Orevkov's speed up result in strange surroundings

Norbert Preining

Japan Advanced Institute of Science and Technology

CTFM 14

Tokyo, Japan

17 February 2014

Background and introduction

- projective geometry
- sequent calculus for projective geometry, cut-elimination
- sketches and equivalence to formal proofs, based on Herbrand disjunctions
- length estimations for proofs with sketches and proofs in full Gentzen-style calculus

Ingredients for the following talk

- Projective geometry
  axioms, examples, Desargues' theorem, algebraization
- Number theory, Algebra
  Robinson's result on definability of the natural numbers, Lagrange
- Herbrand disjunctions
  minimization of terms, length estimations
- Orevkov's sequence of formulas
  coding in a theory

Ingredients for the following talk

- Projective geometry
  axioms, examples, Desargues' theorem, algebraization
- Number theory, Algebra
  Robinson's result on definability of the natural numbers, Lagrange
- Herbrand disjunctions
  minimization of terms, length estimations
- Orevkov's sequence of formulas
  coding in a theory

Ingredients for the following talk

- Projective geometry
  axioms, examples, Desargues' theorem, algebraization
- Number theory, Algebra
  Robinson's result on definability of the natural numbers, Lagrange
- Herbrand disjunctions
  minimization of terms, length estimations
- Orevkov's sequence of formulas
  coding in a theory

Ingredients for the following talk

- Projective geometry
  axioms, examples, Desargues' theorem, algebraization
- Number theory, Algebra
  Robinson's result on definability of the natural numbers, Lagrange
- Herbrand disjunctions
  minimization of terms, length estimations
- Orevkov's sequence of formulas
  coding in a theory

Recapping Orevkov's result

Orevkov (1979) gave the following sequence of formulas C_k

$$\begin{gathered}\forall b_0((\forall w_0 \exists v_0 P(w_0, b_0, v_0) \wedge \\ \wedge \forall u v w(\exists y(P(y, b_0, u) \wedge \exists z(P(v, y, z) \wedge P(z, y, w))) \supset \\ P(v, u, w))) \supset \exists v_k(P(b_0, b_0, v_k) \wedge \\ \wedge \exists v_{k+1}(P(b_0, v_k, v_{k-1}) \wedge \ldots \wedge \exists v_0 P(b_0, v_1, v_0))))\end{gathered}$$

Here $P(a, b, c)$ has the intended interpretation $a + 2^b = c$ and is used to code the non-elementary function $2_i = 2^{(2_{i-1})}$.

Theorem Orevkov, 1979

There is a derivation of C_k with cuts where the number of sequents depends linearly on k, while for any cut-free derivation it depends non-elementary on k.

Recapping Orevkov's result

Orevkov (1979) gave the following sequence of formulas C_k

$$\forall b_0((\forall w_0 \exists v_0 P(w_0, b_0, v_0) \wedge$$
$$\wedge \forall u v w(\exists y(P(y, b_0, u) \wedge \exists z(P(v, y, z) \wedge P(z, y, w))) \supset$$
$$P(v, u, w))) \supset \exists v_k(P(b_0, b_0, v_k) \wedge$$
$$\wedge \exists v_{k+1}(P(b_0, v_k, v_{k-1}) \wedge \ldots \wedge \exists v_0 P(b_0, v_1, v_0))))$$

Here $P(a, b, c)$ has the intended interpretation $a + 2^b = c$ and is used to code the non-elementary function $2_i = 2^{(2_{i-1})}$.

Theorem Orevkov, 1979

There is a derivation of C_k with cuts where the number of sequents depends linearly on k, while for any cut-free derivation it depends non-elementary on k.

