Program Analysis
Lecture 1

Rayna Dimitrova

WS 2016/2017
Administrative

Lectures

- Slides/lecture notes will be posted on http://www.mpi-sws.org/~rayna/pa1617.html
- We will follow closely the WS 2015/2016 edition of the course (lecture notes in German)
- Written exam

Exercises

- Time and place of tutorial to be determined
- Exercise sheet will be posted after each lecture on http://www.mpi-sws.org/~rayna/pa1617.html
- Solutions are due at the beginning of the next lecture
- You need 60% of the total number of points on the exercise sheets during the semester to qualify for the exam
Program analysis

Software
- has bugs
- is often too slow

Applications of program analysis
- software verification
- compiler optimization

Static program analysis
establish properties of a program without executing it

Theorem (Rice)
All non-trivial semantic properties of programs are undecidable.

⇒ develop algorithms that give conservative answers
A simple program

x and y are integer variables

```plaintext
read(x);

if (x < 0) {
    y := 0;
    while x < 0 do {
        x++;
        y++;
    }
}
else {
    y := x;
}

print(y);
```
A simple sign lattice

\[
\begin{align*}
\emptyset & \quad \rightarrow (n,?) \quad \rightarrow (?,n) \quad \rightarrow (?,nn) \quad \rightarrow (nn,?) \\
(n,?) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \quad \rightarrow (nn,n) \\
(n,nn) & \quad \rightarrow (n,n) \quad \rightarrow (nn,n) \quad \rightarrow (nn,nn) \\
(n,n) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \\
(n,?) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \\
(?,n) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \\
(?,nn) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \\
(?,?) & \quad \rightarrow (n,nn) \quad \rightarrow (n,n) \\
\end{align*}
\]

- $n$: negative value, $nn$: non-negative value; $?$: any value in $\mathbb{Z}$
- $(n,nn)$ represents the set $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x < 0, y \geq 0\}$
- An arrow $a \rightarrow b$ denotes the fact that the set represented by $a$ is a subset of the set represented by $b$
- **Note:** we have omitted arrows such as
  - $(n,nn) \rightarrow (n,nn)$ (self-loop),
  - $(n,nn) \rightarrow (?,?)$, induced by the arrows $(n,nn) \rightarrow (n,?)$ and $(n,?) \rightarrow (?)$
Total orders

\((\mathbb{N}, \leq)\) is a **total order**: it satisfies the following conditions

**reflexivity**: \(a \leq a\) for all \(a \in \mathbb{N}\)

**antisymmetry**: \(a \leq b\) and \(b \leq a\) implies \(a = b\)

**transitivity**: \(a \leq b\) and \(b \leq c\) implies \(b \leq c\)

**comparability**: For any \(a, b \in \mathbb{N}\), either \(a \leq b\) or \(b \leq a\)

What about \((\mathcal{P}(\{1, 2, 3\}), \subseteq)\)?
(\(\mathcal{P}(\{1, 2, 3\})\) is the set of all subsets of \(\{1, 2, 3\}\))
Total orders

$(\mathbb{N}, \leq)$ is a **total order**: it satisfies the following conditions

- **reflexivity**: $a \leq a$ for all $a \in \mathbb{N}$
- **antisymmetry**: $a \leq b$ and $b \leq a$ implies $a = b$
- **transitivity**: $a \leq b$ and $b \leq c$ implies $b \leq c$
- **comparability**: For any $a, b \in \mathbb{N}$, either $a \leq b$ or $b \leq a$

What about $(\mathcal{P}([1, 2, 3]), \subseteq)$?
(where $\mathcal{P}([1, 2, 3])$ is the set of all subsets of $\{1, 2, 3\}$)

$\{1, 2\} \not\subseteq \{1, 3\}$ and $\{1, 3\} \not\subseteq \{1, 2\}$

$\{1, 2\}$ and $\{1, 3\}$ are **incomparable**
A **partial order** \((D, \leq)\) consists of a set \(D \neq \emptyset\) and a relation \(\leq \subseteq D \times D\) which has the following properties

**reflexivity:** \(a \leq a\) for all \(a \in \mathbb{N}\)

**antisymmetry:** \(a \leq b\) and \(b \leq a\) implies \(a = b\)

**transitivity:** \(a \leq b\) and \(b \leq c\) implies \(b \leq c\)

\((\mathcal{P}(\{1, 2, 3\}), \subseteq)\) is a **partial order**

**partial order + comparability = total order**
A Hasse diagram for \((\mathcal{P}({1, 2, 3}), \subseteq)\)

- leave out reflexivity self-loops
- leave out edges induced by transitivity
Least and greatest elements of a set

Let \((D, \leq)\) be a partial order and \(X \subseteq D\).

