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.

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

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

For a function $f \in M_n$ let

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

Note that

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

Furthermore, for $f, g \in M_n$

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

$$A(f \wedge g) = A(f) \cap A(g).$$

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

- each input x_i, $1 \leq i \leq n$ by $A(x_i)$,
- 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 $A(f)$.

Idea (Razborov):

Replace in β' the 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 $A(f)$ but an approximation of $A(f)$.

Given the two operations $\sqcap$ and $\sqcup$, we define the <u>legitimate model</u> S to be the smallest subset of $\mathcal{P}(\{0,1\}^n)$ such that

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

ii) S is closed under the operations $\sqcap$ and $\sqcup$.

For $M, N \in S$ let

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

$$\delta_{\sqcap}(M,N) := (M \cap N) \setminus (M \sqcap N).$$

<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 model S we define the <u>distance</u> $p(f,S)$ from f to S to be the minimal t such that there are

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

such that

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

and

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

Theorem 4.1

Let $f \in M_n$ and $(S, \cup, \sqcap)$ be a legitimate model. 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 a topological order.

Consider the network β' which we obtain from β by replacing each $\vee$ by $\sqcup$, each $\wedge$ by $\sqcap$ each 0 by $A(0)$ and each 1 by $A(1)$.

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 gate of β'.

Claim:

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

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

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

$t > 0$:

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 $\Rightarrow$

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

and

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

Furthermore,

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

and

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

Hence we obtain

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

and

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

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 function $f \in NP$.

(1) Choose an approbriate legitimate model $(S, \Gamma, \cup)$.
(2) Prove a lower bound for the distance $\rho(f, S)$ from f to S.

How we should choose a model $(S, \Gamma, \cup)$ such that we can prove a large lower bound for $\rho(f, S)$ where the function f is given?

The chosen model $(S, \Gamma, \cup)$ should depend on the function f whose monotone complexity we like to estimate. S should not contain a "good" approximation of $A(f)$ and the δ-sets should be "small". Furthermore, S should only contain sets M such that $A(f) \setminus M$ or $M \setminus A(f)$ is large.

In the subsequence, we shall consider the clique function

$$cl_{n,k} \in M_N$$

where $N = \binom{n}{2}$ and $cl_{n,k}$ is defined on the variables $x_{i,j}$, $1 \leq i < j \leq n$; i.e.,

$$cl_{n,k} : \{0,1\}^N \longrightarrow \{0,1\}$$

where

$$cl_{n,k}(x) = 1$$

iff the graph $G = (V, E)$ with $V := \{1, 2, \ldots, n\}$ and $E := \{(i,j) \mid x_{i,j} = 1\}$

contains a clique of size k.

Goal:

Construction of a legitimate model $(S, \sqcap, \sqcup)$ such that an exponential lower bound for $\rho(\mathcal{CL}_{n,k}, S)$ can be proved with respect to an appropriate k.

Definition of $(S, \sqcap, \sqcup)$:

Let $\ell \geq 2$, $r \geq 2$ and $V := \{1, 2, \ldots, n\}$. Let

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

be the set of all subsets of size $\leq \ell$ of V.

Consider $W, W_1, W_2, \ldots, W_r \in V(\ell)$ (not necessarily different). Then we say

- $W_1, W_2, \ldots, W_r$ imply W $(W_1, W_2, \ldots, W_r \vdash W)$ iff

$$W_i \cap W_j \subseteq W \quad \text{for } 1 \leq i < j \leq r.$$

- $A \subseteq V(\ell)$ implies W $(A \vdash W)$ iff

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

- $A \subseteq V(\ell)$ is closed iff

$\forall\, W \in V(\ell) : A \vdash W \Rightarrow W \in A.$

- For $A \subseteq V(\ell)$, A^* denotes the closure of A; i.e.

$$A^* := \bigcap \{ B \mid A \subseteq B \subseteq V(\ell) \text{ and } B \text{ is closed} \}.$$

Lemma 4.1

Let $A \subseteq V(e)$. Then

a) A^* is closed.

b) $A \subseteq A^*$.

c) $(A^*)^* = A^*$.

d) $A \subseteq B \subseteq V(e) \Rightarrow A^* \subseteq B^*$.

