Formulas, their size and depth in relation to communication complexity

Maroš Grego

DeMorgan language

An alphabet consisting of:

- an infinite set *Atoms* of atoms: $p, q, ..., x, y \ldots$
- logical connectives
  - constants $\top$ (true) and $\bot$ (false)
  - a unary connective $\neg$ (negation)
  - binary connectives $\wedge$ (conjunction) and $\vee$ (disjunction)
- brackets: *(,)*

Propositional (DeMorgan) formulas

Finite words of DeMorgan alphabet made by applying finitely many times in arbitrary order the following rules:

- constants and atoms are formulas
- if α is a formula, so is $(\neg\alpha)$
- if α, β are formulas, so are $(\alpha \wedge \beta)$ and $(\alpha \vee \beta)$

Capital letters $A, B, \ldots$ will denote formulas.
A **subformula** of a formula α is any subword of α that is a formula.

Lemma of unique readability

If α is a formula then exactly one of the following occurs:

- α is a constant or an atom
- there are formulas β, γ such that $\alpha = (\beta \wedge \gamma)$
- there are formulas β, γ such that $\alpha = (\beta \vee \gamma)$

Definitions

A **literal** (ℓ) is an atom or its negation.
$\ell^1 := \ell$ and $p^0 := \neg p$ and $(\neg p)^0 := p$
A **term** is a conjunction of literals.
A **clause** is a disjunction of literals.
The expression $\alpha(p_1, ..., p_n)$ means all atoms in α are among $p_1, ..., p_n$ (but not all of them have to occur)

Truth assignment

Any function

$$h : Atoms \to \{0, 1\}$$

is extended to the function h^* assigning the truth value to any formula by the following:

- $h^*(\top) = 1$ and $h^*(\bot) = 0$
- $h^*(\neg\alpha) = 1 - h^*(\alpha)$
- $h^*(\alpha \wedge \beta) = min(h^*(\alpha), h^*(\beta))$
- $h^*(\alpha \vee \beta) = max(h^*(\alpha), h^*(\beta))$

Given $h(p_i) =: b_i \in \{0, 1\}$, $h^*(\alpha) =: \alpha(b_1, ..., b_n)$.
1 and 0 represent the truth values *true* and *false*.

.

Boolean functions

$$f : \{0,1\}^n \to \{0,1\}$$

Formula $\alpha(p_1, ..., p_n)$ defines a Boolean **truth table function**:

$$\mathbf{tt}_\alpha = (b_1, ..., b_n) \mapsto \alpha(b_1, ..., b_n)$$

Every Boolean function f is equal to the **tt** function of the formula

$$\bigvee_{\bar{b}\in\{0,1\}^n, f(\bar{b})=1} p_1^{b_1} \wedge ... \wedge p_n^{b_n} \quad \text{(disjunctive normal form (DNF))}$$

or of the function

$$\bigwedge_{\bar{b}\in\{0,1\}^n, f(\bar{b})=0} p_1^{1-b_1} \vee ... \vee p_n^{1-b_n} \quad \text{(conjunctive normal form (CNF))}$$

Monotone Boolean functions

A boolean function f is **monotone** iff $\bigwedge_i (a_i \leq b_i)$ implies $f(a_1, ..., a_n) \leq f(b_1, ..., b_n)$.
A DNF formula of a monotone f can be written without negation:
E.g. if $f(0, a_2, ...) = 1$ then $f(1, a_2, ...) = 0$ and the terms $p_1^0 \wedge p_2^{a_2} \wedge ...$ and $p_1^1 \wedge p_2^{a_2} \wedge ...$ can be merged into $p_2^{a_2} \wedge ...$.

Other connectives

Other languages may use other connectives, possibly with higher arity, such as:

$$a|b = 1 \text{ iff } (a \wedge b) = 0 \quad \text{(Sheffer's stroke (NAND))}$$

$$\oplus(a_1, ..., a_n) = 1 \text{ iff } \sum_i a_i \equiv 1 \mod 2 \quad \text{(parity)}$$

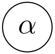
$$TH_k(a_1, ..., a_n) = 1 \text{ iff } \sum_i a_i \geq k \quad \text{(threshold)}$$

When passing from one language to another, how does the size of the formula grow?

