Static Analysis and Verification

SAV 2023/2024

Tomáš Vojnar

vojnar@fit.vutbr.cz

Brno University of Technology
Faculty of Information Technology
Božetěchova 2, 612 66 Brno

Lattices and Fixpoints
A Brief Introduction

Partial Orders

- A tuple $(A, \leq_A)$ is a poset (partially-ordered set) iff A is a set and $\leq_A \subseteq A \times A$ is a partial order (i.e., a reflexive, transitive, and antisymmetric binary relation) on A.

- An example: Given a set S, $(2^S, \subseteq)$ is a poset.

Partial Orders

- A tuple $(A, \leq_A)$ is a poset (partially-ordered set) iff A is a set and $\leq_A \subseteq A \times A$ is a partial order (i.e., a reflexive, transitive, and antisymmetric binary relation) on A.

- An example: Given a set S, $(2^S, \subseteq)$ is a poset.

- Given a poset $(A, \leq_A)$ and a set $B \subseteq A$,
  - an element $a \in A$ is the greatest lower bound of B (glb/infimum/meet of B, $\sqcap B$) iff
    1. $\forall b \in B.\ a \leq_A b$ ("lower bound") and
    2. $\forall a' \in A.\ (\forall b \in B.\ a' \leq_A b) \implies a' \leq_A a$ ("greatest"),

Partial Orders

❖ A tuple $(A, \leq_A)$ is a poset (partially-ordered set) iff A is a set and $\leq_A \subseteq A \times A$ is a partial order (i.e., a reflexive, transitive, and antisymmetric binary relation) on A.

❖ An example: Given a set S, $(2^S, \subseteq)$ is a poset.

❖ Given a poset $(A, \leq_A)$ and a set $B \subseteq A$,

- an element $a \in A$ is the greatest lower bound of B (glb/infimum/meet of B, $\sqcap B$) iff
  1. $\forall b \in B.\ a \leq_A b$ ("lower bound") and
  2. $\forall a' \in A.\ (\forall b \in B.\ a' \leq_A b) \implies a' \leq_A a$ ("greatest"),
- an element $a \in A$ is the least upper bound of B (lub/supremum/join of B, $\sqcup B$) iff
  1. $\forall b \in B.\ b \leq_A a$ ("upper bound") and
  2. $\forall a' \in A.\ (\forall b \in B.\ b \leq_A a') \implies a \leq_A a'$ ("least"),

Partial Orders

- A tuple $(A, \leq_A)$ is a poset (partially-ordered set) iff A is a set and $\leq_A \subseteq A \times A$ is a partial order (i.e., a reflexive, transitive, and antisymmetric binary relation) on A.

- An example: Given a set S, $(2^S, \subseteq)$ is a poset.

- Given a poset $(A, \leq_A)$ and a set $B \subseteq A$,
  - an element $a \in A$ is the greatest lower bound of B (glb/infimum/meet of B, $\sqcap B$) iff
    1. $\forall b \in B.\ a \leq_A b$ ("lower bound") and
    2. $\forall a' \in A.\ (\forall b \in B.\ a' \leq_A b) \Longrightarrow a' \leq_A a$ ("greatest"),
  - an element $a \in A$ is the least upper bound of B (lub/supremum/join of B, $\sqcup B$) iff
    1. $\forall b \in B.\ b \leq_A a$ ("upper bound") and
    2. $\forall a' \in A.\ (\forall b \in B.\ b \leq_A a') \Longrightarrow a \leq_A a'$ ("least"),

- An example: For $(2^{\{a,b,c\}}, \subseteq)$, $\sqcup\{\emptyset, \{a\}, \{b\}\} = \{a, b\}$, and $\{a\} \sqcap \{b, c\} = \emptyset$.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.
  - $\bot_A = \sqcap A$ and $\top_A = \sqcup A$ are the least and greatest elements of a complete lattice, respectively.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.
  - $\bot_A = \sqcap A$ and $\top_A = \sqcup A$ are the least and greatest elements of a complete lattice, respectively.

