The midsequent theorem and witnessing

Ondra Ježil

February 24, 2023

Context

- Cut elimination: proof $\mapsto$ cut free proof

Context

- Cut elimination: proof $\mapsto$ cut free proof
- The midsequent theorem: proof $\mapsto$ (cut free) proof split into two parts

Context

- Cut elimination: proof $\mapsto$ cut free proof
- The midsequent theorem: proof $\mapsto$ (cut free) proof split into two parts
  - an upper part which uses only structural and propositional inferences

Context

- Cut elimination: proof $\mapsto$ cut free proof
- The midsequent theorem: proof $\mapsto$ (cut free) proof split into two parts
  - an upper part which uses only structural and propositional inferences
  - a sequent S' which is the lower sequent of the last propositional inference

Context

- Cut elimination: proof $\mapsto$ cut free proof
- The midsequent theorem: proof $\mapsto$ (cut free) proof split into two parts
  - an upper part which uses only structural and propositional inferences
  - a sequent S' which is the lower sequent of the last propositional inference
  - a lower part which uses only structural and quantifier inferences

Context

- Cut elimination: proof $\mapsto$ cut free proof
- The midsequent theorem: proof $\mapsto$ (cut free) proof split into two parts
  - an upper part which uses only structural and propositional inferences
  - a sequent S' which is the lower sequent of the last propositional inference
  - a lower part which uses only structural and quantifier inferences
- This can be then used to provide some witnessing theorems which are frequently used in the context of bounded arithmetic.

The statement

Theorem (The midsequent theorem)

Let S be a sequent consisting of formulas in prenex form which is provable in LK. Then there is cut free LK-proof P of S which contains a sequent S' (called the midsequent) satisfying:

- *S' is quantifier free*

The statement

Theorem (The midsequent theorem)

Let S be a sequent consisting of formulas in prenex form which is provable in LK. Then there is cut free LK-proof P of S which contains a sequent S' (called the midsequent) satisfying:

- *S' is quantifier free*
- *Every inference above S' is either structural or propositional inference*

The statement

Theorem (The midsequent theorem)

Let S be a sequent consisting of formulas in prenex form which is provable in LK. Then there is cut free LK-proof P of S which contains a sequent S' (called the midsequent) satisfying:

- *S' is quantifier free*
- *Every inference above S' is either structural or propositional inference*
- *Every inference below S' is either structural or quantifier inference*

The proof 1/4

Proof.

We already know, that there exists a cut free proof P of S, we can also assume that only sequents of the form $A \to A$ were used as initial sequents, where A is atomic.

The proof 1/4

Proof.

We already know, that there exists a cut free proof P of S, we can also assume that only sequents of the form $A \to A$ were used as initial sequents, where A is atomic.
Let I be an inference instance in P, we define

$$\mathrm{ord}_P(I) = \text{number of propositional inferences below } I$$

and

$$\mathrm{ord}(P) = \sum_{I \text{ in } P} \mathrm{ord}_P(I).$$

The proof 1/4

Proof.

We already know, that there exists a cut free proof P of S, we can also assume that only sequents of the form $A \to A$ were used as initial sequents, where A is atomic.
Let I be an inference instance in P, we define

$$\mathrm{ord}_P(I) = \text{number of propositional inferences below } I$$

and

$$\mathrm{ord}(P) = \sum_{I \text{ in } P} \mathrm{ord}_P(I).$$

We proceed in constructing the LK-proof from the statement by induction on $\mathrm{ord}(P)$.

The proof 2/4

Proof cont.

Case $\text{ord}(P) = 0$: While in this case there is no propositional inference found below any quantifier instance, the sequenct S_0—defined as the lower sequent of the lowest propositional inference—might still contain formulas with quantifiers.

The proof 2/4

Proof cont.

Case $\text{ord}(P) = 0$: While in this case there is no propositional inference found below any quantifier instance, the sequenct S_0—defined as the lower sequent of the lowest propositional inference—might still contain formulas with quantifiers.

