THE FORMALIZATION OF VICKREY AUCTIONS: A COMPARISON OF TWO APPROACHES IN ISABELLE AND THEOREMA

Alexander Maletzky and Wolfgang Windsteiger
Research Institute for Symbolic Computation (RISC)
Johannes Kepler University Linz (JKU)
CICM'10, Edinburgh, July 18, 2017

JOHANNES KEPLER
UNIVERSITÄT LINZ

RISC
RESEARCH INSTITUTE FOR
SYMBOLIC COMPUTATION

MOTIVATION FOR THIS WORK

- Auction Theory Toolbox (Kerber, Lange, Rowat @ U. Birmingham)
- CICM'2013: Comparison of 4 systems (Isabelle, Mizar, Hets/CASL/TPTP, and Theorema).
- Benchmark example: Formalization of Vickrey's Theorem on Second-Price Auctions.
- Due to re-design & re-implementation of Theorema 2.0: formalization incomplete.

MOTIVATION FOR THIS WORK

- Auction Theory Toolbox (Kerber, Lange, Rowat @ U. Birmingham)
- CICM'2013: Comparison of 4 systems (Isabelle, Mizar, Hets/CASL/TPTP, and Theorema).
- Benchmark example: Formalization of Vickrey's Theorem on Second-Price Auctions.
- Due to re-design & re-implementation of Theorema 2.0: formalization incomplete.

Status quo of Theorema-formalization in 2013:

- Theorema-GUI functional, Theorema language fully available.
- Definitions and Main Theorem available based on pencil-and-paper formalization, which served as basis for the formalizations in the other systems.
- Intermediate lemmas missing, all proofs missing.

PURPOSE OF THIS PRESENTATION

- Present complete formalization of Vickrey's Theorem in Theorema 2.0.
- Compare formalization in Theorema 2.0 to formalization in Isabelle available from the web-page of the ForMaRE project. (Created with Isabelle2013, unfortunately contains some auxiliary lemmas whose proofs are not valid in the current version of Isabelle any more.)
- Why compare only to Isabelle?

PURPOSE OF THIS PRESENTATION

- Present complete formalization of Vickrey's Theorem in Theorema 2.0.
- Compare formalization in Theorema 2.0 to formalization in Isabelle available from the web-page of the ForMaRE project. (Created with Isabelle2013, unfortunately contains some auxiliary lemmas whose proofs are not valid in the current version of Isabelle any more.)
- Why compare only to Isabelle?

About the formalization in Theorema 2.0:

- Formalization based on definitions and the Main Theorem as given in pencil-and-paper formalization, which served as basis for the formalizations in the other systems.

PURPOSE OF THIS PRESENTATION

- Present complete formalization of Vickrey's Theorem in Theorema 2.0.
- Compare formalization in Theorema 2.0 to formalization in Isabelle available from the web-page of the ForMaRE project. (Created with Isabelle2013, unfortunately contains some auxiliary lemmas whose proofs are not valid in the current version of Isabelle any more.)
- Why compare only to Isabelle?

About the formalization in Theorema 2.0:

- Formalization based on definitions and the Main Theorem as given in pencil-and-paper formalization, which served as basis for the formalizations in the other systems. $\rightsquigarrow$ fair basis for comparison!

PURPOSE OF THIS PRESENTATION

- Present complete formalization of Vickrey's Theorem in Theorema 2.0.
- Compare formalization in Theorema 2.0 to formalization in Isabelle available from the web-page of the ForMaRE project. (Created with Isabelle2013, unfortunately contains some auxiliary lemmas whose proofs are not valid in the current version of Isabelle any more.)
- Why compare only to Isabelle?

About the formalization in Theorema 2.0:

- Formalization based on definitions and the Main Theorem as given in pencil-and-paper formalization, which served as basis for the formalizations in the other systems.
- Theory development independent from previously existing formalizations.

