Program verification 2016

Lecture 3: Lattice theory and Galois connection

Instructor: Ashutosh Gupta

TIFR, India

Compile date: 2016-03-21

Where are we?

- Labelled transition system
- Symbolic methods for program analysis (without abstraction)
- SMT solving
- theory solvers for various theories
- theory combination (should have been covered in detail!)

Lecture plan

- Labelled transition system (reminder)
- Fixed point computation and Abstraction
- Lattice theory
- Maps and Galios(read galva) connection
- Fixed point theory
- Asynchronous iterations for fixed points

Topic 3.1

Labeled transition system (reminder)

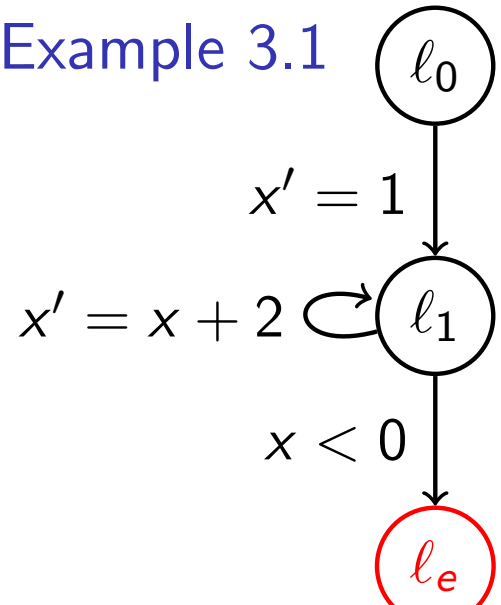
labeled transition system (LTS)

Definition 3.1

A program P is a tuple $(V, L, \ell_0, \ell_e, E)$, where

- *V is a vector of variables,*
- *L be set of program locations,*
- *ℓ_0 is initial location,*
- *ℓ_e is error location, and*
- *$E \subseteq L \times \Sigma(V, V') \times L$ is a set of labeled transitions between locations.*

Example 3.1



$$V = [\mathtt{x}]$$
$$L = \{\ell_0, \ell_1, \ell_e\}$$
$$E = \{(\ell_0, \mathtt{x}' = 1, \ell_1), (\ell_1, \mathtt{x}' = \mathtt{x} + 2, \ell_1), (\ell_1, \mathtt{x} < 0, \ell_e)\}$$

Notation:

If $e = (\ell, \rho(V, V'), \ell') \in E$, then

$e(V, V') \triangleq \rho(V, V')$,

$e(loc) \triangleq \ell$ and

$e(loc') \triangleq \ell'$

Semantics

Consider program $P = (V, L, \ell_0, \ell_e, E)$.

Definition 3.2

A state $s = (\ell, v)$ of a program is program location ℓ and a valuation v of V.

Let $v(x) \triangleq$ value of variable x in v
For state $s = (\ell, v)$, let $s(x) \triangleq v(x)$ and $s(loc) \triangleq \ell$

Definition 3.3

A path $\pi = e_1, \ldots, e_n$ in P is a sequence of transitions such that, for each $0 < i < n$, $e_i = (\ell_{i-1}, \_, \ell_i)$ and $e_{i+1} = (\ell_i, \_, \ell_{i+1})$.

Definition 3.4

An execution corresponding to path $e_1, \ldots, e_n$ is a sequence of states $(\ell_0, v_0), \ldots, (\ell_n, v_n)$ such that $\forall i \in 1..n$, $e_i(v_{i-1}, v_i)$ holds true.
An execution belongs to P if there is a corresponding path in P.

Definition 3.5

P is safe if there is no execution of P from ℓ_0 to ℓ_e.

Reminder: symbolic strongest post

$$sp : \Sigma(V) \times \Sigma(V, V') \to \Sigma(V)$$

We define symbolic post over labels of P as follows.

$$sp(F, \rho) \triangleq (\exists V : F(V) \wedge \rho(V, V'))[V/V']$$

We assume that ρ and F are in a theory that admits quantifier elimination

Using polymorphism, we also define $sp((\ell, F), (\ell, \rho, \ell') \in E) \triangleq (\ell', sp(F, \rho))$.

For path $\pi = e_1, .., e_n$ of P, $sp((\ell, F), \pi) \triangleq sp(sp((\ell, F), e_1), e_2..e_n)$.

Topic 3.2

Fixed point computation and Abstraction

Reachability as fixed point equation

Consider program $P = (V, L, \ell_0, \ell_e, E)$

Let X_ℓ be a variable representing the reachable valuations at location $\ell \in L$

We may compute reachability using *sp* via the following fixed point equation

$$X_{\ell_0} = \top$$

$$\forall \ell' \in L \setminus \{\ell_0\}.\ X_{\ell'} = \bigvee_{(\ell,\rho,\ell') \in E} sp(X_\ell, \rho)$$

Note: For now, we are ignoring the constraints posed by the error location.

Fixed point computation

Initial assignment to variables and iteratively compute the fixed point

Let $X_\ell^i \triangleq$ value of X_ℓ at ith iteration.

In our setting, initially: $X_{\ell_0}^0 \triangleq \top$ and $X_\ell^0 \triangleq \bot$ for each $\ell \neq \ell_0$
and at each iteration

$$X_{\ell_0}^{k+1} = \top$$

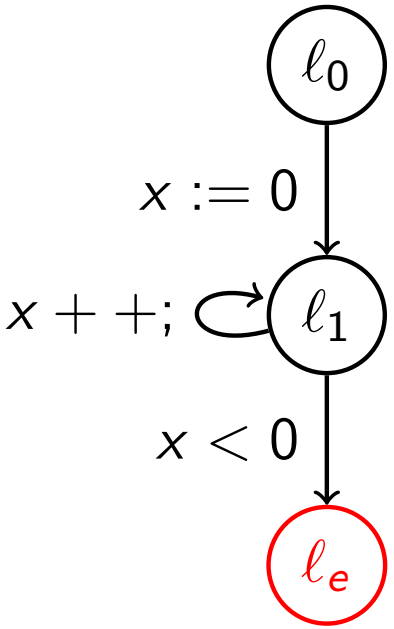
$$\forall \ell' \in L \setminus \{\ell_0\}.\ X_{\ell'}^{k+1} = X_{\ell'}^k \vee \bigvee_{(\ell,\rho,\ell') \in E} sp(X_\ell^k, \rho)$$

If $\forall \ell.\ X_\ell^k = X_\ell^{k+1}$, then we say that the iterations have converged at iteration k and we have computed the fixed point.

