Formale Modellierung 2

Modul 3 (v1.0)

Kanonikvorlesung: Foundations of Computing

Heiko Mantel

MAIS, TU Darmstadt, WS10/11

Übersicht: Modul 3

Beispielmodellierung aus Modul 2 (Wiederholung)

Angemessenheit von formalen Modellen

Alternativen in der Modellierung

- Verwendung von Indexmengen
- Implizite Modellierung von Objekten
- Unterspezifizierte Wertebereiche

Weitere Konzepte zur formalen Modellierung

- Kardinalität
- Disjunkte Vereinigung
- Unendliche Folgen
- Prädikate
- Multimengen
- Partiell geordnete Mengen
- Verbände

Formale Modellierung

Beispiel [aus Kastens, Kleine Büning: Modellierung]

Die EU-Kommission hat beschlossen, die Entscheidungsprozesse der EU mit formalen Methoden zu modellieren. Damit sollen drei Arbeitskreise befasst werden. An der Aktion beteiligen sich zunächst die Nationen Deutschland, Frankreich, Österreich und Spanien. Jede entsendet drei Delegierte. Die Arbeitskreise sollen so gebildet werden, dass in jedem Arbeitskreis jede Nation vertreten ist und dass unter Berücksichtigung der Fremdsprachenkenntnisse der Delegierten es in jedem Arbeitskreis eine gemeinsame Sprache gibt, die alle beherrschen.

In Modul 2 haben Sie gesehen:

- Wie man diesen Sachverhalt formal modellieren kann.
- Wie man systematisch von einer informellen Beschreibung zu einer formalen Modellierung gelangt.

Die Modellierung aus Modul 2

Das formale Modell umfasst:

- Oberbegriffe Nationen, Sprachen, Arbeitskreise und Delegierte
  Wertebereiche: **NATION**, **SPRACHE**, **AKS**, **DEL**
- Potentielle Sprachkenntnisse von Delegierten
  Wertebereich: **SPRACH-MENGE $\subseteq \mathcal{P}$(SPRACHE)**
- Tatsächliche Sprachkenntnisse von Delegierten
  Relation: **SPRACH-KOMPETENZ $\subseteq$ DEL$\times$SPRACHE**
- Nationalität von Delegierten
  Funktion: **nationalität : DEL$\rightarrow$NATION**
- Zuordnung von Delegierten zu Arbeitskreisen
  Funktion: **zuordnung : AKS$\rightarrow\mathcal{P}$(DEL)**
- Hilfsfunktionen
  nationalitäten : AKS$\rightarrow\mathcal{P}$(NATION)
  spricht : DEL$\rightarrow$SPRACH-MENGE
  gemeinsame-sprachen : AKS$\rightarrow$SPRACH-MENGE
- Anforderung: „Jede Nation ist in jedem Arbeitskreis vertreten.“
  Relation: **ANFORDERUNG1 $\subseteq$ AKS$\rightarrow\mathcal{P}$(DEL)**
- Anforderung: „In jedem Arbeitskreis gibt es eine gemeinsame Sprache.“
  Relation: **ANFORDERUNG2 $\subseteq$ AKS$\rightarrow\mathcal{P}$(DEL)**
- Zulässigkeit einer Zuordnung zu Arbeitskreisen
  Relation: **ZULÄSSIG $\subseteq$ AKS$\rightarrow\mathcal{P}$(DEL)**

Angemessenheit

Definition

Ein formales Modell ist für einen realen, informell beschriebenen Sachverhalt **angemessen**, wenn alle Aspekte des Sachverhalts so wiedergeben werden, dass Beobachtungen, die am formalen Modell gemacht werden auch für den realen Sachverhalt gültig sind.

Beachte

Ob ein Modell angemessen ist, hängt auch davon ab,

- wie die Beobachtungen in der Realität interpretiert werden und
- welche Art von Fragestellungen von Interesse sind.

