The Number of Axioms

Juan P. Aguilera [1,2] Matthias Baaz [1] **Jan Bydžovský** [1]

[1]Institute of Discrete Mathematics and Geometry, TU Wien, Austria

[2]Department of Mathematics, Ghent University, Belgium

Logical Perspectives Workshop, June 2021

Motivation

Motivation

Theorem (Statman'79; Orevkov'82)

Motivation

Theorem (Statman'79; Orevkov'82)

There is no elementary bound (i.e of the form $2^{2^{\cdots^{2^n}}}$ *)*

Motivation

Theorem (Statman'79; Orevkov'82)

There is no elementary bound (i.e of the form $2^{2^{\cdots^{2^n}}}$)

- on the number of steps in a minimal cut-free proof of a provable sequent S -

Motivation

Theorem (Statman'79; Orevkov'82)

There is no elementary bound (i.e of the form $2^{2^{\cdots^{2^n}}}$)

- on the number of steps in a minimal cut-free proof of a provable sequent S -

in terms of the number of steps in a minimal proof of S

Motivation

Theorem (Statman'79; Orevkov'82)

There is no elementary bound (i.e of the form $2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}$*)*

- on the number of steps in a minimal cut-free proof of a provable sequent S -

in terms of the number of steps in a minimal proof of S and the number of symbols in S.

A Question

A Question

Is there a FO tautology φ such that the number of distinct axioms in any minimal cut-free proof π of φ is “much smaller” than the number of sequents in π?

A Question

Is there a FO tautology φ such that the number of distinct axioms in any minimal cut-free proof π of φ is "much smaller" than the number of sequents in π?

No.

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and $A(y, x) \vdash A(y, x)$ are distinct axioms

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and $A(y, x) \vdash A(y, x)$ are distinct axioms
$A(x) \vdash A(x)$ and

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and $A(y, x) \vdash A(y, x)$ are distinct axioms
$A(x) \vdash A(x)$ and $B(x) \vdash B(x)$ are distinct axioms

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and $A(y, x) \vdash A(y, x)$ are distinct axioms
$A(x) \vdash A(x)$ and $B(x) \vdash B(x)$ are distinct axioms

m ... the minimal number of steps to cut-free prove S

An Answer

(if x is not y and A is not B then)

$A(x, y) \vdash A(x, y)$ and $A(y, x) \vdash A(y, x)$ are distinct axioms
$A(x) \vdash A(x)$ and $B(x) \vdash B(x)$ are distinct axioms

m ... the minimal number of steps to cut-free prove S
α ... the minimal number of distinct axioms to cut-free prove S

An Answer

(if x is not y and A is not B then)

$A(x,y) \vdash A(x,y)$ and $A(y,x) \vdash A(y,x)$ are distinct axioms
$A(x) \vdash A(x)$ and $B(x) \vdash B(x)$ are distinct axioms

m ... the minimal number of steps to cut-free prove S
α ... the minimal number of distinct axioms to cut-free prove S

$$\sqrt[|S|^3]{\frac{1}{2^{|S|^4+1}} \log_2(m)} \leq \alpha$$

Corollaries part I/II

Corollaries part I/II

There is no elementary bound

Corollaries part I/II

There is no elementary bound

- on the number of distinct axioms needed to cut-free prove a sequent S -

Corollaries part I/II

There is no elementary bound

- on the number of distinct axioms needed to cut-free prove a sequent S -

in terms of the number of symbols in S and the number of steps in a minimal proof of S.

Corollaries part I/II

There is no elementary bound

- on the number of distinct axioms needed to cut-free prove a sequent S -

in terms of the number of symbols in S and the number of steps in a minimal proof of S.