Example: diverging analysis with *sp*

Example 3.2

Consider program:



Fixed point equations:

$X_{\ell_0} = \top$

$X_{\ell_1} = sp(X_{\ell_0}, x' = 0) \vee sp(X_{\ell_1}, x' = x + 1)$

$X_{\ell_e} = sp(X_{\ell_1}, x < 0 \wedge x' = x)$

Iterates:

$X^0_{\ell_0} := \top, X^0_{\ell_1} := \bot, X^0_{\ell_e} := \bot$

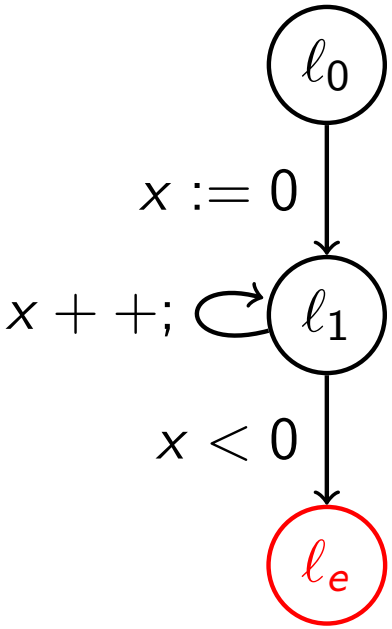
$X^1_{\ell_0} := \top, X^1_{\ell_1} := (x = 0), X^1_{\ell_e} := \bot$

$X^2_{\ell_0} := \top$

$X^2_{\ell_1} := X^1_{\ell_1} \vee sp(X^1_{\ell_1}, x' = x + 1) \vee sp(X^1_{\ell_0}, x' = 0)$
$:= (x = 0) \vee sp(x = 0, x' = x + 1) \vee sp(\top, x' = 0)$
$:= (x = 0 \vee x = 1 \vee x = 0) := (0 \leq x \leq 1)$

$X^2_{\ell_e} := sp(X^1_{\ell_1}, x < 0 \wedge x' = x)$
$:= sp(x = 0, x < 0 \wedge x' = x) := \bot$

Example: diverging analysis with *sp*(contd.)



Iterates(contd.):

$$X^3_{\ell_0} := \top, X^3_{\ell_1} := (0 \leq x \leq 2), X^3_{\ell_e} := \bot$$

$$\vdots$$

$$X^n_{\ell_0} := \top, X^n_{\ell_1} := (0 \leq x \leq n-1), X^n_{\ell_e} := \bot$$

...will never converge

How to compute fixed point effectively?

Abstract post $sp^{\#}$

Now we introduce the key method of verification

Let us define

$$sp^{\#} : \Sigma(V) \times \Sigma(V, V') \to \Sigma(V)$$

Abstract post must satisfy the following condition over labels of P

$$sp(F, \rho) \Rightarrow sp^{\#}(F, \rho)$$

It is up to us how we choose $sp^{\#}$ that satisfies the above condition

Important: We have defined $sp^{\#}$ using formulas. However, any data type (domain) can work that is capable of representing set of states.

Abstract Fixed point

Replace sp by $sp^{\#}$ for faster convergence

initially: $X^0_{\ell_0} \triangleq \top$ and $X^0_{\ell} \triangleq \bot$ for each $\ell \neq \ell_0$
and at each iteration

$$X^{k+1}_{\ell_0} = \top$$

$$\forall \ell' \in L \setminus \{\ell_0\}.\ X^{k+1}_{\ell'} = X^k_{\ell'} \vee \bigvee_{(\ell,\rho,\ell') \in E} sp^{\#}(X^k_{\ell}, \rho)$$

After convergence, X_ℓ will be a superset of reachable states at ℓ.

We will learn lattice theory to guide us in choosing $sp^{\#}$ such that we have better guarantee of convergence.

Topic 3.3

Lattice theory

Partial order and poset

Definition 3.6

On a set X, $\leq \subseteq X \times X$ is a partial order if

- *reflexive:* $\Delta_X \subseteq \leq$
- *anti-symmetric:* $\leq \cap \leq^{-1} \subseteq \Delta_X$
- *transitive:* $\leq \circ \leq \subseteq \leq$

We will use $x \leq y$ to denote $(x, y) \in \leq$
Let $x < y \triangleq (x \leq y \wedge x \neq y)$

Definition 3.7

A poset $(X, \leq)$ is a set equipped with partial order $\leq$ on X

Example 3.3

$(\mathbb{N}, \leq)$

Covering relation

Definition 3.8

The covering relation $\lessdot$ *for poset* $(X, \leq)$ *is*

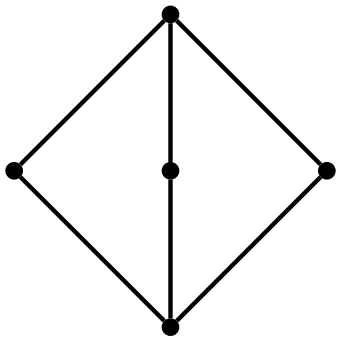
$$x \lessdot y \triangleq (x < y) \wedge \neg(\exists z. x < z \wedge z < y)$$

Hasse diagrams

We draw posets $(X, \leq)$ as DAG. Nodes are from X and edges are from $\lessdot$.

DAG will be vertically aligned, i.e., if there is an edge between x and y, and x is located below y then $x \lessdot y$.

Example 3.4



Nodes at same level are incomparable.

