Formal Methods and Specification (SS 2021)
Lecture 2: Proofs

Stefan Ratschan

Katedra číslicového návrhu
Fakulta informačních technologií
České vysoké učení technické v Praze

Evropský sociální fond Praha & EU: Investujeme do vaší budoucnosti

Checking Correctness of Programs

Example: A friend writes a program for you

Specification:

- Input: $x \in \mathbb{Z}$
- Output: $\hat{x} \in \mathbb{Z}$, $\hat{x} < x$, …

Program:

```
if $f(x) \geq 0$ then                    // we do not know how $f$ behaves
    return $x - f(x) - 1$
else
    return $x + f(x) - 1$
```

Questions: Is it correct?

For input -3, yes! 8? -2? … testing

Alternatively: evidence in form of argument

Problems: Which arguments allowed? programming language specific

Reduction to Logic

Specification:

- Input: $x \in \mathbb{Z}$
- Output: $\hat{x} \in \mathbb{Z}$, $\hat{x} < x$, ...

Program:

```
if $f(x) \geq 0$ then
    return $x - f(x) - 1$
else
    return $x + f(x) - 1$
```

Program is correct iff *verification condition*

$$\forall x \in \mathbb{Z}\,. \quad \begin{array}{l} f(x) \geq 0 \Rightarrow x - f(x) - 1 < x \wedge \\ \neg f(x) \geq 0 \Rightarrow x + f(x) - 1 < x \end{array}$$

holds (independent of f, using properties of $\mathbb{Z}$).

Similar problem: $\mathbb{Z}$ is an infinite set

How to convince somebody with absolute certainty?

Proofs

Proof: Absolutely certain evidence that a formula holds, that everybody can check always and everywhere.

Proofs that are written formally,
can even be checked for correctness by a computer
(viz. proof-carrying code)

“formula ϕ holds”: ϕ is a logical consequence of Φ ($\Phi \models \phi$)
where Φ are the things we know.

Usually we will not state Φ explicitely, and write $\models \phi$.

How to Verify Validity

One can prove $A \Leftrightarrow B$ by
proving that A is equivalent to B based on on equivalence rules
(see MI-TES, Section 1.5 in "Formal Modeling and Automatic Analysis of Complex Systems")

But unfortunately, this is not enough (the method is not complete).

Today: a complete proof method:
There is a proof for every formula that holds.

Example

You will find the animated version of the example in the video.
In written form, you can find it on the next slide.

Example

Example: Prove

$$[p \Rightarrow q] \Rightarrow \big[[p \wedge r] \Rightarrow [q \wedge r] \big]$$

We assume $p \Rightarrow q$ and prove $[p \wedge r] \Rightarrow [q \wedge r]$. For proving $[p \wedge r] \Rightarrow [q \wedge r]$ we assume $p \wedge r$ and prove $q \wedge r$. For proving $q \wedge r$ we prove both q and r:

- Proof of q: From the assumption $p \wedge r$ we we conclude both p and r. From the assumptions p and $p \Rightarrow q$ follows q, which finishes this part of the proof.
- Proof of r: We already know that from the assumption $p \wedge r$ follows r, which finishes also this part of the proof.

Proof Method

For proving something, we keep a list of things that we already know, and

- add known things ("to assume, to conclude"), and
- simplify the thing to prove, until
  what we want to prove is known.

As usual we assume an infinite set of predicate and function symbols

We handle types intuitively.

Proof Rules—Propositional Logic without Negation

A, B meta-variables, i.e., variables that represent arbitrary formulas

The rules refer to the outer-most symbol of a formula
(i.e., the root of its syntactical tree).

How to work on things that we have to prove?

$A \wedge B$: Separately prove A and B

$A \vee B$: Assume $\neg A$ and prove B (or vice versa).

$A \Rightarrow B$: Assume A and prove B.

How to generate new knowledge?

$A \wedge B$: Conclude both A and B

$A \vee B$: Do a case distinction: first write "Case A :", assume A and finish the proof. Then write "Case B :", assume B, and finish the proof.

$A \Rightarrow B$: If we also know A then we conclude B.