Wie argumentiert man, dass ein Modell angemessen ist?

Die Argumentation stellt einen Zusammenhang zwischen einem formalen Modell und einem informell beschriebenen Sachverhalt her. **Die Argumentation kann nur informell geschehen**, da einer der beiden Bezugspunkte nicht formal beschrieben ist.

Übersicht: Modul 3

Beispielmodellierung aus Modul 2 (Wiederholung)

Angemessenheit von formalen Modellen

Alternativen in der Modellierung

- Verwendung von Indexmengen
- Implizite Modellierung von Objekten
- Unterspezifizierte Wertebereiche

Weitere Konzepte zur formalen Modellierung

- Kardinalität
- Disjunkte Vereinigung
- Unendliche Folgen
- Prädikate
- Multimengen
- Partiell geordnete Mengen
- Verbände

Alternativen in der Modellierung

Beobachtung

Oft gibt es mehr als eine Möglichkeit, eine informelle Beschreibung angemessen zu formalisieren. Allerdings können unterschiedliche Modellierungen auch unterschiedlich angemessen sein.

Plan für den ersten Teil dieses Moduls:

Alternativen zur Modellierung aus Modul 2 entwickeln und untersuchen, ob diese angemessen sind.

Plan für den zweiten Teil des Moduls:

Weitere Konzepte einführen, die zur formalen Modellierung eingesetzt werden können, also Erweiterung unseres Vokabulars an formalen Konzepten.

Verwendung von Indexmengen (1)

Modellierung der Delegierten durch Symbole (aus Modul 2)

- **DEL = { d1, d2, d3, f1, f2, f3, au1, au2, au3, es1, es2, es3 }**

Alternative zur Modellierung

Wir modellieren Delegierte durch Paare anstatt durch Symbole:

- **INDEX = { 1, 2, 3 }**
- **DEL´ = NATION×INDEX**

Delegierte werden somit durch Paare der Form **(n,i)** modelliert.

- Interpretation:
  Das Paar **(d,2)** modelliert z.B. den zweiten deutschen Delegierten.

Angemessenheit der Modellierung

- Jeder der 12 Delegierten wird durch ein Element in DEL´ repräsentiert.
- Jedes Element von DEL´ repräsentiert einen Delegierten.
- Der Wertebereich DEL´ ist also eine angemessene Modellierung der Menge aller Delegierten.

Verwendung von Indexmengen (2)

Konsequenz der Änderung

Die Modellierung anderer Konzepte muss u. U. angepasst werden.

- Zur Modellierung der Sprachkompetenzen der Delegierten verwendet man z.B. statt einer Relation über **DEL×SPRACHE** (SPRACH-KOMPETENZ ⊆ DEL×SPRACHE) eine Relation über **DEL´×SPRACHE** (also über **NATION×INDEX×SPRACHE**).

- Zur Modellierung der Nationalitäten von Delegierten verwendet man z.B. eine Funktion aus dem Funktionenraum **DEL´→NATION** anstatt aus dem Funktionenraum **DEL→NATION**. Diese Funktion kann wie folgt definiert werden: nationalität((n,i)) = n.

- Alle anderen Bestandteile des Modells, bei deren Definition DEL verwendet wird, sind entsprechend anzupassen.

Implizite Modellierung von Objekten (1)

Modellierung der Arbeitskreise durch Symbole (aus Modul 2)

- **AKS = { ak1, ak2, ak3 }**

Alternative zur Modellierung

Wir führen keine Bezeichner für Arbeitskreise ein, sondern modellieren die Arbeitskreise durch Mengen von Delegierten also durch Elemente aus dem Wertebereich **AKS´ = $\mathcal{P}$(DEL)**.