Definition of projective geometry

Syntax

2-sorted languages, sorts π and γ, variables of those types: P, Q, ... for π, g, h, ... for γ, constants of type π: $A_0, \ldots, D_0$

function symbols: $[..] : \pi \times \pi \to \gamma$, $(..) : \gamma \times \gamma \to \pi$

predicates: $=$ for both types, $\mathcal{I}$: $\pi \times \gamma$

quantifiers for both types

Axioms of projective geometry

$$\forall P \forall Q (P \neq Q \supset \exists! g (P \, \mathcal{I} \, g \wedge Q \, \mathcal{I} \, g))$$

$$\forall g \forall h (g \neq h \supset \exists P (P \, \mathcal{I} \, g \wedge P \, \mathcal{I} \, h))$$

$$A_0 \not\mathcal{I} \, [B_0 C_0] \wedge \ldots$$

Definition of projective geometry

Syntax

2-sorted languages, sorts π and γ, variables of those types: $P, Q, \ldots$ for π, $g, h, \ldots$ for γ, constants of type π: $A_0, \ldots, D_0$

function symbols: $[..] : \pi \times \pi \to \gamma$, $(..) : \gamma \times \gamma \to \pi$

predicates: $=$ for both types, $\mathcal{I}$: $\pi \times \gamma$

quantifiers for both types

Axioms of projective geometry

$$\forall P \forall Q (P \neq Q \supset \exists! g (P \,\mathcal{I}\, g \wedge Q \,\mathcal{I}\, g))$$
$$\forall g \forall h (g \neq h \supset \exists P (P \,\mathcal{I}\, g \wedge P \,\mathcal{I}\, h))$$
$$A_0 \,\not{\mathcal{I}}\, [B_0 C_0] \wedge \ldots$$

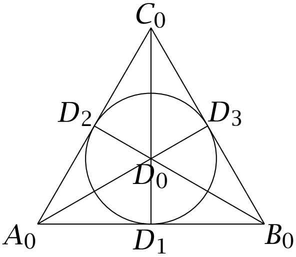
A Gentzen-style calculus for PG

Gentzen LK with two types, plus:

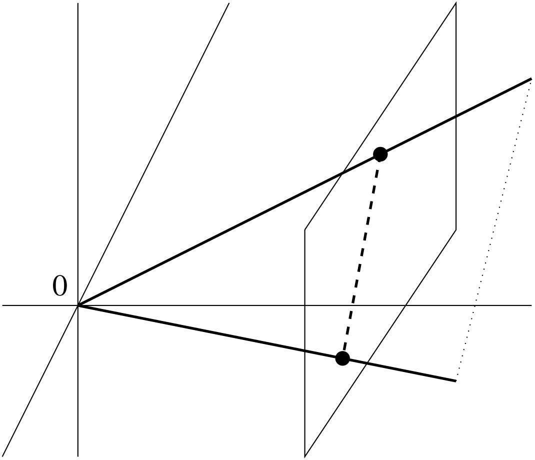
- Structural rules, logical rules, cut rule, equality rules
- $\rightarrow P \mathcal{I} [PQ]$ and $\rightarrow Q \mathcal{I} [PQ]$.
- $\rightarrow (gh) \mathcal{I} g$ and $\rightarrow (gh) \mathcal{I} h$.
- $X = Y \rightarrow$ where $X, Y \in \{A_0, B_0, C_0, D_0\}$ and $X \neq Y$.
- $\rightarrow x = x$ where x is a free variable.
- $$\frac{\Gamma \rightarrow \Delta, P \mathcal{I} g \quad \Gamma \rightarrow \Delta, Q \mathcal{I} g \quad P = Q, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, [PQ] = g}$$
  $$\frac{\Gamma \rightarrow \Delta, X \mathcal{I} [YZ]}{\Gamma \rightarrow \Delta}$$
  where $\neq (X, Y, Z)$ and $X, Y, Z \in \{A_0, B_0, C_0, D_0\}$

Examples for projective planes

Minimal (or Fano) projective plane



Projective plane over $\mathbb{Q}^3$



π lines through 0

γ planes through 0

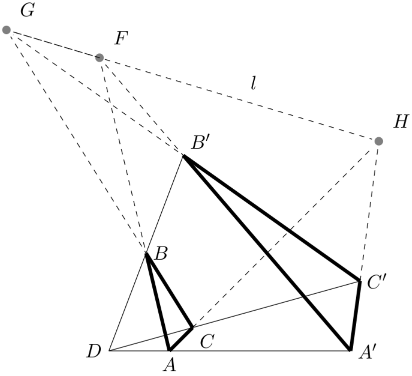
$\mathcal{I}$ is subset

$[PQ]$ is hull taking

(gh) is intersection

Desargues' theorem

A triangle is perspective wrt to a point if it is perspective wrt to a line.



