Lower bounds using communication complexity

Grigory Yaroslavtsev

Academic Physics and Technology University

6 April, 2009

Outline

LK sequent calculus

Connectives of the propositional language:

- Constants 0, 1
- The conjunction $\wedge$ and the disjunction $\vee$ (are of unbounded arity)
- The negation $\neg$ (is allowed only in front of atoms)

Characteristics of formula A:

- The **size** $|A|$ of A is the number of connectives and atoms in it.
- The **depth** dp(A) of A is the maximal nesting of $\vee$ and $\wedge$ in A.

LK sequent calculus

Definition

Cedent *is a finite (possibly empty) sequence of formulas denoted* $\Gamma, \Delta, \ldots$

Definition

Sequent *is an ordered pair of cedents written* $\Gamma \longrightarrow \Delta$ *(here* Γ *is called* **antecedent** *and* Δ *is called* **succedent***).*

A sequent is satisfied if at least one formula in Δ is satisfied of at least one formula in Γ is falsified. Empty sequent cannot be satisfied.

Inference rules of LK sequent calculus

- **Initial sequents**
  - $\longrightarrow 1$
  - $\neg 1 \longrightarrow$
  - $0 \longrightarrow$
  - $\longrightarrow \neg 0$
  - $p \longrightarrow p$
  - $\neg p \longrightarrow \neg p$
  - $p, \neg p \longrightarrow$
  - $\longrightarrow p, \neg p$
- **Weak structural rules** $\frac{\Gamma \to \Delta}{\Gamma' \to \Delta'}$
  - **exchange**: Γ and Δ are any permutations of A
  - **contraction**: Γ' and Δ' are obtained from Γ and Δ by deleting any multiple occurrences of formulas
  - **weakening**: $\Gamma' \supseteq \Gamma$ and $\Delta' \supseteq \Delta$

Inference rules of LK sequent calculus

- **Propositional rules**
  - $\bigwedge$-introduction

$$\frac{A, \Gamma \longrightarrow \Delta}{\bigwedge_i A_i, \Gamma \longrightarrow \Delta} \quad \frac{\Gamma \longrightarrow \Delta, A_1 \ldots \Gamma \longrightarrow \Delta, A_m}{\Gamma \longrightarrow \Delta, \bigwedge_{i \le m} A_i}$$

    where A is one of the A_i in the left rule
  - $\bigvee$-introduction

$$\frac{A_1, \Gamma \longrightarrow \Delta \ldots A_m \Gamma \longrightarrow \Delta}{\bigvee_{i \le m} A_i, \Gamma \longrightarrow \Delta} \quad \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, \bigvee_i A_i}$$

    where A is one of the A_i in the right rule
- **Cut rule**

$$\frac{\Gamma \longrightarrow \Delta, A \quad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

LK-proofs

Definition

LK-proof *of a sequent* S *from the sequents* $S_1, \ldots, S_m$ *is a sequence* $Z_1, \ldots, Z_k$ *such that* $Z_k = S$ *and each* Z_i *is either an initial one or from* $S_1, \ldots, S_m$*, or derived from the previous ones by an inference rule.*

Definition

$k(\pi)$ *is the number of sequents in* π*. The* **size** *of the proof is the sum of the sizes of the formulas in it (counting multiple occurrences of a formula separately)*

LK-proofs

Definition

Resolution refutation *of sequents* $S_1, \ldots, S_m$ *which contain no* $\bigvee, \bigwedge$ *is an LK-proof of the empty sequent from* $S_1, \ldots, S_m$ *in which no* $\bigvee, \bigwedge$ *occur.*

This is obviously equivalent to the more usual definition of resolution with clauses and the resolution rule as a resolution clause

$$\neg p_{i_1}, \ldots, \neg p_{i_a}, p_{j_1}, \ldots p_{j_b}$$

can be represented by the sequent

$$p_{i_1}, \ldots, p_{i_a} \longrightarrow p_{j_1}, \ldots, p_{j_b}$$

and the resolution by the cut rule (and vice versa).

