish two cases.

Case 1: M is not the set of all bipartite graphs (A, B, E) with $|A| = |B| = q$.

We consider those q^s graphs which correspond to a polynomial over $GF(q)$ of degree $\leq s-1$. The assertion follows directly from the following two claims.

Claim 1:

M contains at most $\frac{1}{2} q^s$ of these graphs.

Claim 2:

Each $\delta_\Gamma(M_i, N_i)$ contains at most

$$q^{s - \lceil \frac{e+1}{2} \rceil} (r-1)^{\lceil \frac{e+1}{2} \rceil}$$

of these graphs.

Exercise:

Show that claim 1 and claim 2 imply the lower bound $\frac{1}{6} \left(\frac{q}{r-1} \right)^{s/2}$.

Proof of Claim 1:

Since $\Gamma\phi\Gamma$ is the set of all graphs (A, B, E), each $W \in A$ has cardinality at least one.

Lemma 4.3 $\Rightarrow$

For $1 \leq k \leq l$, the number of minimal sets of cardinality k is

$$\leq (r-1)^k.$$

Each of these is contained either precisely 0 or precisely q^{s-k} graphs corresponding to polynomials of degree at most $s-1$. The total number of such polynomial graphs contained in M is thus at most

$$\sum_{k=1}^{\ell} (r-1)^k q^{s-k} = q^s \sum_{k=1}^{\ell} \left(\frac{r-1}{q}\right)^k$$

$$\leq q^s \sum_{k=1}^{\ell} \left(\frac{1}{3}\right)^k$$

$$< \frac{1}{2} q^s.$$

□

Proof of Claim 2:

Definition $\Rightarrow$

$$\delta_r(M_i, N_i) = (M_i \wedge N_i) \setminus (M_i \barwedge N_i)$$

$$= (\lceil A_i \rceil \wedge \lceil B_i \rceil) \setminus \lceil A_i \wedge B_i \rceil.$$

If a polynomial graph with edge set Z is contained in $\delta_r(M_i, N_i)$ then

- $\exists$ minimal set $U \in A_i$: $U \subseteq Z$,
- $\exists$ minimal set $W \in B_i$: $W \subseteq Z$, and
- no subset of Z is contained in $A_i \wedge B_i$.

Since $U \cup W \subseteq Z$ and A_i, B_i closed there holds

$$|U \cup W| > \ell.$$

Otherwise, $u \cup w \in A_i$ and $u \cup w \in B_i$.

Hence, at least one of u and w contains

$$\geq \left\lceil \frac{\ell+1}{2} \right\rceil$$

elements.

Therefore, we obtain for the total number TN of polynomial graphs in $\delta_\Gamma(M_i, N_i)$

$$TN \leq 2 \cdot \sum_{k=\lceil \frac{\ell+1}{2} \rceil}^{\ell} (r-1)^k \cdot q^{s-k}$$

$$= 2 \cdot q^s \cdot \sum_{k=\lceil \frac{\ell+1}{2} \rceil}^{\ell} \left(\frac{r-1}{q}\right)^k$$

$$\leq 2\, q^{s-\lceil \frac{\ell+1}{2} \rceil} \cdot (r-1)^{\lceil \frac{\ell+1}{2} \rceil} \cdot \sum_{k=1}^{\lceil \frac{\ell+1}{2} \rceil} \left(\frac{r-1}{q}\right)^k$$

$$\leq 2\, q^{s-\lceil \frac{\ell+1}{2} \rceil} \cdot (r-1)^{\lceil \frac{\ell+1}{2} \rceil} \cdot \sum_{k=1}^{\frac{\ell+1}{2}} \left(\frac{1}{3}\right)^k$$

$$< q^{s-\lceil \frac{\ell+1}{2} \rceil} (r-1)^{\lceil \frac{\ell+1}{2} \rceil}.$$

□

Case 2: M is the set of all bipartite graphs (A, B, E) with $|A| = |B| = q$.

Since $M \subseteq \sigma(\mathcal{F}) \cup \dot{\bigcup_{i=1}^{t}} \delta_\sqcup(M_i, N_i)$

each such a graph is contained in

$$\sigma(\mathcal{F}) \cup \dot{\bigcup_{i=1}^{t}} \delta_\sqcup(M_i, N_i).$$

Note that $\delta_U(M_i, N_i) = \lceil C_i^{\uparrow} \rceil - \lceil C_i \rceil$ where $C_i := A_i \cup B_i$.