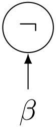
Formula size

Given a DeMorgan formula α, we construct a labeled directed binary tree S_α inductively as follows:

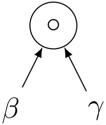
α is an atom or a constant



$\alpha = (\neg\beta)$



$\alpha = (\beta \circ \gamma)$ where $\circ$ is $\wedge$ or $\vee$



The **size of a formula** α is the number of vertices of S_α.
Arrows in S_α define a partial order.

Formula size and string length relationship

Since every connective comes with two brackets, the length of the string representing α is

$$i + 3(|S_\alpha| - i) \leq 3|S_\alpha|$$

where i is the number of leaves of S_α.
When α has n atoms represented by binary words, this increases to

$$\log n \cdot i + 3(|S_\alpha| - i) \leq (3 + \log n) \cdot |S_\alpha| \leq (3 + \log |S_\alpha|) \cdot |S_\alpha|$$

Negation normal form

The formulas α, β are **logically equivalent** ($\models\mid$) iff

$$\forall \bar{a} \in \{0,1\}^n : \alpha(\bar{a}) = \beta(\bar{a})$$

DeMorgan laws state that

$$\neg(\alpha \wedge \beta) \models\mid (\neg\alpha \vee \neg\beta) \text{ and } \neg(\alpha \vee \beta) \models\mid (\neg\alpha \wedge \neg\beta)$$

A formula is in **negation normal form** (NNF) iff negations are applied only to atoms and there are no constants.
Every formula can be transformed into NNF by DeMorgan laws and contracting subformulas with constants.
For a formula α in NNF, we define its **size** ($|S_\alpha|$) to be the number of leaves in S_α.

Translating formulas: an example

Consider the binary parity (xor): $\alpha \oplus \beta \models\!\dashv (\alpha \wedge \neg\beta) \vee (\neg\alpha \wedge \beta)$
Subformulas with $\oplus$ can be replaced iteratively this way (from simpler to complex ones).
E.g. $p_1 \oplus (p_2 \oplus (p_3 \oplus \ldots)\ldots)$ (parity of n atoms) has size n, but this translation has size between 2^n and 2^{n+1}.

Logical depth

The **logical depth** of a formula α in a language L ($\ell dp(\alpha)$) is defined as

- ℓdp of atoms and constants is 0
- $\ell dp(\circ(\beta_1, ..., \beta_k)) = 1 + max(\ell dp(\beta_1), ..., \ell dp(\beta_k))$ for $\circ$ a k-ary connective in L

Spira's lemma

Lemma (Spira's lemma)

Let T be a finite rooted k-ary tree, ordered from root down to leaves, $|T| > 1$.
For a node $a \in T$, let T_a be a subtree of nodes b such that $b \leq a$ and $T^a = T \setminus T_a$ (all b such that $b \not\leq a$).
Then there is a node a in T such that

$$\frac{1}{k+1}|T| \leq |T_a|, |T^a| \leq \frac{k}{k+1}|T|$$

Lemma (Spira's lemma)

$\forall T \ tree, |T| > 1 \ \exists a \in T : \frac{1}{k+1}|T| \leq |T_a|, |T^a| \leq \frac{k}{k+1}|T|$

Proof.

- Walk through T, starting at the root, always going into a maximal subtree (with respect to size). The size can decrease only to $s' \geq \frac{s-1}{k}$.

Lemma (Spira's lemma)

$\forall T$ *tree*, $|T| > 1$ $\exists a \in T : \frac{1}{k+1}|T| \leq |T_a|, |T^a| \leq \frac{k}{k+1}|T|$

Proof.