From the assumption on the proof P, the quantifier formula(s) could have only been introduced using weakenings. But since the end-sequent S is prenex and the proof is cut free, there were no propositional inferences applied to any of them. So the weakening can be "postponed" after S_0 which finished this case.

The proof 3/4

Proof cont.

Case $\text{ord}(P) > 0$: Now there exists some quantifier inference I under which the uppermost logical inference is a propositional inference I'.

The proof 3/4

Proof cont.

Case $\text{ord}(P) > 0$: Now there exists some quantifier inference I under which the uppermost logical inference is a propositional inference I'.We will lower the order of P by exchanging the positions of I and I'.

The proof 3/4

Proof cont.

Case $\text{ord}(P) > 0$: Now there exists some quantifier inference I under which the uppermost logical inference is a propositional inference I'.We will lower the order of P by exchanging the positions of I and I'. We restrict ourself here to the case where I is $\forall$: right so we have

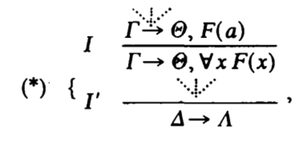
$$(*)\ \left\{\begin{array}{ll} I & \dfrac{\Gamma \to \Theta, F(a)}{\Gamma \to \Theta, \forall x F(x)} \\ & \quad\vdots \\ I' & \dfrac{\qquad\qquad}{\Delta \to \Lambda} \end{array}\right. ,$$

where $(*)$ contains only structural inferences.

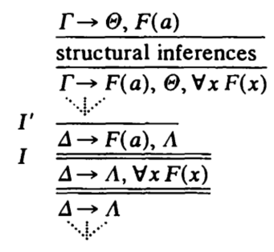
The proof 4/4

Proof cont.

The rearrangement in such a case looks like this:



$\rightarrow$



□

Herbrand's theorem

- With the midsequent theorem at our disposal we can obtain the following classical theorem.

Herbrand's theorem

- With the midsequent theorem at our disposal we can obtain the following classical theorem.

Theorem (Herbrand's theorem; [Jacques Herbrand 1930])

Let T be a universal theory in the language L, $\varphi(x, y)$ a quantifier free L-formula and let

$$T \vdash (\forall x)(\exists y)\varphi(x, y),$$

then there exist L-terms $t_1, \dots, t_n$ such that

$$T \vdash (\forall x)(\varphi(x, t_1(x)) \vee \dots \vee \varphi(x, t_n(x))).$$

Herbrand's theorem

- With the midsequent theorem at our disposal we can obtain the following classical theorem.

Theorem (Herbrand's theorem; [Jacques Herbrand 1930])

Let T be a universal theory in the language L, $\varphi(x, y)$ a quantifier free L-formula and let

$$T \vdash (\forall x)(\exists y)\varphi(x, y),$$

then there exist L-terms $t_1, \dots, t_n$ such that

$$T \vdash (\forall x)(\varphi(x, t_1(x)) \vee \cdots \vee \varphi(x, t_n(x))).$$

- Remark: If L contains no terms or constants, the situation becomes trivial, because the terms are therefore simply variables, and therefore for any universal L-theory T we have that $T \vdash (\forall x)(\exists y)\varphi(x, y)$ implies $T \vdash (\forall x)\varphi(x, x)$. (e.g. the theory of graphs)

Herbrand's theorem – the proof 1/2

Theorem (Herbrand's theorem; [Jacques Herbrand 1930])

Let T be a universal theory in the language L, $\varphi(x, y)$ a quantifier free L-formula and let

$$T \vdash (\forall x)(\exists y)\varphi(x, y),$$

then there exist L-terms $t_1, \dots, t_n$ such that

$$T \vdash (\forall x)(\varphi(x, t_1(x)) \vee \cdots \vee \varphi(x, t_n(x))).$$

Proof.

If $T \vdash (\forall x)(\exists y)\varphi(x, y)$ then there is some finite subset $\Gamma \subseteq T$ such that the sequent $\Gamma \to (\forall x)(\exists y)\varphi(x, y)$ is valid a therefore there is an LK-proof of it, called P, with a midsequent S'.

Herbrand's theorem – the proof 2/2

Proof cont.

