So far, we understand in principle how to obtain inductive invariants using abstract interpretation.
For the actual computation, we rely on Kleene's fixed point theorem.

Definition:

Let $(L, \leq)$ be a lattice.

- A chain is a totally ordered set $K \subseteq L$.
- A function $f : L \to L$ is continuous, if
$$f(\bigsqcup K) = \bigsqcup \underbrace{f(K)}_{\{f(k) \mid k \in K\}} \quad \text{f.a. chains } K \text{ in } L$$
- A lattice satisfies the ascending chain condition (ACC), if for all chains
$$k_0 \leq k_1 \leq k_2 \leq \ldots$$
there is an index i so that $k_i = k_{i+1} = k_{i+2} = \ldots$
We also say the chain stabilizes or becomes stationary.

Lemma:

Let $(L, \leq)$ be a lattice and $f : L \to L$ a function.

1) If f is continuous, then f is monotonic.
2) If L satisfies ACC and f is monotonic, then f is continuous.
3) If f is monotonic, then $(f^i(\bot))_{i \in \mathbb{N}}$ is a chain, with $f^0(\bot) := \bot$ and $f^{i+1}(\bot) := f(f^i(\bot))$.

Proof:

1.) Let $l_1 \leq l_2$.

Then $f(l_1) \leq f(l_1) \sqcup f(l_2)$

$\{\text{cont}\} = f(l_1 \sqcup l_2) = f(l_2)$.

2.) Consider a chain K.

Then $\bigsqcup K = k_i$, with i: the index in which the chain stabilizes.

Now $f(\bigsqcup K) = f(k_i) \overset{\text{(monotonicity)}}{\leq} \bigsqcup f(K)$.

For $\bigsqcup f(K) \leq f(\bigsqcup K)$, use that $f(k) \leq f(\bigsqcup K)$ for all $k \in K$.

3.) We proceed by induction and show that $f^i(\bot) \leq f^{i+1}(\bot)$ for all $i \in \mathbb{N}$.

<u>Base case</u>: $f^0(\bot) = \bot \overset{\text{By definition of } \bot.}{\leq} f(\bot)$

<u>IS</u>: Assume $f^i(\bot) \leq f^{i+1}(\bot)$.

Then $f(f^i(\bot)) \leq f(f^{i+1}(\bot))$ by monotonicity. $\square$

<u>Theorem (Kleene)</u>:

Let $(L, \leq)$ be a lattice and $f: L \to L$ be continuous.

Then $lfp.f = \bigsqcup_{i \geq 0} f^i(\bot)$.

Remark: The result already holds for
the weaker chain-complete partial orders
in which there is a least element
and the least upper bound $\bigsqcup K$
of every chain K belongs to the partial order.

Proof: "$\sqsubseteq$" We have

$$f\left(\bigsqcup_{i\geq 0} f^i(\bot)\right) \overset{\text{(continuity)}}{=} \bigsqcup_{i\geq 1} f^i(\bot) = \bigsqcup_{i\geq 0} f^i(\bot).$$

Hence, $\bigsqcup_{i\geq 0} f^i(\bot)$ is a fixed point.

"$\sqsupseteq$" We show that $f^i(\bot) \leq$ lfp.f f.a. $i \in \mathbb{N}$.

$i=0$: $f^0(\bot) = \bot \leq$ lfp.f.

$i \rightsquigarrow i+1$: Assume $f^i(\bot) \leq$ lfp.f.

Then $f(f^i(\bot)) \underset{\text{(monotonicity)}}{\leq} f(\text{lfp}.f) = \text{lfp}.f$. $\square$

Kleene's fixed point theorem is only helpful
in settings where the ascending chain condition holds.

Fact: If $(L, \leq)$ is finite, then L satisfies (ACC).

The more interesting settings are infinite lattices.
We need a new concept.

Definition: A *quasi order* (qo) $(S, \leq)$ consists of
a set S with $\leq \subseteq S \times S$ reflexive and transitive.