Karchmer-Wigderson games and communication complexity

Definition

- *Let $U, V \subseteq \{0,1\}^n$ be two* **disjoint** *sets.*
- *The Karchmer-Wigderson game (KW-game) is played by two players A and B.*
- *Player A receives $u \in U$ while B receives $v \in V$. They communicate bits of information (following a protocol previously agreed on) until both players agree on the same $i \in 1, \ldots, n$ such that $u_i \neq v_i$.*
- *Their objective is to minimize (over all protocols) the number of bits they need to communicate* **in the worst case**.
- *This minimum is called the* **communication complexity (CC)** *of the game and it is denoted by $C(U, V)$.*

Karchmer-Wigderson game

Boolean function $B(p_1, \ldots, p_n)$ **separates** U from V if and only if $B(x) = 1$ holds (resp. $= 0$) for all $x \in U$ (resp. for all $x \in V$).

Theorem

Let $U, V \subseteq \{0,1\}^n$ be two disjoint sets. Then $C(U, V)$ is precisely the minimal depth of a formula with binary $\wedge$, $\vee$ separating U from V.

Definition of a protocol for KW-game

Definition

Let $U, V \subseteq \{0,1\}^n$ be two disjoint sets. A **protocol** *for the game on the pair (U, V) is a labelled directed graph G satisfying the following four conditions:*

- *G is acyclic and has one* **source** *(the in-degree 0 node) denoted $\emptyset$. The nodes with out-degree 0 are* **leaves**, *all other are inner-nodes.*
- *All leaves are labelled by one of the following formulas:*

$$u_i = 1 \wedge v_i = 0 \quad \text{or} \quad u_i = 0 \wedge v_i = 1$$

for some $i = 1, \ldots, n$.

Definition of a protocol for KW-game (continued)

Every pair $u \in U$ and $v \in V$ defines for every node x a directed path $P^x_{u,v}$ in G from the node x to a leaf: $P^x_{u,v} = x_1, \ldots, x_h$, where $x_1 = x$, the edge $S(u, v, x_i)$ goes from x_i to x_{i+1} and x_h is a leaf.

Definition (continued)

- *There is a function $S(u, v, x)$ (the* **strategy***) such that S assigns to a node x and a pair $u \in U$ and $v \in V$ the edge $S(u, v, x)$ leaving form the node x*
- *For every $u \in U$ and $v \in V$ there is a set $F(u, v) \subseteq G$ satisfying:*
  - $\emptyset \in F(u, v)$
  - $x \in F(u, v) \to P^x_{u,v} \subseteq F(u, v)$
  - *the label of any leaf from $F(u, v)$ is valid for u, v*

Such a set F is called a **consistency condition**

Monotone protocols and communication complexity

Definition

A protocol is called **monotone** *iff every leaf in it is labelled by one of the formulas* $u_i = 1 \wedge v_i = 0, i = 1, \ldots, n$.

Definition

The **communication complexity** *of* G *is the minimal number* t *such that for every* $x \in G$ *the players (one knowing* u *and* x*, the other knowing* v *and* x*) decide whether* $x \in F(u, v)$ *and compute* $S(u, v, x)$ *with at most* t *bits exchanged in the worst case.*

Protocols and circuits

Important examples of protocols are protocols formed from a circuit. Assume C is a circuit separating U from V. Reverse the edges in C, take for $F(u, v)$ those subcircuits differing in the value on u and v, and define the strategy and the labels of the leaves in an obvious way. This determines a protocol for the game on (U, V) with communication complexity 2.

Theorem

Let $U, V \in \{0, 1\}^n$ be two disjoint sets. Let G be a protocol for the game on U, V which has k nodes and the communication complexity t. Then there is a circuit C of size $k2^{O(t)}$ separating U from V. Moreover, if G is monotone, so is C.
On the other hand, any circuit (monotone circuit) C of size m separating U from V determines a protocol (a monotone protocol) G with m nodes whose complexity is 2.

Interpolant

Definition

Interpolant *of a valid implication* $A(p,q) \rightarrow B(p,r)$ *where* $p = (p_1, \ldots, p_n)$ *are the atoms occurring in both* A *and* B*, while* $q = (q_1, \ldots, q_s)$ *occur only in* A *and* $r = (r_1, \ldots, r_t)$ *only in* B*, to be any Boolean function* $I(p)$ *such that both implications*

$$A(p,q) \rightarrow (I(p) = 1) \quad \text{and} \quad ((I(p) = 1) \rightarrow B(p,r))$$

are tautologically valid. If $I(p)$ *is defined by a formula (also denoted* I*) this means that both implications*

$$A \rightarrow I \quad \text{and} \quad I \rightarrow B$$

are tautologies.