Since S' is in P transformed into $\Gamma \to (\forall x)(\exists y)\varphi(x, y)$ by structural and quantifier inferences it has to be of the form:

$$S' : \quad \gamma_0(\bar{a}), \ldots, \gamma_n(\bar{a}) \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n).$$

Herbrand's theorem – the proof 2/2

Proof cont.

Since S' is in P transformed into $\Gamma \to (\forall x)(\exists y)\varphi(x, y)$ by structural and quantifier inferences it has to be of the form:

$$S' : \quad \gamma_0(\bar{a}), \ldots, \gamma_n(\bar{a}) \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n).$$

from which we can in LK infer (here we are using that T is universal)

$$S'' : \quad \Gamma \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n),$$

Herbrand's theorem – the proof 2/2

Proof cont.

Since S' is in P transformed into $\Gamma \to (\forall x)(\exists y)\varphi(x,y)$ by structural and quantifier inferences it has to be of the form:

$$S' : \quad \gamma_0(\bar{a}), \ldots, \gamma_n(\bar{a}) \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n).$$

from which we can in LK infer (here we are using that T is universal)

$$S'' : \quad \Gamma \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n),$$

and by weakening

$$S''' : \quad \Gamma, b_1 = b_2, b_1 = b_3, \ldots, b_1 = b_n \to \varphi(b_1, t_1), \ldots, \varphi(b_n, t_n),$$

from which the sequent $\Gamma \to \varphi(b, t_1(b)), \ldots, \varphi(b, t_n(b))$ logically follows using the equality axioms. □

A non-example

- We will instead start with an example which demonstrates that the assumption on T being universal is crucial for the theorem to hold.

A non-example

- We will instead start with an example which demonstrates that the assumption on T being universal is crucial for the theorem to hold.

Example

Let $T = \mathrm{RCF}$, the theory of real closed fields. One of the axioms of RCF is the existence of a cube root. So we trivially have

$$T \vdash (\forall x)(\exists y)(y^3 = x).$$

However, the language of RCF is the language of rings, so the only terms in L_{RCF} are polynomials with integer coefficients, which for cannot serve as an witness for y when $x := 2 \in \mathbb{R} \models \mathrm{RCF}$ and so the Herbrand disjunction cannot be provable in RCF.

A non-example

- We will instead start with an example which demonstrates that the assumption on T being universal is crucial for the theorem to hold.

Example

Let $T = \text{RCF}$, the theory of real closed fields. One of the axioms of RCF is the existence of a cube root. So we trivially have

$$T \vdash (\forall x)(\exists y)(y^3 = x).$$

However, the language of RCF is the language of rings, so the only terms in L_{RCF} are polynomials with integer coefficients, which for cannot serve as an witness for y when $x := 2 \in \mathbb{R} \models \text{RCF}$ and so the Herbrand disjunction cannot be provable in RCF.

- Can be circumvented by adding a function symbol $\text{cbroot}(-)$ and the axiom $(\forall x)\text{cbroot}(x)^3 = x$.

An example — the theory of commutative rings

- Let $L = \{0, 1, +, -, \cdot\}$ and T be the usual axiomatization of commutative rings (associativity, distributivity, properties of 1 and 0, ...).

An example — the theory of commutative rings

- Let $L = \{0, 1, +, -, \cdot\}$ and T be the usual axiomatization of commutative rings (associativity, distributivity, properties of 1 and 0, ...).
- Let $\varphi(x, p)$ be a system of polynomial equations with parameter p written out as a formula.

An example — the theory of commutative rings

- Let $L = \{0, 1, +, -, \cdot\}$ and T be the usual axiomatization of commutative rings (associativity, distributivity, properties of 1 and 0, ...).
- Let $\varphi(x, p)$ be a system of polynomial equations with parameter p written out as a formula.
- We can see that if the theory

$$T \vdash (\forall p)(\exists x)\varphi(x, p)$$

(the system has solution for every parameter p), then the Herbrand's theorem gives us a list of terms $p_1(p), p_2(p), \ldots, p_n(p)$ (which are essentially polynomials with integer coefficients) such that a solution can be always found by trying all these values.

