Lower bounds on Boolean and Modal Circuit-size

Petar Iliev
Institute of Mathematics and Informatics
Institute of Philosophy and Sociology
Bulgarian Academy of Sciences

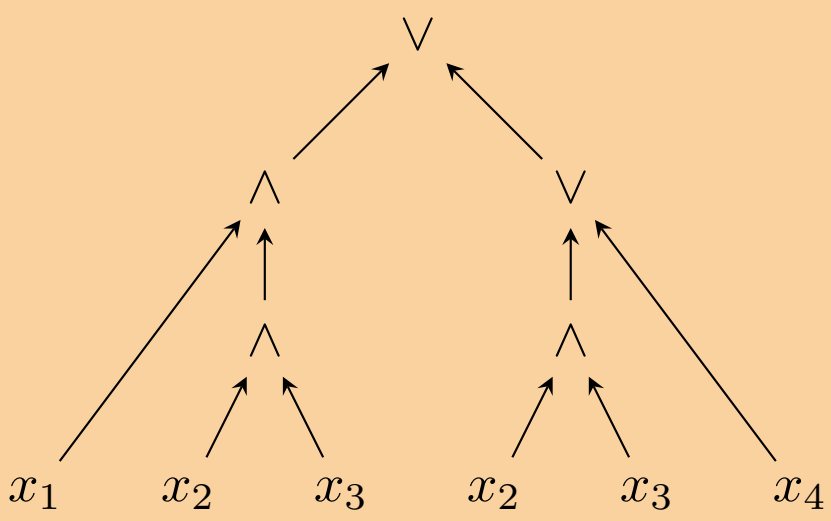
Part One.

Lower Bounds on Boolean Circuit-size

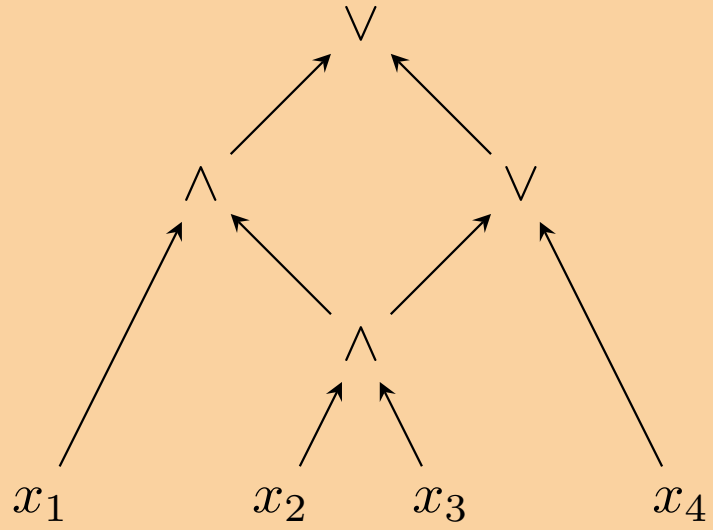
One way to attack the P vs NP question

Here are two Boolean circuits (the tree-like one is a formula). From now on, we are going to consider only circuits over $\{\neg, \wedge, \vee\}$.

$$(x_1 \wedge (x_2 \wedge x_3)) \vee ((x_2 \wedge x_3) \vee x_4)$$



size: 5



size: 4

How?

- Take a language L over $\{0,1\}$.
- For each n, define a Boolean function $f_L^n : B^n \to \{0,1\}$ where $f_L^n(w) = 1$ iff $w \in L$.

Thus, L can be "computed" by an infinite sequence of Boolean circuits, each one computing the respective f_L^n.

How?

- Take a language L over $\{0,1\}$.
- For each n, define a Boolean function $f_L^n : B^n \to \{0,1\}$ where $f_L^n(w) = 1$ iff $w \in L$.

Thus, L can be "computed" by an infinite sequence of Boolean circuits, each one computing the respective f_L^n.

Fix an enumeration of Turing machines

$$M_1, M_2, \ldots, M_n, \ldots.$$

Define the Boolean functions
$f^n(x_1, \ldots, x_n) = 1$ iff M_n halts on the empty tape.

The connection with Turing machines

John Savage, *Computational work and time on finite machines* (1972).
If L can be computed by a deterministic Turing machine in time $T(n)$, then it can be computed by an infinite sequence C_L^n of circuits such that each C_L^n has size at most $O(T(n)log(T(n)))$.