- A qo $(S, \leq)$ is a <u>well quasi order</u> (wqo), if for every infinite sequence $(s_i)_{i \in \mathbb{N}}$ there are $i < j$ so that $s_i \leq s_j$.

- The <u>upward closure</u> of a set $M \subseteq S$ is
$$M\!\uparrow := \{ s \in S \mid \exists m \in M.\ m \leq s \}.$$
A set $U \subseteq S$ is <u>upward closed</u>, if $U\!\uparrow = U$.

- An element $m \in U \subseteq S$ is <u>minimal</u>, if $\nexists m' \in U.\ m' \leq m \wedge m \not\leq m'$
$(\forall m' \in U.\ m' \leq m \rightarrow m \leq m')$.

- An <u>antichain</u> $A \subseteq S$ only contains incomparable elements.

- A qo $(S, \leq)$ is <u>well founded</u>, if all descending chains $d_0 \geq d_1 \geq \dots$ become stationary: $\exists i \in \mathbb{N}.\ d_i = d_{i+1} = d_{i+2} = \dots$

<u>Theorem:</u>
Let $(S, \leq)$ be a qo.
1) $(S, \leq)$ is (a) a wqo iff there are (b) no infinite antichains and $(S, \leq)$ is well-founded.
2) $(S, \leq)$ is (a) a wqo iff (b) every infinite sequence $(s_i)_{i \in \mathbb{N}}$

contains an infinite increasing subsequence $(s_{e(i)})_{i \in \mathbb{N}}$ with

$$s_{e(0)} \leq s_{e(1)} \leq s_{e(2)} \leq \dots$$

3) $(S, \leq)$ is well founded $\overset{(a)}{\text{iff}}$

every set $\emptyset \neq U \subseteq S$ contains$^{(b)}$ a minimal element.

4) $(S, \leq)$ is a $\overset{(a)}{\text{wqo}}$ iff

every set $\emptyset \neq U \subseteq S$ has $\overset{(b)}{\text{a}}$ minimal element and every subset of incomparable minimal elements is finite.

5) $(S, \leq)$ is a $\overset{(a)}{\text{wqo}}$ iff

$\overset{(b)}{\text{every}}$ chain of upward-closed sets

$U_0 \subseteq U_1 \subseteq U_2 \subseteq \dots$ stabilizes.

Proof:

1a) $\Rightarrow$ 1b) Easy.

2b) $\Rightarrow$ 2a) Easy

1b) $\Rightarrow$ 2b) We use Ramsey's theorem to show that if there are no infinite antichains and no infinite strictly descending sequences, then there have to be increasing subsequences.

Theorem (Ramsey):

Consider the infinite complete graph $K_{\mathbb{N}}$.
Consider the edges are colored with finitely many colors.
Assume the edges are colored with finitely many colors.
Then there is an infinite and still complete subgraph $K_{\mathbb{N}'}$ whose edges are colored with a single color.

Consider an infinite sequence $(s_i)_{i \in \mathbb{N}}$.
We understand the elements in the sequence as the nodes in $K_{\mathbb{N}}$.
For an edge

$$s_i — s_j, \text{ with } i < j,$$

we use the color

$$\begin{array}{lll} \text{INCOMP}, & \text{if} & s_i \nleq s_j \text{ and } s_j \nleq s_i, \\ \text{DEC}, & \text{if} & s_i \nleq s_j \text{ and } s_j \leq s_i, \\ \text{INC}, & \text{if} & s_i \leq s_j. \end{array}$$

Ramsey's theorem gives us an infinite monochromatic subgraph.
By assumption, the color cannot be
INCOMP (otherwise, we had an infinite antichain)
and not DEC (otherwise, we violated well-foundedness).
The infinite subgraph corresponds to the infinite increasing subsequence.

3a) $\Rightarrow$ 3b) We construct a strictly decreasing sequence $(u_i)_{i \in I}$ in U.
Using the axiom of choice, we pick u_0 in U.
Assume we already constructed the sequence up to u_i.
If there is $u \in U$ with $u \leq u_i$ and $u_i \nleq u$,
pick such an element as u_{i+1}, again using the axiom of choice.