An example – T_{PV}

- Let L_{PV} be the language containing a function f_M for every polynomial-time machine M with intended interpretation of $f_M(x)$ being the output of the machine M on a number x.

An example – T_{PV}

- Let L_{PV} be the language containing a function f_M for every polynomial-time machine M with intended interpretation of $f_M(x)$ being the output of the machine M on a number x.
- Let T_{PV} be the set of universal PV-sentences true in the intended interpretation.

An example – T_{PV}

- Let L_{PV} be the language containing a function f_M for every polynomial-time machine M with intended interpretation of $f_M(x)$ being the output of the machine M on a number x.
- Let T_{PV} be the set of universal PV-sentences true in the intended interpretation.
- Note that T_{PV} is not recursively. For example the validity of

$$(\forall x)\textsc{DoesHaltInTime}('M', 1^{|x|}) = 0$$

is not recursive for a general machine M.

An example – T_{PV}

- Let L_{PV} be the language containing a function f_M for every polynomial-time machine M with intended interpretation of $f_M(x)$ being the output of the machine M on a number x.
- Let T_{PV} be the set of universal PV-sentences true in the intended interpretation.
- Note that T_{PV} is not recursively. For example the validity of

$$(\forall x)\textsc{DoesHaltInTime}('M', 1^{|x|}) = 0$$

  is not recursive for a general machine M.
- Reasonably axiomatized subsystem PV of T_{PV} is a well studied system of bounded arithmetic and can prove a lot of the contemporary complexity theory.

An example – T_{PV} cont.

- Notice that any quantifier free L_{PV}-formula is testable in polynomial time. (Computing all the terms are equalities can be done in polynomial time.)

An example – T_{PV} cont.

- Notice that any quantifier free L_{PV}-formula is testable in polynomial time. (Computing all the terms are equalities can be done in polynomial time.)
- This is true for every disjunct from Herbrand's theorem, so there exists a polynomial time function which tries all values $t_i(x)$ and picks the one which makes the formula true.

An example – T_{PV} cont.

- Notice that any quantifier free L_{PV}-formula is testable in polynomial time. (Computing all the terms are equalities can be done in polynomial time.)
- This is true for every disjunct from Herbrand's theorem, so there exists a polynomial time function which tries all values $t_i(x)$ and picks the one which makes the formula true.
- So we get that if

$$T_{\mathrm{PV}} \vdash (\forall x)(\exists y)\varphi(x, y),$$

then there exists $f \in L_{\mathrm{PV}}$ such that

$$T_{\mathrm{PV}} \vdash (\forall x)\varphi(x, f(x)).$$

An example – T_{PV} cont.; Some complexity classes

- Let $A(x)$ be some property a number can have.

An example – T_{PV} cont.; Some complexity classes

- Let $A(x)$ be some property a number can have.
- We say $A \in \mathbf{P}$ if there is a polynomial-time machine $M(x)$ such that

$$A(x) \iff M(x) = 1$$

An example – T_{PV} cont.; Some complexity classes

- Let $A(x)$ be some property a number can have.
- We say $A \in \mathbf{P}$ if there is a polynomial-time machine $M(x)$ such that

$$A(x) \iff M(x) = 1$$

- We say $A \in \mathbf{NP}$ if there is a polynomial-time machine $M(x, y)$ and a polynomial p, such that for all x

$$A(x) \equiv \exists y, |y| \leq p(|x|) : M(x, y) = 1.$$

An example – T_{PV} cont.; Some complexity classes

- Let $A(x)$ be some property a number can have.
- We say $A \in \mathbf{P}$ if there is a polynomial-time machine $M(x)$ such that

$$A(x) \iff M(x) = 1$$

- We say $A \in \mathbf{NP}$ if there is a polynomial-time machine $M(x, y)$ and a polynomial p, such that for all x

$$A(x) \equiv \exists y, |y| \leq p(|x|) : M(x, y) = 1.$$

- We say $A \in \mathbf{coNP}$ if there is a polynomial-time machine $M(x, y)$ and a polynomial p, such that for all x