Let G be a random bipartite graph in which each edge appears independently with probability $1-\varepsilon$.

Claim: $\Pr(G \in \sigma(f)) \leq q^s (1-\varepsilon)^q \leq q^s e^{-\varepsilon q}$.

Proof of claim:

Note that $\sigma(f)$ contains only bipartite graphs which contain at least one of the polynomial graphs as a subgraph.

Fix any polynomial p over $GF(q)$ of degree $\leq s-1$. Consider the edges $(0, p(0)), (1, p(1)), \ldots, (q-1, p(q-1))$. Because the start nodes of these edges are pairwise different, these are q different edges.

$\Rightarrow$

$$\Pr\{\{(0,p(0)), (1,p(1)), \ldots, (q-1, p(q-1))\} \subseteq E\} \leq (1-\varepsilon)^q.$$

There are q^s polynomials over $GF(q)$ of degree $\leq s-1$.

$\Rightarrow$

$$\Pr(G \in \sigma(f)) \leq q^s (1-\varepsilon)^q$$

Since $(1+(-\varepsilon)) \leq e^{-\varepsilon}$, we obtain

$$\leq q^s \cdot e^{-\varepsilon q}.$$

□

Choose $\varepsilon := \frac{(s \ln q + \ln 2)}{q} \leq \frac{2s \ln q}{q}$.

$$\Rightarrow \Pr(G \in \mathcal{OT}(f)) \leq q^s \cdot e^{-(s \ln q + \ln 2)}$$

$$\leq \frac{1}{2}.$$

By Lemma 4.8

$$\Pr(G \in [C^*] \setminus [C]) \leq 2r^e (\varepsilon \ell)^r.$$

Hence, we obtain

$$1 \leq \frac{1}{2} + t\left(2r^e (\varepsilon \ell)^r\right)$$

$$\Leftrightarrow \quad t \geq \frac{1}{4r^2}\left(\frac{1}{\varepsilon e}\right)^r \geq \frac{1}{4r^2}\left(\frac{q}{2s^2 \ln q}\right)^r.$$

Thus Case 2 is finished. ∎

As an immediate consequence, we obtain the following corollary.

Corollary 4.2

a) For $s \leq \frac{1}{2}\sqrt{\frac{q}{e \ln q}}$ there holds

$$C_{Sum}(\text{POLY}(q,s)) = q^{\Omega(s)}.$$

b) For $s = \frac{1}{2}\sqrt{\frac{q}{e \ln q}}$ there holds

$$C_{Sum}(\text{POLY}(q,s)) = \exp\left(\Omega\left(n^{1/4} \cdot \sqrt{\ln n}\right)\right).$$

Proof: Exercise

To continue at page 167

∎

5. DNF/CNF-approximators

References:

- Armin Haken, Counting bottlenecks to show monotone P ≠ NP, 36th FOCS (1995), 36-40.
- Stasys Jukna, Combinatorics of monotone computations, Combinatorica 19 (1999), 65-85.
- Christer Berg, Staffan Ulfberg, Symmetric approximation arguments for monotone lower bounds without sunflowers, Comput. Complexity 8 (1999), 1-20.
- Kazuyuki Amano, Akira Maruoka, The potential of the approximation method, SIAM J. Comput. 33 (2004), 433-447.

In 1995, Armin Haken has introduced the so-called "bottleneck counting method" to prove an exponential lower bound for the monotone network complexity of a Boolean function which resembles the clique function. Instead of approximating the behaviour of the network directly, he has defined a function μ which maps inputs to the gates of the network. He has shown that the total number of inputs mapped to the gates by μ has to be "large" and also that only "few" inputs are being mapped to each gate. Hence, the network must contain "many" gates.

Shortly after that, Jukna, Berg and Ulfberg and also Amano and Maruoka have observed that Haken's approach is indeed an approximation argument in disguise. They have translated Haken's proof into an approximation proof which uses DNF/CNF-approximators. We shall sketch the ideas of DNF/CNF-approximators. Before doing this, we shall investigate the structures of the functions which are computed at the nodes of a monotone Boolean network β which computes a monotone Boolean function $f \in B_n$.

