Isabelle/HOL による証明とプログラミング

～ PPL サマースクール 2017 ～

山田晃久 (University of Innsbruck)

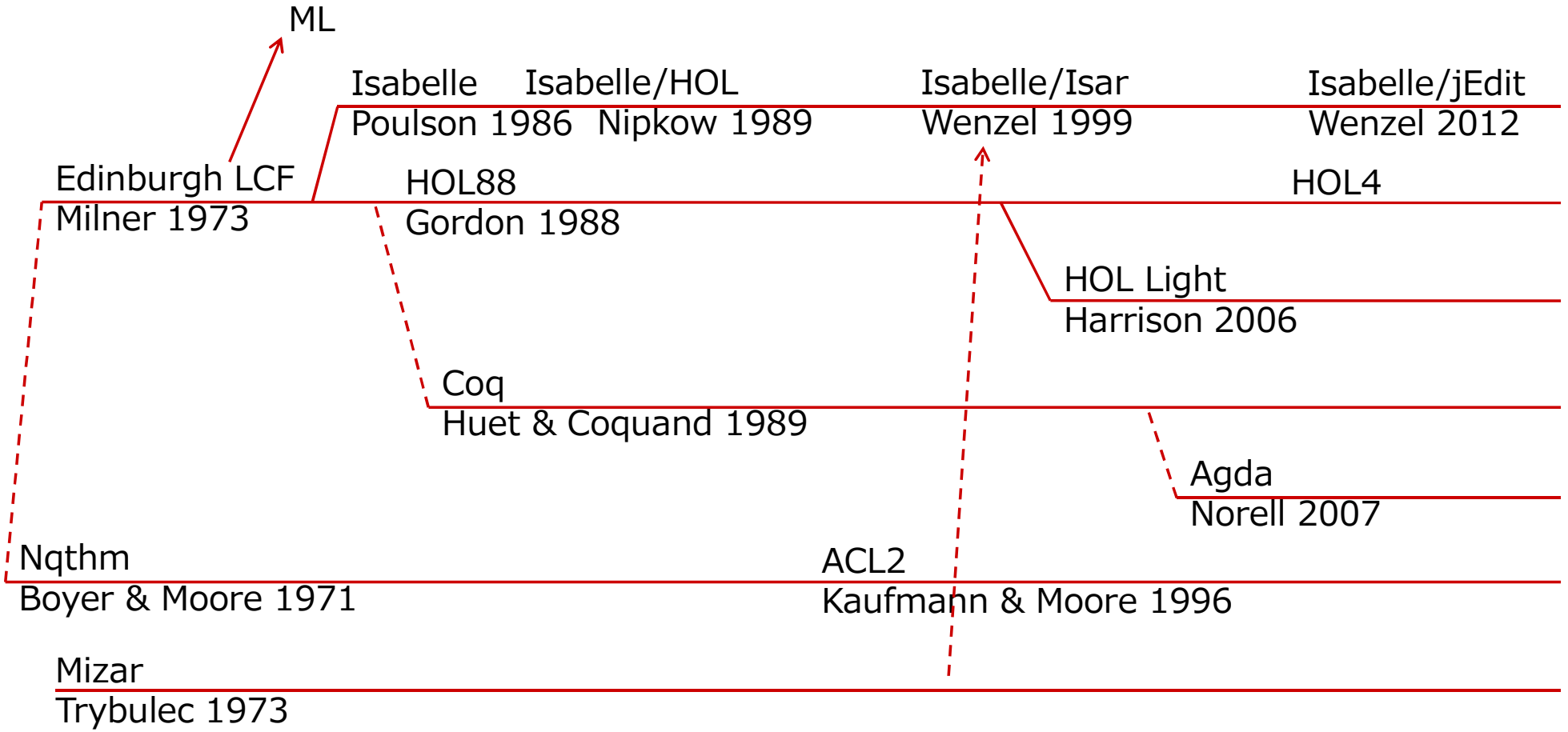
インストールはお済ですか？

- Isabelle の入手先
  - http://isabelle.in.tum.de/
  - 開発バージョン:

    hg clone http://isabelle.in.tum.de/repos/isabelle
- 起動しておいてください
  - ライブラリがビルド (証明チェック) される
  - 一度ビルドしておけば (ライブラリのソースを更新するまで)有効
- Windowsユーザーの方へ
  - Cygwinが丸ごと付いて来ます!!