$$A(x) \equiv \forall y, |y| \leq p(|x|) : M(x, y) = 0.$$

An example – T_{PV} cont.; Some complexity classes

- Let $A(x)$ be some property a number can have.
- We say $A \in \mathbf{P}$ if there is a polynomial-time machine $M(x)$ such that

$$A(x) \iff M(x) = 1$$

- We say $A \in \mathbf{NP}$ if there is a polynomial-time machine $M(x, y)$ and a polynomial p, such that for all x

$$A(x) \equiv \exists y, |y| \leq p(|x|) : M(x, y) = 1.$$

- We say $A \in \mathbf{coNP}$ if there is a polynomial-time machine $M(x, y)$ and a polynomial p, such that for all x

$$A(x) \equiv \forall y, |y| \leq p(|x|) : M(x, y) = 0.$$

- A fundamental problem in complexity theory: Are any of $\mathbf{P}, \mathbf{NP}, \mathbf{coNP}$ equal? What about $\mathbf{P}$ and $\mathbf{NP} \cap \mathbf{coNP}$?

An example – T_{PV} cont.

- It is conjectured that **P** is different from **NP** ∩ **coNP**. (Factoring)

An example – T_{PV} cont.

- It is conjectured that **P** is different from **NP** $\cap$ **coNP**. (Factoring)

Theorem

If for some **NP** *property* φ T_{PV} *proves it is also* **coNP** *(or vice-versa) then* φ *is in fact in* **P**.

An example – T_{PV} cont.

Theorem

If for some **NP** *property* φ T_{PV} *proves it is also* **coNP** *(or vice-versa) then* φ *is in fact in* **P**.

Proof.

Let $\varphi(x)$ be of the form $(\exists y, |y| \leq p(|x|))(f(x,y) = 1)$, let $\psi(x)$ be of the form $(\forall y, |y| \leq q(|x|))(g(x,y) = 1)$, and let

$$T_{\mathrm{PV}} \vdash \varphi(x) \equiv \psi(x),$$

we also have

$$T_{\mathrm{PV}} \vdash \varphi(x) \vee \neg\psi(x).$$

By Herbrand's theorem we have that there exists a polynomial time h such that

$$T_{\mathrm{PV}} \vdash (\forall x)(f(x, h(x)) = 1 \vee g(x, h(x)) = 0)$$

now we can get a p-time algorithm deciding $\varphi(x)$ using f,g and h. □

Generalization — The KPT theorem

- Herbrand's theorem: $\forall\exists$ statement $\rightarrow$ a list of terms $t_1(a), \ldots, t_n(a)$ such that in any model, one of these terms is the witness.

Generalization — The KPT theorem

- Herbrand's theorem: $\forall\exists$ statement $\to$ a list of terms $t_1(a),\ldots,t_n(a)$ such that in any model, one of these terms is the witness.
- KPT theorem: $\forall\exists\forall$ statement $\to$ a list of terms $t_1(a), t_2(a, b_1), \ldots, t_n(a, b_1, \ldots, b_{n-1})$, if the i-th term is not valid in a given model, it gives a value b_i (corresponding to the last $\forall$ quantifier) which can then be used to compute the next value. In any model, one of these terms is the witness.

Generalization — The KPT theorem

- Herbrand's theorem: $\forall\exists$ statement $\to$ a list of terms $t_1(a), \ldots, t_n(a)$ such that in any model, one of these terms is the witness.
- KPT theorem: $\forall\exists\forall$ statement $\to$ a list of terms $t_1(a), t_2(a, b_1), \ldots, t_n(a, b_1, \ldots, b_{n-1})$, if the i-th term is not valid in a given model, it gives a value b_i (corresponding to the last $\forall$ quantifier) which can then be used to compute the next value. In any model, one of these terms is the witness.
- This can be understood as a two player game, the teacher ($\forall$-player) and a student ($\exists$-player), the game is played in any model of the theory we are considering. The teacher always picks some element, the student tries to compute a potential witness using a term, and if the witness is wrong, the teacher provides a counter example, which the student can later use to find another potential witness.

Thank you for your attention!