Let g be any node in β. The function $res_\beta(g)$ can be written as a DNF-formula; i.e.,

$$res_\beta(g) = \bigvee_{j=1}^{t} m_j ,$$

where each m_j is a monomial. Starting at the input nodes of β, we can compute these DNF-formulas by applying the properties of the Boolean operations. We call this representation of $res_\beta(g)$ the <u>DNF-representation</u> $DNF_\beta(g)$ of $res_\beta(g)$.

The function $res_\beta(g)$ can be written as a CNF-formula as well; i.e.,

$$res_\beta(g) = \bigwedge_{j=1}^{s} d_j$$

where each d_j is a clause. We denote this

formula $CNF_\beta(g)$ the <u>CNF-representation</u> of $res_\beta(g)$.

<u>Exercise</u>:
Develop an algorithm which computes for each node g of a given monotone network β $DNF_\beta(g)$ and $CNF_\beta(g)$.

Next we shall characterize $DNF_\beta(g_0)$ where g_0 is the output node of β. Let $p_1, p_2, \ldots, p_r$ be the prime implicants of the function f and let

$$DNF_\beta(g_0) = \bigvee_{j=1}^{t_0} m_j.$$

Then each monomial m_j, $1 \le j \le t_0$ is an implicant of f. Otherwise, $\exists (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ such that

$$f(a_1, a_2, \ldots, a_n) = 0 \text{ but } res_\beta(g_0)(a_1, a_2, \ldots, a_n) = 1.$$

This means that each monomial in $DNF_\beta(g_0)$ contains at least one prime implicant of f.

Moreover, for each prime implicant p_i, $1 \le i \le r$ there is $j \in \{1, 2, \ldots, t_0\}$ with $m_j = p_i$. Otherwise, $\exists (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ such that

$$f(a_1, a_2, \ldots, a_n) = 1 \text{ but } res_\beta(g_0)(a_1, a_2, \ldots, a_n) = 0.$$

Hence, we can restrict our considerations to the prime implicants contained in $DNF_\beta(g_0)$.

Each DNF-formula can be transformed into an equivalent CNF-formula. To see this let

$$\alpha := \bigvee_{i=1}^{t} m_i$$

be a DNF-formula which computes $f \in B_n$. To obtain an equivalent CNF-formula γ, we pick from each monomial m_i, $1 \leq i \leq t$ one literal and perform the disjunction of all chosen literals. Then, the conjunction of all clauses which can be constructed in this way is a CNF-formula

$$\gamma = \bigwedge_{j=1}^{s} d_j$$

which corresponds to the DNF-formula α. We call this transformation a <u>DNF/CNF-switch</u>. Analogously, we can transform a CNF-formula into an equivalent DNF-formula (<u>CNF/DNF-switch</u>).

<u>Exercise</u>:

a) Describe a CNF/DNF-switch.

b) Let α be a DNF-formula (CNF-formula). Prove that the formula γ obtained by a DNF/CNF-switch (CNF/DNF-switch) computes the same function as α.

Now we are prepared to describe DNF/CNF-approximators.

Let $\mathcal{B}$ be a monotone network which computes a function $f \in B_n$. The idea is to approximate

for each node g in β the function $res_\beta(g)$ by two formulas

$$D_g^r = \bigvee_{i=1}^{t_1} m_i \quad \text{and} \quad C_g^k = \bigwedge_{j=1}^{t_2} d_j$$

where each m_i is a monomial of size $< r$ and each d_j is a clause of size $< k$.

The <u>size</u> of a monomial m_i (clause d_j) can be the number of distinct variables in m_i (in d_j) or another measure. The approximators of the nodes in β are defined in the following way:

If the node is an input node x_i then we define

$$C_{x_i}^k := x_i \quad \text{and} \quad D_{x_i}^r := x_i.$$

For the definition of the approximators of the other nodes in β, we consider the nodes in β in any topological order such that always the approximators of both direct predecessors h_1 and h_2 of the considered node g are already defined. Let

$D_{h_1}^r = \bigvee_{i=1}^{t_1'} m_i'$, $C_{h_1}^k = \bigwedge_{j=1}^{t_2'} d_j'$, $D_{h_2}^r = \bigvee_{i=1}^{t_1''} m_i''$ and $C_{h_2}^k = \bigwedge_{j=1}^{t_2''} d_j''$.

According to the type of the node g, we distinguish two cases.