Proof:

Exercise ∎

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

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

Now we define $(S, \sqcap, \sqcup)$ in the following way:

- $S := S(n, \Gamma, e)$
  $:= \emptyset \cup \{ \lceil A \rceil \mid A \subseteq V(e) \text{ is closed} \}$.
- $\lceil A \rceil \sqcap \lceil B \rceil := \lceil A \cap B \rceil$ and
- $\lceil A \rceil \sqcup \lceil B \rceil := \lceil (A \cup B)^* \rceil$.

We identify graphs $G = (V, E)$, $V = \{1, 2, \dots, n\}$ and vectors in $\{0,1\}^N$, $N = \binom{n}{2}$ as described above.

Lemma 4.2

$(S, \sqcap, \sqcup)$ is a legitimate model.

Proof:

- By definition $A(0) = \emptyset \in S$
- Obviously, $V(\epsilon)$ is closed. Moreover, $\emptyset \in V(\epsilon)$

$$\Rightarrow$$

$$A(1) = \{0,1\}^N = \lceil V(\epsilon) \rceil \in S.$$

- Let

$$F_{i,j} := \{ w \in V(\epsilon) \mid i,j \in w \}$$

Definition of $F_{i,j}$ $\Rightarrow$ $F_{i,j}$ is closed.

Furthermore,

$$A(x_{i,j}) = \lceil F_{i,j} \rceil.$$

Definition of S $\Rightarrow$ $\lceil F_{i,j} \rceil \in S$

Hence, $A(x_{i,j}) \in S$ for $1 \leq i < j \leq n$.

It remains to show that S is closed under the operations $\sqcap$ and $\sqcup$.

Claim 1:

$\forall \lceil A \rceil, \lceil B \rceil \in S$ there hold

- $\lceil A \rceil \sqcap \lceil B \rceil$ is well-defined and
- $\lceil A \rceil \sqcap \lceil B \rceil \subseteq \lceil A \rceil \cap \lceil B \rceil$.

Proof:

Let $A, B \subseteq V(\epsilon)$ closed; i.e., $\lceil A \rceil, \lceil B \rceil \in S$

Definition of $\sqcap \Rightarrow$

$$\ulcorner A \urcorner \sqcap \ulcorner B \urcorner = \ulcorner A \wedge B \urcorner.$$

We have to show that $\ulcorner A \wedge B \urcorner \in \mathcal{S}$; i.e., $A \wedge B$ is closed. For showing this consider $W \in V(e)$ with $A \wedge B \vdash W$.

Note that

$$A \wedge B \vdash W \Rightarrow (A \vdash W \text{ and } B \vdash W).$$

Since A and B are closed, it follows

$$W \in A \text{ and } W \in B$$

$$\Rightarrow$$

$$W \in A \wedge B.$$

This proves that $A \wedge B$ is closed and hence,

$$\ulcorner A \urcorner \sqcap \ulcorner B \urcorner = \ulcorner A \wedge B \urcorner \in \mathcal{S}.$$

Consider

$$G \in \ulcorner A \urcorner \sqcap \ulcorner B \urcorner = \ulcorner A \wedge B \urcorner$$

$\Rightarrow$ G contains a clique w.r.t $W \in A \wedge B$.

Hence, $G \in \ulcorner A \urcorner$ and $G \in \ulcorner B \urcorner$.

$\Rightarrow$

$$G \in \ulcorner A \urcorner \cap \ulcorner B \urcorner.$$

This proves $\ulcorner A \urcorner \sqcap \ulcorner B \urcorner \subseteq \ulcorner A \urcorner \cap \ulcorner B \urcorner$.

Claim 2:

$\forall \lceil A \rceil, \lceil B \rceil \in \mathcal{S}$ there hold.