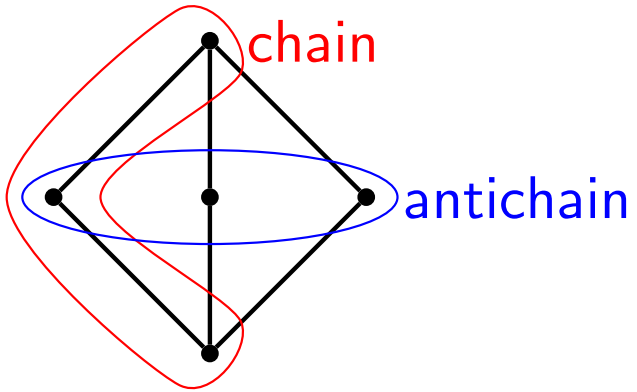
Chain and antichain

Definition 3.9

For a poset $(X, \leq)$, $C \subseteq X$ *is chain if* $\forall x, y \in C.\ x \leq y \vee y \leq x$

Definition 3.10

For a poset $(X, \leq)$, $C \subseteq X$ *is antichain if* $\forall x, y \in C.\ x \leq y \Rightarrow y = x$



- $(X, \leq)$ satisfies ascending chain condition if for any sequence $x_0 \leq x_1 \leq x_2 \leq \ldots$, $\exists k. \forall n > k\ x_k = x_n$
- symmetrically descending chain condition is defined
- $(X, \leq)$ is called well ordered if it satisfies descending chain condition

Exercise 3.1 *Prove* $(X, \leq)$ *has no infinite chains if it satisfies both ascending and descending chain condition*

Minimum(-mal) and Maximum(-mal) elements

For poset $(X, \leq)$ and $S \subseteq X$,
$minimal(S) \triangleq \{x \in S | \neg \exists y \in S.\ y < x\}$

$maximal(S) \triangleq \{x \in S | \neg \exists y \in S.\ y > x\}$

$min(S) \triangleq x$ if $\{x\} = minimal(S)$ //$min(S)$ may not exist

$max(S) \triangleq x$ if $\{x\} = maximal(S)$

If $min(X)$ exists then denoted by $\bot$

If $max(X)$ exists then denoted by $\top$

Upper bound and lower bound

For poset $(X, \leq)$,

- $x \in X$ is upper bound of $S \subseteq X$ if $\forall y \in S.\ y \leq x$
- $x \in X$ is lower bound of $S \subseteq X$ if $\forall y \in S.\ x \leq y$

Definition 3.11

$x \in X$ is least upper bound(lub) of S if x is upper bound of S and

$$\forall u.\ (\forall y \in S.\ y \leq u) \Rightarrow x \leq u$$

lub is usually denoted by $\vee, \sqcup$.

Definition 3.12

$x \in X$ is greatest lower bound(glb) of S if x is lower bound of S and

$$\forall u.\ (\forall y \in S.\ u \leq y) \Rightarrow u \leq x$$

lub is usually denoted by $\wedge, \sqcap$

Note: lub and glb may not exist.

Uniqueness of lub an glb

Theorem 3.1

For poset $(X, \leq)$ and $S \subseteq X$, if $\sqcup S$ exists then it is unique.

Proof.

- Suppose x and y are $\sqcup S$.
- By definition of $\sqcup$, x and y both are upper bounds of S.
- Since x is upper bound and y is $\sqcup S$, therefore $y \leq x$.
- Symmetrically, $x \leq y$.
- Due to anti-symmetry, $x = y$.

□

Therefore, $\sqcup$ and $\sqcap$ are partial functions : $2^X \to X$

- If $S = \{x, y\}$, we will write $x \sqcup y$
- The infix usage usually means, lub of finite elements

Semi-lattice

Definition 3.13

A join semi-lattice $(X, \sqsubseteq, \sqcup)$ *is a poset* $(X, \sqsubseteq)$ *such that* $\forall x, y \in X.\ x \sqcup y$ *exists.*

Theorem 3.2

A join semi-lattice $(X, \sqsubseteq, \sqcup)$ *satisfies*

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ *(associativity)*
- $(a \sqcup b) = (b \sqcup a)$ *(commutativity)*
- $a = (a \sqcup a)$ *(idempotence)*

Exercise 3.2

Prove 3.2

Equivalently, we define meet semi-lattice.

Equivalent definition of semi-lattice

Theorem 3.3

Let X be a set with function $\sqcup : X \times X \to X$ satisfying

$$(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c), \qquad (a \sqcup b) = (b \sqcup a), \quad \textit{and} \quad (a \sqcup a) = a.$$

Let $a \sqsubseteq b \triangleq (a \sqcup b) = b$. Then, $(X, \sqsubseteq, \sqcup)$ is a join semi-lattice.

Proof.

We need to show that $\sqsubseteq$ satisfies poset conditions and $\sqcup$ is lub.

1. $a \sqsubseteq a$ holds because $(a \sqcup a) = a$, (reflexivity proved)
2. Assume $a \sqsubseteq b$ and $b \sqsubseteq c$, and by def of $\sqsubseteq$, $(a \sqcup b) = b$ and $(b \sqcup c) = c$
3. By substitution, $((a \sqcup b) \sqcup c) = c$. By associativity, $a \sqcup (b \sqcup c) = c$
4. Due to 3, $a \sqcup c = c$, therefore $a \sqsubseteq c$, (transitivity proved)
5. Assume $a \sqsubseteq b$ and $b \sqsubseteq a$, and by def of $\sqsubseteq$, $(a \sqcup b) = b$ and $(b \sqcup a) = a$
6. By commutativity, $a = b$ (anti-symmetry proved)
7. Since $a \sqcup (a \sqcup b) = (a \sqcup a) \sqcup b = a \sqcup b$, $b \sqsubseteq a \sqcup b$. Similarly, $a \sqsubseteq a \sqcup b$
8. Let $a \sqsubseteq x$ and $b \sqsubseteq x$. Therefore,
   $(a \sqcup x) = x = (b \sqcup x) \Rightarrow (a \sqcup (b \sqcup x)) = x \Rightarrow ((a \sqcup b) \sqcup x) = x \Rightarrow (a \sqcup b) \sqsubseteq x$
9. Due to 7 and 8, $a \sqcup b = \mathit{lub}(\{a, b\})$

Lattice

$\sqcap$ and $\sqcup$ are forced to exist only for finite set

Definition 3.14

A lattice $(X, \sqsubseteq, \sqcup, \sqcap)$ *is a poset* $(X, \sqsubseteq)$ *such that* $\forall x, y \in X$ *both* $x \sqcup y$ *and* $x \sqcap y$ *exist.*

Properties

- $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$ (associativity)
- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$
- $(a \sqcap b) = (b \sqcap a)$ (commutativity)
- $(a \sqcup b) = (b \sqcup a)$
- $(a \sqcap a) = a = (a \sqcup a)$ (idempotence)
- $a \sqcap (a \sqcup b) = a$ (absorption)
- $b \sqcup (a \sqcap b) = b$

The above properties are axiomatization of lattice

Note: Observe that distributivity is missing!!!

