6. Razborov - approximators

References:

- Alexander A. Razborov, Lower bounds on the monotone complexity of individual monotone functions, Soviet Math. Dokl. 31 (1985), 530 - 534.

- Alexander A. Razborov, Lower bounds 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.

- Stasys Jukna, Boolean Function Complexity: Advances and Frontiers, Springer, 2012, Ch. 9.

To bound the number of minimal monomials which could be removed during the construction of an approximator, Razborov has defined a new ingenious closure operation. He has used this operation for the definition of closed sets wich contain only few minimal elements. The idea is to take care that an approximator always corresponds to a closed set.

We call an approximator which uses Razborov's closure operation Razborov - approximator.

Razborov-approximators are much more complicated than CNF-DNF-approximators. But the properties which a Boolean function f must have to get a large lower bound for its monotone complexity using the method are different.

Both methods need the following property.

<u>P1</u>: Only "few" inputs in $f^{-1}(1)$ fulfill a monomial of size larger than r.

The properties P2 and P3 needed if we use CNF-DNF-approximators are replaced by two other properties $\underline{P2'}$ and P3' if we use Razborov-approximators. Therefore, the sets of functions for which the application of the methods results into a large lower bound for the monotone complexity may be different.

<u>Remark</u>:
With respect to the perfect matching function, we know a proof of a super-polynomial lower bound which uses Razborov-approximators, but no such a proof which uses CNF-DNF-approximators is known.

Moreover, the expandability to non-monotone Boolean networks may be different. Hence, the investigation of Razborov-approximators is of interest.

First of all, we will investigate closed sets.

6.1 Closed sets an their use for proving a lower bound

First we define Razborov's closure operation and closed sets.

Let $\mathcal{F}$ be the power set of a finite set $\mathcal{X}$ of n elements and let ℓ and r be two parameters where $2 \leq \ell, r < n$. $\mathcal{F}_\ell \subset \mathcal{F}$ denotes that sub=set of $\mathcal{F}$ which contains exactly the sets of size at most ℓ. Note that the empty set is in $\mathcal{F}_\ell$. Let $W, W_1, W_2, \ldots, W_r \in \mathcal{F}_\ell$ and $A \subseteq \mathcal{F}_\ell$. Then we de=fine:

not necessarily different

a) $W_1, W_2, \ldots, W_r$ <u>imply</u> W ($W_1, W_2, \ldots, W_r \vdash W$) iff $W_i \cap W_j \subseteq W$ for $1 \leq i < j \leq r$.

b) A <u>implies</u> W ($A \vdash W$) iff $\exists W_1, W_2, \ldots, W_r \in A$: $W_1, W_2, \ldots, W_r \vdash W$.

c) A is <u>closed</u> iff $\forall W \in \mathcal{F}_\ell : A \vdash W \Rightarrow W \in A$.

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

$$A^* := \bigcap \{ B \mid A \subseteq B \subseteq \mathcal{F}_\ell \text{ and } B \text{ is closed} \}.$$

Next we will investigate some combinatorial pro=perties concerning the structure of closed sets.

$C \in A$ is called <u>minimal</u> iff for all $D \in A$ there holds $D \not\subset C$. The following lemma shows that closed systems contain only "few" minimal sets.

Lemma 6.1

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

Proof:

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

$\nexists$ $W, W_1, W_2, \dots, W_r \in \mathfrak{A}$ and $U \subset W$ such that $W_i \cap W_j \subseteq U \ \forall \ 1 \leq i < j \leq r$ (i.e., $\mathfrak{A} \vdash U$).

Note that the system of all minimal sets of A of cardinality $\leq k$ 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 $\mathfrak{A}$ 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 $W_1, W_2 \in \mathfrak{A}$, $W_1 \neq W_2$. Let

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

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

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

$\Longrightarrow$
$$W, W_1, W_2 \in \mathfrak{A}, \quad U \subset W \text{ such that } W_1 \cap W_2 \subseteq U.$$

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

Assume that the assertion holds for $r-1$.