- $\lceil A \rceil \sqcup \lceil B \rceil$ is well-defined and $\lceil A \rceil \cup \lceil B \rceil \subseteq \lceil A \rceil \sqcup \lceil B \rceil$.

Proof:

exercise.

∎

Next we shall investigate the structure of closed sets. Consider $A \subseteq V(e)$ closed. Then the following is fulfilled.

$$B \in A \Rightarrow B' \in A \ \forall B' \text{ with } |B'| \leq e \text{ and } B' \supseteq B$$

This observation allows us to describe closed systems using their minimal sets.

$B \in A$ is called <u>minimal</u> if for all $C \in A$ $C \not\subset B$.

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 $A \subseteq V(e)$ 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 $U \subsetneq W$ such that $W_i \cap W_j \subseteq U \quad \forall\ i \neq j$.

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 $\mathcal{F}$ 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

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

such that

$$W_i' \cap W_j' \subseteq U' \quad \text{for } i \neq j.$$

Let

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

Note that

$$C \subseteq D, \quad W_i \cap W_j \subseteq U \text{ for } i \neq j.$$

$\Rightarrow$

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

By the induction hypothesis

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

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

$$C = W \cap D$$

is fulfilled for only one set C.

Note that

$$(W \cap D = C = W' \cap D \text{ and } W \neq W') \Rightarrow W \setminus C \neq W' \setminus C$$

$\Rightarrow$

$$|\widetilde{\mathcal{F}}| = \sum_{C \subseteq D} |\widetilde{\mathcal{F}}_C|$$

$$\leq \sum_{C \subseteq D} (r-2)^{k-|C|}$$

$$= \sum_{i=0}^{|D|} \binom{|D|}{i} (r-2)^{k-i}$$

$$\underset{\text{since } |D| \leq k}{\leq} \sum_{i=0}^{k} \binom{k}{i} (r-2)^{k-i}$$

$$\underset{\text{binomial Theorem}}{=} (r-1)^k$$

■

To estimate the $\delta_\sqcap$-sets in the case that $|M|$ 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,

$$\delta_\sqcup(\ulcorner A \urcorner, \ulcorner B \urcorner) = \ulcorner (A \cup B)^* \urcorner \setminus \ulcorner A \urcorner \cup \ulcorner B \urcorner$$

$$= \ulcorner (A \cup B)^* \urcorner \setminus \ulcorner \underbrace{A \cup B}_{C} \urcorner$$

$$= \ulcorner C^* \urcorner \setminus \ulcorner C \urcorner.$$

Given C how to construct C^* ?

Let

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

Hence

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

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

Algorithm IMPROVECLOSURE

Input: $C \subsetneq C^*$

Output: $\mathcal{B}$ such that $C \subsetneq \mathcal{B} \subseteq C^*$ and $\mathcal{B}^* = C^*$

Method:

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

(2) $\mathcal{B} := C \cup \{ W' \in V(e) \mid W \subseteq W' \}$

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

Since $W \in V(e)$, the number of improvement steps is bounded by

$$|V(e)| \leq n^e.$$

This upper bound may be improved to

$$e! (r+1)^e$$

but this is not necessary for our purposes.

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

$$h: V \longrightarrow \{1, 2, \ldots, k-1\}$$

of the nodes such that the following is fulfilled

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

A complete $(k-1)$-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 are not able to specify a complete $(k-1)$-partite graph which can be used for the proof of the lower bound. But we can show that such a graph exists. To prove the existence we shall use a probabilistic argument.

We consider randomly chosen complete g-partite graphs or equivalent random colourings of the node set V with g colours. Assume that we have the uniform distribution on all g^n colourings of V where $|V| = n$.