Sequents in LK calculus

In the calculus LK the implication $A \to B$ is represented by the sequent $A \longrightarrow B$ and, in general, the sequent $A_1, \ldots, A_m \longrightarrow B_1, \ldots, B_l$ represents the implication $\bigwedge_i A_i \to \bigvee_j B_j$.

The Craig interpolation theorem

Theorem

Let π be a cut-free LK-proof of the sequent

$$A_1(p,q),\dots,A_m(p,q) \longrightarrow B_1(p,r),\dots,B_l(p,r)$$

with $p=(p_1,\dots,p_n)$ the atoms occurring simultaneously in some A_i and B_j, and $q=(q_1,\dots,q_s)$ and $r=(r_1,\dots,r_l)$ all other atoms occurring in some A_i or in some B_j respectively. Then there is an interpolant $I(p)$ of the implication: $\bigwedge_{i\le m} A_i \longrightarrow \bigvee_{j\le l} B_j$ whose circuit-size is at most $k(\pi)^{O(1)}$.
If the atoms p occur only positively in all A_i or all B_j then there is monotone interpolant with monotone circuit-size at most $k(\pi)^{O(1)}$.

The Craig interpolation theorem

Proof

Define two sets $U, V \subseteq \{0,1\}^n$ *by:*

$$U = \{u \in \{0,1\}^n \mid \exists q^u \in \{0,1\}^s, \bigwedge_{i \le m} A_i(u, q^u)\}$$

$$V = \{v \in \{0,1\}^n \mid \exists r^v \in \{0,1\}^t, \bigwedge_{j \le l} \neg B_j(v, r^v)\}$$

Note that the fact that the sequent $A_1, \ldots, A_m \longrightarrow B_1, \ldots, B_l$ *is tautologically valid is equivalent to the fact that the sets* U, V *are disjoint, and that any Boolean function separates* U *from* V *iff it is interpolant of the sequent.*

Proof of the Craig interpolation theorem using CC

Proof

Using the proof π we define a protocol for the game on U, V. Assume that player A received $u \in U$ and B received $v \in V$. Player A fixes some $q^u \in \{0,1\}^s$ such that $\bigwedge_{i \leq m} A_i(u, q^u)$ holds and player B fixes some $r^v \in \{0,1\}^t$ for which $\bigwedge_{j \leq l} \neg B_j(v, r^v)$ holds. Exchanging some bits they will construct the path $P = S_0, \ldots, S_h$ of sequents of π satisfying the following conditions:

- *S_0 is the end-sequent, S_h is an initial sequent*
- *S_{i+1} is an upper sequent of the inference giving S_i*
- *For any $a = 0, \ldots, h$: if S_a has the form:*

$$E_1(p,q), \ldots, E_e(p,q) \longrightarrow F_1(p,r), \ldots, F_f(p,r)$$

then $\bigwedge_{i \leq e} E_i(u, q^u)$ holds while $\bigvee_{j \leq f} F_j(v, r^v)$ fails.

Proof of the Craig interpolation theorem using CC

Proof

Note that as the proof is cut-free and there are no ¬-rules, no formula in the antecedent (resp. the succedent) of a sequent in the proof contains an atom r_i (resp. the atom q_i).
To find S_{a+1} they proceed as follows:

- *If S_a was deduced by an inference with only one hypothesis, they put S_{a+1} to be that hypothesis and exchange no bits.*
- *If the inference yielding S_a was the introduction of $\bigwedge_{i \leq g} D_i$ to the succedent the player B, who thinks that $\bigwedge_{i \leq g} D_i$ is false, sends to A $\lceil \log g \rceil$ bits identifying one particular $D_i(v, r^v), i \leq g$, which is false. They take for S_{a+1} the upper sequent of the inference containing the minor formula D_i*
- *Introduction of $\bigvee_{i \leq g} D_i$ to the antecedent is treated similarly.*

