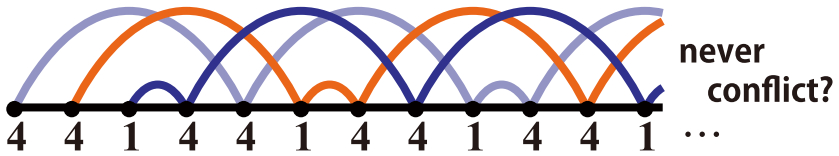
証明士入門

——— そのプログラム，本当に正しいですか？ ———

数学者だけでなくプログラマにも証明の技術が必要となる時代が近づいています．

「証明」は命題の数学的な正しさの根拠となるものですが，数学に限ったものではありません．昨今多発しているプログラムミスによる事故や損失を回避するために，プログラムの動作を事前に確認する方法としても数学的な証明が活躍しています．ただ，証明そのものが正しくなければ意味がありません．数学者が通常行う紙と鉛筆による証明では，論理の飛躍や不注意による誤りを含む可能性があります．

この問題を解決するために開発されたのが定理証明支援系 Coq です．Coq では機械的に証明の正しさを検査できる枠組みが実現されており，フィールズ賞を受賞した数学者にも採用されたという実績もあるツールです．本研修では，Coq を扱うことができる証明士を目指し，簡単な証明から徐々に難しい証明へチャレンジしてもらいます．



形式化

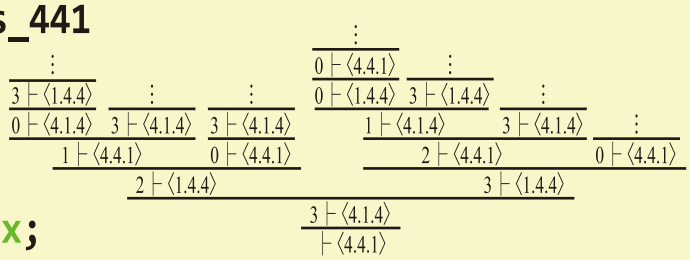
$$\frac{\vdash t}{\vdash 0 ::\sim t}\ (\textsc{Waiting}) \qquad \frac{n \vdash t}{\vdash (n+1) ::\sim t}\ (\textsc{FirstToss})$$

$$\frac{n \vdash t}{0 \vdash (n+1) ::\sim t}\ (\textsc{CatchToss}) \qquad \frac{n \vdash t}{n+1 \vdash 0 ::\sim t}\ (\textsc{NoToss})$$

$$\frac{n \vdash t \qquad m \vdash t \qquad n \neq m}{n+1 \vdash (m+1) ::\sim t}\ (\textsc{Tossable})$$

証明

```
Theorem toss_441_valid : ⊢ toss_441
Proof.
  assert(0 ⊢ toss_441); cofix;
    assert(1 ⊢ toss_441); cofix;
      assert(2 ⊢ toss_441); cofix;
        rewrite eq_unfold_toss; simpl; repeat constructor; auto.
Qed.
```



[参考図書]

萩原 学，アフェルト レナルド著「Coq/SSReflect/MathComp による定理証明」（森北出版）

Daniel P. Friedman, Carl Eastlund 著，中野 圭介 監訳「定理証明手習い」（ラムダノート社）