Proof by Contradiction

Example:

$$[p \wedge \neg p] \Rightarrow q.$$

Holds, due to left-hand side $p \wedge \neg p$

To prove the formule, we assume $p \wedge \neg p$ and prove q. From the assumption $p \wedge \neg p$ we know both p and $\neg p$, which is a ....

Contradiction: We know both a formula and its negation.

A contradiction finishes every proof (successfully!)

So: this proves what we originally wanted to prove!

Attention: The rules for
  proving conjunction and using disjunction in assumption
    start two separate proofs.

A contradiction only finishes the proof in which it occurs.

Negations: Example

You will find the animated version of the example in the video.
In written form, you can find it on the next slide.

Example

$$\big[\,[p \Rightarrow q] \wedge [p \Rightarrow \neg q]\,\big] \Rightarrow \neg p$$

We assume $[p \Rightarrow q] \wedge [p \Rightarrow \neg q]$ and prove $\neg p$. For proving $\neg p$ we assume p and try to find a contradiction.

From the assumption $[p \Rightarrow q] \wedge [p \Rightarrow \neg q]$ we know the assumptions $p \Rightarrow q$ and $p \Rightarrow \neg q$. From the assumptions p and $p \Rightarrow q$ follows q, and from the assumptions p and $p \Rightarrow \neg q$ follows $\neg q$. So we have both assumptions q and $\neg q$, which is a a contradiction. This finishes the proof.

Proof Rules—Propositional Case

How to work on things that we have to prove?

$A \wedge B$: Separately prove A and B

$A \vee B$: Assume $\neg A$ and prove B (or vice versa).

$A \Rightarrow B$: Assume A and prove B.

$\neg A$: Assume A, and try to find a contradiction

How to generate new knowledge?

$A \wedge B$: Conclude both A and B

$A \vee B$: Do a case distinction: first write "Case A :", assume A and finish the proof. Then write "Case B :", assume B, and finish the proof.

$A \Rightarrow B$: If we also know A then we conclude B.

Reminder

For us, the scope of quantifiers is as far to the right as possible!

So

$$\exists x \,.\, P(x) \wedge Q(x)$$

means

$$\exists x \,.\, [P(x) \wedge Q(x)],$$

and not

$$[\exists x \,.\, P(x)] \wedge Q(x).$$

Universal Quantifiers: Example

Assumptions:

> Assumptions:
>
> $f(a) \geq 0$
>
> To prove:
>
> $a - f(a) - 1 < a$

> Assumptions:
>
> $\neg f(a) \geq 0$
>
> To prove:
>
> $a + f(a) - 1 < a$

To prove:

$$\forall x \in \mathbb{Z}\,.\quad \begin{array}{l} f(x) \geq 0 \Rightarrow x - f(x) - 1 < x \land \\ \neg f(x) \geq 0 \Rightarrow x + f(x) - 1 < x \end{array}$$

$$\begin{array}{l} f(a) \geq 0 \Rightarrow a - f(a) - 1 < a \land \\ \neg f(a) \geq 0 \Rightarrow a + f(a) - 1 < a \end{array} ,$$

where a is new.

Universal Quantifiers: Example

$$\forall x \in \mathbb{Z}\,.\quad \begin{array}{l} f(x) \geq 0 \Rightarrow x - f(x) - 1 < x \wedge \\ \neg f(x) \geq 0 \Rightarrow x + f(x) - 1 < x \end{array}$$

We want to prove the formula for an arbitrary integer, that is, an integer, about which we do not know anything. So we introduce a new constant a, and prove

$$\begin{array}{l} f(a) \geq 0 \Rightarrow a - f(a) - 1 < a \wedge \\ \neg f(a) \geq 0 \Rightarrow a + f(a) - 1 < a \end{array}$$

To prove the conjunction we prove both $f(a) \geq 0 \Rightarrow a - f(a) - 1 < a$ and $\neg f(a) \geq 0 \Rightarrow a + f(a) - 1 < a$. To prove $f(a) \geq 0 \Rightarrow a - f(a) - 1 < a$ we assume $f(a) \geq 0$ and prove $a - f(a) - 1 < a$ which clearly holds under this assumption $\neg f(a) \geq 0 \Rightarrow a + f(a) - 1 < a$ is similar.