- Walk through T, starting at the root, always going into a maximal subtree (with respect to size). The size can decrease only to $s' \geq \frac{s-1}{k}$.
- Stop at the first node a such that $|T_a| \leq (k/(k+1))|T|$. Then also $(1/(k+1))|T| \leq |T_a|$ (since by the bound above, the previous subtree had size $s \leq k|T_a|$; if $|T_a| < (1/(k+1))|T|$ then $s \leq (k/(k+1))|T|$ and we would have stopped then).

Lemma (Spira's lemma)

$\forall T$ *tree*, $|T| > 1$ $\exists a \in T : \frac{1}{k+1}|T| \le |T_a|, |T^a| \le \frac{k}{k+1}|T|$

Proof.

- Walk through T, starting at the root, always going into a maximal subtree (with respect to size). The size can decrease only to $s' \ge \frac{s-1}{k}$.
- Stop at the first node a such that $|T_a| \le (k/(k+1))|T|$. Then also $(1/(k+1))|T| \le |T_a|$ (since by the bound above, the previous subtree had size $s \le k|T_a|$; if $|T_a| < (1/(k+1))|T|$ then $s \le (k/(k+1))|T|$ and we would have stopped then).
- As $|T^a| = |T| - |T_a|$, also $(1/(k+1))|T| \le |T^a| \le (k/(k+1))|T|$

□

On the logical depth

Lemma

Let α be a formula in a language with at most k-ary connectives and with size s.
Then, there is a logically equivalent DeMorgan formula β of logical depth $\ell dp(\beta) \leq O(\log_{(k+1)/k} s) = O(\log s)$.

Substitution

A **substitution** of formulas for atoms in a formula $\alpha(p_1, ..., p_n)$ is a map assigning to each p_i a formula β_i.
The formula arising from applying the substitution is denoted by $\alpha(p_1/\beta_1, ..., p_n/\beta_n)$ and constructed by simultaneously replacing all occurences of p_i in α by β_i, $i = 1, ..., n$.

On the logical depth

Lemma

$\forall\alpha$ *formula with at most k-ary connectives, size s*
$\exists\beta$ *DeMorgan formula* $\models\!\!\mid \alpha$*:* $\ell dp(\beta) \leq O(\log_{(k+1)/k} s) = O(\log s)$.

Proof.

- Assume atoms of α are $\bar{p}$, let q be a new atom and $\gamma(\bar{p}, q)$ and $\delta(\bar{p})$ formulas such that $\alpha = \gamma(q/\delta)$ (α is created by substituting δ for q in γ).

On the logical depth

Lemma

$\forall\alpha$ *formula with at most k-ary connectives, size s*
$\exists\beta$ *DeMorgan formula* $\models\!\mid \alpha$*:* $\ell dp(\beta) \leq O(\log_{(k+1)/k} s) = O(\log s)$*.*

Proof.

- Assume atoms of α are $\bar{p}$, let q be a new atom and $\gamma(\bar{p}, q)$ and $\delta(\bar{p})$ formulas such that $\alpha = \gamma(q/\delta)$ (α is created by substituting δ for q in γ).
- α is equivalent to $(\gamma(\bar{p}, 1) \wedge \delta) \vee (\gamma(\bar{p}, 0) \wedge \neg\delta)$. The logical depth of the new formula is $2 + max(\ell dp(\gamma), \ell dp(\delta))$.

On the logical depth

Lemma

$\forall\alpha$ *formula with at most* k*-ary connectives, size* s
$\exists\beta$ *DeMorgan formula* $\models\!\mid \alpha$*:* $\ell dp(\beta) \leq O(\log_{(k+1)/k} s) = O(\log s)$.

Proof.

- Assume atoms of α are $\bar{p}$, let q be a new atom and $\gamma(\bar{p}, q)$ and $\delta(\bar{p})$ formulas such that $\alpha = \gamma(q/\delta)$ (α is created by substituting δ for q in γ).
- α is equivalent to $(\gamma(\bar{p}, 1) \wedge \delta) \vee (\gamma(\bar{p}, 0) \wedge \neg\delta)$. The logical depth of the new formula is $2 + max(\ell dp(\gamma), \ell dp(\delta))$.
- By Spira's lemma, choose γ such that $|\gamma|, |\delta| \leq k/(k+1) \cdot s$. By induction, we assume the statement holds for formulas of the size smaller than s.