PURPOSE OF THIS PRESENTATION

- Present complete formalization of Vickrey's Theorem in Theorema 2.0.
- Compare formalization in Theorema 2.0 to formalization in Isabelle available from the web-page of the ForMaRE project. (Created with Isabelle2013, unfortunately contains some auxiliary lemmas whose proofs are not valid in the current version of Isabelle any more.)
- Why compare only to Isabelle?

About the formalization in Theorema 2.0:

- Formalization based on definitions and the Main Theorem as given in pencil-and-paper formalization, which served as basis for the formalizations in the other systems.
- Theory development independent from previously existing formalizations.
  $\rightsquigarrow$ structurally different formalizations!

THEOREMA 2.0 VS. ISABELLE: USER'S POINT OF VIEW

	Theorema 2.0	Isabelle
Theory Development	Mathematica notebook documents	Plain-text documents

THEOREMA 2.0 VS. ISABELLE: USER'S POINT OF VIEW

	Theorema 2.0	Isabelle
Theory Development	Mathematica notebook documents	Plain-text documents
Syntax	2D human-oriented	linear unicode

THEOREMA 2.0 VS. ISABELLE: USER'S POINT OF VIEW

	Theorema 2.0	Isabelle
Theory Development	Mathematica notebook documents	Plain-text documents
Syntax	2D human-oriented	linear unicode
Proof Generation	fully automatic	interactive

THEOREMA 2.0 VS. ISABELLE: USER'S POINT OF VIEW

	Theorema 2.0	Isabelle
Theory Development	Mathematica notebook documents	Plain-text documents
Syntax	2D human-oriented	linear unicode
Proof Generation	fully automatic	interactive
Proof Presentation	human-like (explanatory text for each logical step, logical steps in natural-style)	program-like

VICKREY AUCTIONS

Second-price auctions: n bidders participating in the auction of a single indivisible good.

VICKREY AUCTIONS

Second-price auctions: n bidders participating in the auction of a single indivisible good.

Each bidder submits a sealed bid, a bidder with the highest bid wins and has to pay the price given by the second-highest bid, i. e. the maximum of the remaining bids.

VICKREY AUCTIONS

Second-price auctions: n bidders participating in the auction of a single indivisible good.

Each bidder submits a sealed bid, a bidder with the highest bid wins and has to pay the price given by the second-highest bid, i. e. the maximum of the remaining bids.

Theorem of Vickrey:

1. truthful bidding, i. e. bidding the true valuation of the good, is a weakly dominant strategy for every participant. For each bidder the payoff is not less than the payoff resulting from a different bid.

VICKREY AUCTIONS

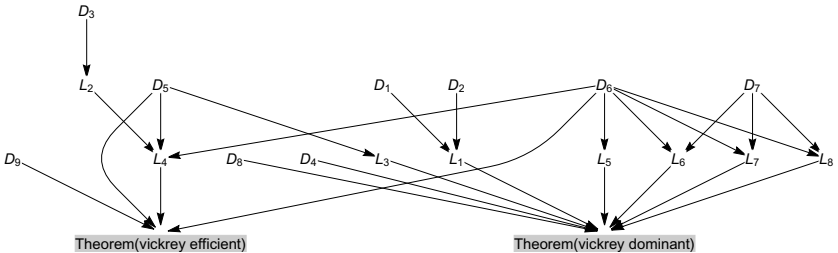
Second-price auctions: n bidders participating in the auction of a single indivisible good.

Each bidder submits a sealed bid, a bidder with the highest bid wins and has to pay the price given by the second-highest bid, i. e. the maximum of the remaining bids.

Theorem of Vickrey:

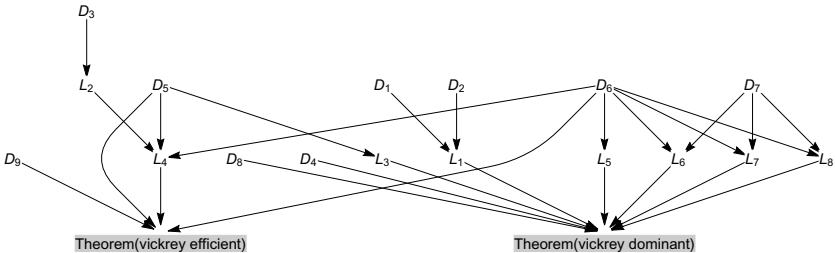
1. truthful bidding, i. e. bidding the true valuation of the good, is a weakly dominant strategy for every participant. For each bidder the payoff is not less than the payoff resulting from a different bid.
2. truthful bidding is also efficient. It is guaranteed that the winner is a bidder with maximal valuation of the good.