<u>$r-1 \rightsquigarrow r$</u>:

Let $\mathfrak{A}$ be a system having property $P(r,k)$ and let $D \in \mathfrak{A}$. For all $C \subseteq D$ define
$$\mathfrak{A}_C := \{ W \setminus C \mid W \in \mathfrak{A} \text{ and } W \cap D = C \}.$$

<u>Claim 2:</u>

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

<u>Proof:</u>

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

Choose
$$W', W_1', W_2', \dots, W_{r-1}' \in \mathfrak{A}_C, \quad U' \subset W'$$
such that
$$W_i' \cap W_j' \subseteq U' \quad \text{for } 1 \leq i < j \leq r-1.$$

Let
$$W := W' \cup C \quad \in \mathfrak{A}$$
$$U := U' \cup C \quad \subset W$$

$W_i := W_i' \cup C \quad \in \mathfrak{A} \quad$ for $1 \le i \le r-1$

$W_r := D \quad \in \mathfrak{A}$

Note that

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

$\Longrightarrow$

$\mathfrak{A}$ has not property $P(r,k)$, a contradiction.

$\square$

By the induction hypothesis

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

Since $D \in \mathfrak{A}$ is chosen fixed, the condition

$$C = W \cap D$$

is fulfilled for only one set C.

Note that

$(W \cap D = C = \tilde{W} \cap D$ and $W \ne \tilde{W}) \Rightarrow W \setminus C \ne \tilde{W} \setminus C$.

$\Longrightarrow$

$$\begin{aligned}
|\mathfrak{A}| &= \sum_{C \subseteq D} |\mathfrak{A}_C| \\
&\le \sum_{C \subseteq D} (r-2)^{k-|C|} \\
&= \sum_{i=0}^{|D|} \binom{|D|}{i} (r-2)^{k-i} \\
&\underset{\text{since } |D| \le k}{\le} \sum_{i=0}^{k} \binom{k}{i} (r-2)^{k-i} \\
&\underset{\text{binomial Theorem}}{=} (r-1)^k.
\end{aligned}$$

Given a system $C \subset \mathcal{F}_e$, the question is how to construct its closure C^*. Let

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

Then

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

The following algorithm improves C with respect to its closure C^*

<u>Algorithm</u> IMPROVECLOSURE

<u>Input:</u> $C \subset C^*$

<u>Output:</u> D such that $C \subset D \subseteq C^*$

<u>Method:</u>

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

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

This algorithm can be repeated until $C' = \emptyset$. Since $W \in \mathcal{F}_e$, the number of improvement steps is bounded by $|\mathcal{F}_e| \leq n^e$. The following lemma improves this upper bound.

<u>Lemma 6.2</u>

The number of improvement steps, applied to a system $C \subset \mathcal{F}_e$ until C^* is obtained, is at most $2 \cdot r^e$.

<u>Proof:</u>

Let $S := (W_1, W_2, \ldots, W_p)$ be a sequence of distinct sets. We say that S has <u>property $T(r,\ell)$</u> if

i) $|W_i| \leq \ell$ for $1 \leq i \leq p$, and
ii) $\nexists$ $i_1 \leq i_2 \leq \ldots \leq i_r < i_{r+1}$ and $U \subset W_{i_{r+1}}$ such that
$$W_{i_j} \cap W_{i_h} \subseteq U \quad \text{for } 1 \leq j < h \leq r$$
(i.e., $W_{i_1}, W_{i_2}, \ldots, W_{i_r} \vdash U$).

If $S = (W_1, W_2, \ldots, W_p)$ 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 $W_{i_{r+1}}$ at the moment when it has been chosen.

$\Longrightarrow$

To prove the lemma, it suffices to prove:

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

<u>Proof</u>: (by induction on r)

<u>$r = 1$</u>: (then $2r^\ell = 2$).

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

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

a) $W_2 \neq \emptyset$

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

b) $W_3 \neq \emptyset$

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

This proves the claim for $r = 1$.

Assume that the assertion holds for $r-1$.

$\underline{r-1 \rightsquigarrow r}$:

Let
$$D := W_1.$$
For each $C \subseteq D$ define

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

Claim 2:

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

Proof:

Assume that S_C has not property $T(r-1, e-|C|)$.
Choose
$$i_1 \leq i_2 \leq \ldots \leq i_{r-1} < i_r \quad \text{and} \quad U' \subset W_{i_r}'$$
such that

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

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

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

where

$$\begin{aligned} i_j' &:= i_j \quad \text{for } 1 \leq j \leq r-1, \\ i_r' &:= i_{r-1}, \\ i_{r+1}' &:= i_r, \quad \text{and} \\ U &:= U' \cup C. \end{aligned}$$

Obviously, $W_{i_j'} \cap W_{i_h'} \subseteq U$ for $1 \leq j < h \leq r$.

$\Rightarrow$

S has not property $T(r,e)$, a contradiction.