- Die Menge **{ d1, f1, f3, es2 }** modelliert z.B. einen Arbeitskreis mit dem ersten deutschen Delegierten, dem ersten und dritten französischem Delegierten und dem zweiten spanischen Delegierten.
- Die Menge **{ d1, d2, d3 }** modelliert z.B. einen Arbeitskreis, dem alle deutschen Delegierten aber keine Delegierten anderer Nationen zugeordnet sind.
- Die Menge **{ }** modelliert z.B. einen Arbeitskreis, dem gar keine Delegierten zugeordnet sind.

Implizite Modellierung von Objekten (2)

Vorteile und Nachteile der impliziten Modellierung

Vorteil:

- Es müssen keine neuen Symbole eingeführt werden.

Nachteil:

- Sind zwei Arbeitskreisen exakt die gleichen Delegierten zugeordnet, so lassen sich diese Arbeitskreise im Modell nicht unterscheiden, da sie durch die gleiche Menge modelliert werden.

Anpassung der Modellierung

Die Zuordnung von Delegierten zu Arbeitskreisen könnte z.B. durch ein Tripel von Mengen wie folgt modelliert werden:

- **ZUORDNUNG** $\in$ **AKS´** $\times$ **AKS´** $\times$ **AKS´**,
  also **ZUORDNUNG** $\in$ $\mathcal{P}$**(DEL)** $\times$ $\mathcal{P}$**(DEL)** $\times$ $\mathcal{P}$**(DEL)**.

Übung: Argumentiere warum obige Modellierung für das Beispielszenario angemessen ist!

Unterspezifizierte Wertebereiche (1)

Modellierung der Nationen durch Symbole (aus Modul 2)

- **NATION = { d, f, au, es }**

Angemessenheit der Modellierung

- Es gibt Nationen, die nicht durch diese Modellierung erfasst werden.
- **Trotzdem ist die Modellierung angemessen**, da nur die vier modellierten Nationen für das Beispielszenario relevant sind.

Was wäre wenn?

- Eine Anforderung wie z.B. „**Jede Nation der EU ist in jedem Arbeitskreis vertreten**“ gestellt würde.
- **Dann wäre die Modellierung nicht mehr angemessen.**

1. Die Modellierung könnte so angepasst werden, dass **jede Nation der EU durch ein Symbol in der Menge NATION** modelliert wird.
2. Alternativ könnte man die Menge der Nationen unterspezifiziert lassen und z.B. wie folgt definieren
   - **NATION = { d, f, au, es } ∪ WEITERE-NATIONEN**

   wobei die Definition der Menge WEITERE-NATIONEN offen bleibt.

Unterspezifizierte Wertebereiche (2)

Modellierung der Sprachen durch Symbole (aus Modul 2)

- **SPRACHE = { s-d, s-f, s-es }**

Angemessenheit der Modellierung

- Es gibt Sprachen, die nicht durch die Modellierung erfasst werden.
- **Die Modellierung ist nicht angemessen**, wenn manche Delegierte weitere Sprachen sprechen (z.B. Englisch).

1. Die Modellierung könnte so angepasst werden, dass **jede Sprache, die von mindestens einem Delegierten gesprochen wird, durch ein Symbol in der Menge SPRACHE** modelliert wird.
2. Alternativ könnte man die Menge der Sprachen unterspezifiziert lassen und z.B. wie folgt definieren
   - **SPRACHE = {s-d, s-f, s-es } ∪ WEITERE-SPRACHEN**

   wobei die Definition der Menge WEITERE-SPRACHEN offen bleibt.

Unterspezifizierte Wertebereiche (3)

Vorteile und Nachteile der beiden Alternativen

- Um die Menge **SPRACHE** extensional definieren zu können (d.h. durch Aufzählen aller Elemente) muss man **alle** (!) Sprachen kennen, die von einem Delegierten gesprochen werden könnten.
- Die Modellierung durch die Menge
  - **SPRACHE = {s-d, s-f, s-es } ∪ WEITERE-SPRACHEN**

  kann angegeben werden, ohne alle Sprachen zu kennen. Die Definition der Menge **SPRACHE** lässt die Definition der Menge der weiteren Sprachen offen.