THEOREMA FORMALIZATION: STRUCTURE



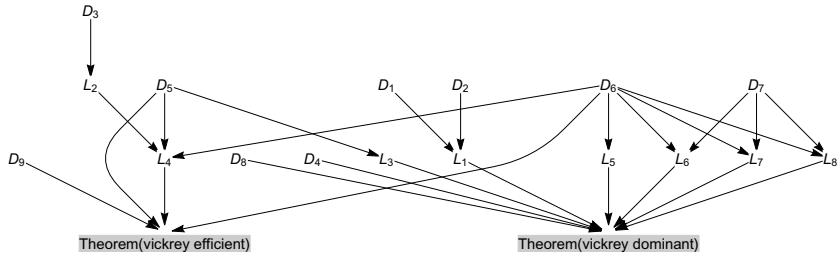
- Bids, valuations, and payments: n-tuples of numbers (Def. D_1–D_3), where b_i (v_i, p_i) represents participant i's bid (valuation, payment) of the good.

THEOREMA FORMALIZATION: STRUCTURE



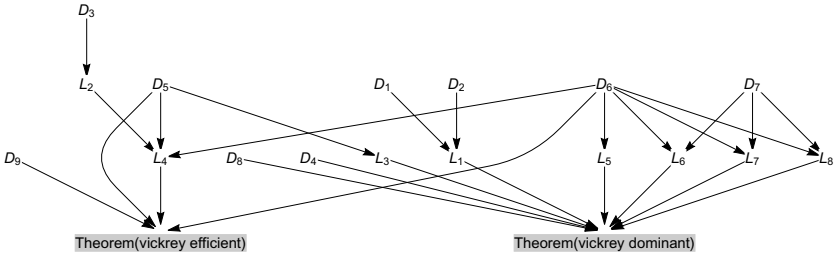
- Bids, valuations, and payments: n-tuples of numbers (Def. D_1–D_3), where b_i (v_i, p_i) represents participant i's bid (valuation, payment) of the good.
- An allocation tuple x contains exactly one 1 and otherwise 0, where $x_i = 1$ means that participants i gets the good.

THEOREMA FORMALIZATION: STRUCTURE



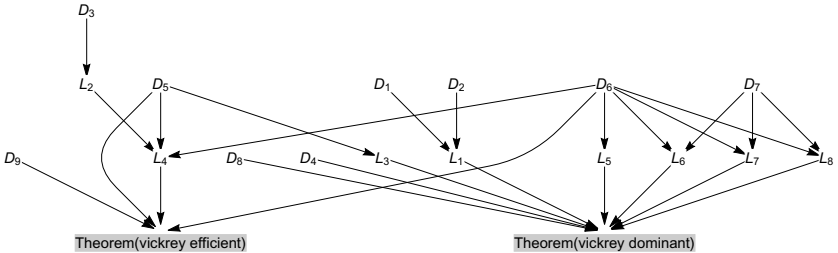
- Bids, valuations, and payments: n-tuples of numbers (Def. D_1–D_3), where b_i (v_i, p_i) represents participant i's bid (valuation, payment) of the good.
- An allocation tuple x contains exactly one 1 and otherwise 0, where $x_i = 1$ means that participants i gets the good.
- Participant i's payoff (Def. D_4): $v_i x_i - p_i$, i. e. if she gets the good it is the difference of her valuation and the payment, if she does not get the good the payoff is 0.