Exercise 3.3

a. Prove absorption.

b. Show that semi-lattices $(X, \sqsubseteq_1, \sqcup)$ *and* $(X, \sqsubseteq_2, \sqcap)$*, and absorption properties imply* $(X, \sqsubseteq_1, \sqcup, \sqcap)$ *is a lattice.*

Complete partial order/lattice

Definition 3.15

A complete partial order(cpo) is a poset $(X, \sqsubseteq)$ such that every increasing chain in X has a lub in X

Definition 3.16

A complete lattice is a poset $(X, \sqsubseteq)$ such that for all $S \subseteq X$ has $\sqcup S$ in X.

Theorem 3.4

a. complete lattice has $\bot$

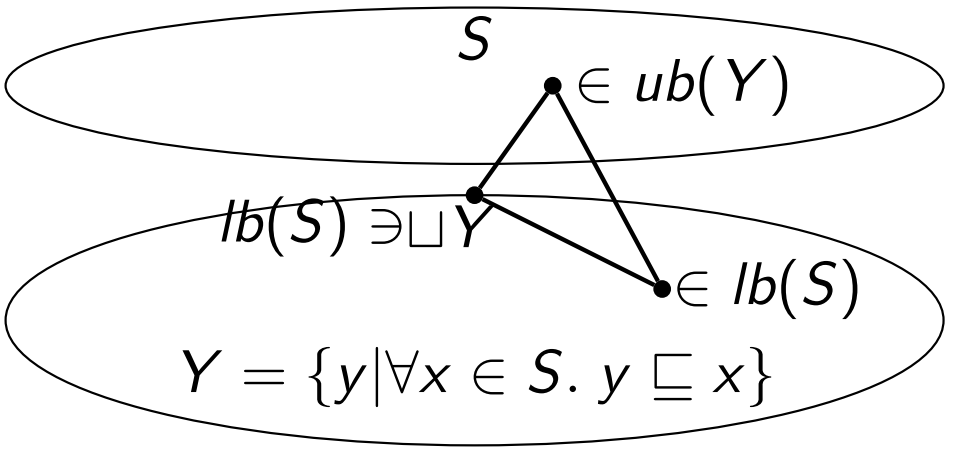
b. complete lattice has $\top$

c. $\sqcap S \triangleq \sqcup\{y | \forall x \in S.\ y \sqsubseteq x\}$

Exercise 3.4

Prove 3.4(a) and (b)

Proof 3.4c.



□

Exercise 3.5

a. Finite lattices are complete

b. Show if $(X, \sqsubseteq, \sqcup, \sqcap)$ satisfies ACC and has $\bot$ then it is a complete lattice.

Moore family

Definition 3.17

For a poset $(X, \sqsubseteq)$ with $\top$ element, a moore family $M \subseteq X$ is such that

- $\top \in M$
- $\forall S \subseteq M. \sqcap S$ *exists and* $\sqcap S \in M$

Theorem 3.5

Let $(X, \leq)$ be a poset with $\top$ element. If $M \subseteq X$ is a moore family then $(M, \sqsubseteq, \top, \sqcap M)$ is a complete lattice.

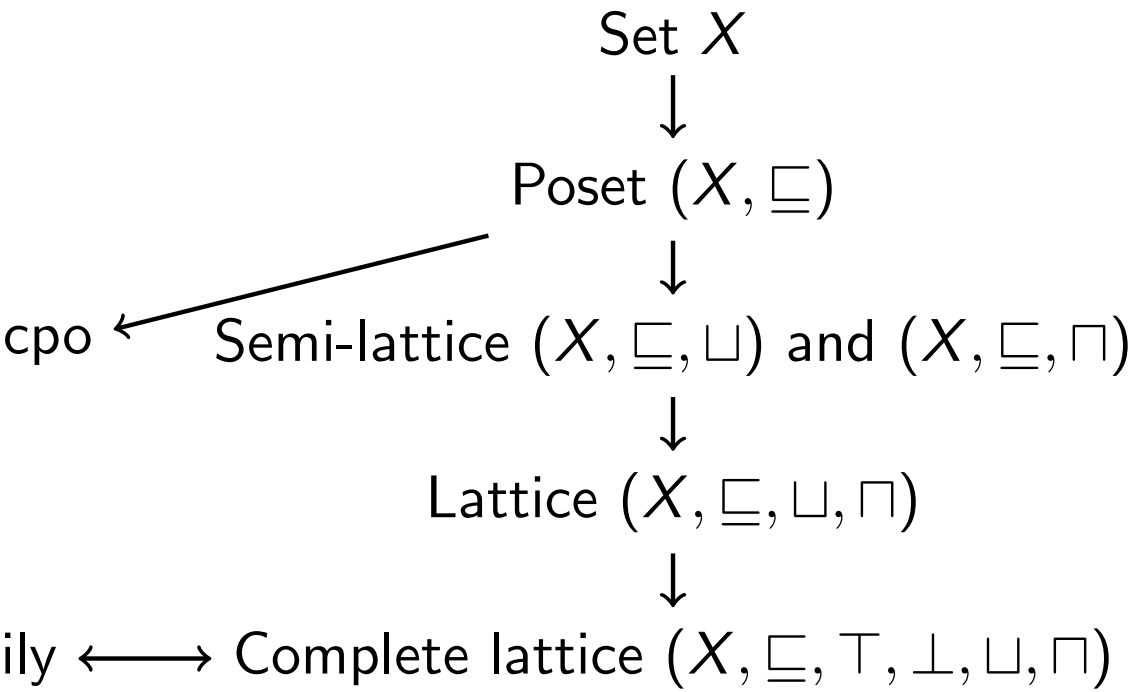
Proof.

1. $(X, \leq)$ is poset then $(M, \leq)$ is a poset
2. Since $\forall S \subseteq M. \sqcap S$ exists, M is a complete lattice due to Theorem 3.4.