$\square$

By the induction hypothesis

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

Since D is chosen fixed, the condition

$$W_i \cap D = C$$

is fulfilled for exactly one set C.

$\Rightarrow$

$$|S| = \sum_{C \subseteq D} |S_C|$$

$$\leq 2 \cdot \sum_{i=0}^{|D|} \binom{|D|}{i} (r-1)^{e-i}$$

$$\underset{|D|\le \ell}{\le} \; 2 \cdot \sum_{i=0}^{\ell} \binom{\ell}{i} (r-1)^{\ell-i}$$

$$\underset{\substack{\text{binomial}\\ \text{Theorem}}}{=} \; 2\, r^{\ell}$$

■

Now we will show how to used closed systems in a lower bound proof for the size of a monotone Boolean network β which computes a given Boolean function f. Closed systems are used to bound the number of minimal monomials which could be removed during the construction of an approximator.

Let $g_1, g_2, \ldots, g_t$ be the nodes of a monotone Boolean network β computing a function $f \in \mathbb{B}_n$ in any topological order. Instead of approximating $DNF_\beta(g_i)$ directly, the set of types of the monomials contained in $DNF_\beta(g)$ is approximated. For doing this, Razborov's closure operation is used where $\mathcal{K}$ is the set of elements used for the definition of the type of the monomials. Then, in dependence of the set of types obtained after the approximation, $DNF'_\beta(g_i)$ is defined.

Let α be a DNF-formula. Then

$$T(\alpha) := \{ T(m) \mid m \text{ is a monomial in } \alpha \}$$

is the set of types of the monomials in α.

For a node g_i in β, $T(g_i)$ denotes the set of types used for the definition of $DNF'_\beta(g_i)$.

We consider only the case that for each type $\mathcal{B} \in T(g_i)$ exactly one monomial $m_{\mathcal{B}}$ is contained in $DNF'_\beta(g_i)$. For the definition of $DNF'_\beta(g_i)$, we have to define this monomial for each type $\mathcal{B} \in T(g_i)$.

Razborov's closure operation is used to bound the number of minimal sets in $T(g_i)$ and therefore the number of minimal monomials in $DNF'_\beta(g_i)$.

Now we will describe the approximation of the sets of types corresponding to the nodes in β. We assume that β is simplified; i.e., for all input nodes g_i, $op_i \notin \{0,1\}$. Starting at the input nodes, we consider the nodes in β in topological order. In dependence of the approximators corresponding to the direct predecessors g_{i_1} and g_{i_2} of g_i and the operation op_i of g_i, we define the approximator $T(g_i)$; i.e., we determine a closed set $A_i \subseteq F_\ell$ and define

$$T(g_i) := A_i.$$

Then we use $T(g_i)$ for the definition of the approximator $DNF'_\beta(g_i)$ of $DNF_\beta(g_i)$. We distinguish three cases.

Case 1: $op(g_i) = x_j$, $j \in \{1, 2, \dots, n\}$

Then we define A_i to be a closed set which contains $T(x_j)$.

For example, if the type of a monomial m is the set of variables contained in m; i.e., $\mathcal{K} = V_n$ then

$$A_i := \{ B \in \mathcal{F}_e \mid x_j \in B \}.$$

If the type of a monomial m is the set of nodes touched by m; i.e., $\mathcal{K} = V$ and the nodes $v, w \in V$ are the two nodes touched by x_j then

$$A_i := \{ B \in \mathcal{F}_e \mid v, w \in B \}.$$

In both examples, the definition of A_i implies that A_i is closed.

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

Let $A_{i_1} = T(g_{i_1})$ and $A_{i_2} = T(g_{i_2})$. Since the union of closed sets must not be closed, we define

$$A_i := (A_{i_1} \cup A_{i_2})^*.$$

By construction, A_i is closed.

Case 3: g_i is an $\wedge$-gate.

Then we define

$$A_i := A_{i_1} \cap A_{i_2}.$$

Since the intersection of closed sets is closed, the set A_i is also closed.

Given $T(g_i)$, we describe the definition of $DNF'_\beta(g_i)$. For each type $B \in T(g_i)$, a monomial m_B is defined. With respect to the definition of m_B, we have some latitude as long as the union property of the types of the monomials is maintained. The union property implies for $B, B' \in F_e$

$$B \subseteq B' \text{ iff } m_B \subseteq m_{B'}.$$

Hence, for the definition of $DNF'_\beta(g_i)$, we can restrict us to the minimal sets in A_i. We define

$$DNF'_\beta(y_i) := \bigvee_{B \in A_i \text{ minimal}} m_B.$$

The other elements of A_i can be considered as the set of all possible extensions of the minimal sets in A_i such that the corresponding set has size at most l.