Desargues' axiom

The previous “theorem” is only valid in some projective planes, it can be added as an axiom with the following consequences:

- any Desargues projective plane is algebraizable, i.e., can be represented as the lines and planes of a vector space $\mathbb{K}^3$ for some field $\mathbb{K}$.
- addition and multiplication can be defined as follows: $g \neq h$; $0, 1 \,\mathcal{I}\, h$; $0, 1 \not\mathcal{I}\, g$; $R \,\mathcal{I}\, g$; $R \not\mathcal{I}\, h$; $l \neq g, h$; $(gh) \,\mathcal{I}\, l$ and defined addition and multiplication as

$$X + Y := (h[([([0R]l)X]g)([RY]l)])$$

$$X \cdot Y := (h[([([1R]l)X]g)([RY]l)])$$

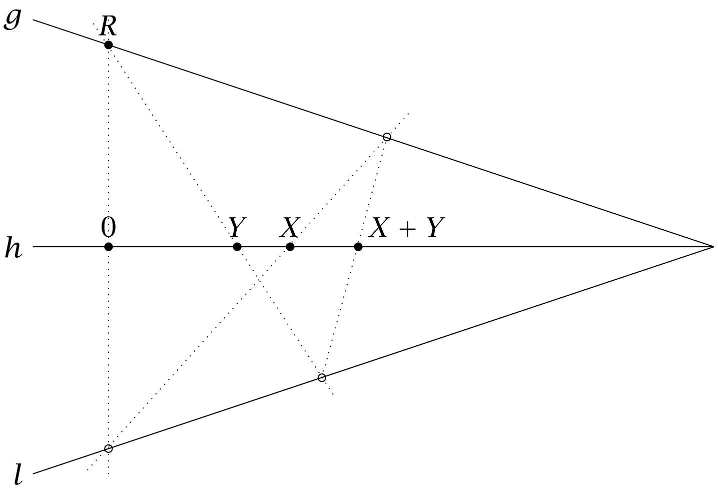
Desargues' axiom

The previous "theorem" is only valid in some projective planes, it can be added as an axiom with the following consequences:

- any Desargues projective plane is algebraizable, i.e., can be represented as the lines and planes of a vector space $\mathbb{K}^3$ for some field $\mathbb{K}$.
- addition and multiplication can be defined as follows: $g \neq h$; $0, 1 \mathcal{I} h$; $0, 1 \not\mathcal{I} g$; $R \mathcal{I} g$; $R \not\mathcal{I} h$; $l \neq g, h$; $(gh) \mathcal{I} l$ and defined addition and multiplication as

$$X + Y := (h[([([0R]l)X]g)([RY]l)])$$
$$X \cdot Y := (h[([([1R]l)X]g)([RY]l)])$$

Algebraizing projective geometry



FROM $\mathbb{Q}$ TO $\mathbb{N}$

- Current status: One model where 'being a rational' $R(x)$ can be defined ($P\ \mathcal{I}\ g \wedge P \neq (gh)$)
- Basic operations can be defined: $+$, $\cdot$, $-$, $/$
- Notion of integer can be defined (Robinson, 1949) by

$$I(z) \leftrightarrow R(z) \wedge \forall x \forall y \{R(x) \wedge R(y) \wedge \Phi(x,y,0) \wedge \forall u[R(u) \wedge \Phi(x,y,u) \supset \Phi(x,y,u+1)] \supset \Phi(x,y,z)\}$$

where $\Phi(x,y,z)$ is

$$\forall r,s,t[R(r) \wedge R(s) \wedge R(t) \supset 2 + xyz^2 + yr^3 \neq s^2 + xt^2]$$

From $\mathbb{Q}$ to $\mathbb{N}$

- Current status: One model where 'being a rational' $R(x)$ can be defined ($P \mathcal{I} g \land P \neq (gh)$)
- Basic operations can be defined: $+$, $\cdot$, $-$, $/$
- Notion of integer can be defined (Robinson, 1949) by

$$I(z) \leftrightarrow R(z) \land \forall x \forall y \{R(x) \land R(y) \land \Phi(x,y,0) \land \\ \forall u [R(u) \land \Phi(x,y,u) \supset \Phi(x,y,u+1)] \supset \Phi(x,y,z)\}$$

where $\Phi(x,y,z)$ is

$$\forall r,s,t [R(r) \land R(s) \land R(t) \supset 2 + xyz^2 + yr^3 \neq s^2 + xt^2]$$