Proof of the Craig interpolation theorem using CC

Proof

Let S_h be the initial sequent players arrive at in the path P. It must be one of the following formulas: $p_i \longrightarrow p_i$ or $\neg p_i \longrightarrow \neg p_i$ for some $i = 1, \ldots, n$. This is because all other initial sequents either contain an atom r_i in the antecedent or an atom q_i in the succedent, or violate the last condition from the definition of P.
If S_h is the former then $u_i = 1 \wedge v_i = 0$, if it is the latter then $u_i = 0 \wedge v_i = 1$.
The communication complexity of the defined protocol is $\leq \lceil \log g \rceil + 2 \leq \lceil \log k(\pi) + 2$.
Thus there is a circuit of size $k(\pi)^{O(1)}$ separating U form V. If all atoms occur only positively in the antecedent or in the succedent of the end-sequent then the players always arrive to an initial sequent of the form $p_i \longrightarrow p_i$. This yields the monotone case.

Final thoughts about Craig interpolation theorem

The proof of the theorem can be modified for the case when π is not necessarily cut-free but no cut-formula contains atoms q and r at the same time. To maintain the condition that q (resp. r) do not occur in the succedent (resp. the antecedent) we picture a cut-inference with the cut-formula D as

$$\frac{\neg D, \Gamma \longrightarrow \Delta \quad D, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

or

$$\frac{\Gamma \longrightarrow \Delta, D \quad \Gamma \longrightarrow \Delta, \neg D}{\Gamma \longrightarrow \Delta}$$

according to whether atoms q do or do not occur in D.
The modification of the proof is then straightforward as the truth-value of any cut-formula is known to one of the players and he can direct the path by sending one bit.

Definition of semantic derivation

Definition

Let N be a fixed natural number.

- *The* **semantic rule** *allows to infer from two subsets $A, B \subseteq \{0,1\}^N$ a third one: $\frac{A \quad B}{C}$ iff $C \supseteq A \cap B$*
- *A* **semantic derivation** *of the set $C \subseteq \{0,1\}^N$ from the sets $A_1, \ldots, A_m \subseteq \{0,1\}^N$ is a sequence of sets $B_1, \ldots, B_k \subseteq \{0,1\}^N$ such that $B_k = C$, each B_i is either one of A_j or derived from two previous B_{i_1}, B_{i_2} by the semantic rule*
- *Let $\mathcal{X}$ be a set of subsets of $\{0,1\}^N$. Semantic derivation $B_1, \ldots, B_k$ is an $\mathcal{X}$-***derivation** *iff all $B_i \in \mathcal{X}$*

Filters and semantic derivations

Definition

Filter *of subsets of* $\{0,1\}^N$ *is a family* $\mathcal{X}$ *closed upwards* $((A \in \mathcal{X}) \wedge (B \supseteq A) \to B \in \mathcal{X})$ *and closed under intersection* $(A, B \in \mathcal{X} \to A \cap B \in \mathcal{X})$

Lemma

Let $A_1, \ldots, A_m, C \in \{0,1\}^N$. *Then the following three conditions are equivalent:*

- C *can be semantically derived from* $A_1, \ldots, A_m$
- C *can be semantically derived from* $A_1, \ldots, A_m$ *in* $m-1$ *steps*
- C *is in the smallest filter containing* $A_1, \ldots, A_m$

Non-trivial semantic derivations

To have a non-trivial meaning of length of semantic derivation we must restrict to $\mathcal{X}$-derivations, where $\mathcal{X}$ is not a filter. A family $\mathcal{X}$ formed by subsets of $\{0,1\}^N$ definable by disjunctions of literals yields a non-trivial notion.

Communication complexity

Definition

Let $N = n + s + t$ be fixed and let $A \subseteq \{0,1\}^N$. Let $u, v \in \{0,1\}^n$, $q^u \in \{0,1\}^s$ and $r^v \in \{0,1\}^t$. Consider three tasks:

- *Decide whether $(u, q^u, r^v) \in A$*
- *Decide whether $(v, q^u, r^v) \in A$*
- *If $(u, q^u, r^v) \in A \neq (v, q^u, r^v) \in A$ find $i \leq n$ such that $u_i \neq v_i$*