Beobachtung

Man kann Oberbegriffe formal modellieren, ohne die Instanzen des Oberbegriffs zu kennen. Dazu führt man eine Menge ein, ohne zu definieren, welche Elemente die Menge enthält.

Übersicht: Modul 3

Beispielmodellierung aus Modul 2 (Wiederholung)

Angemessenheit von formalen Modellen

Alternativen in der Modellierung

- Verwendung von Indexmengen
- Implizite Modellierung von Objekten
- Unterspezifizierte Wertebereiche

Weitere Konzepte zur formalen Modellierung

- Kardinalität
- Disjunkte Vereinigung
- Unendliche Folgen
- Prädikate
- Multimengen
- Partiell geordnete Mengen
- Verbände

Kardinalität (1)

Definition

Die **Kardinalität** einer endlichen Menge M ist die Anzahl ihrer Elemente. Man schreibt **|M|** für die Kardinalität der Menge M.

Beobachtungen

- Für die Vereinigung, Schnittmenge und Differenz von zwei endlichen Mengen M und N gilt:
  - **$|M| \leq |M \cup N|$, $|N| \leq |M \cup N|$, $|M \cup N| \leq |M|+|N|$**
  - **$|M \cap N| \leq |M|$, $|M \cap N| \leq |N|$**
  - **$|M|-|N| \leq |M \setminus N| \leq |M|$**
- Für das kartesische Produkt gilt:
  - **$|M \times N| = |M|*|N|$**
- Für die Potenzmengenkonstruktion gilt:
  - **$|\mathcal{P}(M)| = 2^{|M|}$**
- Unabhängig von der Kardinalität einer nicht leeren Menge M, haben die Mengen M^+ und M^* unendlich viele Objekte.

Kardinalität (2)

Beobachtung

- Für die Kardinalität von Funktionenräumen gilt
  - $|D \rightarrow B| = (|B|+1)^{|D|}$

Beispiel

In Modul 2 wurden die Sprachkenntnisse der Delegierten zunächst durch eine Relation $\text{SPRACH-KOMPETENZ} \subseteq \text{DEL} \times \text{SPRACHE}$ modelliert. Bei der Modellierung der Anforderungen wurden die Fremdsprachenkenntnisse zusätzlich durch eine Funktion $\text{spricht} : \text{DEL} \rightarrow \mathcal{P}(\text{SPRACHE})$ modelliert.

- Für die Menge aller Relationen SPRACH-KOMPETENZ gilt
  - $|\mathcal{P}(\text{DEL} \times \text{SPRACHE})| = 2^{(12 * 3)} = (2^3)^{12} = 8^{12}$.
- Für die Menge aller Funktionen $\text{DEL} \rightarrow \mathcal{P}(\text{SPRACHE})$ gilt
  - $|\text{DEL} \rightarrow \mathcal{P}(\text{SPRACHE})| = (2^3+1)^{12} = 9^{12}$.

Übung: Warum unterscheidet sich die Kardinalität der beiden Wertebereiche, obwohl beide dasselbe modellieren?

Disjunkte Vereinigung (1)

Definition

Sei I:={ 1, …, n } eine Indexmenge mit n>1. Dann ist die **disjunkte Vereinigung** von Mengen W_1, …, W_n wie folgt definiert:

- $W_1 \uplus \ldots \uplus W_n = \{ (i,w) \mid i \in I \text{ und } w \in W_i \}$.

Beispiel

Auf Folie 8 wurde die Menge der Delegierten wie folgt definiert:

- **INDEX = { 1, 2, 3 }**
- **DEL´ = NATION×INDEX**

Man kann die Menge auch mit disjunkter Vereinigung modellieren:

- **DEL´´ = INDEX ⊎ INDEX ⊎ INDEX ⊎ INDEX**

Allerdings muss man jetzt explizit angeben, welches Element der Indexmenge welcher Nation entspricht. Z.B. könnte man festlegen, dass **deutsche Delegierte** durch Paare der Form **(1,j)**, **franz. Delegierte** durch Paare der Form **(2,j)**, **österreichische Delegierte** durch Paare der Form **(3,j)** und **spanische Delegierte** durch Paare der Form **(4,j)** modelliert werden (wobei j∈INDEX).