- Examples:
  - $(2^{\{a,b,c\}}, \subseteq)$ is a complete lattice, $\sqcap$ corresponds to $\cap$, $\sqcup$ to $\cup$, $\bot$ to $\emptyset$, and $\top$ to $\{a, b, c\}$.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.
  - $\bot_A = \sqcap A$ and $\top_A = \sqcup A$ are the least and greatest elements of a complete lattice, respectively.

- Examples:
  - $(2^{\{a,b,c\}}, \subseteq)$ is a complete lattice, $\sqcap$ corresponds to $\cap$, $\sqcup$ to $\cup$, $\bot$ to $\emptyset$, and $\top$ to $\{a, b, c\}$.
  - $(\mathbb{N}, \leq)$ is a lattice with $\sqcup$ being max and $\sqcap$ being min, but not a complete lattice since $\sqcup\mathbb{N}$ does not exist in $\mathbb{N}$.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.
  - $\bot_A = \sqcap A$ and $\top_A = \sqcup A$ are the least and greatest elements of a complete lattice, respectively.

- Examples:
  - $(2^{\{a,b,c\}}, \subseteq)$ is a complete lattice, $\sqcap$ corresponds to $\cap$, $\sqcup$ to $\cup$, $\bot$ to $\emptyset$, and $\top$ to $\{a, b, c\}$.
  - $(\mathbb{N}, \leq)$ is a lattice with $\sqcup$ being max and $\sqcap$ being min, but not a complete lattice since $\sqcup\mathbb{N}$ does not exist in $\mathbb{N}$.
  - $(\mathbb{N}_\infty, \leq)$, where $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ and $\forall n \in \mathbb{N}.\ n \leq \infty$, is a complete lattice.

Lattices

- A poset $(A, \leq_A)$ is a lattice iff each *non-empty, finite* subset B of A has a lub as well as a glb in A.

- A poset $(A, \leq_A)$ is a complete lattice iff each subset B of A has a lub as well as a glb in A.
  - $\bot_A = \sqcap A$ and $\top_A = \sqcup A$ are the least and greatest elements of a complete lattice, respectively.

- Examples:
  - $(2^{\{a,b,c\}}, \subseteq)$ is a complete lattice, $\sqcap$ corresponds to $\cap$, $\sqcup$ to $\cup$, $\bot$ to $\emptyset$, and $\top$ to $\{a, b, c\}$.
  - $(\mathbb{N}, \leq)$ is a lattice with $\sqcup$ being max and $\sqcap$ being min, but not a complete lattice since $\sqcup\mathbb{N}$ does not exist in $\mathbb{N}$.
  - $(\mathbb{N}_\infty, \leq)$, where $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ and $\forall n \in \mathbb{N}.\ n \leq \infty$, is a complete lattice.

- Given a poset $(A, \leq_A)$, a set $B \subseteq A$ is a chain iff $\forall b, b' \in B.\ b \leq_A b' \ \vee\ b' \leq_A b$.
  - E.g., $\{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$ is a chain wrt. $(2^{\{a,b,c\}}, \subseteq)$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.
- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \Longrightarrow f(a) \leq_B f(a')$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.
- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \implies f(a) \leq_B f(a')$.
- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.

- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \Longrightarrow f(a) \leq_B f(a')$.

- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

- An element $a \in A$ is a fixpoint of a function $f : A \longrightarrow A$ iff $f(a) = a$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.

- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \Longrightarrow f(a) \leq_B f(a')$.

- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

- An element $a \in A$ is a fixpoint of a function $f : A \longrightarrow A$ iff $f(a) = a$.

- An example: Consider the function $f : \mathbb{N}_\infty \longrightarrow \mathbb{N}_\infty$ defined such that $\forall n \in \mathbb{N}.\ f(n) = 0$ and $f(\infty) = \infty$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.

- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \implies f(a) \leq_B f(a')$.

- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

- An element $a \in A$ is a fixpoint of a function $f : A \longrightarrow A$ iff $f(a) = a$.

- An example: Consider the function $f : \mathbb{N}_\infty \longrightarrow \mathbb{N}_\infty$ defined such that $\forall n \in \mathbb{N}.\ f(n) = 0$ and $f(\infty) = \infty$.
  - f is monotonic since (1) $\forall n_1, n_2 \in \mathbb{N}.\ f(n_1) = 0 \leq 0 = f(n_2)$ and (2) $\forall n \in \mathbb{N}.\ f(n) = 0 \leq \infty = f(\infty)$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.

- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \Longrightarrow f(a) \leq_B f(a')$.

- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

- An element $a \in A$ is a fixpoint of a function $f : A \longrightarrow A$ iff $f(a) = a$.

- An example: Consider the function $f : \mathbb{N}_\infty \longrightarrow \mathbb{N}_\infty$ defined such that $\forall n \in \mathbb{N}.\ f(n) = 0$ and $f(\infty) = \infty$.
  - f is monotonic since (1) $\forall n_1, n_2 \in \mathbb{N}.\ f(n_1) = 0 \leq 0 = f(n_2)$ and (2) $\forall n \in \mathbb{N}.\ f(n) = 0 \leq \infty = f(\infty)$.
  - f is not $\sqcup$-continuous since $\mathbb{N}$ is a chain and $f(\sqcup\mathbb{N}) = f(\infty) = \infty$, but $\sqcup\{f(n) \mid n \in \mathbb{N}\} = \sqcup\{0\} = 0$.

Functions on Lattices

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be lattices.

- A function $f : A \longrightarrow B$ is monotonic iff $\forall a, a' \in A.\ a \leq_A a' \implies f(a) \leq_B f(a')$.

- A function $f : A \longrightarrow B$ is $\sqcup$-continuous iff for every chain $C \subseteq A$, we have $f(\sqcup C) = \sqcup\{f(c) \mid c \in C\}$. Analogously, one can define $\sqcap$-continuous functions.

- An element $a \in A$ is a fixpoint of a function $f : A \longrightarrow A$ iff $f(a) = a$.

- An example: Consider the function $f : \mathbb{N}_\infty \longrightarrow \mathbb{N}_\infty$ defined such that $\forall n \in \mathbb{N}.\ f(n) = 0$ and $f(\infty) = \infty$.
  - f is monotonic since (1) $\forall n_1, n_2 \in \mathbb{N}.\ f(n_1) = 0 \leq 0 = f(n_2)$ and (2) $\forall n \in \mathbb{N}.\ f(n) = 0 \leq \infty = f(\infty)$.
  - f is not $\sqcup$-continuous since $\mathbb{N}$ is a chain and $f(\sqcup\mathbb{N}) = f(\infty) = \infty$, but $\sqcup\{f(n) \mid n \in \mathbb{N}\} = \sqcup\{0\} = 0$.
  - 0 is the least fixpoint of f and ∞ is the greatest fixpoint of f.

Knaster–Tarski Theorem

❖ **Knaster–Tarski Theorem.** Let $(A, \leq_A)$ be a complete lattice and let $f : A \longrightarrow A$ be a monotonic function. Then the set of fixpoints of f in $(A, \leq_A)$ is also a complete lattice.

❖ Since complete lattices have the least and the greatest element, the theorem in particular guarantees the existence of a least and greatest fixpoint of f in A.

Knaster–Tarski Theorem

❖ **Knaster–Tarski Theorem.** Let $(A, \leq_A)$ be a complete lattice and let $f : A \longrightarrow A$ be a monotonic function. Then the set of fixpoints of f in $(A, \leq_A)$ is also a complete lattice.

❖ Since complete lattices have the least and the greatest element, the theorem in particular guarantees the existence of a least and greatest fixpoint of f in A.

