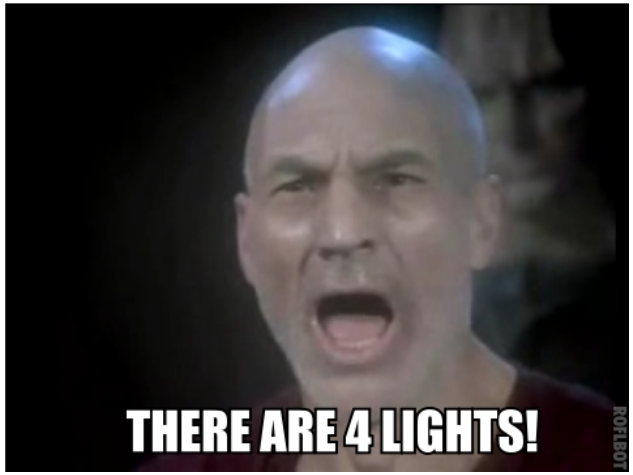
What's in a Proof?

Alex Vondrak

Cal Poly Pomona

November 14, 2012



An Anecdote

The Reason

```
Theorem a: 2 + 2 = 4.
```

The Reason

```
Theorem a: 2 + 2 = 4.
```

```
Proof.
  trivial.
Qed.
```

Coq

- An interactive theorem prover started in 1984
- Provides a formal language and environment for mathematical definitions, algorithms, theorems, and machine-checked proofs
- Language based on a derivative of the calculus of constructions (CoC)

Example

```
Theorem two_and_two_make_four: 2 + 2 = 4.
Proof.
  trivial.
Qed.
```

Coq

- An interactive theorem prover started in 1984
- Provides a formal language and environment for mathematical definitions, algorithms, theorems, and machine-checked proofs
- Language based on a derivative of the calculus of constructions (CoC)

Example

```
Theorem two_and_two_make_four: 2 + 2 = 4.
Proof.
  auto 1.
Qed.
```

Proof Automation

Rough Algorithm

```
auto n =
  if no more subgoals then
    success
  if n == 0 then
    failure
  foreach term in hypotheses ∪ hints :
    try
      apply term.
      foreach subgoal generated :
        auto (n - 1) on that subgoal
```