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

$$\sigma_1(f) := \{ a \in \{0,1\}^n \mid f(a) = 1 \}.$$

Note that

$$\sigma_1(0) = \emptyset \quad \text{and} \quad \sigma_1(1) = \{0,1\}^n.$$

Furthermore, for $f, g \in B_n$

$$\sigma_1(f \vee g) = \sigma_1(f) \cup \sigma_1(g) \quad \text{and}$$

$$\sigma_1(f \wedge g) = \sigma_1(f) \wedge \sigma_1(g).$$

Given any monotone Boolean network β for a function $f \in M_n$, we obtain a network β' which computes $\sigma_1(f)$ if we replace

- each input x_i, $1 \leq i \leq n$ by $\sigma_1(x_i)$,
- 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 $\sigma_1(f)$.

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 $\sigma_1(f)$ but an approximation of $\sigma_1(f)$.

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

i) $\sigma_1(0), \sigma_1(1), \sigma_1(x_1), \sigma_1(x_2), \ldots, \sigma_1(x_n) \in S$ and

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

iii) $M \sqcap N \subseteq M \cap N$ and $M \cup N \subseteq M \sqcup N$. $\forall M, N \in S$.

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 lattice 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

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

and

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

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:

$$o_1(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_\sqcap(M_i, N_i) \quad \text{and}$$

$$M \subseteq o_1(f) \cup \bigcup_{i=1}^{t} \delta_\sqcup(M_i, N_i).$$

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 $o_1(f) \in S$.

$t > 0$:

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 $\Rightarrow$

$$M_t \subseteq o_1(f_t) \cup \bigcup_{i=1}^{t-1} \delta_\sqcup(M_i, N_i)$$

and

$$N_t \subseteq o_1(h_t) \cup \bigcup_{i=1}^{t-1} \delta_\sqcup(M_i, N_i).$$

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 $\delta(f, S)$ from f to S.

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

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

To get these properties, Razborov defined a class of legitimate lattices based on the prime implicant structure of any given monotone function and a new clever "closure" operation. We shall develop Razborov's method for any $f \in M_n$.

Let $r \geq 2$ and $\ell \geq 1$ be natural numbers. Then we define

$$U_\ell(f) := \{ m \mid m \text{ monomial with } |m| \leq \ell \text{ and } \exists p \in PI(f) : p \leq m \}$$

This means that $U_\ell(f)$ contains exactly the submonomials of length $\leq \ell$ of the prime implicants of f.

In the subsequence, we also identify a monomial as the set of variables defining it such that the intersection and the union of monomials are defined.

Consider $W, W_1, W_2, \ldots, W_r \in U_e(f)$ (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
  $W_i \cap W_j \subseteq W$ for $1 \leq i < j \leq r$.
- $A \subseteq U_e(f)$ implies W ($A \vdash W$) iff
  $\exists W_1, W_2, \ldots, W_r \in A : W_1, W_2, \ldots, W_r \vdash W$.
- $A \subseteq U_e(f)$ is closed iff
  $\forall W \in U_e(f) : A \vdash W \Rightarrow W \in A$.
- For $A \subseteq U_e(f)$, A^* denotes the closure of A; i.e.,
  $A^* := \bigcap \{B \mid A \subseteq B \subseteq U_e(f) \text{ and } B \text{ is closed}\}$.

06.06.

Lemma 4.1

Let $A \subseteq U_e(f)$. Then

a) A^* is closed,

b) $A \subseteq A^*$,

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

d) $A \subseteq B \subseteq U_e(f) \Rightarrow A^* \subseteq B^*$.

Proof:

Exercise

For $A \subseteq U_e(f)$ we define

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

Assume that the Boolean function $f \in M_n$ depends on each variable $x_i \in V_n$.

$\Rightarrow$

$\forall x_i \in V_n \; \exists p \in PIM(f) : p \leq x_i$.

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

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

Lemma 4.2: $(S, \sqcap, \sqcup)$ is a legitimate lattice.

Proof:

- By definition, $\sigma(0) = \emptyset \in S$.
- Obviously, $U_e(f)$ is closed. Moreover, $\emptyset \in U_e(f)$

  $\Rightarrow$

  $\sigma(1) = \sigma(\emptyset) = \{0,1\}^n = \lceil U_e(f) \rceil \in S$.
- Let

  $$A_i := \{w \in U_e(f) \mid x_i \in w\}.$$

  Definition of $A_i \Rightarrow A_i$ is closed.

  Furthermore, $\sigma(x_i) = \lceil A_i \rceil$.

Definition of $S \Rightarrow \lceil A_i \rceil \in S$.

Hence, $\sigma(x_i) \in S$ for $1 \leq i \leq n$.

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 $A, B \subseteq U_e(f)$ closed; i.e., $\lceil A \rceil, \lceil B \rceil \in S$.

