Nakano Lab. at RIEC

Be a Little Prover !

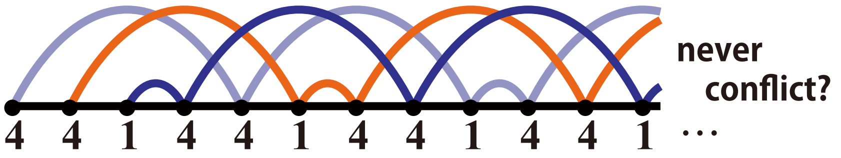
——— Is your program really correct? ———

Proof technique is no longer only for mathematicians but also programmars!

Proof of a mathematical statement, which is logical evidence to establish the truth of the statement, is not only for mathematics but also for informatics. For example, fatal accidents and economic damage caused by program bugs might be avoided by having proof for program behavior properties. The proof in this context must be definitely correct. They must not contain either logical leap or human errors, which apt to occur in pencil-and-paper proofs as usually done by mathematicians.

An interactive proof assistant, called Coq, has been developed to solve this problem and is now used for certifying proofs mechanically by programmers and mathematicians, including a Fields Medalist, V. Voevodsky.

The goal of this lecture is to be a `prover' by challenging theorem proving problems from easy to hard.



Formalization

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

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

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

Proof

```
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.
```

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{3 \vdash \langle 1.4.4\rangle}}{0 \vdash \langle 4.1.4\rangle} \quad \dfrac{\vdots}{3 \vdash \langle 4.1.4\rangle}}{1 \vdash \langle 4.4.1\rangle} \quad \dfrac{\dfrac{\vdots}{3 \vdash \langle 4.1.4\rangle}}{0 \vdash \langle 4.4.1\rangle}}{2 \vdash \langle 1.4.4\rangle} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{0 \vdash \langle 4.4.1\rangle}}{0 \vdash \langle 1.4.4\rangle} \quad \dfrac{\vdots}{3 \vdash \langle 1.4.4\rangle}}{1 \vdash \langle 4.1.4\rangle} \quad \dfrac{\vdots}{3 \vdash \langle 4.1.4\rangle}}{2 \vdash \langle 4.4.1\rangle} \quad \dfrac{\vdots}{0 \vdash \langle 4.4.1\rangle}}{3 \vdash \langle 1.4.4\rangle}}{3 \vdash \langle 4.1.4\rangle}}{\vdash \langle 4.4.1\rangle}$$