Organisation der Übungen:

Ausgabe der Zettel: Di-Nacht

Abgabe der Zettel: Di 14^{00}

Zulassungsvoraussetzung:

- 60 % Aufgaben mit "+"
- Vorstellung einer Aufgabe an der Tafel

1.) Verbände und der Satz von Knaster und Tarski

1.1) Verbände in der Programmanalyse

Ziel: Ermittle Menge der Zustände,
die an einem Programmpunkt eingenommen werden
(aufgrund verschiedener Ausführungen).

Ansatz: Vereinigung über alle Zustände,
die von Ausführungen erreicht werden,
die zu diesen Punkt führen.

Beispiel:

```
1: p := 5;
2: q := 2;
3: while (p > q) {
4:    p := p+1;
5:    q := q+2;
   }
6: print p;
```

Es gibt nur eine Ausführung, die Punkt 5 mehrfach erreicht und folgende Zustände erzeugt:

$\{(6,2), (7,4), (8,6)\}$

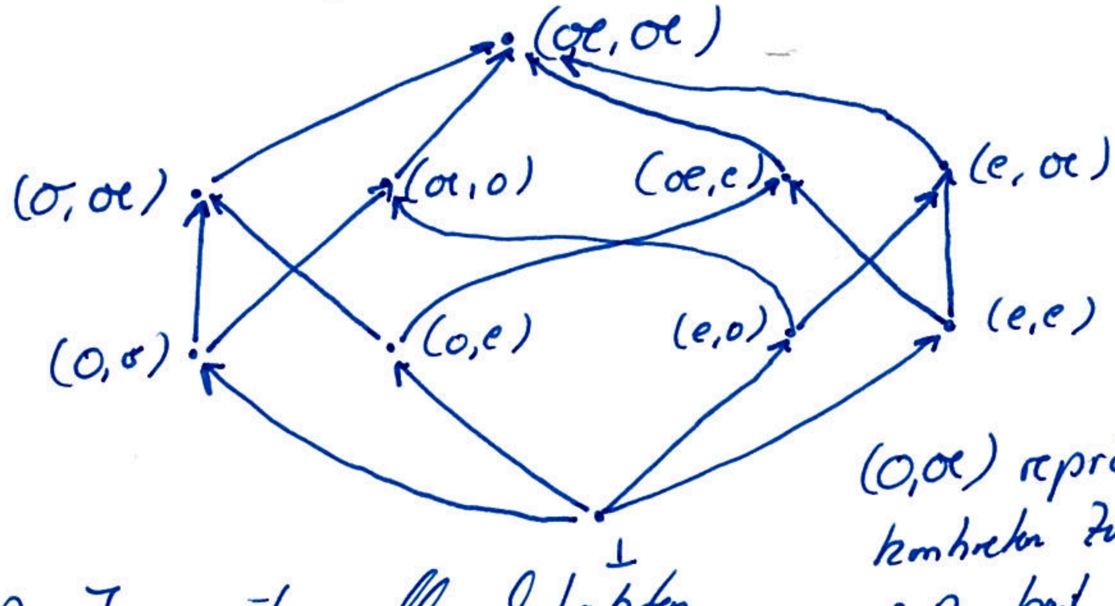
Problem: Vereinigung über alle Zustände nicht berechenbar
(Satz von Rice).

Ansatz: Abstraktion

- Führe das Programm auf abstrakten Zuständen aus, interpretiere die Befehle in der abstrakten Domäne.

- Die konkreten Zustände an einem Punkt werden (neben anderen Zuständen) durch die abstrakten Zustände an diesem Punkt dargestellt.
- Bilde den Join ($\sqcup$) der abstrakten Zustände
  (Join-over-all-paths (JOP)
  (in der Literatur auch Meet-over-all-paths)
- Falls die abstrakten Zustände einen vollständigen Verband bilden, existiert der Join-Zustand.

Am Beispiel:
Vollständiger Verband der abstrakten Werte



(o, oe) repräsentiert alle konkreten Zustände mit
- p hat einen ungeraden Wert
- q hat irgendeinen Wert.

Der Join über alle abstrakten Ausführungen, die zu Punkt 5 führen, ist:

$\perp \sqcup (e,e) = (e,e)$

$(e,e) \sqcup (o,e) = (oe,e)$

$(oe,e) \sqcup (oe,e) = (oe,e)$.

Warum benötigen wir Fixpunkte?
- Anstelle des JOP, berechne Fixpunkt von Funktionen auf dem Verband.

- Unter weiteren Annahmen ist garantiert, dass der Fixpunkt JOP überapproximiert.
- Satz von Knaster-Tarski sagt, wann Fixpunkte existieren und wie sie aussehen.