For the more curious:

❖ In more constructive terms, the least fixpoint of f is the stationary limit of $f^\alpha(\perp_A)$ for α ranging over the ordinals.

- An ordinal is the order type of a well-ordered set.

Knaster–Tarski Theorem

❖ **Knaster–Tarski Theorem.** Let $(A, \leq_A)$ be a complete lattice and let $f : A \longrightarrow A$ be a monotonic function. Then the set of fixpoints of f in $(A, \leq_A)$ is also a complete lattice.

❖ Since complete lattices have the least and the greatest element, the theorem in particular guarantees the existence of a least and greatest fixpoint of f in A.

For the more curious:

❖ In more constructive terms, the least fixpoint of f is the stationary limit of $f^\alpha(\perp_A)$ for α ranging over the ordinals.

- An ordinal is the order type of a well-ordered set.
- Every ordinal can be represented as the set of all smaller ordinals. There is the zero ordinal, successor ordinals, and limit ordinals. Natural numbers correspond to the so called finite ordinals (ordering types of finite sets), the set of natural numbers is the first infinite ordinal, and so on.

Knaster–Tarski Theorem

❖ **Knaster–Tarski Theorem.** Let $(A, \leq_A)$ be a complete lattice and let $f : A \longrightarrow A$ be a monotonic function. Then the set of fixpoints of f in $(A, \leq_A)$ is also a complete lattice.

❖ Since complete lattices have the least and the greatest element, the theorem in particular guarantees the existence of a least and greatest fixpoint of f in A.

For the more curious:

❖ In more constructive terms, the least fixpoint of f is the stationary limit of $f^\alpha(\perp_A)$ for α ranging over the ordinals.

- An ordinal is the order type of a well-ordered set.
- Every ordinal can be represented as the set of all smaller ordinals. There is the zero ordinal, successor ordinals, and limit ordinals. Natural numbers correspond to the so called finite ordinals (ordering types of finite sets), the set of natural numbers is the first infinite ordinal, and so on.
- f^α is defined by transfinite induction: $f^{\alpha+1} = f(f^\alpha)$ and f^γ for a limit ordinal γ is the least upper bound of f^β for all ordinals β smaller than γ.

Knaster–Tarski Theorem

❖ **Knaster–Tarski Theorem.** Let $(A, \leq_A)$ be a complete lattice and let $f : A \longrightarrow A$ be a monotonic function. Then the set of fixpoints of f in $(A, \leq_A)$ is also a complete lattice.

❖ Since complete lattices have the least and the greatest element, the theorem in particular guarantees the existence of a least and greatest fixpoint of f in A.

For the more curious:

❖ In more constructive terms, the least fixpoint of f is the stationary limit of $f^\alpha(\bot_A)$ for α ranging over the ordinals.

- An ordinal is the order type of a well-ordered set.
- Every ordinal can be represented as the set of all smaller ordinals. There is the zero ordinal, successor ordinals, and limit ordinals. Natural numbers correspond to the so called finite ordinals (ordering types of finite sets), the set of natural numbers is the first infinite ordinal, and so on.
- f^α is defined by transfinite induction: $f^{\alpha+1} = f(f^\alpha)$ and f^γ for a limit ordinal γ is the least upper bound of f^β for all ordinals β smaller than γ.

❖ A dual result holds for the greatest fixpoint.

Kleene Fixpoint Theorem

❖ **Kleene Fixpoint Theorem.** Let $(A, \leq_A)$ be a complete lattice and $f : A \longrightarrow A$ a function.

- If f is $\sqcup$-continuous, the least fixpoint of f is $\mu f = \sqcup\{f^i(\bot_A) \mid i \geq 0\}$.