\(a \in X\) is a \textbf{minimal} element of \(X\)
if there does not exist \(x \in X\) such that \(x \leq a\) and \(x \neq a\).

\(l \in X\) is the \textbf{least} element of \(X\)
if for all \(x \in X\) it holds that \(l \leq x\).
Least and greatest elements of a set

Let \((D, \leq)\) be a partial order and \(X \subseteq D\).

\(a \in X\) is a **minimal** element of \(X\)
if there does not exist \(x \in X\) such that \(x \leq a\) and \(x \neq a\).

\(l \in X\) is the **least** element of \(X\)
if for all \(x \in X\) it holds that \(l \leq x\).

**Example**
Consider \((\mathcal{P}(\{1, 2, 3\}), \subseteq)\).
The set \(\{\{1, 2\}, \{2, 3\}\}\) has two minimal elements.
The set \(\{\{1, 2\}, \{2, 3\}\}\) does not have a least element.

**Example**
Consider \((\mathbb{Z} \cup \{\#\}, \leq)\) where \(\leq\) is the less-than-or-equal relation on \(\mathbb{Z}\), and \(\#\) is incomparable with each of the elements of \(\mathbb{Z}\). The set \(\mathbb{Z} \cup \{\#\}\) has exactly one minimal element, \(\#\), and no least element.
Least and greatest elements of a set

Let \((D, \leq)\) be a partial order and \(X \subseteq D\).

\(a \in X\) is a **minimal** element of \(X\)
if there does not exist \(x \in X\) such that \(x \leq a\) and \(x \neq a\).

\(l \in X\) is the **least** element of \(X\)
if for all \(x \in X\) it holds that \(l \leq x\).

\(b \in X\) is a **maximal** element of \(X\)
if there does not exist \(x \in X\) such that \(b \leq x\) and \(x \neq b\).

\(g \in X\) is the **greatest** element of \(X\)
if for all \(x \in X\) it holds that \(x \leq g\).
Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)
Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)

\(u \in D\) is called an **upper bound** for \(X\) if \(x \leq u\) for all \(x \in X\)
Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)

\(u \in D\) is called an **upper bound** for \(X\) if \(x \leq u\) for all \(x \in X\)

\(u \in D\) is called a **least upper bound** for \(X\) (also **join** of \(X\)) if

- \(u\) is an upper bound for \(X\)
- \(u \leq u'\) for all upper bounds \(u'\) for \(X\)
Let \((D, \leq)\) be a partial order and let \(X \subseteq D\).

\(u \in D\) is called an **upper bound** for \(X\) if \(x \leq u\) for all \(x \in X\).

\(u \in D\) is called a **least upper bound** for \(X\) (also **join** of \(X\)) if

- \(u\) is an upper bound for \(X\)
- \(u \leq u'\) for all upper bounds \(u'\) for \(X\)

By definition, if it exists, the least upper bound of \(X\) is unique.

The least upper bound of \(X\) is denoted by \(\sqcup X\).

Instead of \(\sqcup \{a, b\}\) we write \(a \sqcup b\).
Meet

Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)
Meet

Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)

\(l \in D\) is called a **lower bound** for \(X\) if \(l \leq x\) for all \(x \in X\)
Meet

Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)

\(l \in D\) is called a **lower bound** for \(X\) if \(l \leq x\) for all \(x \in X\)

\(l \in D\) is called a **greatest lower bound** for \(X\) (also **meet** of \(X\)) if

- \(l\) is a lower bound for \(X\)
- \(l' \leq l\) for all lower bounds \(l'\) for \(X\)
Meet

Let \((D, \leq)\) be a partial order and let \(X \subseteq D\)

\(l \in D\) is called a **lower bound** for \(X\) if \(l \leq x\) for all \(x \in X\)

\(l \in D\) is called a **greatest lower bound** for \(X\) (also **meet** of \(X\)) if

- \(l\) is a lower bound for \(X\)
- \(l' \leq l\) for all lower bounds \(l'\) for \(X\)

By definition, if it exists, the greatest lower bound of \(X\) is unique.