Now we define m_B for the v-type and the n-type of monomials. Let

$$m_B := \begin{cases} \bigwedge_{x_z \in B} x_z & \text{if } B \text{ v-type and } |B| > 0, \\ \bigwedge_{h,k \in B,\, h \neq k} x_{hk} & \text{if } B \text{ n-type and } |B| > 1, \\ \varepsilon & \text{if } |B| = 0 \text{ or } |B| = 1 \text{ and } B \text{ n-type.} \end{cases}$$

Next we relate the construction of the approximator and the general idea as described in Section 4.

- Since for an input node g_i there holds
$$DNF'_B(g_i) = DNF_B(g_i),$$
the approximators for the input nodes do not introduce any error.

- If g_i is an $\wedge$-gate then before the approximation
$$DNF_B(g_i) = \bigvee_{B \in A_{i_1},\, C \in A_{i_2}} m_B m_C .$$
Since A_{i_1} and A_{i_2} are closed sets,
$$|B \cup C| \leq \ell \text{ implies } B \cup C \in A_{i_1} \cap A_{i_2}$$
$\Longrightarrow$
$$DNF'_B(g_i) = \bigvee_{B \in A_{i_1} \cap A_{i_2} \text{ minimal}} m_B$$
would be also obtained after the construction of $DNF_B(g_i)$ followed by the removal of all monomials of size larger than ℓ and all monomials $m_B m_C = m_{B \cup C}$ where $B \cup C$ is not a minimal set in $A_{i_1} \cap A_{i_2}$.

This is exactly the obvious way as described in Section 4 where we restrict us to minimal monomials with the additional property that A_{i_1} and A_{i_2} are closed.

Because of this additional property, we can apply Lemma 6.1 to obtain an upper bound for the number of minimal monomials removed because of the construction of the approximator.

Since no monomial is added to $DNF_\beta(g_t)$, only for $c \in f^{-1}(1)$, an error could be introduced because before the approximation, $DNF_\beta(g_t)$ contains a monomial m_c which is fulfilled by the input c but after the approximation, no such a monomial in $DNF_\beta(g_t)$ exists.

For $A \subseteq F_e$, we define

$$M(A) := \bigcup_{B \in A \text{ minimal}} m_B.$$

The following lemma describes a property for an input $c \in f^{-1}(1)$ for which an error is introduced because of the approximation of $DNF_\beta(g_i)$ where g_i is an $\wedge$-gate.

Lemma 6.3

Let g_i be an $\wedge$-gate, g_{i_1} and g_{i_2} its direct predecessors and $c \in f^{-1}(1)$ be an input for which an error is introduced because of the approximation of $DNF_\beta(g_i)$. Then $M(A_{i_1})$ or $M(A_{i_2})$ contains a monomial of size at least $\lceil \frac{e+1}{2} \rceil$ which is satisfied by the input c.

Proof:

Since the replacement of $DNF_B(g_i)$ by $DNF'_B(g_i)$ introduces an error for the input $c \in f^{-1}(1)$, before the replacement, $DNF_B(g_t)$ contains a mono= mial m_c which is fulfilled by c but which is not contained in $DNF_B(g_t)$ after the replace= ment.

$\Rightarrow$

$\exists\ m_1 \in M(A_{i_1}),\ m_2 \in M(A_{i_2})$ with

$$m_1 m_2 \subseteq m_c \quad \text{but} \quad m_1 m_2 \notin M(A_i).$$

By construction, $m_1 \neq m_2$.

Since A_{i_1} and A_{i_2} are closed sets, the size of the monomial $m_1 m_2$ is at least $\ell+1$. Otherwise, $m_1 m_2 \in M(A_{i_1} \cap A_{i_2})$ and hence, $m_1 m_2 \in M(A_i)$.

Hence, because of the union property, at least one of the monomials m_1 and m_2 has size at least

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

∎

- To take care that the constructed approximators always correspond to a closed subset of F_ℓ, we have to add some monomials during the construc= tion of the approximator corresponding to an $\vee$-gate g_i. But using Lemma 6.2, we can bound the number of minimal monomials added during the approximation. Adding monomials to a DNF-formula yields the introduction of errors only with respect to inputs in $f^{-1}(0)$.