Lemma 4.4

Let $g \geq \ell$, $A \subseteq V(\ell)$, $W, W_1, W_2, \ldots, W_r \in A$ and $W_1, W_2, \ldots, W_r \vdash W$. Let E and E_i, respectively be the event that W and W_i, respectively is 'properly coloured. Let CE_i be the complementary event of E_i. Then

$$\Pr(E \wedge CE_1 \wedge CE_2 \wedge \ldots \wedge CE_r) \leq \left[1 - \frac{g(g-1)\ldots(g-\ell+1)}{g^\ell}\right]^r.$$

Proof:

Note that $W_i \wedge W_j \subseteq W$ for $1 \leq i \neq j \leq r$.

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

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

$$\Pr(E \wedge CE_1 \wedge CE_2 \wedge \ldots \wedge CE_r) \leq \Pr(CE_1 \wedge CE_2 \wedge \ldots \wedge E_r \mid E)$$

$$= \prod_{1 \le i \le r} Pr(\overline{E_i} \mid E)$$

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

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

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

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 $W \setminus W_i$ are coloured with $q(i)$ different other colours is

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

$$\geq \prod_{0 \le j < \ell} \frac{q-j}{q} = \frac{q(q-1) \cdot \ldots \cdot (q-\ell+1)}{q^\ell}.$$

This proves the lemma.

∎

Lemma 4.5

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

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

Proof:

The algorithm IMPROVECLOSURE constructs C^* from C in at most n^ℓ steps.

Let

$$C = C_0, C_1, C_2, \ldots, C_p = C^* \qquad 0 \leq p \leq n^\ell$$

be the results of the steps in this construction.

It suffices to prove

$$Pr(G(h) \in \lceil C_i \rceil \setminus \lceil C_{i-1} \rceil) \leq \left(1 - \frac{g(g-1)\cdot\ldots\cdot(g-\ell+1)}{g^\ell}\right)^{\binom{\ell}{2}}.$$

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

$G(h)$ contains a clique on 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.

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., $B_1, B_2, \ldots, B_r \vdash W_i$ for sets $B_j \in C_{i-1}$, $1 \leq j \leq r$ that

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

The probability for this event has been upper bounded by Lemma 4.4.

∎

Lemma 4.5 gives us a useful bound for the probability that a random $\ldots (k-1)$-partite graph is in some δ_u-set. Now we are prepared to prove the lower bound.

Theorem 4.2

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

$$c\ell_{n,k} \geq \frac{1}{8} \cdot \left[\frac{n}{k(r-1)}\right]^{\lceil \frac{e+1}{2} \rceil}.$$

Proof:

Because of Theorem 4.1 it suffices to prove

$$\rho(cl_{n,k}, S(n,r,\ell)) \geq \frac{1}{8}\left[\frac{n}{k(r-1)}\right]^{\left\lceil\frac{\ell+1}{2}\right\rceil}.$$

Let

$$t := \rho(cl_{n,k}, \underbrace{S(n,r,\ell)}_{S})$$

and let

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

such that

$$A(cl_{n,k}) \subseteq M \cup \bigcup_{i=1}^{t} \delta_\Pi(M_i, N_i)$$

and

$$M \subseteq A(cl_{n,k}) \cup \bigcup_{i=1}^{t} \delta_\sqcup(M_i, N_i).$$

The definition of S implies that

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

such that

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

We distinguish two cases.

Case 1:

M is not the set of all graphs.

We consider those $\binom{n}{k}$ graphs which contain exactly the edges of a k-clique. These are exactly those graphs which correspond to the prime implicants of the function $cl_{n,k}$.

The assertion follows directly from the following two claims.

Claim 1:

M contains at most $\frac{1}{2} \cdot \binom{n}{k}$ of these graphs (k-cliques).

Claim 2:

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

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

k-cliques.

Note that

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

Proof of Claim 1:

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

$\Rightarrow$

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

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

Lemma 4.3 $\Rightarrow$

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

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

Each of those elements is contained in exact

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

k-cliques.

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

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

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

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

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

$$< \frac{1}{2}\binom{n}{k}$$

□

Proof of claim 2:

Definition $\Rightarrow$

$$\begin{aligned}\delta_{\sqcap}(M_i, N_i) &= (M_i \sqcap N_i) \setminus (M_i \sqcap N_i) \\ &= \left(\lceil A_i \rceil \cap \lceil B_i \rceil\right) \setminus \lceil A_i \cap B_i \rceil\end{aligned}$$

If a k-clique on node set Z is contained in $\delta_{\sqcap}(M_i, N_i)$ 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 $A_i \sqcap B_i$.