□

Hierarchy of objects

We have seen the following objects



Topic 3.4

Maps and Galois connection

Morphisms

Definition 3.18

For sets X and Y, $f : X \to Y$ is a morphism relative to functions $g : X \to X$ and $g' : Y \to Y$ if

$$\forall x.\ f(g(x)) = g'(f(x))$$

A morphism may be defined relative to relations

Definition 3.19

For sets X and Y, $f : X \to Y$ is a morphism relative to relations $R : X \times X$ and $R' : Y \times Y$ such that

$$\forall x, y.\ (x, y) \in R \Rightarrow (f(x), f(y)) \in R'$$

Monotone maps

Definition 3.20

For posets $(X, \leq)$ *and* $(Y, \sqsubseteq)$, $f : X \to Y$ *is a monotone map if*

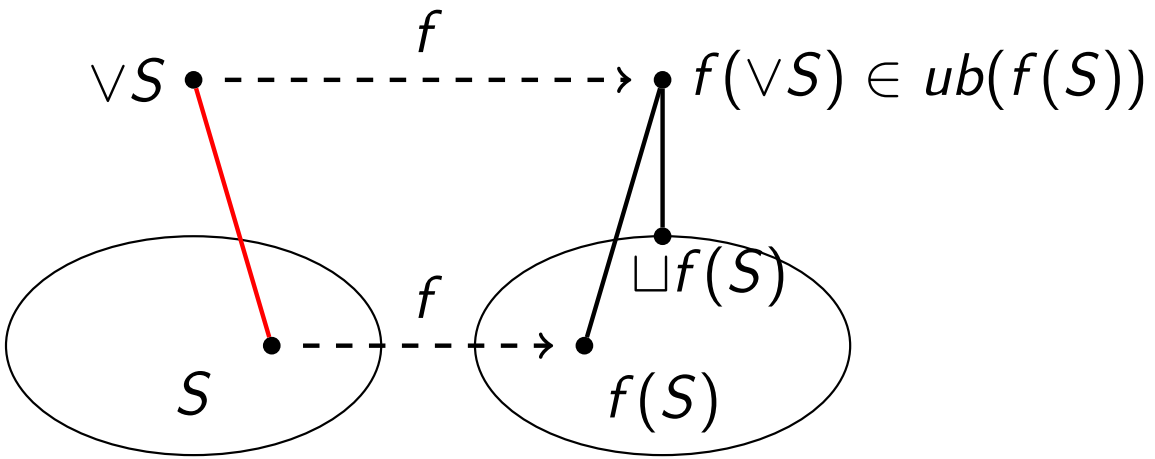
$$\forall x, y \in X.\ x \leq y \Rightarrow f(x) \sqsubseteq f(y)$$

Theorem 3.6

For posets $(X, \leq)$ *and* $(Y, \sqsubseteq)$, *let* $f : X \to Y$ *be monotone map. For* $S \subseteq X$, $\vee S$ *and* $\sqcup f(S)$ *exist then*

$$f(\vee S) \sqsubseteq \sqcup f(S)$$

Proof.



□

Order embedding

Definition 3.21

For posets $(X, \leq)$ and $(Y, \sqsubseteq)$, $f : X \to Y$ is an order embedding if

$$\forall x, y \in X.\ x \leq y \Leftrightarrow f(x) \sqsubseteq f(y)$$

Theorem 3.7

For posets $(X, \leq)$ and $(Y, \sqsubseteq)$, let $f : X \to Y$ be order embedding then f is injective.

Exercise 3.6

Prove 3.7

Order isomorphism

Definition 3.22

For posets $(X, \leq)$ and $(Y, \sqsubseteq)$,
$f : X \to Y$ is an order isomorphism if f is order embedding and onto.
$(X, \leq)$ and $(Y, \sqsubseteq)$ are order isomorphic if there is an order isomorphism between then.

Theorem 3.8

Posets $(X, \leq)$ and $(Y, \sqsubseteq)$ are order-isomorphic iff there exists $f : X \to Y$ and $g : Y \to X$ such that

- $f \circ g = 1_X$,
- $g \circ f = 1_Y$, *and*
- f *and* g *are monotone.*

Exercise 3.7

Prove theorem 3.8

Continuous maps

Definition 3.23

For posets $(X, \leq)$ and $(Y, \sqsubseteq)$, $f : X \to Y$ is continuous (upper-continuous) if for all chains $C \subseteq X$ such that $\vee C$ exists then $\sqcup f(C)$ exists and

$$f(\vee C) = \sqcup f(C)$$

Symmetrically, lower-continuous is defined.

Theorem 3.9

Continuous maps are monotonic

Exercise 3.8

Show if $x \sqsubseteq y$ and f is continuous then $f(y) = f(x) \sqcup f(y)$

Closure operators

Definition 3.24

On a poset $(X, \leq)$, f is an upper closure operator if for all $x, y \in X$

- $x \leq f(x)$ *(extensive)*
- $x \leq y \Rightarrow f(x) \leq f(y)$, *and* *(monotone)*
- $f(f(x)) = f(x)$. *(idempotent)*

Theorem 3.10

f is upper closure operator iff $x \leq f(y) \Leftrightarrow f(x) \leq f(y)$

Proof.

Assume f is upper closer

1. $x \leq f(y) \Rightarrow f(x) \leq f(f(y)) \Rightarrow f(x) \leq f(y)$ (proved forward implication)
2. $f(x) \leq f(y) \Rightarrow x \leq f(x) \leq f(y) \Rightarrow x \leq f(y)$ (proved backward implication)

Assume $x \leq f(y) \Leftrightarrow f(x) \leq f(y)$

1. $f(x) \leq f(x) \Rightarrow f \leq f(x)$ (proved extensive)
2. $x \leq y \Rightarrow x \leq y \leq f(y) \Rightarrow x \leq f(y) \Rightarrow f(x) \leq f(y)$ (proved monotonic)
3. $f(x) \leq f(x) \Rightarrow f(f(x)) \leq f(x)$ and $f(f(x)) \leq f(f(x)) \Rightarrow f(x) \leq f(f(x))$ (proved idempotent)