How to show that P is strictly contained in NP

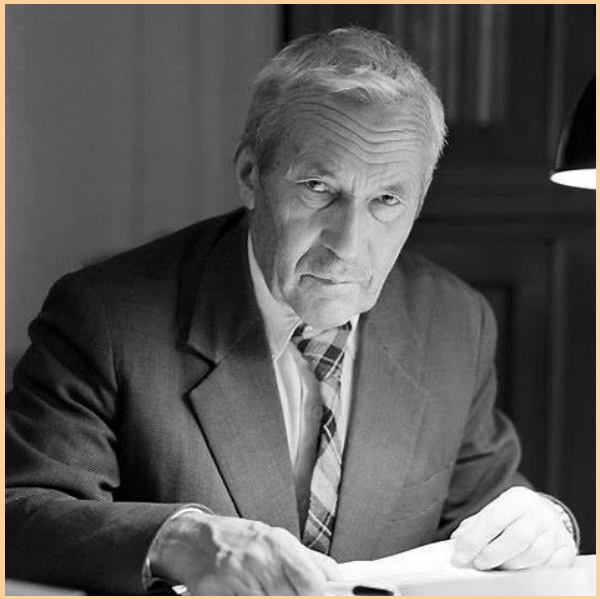
- Take a language L in NP.
- For each n, define the Boolean function $f_L^n : B^n \to \{0,1\}$ where $f_L^n(w) = 1$ iff $w \in L$.
- Prove that the sizes of the smallest circuits computing the functions f_L^n grow superpolinomially in n.

What shall we do about the non-uniformity of the circuit model?

Some people do not seem to care too much.

What shall we do about the non-uniformity of the circuit model?

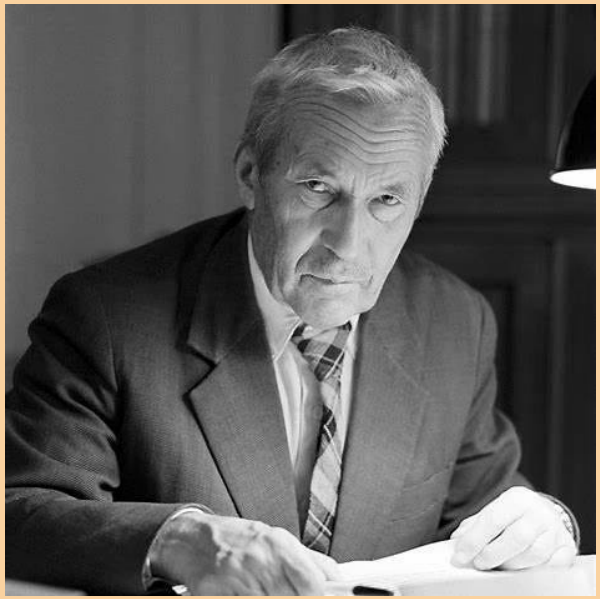
Some people do not seem to care too much.



But Andrey Kolmogorov conjectured that all languages in P can be computed by families of linear sized circuits.

What shall we do about the non-uniformity of the circuit model?

Some people do not seem to care too much.



But Andrey Kolmogorov conjectured that all languages in P can be computed by families of linear sized circuits.

Today, we know that his conjecture implies $P \neq NP$.

The infamous problems in one slide.

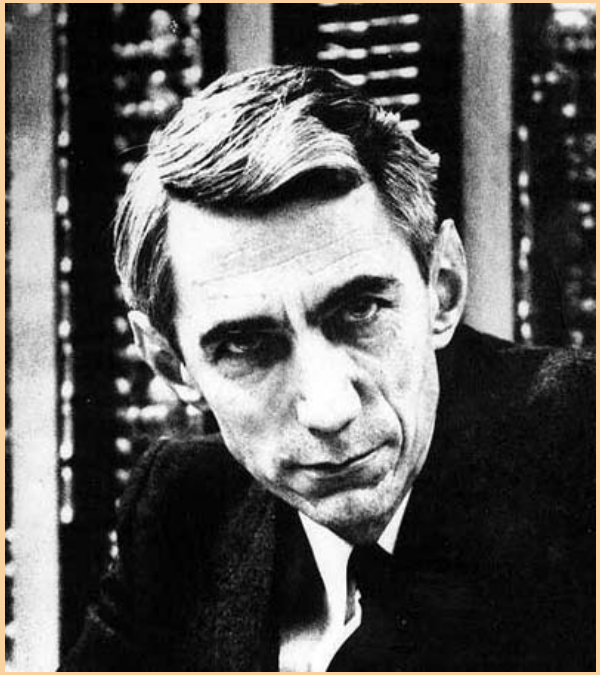
1. Construct a sequence of Boolean functions computing a problem in NP