    .../Isabelle2016-1/Cygwin-Terminal.bat

証明支援ツール系図


ML
Isabelle
Poulson 1986
Isabelle/HOL
Nipkow 1989
Isabelle/Isar
Wenzel 1999
Isabelle/jEdit
Wenzel 2012
Edinburgh LCF
Milner 1973
HOL88
Gordon 1988
HOL4
HOL Light
Harrison 2006
Coq
Huet & Coquand 1989
Agda
Norell 2007
Nqthm
Boyer & Moore 1971
ACL2
Kaufmann & Moore 1996
Mizar
Trybulec 1973

Isabelleの特徴

- スマートな証明環境 (Prover IDE)
- 自由な記法
- 自動証明
  - simp, auto, meson, presburger, ...
  - sledgehammer
- 証明 ≠ プログラム
  - プログラム"抽出" vs. "輸出" (code_export)
- 豊富なライブラリ
  - .../Isabelle2016-1/src/HOL/*
  - Archive of Formal Proofs (http://www.isa-afp.org)

注意点

- クセ
  - ダブルクオート(")が多い … 本質ではない
  - 自由すぎる記法 … グローバルな記法の導入は慎重に
  - 同義語が多い … 覚えなくてよい
  - 2段階のロジック … 無限でないだけマシ，本質ではない
- Isabelleは歴史が深い
  - 掘れば遺構が出てくる … 掘らない
- Isabelleは発展途上
  - 互換性... … 保守性を意識した証明を

本日の計画

10:00 ----

Isabelleの基礎，ロジック: Pure & HOL

～小休憩～

関数定義，code export

12:00 ----

～昼休み～

13:30 ----

Isabelleによるプログラミングと証明(インサートソート)