$\square$

Karchmer-Wigderson game

A **multi-function** defined on $U \times V$ with values in $I \neq \emptyset$ $(U \times V \xrightarrow{multi} I)$ is a relation $R \subseteq U \times V \times i$ such that $\forall \bar{u} \in U, \bar{v} \in V \exists i \in I : R(\bar{u}, \bar{v}, i)$.
The task to find, given $\bar{u} \in U, \bar{v} \in V$ any $i \in I$ such that $R(\bar{u}, \bar{v}, i)$ leads to to a two player game.
The **U-player** receives $\bar{u}$, then **V-player** receives $\bar{v}$.
They exchange bits of information according to a **Karchmer-Wigderson protocol**.

Karchmer-Wigderson protocol

The **KW-protocol** is a finite binary tree T such that

- each non-leaf is labeled by U or V and the two edges leaving it are labeled by 0 or 1
- each leaf is labeled by some $i \in I$

together with strategies S_U, S_V for the players, which are functions $U \times T_0$ (resp $V \times T_0$) $\rightarrow \{0, 1\}$ (T_0 are the non-leaves of T).

Karchmer-Wigderson protocol

- The players start at the root of T.
- If the current node x is a non-leaf, its label tells them who should send a bit
  (if it's U, the U-player sends $S_U(\bar{u}, x)$, if V, the V-player sends $S_V(\bar{v}, x)$).
  This bit determines the edge out of x and hence the next node $x' \in T$.
- If the current node is a leaf, its label i is the output of the play on $(\bar{u}, \bar{v})$.

The label must be a valid value of the multi-function.
The **communication complexity** of R ($CC(R)$) is the minimum height of a KW-protocol tree that computes R.

Karchmer-Wigderson multi-function

The **KW-multi-function** is a multi-function on disjoint $U, V \subseteq \{0,1\}^n$ with values in $[n]$ for which a valid value for $(\bar{u}, \bar{v})$ is i iff $u_i \neq v_i$. It is denoted $KW[U, V]$.
If U is closed upwards or V downwards, the monotone $KW^m[U, V]$ has a valid value i iff $u_i = 1 \wedge v_i = 0$.

Karchmer-Wigderson theorem

Theorem (Karchmer and Wigderson)

Let $U, V \subseteq \{0,1\}^n$ *be disjoint. Then* $CC(KW[U,V])$ *equals to the minimum depth of a DeMorgan formula* φ *in the negation normal form that separates* U *from* V
(i.e. φ *is constantly* 1 *on* U *and* 0 *on* V*),*
where we count depth of a literal as 0*.*

If U *is closed upwards or* V *downwards then* $CC(KW^m[U,V])$ *equals to the minimum depth of a DeMorgan formula* φ *without negations that separates* U *from* V*.*

Theorem (Karchmer and Wigderson)

$U, V \subseteq \{0,1\}^n$ disjoint, $CC(KW[U,V])$ equals to the minimum depth of a DeMorgan formula φ in NNF separating U from V.

Proof.

- Given a separating φ, the players start at the top connective and walk down to smaller subformulas, maintaining an invariant that the the surrent subformula gives value 1 for $\bar{u} \in U$ and 0 for $\bar{v} \in V$.

Theorem (Karchmer and Wigderson)

$U, V \subseteq \{0,1\}^n$ disjoint, $CC(KW[U,V])$ equals to the minimum depth of a DeMorgan formula φ in NNF separating U from V.

Proof.