6.2 Applications

We will use Razborov-approximators to prove exponential lower bounds for the monotone complexity of the clique function and of Andreev's function. We consider the clique function first.

Let $f := \mathrm{CLIQUE}(m,s)$. Again, we will use the following subsets $T_1 \subseteq f^{-1}(1)$ and $T_0 \subseteq f^{-1}(0)$.

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

$$T_0 := \{ I_0(d(h)) \mid h : V \to \{1,2,\dots,s-1\} \text{ is a colouring} \}.$$

The lower bound proof uses Lemma 6.3 and the fact that only "few" inputs in T_1 fulfill a monomial of size at least $\lceil \frac{e+1}{2} \rceil$.

Observation:

A node set of size $k < s$ is contained in $\binom{m-k}{s-k}$ s-cliques.

$\Longrightarrow$

The number of inputs $c \in T_1$ fulfilling a monomial of size k is at most $\binom{m-k}{s-k}$.

With respect to the inputs in T_0 for which an error could be introduced at an $\vee$-gate, we will use a probablistic argument. More precisely, we consider random colourings of the node set V with g colours. Let h be such a colouring. We say that $W \subseteq V$ is <u>properly coloured</u> (<u>pc</u> for short) by h if each node in W has a different colour. The following lemma gives an upper bound of the probability that a random g-colouring h of the node set V properly colours W but does not properly colour any nodes set in A where $A \vdash W$.

<u>Lemma 6.4</u>

Suppose that $A \subseteq F_\ell$ where $\mathcal{K} = V$ and that $A \vdash W$. Let h be a random g-colouring of V. Then

$$Pr[W \text{ is pc and no set in } A \text{ is pc by } h]$$
$$\leq \left(1 - \frac{g(g-1)\cdot\ldots\cdot(g-\ell+1)}{g^\ell}\right)^r.$$

<u>Proof</u>:

Since $A \vdash W$ there are $W_1, W_2, \ldots, W_r \in A$ such that

$$W_1, W_2, \ldots, W_r \vdash W.$$

Let E and E_i, respectively be the event that W and W_i, respectively is pc by h. Let CE_i be the complementary event of E_i.

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

$\Rightarrow$

W pc implies that the events $CE_1, CE_2, \dots, CE_r$ are independent.

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

Pr [W is pc and no set in A is pc by h]

$$\le Pr\left(E \cap \bigcap_{i=1}^{r} CE_i\right) \le Pr\left(\bigcap_{i=1}^{r} CE_i \;\middle|\; E\right)$$

$$= \prod_{i=1}^{r} Pr(CE_i \mid E)$$

$$= \prod_{i=1}^{r} \left(1 - Pr(E_i \mid E)\right)$$

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

$$Pr(E_i \mid E) \geq \frac{g(g-1)\cdot \ldots \cdot (g-\ell+1)}{g^\ell}.$$

For doing this let

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

Then

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

The even 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

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

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

This proves the lemma.

∎

Our goal is now to bound the probability that an error is introduced for a random input $b \in T_0$. Since for each $b \in T_0$ there exists a coulouring h such that $b = I_0(d(h))$, we shall consider random colourings of the node set V.

At an $\vee$-gate g_i

$$A_i := (A_{i_1} \cup A_{i_2})^*$$

is constructed. Let

$$C := A_{i_1} \cup A_{i_2}.$$

By Lemma 6.2, $A_i := C^*$ is constructed from C by the application of $p \le 2r^{\ell}$ improvement steps. Let

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

be the results of the steps in this construction. Let B_i be the chosen set for the construction of C_i from C_{i-1}, $1 \le i \le p$.

Let $g \geq \ell$ and h be a random colouring of the node set V with g colours.

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

The construction of C_i from C_{i-1}, $1 \leq i \leq p$ introduces an error with respect to the input

$$b := I_0(d(h))$$

iff a set in C_i is pc but no set in C_{i-1} is pc.

$\Leftrightarrow$ B_i is pc but no set in C_{i-1} is pc by h.

By construction, $C_{i-1} \vdash B_i$.

Lemma 6.4 $\Rightarrow$

$$\Pr(B_i \text{ is pc and no set in } C_{i-1} \text{ is pc by } h)$$
$$\leq \left(1 - \frac{g(g-1)\cdot\ldots\cdot(g-\ell+1)}{g^\ell}\right)^r$$

Applying this to each improvement step proves the following lemma.