$$f^2(x_1, x_2),\ f^3(x_1, x_2, x_3),\ \ldots,\ f^n(x_1, \ldots, x_n),\ \ldots$$

   - Prove that the sizes of the smallest Boolean circuits computing these functions grow super-polynomially (e.g. n^{logn}).
     This will show $P \subset NP$.
   - Prove that the sizes of the smallest Boolean formulae grow super-polynomially.

2. Prove that there is no subexponential equivalence preserving translation from circuits to formulae. This will show $NC_1 \subset P$.

How it started



Claude Shannon, *The synthesis of two switching circuits* (1949).
For almost all $f : \{0,1\}^n \to \{0,1\}$ there are no circuits with size $< \frac{2^n}{10n}$.
Proof: Too many functions 2^{2^n}; too few circuits with size $< \frac{2^n}{10n}$.

What has been done since 1949?

We have the following depressing situation.
No one has been able to find an **explicit** sequence of Boolean functions

$$f^2(x_1, x_2),\ f^3(x_1, x_2, x_3),\ \ldots,\ f^n(x_1, \ldots, x_n),\ \ldots$$

Circuits: > 5.2, > 5.3, $\ldots$, $> 5.n$, $\ldots$
K. Iwama, H. Morizumi, *An explicit lower bound of 5n-o(n) for Boolean circuits* (2002)

What has been done since 1949?

We have the following depressing situation.
No one has been able to find an **explicit** sequence of Boolean functions

$$f^2(x_1, x_2),\ f^3(x_1, x_2, x_3),\ \ldots,\ f^n(x_1, \ldots, x_n),\ \ldots$$

Circuits: > 5.2, > 5.3, $\ldots$, $> 5.n$, $\ldots$
K. Iwama, H. Morizumi, *An explicit lower bound of 5n-o(n) for Boolean circuits* (2002)

or

Formulae: $> 2^3$, $> 3^3$, $\ldots$, $> n^3$, $\ldots$
J. Håstad, *The shrinkage exponent is 2* (1998).

One of the many problems.

M. Sipser, *The history and status of the P versus NP question* (1992)
One of the impediments in the lower bounds area is a shortage of problems of intermediate difficulty which lend insight into the harder problems. Most of known problems (boolean functions) are either "easy" (parity, majority, etc.) or are "very hard" (clique problem, satisfiability of CNFs, and all other NP-hard problems).

Part Two.

Lower Bounds on Modal Circuit-size

How do we find problems of intermediate difficulty?

Consider the classical calculus CL that is consistent and complete for the usual Boolean semantics.

(A1) $p_0 \to (p_1 \to p_0)$,

(A2) $(p_0 \to (p_1 \to p_2)) \to ((p_0 \to p_1) - > (p_0 \to p_2))$,

(A3) $p_0 \wedge p_1 \to p_0$,

(A4) $p_0 \wedge p_1 \to p_1$,

(A5) $p_0 \to (p_1 \to p_0 \wedge p_1)$,

(A6) $p_0 \to p_0 \vee p_1$,

(A7) $p_1 \to p_0 \vee p_1$,

(A8) $(p_0 \to p_2) \to ((p_1 \to p_2) \to (p_0 \vee p_1 \to p_2))$,

(A9) $\bot \to p_0$,

(A10) $p_0 \vee (p_0 \to \bot)$.

(Inference rules:) Modus ponens and substitution.

What if?

Simply by dropping (**A10**), we obtain the intuitionistic propositional calculus INT which is consistent and complete for the Kripke semantics of the intuitionistc formulae over $\{\bot, \vee.\wedge, \rightarrow\}$

(A1) $p_0 \rightarrow (p_1 \rightarrow p_0)$,

(A2) $(p_0 \rightarrow (p_1 \rightarrow p_2)) \rightarrow ((p_0 \rightarrow p_1) - > (p_0 \rightarrow p_2))$,

(A3) $p_0 \wedge p_1 \rightarrow p_0$,

(A4) $p_0 \wedge p_1 \rightarrow p_1$,

(A5) $p_0 \rightarrow (p_1 \rightarrow p_0 \wedge p_1)$,

(A6) $p_0 \rightarrow p_0 \vee p_1$,

(A7) $p_1 \rightarrow p_0 \vee p_1$,

(A8) $(p_0 \rightarrow p_2) \rightarrow ((p_1 \rightarrow p_2) \rightarrow (p_0 \vee p_1 \rightarrow p_2))$,

(A9) $\bot \rightarrow p_0$.