Disjunkte Vereinigung (2)

Beispiel

Die disjunkte Vereinigung erlaubt auch die Modellierung unterschiedlicher Aspekte. Während man anhand der Vereinigung der beiden Mengen

- **Kunde = { Benteler, Siemens, VW }**
- **Lieferant = { Orga, Siemens }**

also der Menge

- **Kunde ∪ Lieferant = { Benteler, Orga, Siemens, VW }**

nicht mehr erkennen kann, ob ein Element Kunde oder Lieferant ist, kann man den Elementen der disjunkten Vereinigung

- **Kunde ⊎ Lieferant =**

  { (1,Benteler), (1,Siemens), (1,VW), (2,Orga), (2,Siemens) }

diese Information entnehmen.

Unendliche Folgen (1)

Definitionen [aus Modul 2]

Die **Menge aller nicht leeren, endlichen Folgen über einer Menge M** ist die wie folgt definierte Menge $M^+ = \cup_{i \in \mathbb{N}, i>0} M^i$.

Die **Menge aller endlichen Folgen über M** ist die Menge $M^* = M^+ \cup \{()\}$.

Alternative Definition von endlichen Folgen

Nach obigen Definitionen wird eine Folge über M der Länge n durch ein Tupel t mit n Elementen aus M repräsentiert. Alternativ könnte man eine solche Folge durch eine Funktion f aus dem Funktionenraum $\{ 1, \ldots, n \} \rightarrow M$ repräsentieren, wobei **der Wert der Funktion f an der Stelle $i \in \{1, \ldots, n\}$ das i´te Element des Tupels t ist, d.h. $f(i)=t_i$** .

Definition

Die **Menge aller unendlichen Folgen über M** ist die Menge $M^\infty: \mathbb{N} \rightarrow M$.

Eine unendliche Folge wird also repräsentiert durch eine Funktion mit den natürlichen Zahlen als Definitionsbereich.

Unendliche Folgen (2)

Modellierung von Systemverhalten

Sowohl endliche als auch unendliche Folgen können zur Modellierung von Systemverhalten eingesetzt werden. Die Folge

(sende(42), transportiere(42), empfange(42), addiere(42,1))

könnte z.B. eingesetzt werden, um die Kommunikation einer Nachricht mit dem Wert **42** und eine anschließende Addition zu modellieren.

Interpretation von endlichen Folgen

Die obige Folge kann unterschiedlich interpretiert werden:

- Es passieren die vier angegebenen Aktionen, weitere können folgen.
- Es passieren die vier angegebenen Aktionen und das System stoppt.

Verwendung von unendlichen Folgen in der Modellierung

Mit unendlichen Folgen können die möglichen Verhalten von Systemen beschrieben werden, die nicht immer terminieren.

Wie modelliert man terminierende Verhalten mit unendlichen Folgen?

Prädikate (1)

Definition

Ein **Prädikat über einer Menge** M ist eine Funktion p: M→Bool, also eine totale Funktion mit den booleschen Werten als Bildbereich (Bool = { w,f }).

Beobachtung

Es gibt eine enge Beziehung zwischen Prädikaten und Mengen:

- Die **charakteristische Funktion** einer Teilmenge $K \subseteq M$ ist das wie folgt definierte Prädikat über M:
  - $\chi(m) = w$ falls $m \in K$ gilt und
  - $\chi(m) = f$ falls $m \notin K$ gilt.
- Ein Prädikat p: M→Bool induziert zwei Mengen:
  - Die Menge aller Elemente aus M für die p wahr ist:
    $W_p = \{ m \in M \mid p(m) = w \}$.
  - Die Menge aller Elemente aus M für die p falsch ist:
    $F_p = \{ m \in M \mid p(m) = f \}$.