From $\mathbb{Q}$ to $\mathbb{N}$

- Current status: One model where 'being a rational' $R(x)$ can be defined ($P \, \mathcal{I} \, g \wedge P \neq (gh)$)
- Basic operations can be defined: $+$, $\cdot$, $-$, $/$
- Notion of integer can be defined (Robinson, 1949) by

$$I(z) \leftrightarrow R(z) \wedge \forall x \forall y \{R(x) \wedge R(y) \wedge \Phi(x,y,0) \wedge \\ \forall u[R(u) \wedge \Phi(x,y,u) \supset \Phi(x,y,u+1)] \supset \Phi(x,y,z)\}$$

where $\Phi(x,y,z)$ is

$$\forall r,s,t[R(r) \wedge R(s) \wedge R(t) \supset 2 + xyz^2 + yr^3 \neq s^2 + xt^2]$$

From $\mathbb{Q}$ to $\mathbb{N}$, cont.

- define $<$ via identity of Lagrange: every positive number is the sum of four squares: $n = a^2 + b^2 + c^2 + d^2$
- define all recursive functions (e.g., Shoenfield, 1967) using Gödel's β-function

From $\mathbb{Q}$ to $\mathbb{N}$, cont.

- define $<$ via identity of Lagrange: every positive number is the sum of four squares: $n = a^2 + b^2 + c^2 + d^2$
- define all recursive functions (e.g., Shoenfield, 1967) using Gödel's β-function

Some missing pieces

- Sketches are basically Herbrand disjunctions
- Estimating the length of proofs by sketches depends on the term depth as constructing the terms is the longest procedure
- we have to guarantee that the terms are not ridiculously long
- how to bound the length of terms to the Herbrand disjunction?

Some missing pieces

- Sketches are basically Herbrand disjunctions
- Estimating the length of proofs by sketches depends on the term depth as constructing the terms is the longest procedure
- we have to guarantee that the terms are not ridiculously long
- how to bound the length of terms to the Herbrand disjunction?

Some missing pieces

- Sketches are basically Herbrand disjunctions
- Estimating the length of proofs by sketches depends on the term depth as constructing the terms is the longest procedure
- we have to guarantee that the terms are not ridiculously long
- how to bound the length of terms to the Herbrand disjunction?

Some missing pieces

- Sketches are basically Herbrand disjunctions
- Estimating the length of proofs by sketches depends on the term depth as constructing the terms is the longest procedure
- we have to guarantee that the terms are not ridiculously long
- how to bound the length of terms to the Herbrand disjunction?

Minimizing terms in HDs

Assume a Herbrand disjunction

$$H = A(\vec{t}_1, \vec{T}_1) \vee \ldots \vee A(\vec{t}_n, \vec{T}_n)$$

is given where the T_i are Skolem terms, and the t_i are regular terms.

Substitute new variables for the regular terms we obtain the *Herbrand skeleton*

$$H^{\#} = A(\vec{x}_1, \vec{S}_1) \vee \ldots \vee A(\vec{x}_n, \vec{S}_n)$$

Minimizing terms in HDs

Assume a Herbrand disjunction

$$H = A(\vec{t}_1, \vec{T}_1) \vee \ldots \vee A(\vec{t}_n, \vec{T}_n)$$

is given where the T_i are Skolem terms, and the t_i are regular terms.

Substitute new variables for the regular terms we obtain the *Herbrand skeleton*

$$H^{\#} = A(\vec{x}_1, \vec{S}_1) \vee \ldots \vee A(\vec{x}_n, \vec{S}_n)$$

Minimization, cont.

Collect the positions (path in the tree of the construction of the formula) where atomic formulas at that position in the original formula are equal

$$M = \{(p_i, p_j) \quad | \quad \mathrm{Atom}(H, p_i) = \mathrm{Atom}(H, p_j)\}$$

Create the 'equality system' where corresponding atoms in the new formula are equated:

$$G = \{\mathrm{Atom}(H^\#, p_i) = \mathrm{Atom}(H^\#, p_j) \quad | \quad (p_i, p_j) \in M\}$$

This equality system has of course a solution, the original substitution from the Herbrand skeleton $H^\#$ to H.