THEOREMA FORMALIZATION: STRUCTURE



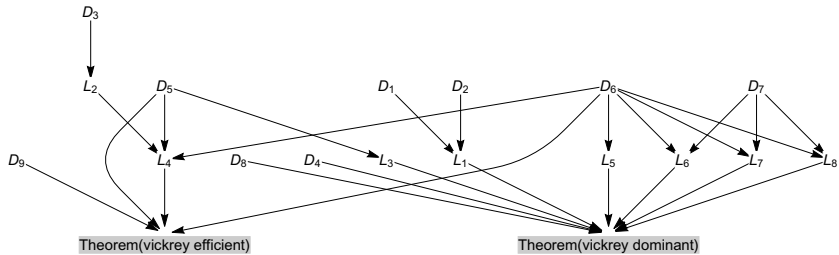
- Valuation is permitted as a bid (Lemma L_1).

THEOREMA FORMALIZATION: STRUCTURE



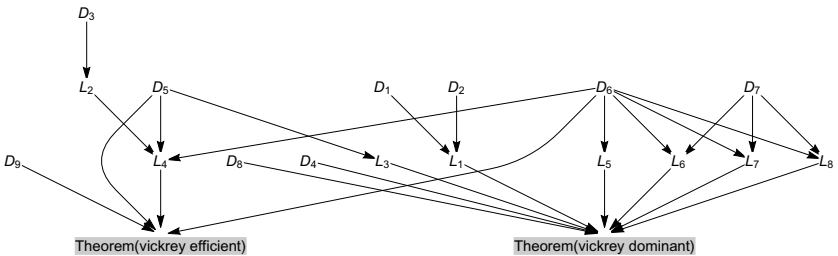
- Valuation is permitted as a bid (Lemma L_1).
- The good cannot be assigned to more than one bidder (Lemma L_2).

THEOREMA FORMALIZATION: STRUCTURE



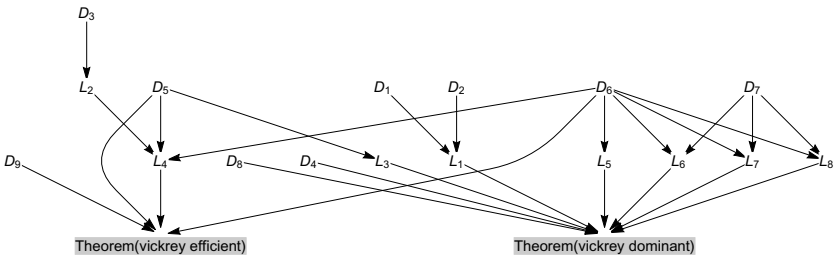
- Valuation is permitted as a bid (Lemma L_1).
- The good cannot be assigned to more than one bidder (Lemma L_2).
- Outcome of a second-price auction and participant i being winner (or loser) in a second-price auction (Def. D_5–D_7).

THEOREMA FORMALIZATION: STRUCTURE



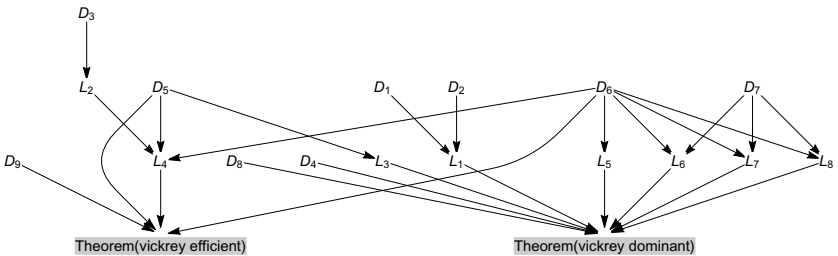
- Theorem is not proved from the definitions: one layer of intermediate lemmas (L_3–L_8).