+小休憩

15:00 ----

～休憩～

15:30 ----

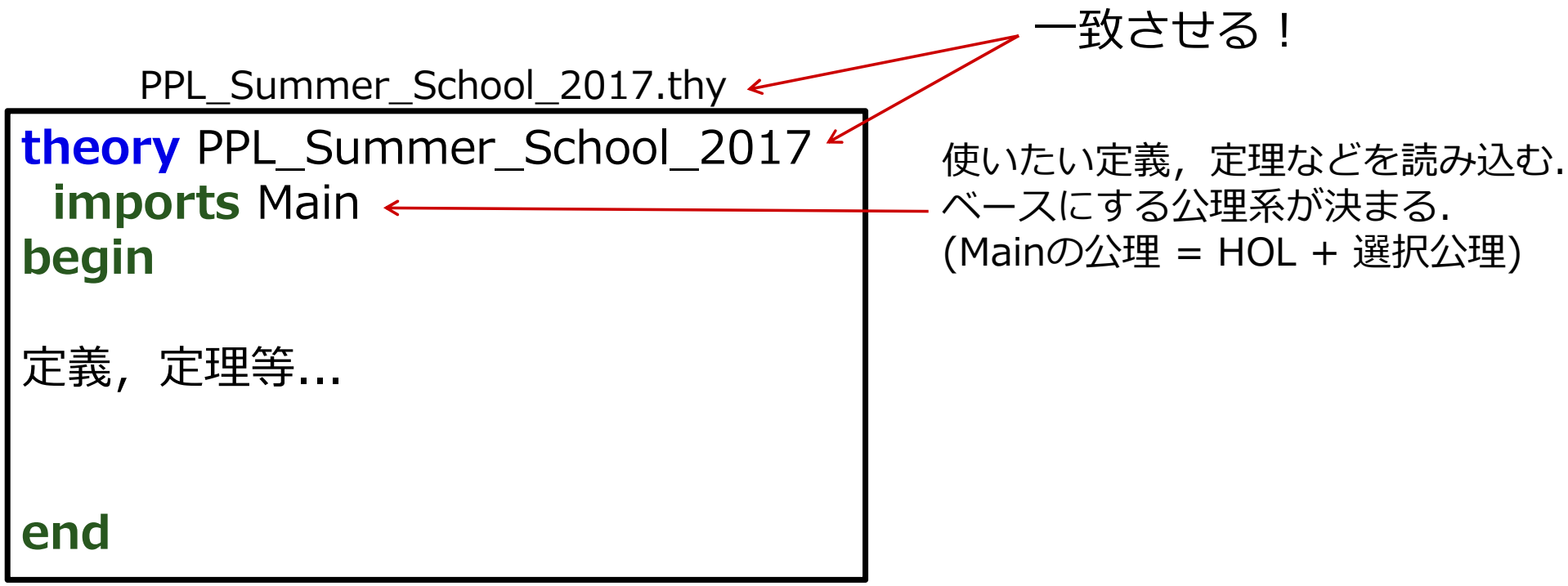
クラス，ロケール

～小休憩～

Archive of Formal Proofsの紹介，まとめ

17:00 ----

Theory (.thy) ファイル



定義と定理

- **definition** [定数名 [:: "型"] **where**] "左辺 = 右辺"
  - 非再帰的
- **fun** 定数名 [:: "型"] **where** "左辺 = 右辺" | ...
  - 再帰的
  - 全域性，停止性が自動証明 (失敗する場合 **function**)

≡でも可

≡は不可

- **theorem**/**lemma**/**proposition**/**corollary** 定理名:
  "結論" [**and** ...]
  〈証明〉

証明: Isar と apply

- applyスクリプト (旧)

```
apply (rule my_theorem)
apply (unfold my_def)
apply auto
done
```

  - トップダウン
  - ゴールの変形を繰り返す
  - 極力避ける
  - 作業中はよく使う

- Isar (新)

```
proof-
  assume "xxx"
  then have y: "yyy"
    by (unfold my_def)
  show "zzz" using y by auto
qed
```

  - ボトムアップ
  - 補題の積み重ね
  - 人が書く証明に近い
  - メンテしやすい

Isabelleのロジック: Pure と HOL

- Pure:

$$x \mid \Phi \Longrightarrow \Phi \mid \bigwedge x.\, \Phi \mid \Phi \;\&\&\&\; \Phi \mid \Phi \equiv \Phi \mid \lambda x.\, \Phi \mid \Phi\ \Phi$$

  - 直観主義的(?)
  - Isabelleが(ほぼ)自動的に処理

- HOL (Higher Order Logic):

$$x \mid \phi \longrightarrow \phi \mid \forall x.\, \phi \mid \phi \wedge \phi \mid \phi = \phi \mid \phi \vee \phi \mid \exists x.\, e \mid \mathrm{True} \mid \mathrm{False}$$

  - 古典論理，表現力が豊か
  - 公理・補題を適用してPureレベルに変換する必要がある

実践

本日の計画

10:00 ----

Isabelleの基礎，ロジック: Pure & HOL

～小休憩～

関数定義，code export

12:00 ----

～昼休み～

13:30 ----

Isabelleによるプログラミングと証明(インサートソート)

+小休憩

15:00 ----

～休憩～

15:30 ----

クラス，ロケール

～小休憩～

Archive of Formal Proofsの紹介，まとめ

17:00 ----

Archive of Formal Proofs

- Isabelle証明を集めた "Journal"
  - Number of Articles: 375
  - Number of Authors: 264
  - Number of lemmas: ~100,100
  - Lines of Code: ~1,675,000
- 投稿するメリット
  - Isabelle開発者に保守責任
- デメリット
  - 公開しなければならない
  - 変更はできるが，しづらい (他の人に使われる想定)

AFPデモ

- Algebraic Numbers

その他

- Isabelleの活きる用途
  - 論文書き: 証明を間違えるリスクがない
  - ライブラリ開発 (簡潔な再帰構造を持つ)
  - 自動解析ツールの Certification

    証明を見つけるのは大変，見つかった証明をチェックするのは簡単
    - CeTA [Sternagel, Thiemann, et al. '09~]
    - "Efficient Verified (UN)SAT Certificate Checking" [Lammich '17]
- Isabelleの(まだ)活きない用途
  - **fun** はスケールしない (大規模プログラムに弱い)
    - cf. https://sel4.systems/

メジャーな国際会議

- ITP: International Conference on Interactive Theorem Proving
  - 例年夏～秋開催
  - 2018年は7月にOxfordにて
    http://www.floc2018.org/
  - 'Interactive'な要素が好まれる(？)
- CPP: ACM SIGPLAN Conference on Certified Programs and Proofs
  - 例年1月開催 (POPLと共同)，投稿締め切り10月ごろ