<u>Lemma 6.5</u>

Let $C \subseteq V(\ell)$, $g \geq \ell$ and h be a random colouring of the node set V with g colours. Then the probability that replacing C by C^* introduces an error with respect to $I_0(d(h))$ is at most

$$2r^\ell \left[1 - \frac{g(g-1)\cdot\ldots\cdot(g-\ell+1)}{g^\ell}\right]^r.$$

Now we are prepared to prove the lower bound.

Theorem 6.1

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

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

Proof:

Let $f = \text{CLIQUE}(m,s)$ and $\beta = g_1, g_2, \dots, g_t$ be a monotone Boolean network computing f at the output node g_t.

We distinguish two cases.

Case 1: $DNF'_\beta(g_t)$ does not compute the constant function one.

We consider the inputs in T_1. Each such an input corresponds to a graph which contain exactly the edges of an s-clique and each such a graph corresponds to an input in T_1. The assertion follows directly from the following two claims

Claim 1:

$DNF'_\beta(g_t)$ computes for at most the half of the $\binom{m}{s}$ inputs in T_1 the value 1.

Claim 2:

At an $\wedge$-gate g_i for at most
$$4 \cdot \left(\frac{s(r-1)}{m}\right)^{\lceil \frac{e+1}{2} \rceil} \cdot \binom{m}{s}$$
inputs in T_1, an error is introduced by $DNF'_\beta(g_i)$.

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

Proof of Claim 1:

By construction
$$DNF'_\beta(g_t) = \bigvee_{B \in A_t \text{ minimal}} m_B$$

where
$$m_B = \begin{cases} \bigwedge_{u,k \in B} x_{uk} & \text{if } |B| > 1 \\ \varepsilon & \text{if } |B| \leq 1. \end{cases}$$

Since the empty monomial is the constant function one, each minimal set in A_t has at least size two.

Each input $a \in T_1$ with $DNF'_\beta(g_t)(a) = 1$ satisfies a monomial m_B with $B \in A_t$ minimal; i.e., the corresponding s-clique contains a clique on B.

Lemma 6.1 $\Rightarrow$

For $2 \le k \le \ell$, the number of minimal sets of size k is

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

Each of these sets is contained in exactly

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

s-cliques.

Hence, the total number of inputs $\alpha \in T_1$ with $DNF'_\beta(g_t)(\alpha) = 1$ is bounded by

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

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

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

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

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

$\square$

Proof of Claim 2:

Assume that g_{i_1} and g_{i_2} are the direct predecessors of the $\wedge$-gate g_i.

Lemma 6.3 $\Rightarrow$

For each input $a \in T_1$ for which $DNF'_{\mathcal{B}}(g_i)$ introduces an error, $M(A_{i_1})$ or $M(A_{i_2})$ contains a monomial $m_{\mathcal{B}}$ of size at least $\lceil \frac{\ell+1}{2} \rceil$ which is satisfied by the input a. By construction, $\mathcal{B}$ is a minimal set of A_{i_1} or of A_{i_2}. This implies that the s-clique corresponding to the input a contains the node set $\mathcal{B}$.

$\Longrightarrow$

The total number of inputs in T_1 for which an error is introduced by $DNF'_{\mathcal{B}}(g_i)$ is

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

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

$$< 2 \binom{m}{s} \cdot \left(\frac{s(r-1)}{m} \right)^{\lceil \frac{\ell+1}{2} \rceil} \cdot \sum_{j=0}^{\infty} \left(\frac{1}{2} \right)^j$$

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

$\square$

<u>Case 2</u>: $DNF'_{\mathcal{B}}(g_t)$ computes the constant function one.

Then for each input $b \in T_0$, the value is correctly computed by $DNF'_{\mathcal{B}}(g_t)$.

Let h be a random $(s-1)$-colouring of the node set V. Let g_i be an v-gate in β.

$$\Pr\left(\mathrm{DNF}'_{\beta}(g_i) \text{ introduce an error w.r.t. } I_0(d(h))\right)$$

$$\leq 2r^{\ell}\left(1-\frac{(s-1)(s-2)\cdots(s-\ell)}{(s-1)^{\ell}}\right)^{r}$$

$$< m^{\ell}\left(1-\frac{(s-1)(s-2)\cdots(s-\ell)}{(s-1)^{\ell}}\right)^{r}$$

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

$$\leq m^{\ell}\left(1-\left(1-\frac{\ell-1}{s-1}\right)^{\ell-1}\right)^{r}$$

Bernoulli inequality

$$\leq m^{\ell}\left(1-\left(1-(\ell-1)\frac{\ell-1}{s-1}\right)\right)^{r}$$

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

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

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

Hence, we obtain

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

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

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

Therefore the probability that an error w.r.t. $I_0(d(h))$ is introduced at any v-gate in β is

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

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

$$t \cdot m^{-\sqrt{s}} < 1.$$

$\Rightarrow$ There is at least one input in T_0 for which no error has been introduced at any v-gate of β, a contradiction.