Prädikate (2)

Beispiel

Wir modellieren, ob ein gegebener Delegierter einem gegebenen Arbeitskreis zugeordnet wurde, indem wir ein Prädikat **ist-zugeordnet** über der Menge **DEL×AKS** wie folgt definieren:

- **ist-zugeordnet(v,ak) = w**
  genau dann wenn v∈ zuordnung(ak)
- **ist-zugeordnet(v,ak) = f**
  genau dann wenn v∉ zuordnung(ak).

Multimengen

Definition

Eine **Multimenge über einer Menge M** ist eine Funktion m: M→ℕ, also eine totale Funktion mit den natürlichen Zahlen als Bildbereich.

Verwendung von Multimengen

Multimengen eignen sich, um Ressourcen zu modellieren.

Beispiel

Einen Vorrat von 200 Bausteinen kann man z.B. durch die Funktion aus dem Funktionenraum **{stein}→ℕ** modellieren, die dem Symbol **stein** die Zahl **200** zuordnet.

Partiell Geordnete Mengen (1)

Definition (aus Modul 2)

Eine zweistellige Relation $R \subseteq M \times M$ heißt **Ordnung** (oder auch **partielle Ordnung**) wenn sie reflexiv, antisymmetrisch und transitiv ist.

Definition (aus Modul 2)

Eine zweistellige Relation $R \subseteq M \times M$ heißt **totale Ordnung** (oder auch **lineare Ordnung**) wenn sie alternativ, reflexiv, antisymmetrisch und transitiv ist.

Definition

Eine **partiell geordnete Menge** ist ein Paar $(M,\leq)$, wobei

- M eine Menge ist, die Trägermenge genannt wird, und
- $\leq \subseteq M \times M$ eine partielle Ordnung ist.

Eine **geordnete Menge** ist eine partiell geordnete Menge $(M,\leq)$, wobei $\leq \subseteq M \times M$ eine totale Ordnung ist.

Partiell Geordnete Mengen (2)

Visualisierung

Partiell geordnete Mengen können durch **Hasse Diagramme** als Graph visualisiert werden. Das Hasse Diagramm für eine partiell geordnete Menge $(M,\leq)$ zeichnet man wie folgt:

- **Jedes $m \in M$ wird durch einen Knoten im Graph repräsentiert.**
- **Wenn $m1 \leq m2$ für zwei Knoten $m1,m2 \in M$ gilt, dann**
  - **zeichnet man den Knoten für $m2$ oberhalb des Knotens für $m1$ und,**
  - **falls es kein $m \in M$ mit $m1 \leq m \leq m2$, $m \neq m1$ und $\neq m2$ gibt, dann verbindet man die Knoten $m1$ und $m2$ mit einer Kante.**

Partiell Geordnete Mengen (3)

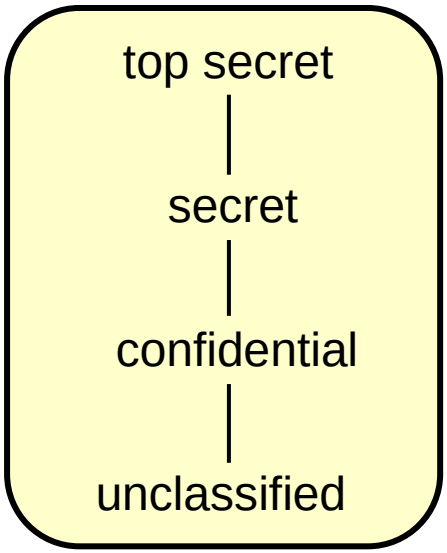
Beispiel

Partielle Ordnungen können zur Modellierung von Sicherheitspolitiken eingesetzt werden. Die partiell geordnete Menge