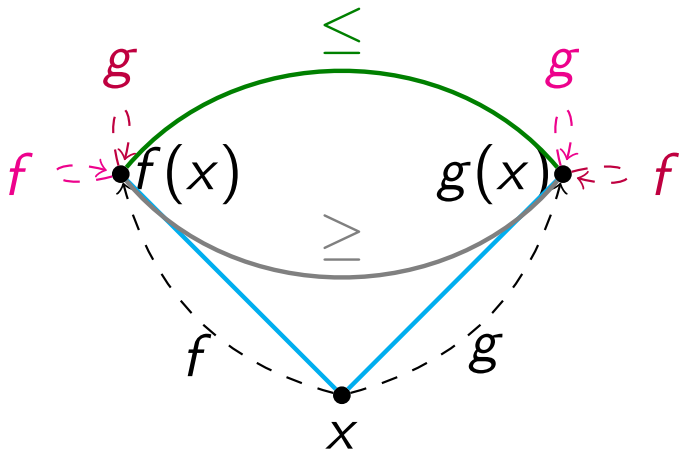
Fixed points of closure operators

Theorem 3.11

An upper closure operator is uniquely defined by its fixed points

Proof.

Let f and g be two upper closure operators that have same fixed points.
But, differ at point x, i.e., $f(x) \neq g(x)$.



due to idempotence of f and g

due to shared fixed points

due to extensive property

due to monotone g

due to monotone f

Contradiction: $f(x) = g(x)$

□

Exercise 3.9

a. Show $f(x) \sqcup f(y)$ is a fixed point

b. Show image of complete lattice by closure operator is complete lattice

Galois connection

Definition 3.25

For posets $(X, \leq)$ *and* $(Y, \sqsubseteq)$*, a pair of maps* (α, γ) *of maps* $\alpha : X \to Y$ *and* $\gamma : Y \to X$ *is a galois connection if*

$$\forall x \in X \forall y \in Y.\ \alpha(x) \sqsubseteq y \Leftrightarrow x \leq \gamma(y)$$

which is usually written

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$

α and γ are called upper and lower adjoints respectively.

Unique adjoints

Theorem 3.12

In $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$, α *uniquely defines* γ *and vice-versa.*

$$\alpha(x) = \sqcap\{y | x \leq \gamma(y)\} \qquad \gamma(y) = \vee\{x | \alpha(x) \sqsubseteq y\}$$

Proof.

- By definition of meet, $\sqcap\{y|\alpha(x) \sqsubseteq y\}$ exists and

$$\alpha(x) = \sqcap\{y|\alpha(x) \sqsubseteq y\}$$

- By def. of galois connection

$$\alpha(x) = \sqcap\{y|x \leq \gamma(y)\}$$

Symmetrically for $\gamma(x)$. □

Properties galois connection

Let $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$ then

1. $\forall x \in X. x \leq \gamma \circ \alpha(x)$
2. $\forall y \in Y. \alpha \circ \gamma(y) \sqsubseteq y$
3. α is monotone
4. γ is monotone
5. $\alpha \circ \gamma \circ \alpha = \alpha$
6. $\gamma \circ \alpha \circ \gamma = \gamma$
7. α is onto $\Leftrightarrow$ γ is one-to-one $\Leftrightarrow$ $\alpha \circ \gamma = 1_X$
8. γ is onto $\Leftrightarrow$ α is one-to-one $\Leftrightarrow$ $\gamma \circ \alpha = 1_Y$

Exercise 3.10

Prove the above properties

Exercise 3.11

Prove properties 1-4 also define galois connection

Topic 3.5

Fixed point theory

Fixed points

Let X be a set.
A fixed point of a operator $f : X \to X$ is $x \in X$ such that $f(x) = x$

Let f be an operator on poset $(X, \leq)$:

- $fp(f) \triangleq \{x | f(x) = x\}$
- $prefp(f) \triangleq \{x | x \leq f(x)\}$
- $postfp(f) \triangleq \{x | f(x) \leq x\}$
- least fixed point $lfp(f) \triangleq min(fp(f))$
- greatest fixed point $gfp(f) \triangleq max(fp(f))$

Note: $fp(f) = prefp(f) \cap postfp(f)$

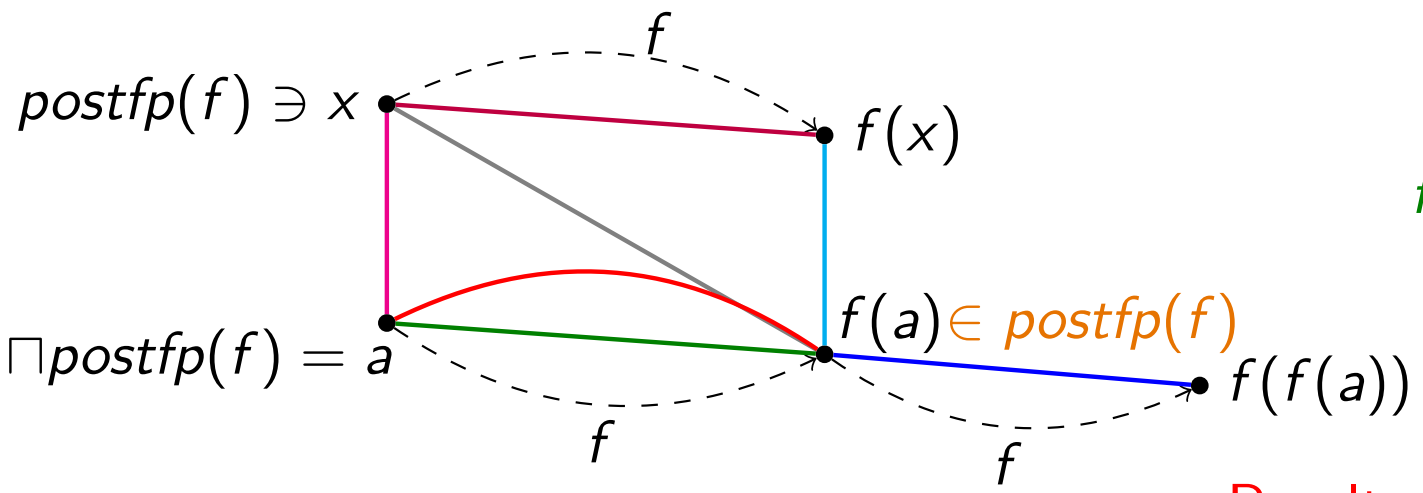
Knaster-Tarski fixed point theorem

Theorem 3.13

A monotonic map $f : X \to X$ on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$ has a least fixed point and a greatest fixed point, which are

$$lfp(f) = \sqcap postfp(f) = \sqcap\{x | f(x) \sqsubseteq x\}$$
$$gfp(f) = \sqcup prefp(f) = \sqcup\{x | x \sqsubseteq f(x)\}$$

Proof.