The greatest lower bound of \(X\) is denoted by \(\bigcap X\).

Instead of \(\bigcap\{a, b\}\) we write \(a \cap b\).
Lattices

A lattice is a partial order \((D, \leq)\) in which for every pair \(a, b \in D\) there exist least upper bound \(a \sqcup b\) and greatest lower bound \(a \sqcap b\).

A lattice is called **complete** if for every subset \(X \subseteq D\) there exist the least upper bound \(\bigcup X\) and the greatest lower bound \(\bigcap X\).
Lattices

A lattice is a partial order \((D, \leq)\) in which for every pair \(a, b \in D\) there exist least upper bound \(a \sqcup b\) and greatest lower bound \(a \sqcap b\).

A lattice is called complete if for every subset \(X \subseteq D\) there exist the least upper bound \(\bigcup X\) and the greatest lower bound \(\bigcap X\).

Examples

\[ \begin{array}{c}
x \\
x_1 & \xrightarrow{\quad} & x_2 \\
x \\
\end{array} \]

not a lattice: \(\{x_1, x_2\}\) does not have a lower bound

\[ \begin{array}{c}
a_6 \\
a_4 & \xrightarrow{\quad} & a_5 \\
a_2 & \xrightarrow{\quad} & a_3 \\
a_1 \\
\end{array} \]

not a lattice: \(\{a_2, a_3\}\) has upper bounds \(a_4, a_5, a_6\) but no least upper bound \((a_4, a_5\) not comparable)
Lattices

A **lattice** is a partial order \((D, \leq)\) in which for every pair \(a, b \in D\) there exist least upper bound \(a \sqcup b\) and greatest lower bound \(a \sqcap b\).

A lattice is called **complete** if for every subset \(X \subseteq D\) there exist the least upper bound \(\bigvee X\) and the greatest lower bound \(\bigwedge X\).

**Example**

\((\mathbb{N}, \leq)\) is a lattice but not a complete lattice:

- \(a \sqcup b = \max (a, b), a \sqcap b = \min (a, b)\)
- the set \(\mathbb{N}\) does not have an upper bound
Lattices

A lattice is a partial order \((D, \leq)\) in which for every pair \(a, b \in D\) there exist least upper bound \(a \sqcup b\) and greatest lower bound \(a \sqcap b\).

A lattice is called **complete** if for every subset \(X \subseteq D\) there exist the least upper bound \(\bigcup X\) and the greatest lower bound \(\bigcap X\).

**Lemma**

Every complete lattice \((D, \leq)\) has a unique least element (bottom)

\[ \bot := \bigcup \emptyset = \bigcap D, \]

Every complete lattice \((D, \leq)\) has a unique greatest element (top)

\[ \top := \bigcap \emptyset = \bigcup D \]

Every lattice \((D, \leq)\) where \(D\) is finite is complete.
Fixpoints

Let \((D, \leq)\) be a partial order and let \(f : D \to D\) be a function.

A **fixpoint** of \(f\) is an element \(x \in D\) such that \(f(x) = x\).
Fixpoints

Let \((D, \leq)\) be a partial order and let \(f : D \rightarrow D\) be a function.

A **fixpoint** of \(f\) is an element \(x \in D\) such that \(f(x) = x\).

A function \(f : D \rightarrow D\) is called **monotonic** if

\[ a \leq b \text{ implies } f(a) \leq f(b). \]
Fixpoints

Let \((D, \leq)\) be a partial order and let \(f : D \to D\) be a function.

A fixpoint of \(f\) is an element \(x \in D\) such that \(f(x) = x\).