Existential Quantifiers: Example

$$\exists x \in \mathbb{N} \,.\, x \geq 4 \land 2 \nmid x$$

For proving that something exists that fulfills a certain property, we just have to find one object that fulfills this property.

For example, here: 7

Substitute, the result is $7 \geq 4 \land 2 \nmid 7$

Clearly both $7 \geq 4$ and $2 \nmid 7$.

Proof Rules Including Quantifiers 1

How to work on things that we have to prove?

- $\exists x \,.\, A$: Choose (by intuition, creativity, or any other special connection with god) a term t, and prove $A[x \leftarrow t]$
- $\forall x \,.\, A$: Choose a new constant, e.g., a, write/say "let a be arbitrary but fixed" and prove $A[x \leftarrow a]$, instead
- $A \wedge B$: Separately prove A and B
- $A \vee B$: Assume $\neg A$ and prove B (or vice versa).
- $A \Rightarrow B$: Assume A and prove B.
- $\neg A$: Assume A, and try to find a contradiction

Remember the definition of the notion "term".

Especially: Every constant is a term
(as usual, we assume that there are infinitely many constants).

Proof Rules Including Quantifiers 2

How to generate new knowledge?

$\exists x \,.\, A$: Choose a new constant, e.g., a, write/say "let a be such that $A[x \leftarrow a]$", and add $A[x \leftarrow a]$ to our knowledge base

$\forall x \,.\, A$: Choose (by intuition, creativity, or any other special connection with god) a term t and conclude $A[x \leftarrow t]$

$A \wedge B$: Conclude both A and B

$A \vee B$: Do a case distinction: first write "Case A :", assume A and finish the proof. Then write "Case B :", assume B, and finish the proof.

$A \Rightarrow B$: If we also know A then we conclude B.

Example

You will find the animated version of the example in the video.
In written form, you can find it on the next slide.

Example

$$\big[\,[\forall x\,.\,P(x) \Rightarrow Q(x)] \wedge [\exists x\,.\,P(f(x))]\,\big] \Rightarrow [\exists x\,.\,Q(x)]$$

(scope of quantifiers as far as possible!)

We assume $[\forall x\,.\,P(x) \Rightarrow Q(x)] \wedge [\exists x\,.\,P(f(x))]$, that is, we assume both $\forall x\,.\,P(x) \Rightarrow Q(x)$ and $\exists x\,.\,P(f(x))$. We want to prove $\exists x\,.\,Q(x)$.

Due to the assumption $\exists x\,.\,P(f(x))$ we can choose a new constant a such that $P(f(a))$. Due to the assumption $\forall x\,.\,P(x) \Rightarrow Q(x)$ we can conclude $P(f(a)) \Rightarrow Q(f(a))$. For proving $\exists x\,.\,Q(x)$ we choose for x the term $f(a)$, and now it suffices to prove $Q(f(a))$, which follows from the assumptions $P(f(a))$ and $P(f(a)) \Rightarrow Q(f(a))$. This finishes the proof.

Proof Rules for Equalities

For every term t we can assume $t = t$.

If we know $t_1 = t_2$,
then we can always replace t_1 by t_2 and vice versa.

Example:
If we know $a = b$ and $P(a)$,
then we can add the assumption $P(b)$.

Here, the replacement must
not change bound variables or introduce new bound variables:

Example: If we know both $\exists x \,.\, P(x, y)$ and $y = f(x)$, then
we are not allowed to replace y by $f(x)$ in $\exists x \,.\, P(x, y)$
since the result $\exists x \,.\, P(x, f(x))$ would have a new bound variable.

Proof Rules for Equivalences

It is always allowed to replace equivalences

Strictly necessary is only the equivalence between A and $\neg\neg A$
all other equivalences can be derived using our method
(ignoring the Boolean constants $\bot$, $\top$).

Especially: When proving A, we can

1. replace it by $\neg\neg A$,
2. apply the rule for proving negations,
3. and add $\neg A$ as additional knowledge.

Substitution

Attention: It is forbidden to use terms
that result in new bound variables!