- Given a separating φ, the players start at the top connective and walk down to smaller subformulas, maintaining an invariant that the the surrent subformula gives value 1 for $\bar{u} \in U$ and 0 for $\bar{v} \in V$.
- That is true at the start. If the current connective is $\vee$, the U-player indicates by one bit whetere the left or right subformula is true.
  If it is $\wedge$, the V-player indicates which one is false.

Theorem (Karchmer and Wigderson)

$U, V \subseteq \{0,1\}^n$ disjoint, $CC(KW[U,V])$ equals to the minimum depth of a DeMorgan formula φ in NNF separating U from V.

Proof.

- Given a separating φ, the players start at the top connective and walk down to smaller subformulas, maintaining an invariant that the the surrent subformula gives value 1 for $\bar{u} \in U$ and 0 for $\bar{v} \in V$.
- That is true at the start. If the current connective is $\vee$, the U-player indicates by one bit whetere the left or right subformula is true.
  If it is $\wedge$, the V-player indicates which one is false.
- The literal they arrive at is a valid value for $KW[U,V]$ (and also for $KW^m[U,V]$ if there is no negation in φ).

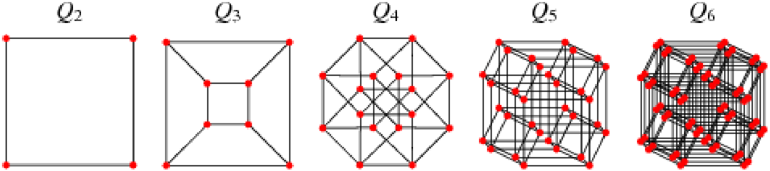
Theorem (Karchmer and Wigderson)

$U, V \subseteq \{0,1\}^n$ disjoint, $CC(KW[U,V])$ equals to the minimum depth of a DeMorgan formula φ in NNF separating U from V.

Proof.

- Given a separating φ, the players start at the top connective and walk down to smaller subformulas, maintaining an invariant that the the surrent subformula gives value 1 for $\bar{u} \in U$ and 0 for $\bar{v} \in V$.
- That is true at the start. If the current connective is $\vee$, the U-player indicates by one bit whetere the left or right subformula is true.
  If it is $\wedge$, the V-player indicates which one is false.
- The literal they arrive at is a valid value for $KW[U,V]$ (and also for $KW^m[U,V]$ if there is no negation in φ).
- For the opposite direction, construct φ by induction on the computational complexity of $KW[U,V]$ (resp. $KW^m[U,V]$).

Krapchenko's bound



Let Q_n denote the graph of the n-cube (node set $\{0,1\}^n$, two nodes adjacent iff they differ in one coordinate).
A subset $A \subseteq Q_n$ induces a subgraph G_A of Q_n; for a node x, denote $d_A(x)$, resp. $N_A(x)$ as the degree of x in A, resp. the set of neighbours of x in A.

Theorem (Krapchenko)

Let $U, V \subseteq \{0,1\}^n$ be disjoint, $A = Q_n \cap (U \times V)$. Then, for every formula φ separating U and V, we mave

$$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|} = \log \frac{|A|}{|U|} + \log \frac{|A|}{|V|}$$

Theorem (Krapchenko)

$U, V \subseteq \{0,1\}^n$ disjoint, $A = Q_n \cap (U \times V)$, $\forall \varphi$ separating U, V:
$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|}$

Proof.

- Fix a protocol, let $C(\bar{u}, \bar{v})$ be the number of bits it uses on $\bar{u}, \bar{v}$. We will prove that for inputs taken uniformly from A $E(C(\bar{u}, \bar{v})) \geq \log \frac{|A|^2}{|U||V|}$ (where E is expected value).

Theorem (Krapchenko)

$U, V \subseteq \{0,1\}^n$ disjoint, $A = Q_n \cap (U \times V)$, $\forall\varphi$ separating U, V:
$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|}$

Proof.