THEOREMA FORMALIZATION: STRUCTURE



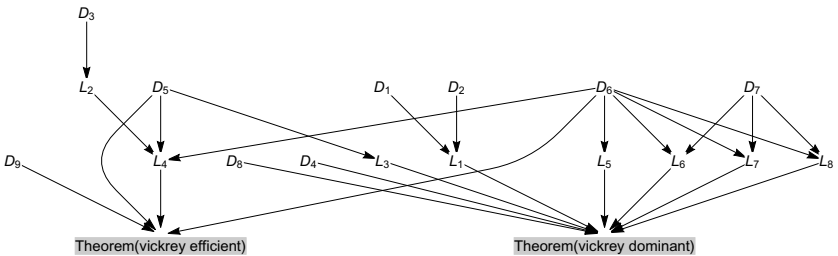
- Theorem is not proved from the definitions: one layer of intermediate lemmas (L_3–L_8).
- 4 key Lemmas L_5 to L_8.

THEOREMA FORMALIZATION: STRUCTURE



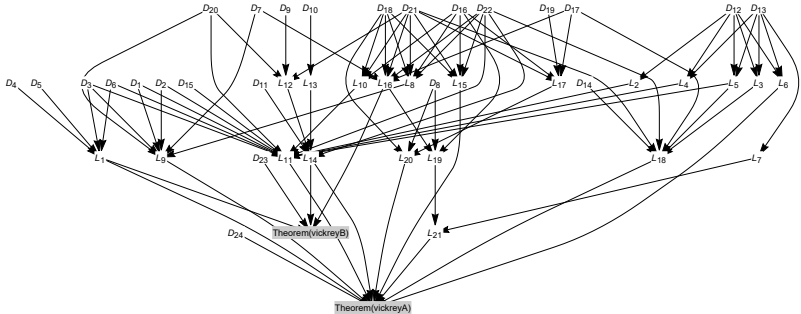
- Theorem is not proved from the definitions: one layer of intermediate lemmas (L_3–L_8).
- 4 key Lemmas L_5 to L_8.
- Lemmas L_5 and L_6 cover the cases where participant i wins with bid b_i and wins/loses with a modified bid a.

THEOREMA FORMALIZATION: STRUCTURE



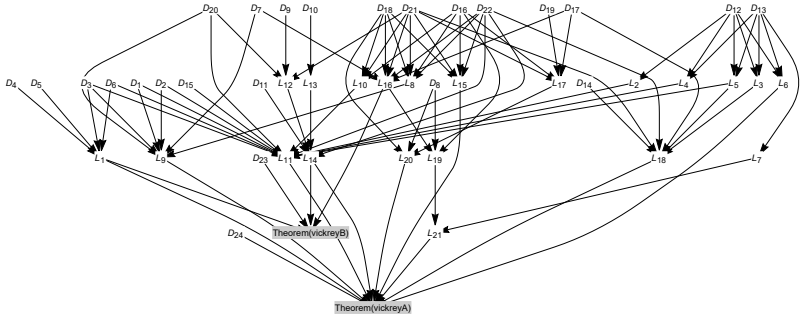
- Theorem is not proved from the definitions: one layer of intermediate lemmas (L_3–L_8).
- 4 key Lemmas L_5 to L_8.
- Lemmas L_5 and L_6 cover the cases where participant i wins with bid b_i and wins/loses with a modified bid a.
- Lemmas L_7 and L_8 are their counterparts for the case when i loses with bid b_i.

ISABELLE FORMALIZATION: STRUCTURE



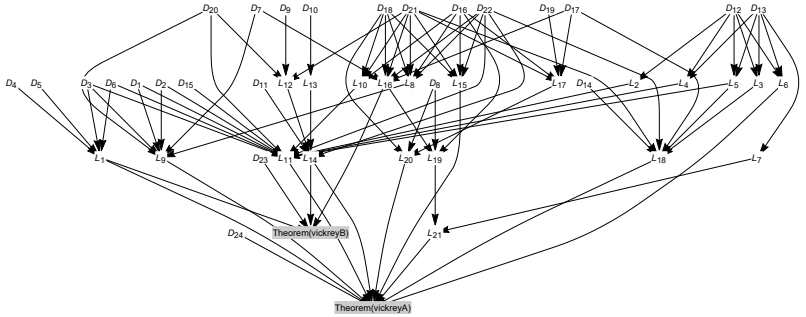
- Maximum.thy, Vectors.thy: general facts about the maximum of functions over (finite) sets and about vectors of real numbers.