<u>Case 1</u>: g is an $\wedge$-gate.

Then

$$C_g^k := C_{h_1}^k \wedge C_{h_2}^k.$$

Since each clause in $C^k_{u_1}$ and in $C^k_{u_2}$ has size less than k, all clauses in C^k_g have also size less than k.

The approximator D^r_g is constructed from the approximator C^k_g by

- performing a CNF/DNF - switch first obtaining an equivalent DNF-formula $\tilde{D}_g$ and
- removing all monomials of size $\geq r$.

Case 2: g is an $\vee$-gate.

Then $$D^r_g := D^r_{u_1} \vee D^r_{u_2}.$$

Since each monomial in $D^r_{u_1}$ and in $D^r_{u_2}$ has size less than r, all monomials in D^r_g have also size less than r.

The approximator C^k_g is constructed from the approximator D^r_g by

- performing a DNF/CNF - switch first obtaining an equivalent CNF-formula $\tilde{C}_g$ and
- removing all clauses of size $\geq k$.

Next, we shall describe the performance of a CNF\DNF - switch for the case that the size of a monomial or of a clause is the number of different variables in it.

A CNF\DNF- switch can be organized as the construction of a tree T as follows.

(1) Each edge in T is labelled by a variable. With each node w in T we associate the monomial m(w) which is obtained by the conjunction of the variables on the unique path from the root of T to w. T is constructed while expanding $d_0, d_1, d_2, \ldots, d_t$ where d_0 is the empty clause.

(2) While expanding d_0, the root of T is created. The associated monomial is the empty monomial.

(3) Suppose that w is a leaf that was created while expanding d_i. Then the clause d_{i+1} is expanded at the leaf w in the following way: The leaf w obtains for each variable in d_{i+1} which is not contained in m(w) a new son w'. The edge (w,w') is labelled with the corresponding variable.

Remark:

An important property of the construction above is that the size of m(w) is equal the length of the path from the root of T to the node w. No matter what the definition of the size of a monomial or of a clause is, we have to take care that this property holds.

Next we shall analyze the approximator D_g^r where g is an $\wedge$-gate.

Performing a CNF/DNF-switch on C_g^k, a DNF-formula $\tilde{D}_g$ is constructed. In $\tilde{D}_g$, each monomial

m of size $\geq r$ is replaced by zero. For $a \in f^{-1}(1)$, the effect of this replacement on the computation of the value $f(a)$ at the output node g_0 of β is the following.

1) If $m(a) = 0$ then this replacement has no influence to the computation since $m(a)$ and the used value are the same.

2) If $m(a) = 1$ then it is possible that before the replacement, the correct value is computed but after the replacement, $f(a)$ is computed incorrectly.

Since the replacement of a monomial by zero cannot change the computation of a value from zero to one, the replacement of m by zero cannot cause the incorrect computation of $f(b)$ for all $b \in f^{-1}(0)$.

Each monomial m which is replaced by zero contains a submonomial $m(u)$ where u is a node in T with the property that the length of the path from the root of T to u is exactly r. Since the size of each clause d_i, $1 \leq i \leq t$ is at most $k-1$, the number of such nodes in T is $\leq (k-1)^r$.

Analogously, a DNF/CNF-switch can be organized as the construction of a tree T. In the constructed CNF-formula $\tilde{C}_g$, g is an $\vee$-gate, each clause d of size $\geq k$ is replaced by one. For $b \in f^{-1}(0)$,

this can destroy the correct computation of $f(b)$ at the output node g_0 iff $a(b) = 0$. This replacement cannot cause the incorrect computation of $f(a)$ for all $a \in f^{-1}(1)$.

Each clause d which is replaced by one contains a subclause $d(u)$ where u is a node in T such that the length of the path from the root of T to u is exactly k. The number of such nodes is $\leq (r-1)^k$.

Idea:

Choose $T_1 \subseteq f^{-1}(1)$ and $T_0 \subseteq f^{-1}(0)$ such that

a) The number $n_1(T_1, r)$ of inputs a in T_1 with $m(a) = 1$ is "small enough" for all monomials m of size r and $|T_1|$ is "large enough"

b) The number $n_0(T_0, k)$ of inputs $b \in T_0$ with $d(b) = 0$ is "small enough" for all clauses d of size k and $|T_0|$ is "large enough"

$\rightsquigarrow$

1) $(k-1)^r \cdot n_1(T_1, r)$ is an upper bound for the number of inputs a in T_1 such that the correct computation of $f(a)$ at the output node g_0 can be destroyed at an $\wedge$-gate g because of the construction of the approximator D_g^r.