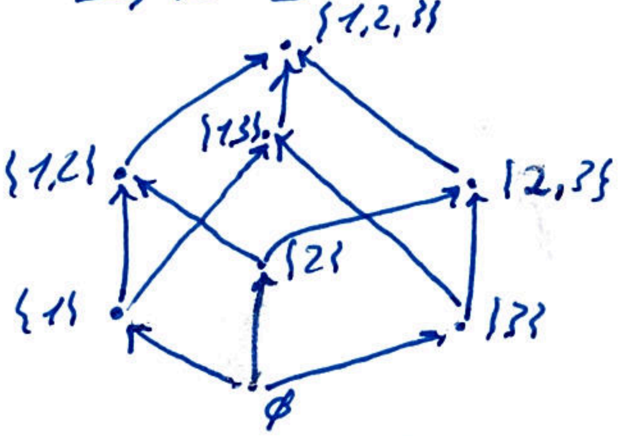
1.2) Partielle Ordnungen und Verbände:

- $(\mathbb{N}, \leq)$ ist <u>total</u> geordnet: jeweils zwei Elemente sind in der Ordnung vergleichbar.
- Einige Domänen sind nur partiell geordnet:

<u>Beispiele</u>:

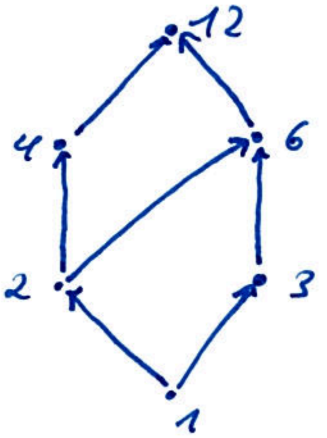
Teilmengen von $\{1,2,3\}$

$\rightarrow \; := \; \subseteq$



$\{1,2\}$ und $\{2,3\}$ sind unvergleichbar

Teiler von 12



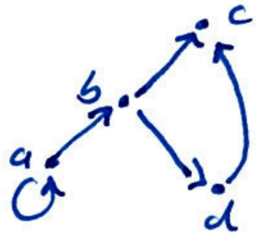
2 und 3 sind unvergleichbar.

<u>Definition (Partielle Ordnung)</u>:

Eine <u>partielle Ordnung</u> $(D, \leq)$ besteht aus
einer Menge $D \neq \emptyset$ und
einer Relation $\leq \subseteq D \times D$ mit folgenden Eigenschaften:

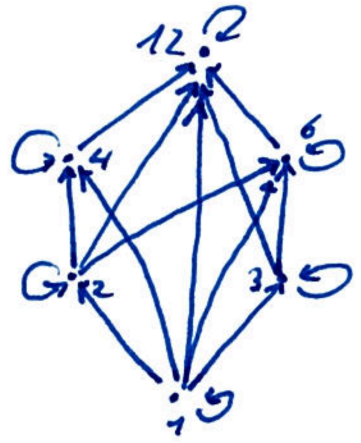
- reflexiv $(\forall d \in D: d \leq d)$
- transitiv $(\forall d, d', d'' \in D: d \leq d' \wedge d' \leq d'' \Rightarrow d \leq d'')$
- anti-symmetrisch $(\forall d, d' \in D: d \leq d' \wedge d' \leq d \Rightarrow d = d')$.

- Binäre Relationen lassen sich als gerichtete Graphen auffassen:

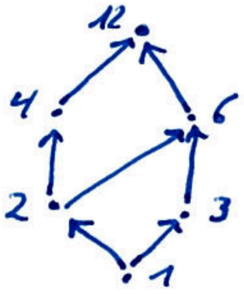
$\{(a,a),\ (a,b),\ (b,c),\ (b,d),\ (d,c)\} =$ 

- Partielle Ordnungen liefern besondere Graphen:
  Reflexivität = Schleifen an Knoten
  Anti-Symmetrie = Keine nicht-trivialen Kreise
  Transitivität = Transitivität der Kanten

  Am Beispiel (Teiler von 12):



Hasse-Diagramm lässt
- Schleifen und
- induzierte Kanten weg.



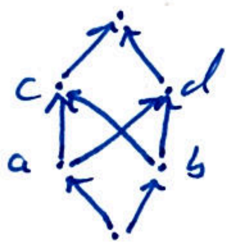
Definition (Join und Meet):

Sei $(D,\leq)$ eine partielle Ordnung.

- Ein Element $o \in D$ heißt obere Schranke einer Menge $X \subseteq D$, falls
  $$x \leq o \quad \text{für alle } x \in X.$$
- Ein Element $o \in D$ heißt kleinste obere Schranke von $X \subseteq D$, auch Join von X genannt, falls
  - o ist obere Schranke und
  - $o \leq o'$ für alle oberen Schranken o' von X.