Reasons:

complete lattice $\Rightarrow \sqcap$ exist

$x \in postfp(f)$

f is monotone

transitivity

$f(a)$ is lb and a is glb

f is monotone

def. $postfp(f)$

def. $\sqcap postfp(f)$

Result: $f(a) = a \in postfp(f)$

Since $fp(f) \subseteq postfp(f)$, a is lfp. (why $postfp(f) \neq \emptyset$?) □

lfp greater than a prefix point

Definition 3.26

Let $f : X \to X$ be a monotonic map on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$. Let $a \in X$. Let $lfp_a(f)$ be the least fixed point of f greater than a, i.e.,

$$a \sqsubseteq lfp_a(f) \qquad lfp_a(f) = f(lfp_a(f)) \qquad \forall x.\ a \sqsubseteq x = f(x) \Rightarrow lfp_a(f) \sqsubseteq x$$

Theorem 3.14

If $a \in prefp(f)$ then $lfp_a(f)$ exists and $lfp_a(f) = lfp(\lambda x.a \sqcup f(x))$.

Proof.

1. Let $p = lfp(\lambda x.a \sqcup f(x))$. So, $p = a \sqcup f(p)$.
2. By def. of $\sqcup$, $a \sqsubseteq p$, the first condition satisfied
3. Due to monotonic f, $f(a) \sqsubseteq f(p)$
4. Due to $a \sqsubseteq f(a)$ and transitivity, $a \sqsubseteq f(p)$
5. Therefore, $f(p) = a \sqcup f(p)$ and $p = f(p)$, the second condition satisfied
6. Choose q such that $a \sqsubseteq q$ and $q = f(q)$, then $a \sqcap f(q) = q$.
7. Therefore, $q \in postfp(\lambda x.a \sqcup f(x))$.
8. Kanaster-Tarski, $p \sqsubseteq q$, the third condition satisfied

□

Fixed point lattice

Theorem 3.15

Let $f : X \to X$ be a monotonic map on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$. $fp(f)$ forms a complete lattice.

Exercise 3.12

For $S \subseteq fp(f)$, show that $lfp_{\sqcup S}(f)$ exists and is lub of X in poset $(fp(f), \sqsubseteq)$
Hint: use previous theorem

Fixed point compose

Theorem 3.16

Let $(X, \leq)$ and $(Y, \sqsubseteq)$ be complete lattices, and $f : X \to Y$ and $g : Y \to X$ are monotonic then

$$g(lfp(f \circ g)) = lfp(g \circ f)$$

Proof.

1. $(g \circ f)g((lfp(f \circ g))) = g(f \circ g(lfp(f \circ g))) = g(lfp(f \circ g))$
2. Therefore, $g(lfp(f \circ g))$ is a fixed point of $g \circ f$
3. Assume $x = g \circ f(x)$
4. $\Rightarrow f(x) = f \circ g \circ f(x) \Rightarrow f(x) = f \circ g \circ f(x) \Rightarrow f(x) = f \circ g(f(x))$
5. Therefore, by Kanaster-tarski, $lfp(f \circ g) \sqsubseteq f(x)$
6. Since g is monotone, $g(lfp(f \circ g)) \leq g \circ f(x)$
7. Due to 3, $g(lfp(f \circ g)) \leq x$
8. Therefore, $g(lfp(f \circ g))$ is lfp of $g \circ f$

□

Greater function

Theorem 3.17

Let $f, g : X \to X$ *be monotonic maps on a complete lattice* $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$ *such that for all* $x \in X$, $f(x) \sqsubseteq g(x)$ *then*

$$lfp(f) \sqsubseteq lfp(g)$$

Exercise 3.13

Prove the above theorem

Transfinite iterates

Let $f : X \to X$ be an operator on a poset $(X, \sqsubseteq, \sqcap, \sqcup)$.

Definition 3.27

For some ordinal number λ, the upward iterates $(\mathrm{I}^k, k \leq \lambda)$ of f from a is a sequence such that

- $\mathrm{I}^k = a$
- $\mathrm{I}^{k+1} = f(\mathrm{I}^k)$
- $\mathrm{I}^\lambda = \sqcup_{k<\lambda} \mathrm{I}^k$

Definition 3.28

For some ordinal number λ, the downward iterates $(\mathrm{I}^k, k \leq \lambda)$ of f from a is a sequence such that

- $\mathrm{I}^k = a$
- $\mathrm{I}^{k+1} = f(\mathrm{I}^k)$
- $\mathrm{I}^\lambda = \sqcap_{k<\lambda} \mathrm{I}^k$

In poset, $\sqcap$ and $\sqcup$ are partially defined. Consequently, iterates are partially defined. If X is a lattice or cpo then iterates are well-defined.

A condition for finite iterates converging to lfp

Theorem 3.18

If

- $(X, \sqsubseteq, \sqcup, \sqcap)$ *is poset,*
- $f : X \to X$ *is a monotone operator,*
- $a \in prefp(f)$,
- *upward iterates* $(\mathrm{I}^k, k \leq \omega)$ *of* f *from* a *exists, and*
- $\mathrm{I}^\omega \in fp(f)$

then $(\mathrm{I}^k, k \leq \omega)$ *is increasing chain and* $\mathrm{I}^\omega = lfp_a(f)$.

Assumed $\mathrm{I}^\omega \in fp(f)$.
When $\mathrm{I}^\omega \in fp(f)$?

Proof.