2) $(r-1)^k \cdot n_0(T_0, k)$ is an upper bound for the number of inputs b in T_0 such that the correct computation of $f(b)$ at the output node g_0 can be destroyed at an $\vee$-gate g because of the construction of the approximator C_g^k.

Next we shall characterize $C_{g_0}^k$. In dependence of its structure, we distinguish two cases.

Case 1: $C_{g_0}^k$ is the constant function 1.

Then the correct computation of $f(b)$ $\forall\, b \in T_0$ has been destroyed during the approximation

$\Rightarrow$ A lower bound of $\frac{|T_0|}{(r-1)^k \cdot n_0(T_0, k)}$ for $C_{\Omega_m}(f)$.

Case 2: $C_{g_0}^k$ is not the constant function 1.

Then $C_{g_0}^k$ contains a clause d of size $\leq k-1$. Let $N(T_1, var)$ be an upper bound for the number of inputs a in T_1 such that

$$x_\ell(a) = 1$$

for any given variable x_ℓ.

For at most

$$(k-1) \cdot N(T_1, var)$$

inputs $a \in T_1$, the value $f(a)$ can be computed correctly at the output node g_0.

$\Rightarrow$

A lower bound of $\frac{|T_1| - (k-1)\, N(T_1, var)}{(k-1)^r \cdot n_1(T_1, r)}$ for $C_{\Omega_m}(f)$.

A monotone function $f \in B_n$ which allow the use of DNF/CNF-approximators to prove a large lower bound for $C_{\mathcal{L}_m}(f)$ must have the following properties:

- It can be chosen appropriate $T_1 \subseteq f^{-1}(1)$, $T_0 \subseteq f^{-1}(0)$, r and k such that
  1) $|T_1|$ and $|T_0|$ are large,
  2) $n_1(T_1, r)$ and $n_0(T_0, k)$ are small,
  3) $N(T_1, var)$ is small enough such that $|T_1| - (k-1) N(T_1, var)$ is large.

Jukna, Berg and Ulfberg and also Amano and Maruoka have used DNF/CNF-approximators to prove exponential lower bounds for the monotone complexity of the clique function and few other functions. Exemplary, we shall treat Berg and Ulfberg's lower bound proof for the clique function CLIQUE(m,s).

Remember that CLIQUE(m,s) is the Boolean function of $n := \binom{m}{2}$ variables representing the edges of an undirected graph $G = (V, E)$ on m nodes. CLIQUE(m,s) = 1 iff the corresponding graph G contains a clique of size s. In the subsequence, f denotes the function CLIQUE(m,s).

First, we shall spezify the size of a monomial and the size of a clause. We say that a monomial m or a clause d <u>touchs</u> a node $v \in V$ iff

there is at least one variable in m or in d which corresponds to an edge in E with end node v. The <u>size of a monomial m</u> is the number of different nodes touched by m. For the definition of the size of a clause d, we consider the graph $G(d) := (V, E(d))$ where $E(d)$ contains exactly those edges which correspond to the variables in d. The <u>size of the clause d</u> is m minus the number of connected components in $G(d)$.

For the approximators D_g^r and C_g^k, we use the values

$$r := \lfloor \sqrt{s} \rfloor \quad \text{and} \quad k := \left\lfloor \frac{m}{8s} \right\rfloor .$$

Since $r = \lfloor \sqrt{s} \rfloor$, less than $\lfloor \sqrt{s} \rfloor$ different nodes in V can be touched by a monomial in D_g^r. Hence, the number of variables in such a monomial is bounded by $\frac{r^2}{2} \leq \frac{s}{2}$.

$k = \lfloor \frac{m}{8s} \rfloor$ implies that a graph corresponding to a clause in C_g^k has more than $m - \lfloor \frac{m}{8s} \rfloor$ connected components. If we mark in each connected component one node, less than $\lfloor \frac{m}{8s} \rfloor$ nodes remain unmarked. The number of different end nodes of the edges in such a graph is maximized if the number of connected components with exactly two nodes is maximized. Therefore, we obtain the maximum number of different end nodes if the unmarked nodes are

distributed to pairwise different connected components. Hence, the number of different end nodes of the edges in such a graph is less than

$$2k \leq \frac{m}{4s}.$$

$\Rightarrow$

A clause d in C_8^k touches less than $\frac{m}{4s}$ nodes in V.