  Schreibe $o = \sqcup X$
- Analog ist $u = \sqcap X$ die größte untere Schranke, auch Meet von X genannt.

Beispiel:



a und b haben
- c und d als obere Schranken
- aber keine kleinste obere Schranke.

Definition (Verband):

- Ein **Verband** ist eine partielle Ordnung $(D, \sqsubseteq)$ in der für jedes Paar $a, b \in D$ von Elementen Join $a \sqcup b$ und Meet $a \sqcap b$ existieren. Dabei ist $a \sqcup b$ Infixnotation für $\sqcup\{a, b\}$.
- Ein Verband heißt **vollständig**, falls jede Teilmenge $X \subseteq D$ von Elementen Join und Meet hat.

Beispiele:

$a \cdot \quad \cdot b$ = kein Verband

= kein vollständiger Verband.

Lemma:

(1) Ein vollständiger Verband $(D, \sqsubseteq)$ hat ein kleinstes Element

$$\bot := \sqcup \emptyset = \sqcap D.$$

Das kleinste Element ist eindeutig.

(2) Ein vollständiger Verband hat ein eindeutiges größtes Element:

$$\top := \sqcap \emptyset = \sqcup D$$

(3) Jeder endliche Verband $(D, \sqsubseteq)$ (mit D endlich) ist bereits vollständig.

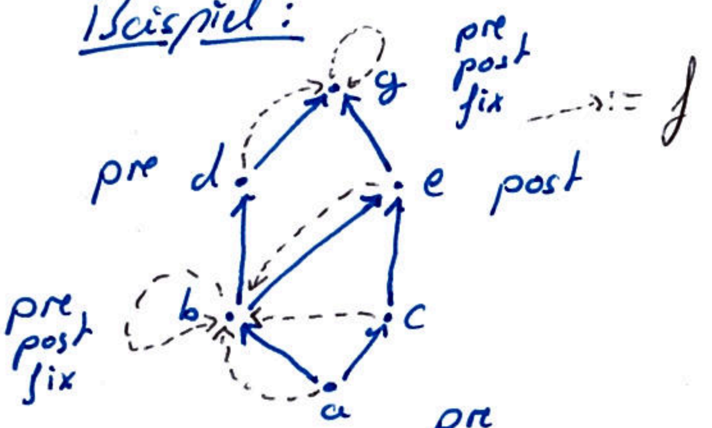
1.3) Monotone Funktionen und der Satz von Knaster und Tarski:

Definition (Monotone Funktionen und Fixpunkte):

Sei $(D,\le)$ eine partielle Ordnung.

- Eine Funktion $f: D \to D$ heißt **monoton**, falls
$$x \le y \quad \text{impliziert} \quad f(x) \le f(y).$$
- Sei $f: D \to D$ eine Funktion auf einer partiellen Ordnung $(D,\le)$.
  - ↳ Ein **Fixpunkt** von f ist ein Element $x \in D$ mit
$$f(x) = x.$$
  - ↳ Ein **Pre-Fixpunkt** von f ist ein Element $x \in D$ mit
$$x \le f(x).$$
  - ↳ Ein **Post-Fixpunkt** von f ist ein Element $x \in D$ mit
$$f(x) \le x.$$

Beispiel:



Satz (Knaster und Tarski '55):

Sei $(D,\le)$ ein vollständiger Verband und $f: D \to D$ monoton.

(i) Dann besitzt f einen **kleinsten** Fixpunkt, gegeben durch
$$lfp(f) := \sqcap \, Postfix(f)$$
(ii) Ferner besitzt f einen **größten** Fixpunkt, gegeben durch
$$gfp(f) := \sqcup \, Prefix(f)$$

Beweis:

Zeige die Behauptung für $lfp(f)$.

Sei
$$l := \sqcap Postfix(f).$$

- Zeige zunächst
$$f(l) \leq l.$$
Da
$$l \leq l' \quad \text{für alle } l' \in Postfix(f)$$
und da f monoton, folgt
$$f(l) \leq f(l') \leq l' \quad \text{für alle } l' \in Postfix(f).$$
Da
$$l = \sqcap Postfix(f)$$
folgt
$$f(l) \leq l. \qquad (*)$$

- Zeige nun
$$l \leq f(l).$$
Mit $(*)$ gilt
$$f(f(l)) \leq f(l).$$
Damit gilt $f(l) \in Postfix(f)$
und so
$$l \leq f(l). \qquad (**).$$
Mit Anti-Symmetrie folgt aus $(*)$ und $(**)$:
$$l = f(l).$$

$\square$