Kleene Fixpoint Theorem

- **Kleene Fixpoint Theorem.** Let $(A, \leq_A)$ be a complete lattice and $f : A \longrightarrow A$ a function.
  - If f is $\sqcup$-continuous, the least fixpoint of f is $\mu f = \sqcup\{f^i(\bot_A) \mid i \geq 0\}$.
    - Moreover, a $\sqcup$-continuous function is monotone, and hence one in fact computes the supremum of the ascending chain $\bot_A \leq_A f(\bot_A) \leq_A f(f(\bot_A)) \leq ....$

Kleene Fixpoint Theorem

❖ **Kleene Fixpoint Theorem.** Let $(A, \leq_A)$ be a complete lattice and $f : A \longrightarrow A$ a function.

- If f is $\sqcup$-continuous, the least fixpoint of f is $\mu f = \sqcup\{f^i(\bot_A) \mid i \geq 0\}$.
  - Moreover, a $\sqcup$-continuous function is monotone, and hence one in fact computes the supremum of the ascending chain $\bot_A \leq_A f(\bot_A) \leq_A f(f(\bot_A)) \leq \ldots$.
- If f is $\sqcap$-continuous, the greatest fixpoint of f is $\nu f = \sqcap\{f^i(\top_A) \mid i \geq 0\}$.
  - Moreover, a $\sqcap$-continuous function is monotone, and hence one in fact computes the infimum of the descending chain $\top_A \geq_A f(\top_A) \geq_A f(f(\top_A)) \geq \ldots$.

Kleene Fixpoint Theorem

- **Kleene Fixpoint Theorem.** Let $(A, \leq_A)$ be a complete lattice and $f : A \longrightarrow A$ a function.
  - If f is $\sqcup$-continuous, the least fixpoint of f is $\mu f = \sqcup\{f^i(\bot_A) \mid i \geq 0\}$.
    - Moreover, a $\sqcup$-continuous function is monotone, and hence one in fact computes the supremum of the ascending chain $\bot_A \leq_A f(\bot_A) \leq_A f(f(\bot_A)) \leq \ldots$.
  - If f is $\sqcap$-continuous, the greatest fixpoint of f is $\nu f = \sqcap\{f^i(\top_A) \mid i \geq 0\}$.
    - Moreover, a $\sqcap$-continuous function is monotone, and hence one in fact computes the infimum of the descending chain $\top_A \geq_A f(\top_A) \geq_A f(f(\top_A)) \geq \ldots$.

- **Theorem.** For finite complete lattices, every monotonic function is $\sqcap$- and $\sqcup$-continuous.

Kleene Fixpoint Theorem

- **Kleene Fixpoint Theorem.** Let $(A, \leq_A)$ be a complete lattice and $f : A \longrightarrow A$ a function.
  - If f is $\sqcup$-continuous, the least fixpoint of f is $\mu f = \sqcup\{f^i(\bot_A) \mid i \geq 0\}$.
    - Moreover, a $\sqcup$-continuous function is monotone, and hence one in fact computes the supremum of the ascending chain $\bot_A \leq_A f(\bot_A) \leq_A f(f(\bot_A)) \leq \ldots$.
  - If f is $\sqcap$-continuous, the greatest fixpoint of f is $\nu f = \sqcap\{f^i(\top_A) \mid i \geq 0\}$.
    - Moreover, a $\sqcap$-continuous function is monotone, and hence one in fact computes the infimum of the descending chain $\top_A \geq_A f(\top_A) \geq_A f(f(\top_A)) \geq \ldots$.

- **Theorem.** For finite complete lattices, every monotonic function is $\sqcap$- and $\sqcup$-continuous.

- **Corollary.** On finite lattices, the Kleene fixpoint theorem is applicable, hence,
  - to compute the least fixpoint, start with $\bot_A$ and iteratively apply f till $f^i(\bot_A) = f^{i+1}(\bot_A) = \mu f$,
  - to compute the greatest fixpoint, start with $\top_A$ and iteratively apply f till $f^i(\top_A) = f^{i+1}(\top_A) = \nu f$.