(Inference rules:) Modus ponens and substitution.

The connectives are independent in INT

Mordechaj Wajsberg

John Mckinsey

M. Wajsberg, Untersuchungen über den Aussagenkalkül von A. Heyting (1938).
J. McKinsey. Proof of the Independence of the Primitive Symbols of Heyting's Calculus of Propositions (1939).

An exponential lower bound on formula-size in INT

- $\varphi_1 = (p_1 \leftrightarrow p_0)$;
- $\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1)$;
- $\vdots$
- $\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1})$.
- $\vdots$

Where $\varphi \leftrightarrow \psi$ is an abbreviation of $\varphi \to \psi \wedge \psi \to \varphi$.

Every formula over $\{\to, \vee, \wedge, \bot\}$ that is equivalent to φ_n in INT has size at least 2^n.

Circuits vs Formulae in INT

Note that in INT $\varphi \leftrightarrow \psi$ is equivalent to $(\varphi \vee \psi) \rightarrow (\varphi \wedge \psi)$. Thus,
$\varphi_1 = (p_1 \leftrightarrow p_0)$ is equivalent to $\varphi_1' = (p_0 \vee p_1) \rightarrow (p_0 \wedge p_1)$;
$\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1) \equiv (p_2 \vee p_1 \vee \varphi_1') \rightarrow (p_2 \wedge (p_1 \vee \varphi_1'))$;
$\vdots$
$\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1}) \equiv (p_n \vee p_{n-1} \vee \varphi_{n-1}') \rightarrow (p_n \wedge (p_{n-1} \vee \varphi_{n-1}'))$
$\vdots$

Circuits vs Formulae in INT

Note that in INT $\varphi \leftrightarrow \psi$ is equivalent to $(\varphi \vee \psi) \rightarrow (\varphi \wedge \psi)$. Thus,
$\varphi_1 = (p_1 \leftrightarrow p_0)$ is equivalent to $\varphi_1' = (p_0 \vee p_1) \rightarrow (p_0 \wedge p_1)$;
$\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1) \equiv (p_2 \vee p_1 \vee \varphi_1') \rightarrow (p_2 \wedge (p_1 \vee \varphi_1'))$;
$\vdots$
$\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1}) \equiv (p_n \vee p_{n-1} \vee \varphi_{n-1}') \rightarrow (p_n \wedge (p_{n-1} \vee \varphi_{n-1}'))$
$\vdots$

We have an equivalent linear circuit over $\{\bot, \vee, \wedge, \rightarrow\}$. This implies that there is no polynomial equivalence preserving translation from intuitionistic circuits over $\{\bot, \wedge, \vee, \rightarrow\}$ to intuitionistic formulae over $\{\bot, \wedge, \vee, \rightarrow\}$.

What if?

By replacing (A10) with $(p_0 \to \bot) \vee (p_0 \to \bot) \to \bot$ we obtain the intuitionistic calculus KC of the weak excluded middle that is consistent and complete for finite rooted intuitionistic frames with a last element.

(A1) $p_0 \to (p_1 \to p_0)$,

(A2) $(p_0 \to (p_1 \to p_2)) \to ((p_0 \to p_1) - > (p_0 \to p_2))$,

(A3) $p_0 \wedge p_1 \to p_0$,

(A4) $p_0 \wedge p_1 \to p_1$,

(A5) $p_0 \to (p_1 \to p_0 \wedge p_1)$,

(A6) $p_0 \to p_0 \vee p_1$,

(A7) $p_1 \to p_0 \vee p_1$,

(A8) $(p_0 \to p_2) \to ((p_1 \to p_2) \to (p_0 \vee p_1 \to p_2))$,

(A9) $\bot \to p_0$,

(A10) $(p_0 \to \bot) \vee ((p_0 \to \bot) \to \bot)$.

(Inference rules:) Modus ponens and substitution.