These tasks can be solved by two players, one knowing u, q^u and the other one knowing v, r^v. The **communication complexity of** *A, $CC(A)$, is the minimal number of bits they need to exchange in the worst case in solving any of these three tasks.*

Monotone communication complexity

Definition

Consider two more tasks:

- *If $(u, q^u, r^v) \in A$ and $(v, q^u, r^v) \notin A$ either find $i \leq n$ such that $u_i = 1 \wedge v_i = 0$ or learn that there is some u' satisfying $u' \geq u \wedge (u', q^u, r^v) \notin A$ ($u \leq u'$ means $\bigwedge_{i \leq n} u_i \leq u'_i$)*
- *If $(u, q^u, r^v) \notin A$ and $(v, q^u, r^v) \in A$ either find $i \leq n$ such that $u_i = 1 \wedge v_i = 0$ or learn that there is some u' satisfying $v' \leq v \wedge (v', q^u, r^v) \notin A$*

The **monotone CC** *w.r.t. U of A, $MCC_U(A)$ is the minimal $t \geq CC(A)$ such that the first task can be solved communicating $\leq t$ bits in the worst case. $MCC_V(A)$ is defined similarly for the second task.*

Some definitions

Definition

Let $N = n + s + t$ be fixed. For $A \subseteq \{0,1\}^{n+s}$ define the set $\tilde{A}$ by:

$$\tilde{A} := \bigcup_{(a,b)\in A} \{(a,b,c) \mid c \in \{0,1\}^t\}$$

where a, b, c range over $\{0,1\}^n$, $\{0,1\}^s$ and $\{0,1\}^t$ respectively, and similarly for $B \subseteq \{0,1\}^{n+t}$ define $\tilde{B}$:

$$\tilde{B} := \bigcup_{(a,c)\in B} \{(a,b,c) \mid b \in \{0,1\}^s\}$$

Interpolation theorem for semantic derivations

Theorem

Let $A_1, \ldots, A_m \subseteq \{0,1\}^{n+s}$ *and* $B_1, \ldots, B_l \subseteq \{0,1\}^{n+t}$. *Assume that there is a semantic derivation* $\pi = D_1, \ldots, D_k$ *of the empty set* $\emptyset = D_k$ *from the sets* $\tilde{A}_1, \ldots, \tilde{A}_m, \tilde{B}_1, \ldots, \tilde{B}_l$ *such that* $CC(D_i) \leq t$ *for all* $i \leq k$. *Then the two sets*

$$U = \{u \in \{0,1\}^n \mid \exists q^u \in \{0,1\}^s ; (u, q^u) \in \bigcap_{j \leq m} A_j\}$$

and

$$V = \{v \in \{0,1\}^n \mid \exists r^v \in \{0,1\}^t ; (v, r^v) \in \bigcap_{j \leq l} B_j\}$$

can be separated by a circuit of size at most $(k + 2n)2^{O(t)}$

Interpolation theorem for semantic derivations (continued)

Theorem

Moreover, if the sets $A_1, \ldots, A_m$ satisfy the following monotonicity condition w.r.t. U:

$$(u, q^u) \in \bigcap_{j \le m} A_j \wedge u \le u' \to (u', q^u) \in \bigcup_{j \le m} A_j$$

and $MCC_U(D_i) \le t$ for all $i \le k$, or if the sets $B_1, \ldots, B_l$ satisfy:

$$(v, r^v) \in \bigcap_{j \le l} B_j \wedge v \ge v' \to (v', r^v) \in \bigcup_{j \le l} B_j$$

and $MCC_V(D_i) \le t$ for all $i \le k$, then there is a monotone circuit separating U from V of size at most $(k+n)2^{O(t)}$.