- Fix a protocol, let $C(\bar{u}, \bar{v})$ be the number of bits it uses on $\bar{u}, \bar{v}$. We will prove that for inputs taken uniformly from A $E(C(\bar{u}, \bar{v})) \geq \log \frac{|A|^2}{|U||V|}$ (where E is expected value).
- Let $b_X(\bar{u}, \bar{v})$ be the number of bits the player X sends on the given input, then:

$$E(C(\bar{u}, \bar{v})) = \frac{1}{|A|} \sum_{(\bar{u}, \bar{v}) \in A} (b_U(\bar{u}, \bar{v}) + b_V(\bar{u}, \bar{v}))$$

$$= \frac{1}{|A|} [\sum_{\bar{v} \in V} \sum_{\bar{u} \in N(\bar{v})} b_U(\bar{u}, \bar{v}) + \sum_{\bar{u} \in U} \sum_{\bar{v} in N(\bar{u})} b_V(\bar{u}, \bar{v})]$$

Theorem (Krapchenko)

$U, V \subseteq \{0,1\}^n$ disjoint, $A = Q_n \cap (U \times V)$, $\forall \varphi$ separating U, V:
$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|}$

Proof.

- For any $\bar{v} \in V, \sum_{\bar{u} \in N(\bar{v})} b_U(\bar{u}, \bar{v}) \geq d(\bar{v}) \log d(\bar{v})$ (since even if player U knows $\bar{v}$, they need to tell V what $\bar{u}$ they have). Analogically for $\bar{u} \in U$.

Theorem (Krapchenko)

$U, V \subseteq \{0,1\}^n$ disjoint, $A = Q_n \cap (U \times V)$, $\forall \varphi$ separating U, V:
$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|}$

Proof.

- For any $\bar{v} \in V, \sum_{\bar{u} \in N(\bar{v})} b_U(\bar{u}, \bar{v}) \geq d(\bar{v}) \log d(\bar{v})$ (since even if player U knows $\bar{v}$, they need to tell V what $\bar{u}$ they have). Analogically for $\bar{u} \in U$.
- $E(C(\bar{u}, \bar{v})) \geq \frac{1}{|A|}[\sum_{\bar{v} \in V} d(\bar{v}) \log d(\bar{v}) + \sum_{\bar{u} \in U} d(\bar{u}) \log d(\bar{u})]$
  $\geq \frac{1}{|A|}[\sum_{\bar{v} \in V} \frac{|A|}{|V|} \log \frac{|A|}{|V|} + \sum_{\bar{u} \in U} \frac{|A|}{|U|} \log \frac{|A|}{|U|}] = \log \frac{|A|^2}{|U||V|}$

Theorem (Krapchenko)

$U, V \subseteq \{0,1\}^n$ disjoint, $A = Q_n \cap (U \times V)$, $\forall \varphi$ separating U, V:
$\ell dp(\varphi) \geq \log \frac{|A|^2}{|U||V|}$

Proof.

- For any $\bar{v} \in V, \sum_{\bar{u} \in N(\bar{v})} b_U(\bar{u}, \bar{v}) \geq d(\bar{v}) \log d(\bar{v})$ (since even if player U knows $\bar{v}$, they need to tell V what $\bar{u}$ they have). Analogically for $\bar{u} \in U$.
- $E(C(\bar{u}, \bar{v})) \geq \frac{1}{|A|}[\sum_{\bar{v} \in V} d(\bar{v}) \log d(\bar{v}) + \sum_{\bar{u} \in U} d(\bar{u}) \log d(\bar{u})]$
  $\geq \frac{1}{|A|}[\sum_{\bar{v} \in V} \frac{|A|}{|V|} \log \frac{|A|}{|V|} + \sum_{\bar{u} \in U} \frac{|A|}{|U|} \log \frac{|A|}{|U|}] = \log \frac{|A|^2}{|U||V|}$
- The result follows from the KW-theorem.

□

Sources

- J.Krajíček, Proof Complexity, CUP, 2019
- M.Karchmer and A.Wigderson, Monotone circuits for connectivity require super-logarithmic depth, SIAM Journal on Discrete Mathematics, 1990

Thank you for attention!