No Counter-Example Interpretation (based on Section 2.3 of Kohlenbach's "Applied Proof Theory")

Bruno Woltzenlogel Paleo

Theoretische Informatik und Logik
Institut für Computersprachen
Technische Universität Wien

2008, November 27th

- Unwinding of Proofs | Proof Mining | Applied Proof Theory
  - “What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?” - Kreisel
  - Extraction of ‘constructive data’ from proofs, e.g. extraction of functionals that realize (or at least establish bounds for) the existential quantifiers in the proved theorems.

- Successful cases for Π^0_2-sentences (Infiniteness):
  - An upper bound for the $(r + 1)$-th prime number extracted from Euclid's proof of the infiniteness of primes.
  - A better upper bound extracted from Euler's proof of the infiniteness of primes.
- A successful case for a Σ^0_2-sentence (Finiteness):
  - Luckhardt's analysis of a proof of Roth's theorem.

What we have learned so far...

The failures so far...

- Unsuccessful cases:
  - Σ^0_2-sentences in Peano Arithmetic (Proposition 2.4: can contradict Goedel's second incompleteness theorem)
  - Π^0_3-sentences:
    - $\forall u \exists v \forall w (T(u,u,v) \vee \neg T(u,u,w))$ (Page 2: any function f realizing $\exists v$ could be used to decide the halting problem.)
    - $\forall k \exists n \forall m (|a_n - a_{n+m}| < 2^{-k})$

How to Handle the Unsuccesful Cases?

- Herbrand (Skolem) Normal Form
- Herbrand's Theorem and Herbrand Disjunctions
- No Counter-example Interpretation

Skolem Normal Form

Definition (According to the book)

$$A \equiv \forall x_1 \exists y_1 \dots \forall x_n \exists y_n A_0[x_1, y_1, \dots, x_n, y_n]$$

$$A^S \equiv \forall x_1 \dots \forall x_n A_0[x_1, f_1(x_1), \dots, x_n, f_n(x_1, \dots, x_n)]$$

Properties

- A is unsatisfiable iff A^S is unsatisfiable
- $\models \neg A$ iff $\models \neg A^S$

Remarks

- It is not a perfect definition.
  - It does not consider blocks of quantifiers of the same type (e.g. $A \equiv \forall x_1 \forall x_2 \exists y_1 \exists y_2 A_0[x_1, x_2, y_1, y_2]$).
  - It requires prenex forms (and prenexification is bad).
    - e.g. for $A \equiv \forall x P(x) \vee \exists y P(y)$, prenex skolemization possibly gives $\forall x (P(x) \vee P(f(x)))$, while structural skolemization gives $\forall x P(x) \vee P(c)$.

Herbrand Normal Form

Definition (Almost according to the book)

$$A \equiv \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0[x_1, y_1, \ldots, x_n, y_n]$$

$$A^H \equiv \exists x_1 \ldots \exists x_n A_0[x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)]$$

Properties

- A is valid iff A^H is valid
- $\models A$ iff $\models A^H$
- $PL \nvdash A^H \rightarrow A$
- $PL_{-=} \vdash A \rightarrow A^H$

Remarks

- Herbrandization is the dual of Skolemization.
- The same remarks as for Skolem normal form.

Herbrand Normal Form

Definition (According to the book)

$$A \equiv \forall y_0 \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0[y_0, x_1, y_1, \ldots, x_n, y_n]$$

$$A^H \equiv \forall y_0 \exists x_1 \ldots \exists x_n A_0[y_0, x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)]$$

Remarks

- Why? To extract functions!

Herbrand Normal Form

Definition (If a higher-order language is available)

$$A \equiv \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0[x_1, y_1, \ldots, x_n, y_n]$$

$$A^H \equiv \forall f_1 \ldots \forall f_n \exists x_1 \ldots \exists x_n A_0[x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)]$$

Properties

- A is valid iff A^H is valid
- $\models A$ iff $\models A^H$
- $PL \nvdash A^H \rightarrow A$
- $PL_{-=} \vdash A \rightarrow A^H$
- $PL^2_{-=} + \mathrm{AxiomofChoice} \vdash A^H \rightarrow A$
- AC Schema: $\forall x \exists y A[x, y] \rightarrow \exists f \forall x A[x, f(x)]$
- AC: $\forall P(\forall x \exists y P(x, y) \rightarrow \exists f \forall x P(x, f(x)))$

Very Informal Definition

Let s be a sequent. Remove all strong quantifiers (Qx) and replace the respective strongly quantified variables x by skolem terms $f_x(y_1, \ldots, y_n)$, where $y_1, \ldots, y_n$ are all the weakly quantified variables whose quantifiers have scope over (Qx).

Remarks

- Skolemization in the antecedent.
- Herbrandization in the consequent.
- Avoids Prenexification.

Herbrand's Theorem

Herbrand's Theorem

$\models \exists y_1 \ldots \exists y_k A[y_1, \ldots, y_k]$ iff there is a finite sequence of terms t_{ij} with $1 \leq i \leq r$ and $1 \leq j \leq k$ such that

$$\models \bigvee_{i=0}^{r} A[t_{i1}, \ldots, t_{ik}]$$

Remarks

- Proof via completeness of cut-free *LK* and elimination|introduction of quantifiers and contractions. (Buss' "Handbook of Proof Theory")
- As stated above, applicable to prenex Σ_1^0 formulas. Can be extended to arbitrary Δ_n^0 formulas, by first Herbrandizing the formulas.
- Can be extended to non-prenex formulas.
- Can be extended to theorems of "open" theories, and also to arbitrary theories if they are skolemized first.
- Herbrand's original theorem was general. (Buss' "Handbook . . . ")
- Can be extended to higher-order logics. (Miller's Ph.D. Thesis)

Example of Herbrand Disjunction

$$A \equiv \forall u \exists v \forall w (T(u,u,v) \vee \neg T(u,u,w))$$

$$A^H \equiv \forall u \forall g \exists v (T(u,u,v) \vee \neg T(u,u,g(v)))$$

There is no f such that:

$$\forall u \forall g (T(u,u,f(u)) \vee \neg T(u,u,g(f(u))))$$

But a Herbrand disjunction exists:

$$A^{HD} \equiv \forall u \forall g ((T(u,u,u) \vee \neg T(u,u,g(u))) \vee (T(u,u,g(u)) \vee \neg T(u,u,g(g(u)))))$$

The disjunction can be "summarized" by using a functional. There exists Φ such that:

$$\forall u \forall g ((T(u,u,\Phi(u,g)) \vee \neg T(u,u,g(\Phi(u,g))))$$

$$\Phi(u,g) \equiv \textbf{if} \quad \neg T(u,u,g(u)) \quad \textbf{then} \quad u \quad \textbf{else} \quad g(u)$$

No Counter-Example Interpretation

$$A \equiv \exists x \forall y A_0[x, y]$$

$$nci(A) \equiv \exists \Phi \forall f A_0[\Phi(f), f(\Phi(f))]$$

Remarks

- $A \equiv_{AC} nci(A)$
- "Dependence" on axiom of choice is not mentioned in the book.
- There is no guarantee that Φ is computable|recursive (but examples will show that at least sometimes it is).
- Φ "satisfies the no counter-example of" A.

Examples

- Proposition 2.26
- Proposition 2.23
- Proposition 2.24
- Proposition 2.25

What comes next?

- *No Counter-Example Interpretation* does not work in the presence of Modus Ponens in Proofs.
- This problem will be solved next week.