Proof of interpolation theorem for semantic derivations (informal)

Proof

Let $\pi = D_1, \ldots, D_k$ be a semantic derivation of $\emptyset$ from $\tilde{A}_1, \ldots, \tilde{B}_l$. The two players A and B, one knowing $(u, q^u) \in \bigcap_j A_j$ and the other one knowing $(v, r^v) \in \bigcap_j B_j$, attempt to construct a path $P = S_0, \ldots, S_h$ through π. $S_0 = \emptyset = D_k$, S_{a+1} is one of the two sets which are the hypotheses of the semantic inference yielding S_a and $S_h \in \{\tilde{A}_1, \ldots, \tilde{B}_l\}$. Moreover, both tuples (u, q^u, r^v) and (v, q^u, r^v) are **not** *in S_a, $a = 0, \ldots, h$.*

Proof of interpolation theorem for semantic derivations (informal)

Proof

If the players know S_a which was deduced in the inference $\frac{X \quad Y}{S_a}$ then they first determine whether $(u, q^u, r^v) \in X$ and $(v, q^u, r^v) \in X$. There are three possible outcomes:

- *both (u, q^u, r^v) and (v, q^u, r^v) are in X ($S_{a+1} := Y$)*
- *none of (u, q^u, r^v), (v, q^u, r^v) is in X ($S_{a+1} := X$)*
- *only one of (u, q^u, r^v), (v, q^u, r^v) is in X (stop constucting the path and enter a protocol for finding $i \leq n$ such that $u_i \neg v_i$).*

The players must sooner or later enter the third case as none of the initial sets $\tilde{A}_1, \ldots, \tilde{B}_l$ avoids both (u, q^u, r^v), (v, q^u, r^v).

Proof of the interpolation theorem for semantic derivations (monotone case)

Proof

- *We will define the protocol for the monotone case only (non-montone is similar).*
- *Assume that the sets $A_1, \dots, A_m$ satisfy the monotonicity condition w.r.t. U and that $MCC_U(D_i) \le t$ for all $i \le k$ (the case of the monotonicity w.r.t. V is analogous).*
- *The protocol has $(k+n)$ nodes, the k steps of derivation π plus n additional nodes labelled by formulas $u_i = 1 \wedge v_i = 0, i = 1, \dots, n$.*
- *The consistency condition $F(u, v)$ consists of of those D_j such that $(v, q^u, r^v) \notin D_j$ and of those additional n nodes whose label is valid for particular u, v.*

Proof of the interpolation theorem for semantic derivations (monotone case)

Proof

The players use the protocol for solving the first task from the definition of the MCC. There are two possible outcomes:

- *They decide that the condition*

$$\exists u' \geq u, (u', q^u, r^v) \notin D_j$$

  is true for u, v. Then they put $S(u, v, D_j) := X$ if $(v, q^u, r^v) \notin X$ or Y otherwise.
- *They find $i \leq n$ such that $u_i = 1 \wedge v_i = 0$. $S(u, v, D_i)$ is then the additional node with the label $u_i = 1 \wedge v_i = 0$.*

Proof of the interpolation theorem for semantic derivations (monotone case)

Proof

- *By the monotonicity imposed on $A_1, \ldots, A_m$, for every u' occurring above it holds: $(u', q^u, r^v) \in \bigcap_{j \le m} A_j$*
- *This implies that the players have to find sooner or later $i \le n$ such that $u_i = 1 \wedge v_i = 0$.*
- *By the assumption about the monotone communication complexity of all D_j, both the relation $x \in F(u, v)$ and the function $S(u, v, x)$ can be computed exchanging $O(t)$ bits.*
- *As G has $(k + n)$ nodes, theorem about connection between protocols and circuits yields the wanted monotone circuit separating U from V and having the size at most $(k + n) \cdot 2^{O(t)}$.*

Upper bound for resolution refutation

Theorem

Assume that the set of clauses $\{A_1, \dots, A_m, B_1, \dots, B_l\}$ *where:*
$A_i \subseteq \{p_1, \dots, p_n, \neg p_1, \dots, \neg p_n, q_1, \dots, q_s, \neg q_1, \dots, \neg q_s\}, i \leq m$
$B_j \subseteq \{p_1, \dots, p_n, \neg p_1, \dots, \neg p_n, r_1, \dots, r_l, \neg r_1, \dots, \neg r_l\}, j \leq l$
has a resolution refutation with k *clauses.*
Then the implication:

$$\bigwedge_{i \leq m} (\bigvee A_i) \longrightarrow \bigvee_{j \leq l} (\bigwedge \neg B_j)$$

has an interpolant $I(p)$ *whose circuit-size is* $kn^{O(1)}$
Moreover, if all atoms in p *occur positively in all* A_i*, or if all* p *occur only negatively in all* B_j*, then there is a monotone interpolant whose monotone circuit-size is* $kn^{O(1)}$.