Few bits of the argument

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S

Few bits of the argument

α … the minimal number of distinct axioms to cut-free prove S
m … minimal number of steps to cut-free prove S

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S
m ... minimal number of steps to cut-free prove S

Assume $\pi : S$ with α and m' steps and $\alpha << m \leq m'$

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S
m ... minimal number of steps to cut-free prove S

Assume $\pi : S$ with α and m' steps and $\alpha << m \leq m'$

sub-furmula property of $\pi \Rightarrow$ *many terms* in π are not subterms of any term in an axiom or in S

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S
m ... minimal number of steps to cut-free prove S

Assume $\pi : S$ with α and m' steps and $\alpha << m \leq m'$

sub-furmula property of $\pi \Rightarrow$ *many terms* in π are not subterms of any term in an axiom or in S

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S
m ... minimal number of steps to cut-free prove S

Assume $\pi : S$ with α and m' steps and $\alpha << m \leq m'$

sub-furmula property of $\pi \Rightarrow$ *many terms* in π are not subterms of any term in an axiom or in S

Main Idea:

every *many term* t is uniquely determined by its position wrt to the terms below t that appear in axioms

Few bits of the argument

α ... the minimal number of distinct axioms to cut-free prove S
m ... minimal number of steps to cut-free prove S

Assume $\pi : S$ with α and m' steps and $\alpha << m \leq m'$

sub-furmula property of $\pi \Rightarrow$ *many terms* in π are not subterms of any term in an axiom or in S

Main Idea:

every *many term* t is uniquely determined by its position wrt to the terms below t that appear in axioms

number of positions can be bounded in terms of α

Corollaries part I/II

Corollaries part I/II

The argument works for many other sequent calculi!

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts)

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**+ Equality + Theory (with essential cuts)

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**, **S5**

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**, **S5**,...,

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**, **S5**,..., even for **LK**$^{++}$

and

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**, **S5**,..., even for $\mathbf{LK}^{++}$

and

"any" calculus with contraction and weakening rule

Corollaries part I/II

The argument works for many other sequent calculi!

LK with equality (with essential cuts), **LK**$+$ Equality $+$ Theory (with essential cuts), **LJ**, **S5**,..., even for **LK**$^{++}$

and

"any" calculus with contraction and weakening rule

probably does not hold for Linear Logic

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**,

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough,

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough, but what about the other axioms?

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough, but what about the other axioms?

Proofs with **cuts**?

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough, but what about the other axioms?

Proofs with **cuts**?

Is there a provable φ such that the number of distinct axioms in any minimal proof π of φ is "much smaller" than the number of sequents in π?

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough, but what about the other axioms?

Proofs with **cuts**?

Is there a provable φ such that the number of distinct axioms in any minimal proof π of φ is "much smaller" than the number of sequents in π?

Have time?

Remarks and Open Problems

Any theorem of **PA** can be proven with one instance of induction rule (use reflection).

Can any theorem of **PA** be proven with one instance of $x \cdot S(y) = x \cdot y + x$?

For **ZFC**, probably one replacement and one axiom of choice is enough, but what about the other axioms?

Proofs with **cuts**?

Is there a provable φ such that the number of distinct axioms in any minimal proof π of φ is "much smaller" than the number of sequents in π?

Have time?

Try Propositional BONUS

Propositional case

Do *symmetric* tautologies need *asymmetric* proofs?

Symmetric proof $\Rightarrow$ the frequencies of axioms are similar

Propositional case

Do *symmetric* tautologies need *asymmetric* proofs?

Symmetric proof $\Rightarrow$ the frequencies of axioms are similar
Cut-free LK proofs of PHP_n *can* have similar axiom frequencies.

Propositional case

Do *symmetric* tautologies need *asymmetric* proofs?

Symmetric proof $\Rightarrow$ the frequencies of axioms are similar
Cut-free LK proofs of PHP_n *can* have similar axiom frequencies.

Can LK_d proofs of PHP_n have similar axiom frequencies?

Propositional case

Do *symmetric* tautologies need *asymmetric* proofs?

Symmetric proof $\Rightarrow$ the frequencies of axioms are similar
Cut-free LK proofs of PHP_n *can* have similar axiom frequencies.

Can LK_d proofs of PHP_n have similar axiom frequencies?