An exponential lower bound on formula-size in KC

- $\varphi_1 = (p_1 \leftrightarrow p_0)$;
- $\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1)$;
- $\vdots$
- $\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1})$.
- $\vdots$

Where $\varphi \leftrightarrow \psi$ is an abbreviation of $\varphi \rightarrow \psi \wedge \psi \rightarrow \varphi$.

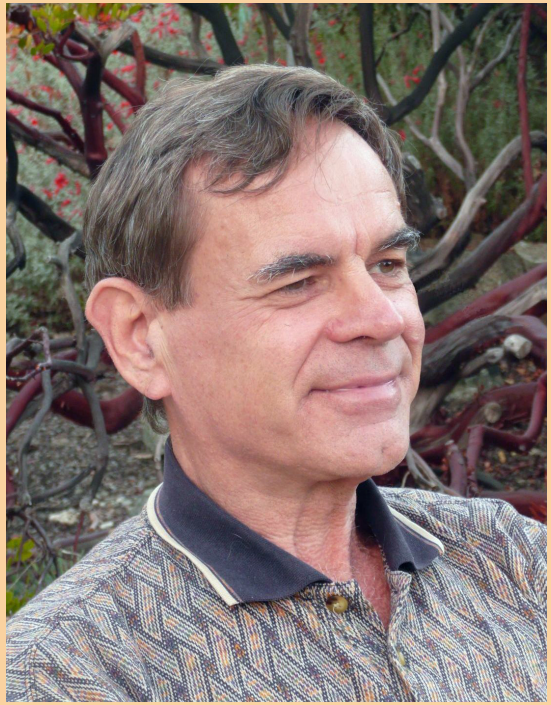
Every formula over $\{\rightarrow, \vee, \wedge, \bot\}$ that is equivalent to φ_n in KC has size at least 2^n.

Circuits vs Formulae in KC

Note that in INT $\varphi \leftrightarrow \psi$ is equivalent to $(\varphi \vee \psi) \rightarrow (\varphi \wedge \psi)$. Thus,
$\varphi_1 = (p_1 \leftrightarrow p_0)$ is equivalent to $\varphi_1' = (p_0 \vee p_1) \rightarrow (p_0 \wedge p_1)$;
$\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1) \equiv (p_2 \vee p_1 \vee \varphi_1') \rightarrow (p_2 \wedge (p_1 \vee \varphi_1'))$;
$\vdots$
$\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1}) \equiv (p_n \vee p_{n-1} \vee \varphi_{n-1}') \rightarrow (p_n \wedge (p_{n-1} \vee \varphi_{n-1}'))$
$\vdots$
We have an equivalent linear circuit over $\{\bot, \vee, \wedge, \rightarrow\}$.
Hence,

- there is no polynomial equivalence preserving translation from intuitionistic circuits over $\{\bot, \wedge, \vee, \rightarrow\}$ to intuitionistic formulae over $\{\bot, \wedge, \vee, \rightarrow\}$ in KC.
- there is no polynomial equivalence preserving translation from formulae over $\{\leftrightarrow, \bot, \wedge, \vee, \rightarrow\}$ to formulae over $\{\bot, \wedge, \vee, \rightarrow\}$ in KC.

Formulae with $\leftrightarrow$ vs Formulae without in CL



Vaughan Pratt

V. Pratt, *The effect of basis on size of Boolean expressions.* (1975).
For any Boolean formula of size n over the basis $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, there is an equivalent formula over the basis $\{\neg, \wedge, \vee, \rightarrow\}$ of size $\leq c \times n^{\log_3 10}$.

Back to Sipser

What exactly is a problem of “intermediate difficulty”?

Back to Sipser

What exactly is a problem of "intermediate difficulty"?

Сергей Мардаев

С. И. Мардаев, *Вложения импликативных решеток и суперинтуиционистские логики* (1987).
There is a continuum of intermediate logics $KC \subseteq L$

For what it's worth

I cannot do anything about linear frames.

Open problem

Take the Dummett logic LC obtained by adding $(p \to q) \vee (q \to p)$ to INT. It is consistent and complete for finite linearly ordered Kripke frames.