ISABELLE FORMALIZATION: STRUCTURE



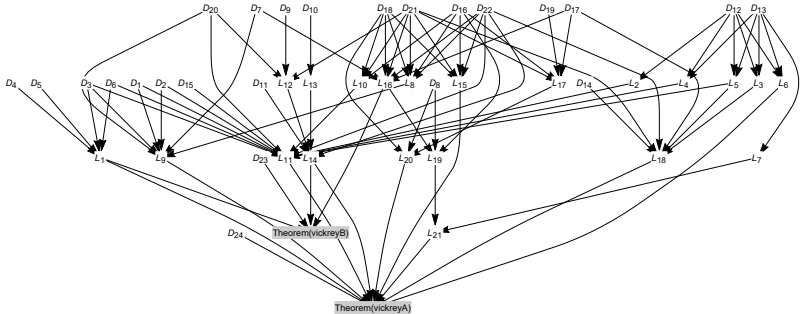
- Maximum.thy, Vectors.thy: general facts about the maximum of functions over (finite) sets and about vectors of real numbers.
- SingleGoodAuction.thy: bids, valuations, payments, etc. (only L_1 needed later, corresponds to L_1 in Theorema.)

ISABELLE FORMALIZATION: STRUCTURE



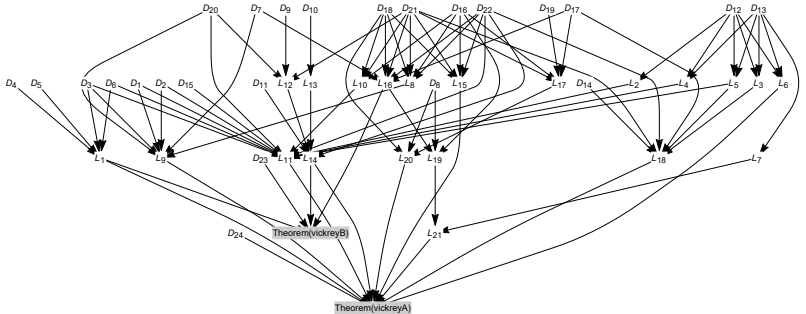
- SecondPriceAuction.thy: the property of being a second-price auction and various other auxiliary notions (e. g. winners and losers of second-price auctions).

ISABELLE FORMALIZATION: STRUCTURE



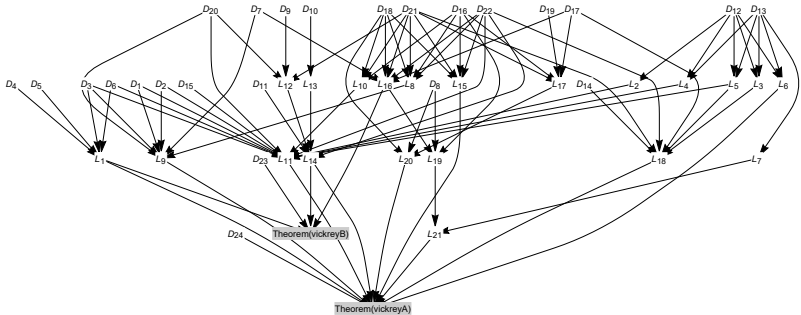
- SecondPriceAuction.thy: the property of being a second-price auction and various other auxiliary notions (e. g. winners and losers of second-price auctions).
- SingleGoodAuctionProperties.thy: definitions of weakly dominant strategies and efficiency.

ISABELLE FORMALIZATION: STRUCTURE



- Vickrey.thy: several auxiliary lemmas (second-price auctions result in non-negative payments for all participants (L_{11}), every second-price auction is also a single-good auction (L_{14}), payoffs of the winner and the losers, payoff of the winner if she deviates from her valuation (L_{21})).

ISABELLE FORMALIZATION: STRUCTURE



- Vickrey.thy: statements and proofs of the two main theorems (vickreyA, vickreyB).