Next, we shall define appropriate $T_1 \subseteq f^{-1}(1)$ and $T_0 \subseteq f^{-1}(0)$. For an implicant m of f, the input $I(m)$ is defined by.

$$I_1(m) := \{ a \in \{0,1\}^n \mid a_i = 1 \text{ if } m \leq a_i \text{ and } a_i = 0 \text{ otherwise} \}.$$

This means that $I(m)$ assigns the value one to a variable x_i iff x_i is contained in m.

For an f-clause d of f, the input $I_0(d)$ is defined by

$$I_0(d) := \{ b \in \{0,1\}^n \mid b_i = 0 \text{ iff } x_i \text{ is contained in } d \}.$$

Then we set

$$T_1 := \{ I_1(p) \mid p \in PIM(f) \}.$$

For the definition of T_0, we consider colourings $h: V \to \{1, 2, \ldots, s-1\}$ of the nodes in V by $s-1$ colours. The graph

$$G(h) := (V, E(h))$$

corresponding to the colouring h contains all edges between two nodes in different colour classes and no edge between two nodes in the same colour class.

$\Rightarrow$

$G(h)$ is a complete ℓ-partite graph where $\ell \in \{1, 2, \ldots, s-1\}$ is the number of colours used by h.

The clause $d(h)$ corresponding to the colouring h contains exactly those variables x_{uv} with both nodes u and v are coloured with the same colour; i.e., $h(u) = h(v)$.

$\ell \leq s-1 \Rightarrow$

Each s-clique must contain at least two nodes which are in the same colour class.

$\Rightarrow$ $d(h)$ is an f-clause.

Now we are prepared to define T_0.

$$T_0 := \{ I_0(d(h)) \mid h: V \to \{0, 1, \ldots, s-1\} \text{ is a colouring of } V. \}.$$

Next we shall adapt the CNF/DNF- and DNF/CNF-switches such that the length of the paths from the root to the nodes in T is equal to the size of the corresponding monomial and clause, respectively.

CNF/DNF - Switch:

Let $d_1, d_2, \dots, d_t$ be the clauses in C_g^k given in any fixed order and let d_0 be the empty clause. Assume that w is a leaf which was created while expanding d_i.

Treatment of d_{i+1} w.r.t. w:

We call a variable x_{uv} tight for a monomial m iff both end nodes u and v are touched by m. We distinguish two cases.

Case 1: d_{i+1} contains a variable x_{uv} which is tight for $m(w)$.

For each $a \in T_1$ which satisfies $m(w)$, both nodes u and v have to be contained in the clique which corresponds to a.

$$\Rightarrow \quad x_{uv}(a) = 1$$

We create only one son w' for w and label the edge (w, w') with x_{uv}.

Case 2: d_{i+1} contains no variable which is tight for $m(w)$.

Then the variables in d_{i+1} separates into the following two sets:

$$Var_0 := \{ x_{uv} \mid \text{both end nodes } u \text{ and } v \text{ are not touched by } m(w) \}.$$

$Var_1 := \{ x_{uv} \mid$ exactly one of u and v is touched by $m(w) \}$.

First, we shall consider the variables in Var_1. Let

$$V' := \{ u \in V \mid u \text{ is not touched by } m(w) \text{ but } \exists\, x_{uv} \in Var_1 \}.$$

For each $u \in V'$ let

$$N(u) := \{ v \in V \mid x_{uv} \in Var_1 \}.$$

For each $u \in V'$, we choose any $v \in N(u)$ and create a son w_u of the node w. The edge (w, w_u) is labelled with the variable x_{uv} and we define that the edge (w, w_u) is touched by the node u.

This suffices since two monomials touching the same nodes are submonomials of the same prime implicants of the clique function. Since d_{i+1} touches less than $2k$ nodes, less than

$$2k \leq \frac{m}{4s}$$

sons are created.

Now we shall consider the variables in Var_0. As long as there is an edge corresponding to a variable in Var_0 such that none of its two end nodes is chosen, we choose an end node u of such an edge and create a son w'_u for w.