(A1) $p_0 \to (p_1 \to p_0)$,

(A2) $(p_0 \to (p_1 \to p_2)) \to ((p_0 \to p_1) - > (p_0 \to p_2))$,

(A3) $p_0 \wedge p_1 \to p_0$,

(A4) $p_0 \wedge p_1 \to p_1$,

(A5) $p_0 \to (p_1 \to p_0 \wedge p_1)$,

(A6) $p_0 \to p_0 \vee p_1$,

(A7) $p_1 \to p_0 \vee p_1$,

(A8) $(p_0 \to p_2) \to ((p_1 \to p_2) \to (p_0 \vee p_1 \to p_2))$,

(A9) $\bot \to p_0$,

(A10) $(p \to q) \vee (q \to p)$.

(Inference rules:) Modus ponens and substitution.

Open problem.

Is there a sub-exponential equivalence preserving translation from intuitionistic propositional formulae over $\{\leftrightarrow, \rightarrow, \vee, \wedge, \bot\}$ to formulae over $\{\rightarrow, \vee, \wedge, \bot\}$ in LC? In particular, are there short formulae without $\leftrightarrow$ that are equivalent in LC to

- $\varphi_1 = (p_1 \leftrightarrow p_0)$;
- $\varphi_2 = p_2 \leftrightarrow (p_1 \vee \varphi_1)$;
- $\vdots$
- $\varphi_n = p_n \leftrightarrow (p_{n-1} \vee \varphi_{n-1})$.
- $\vdots$

Where $\varphi \leftrightarrow \psi$ is an abbreviation of $\varphi \rightarrow \psi \wedge \psi \rightarrow \varphi$.

Another one about linear frames

The future according to everyday intutiont.

$$F\varphi = \langle < \rangle \varphi$$

Another one about linear frames

The future according to everyday intutiont.

$$F\varphi = \langle < \rangle \varphi$$

The future according to people working in formal verification.

or

$$F\varphi = \langle \leq \rangle \varphi$$

Another one about linear frames

The future according to everyday intutiont.

$$F\varphi = \langle < \rangle \varphi$$

The future according to people working in formal verification.

or

$$F\varphi = \langle \leq \rangle \varphi$$

$$\langle \leq \rangle \varphi \equiv \varphi \vee \langle < \rangle \varphi.$$

Another one about linear frames

I. Hodkinson and M. Reynolds, *Separation - past, present, and future* (2005).

They say it is possible that there are formulae:
$\langle \leq \rangle$: $\varphi_1, \quad \varphi_2, \quad \ldots \quad , \varphi_n, \quad \ldots, |\varphi_n| = k.n$ such that formulae with
$\langle < \rangle$: $\geq 2^1, \quad \geq 2^2, \quad \ldots \quad , \geq 2^n, \quad \ldots$

Another one about linear frames

I conjecture that one such sequence is:

$$\begin{aligned}
\varphi_1 &= \langle\leq\rangle p_1, \\
\varphi_2 &= \langle\leq\rangle(p_2 \wedge \langle\leq\rangle p_1), \\
&\vdots \\
\varphi_n &= \langle\leq\rangle(p_n \wedge \varphi_{n-1}), \\
&\vdots
\end{aligned}$$

A random selection of articles

1. AI
   - M. Cadoli, et al, *The size of a revised knowledge base* (1995)
   - M. Cadoli, et al, *On compact representation of propositional circumscription* (1997)
   - G. Gogic, et al, *The comparative linguistics of knowledge representation* (1995)
   - B. Nebel, *On the compilability and expressive power of propositional planning formalisms* (2000)
2. Data bases
   - M. Grohe, N. Schweikardt, *Comparing the succinctness of monadic query languages over finite trees* (2003)
   - B. ten Cate, et al, *Navigational xpath: calculus and algebra* (2007)
3. Formal verification
   - M. Adler, N. Immerman, *An $n!$ lower bound on formula size* (2001)
   - K. Etessami et al, *First-order logic with two variables and unary temporal logic* (2002)
   - T. Wilke, *CTL+ is exponentially more succinct than CTL* (1999)

A random selection of articles

4 Modal logic

- S. Figueira, D. Gorin *On the size of shortest modal descriptions* (2010)
- L. Hella, M. Vilander, *Formula size games for modal logic and μ-calculus* (2019)
- P. Balbiani et al. *Frame-validity games and lower bounds on the complexity of modal axioms* (2019),
- D. Vakarelov, *Modal definability in languages with a finite number of propositional variables and a new extension of the Sahlqvist's class* (2003)
- B ten Cate, L. Kuijer, and F. Wolter *The Size of Interpolants in Modal Logics* (2025).

Prof. Tinchev according to his students

Prof. Tinchev according to his students


ТИНКО
АЗ