Minimization, cont.

Collect the positions (path in the tree of the construction of the formula) where atomic formulas at that position in the original formula are equal

$$M = \{(p_i, p_j) \quad | \quad \mathrm{Atom}(H, p_i) = \mathrm{Atom}(H, p_j)\}$$

Create the 'equality system' where corresponding atoms in the new formula are equated:

$$G = \{\mathrm{Atom}(H^\#, p_i) = \mathrm{Atom}(H^\#, p_j) \quad | \quad (p_i, p_j) \in M\}$$

This equality system has of course a solution, the original substitution from the Herbrand skeleton $H^\#$ to H.

Minimization, cont.

The subsets of G form a po-set (even a lattice), and all of them, too, have solutions (the projection of the original substitution).

If such a subset has a solution that transforms the Herbrand skeleton into a tautology (i.e., into a valid Herbrand disjunction), we call it *alternative equality system*.

Again, the alternative equality systems form a po-set (but normally not a lattice). We call an element g of it *minimal* (not unique!) if all proper subsets of g are not alternative equality systems.

Minimization, cont.

The subsets of G form a po-set (even a lattice), and all of them, too, have solutions (the projection of the original substitution).

If such a subset has a solution that transforms the Herbrand skeleton into a tautology (i.e., into a valid Herbrand disjunction), we call it *alternative equality system*.

Again, the alternative equality systems form a po-set (but normally not a lattice). We call an element g of it *minimal* (not unique!) if all proper subsets of g are not alternative equality systems.

Minimization, cont.

The subsets of G form a po-set (even a lattice), and all of them, too, have solutions (the projection of the original substitution).

If such a subset has a solution that transforms the Herbrand skeleton into a tautology (i.e., into a valid Herbrand disjunction), we call it *alternative equality system*.

Again, the alternative equality systems form a po-set (but normally not a lattice). We call an element g of it *minimal* (not unique!) if all proper subsets of g are not alternative equality systems.

Consequences of the minimization

Theorem

The length of a given term in any minimal Herbrand disjunction is bound by the following $|t| \le d2^{kl}$.
d is the maximal depth of the Herbrand skeleton, k the length of the HD, l the number of variable places in an instance

Theorem

For any formula A and any integer k it is possible to check whether there is an Herbrand disjunction for A with length smaller than k.

Consequences of the minimization

Theorem

The length of a given term in any minimal Herbrand disjunction is bound by the following $|t| \leq d2^{kl}$.
d is the maximal depth of the Herbrand skeleton, k the length of the HD, l the number of variable places in an instance

Theorem

For any formula A and any integer k it is possible to check whether there is an Herbrand disjunction for A with length smaller than k.

Estimating HDs

Some notations

- $|H|$: length of an HD is the number of disjunction terms
- $\mathsf{HD}(A)$: an HD which is minimal wrt length
- $\mathsf{HD}_{\mathcal{M}}(A)$: a minimal HD which is equivalent to A in the model $\mathcal{M}$ (that can be a much shorter HD)
- $x <_f y : x < f(y)$ for an at most exponential function f

Estimating $|H|$

The following equivalences can be shown

- $|\mathsf{HD}_{\mathcal{M}}(A)| \leq |\mathsf{HD}(A)|$
- $|\mathsf{HD}_{(\mathcal{M})}(A)| \leq |\mathsf{HD}_{(\mathcal{M})}(A \wedge B)|$
- $|\mathsf{HD}_{\mathcal{M}}(A)| \leq f(|\mathsf{HD}_{\mathcal{M}}(A \vee B)|)$
  if B is not valid in $\mathcal{M}$ and is of bounded complexity

Glueing it all together

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

GLUEING IT ALL TOGETHER

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

Glueing it all together

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

Glueing it all together

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

Glueing it all together

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

Glueing it all together

- working in the specific model of $\mathbf{PG}_{\mathbb{Q}}$ allows us to define rationals
- the equalities of Robinson allow us to define integers from it
- the Lagrange identity allows us to define positive
- Gödel's β-function and encoding allows us to encode exponentials
- use this to replace Orevkov's $P(x, y, z)$ encoding $x = y + 2^z$ in his sequence of formulas
- estimate the length of the Herbrand disjunction of the resulting (monster) formula