WHY IS ISABELLE STRUCTURE MORE ELABORATE?

- Properties of ‘max’ proved on object-level, while Theorema uses built-in rules for ‘max’, since it is part of the Theorema language.

WHY IS ISABELLE STRUCTURE MORE ELABORATE?

- Properties of ‘max’ proved on object-level, while Theorema uses built-in rules for ‘max’, since it is part of the Theorema language.
- Goal of Isabelle formalization was more ambitious (not only Vickrey’s Theorem).

WHY IS ISABELLE STRUCTURE MORE ELABORATE?

- Properties of ‘max’ proved on object-level, while Theorema uses built-in rules for ‘max’, since it is part of the Theorema language.
- Goal of Isabelle formalization was more ambitious (not only Vickrey’s Theorem).
- The four crucial lemmas L_5–L_8 in the Theorema formalization do not have analogues in Isabelle. Instead, the four cases in the proof of vickreyA are proved directly, without making use of any lemmas.

SIZE/COMPLEXITY OF FORMALIZATIONS

‘De Bruijn factor’ (= formalization size divided by the size of an informal TEX-source, measured after stripping comments and xz-compression): does not reflect complexity/difficulty.

Counts formatting information and automatically generated content.

SIZE/COMPLEXITY OF FORMALIZATIONS

‘De Bruijn factor’ (= formalization size divided by the size of an informal TEX-source, measured after stripping comments and xz-compression): does not reflect complexity/difficulty.

Counts formatting information and automatically generated content.

Instead, we count proof steps.

SIZE/COMPLEXITY OF FORMALIZATIONS

Theorema: One proof step = one application of an inference rule.

- Not necessarily one inference rule in classical logic, because Theorema allows specialized proof rules.
- Depends target audience.
- Here: standard predicate logic prover + a few special rules dealing with tuples and max.

SIZE/COMPLEXITY OF FORMALIZATIONS

Theorema: One proof step = one application of an inference rule.

- Not necessarily one inference rule in classical logic, because Theorema allows specialized proof rules.
- Depends target audience.
- Here: standard predicate logic prover + a few special rules dealing with tuples and max.

Isabelle: Counting proof steps is tricky.

- '**unfolding** ⟨*defs*⟩ **by** *simp*': 2 steps?
- the same effect achieved by: '**by** (*simp add:* ⟨*defs*⟩)': 1 step?
- Here: **fix**, **assume**, **obtain**, **have**, **define**, **unfolding**, **qed**, **next**, *of*, *OF*, etc.: 1 step;
  proof, **apply** and **by**: n steps, where n is the number of proof methods passed as arguments.

SIZE/COMPLEXITY OF FORMALIZATIONS

	Theorema 2.0	Isabelle	Isabelle new
# steps total	171	247	185
# steps Vickrey part 1	41	113	50
# steps Vickrey part 2	20	13	13

FORMALIZATION OF VICKREY AUCTIONS: TECHNICAL COMPARISON

- Theorema uses predicates for properties, Isabelle often uses sets.

FORMALIZATION OF VICKREY AUCTIONS: TECHNICAL COMPARISON

- Theorema uses predicates for properties, Isabelle often uses sets.
- Theorema uses a more specialized definition for losers than Isabelle.

FORMALIZATION OF VICKREY AUCTIONS: TECHNICAL COMPARISON

- Theorema uses predicates for properties, Isabelle often uses sets.
- Theorema uses a more specialized definition for losers than Isabelle.
- Theorema uses symbolic tuple computations in various places, e.g.

$$(t_{i \leftarrow x})_i = x$$

Not all side-conditions are checked, yet. In particular, in the presence of ‘max’. This needs an improvement of the computation mechanism, in order to access the knowledge base of the current proof. (see demo)

THE PROOFS IN THE TWO SYSTEMS

- System Demo: Theorema 2.0
- System Demo: Isabelle

CONCLUSION & OUTLOOK

- Improve symbolic computation in Theorema.
- Knowledge archives in Theorema in order to store/distribute structured formalizations.