Theorem (Knaster, Tarski’55)

Let \((D, \leq)\) be a complete lattice and let \(f : D \to D\) a monotonic function. Then,

1. there exists a (unique) least fixpoint of \(f\) given by
   \[
   \text{lfp}(f) := \bigcap \{x \in D \mid f(x) \leq x\}
   \]
2. there exists a (unique) greatest fixpoint of \(f\) given by
   \[
   \text{gfp}(f) := \bigcup \{x \in D \mid x \leq f(x)\}
   \]
Proof

Let \((D, \leq)\) be a complete lattice and let \(f : D \rightarrow D\) be monotonic. We show that \(l := \text{lfp}(f)\) is the least fixpoint of \(f\), meaning that \(l\) is a fixpoint of \(f\), and for every fixpoint \(d\) of \(f\), we have that \(l \leq d\).

We show that \(f(l) \leq l\) for \(l = \bigcap D', D' = \{x \in D \mid f(x) \leq x\}\).

Since \(l\) is the greatest lower bound of \(D'\), if we show that \(f(l)\) is a lower bound of \(D'\), then we have \(f(l) \leq l\).

\[
\begin{align*}
l &\leq x \text{ for all } x \in D' \text{(} l \text{ is a lower bound for } D') \\
f(l) &\leq f(x) \text{ for all } x \in D' \text{(} f \text{ is monotonic)} \\
f(l) &\leq x \text{ for all } x \in D' \text{(definition of } D'\text{, transitivity)}
\end{align*}
\]

Thus, \(f(l)\) is a lower bound of \(D'\). So, we have \(f(l) \leq \bigcap D' = l\).
Proof continued

- We show that \( l \leq f(l) \) for \( l = \bigcap D' \), \( D' = \{ x \in D \mid f(x) \leq x \} \).
  If we show \( f(l) \in D' \), then \( l \leq f(l) \), because \( l \) is a lower bound for \( D' \).
  Above we showed that \( f(l) \leq l \).
  By monotonicity of \( f \), \( f(f(l)) \leq f(l) \).
  By definition of \( D' \), \( f(l) \in D' \). Thus, \( l \leq f(l) \).

By antisymmetry, from \( f(l) \leq l \) and \( l \leq f(l) \) we get \( f(l) = l \).

Now, suppose that \( d \in D \) is such that \( f(d) = d \). We show that \( l \leq d \).
By the choice of \( d \) and reflexivity, we have \( f(d) \leq d \). Hence, \( d \in D' \).
Then, \( l \leq d \), because \( l \) is a lower bound for \( D' \).

From this we conclude that \( l \) is the least fixpoint of \( f \).

The proof for \( \text{gfp}(f) \) is analogous.
Chains

Let \((D, \leq)\) be a partial order.

- A **chain** in \(D\) is a totally ordered non-empty subset \(C \subseteq D\).
  (For any \(a, b \in C\), either \(a \leq b\) or \(b \leq a\).)

- A sequence \((c_i)_{i \in \mathbb{N}}\) is called
  - **ascending chain** if \(c_i \leq c_{i+1}\) for all \(i \in \mathbb{N}\).
  - **descending chain** if \(c_{i+1} \leq c_i\) for all \(i \in \mathbb{N}\).

- A partial order \((D, \leq)\) has
  - **finite height** if every chain \(C\) in \(D\) is finite.
  - **bounded height** if there exists \(h \in \mathbb{N}\) such that every chain \(C\) in \(D\) has at most \(h\) elements.
⊔-continuous and ⊓-continuous functions

Let \((D, \leq)\) be a complete lattice and let \(f : D \to D\) be a function.

\(f\) is called \(\sqcup\)-continuous if for every chain \(C\) in \(D\),

\[
f(\bigsqcup C) = \bigsqcup \{f(c) \mid c \in C\}.
\]

\(f\) is called \(\sqcap\)-continuous if for every chain \(C\) in \(D\),

\[
f(\bigcap C) = \bigcap \{f(c) \mid c \in C\}.
\]
Ascending and descending chain conditions

A partial order \((D, \leq)\)

- satisfies the **ascending chain condition (ACC)** if
  for every ascending chain \(c_0 \leq c_1 \leq \ldots\)
  there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).