$\Rightarrow$

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

■

Corollary 6.1

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

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

Alon and Boppana have used Razborov approximators to improve Andreev's lower bound for the function POLY(q,s) from $2^{\Omega(n^{1/8}/\sqrt{\ln n})}$ to $2^{\Omega(n^{1/4}\cdot\sqrt{\ln n})}$.

Now we will present this proof within our framework. In the subsequence, f denotes the function POLY(q,s). Remember that the input corresponds to a bipartite graph $G=(A,B,E)$ where $A = GF(q)$ and $B = GF(q)$. We identify the variable x_{ij} and the edge (i,j).

The size of a monomial is its length. Therefore we use $\mathcal{K} := A \times B$ for the definition of the closure operation.

First, we will prove some combinatorial lemmas used in the lower bound proof.

Lemma 6.6

Let $G = (A, B, E)$ be a random bipartite graph in which each edge appears independently with probability $1-\varepsilon$. Suppose $\mathcal{A} \subseteq \mathcal{F}_\ell$ and $\mathcal{A} \vdash W$. Then

$$\Pr(W \subseteq E \text{ and no set in } \mathcal{A} \text{ is contained in } E)$$

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

Proof:

$$\mathcal{A} \vdash W \Rightarrow \exists W_1, W_2, \dots, W_r \in \mathcal{A} : W_1, W_2, \dots, W_r \vdash W.$$

Hence,

$$\Pr(W \subseteq E \text{ and no set in } \mathcal{A} \text{ is contained in } E)$$

$$\leq \Pr(W_i \not\subseteq E, 1 \leq i \leq r \mid W \subseteq E)$$

By the definition of $\vdash$, the events $\{W_i \subseteq E \mid W \subseteq E\}$ are independent. Hence,

$$= \prod_{i=1}^{r} \Pr(W_i \subseteq E \mid W \subseteq E).$$

Furthermore,

$$\Pr(W_i \not\subseteq E \mid W \subseteq E) = 1 - (1-\varepsilon)^{|W_i \setminus W|}$$
$$\leq 1 - (1-\varepsilon)^{\ell}.$$

Hence,

$\Pr($ $W \subseteq E$ and no set in A is contained in E $)$

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

Bernoulli's inequality $\Rightarrow$

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

$\Rightarrow$

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

and hence,

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

∎

<u>Lemma 6.7</u>

Let $G = (A, B, E)$ be a random bipartite graph in which each edge appears independently with probability $1-\varepsilon$. Suppose $C \subseteq \mathcal{F}_\ell$. Then

$\Pr($ $\exists W \in C^*$: $W \subseteq E$ and no set in C is contained in E $)$

$$\leq 2 r^{\ell} (\varepsilon \ell)^{r}$$

<u>Proof</u>:

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

Lemma 6.2 $\Rightarrow$

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

Let

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

be the results of the improvement steps in this construction. For $1 \leq i \leq p$ let

$$W_i \in \{ W \in C_{i-1} \mid C_{i-1} \vdash W \}$$

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

Lemma 6.6 $\Rightarrow$

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

Altogether,

$$\Pr (\exists W \in C^* : W \subseteq E \text{ and no set in } C \text{ is contained in } E)$$

$$\leq \sum_{i=1}^{p} \Pr (W_i \subseteq E \text{ and no set in } C_{i-1} \text{ is contained in } E \}$$

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

∎

Now we are prepared to prove the lower bound.

<u>Theorem 6.2</u>

Let $\ell = s$ and $2 \leq r \leq \frac{q}{3} + 1$. Then

$$C_{\Omega_m}(\mathrm{POLY}(q,s)) \geq \min \left\{ \frac{1}{2} \left(\frac{q}{r-1} \right)^{s/2} , \frac{1}{4r^\ell} \cdot \left(\frac{q}{2s^2 \ln q} \right)^r \right\}.$$

Proof:

Let $\beta = g_1, g_2, \ldots, g_t$ be a monotone Boolean network which computes $f = \mathrm{POLY}(q, s)$ at its output node g_t.

