Things We Know
Or: Things We Should Know

April 4, 2016
Outline

1. Types

2. Notation

3. Starting and Finishing Proofs
What’s Wrong?

```java
int a = 20;
int r = 100;
boolean sum = a * r;
```
What’s Wrong?

```java
int sum = 0;
int A[] = new int[10];
fill(A);  // defined to fill the array
for (int i = 0; i < 10; i++) {
    if (A[i])
        sum += A[i];
}
```
And Now?

Prove: For all positive $n$, $5|n^5 + n$
Basis:
$P(1) = 0$ check.
And Now?

$$\sum_{i=0}^{n} F_i = F_{n+2} + 1 \rightarrow F_{n+1}$$
Notation

\[ \sum_{i=0}^{n} f(i) \]

\[ \sum_{i=0}^{n} a_i \]
Notation

- \( \sum_{i=0}^{n} f(i) \)
- \( \sum_{i=0}^{n} a_i \)
- \( \prod_{i=0}^{n} f(i) \)
- \( \prod_{i=0}^{n} a_i \)
Notation

\[ \sum_{i=0}^{n} a_i \]

What are the types of \( a_i \)?

\[ \prod_{i=0}^{n} a_i \]

What are the types of \( p_i \)?

\[ \bigcup_{i=0}^{n} p_i \]

What are the types of \( s_i \)?
Notation

- \( \sum_{i=0}^{n} a_i \) What are the types of \( a_i \)?

- \( \prod_{i=0}^{n} a_i \) What are the types of \( a_i \)?
Notation

- $\sum_{i=0}^{n} a_i$
- $\prod_{i=0}^{n} a_i$ What are the types of $a_i$?
- $\bigwedge_{i=0}^{n} p_i$

What are the types of $p_i$?
Notation

\[ \sum_{i=0}^{n} a_i \]

\[ \prod_{i=0}^{n} a_i \] What are the types of \( a_i \)?

\[ \bigwedge_{i=0}^{n} p_i \]

\[ \bigvee_{i=0}^{n} p_i \] What are the types of \( p_i \)?

Things We Know

April 4, 2016 8 / 15
Notation

\[ \sum_{i=0}^{n} a_i \]
What are the types of \( a_i \)?

\[ \prod_{i=0}^{n} a_i \]
What are the types of \( a_i \)?

\[ \bigwedge_{i=0}^{n} p_i \]
What are the types of \( p_i \)?

\[ \bigvee_{i=0}^{n} p_i \]
What are the types of \( p_i \)?

\[ \bigcup_{i=0}^{n} s_i \]
Notation

- $\sum_{i=0}^{n} a_i$  What are the types of $a_i$?
- $\prod_{i=0}^{n} a_i$  What are the types of $a_i$?
- $\bigwedge_{i=0}^{n} p_i$  What are the types of $p_i$?
- $\bigvee_{i=0}^{n} p_i$  What are the types of $p_i$?
- $\bigcup_{i=0}^{n} s_i$  What are the types of $s_i$?
- $\bigcap_{i=0}^{n} s_i$  What are the types of $s_i$?
Proof Setup

Prove: The product of two odd numbers is odd.
Proof Setup

Prove: The product of two odd numbers is odd.
\[ \forall a, b \in \mathbb{Z} \ odd(a) \land odd(b) \rightarrow odd(ab) \]
What are the premises and consequence for a proof by contradiction?
Proof Setup

Prove: The product of two odd numbers is odd.
\( \forall a, b \in \mathbb{Z} \; odd(a) \land odd(b) \rightarrow odd(ab) \)

What are the premises and consequence for a proof by contradiction?

Premises: \( \forall a, b \in \mathbb{Z} \; odd(a) \land odd(b) \land \neg odd(ab) \)

Consequence: Some contradiction
\( \forall a, b \in \mathbb{Z} \; odd(a) \land odd(b) \land \neg odd(ab) \rightarrow False \)
Proof Setup

Prove: The product of two odd numbers is odd.
\[ \forall a, b \in \mathbb{Z} \quad odd(a) \land odd(b) \rightarrow odd(ab) \]

What are the **premises** and **consequence** for a proof by contrapositive?
Proof Setup

Prove: The product of two odd numbers is odd.
\( \forall a, b \in \mathbb{Z} \ odd(a) \land odd(b) \rightarrow odd(ab) \)

What are the premises and consequence for a proof by contrapositive?
Premises: \( \forall a, b \in \mathbb{Z} \neg odd(ab) \)
Consequence: \( \neg (odd(a) \land odd(b)) \)
\( \forall a, b \in \mathbb{Z} \neg odd(ab) \rightarrow \neg (odd(a) \land odd(b)) \)
Proof Setup

Prove: The product of two odd numbers is odd.
\[\forall a, b \in \mathbb{Z} \, odd(a) \land odd(b) \rightarrow odd(ab)\]
What are the *premises* and *consequence* for a direct proof?
Proof Setup

Prove: The product of two odd numbers is odd.
\( \forall a, b \in \mathbb{Z} \) \( odd(a) \land odd(b) \rightarrow odd(ab) \)

What are the premises and consequence for a direct proof?
Premises: \( \forall a, b \in \mathbb{Z} \) \( odd(a) \land odd(b) \)
Consequence: \( odd(ab) \)
Finishing a Proof

Prove: The product of two odd numbers is odd.
\[ \forall a, b \in \mathbb{Z} \text{ odd}(a) \land \text{odd}(b) \rightarrow \text{odd}(ab) \]
Regardless of the type of proof used, what is the conclusion of the proof?
Prove: The product of two odd numbers is odd.
\[ \forall a, b \in \mathbb{Z} \text{ } odd(a) \land odd(b) \rightarrow odd(ab) \]
Regardless of the type of proof used, what is the conclusion of the proof?
... some valid argument ...
:\[ \forall a, b \in \mathbb{Z} \text{ } odd(a) \land odd(b) \rightarrow odd(ab) \]
Direct Proof Template

\[ P_1 \land P_2 \land P_3 \land \ldots \land P_k \rightarrow C_1 \land C_2 \land \ldots \land C_n \]

Given: \( P_1 \land P_2 \land P_3 \land \ldots \land P_k \)
Show that: \( C_1 \land C_2 \land \ldots \land C_n \) follows

\[ \vdash P_1 \land P_2 \land P_3 \land \ldots \land P_k \rightarrow C_1 \land C_2 \land \ldots \land C_n \]