- **MILITARY = ({unclassified, confidential, secret, top secret}, ≤)**

wird im Bereich der nationalen Sicherheit verwendet, wobei ≤ als die kleinste Relation definiert ist, für die folgendes gilt:

- unclassified ≤ unclassified,
  unclassified ≤ confidential,
  unclassified ≤ secret,
  unclassified ≤ top secret,
- confidential ≤ confidential,
  confidential ≤ secret,
  confidential ≤ top secret,
- secret ≤ secret,
  secret ≤ top secret und
- top secret ≤ top secret



Hasse Diagramm

Partiell Geordnete Mengen (4)

Beispiel (Fortsetzung)

Die Ordnung **MILITARY** drückt Anforderungen an die Vertraulichkeit von Informationen aus.

Wie setzt man MILITARY in einem konkreten Szenario ein?

- Identifiziere alle zu schützenden Objekte im Szenario
  - **Objekte** sind passive Dinge, z.B. Programmvariablen oder Dateien.
- Identifiziere alle Subjekte, die auf Objekte zugreifen könnten
  - **Subjekte** sind aktive Dinge, z.B. Benutzer oder Prozesse.
- Ordne jedem Objekt und jedem Subjekt eine **Sicherheitsstufe** aus
  - {unclassified, confidential, secret, top secret} zu.

Was bedeutet MILITARY in einem konkreten Szenario?

- Ein Subjekt s darf ein Objekt o nur dann lesen, wenn die Sicherheitsstufe von s größer oder gleich der Sicherheitsstufe von o ist.

Andere Auslegungen sind möglich

- **siehe Vorlesung Formal Methods for Information Security (4+2)**

Partiell Geordnete Mengen (5)

Beispiel

Eine weitere typische Sicherheitspolitik aus dem Bereich der nationalen Sicherheit lässt sich wie folgt modellieren:

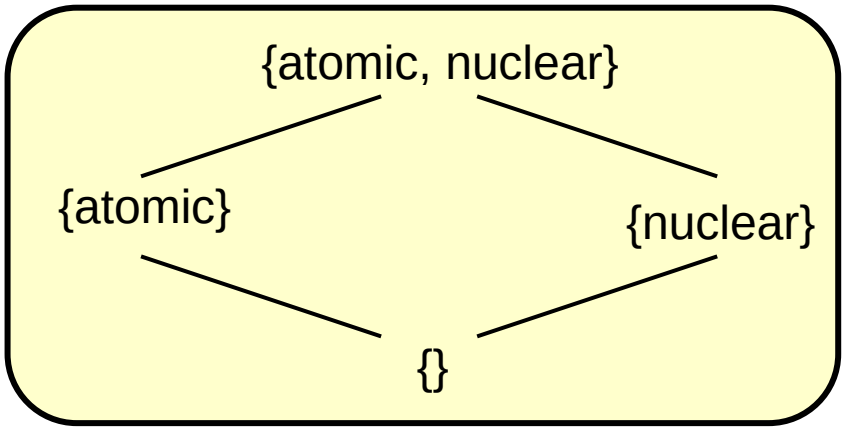
COMPARTMENT = ({{}, {atomic}, {nuclear}, {atomic, nuclear}}, ⊆)

wobei ⊆ als die kleinste Relation definiert ist, für die gilt:

- {} ⊆ {},
  {} ⊆ {atomic},
  {} ⊆ {nuclear},
  {} ⊆ {atomic, nuclear},
- {atomic} ⊆ {atomic},
  {atomic} ⊆ {atomic, nuclear},
- {nuclear} ⊆ {nuclear},
  {nuclear} ⊆ {atomic, nuclear}

und

- {atomic, nuclear}
  ⊆ {atomic, nuclear}.



Hasse Diagramm

Partiell Geordnete Mengen (6)

Beispiel (Fortsetzung)

Die Ordnung **COMPARTMENT** drückt Anforderungen an die Vertraulichkeit von Informationen aus.