- satisfies the **descending chain condition (DCC)** if
  for every descending chain \(c_0 \geq c_1 \geq \ldots\)
  there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).
Ascending and descending chain conditions

A partial order \((D, \leq)\)

- satisfies the **ascending chain condition (ACC)** if for every ascending chain \(c_0 \leq c_1 \leq \ldots\) there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).

- satisfies the **descending chain condition (DCC)** if for every descending chain \(c_0 \geq c_1 \geq \ldots\) there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).

**Example**

\((\mathbb{N}, \leq)\) is a totally ordered set that satisfies the (DCC) condition. Such totally ordered sets are called **well-ordered**.
Ascending and descending chain conditions

A partial order \((D, \leq)\)

- satisfies the **ascending chain condition (ACC)** if for every ascending chain \(c_0 \leq c_1 \leq \ldots\) there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).

- satisfies the **descending chain condition (DCC)** if for every descending chain \(c_0 \geq c_1 \geq \ldots\) there exists \(n \in \mathbb{N}\) such that for all \(i \geq n\) we have \(c_i = c_n\).

**Theorem**

Let \((D, \leq)\) be a **complete lattice** and let \(f : D \to D\) be a **monotonic function**. Then

1. if \((D, \leq)\) satisfies (ACC), then \(f\) is \(\sqcup\)-continuous.
2. if \((D, \leq)\) satisfies (DCC), then \(f\) is \(\sqcap\)-continuous.
Proof

Let \((D, \leq)\) be a complete lattice satisfying (ACC) and \(f : D \to D\) be monotonic. We show that \(f\) is \(\sqcup\)-continuous. Let \(C \subseteq D\) be a chain.

- We show that \(f(\bigsqcup C) \leq \bigsqcup \{f(c) \mid c \in C\}\).

Since \(\bigsqcup \{f(c) \mid c \in C\}\) is an upper bound for \(\{f(c) \mid c \in C\}\) it suffices to show that \(f(\bigsqcup C) \in \{f(c) \mid c \in C\}\). We show \(\bigsqcup C \in C\).

First, we show that there exists \(\hat{c} \in C\) such that \(c \leq \hat{c}\) for all \(c \in C\).

Assume this is not true. Then, for every \(d \in C\) there exists \(c \in C\) such that \(d < c\) (\(d \leq c\) and \(d \neq c\)), or \(c\) and \(d\) are incomparable. Since \(C\) is a chain, \(c\) and \(d\) cannot be incomparable. Thus, we can construct a sequence \(c_0 < c_1 < \ldots\), which contradicts (ACC).

\[\bigsqcup C\] is an upper bound for \(C\) \(\implies\) \(\hat{c} \leq \bigsqcup C\) (since \(\hat{c} \in C\))
\(\hat{c}\) is an upper bound for \(C\) \(\implies\) \(\bigsqcup C \leq \hat{c}\)

By antisymmetry we get \(\hat{c} = \bigsqcup C\), and thus, \(\bigsqcup C \in C\).
Proof continued

We show that \( \bigcup \{ f(c) \mid c \in C \} \leq f(\bigcup C) \).

Since \( \bigcup \{ f(c) \mid c \in C \} \) is the least upper bound for \( \{ f(c) \mid c \in C \} \) it suffices to show that \( f(\bigcup C) \) is an upper bound for \( \{ f(c) \mid c \in C \} \).

\[
c \leq \bigcup C \quad \text{for all } c \in C \quad (\bigcup C \text{ is an upper bound for } C)
f(c) \leq f(\bigcup C) \quad \text{for all } c \in C \quad (f \text{ is monotonic})
\]

Thus, \( f(\bigcup C) \) is an upper bound for \( \{ f(c) \mid c \in C \} \), which concludes the proof.

From \( f(\bigcup C) \leq \bigcup \{ f(c) \mid c \in C \} \) and \( \bigcup \{ f(c) \mid c \in C \} \leq f(\bigcup C) \) by antisymmetry we conclude that \( f(\bigcup C) = \bigcup \{ f(c) \mid c \in C \} \).