Example: If we want to prove

$$\exists x \forall y \; . \; p(x, z)$$

we are not allowed to choose $f(y)$ for the variable x, since
$[\forall y \; . \; p(x, y)][x \leftarrow f(y)]$ is $\forall y \; . \; p(f(y), z)$,
where y is suddenly bound by a quantifier .

Lemmas: Example:

You will find the animated version of the example in the video.
In written form, you can find it on the next slide.

Lemmas: Example:

$$\Big[p \wedge \big[[p \vee q] \Rightarrow r\big]\Big] \Rightarrow r$$

We assume p, $[p \vee q] \Rightarrow r$ and try to prove r.

Now it would be useful to know $p \vee q$,
which would be easy to prove from p.

This is possible, but needs a separate proof (lemma).

Proof of the lemma $p \vee q$ from our current knowledge: For proving $p \vee q$ we assume $\neg q$, and prove p. The formula p is already a known fact, so the proof of the lemma is finished.

Now we add the formula $p \vee q$ to our know facts. From the formula $[p \vee q] \Rightarrow r$ we know r which finishes the main proof.

Lemmas in General

We also have only one formula to prove,
but we may have several assumptions.

If we would like to prove some additional knowledge,
we can prove it in a separate proof (from the current knowledge)
we can add to our knowledge.

A lemma may recursively contain further lemmas etc

Usage of Lemmas: Typical Examples

If we know $A \Rightarrow B$, then
we can try to prove A using a lemma, and
then from this, because of $A \Rightarrow B$ we can conclude B.

$A \vee \neg A$ (case distinction) can be proved without any assumptions,
so we can add formulas of this form always.

If we know $\neg A$ (A can be a complicated formula),
we can try to prove A using a lemma,
which results in a contradiction, and hence in a successful proof.

Attention: A lemma is a separate proof!
Except for the formula that we prove in the lemma,
this proof may not influence the main proof in any way.

Example:

You will find the animated version of the example in the video.
In written form, you can find it on the next slide.

Example:

$$[\neg \forall x \, . \, P(f(g(x)))] \Rightarrow [\exists x \, . \, \neg P(x)]$$

We assume $\neg \forall x \, . \, P(f(g(x)))$ and prove $\exists x \, . \, \neg P(x)$. For proving an existential quantifier, we would need a term to substitute, but we do not know anything useful. So we add a double negation, resulting in $\neg\neg\exists x \, . \, \neg P(x)$, and apply the rule for proving negations which adds $\neg\exists x \, . \, \neg P(x)$ as additional knowledge.

Now we have two formulas with negations as knowledge. If we would know $\forall x \, . \, P(f(g(x)))$, we would arrive at a contradiction. Hence we prove this formula in a lemma.

Lemma: Proof of $\forall x \,.\, P(f(g(x)))$

In the lemma, we apply the proof rule for universal quantifiers, and prove $P(f(g(a)))$ for a new, arbitrary, but fixed constant a. Now we do not have any proof rule left to apply. So we again add a double negation, and then add $\neg P(f(g(a)))$ as additional knowledge.

At this point, we are still proving the lemma. We know $\neg\exists x \,.\, \neg P(x)$ and $\neg P(f(g(a)))$. The latter formula contains the term $f(g(a))$ that we may use to prove an existential quantifier. Hence, we prove $\exists x \,.\, \neg P(x)$ using a another lemma within the current lemma.

Example continued

The proof of this second lemma immediately succeeds by choosing $f(g(a))$ for x. Hence we can add $\exists x \,.\, \neg P(x)$ to the knowledge in the original lemma. This creates a contradiction which proves this original lemma. As a consequence, we can add $\forall x \,.\, P(f(g(x)))$ to the main proof. This again creates a contradiction which finishes the proof.

Unsuccessful Proofs . . .

What follows from this? nothing!

The formula either

- holds and we were not able to prove it, or it
- does not hold.

For showing that a formula does not hold we may

- find a counter-example, or
- even try to prove the negation of the formula.

Unsuccessful Proofs: Examples

$$p \vee [\neg p \wedge q]$$

Counter-example: $\{p \mapsto \bot, q \mapsto \bot\}$

$$\neg[p \vee [\neg p \wedge q]]$$

Counter-example: $\{p \mapsto \top, q \mapsto \bot\}$

$$p \wedge \neg p$$

Not only has a counter-example, but we can even prove negation.