Proof of upper bound for resolution refutation

Proof

Let $\pi = C_1, \ldots, C_k$ be a resolution refutation of $A_1, \ldots, B_l$. For a clause C denote by $\tilde{C}$ the subset of $\{0,1\}^{n+s+t}$ of all those truth assignments satisfying C. Then $\tilde{\pi} = \tilde{C}_1, \ldots, \tilde{C}_k$ is a semantic derivation of $\emptyset$ from $\tilde{A}_1, \ldots, \tilde{B}_l$.
Obviously, for any clause C both the communication complexity and the monotone communication complexity of $\tilde{C}$ is at most $CC(\tilde{C}) \leq \lceil \log n \rceil + 2$. Hence the previous theorem yields circuit of size $(k+2n) \cdot n^{O(1)} \leq k \cdot n^{O(1)}$. Similarly for the monotone case.

General idea of lower bounds

Assume that for a propositional proof system P we have a good interpolation theorem, allowing good estimates of the complexity of the monotone interpolants.
Then implication which cannot have a small monotone interpolant must have long P-proofs.

$Clique_{n,\omega}$

Definition

Let $n, \omega, \xi \geq q$ be natural numbers, and let $\binom{n}{2}$ denote the set of two-element subsets of $1, \ldots, n$. The set $Clique_{n,\omega}(p, q)$ is a set of the following formulas in the atoms $p_{ij}, i, j \in \binom{n}{2}$, and $q_{ui}, u = 1, \ldots, \omega$ and $i = 1, \ldots, n$:

- $\bigvee_{i \leq n} q_{iu}$, *for all* $u \leq \omega$
- $\neg q_{ui} \vee \neg q_{vi}$, *for all* $u < v \leq \omega$ *and* $i = 1, \ldots, n$.
- $\neg q_{ui} \vee \neg q_{vj} \vee p_{ij}$, *for all* $u < v \leq \omega$ *and* $i, j \in \binom{n}{2}$

$Color_{n,\xi}$

Definition

The set $Color_{n,\xi}(p, r)$ *is the set of the following formulas in the atoms* $p_{ij}, i, j \in \binom{n}{2}$, *and* $r_{ia}, i = 1, \ldots, n$ *and* $a = 1, \ldots, \xi$:

- $\bigvee_{a \leq \xi} r_{ia}$, *for all* $i \leq n$
- $\neg r_{ia} \vee \neg r_{ib}$, *for all* $a < b \leq \xi$ *and* $i \leq n$
- $\neg r_{ia} \vee \neg r_{ja} \vee \neg pij$, *for all* $a \leq \xi$ *and* $i, j \in \binom{n}{2}$

$Clique_{n,\omega} \longrightarrow \neg Color_{n,\xi}$

The expression $Clique_{n,\omega} \to \neg Color_{n,\xi}$ is an abbreviation of the sequent whose antecedent consists of all formulas in $Clique_{n,\omega}$ and whose succedent consists of the negations of the formulas in $Color_{n,\xi}$.
This sequent is tautologically valid if $\xi < \omega$.

Theorem

Assume that $3 \le \xi < \omega$ *and* $\sqrt{\xi}\omega \le \frac{n}{8 \log n}$. *Then the sequent*

$$Clique_{n,\omega} \to \neg Color_{n,\xi}$$

has no interpolant of the monotone circuit-size smaller than:

$$2^{\Omega(\sqrt{\xi})}$$

Lower bound for resolution refutation

Corollary

Let n be sufficiently large and let $\xi = \lceil \sqrt{n} \rceil, \omega = \xi + 1$. Then:

- *Every resolution refutation of the clauses $Clique_{n,\omega} \cup Color_{n,\xi}$ must have at least $2^{\Omega(n^{\frac{1}{4}})}$ clauses*

Proof

Theorem about upper bounds for resolution refutation with k clauses would imply the existence of an interpolant with monotone circuit size $kn^{O(1)}$. The hypothesis of the previous theorem is fulfilled and so it must hold:

$$kn^{O(1)} \geq 2^{\Omega(n^{\frac{1}{4}})}$$

and hence $k \geq 2^{\Omega(n^{\frac{1}{4}})}$