We distinguish two cases:

Case 1: $\mathrm{DNF}'_\beta(g_t)$ does not compute the constant function one.

Again, we use

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

The assertion follows directly from the following two claims.

Claim 1:

$\mathrm{DNF}'_\beta(g_t)$ computes for at most the half of the q^s inputs in T_1 the value 1.

Claim 2:

At an $\wedge$-gate g_i, for at most

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

inputs in T_1, an error is introduced by $\mathrm{DNF}'_\beta(g_i)$.

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:

By construction

$$DNF'_\beta(g_t) = \bigvee_{B \in A_t \text{ minimal}} m_B$$

where

$$m_B = \begin{cases} \bigwedge_{(h,k) \in B} x_{hk} & \text{if } |B| > 0 \\ \varepsilon & \text{if } |B| = 0 \end{cases}$$

Since the empty monomial is the constant function one, each minimal set in A_t has at least the cardinality one.

Lemma 6.1 $\Rightarrow$

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

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

Each of these is contained in either precisely 0 or presisely q^{s-k} graphs corresponding to polynomials of degree at most $s-1$.

Hence, the total number of inputs $a \in T_1$ with $DNF'_\beta(g_t)(a) = 1$ is bounded by

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

$$\le q^s \sum_{k=1}^{l} \left(\frac{1}{3}\right)^k < \frac{1}{2} q^s.$$

$\square$

Proof of Claim 2:

Assume that g_{i_1} and g_{i_2} are the direct predecessors of the $\wedge$-gate g_i.

Lemma 6.3 $\Longrightarrow$

For each input $a \in T_1$ for which $DNF'_\beta(g_i)$ introduces an error, $M(A_{i_1})$ or $M(A_{i_2})$ contains a monomial m_β of size $\geq \lceil \frac{e+1}{2} \rceil$ which is satisfied by the input a. This implies that the bipartite graph corresponding to the input a contains the edge set B. By construction, B is a minimal set of A'_{i_1} or of A'_{i_2}.

$\Longrightarrow$

The total number of inputs in T_1 for which an error is introduced by $DNF'_\beta(g_i)$ is

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

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

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

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

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

$\square$

<u>Case 2</u>: $DNF'_\beta(g_t)$ computes the constant function one.

We call the graphs corresponding to the prime implicants of f <u>polynomial graphs</u>. Let $G(f)$ denotes the set of graphs corresponding to the inputs in $f^{-1}(1)$. Then each graph in $G(f)$ contains at least one of the polynomial graphs as a subgraph.

Let $G=(A,B,E)$ be a random bipartite graph in which each edge appears independently with probability $1-\varepsilon$.

<u>Claim 3</u>: $\Pr(G \in G(f)) \leq q^s(1-\varepsilon)^q \leq q^s e^{-\varepsilon q}$.

<u>Proof of claim 3</u>:

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.

$\Longrightarrow$

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

$$\leq (1-\varepsilon)^q$$

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

$\Longrightarrow$

$$\Rightarrow \quad Pr\big(G \in G(f)\big) \le q^s (1-\varepsilon)^q$$

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

$$\le q^s e^{-\varepsilon q}.$$

$\square$

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

$\Rightarrow$

(*) $Pr(G \in G(f)) \le q^s \, e^{-(s \ln q + \ln 2)} = \frac{1}{2}.$

By Lemma 6.7

$Pr(\exists W \in C^*: W \subseteq E$ and no set in C is contained in $E)$
$\le 2r^e (\varepsilon e)^r.$

$\Rightarrow$

At an $\vee$-gate g_i, the probability that a monomial is added to $DNF'_\beta(g_i)$ which is satisfied by the input corresponding to G is

$$\le 2r^e(\varepsilon e)^r.$$

(*) $\Rightarrow$

The probability that G corresponds to an input in $f^{-1}(0)$ is $\ge \frac{1}{2}$.

Hence, we obtain

$$1 \le \frac{1}{2} + t \cdot (2r^e(\varepsilon e)^r)$$

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

As an immediate consequence, we obtain the following corollary.

Corollary 6.2

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

$$C_{\Omega_m}(\mathrm{POLY}(q,s)) = q^{\Omega(s)}.$$

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

$$C_{\Omega_m}(\mathrm{POLY}(q,s)) = \exp(\Omega(n^{1/4}\cdot\sqrt{\ln n})).$$

Proof:

Exercise

■

7. 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), 18-19.
- Alexander A. Razborov, Steven Rudich, Natural proofs, JCSS 55 (1997), 24-35.