Wie setzt man COMPARTMENT in einem konkreten Szenario ein?

- Identifiziere alle zu schützenden Objekte im Szenario.
- Identifiziere alle Subjekte, die auf Objekte zugreifen könnten.
- Ordne jedem Objekt und jedem Subjekt Abteilungen aus der Menge
  - {atomic, nuclear}

  zu.

Was bedeutet COMPARTMENT in einem konkreten Szenario?

- Ein Subjekt s darf nur dann ein Objekt o lesen, wenn s allen Abteilungen zugeordnet ist, denen o zugeordnet ist.

Mehrstufige Sicherheit

Begriff

Sicherheitspolitiken, die sich durch geordnete Mengen wie z.B. **MILITARY** oder **COMPARTMENT** ausdrücken lassen, werden als **mehrstufige Sicherheitspolitiken** bezeichnet.

Typische Fragestellungen

- Welche Sicherheitsstufe muss ein Subjekt mindestens haben, um zwei gegebene Objekte lesen zu dürfen?
- Welche Sicherheitsstufe darf ein Objekt höchstens haben, damit es von zwei gegebenen Subjekten gelesen werden darf?

Wie modelliert man mehrstufige Sicherheit, wenn solche Fragen beantwortet werden sollen?

- **Man verwendet Verbände.**

Obere und Untere Schranken

Definition

Sei $(M,\leq)$ eine geordnete Menge.

- Eine Funktion $\sqcup : M \times M \rightarrow M$ heißt **Vereinigungsoperator** gdw.

  $m1 \sqcup m2$ die **kleinste obere Schranke** für $m1, m2 \in M$ ist, d.h.

  - $m1 \leq (m1 \sqcup m2)$ und $m2 \leq (m1 \sqcup m2)$
  - $m1 \leq m \wedge m2 \leq m \Rightarrow (m1 \sqcup m2) \leq m$ für alle $m \in M$

- Eine Funktion $\sqcap : M \times M \rightarrow M$ heißt **Schnittoperator** gdw.

  $m1 \sqcap m2$ die **größte untere Schranke** für $m1, m2 \in M$ ist, d.h.

  - $(m1 \sqcap m2) \leq m1$ und $(m1 \sqcap m2) \leq m2$
  - $m \leq m1 \wedge m \leq m2 \Rightarrow m \leq (m1 \sqcap m2)$ für alle $m \in M$

Verbände

Definition

Ein **Verband** ist ein Tupel **$(M,\leq,\sqcup,\sqcap)$** so dass

- $(M,\leq)$ eine geordnete Menge ist;
- $\sqcup$ ein Vereinigungsoperator auf $(M,\leq)$ ist; und
- $\sqcap$ ein Schnittoperator auf $(M,\leq)$ ist;

Typische Fragestellungen (wie zuvor)

- Welche Sicherheitsstufe muss ein Subjekt mindestens haben, um zwei gegebene Objekte lesen zu dürfen?
- Welche Sicherheitsstufe darf ein Objekt höchstens haben, damit es von zwei gegebenen Subjekten gelesen werden darf?

Diese Fragen können mit Hilfe der Operatoren $\sqcup$ und $\sqcap$ beantwortet werden.

Rückblick auf Modul 3

Einige wesentliche Lernziele dieses Moduls

- Wann ist ein formales Modell angemessen?
  - Es kann mehr als eine angemessene Modellierung geben.
  - Man muss üben, um sich im Lösungsraum zurecht zu finden.
- Erweiterung des Wortschatzes an formalen Konzepten
  - Wie kann ich die weiteren Konzepte zur formalen Modellierung von informell beschriebenen Sachverhalten verwenden.

Literatur

Uwe Kastens, Hans Kleine Büning

Modellierung – Grundlagen und formale Methoden; Kapitel 2
Hanser Verlag, 2008, 2. Auflage (oder 1. Auflage von 2005).