The sequence cannot be infinite by assumption,
so it ends in an element that is minimal.

3b) $\Rightarrow$ 3a) Consider a descending chain $d_0 \geq d_1 \geq \dots$

We understand it as a set U.
By assumption, U has a minimal element d_i.
This is the moment the chain stabilizes.

4a) $\Rightarrow$ 4b) Holds by 4a) = 1a),
by 1a) $\Rightarrow$ 1b),
by 1b) = 3a) + no inf. antichains,
by 3a) + no inf. antichains $\Rightarrow$ 4b)

4b) $\Rightarrow$ 4a) Is also via 1) and 3).

5a) $\Rightarrow$ 5b) Consider a chain of upward-closed sets $(U_i)_{i \in \mathbb{N}}$.

Towards a contradiction, assume we can isolate
a strictly increasing subsequence
$$U_{e(0)} \subsetneq U_{e(1)} \subsetneq \dots$$
Let $u_{e(i+1)} \in U_{e(i+1)} \setminus U_{e(i)}$.
Then $(u_{e(i)})_{i \in \mathbb{N}}$ contradicts the wqo assumption.

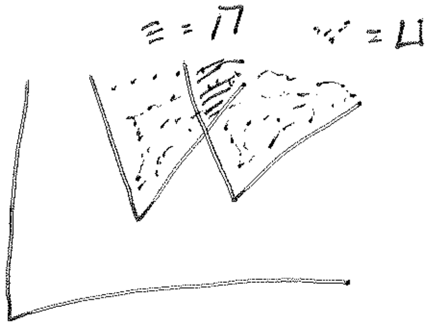
5b) $\Rightarrow$ 5a) Consider a sequence $(s_i)_{i \in \mathbb{N}}$.
Take the chain of upward-closed sets $(U_i)_{i \in \mathbb{N}}$
with $U_i := \{s_0, \dots, s_i\}\uparrow$.
Since this chain stabilizes, there are $i < j$ with
$s_i \leq s_j$. $\square$

The theorem shows us another instance of lattices with (ACC), namely $\boxed{\text{upward-closed sets in a wqo.}}$

Lemma:

Let $(S, \leq)$ be a wqo.
The set $(\mathbb{P}_{\uparrow}(S), \subseteq)$ of upward-closed sets in S ordered by inclusion is a lattice that satisfies (ACC).

Proof:



- That we have (ACC) is 5b) in the previous theorem.
- To see that we have a lattice, note that upward-closed sets are closed under arbitrary joins and arbitrary meets. $\square$

By 4b), every upward-closed set only has finitely many minimal elements that are incomparable.

> We want to use these elements as the abstraction.

To avoid the problem of having to deal with comparable minimal elements, we assume $(S, \leq)$ is actually a partial order (po).
Note that every qo $(S, \leq)$ can be turned into the po $(S/_{\equiv}, \leq)$ with $s_1 \equiv s_2$ iff $s_1 \leq s_2 \wedge s_2 \leq s_1$.

Then $\min : \mathbb{P}(S) \to \mathbb{P}(S)$ with $\min(U) =$ minimal elements in U well-defined.

Definition:

Let $(S, \leq)$ be a wpo.

Let $\mathbb{AC}(S)$ be the set of antichains in S.

We define $(\mathbb{AC}(S), \leq)$ the lattice with

$$B_1 \leq B_2 \text{, if } B_1\uparrow \subseteq B_2\uparrow.$$

Then we have $(\mathbb{ACC})$ by 5b) above.

$\forall b_1 \in B_1$
$\exists b_2 \in B_2.$
$b_2 \leq b_1.$

We are now ready to give the Galois connection for

Definition:

$$(\mathbb{P}_\uparrow(S), \subseteq) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} (\mathbb{AC}(S), \leq)$$

with $\alpha = \min(-)$

$\gamma = -\uparrow$

is a Galois connection.

Even more, $\min(\mathcal{U})\uparrow = \mathcal{U}$ holds.