The corresponding edge (w, w'_u) obtains no label. We define that the edge (w, w'_u) is touched by the node u. Since d_{i+1} touches less than $2k$ nodes, less than

$$2k \leq \frac{m}{4s}$$

sons are created. Let

$$V'' := \{ u \in V \mid w'_u \text{ is created} \}$$

and for each $u \in V''$ let

$$N'(u) := \{ v \in V \mid x_{uv} \in Var_0 \}.$$

For each $u \in V''$ for each $v \in N'(u)$, we create a son w''_v of the node w'_u and label the edge (w'_u, w''_v) with the variable x_{uv}. We define that the node v touches the edge (w'_u, w''_v). Again, since d_{i+1} touches less than $2k$ nodes, less than

$$2k \leq \frac{m}{4s}$$

sons for w'_u are created.

After the construction of T, the monomials corresponding to the paths from the root of T to the leaves are the monomials in $\tilde{D}_g$.

Exercise:

Show that the number of inputs in T_1 for which the approximator D_g^r could introduce an error is bounded by $\binom{m-r}{s-r}\left(\frac{m}{4s}\right)^r$.

DNF/CNF-switch:

Let $m_1, m_2, \ldots, m_t$ be the monomials in D_g^r given in any fixed order and let m_0 be the empty monomial. Suppose that w is a leaf which was created while expanding m_i.

Treatment of m_{i+1} w.r.t w:

A variable x_{uv} in m_{i+1} is called good iff both end nodes of the edge (u,v) are contained in the same connected component of the graph

$$G(d(w)) = (V, E(d(w))).$$

By construction, each input $b \in T_0$ which falsifies $d(w)$ has the property that each connected component of $G(d(w))$ is contained in one colour class with respect to the colouring h where $b = I_0(d(h))$.

$\Rightarrow$ b must falsify each good variable as well.

We distinguish two cases:

Case 1: m_{i+1} contains a good variable x_{uv}.

Since each input $b \in T_0$ which falsifies $d(w)$ also falsifies the variable x_{uv}, $b_{uv} = 0$.

$\Rightarrow$

It suffices to create one son w' of w and to label the edge (w,w') with x_{uv}.

Case 2: m_{i+1} contains no good variable

Then each variable x_{uv} in m_{i+1} connects two connected components of $G(d(w))$. The leaf w obtains for each variable x_{uv} in m_{i+1} a new son w'. The edge (w,w') is labelled with the variable x_{uv}.

By construction, when decending on an edge to a son from a node with more than one son, the number of connected components of the associated graph decreases by one.

$\Rightarrow$

The size of the corresponding clause increases by one.

$\Rightarrow$

There are $\leq k$ such nodes on a path from the root to a node with the property that the corresponding clause has exactly size k. Since each monomial in D_g^r contains $\leq \frac{s}{2}$ variables, each node in T has at most degree $\frac{s}{2}$.

$\Rightarrow$

$$\leq \left(\frac{s}{2}\right)^k$$

nodes in T with the corresponding clause has exactly size k exists.

Note that different colorings can yield the same input in T_0. For counting properties,

it would be simpler to consider such inputs as different. Then $|T_0| = (s-1)^m$.

Exercise

Show that the number of inputs in T_0 for which the approximator $C^k_{8/k}$ could introduce an error is bounded by $\left(\frac{s}{2}\right)^{8/k} \cdot (s-1)^{m-k}$.

Exercise:

Show that either $C^k_{8\cdot}$ computes the constant function 1 or $C^k_{8\cdot}$ computes the value of at least half of the inputs in T_1 incorrectly.

Altogether, we obtain the following theorem.

Theorem 5.1

Let $s \leq m^{2/3}$. Then $C_{\Sigma_m}(CLIQUE(m,s)) \geq 2^{\Omega(\sqrt{s})}$.

Proof: Exercise. ∎

6. From monotone to non-monotone complexity.

References:

- Norbert Blum, On negations in Boolean networks, in Albers S., Alt H., Näher S. (eds.), Efficient Algorithms: Essays Dedicated to Kurt Mehlhorn on the Occasion of His 60th Birthday, LNCS 5760 (2009), 13-18.

- Alexander A. Razborov, Steven Rudich, Natural proofs, JCSS 55 (1997), 24-35.