Definition of $\sqcap \Rightarrow$

$$\lceil A \rceil \sqcap \lceil B \rceil = \lceil A \cap B \rceil.$$

We have to show that $\lceil A \cap B \rceil \in S$; i.e., $A \cap B$ is closed. For doing this consider $W \in U_e(f)$ with $A \cap B \vdash W$.

Note that

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

Since A and B are closed, it follows

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

$$\Rightarrow$$

$$W \in A \cap B.$$

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

$$\lceil A \rceil \sqcap \lceil B \rceil = \lceil A \cap B \rceil \in S.$$

Consider

$$a = (a_1, a_2, \ldots, a_n) \in \lceil A \rceil \sqcap \lceil B \rceil = \lceil A \cap B \rceil.$$

$\Rightarrow$

$\exists\, W \in A \cap B,\ p \in PIM(f)$:

$p \leq W$ and $p(a) = 1$.

$\Rightarrow \quad W(a) = 1$

Hence, $a \in \lceil A \rceil$ and $a \in \lceil B \rceil$.

$\Rightarrow \quad a \in \lceil A \rceil \cap \lceil B \rceil.$

This proves $\lceil A \rceil \sqcap \lceil B \rceil \subseteq \lceil A \rceil \cap \lceil B \rceil$. □

Claim 2:

$\forall\, \lceil A \rceil, \lceil B \rceil \in S$ 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 $A \subseteq U_e(f)$. Then the following

is fulfilled.

$C \in A \Rightarrow D \in A$ for all D with $|D| \leq \ell$ and $C \subseteq D$.

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

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

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.

<u>Lemma 4.3</u>

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

<u>Proof</u>:

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

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

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 $\mathcal{F}$ 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

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

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

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

$\Rightarrow$

$$|\widehat{\mathcal{F}}| = \sum_{C \in D} |\widehat{\mathcal{F}}_C|$$

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

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

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

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

■

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

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

Then

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

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

Algorithm IMPROVECLOSURE

Input: $C \subseteq C^*$.

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

Method:

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

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

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

Since $W \in U_\ell(f)$, the number of improvement steps is bounded by $|U_\ell(f)| \leq n^\ell$.

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 $2 r^\ell$.

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) $\nexists\ i_1 \leq i_2 \leq \dots \leq i_r < i_{r+1}$ and $U \subset W_{i_{r+1}}$ 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 $W_{i_{r+1}}$ when it was 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 $W_i' := W_i \setminus C$ 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

$$i'_1 \leq i'_2 \leq \ldots \leq i'_r < i'_{r+1} \text{ and } U \subseteq W_{i'_{r+1}}$$

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.

$\Rightarrow$

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

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

since $|D| \leq \ell$

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

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 correspond to the edge (i,j). We shall identify the edge (i,j) and the variable x_{ij}.

The submonomials of the prime implicants used in the lower bound proof are cliques on a node set of bounded size. Hence, instead of $U_\ell(f)$, we use

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

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

For $A \subseteq V(\ell)$ 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 define the lattice $(S, \sqcap, \sqcup)$ exactly in the same way as done with respect to $U_\ell(f)$.

Since the lemmas 4.1, 4.2, 4.3 and 4.4 do not depend on the interpretation of $U_\ell(f)$ and $\lceil A \rceil$, they also hold with respect to $V(\ell)$ and $\lceil A \rceil$ defined above.

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.

A $(s-1)$-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

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

of the nodes such that the following is fulfilled:

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

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 approbriate g. To prove the existence of such a graph having a certain probserty, we shall use a probabilistic argument. This means that we consides 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

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

<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 $1 \le i \le r$

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

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

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

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

This proves the lemma. ∎

Lemma 4.6

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

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

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

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

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 δ_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

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

Proof:

By Theorem 4.1, it suffices to prove

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

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

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

Consider

$$M, M_1, N_1, M_2, N_2, \ldots, M_t, N_t \in \binom{S}{\ell}$$

such that

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

and

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

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

The definition of S implies that

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

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

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

s-cliques.

Note that

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

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 $\Rightarrow$

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

$$\begin{aligned}
&\sum_{k=2}^{\ell} (r-1)^k \cdot \binom{m-k}{s-k} \\
&\le \sum_{k=2}^{\ell} (r-1)^k \binom{m}{s} \cdot \left(\frac{s}{m}\right)^k \\
&= \binom{m}{s} \cdot \sum_{k=2}^{\ell} \left(\frac{s(r-1)}{m}\right)^k \\
&\le \binom{m}{s} \cdot \sum_{k=2}^{\ell} \left(\frac{1}{2}\right)^k \\
&< \frac{1}{2} \binom{m}{s}.
\end{aligned}$$

□

Proof of Claim 2:

Definition $\Rightarrow$

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

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 $\delta_\Pi(M_i, N_i)$

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

□

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 $\Rightarrow$

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

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

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

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, we obtain

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

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

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

$\Rightarrow$

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.

$\Rightarrow$

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

■

Corollary 4.1

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

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

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