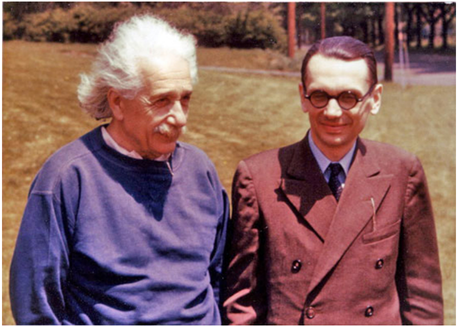
$$\forall x \, . \, P(x)$$

Counter-example:

over the integers, when interpreting $P(x)$ as "x is even",
the formula certainly does not hold.

The negation $\neg\forall x \, . \, P(x)$ also does not hold!

Completeness



Kurt Gödel, 1906 (Brno) — 1978 (Princeton): Ph.D. thesis, 33 pages:

For every formula ϕ s.t. $\models \phi$, there is proof.

Then: . . . in a different proof system [Gödel, 1929].

But it also holds for our system

(when including the equivalence between A and $\neg\neg A$)

Different Methods, Literature

Our method: Informal version of *natural deduction*

There are various variants

Formal rules (`deduction_rules.pdf`), graphical proof representation

Other descriptions of variants of natural deduction:

- Barwise and Etchemendy [2002] (long-winding, low bachelor level)
- Broda et al. [1994] (bachelor level)
- Gries [1981], Huth and Ryan [2004] (bachelor/master level)

Internet (attention: subtle differences)

Alternative Proof Systems

- Hilbert calculus
- Sequent calculus

Useful for studying the basics of mathematics, but not for everyday proving.

Further Lectures

- Data structures: sets, lists, arrays etc.
- Program correctness
- Program correctness
- Program correctness
- Program correctness
- ...

Quantifiers, Equality, Equivalence: Example

$$\forall x \in \mathbb{N} \,.\, x \text{ is divisible by } 2 \Rightarrow 6x \text{ is divisible by } 4$$

We want to prove the implication for an arbitrary natural number, that is, a natural number, about which we do not know anything. So we introduce a new constant a, and prove

$$a \text{ is divisible by } 2 \Rightarrow 6a \text{ is divisible by } 4,$$

that is, we assume that a is divisible by 2 and prove: $6a$ is divisible by 4.

The definition of divisibility is:
$\forall x, y \;.\; x \text{ is divisible by } y :\Leftrightarrow \exists k \in \mathbb{N} \,.\, yk = x$

Especially:

- a is divisible by 2 $:\Leftrightarrow \exists k \in \mathbb{N} \,.\, 2k = a$
- $6a$ is divisible by 4 $:\Leftrightarrow \exists k \in \mathbb{N} \,.\, 4k = 6a$

So we can replace the formulas in the proof by equivalent ones

Quantifiers, Equality, Equivalence: Example Continued

From the assumption

$$\exists k \in \mathbb{N} \, . \, 2k = a$$

we prove

$$\exists k \in \mathbb{N} \, . \, 4k = 6a.$$

We give a name to the symbol k in the assumptions, e.g., k', so we know

$$2k' = a.$$

We can write this equivalently as

$$12k' = 6a$$

$$4 \; 3 \; k' = 6a$$

For proving the existential quantifier we choose for k the term $3k'$, so it suffices to prove

$$4 \; 3 \; k' = 6a$$

which we already know. This finishes the proof.

Literature I

Jon Barwise and John Etchemendy. *Language, Proof and Logic*. Center for the Study of Language, 2002.

Krysia Broda, Hessam Khoshnevisan, and Susan Eisenbach. *Reasoned programming*. Prentice Hall, 1994. URL `http://www.doc.ic.ac.uk/pandora/firstyearbook.pdf`.

Kurt Gödel. *Über die Vollständigkeit des Logikkalküls*. PhD thesis, Universität Wien, 1929.

David Gries. *The science of programming*, volume 1981. Springer Heidelberg, 1981.

Michael Huth and Mark Ryan. *Logic in Computer Science*. Cambridge University Press, 2004.