Estimating the length of Orevkov's formulas

Orevkov's formula F_k:

$$\mathcal{AX} \supset (A_0 \wedge C \supset B_k(0))$$

where

$$B_k(0) \equiv (\exists v_k) \ldots (\exists v_0)(\mathrm{Nat}(v_k, \ldots, v_0) \wedge \\ \wedge P(0, 0, v_k) \wedge P(0, v_k, v_{k-1}) \wedge \ldots \wedge P(0, v_1, v_0))$$

Each $P(a, b, c)$ describing $a + 2^b = c$ again looks like $\exists z(a + z = c \wedge G(b, z))$ with $G(x, y)$ describing $y = 2^x$.

Estimations, cont.

With the abbreviations

$$G_0 \equiv v_k = 1 \qquad\qquad G_i \equiv G(v_i, v_{i-1}) \quad i > 0$$

we can estimate the HD by

$$|\mathsf{HD}_{\mathbf{PG}_{\mathbb{Q}}}(B_k(0))| \geq_f |\mathsf{HD}_{\mathbf{PG}_{\mathbb{Q}}}(G_1)|$$

where $v_0 = 2_k$ and $v_1 = 2_{k-1}$ and so on. This is obvious from the fact that the v_i are the computed values of 2_l, i.e. $v_i = 2_{k-i}$.

Using Gödels representations we end up with

$$G(x, z) \equiv 2\beta((\mu k)Q(x, k), x - 1) = z$$

where

$$Q(x, k) \equiv \mathrm{Nat}(k) \wedge \mathrm{Seq}(k) \wedge \mathrm{lh}(k) = x \wedge (k)_0 = 1 \wedge \\ \wedge (\forall i_{i<x})(i \neq 0 \supset (k)_i = 2(k)_{i-1}).$$

Estimations, cont.

For $G_1 = G(v_1, v_0)$ we obtain

$$
\begin{aligned}
(\exists w_1)(\mathrm{Nat}(w_1) \wedge 2\beta(w_1, v_1 - 1) = v_0 \wedge \\
w_1 = (\mu s)(\mathrm{Seq}(s) \wedge \mathrm{lh}(s) = v_1 \wedge (s)_0 = 1 \wedge \\
(\forall i_{i<v_1})(i \neq 0 \supset (s)_i = 2(s)_{i-1})))
\end{aligned}
$$

This means that $w_1 = \ulcorner (2^0, 2^1, \ldots, v_k) \urcorner$ the Gödel number of the respective sequence.

So we can estimate the length of the Herbrand-disjunction again

$$
|\mathsf{HD}_{\mathbf{PG}_{\mathbb{Q}}}(G_1)| \geq |\mathsf{HD}_{\mathbf{PG}_{\mathbb{Q}}}(w_1 = (\mu s) Q(v_1, s))|
$$

Estimations, cont.

Continuing in this matter we arrive at

$$|\mathsf{HD}(\mathcal{A}\mathcal{X} \supset (A_0 \wedge C \supset B_k(0)))| \geq_f v_1$$

where $v_1 = 2_{k-1}$ and f is an at most exponential function.

The 'fast' proof can be used more or less 1-1 from Orevkov's paper.

Theorem

In projective geometry, proving with sketches is in some cases non-elementary slower than using the sequent system with cuts.

Estimations, cont.

Continuing in this matter we arrive at

$$|\mathsf{HD}(\mathcal{A}\mathcal{X} \supset (A_0 \wedge C \supset B_k(0)))| \geq_f v_1$$

where $v_1 = 2_{k-1}$ and f is an at most exponential function.

The 'fast' proof can be used more or less 1-1 from Orevkov's paper.

Theorem

In projective geometry, proving with sketches is in some cases non-elementary slower than using the sequent system with cuts.

Conclusions

- yet another example that proof theory and properties of Herbrand disjunctions can be used outside the purely proof theoretic realm
- combining Stateman/Orevkov's result with other 'tricks' allows transferring it to theories (as long as the models of the theory are sufficiently expressive)
- although Herbrand disjunctions are not so on vogue (proof theory and automatic reasoning being an exception), many properties are still there to uncover