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

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

Hence, at least one of the both sets U and W contains

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

elements.

Hence, we obtain for the total number TN of k-cliques in $\delta_{\sqcap}(M_i, N_i)$

$$\begin{aligned}TN &\leq 2 \cdot \sum_{s=\lceil \frac{\ell+1}{2} \rceil}^{\ell} (r-1)^s \binom{n-s}{k-s} \\ &\leq 2\binom{n}{k} \cdot \sum_{s=\lceil \frac{\ell+1}{2} \rceil}^{\ell} \left(\frac{k(r-1)}{n}\right)^s\end{aligned}$$

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

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

□

Case 2:

M is the set of all graphs.

Note that no complete $(k-1)$-partite graph is contained in $A(cl_{n,k})$. Hence, all these graphs have to be contained in

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

Definition $\Rightarrow$

$$\delta_{\sqcup}(M_i, N_i) = (M_i \sqcup N_i) \setminus (M_i \cup N_i)$$

$$= \lceil (A_i \cup B_i)^* \rceil \setminus \lceil \underbrace{A_i \cup B_i}_{C_i} \rceil$$

$$= \lceil C_i^* \rceil \setminus \lceil C_i \rceil .$$

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

Lemma 4.5 $\Rightarrow$

$$Pr\left(G(h) \in \lceil C_i^* \rceil \setminus \lceil C_i \rceil\right)$$

$$\leq n^{\ell} \cdot \left(1 - \frac{(k-1)(k-2)\cdot\ldots\cdot(k-\ell)}{(k-1)^{\ell}}\right)^{r}.$$

$$= n^{\ell}\left(1 - 1\cdot\left(1-\tfrac{1}{k-1}\right)\left(1-\tfrac{2}{k-1}\right)\cdots\left(1-\tfrac{\ell-1}{k-1}\right)\right)^{\Gamma}$$

$$\leq n^{\ell}\left(1-\left(1-\tfrac{\ell-1}{k-1}\right)^{\ell-1}\right)^{\Gamma}$$

$$< n^{\ell}\left(1-\left(1-(\ell-1)\tfrac{\ell-1}{k-1}\right)\right)^{\Gamma}$$

Bernoulli inequality

$$= n^{\ell}\left(\frac{(\ell-1)^2}{k-1}\right)^{\Gamma}$$

Because of $\ell = \Gamma \frac{1}{2}\sqrt{k}\,\urcorner$ we obtain

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

Hence, we obtain

$$< n^{\ell}\cdot\left(\tfrac{1}{4}\right)^{\Gamma}$$

$$= n^{\Gamma\frac{1}{2}\sqrt{k}\urcorner}\cdot 2^{-2\cdot\lceil 4\sqrt{k}\cdot\lg n\rceil}$$

$$< n^{-\sqrt{k}}.$$

Hence, we obtain

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

$$\leq t\cdot n^{-\sqrt{k}}$$

For $t < \frac{1}{8}\left(\frac{n}{k(r-1)}\right)^{\Gamma\frac{\ell+1}{2}\urcorner} < n^{\sqrt{k}}$ there holds

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

$\Rightarrow$

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

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

a contradiction.

$\Rightarrow$

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

∎

Corollary 4.1

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

$$C_{\Omega_m}(cl_{n,k}) = \exp\left(\Omega\left(\left(\frac{n}{\log n}\right)^{\frac{1}{3}}\right)\right).$$

Remark:

In the proof of the lower bound, the structure of an optimal Ω_m-network is not used. Especially, we do not start with the sets $A(0), A(1), A(x_1), A(x_2), \ldots, A(x_n) \in S$ and the other used elements of the legitimate model are induced by the optimal Ω_m-network under consideration.