1. Since $a \sqsubseteq f(a)$, $\mathrm{I}_0 \sqsubseteq \mathrm{I}_n$
2. Induction hyp, $\mathrm{I}^n \sqsubseteq \mathrm{I}^{n+1}$. Due to monotone f, $f(\mathrm{I}^n) \sqsubseteq f(\mathrm{I}^{n+1}) \Rightarrow \mathrm{I}^{n+1} \sqsubseteq \mathrm{I}^{n+2}$
3. By induction, $\forall n < \omega.\ \mathrm{I}^n \sqsubseteq \mathrm{I}^{n+1}$
4. Since $X^\omega = \sqcup_{k<\omega} \mathrm{I}^k$ and X^ω exists, $\forall n \leq \omega.\ \mathrm{I}^n \sqsubseteq \mathrm{I}^{n+1}$ (proved increasing chain)
5. Since $a = \mathrm{I}_0$, $a \sqsubseteq X^\omega$
6. Assume $a = \mathrm{I}^0 \sqsubseteq x = f(x)$. Since f is monotone, $I^n \sqsubseteq x \Rightarrow \mathrm{I}^{n+1} = f(\mathrm{I}^n) \sqsubseteq f(x) = x$
7. By induction and def. of X^ω, $\forall n \leq \omega. \mathrm{I}^n \sqsubseteq x$. Therefore $X^\omega = lfp_a(f)$

Kleene fixed point theorem

Theorem 3.19

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \to X$ *is upper continuous,*
- $a \in \mathit{prefp}(f)$, *and*
- $(\mathrm{I}^k, k \leq \omega)$ *be upward iterates of* f *from* a

then $\mathrm{I}^\omega = \mathit{lfp}_a(f)$.

Proof.

1. f is continuous $\Rightarrow$ f is monotone $\Rightarrow$ $(\mathrm{I}^k, k \leq \omega)$ increasing chain
2. Since X is cpo, I^ω exists.
3. $f(\mathrm{I}^\omega) = f(\sqcup_{k<\omega} \mathrm{I}^k)$
4. $= \sqcup_{k<\omega} f(\mathrm{I}^k)$, since f is continuous.
5. $= \sqcup_{0<k<\omega} \mathrm{I}^k = a \sqcup_{0<k<\omega} \mathrm{I}^k = \sqcup_{k<\omega} \mathrm{I}^k = \mathrm{I}^\omega$
6. Due to previous theorem, $\mathrm{I}^\omega = \mathit{lfp}_a(f)$

Knaster-Tarski for CPOs

We can prove Knaster-Tarski Theorem like results on cpos.

Theorem 3.20

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \to X$ *is upper continuous, and*
- $a \in \mathit{prefp}(f)$

then $\mathit{lfp}_a(f) = \sqcap\{x \in X | a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$.

Proof.

Let $P = \{x \in X | a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$. Let $(\mathrm{I}^k, k \leq \omega)$ are iterates of f from a.

1. Due to previous theorem, $\mathit{lfp}_a(f) = \mathrm{I}^\omega$. And, $\mathrm{I}^\omega \in P$.
2. Choose x, $a \sqsubseteq x \in P$
3. Induction hyp, $\mathrm{I}^n \leq x \Rightarrow f(\mathrm{I}^n) \leq f(x) \leq x \Rightarrow \mathrm{I}^{n+1} \leq x$
4. By induction, $\forall n < \omega, \mathrm{I}^n \leq x$.
5. By def. of I^ω, $\mathrm{I}^\omega \leq x$
6. Therefore, $\mathit{lfp}_a(f) \sqsubseteq \sqcap P$

Fixed point for monotone functions on cpos

Theorem 3.21

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \to X$ *is monotone function,*
- $a \in \mathit{prefp}(f)$, *and*
- *for some ordinal* λ, $(\mathrm{I}^k, k \leq \lambda)$ *be upward iterates of* f *from* a

then $(\mathrm{I}^k, k \leq \lambda)$ *is increasing chain, which is ultimately stationary and converges to* $\mathit{lfp}_a(f)$.

Monotone is weaker condition than continuous. Therefore, we need larger ordinals

We will skip the proof. However, the length to the stationary point is bounded by the ordinal size of the cpo

Topic 3.6

Asynchronous iterations for fixed points

System of simultaneous fixed point equations

For $i \in 1..n$, $(X_i, \sqsubseteq_i, \bot_i, \top_i, \sqcup_i, \sqcap_i)$ be complete lattices.

Let complete lattice $(X, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ be

- $X = X_1 \times \cdots \times X_n$
- $x \sqsubseteq y = (\wedge_{i=1}^{n} x_i \sqsubseteq_i y_i)$

Let $f : X \times X$ and $f_i : X \times X_i$ be $f_i(X) = (f(X))_i$

The fixed point equation $x = f(x)$ can be written as the following simultaneous fixed point equation.

$$\begin{aligned} x_1 &= f_1(x_1, \ldots, x_n) \\ &\vdots \\ x_n &= f_n(x_1, \ldots, x_n) \end{aligned}$$

Asynchronous iterations

We need not update each component at each iteration. We only need to ensure that each component is updated fairly.

Definition 3.29 (Chaotic iterations)

Let $(J^k, k \in \mathbb{O})$ *be a sequence of subsets of* $[1, n]$*, which is weakly fair, i.e.,*

$$\forall i \in 1..n\, \forall j \in \mathbb{O}.\ \exists k > j.\ i \in J^k$$

The iterates $(\mathrm{I}^k, k < \lambda)$ *starting from* $a \in X$ *for* F *defined by* $(J^k, k \in \mathbb{O})$ *is*

$$\begin{aligned} \mathrm{I}^0 &= a \\ \mathrm{I}_i^k &= f_i(\mathrm{I}^{k-1}) && \text{if } i \in J^k \\ \mathrm{I}_i^k &= \mathrm{I}^{k-1} && \text{if } i \notin J^k \\ \mathrm{I}^\lambda &= \sqcup_{k<\lambda} I^k \end{aligned}$$

Theorem 3.22

$(\mathrm{I}^k, k < \lambda)$ *is increasing chain, ultimately stationary, and limit is* $lfp_a(f)$

Example: asynchronous iterations

- Jacobi iterations: $J^k = [1, n]$
  - update every component in each step
- Gauss-Seidel iterations: $J^k = \{k \ mod \ n\}$
  - update only one component in each step

End of Lecture 3