Übungen Interaktives Spezifizieren und Verifizieren

Die mit ⋆ gekennzeichneten Übungen sind für „Experten“.

A Erste Begegnung mit Alloy

1. Verschönerung von diehard

Verwenden Sie die am Beispiel des Echo-Algorithmus vorgestellte Mimik, um das Beispiel von „diehard“ so zu erweitern, dass nicht nur der Ablauf angezeigt wird, sondern jeweils auch welche Transition ausgeführt wird.

B Spezifikation struktureller Eigenschaften

2. Verwandtschaftsverhältnisse

Starten Sie mit folgender Spezifikation:

```
abstract sig Person {
  children: set Person,
  siblings: set Person
}

sig Man, Woman extends Person {}

sig Married in Person {
  spouse: one Married
}
```

(a) Erzeugen Sie Modelle zu dieser Spezifikation und überlegen Sie welche merkwürdigen Fälle auftreten können.

(b) Erweitern Sie die Spezifikation um solche Fälle auszuschließen.

(c) Formulieren Sie Annahmen und überprüfen Sie sie für folgende Punkte

- Es kann nicht sein, dass ein Elternteil einer Person gleichzeitig ein Geschwister ist.
- Wenn eine andere Person eine Geschwister ist, dann ist dies auch umgekehrt der Fall.
- Verheiratete Personen haben keinen gemeinsamen Vorfahr.

3. Generalisierung/Spezialisierung in der Unified Modeling Language UML

In der Spezifikation der Unified Modeling Language werden für Generalisierungen bzw. Spezialisierungen in Table 9.1 Integritätsbedingungen definiert:

`{complete, disjoint}`: Indicates the generalization set is covering and its specific Classifiers have no common instances.

`{incomplete, disjoint}`: Indicates the generalization set is not covering and its specific Classifiers have no common instances.

`{complete, overlapping}`: Indicates the generalization set is covering and its specific Classifiers do share common instances.

`{incomplete, overlapping}`: Indicates the generalization set is not covering and its specific Classifiers do share common instances.

Spezifizieren Sie in Alloy Beispiele für die vier Möglichkeiten.

4. Eigenschaften binärer Relationen

Gegeben sei eine Relation $r \subseteq A \times B$ (in Alloy: `r in A -> B`).

Man sagt

(a) die Relation ist *injektiv*, wenn zwei Elemente von A niemals dasselbe Element von B zugeordnet haben.

(b) die Relation ist *surjektiv*, wenn jedes Element von B mindestens einem Element von A zugeordnet ist.

(c) die Relation ist eine *partielle Funktion*, wenn jedes Element von A höchstens einem Element von B zugeordnet ist.

(d) die Relation ist *total*, wenn jedes Element von A mindestens einem Element von B zugeordnet ist.

(e) die Relation ist einen (totale) *Funktion*, wenn jedes Element von A genau einem Element von B zugeordnet ist.

(f) die Relation ist eine *Darstellung*, wenn sie partiell und injektiv ist.

(g) die Relation ist eine *Abstraktion*, wenn sie partiell und surjektiv ist.

(h) die Relation ist eine *Injektion*, wenn sie eine Funktion und injektiv ist.

(i) die Relation ist eine *Surjektion*, wenn sie eine Funktion und surjektiv ist.

(j) die Relation ist eine *Bijektion*, wenn sie eine Injektion und eine Surjektion ist.

Drücken Sie diese Eigenschaften durch *Multiplizitäten* in Alloy aus.

5. Hochschule

Entwerfen Sie eine Spezifikation der Situation an einer Hochschule, die folgende Gegebenheiten berücksichtigt:

- Es gibt Professoren, Dozenten und Studenten. Studenten sind entweder Bachelorstudenten oder Masterstudenten. Dozenten sind Professoren oder Masterstudenten. Studenten haben eine eindeutige Matrikelnummer und sind in einem Fachbereich eingeschrieben.
- Professoren betreuen Studenten.
- Studenten haben Kurse absolviert.
- Kurse werden von jeweils einem Dozenten angeboten. Kurse haben andere Kurse als Voraussetzung. In einen Kurs sind Studenten eingeschrieben, andere Studenten sind auf der Warteliste für den Kurs.
- Fachbereiche bieten Kurse an, von denen einige Pflichtkurse sind.
- Alle Dozenten sind Profs oder Masterstudenten.
- Jeder Fachbereich hat mindestens einen Dozenten.
- Pflichtkurse werden nur von Profs angeboten.
- Wenn kein Student in einen Kurs eingeschrieben ist, ist die Warteliste leer.
- Ein Student ist nicht zugleich eingeschrieben und auf der Warteliste sein.
- Ein Master kann nur Dozent eines Kurses sein, zu dem er sich nicht angemeldet hat.

- Es gibt keinen Zyklus bei den Voraussetzungen eines Kurses.
- Ein Student kann sich nur zu einem Kurs anmelden, dessen Voraussetzungen er hat.
- Der Mentor eines Masterstudenten betreut ihn auch.

Überprüfen Sie folgende Annahmen und korrigieren Sie ggfs. die Spezifikation:

- Ein Stuudent muss in mindestens einem Pflichtkurs eingeschrieben sein.
- Ein Student hat alle vorausgesetzten Kurse seiner absolvierten Kurse absolviert.
- Kein Dozent ist auf der Warteliste eines der Kurse, die er anbietet

Welche weiteren Integritätsbedingungen könnte man formulieren?

6. Erdkunde-Klassenarbeit

Logelei aus dem ZEIT-Magazin vom 24.05.2007

> Claudia musste für den Erdkundeunterricht vier Berge auswendig lernen. Am nächsten Tag in der Klassenarbeit kann sie sich noch an Folgendes erinnern:
> Auf dem Felderer findet sich kein Steinhaufen.
> Der Berg in Barunien heißt weder Schneehorn, noch ist er 2317 Meter hoch.
> Auf einem der Berge war ein gigantischer Felsen.
> Weder der Berg in Gorabien noch der Felderer ist 2581 Meter hoch.
> Der Berg in Seborien ist 2128 Meter hoch.
> Das Schneehorn ist nicht 2222 Meter hoch.
> Der Berg mit der Hütte darauf ist weder 2222 Meter hoch noch der Borken, noch in Seborien.
> Der Berg in Gorabien ist nicht 2317 Meter hoch.
> Weder auf dem 2222 Meter hohen Berg noch auf dem Borken gibt es einen See. Es gab einen Weldberg.
> Claudia grübelt und grübelt, aber mehr will ihr partout nicht einfallen. Da fällt ihr auf, dass die Tafel nicht geputzt ist. Dort steht noch, wohl von einem Erdkundeunterricht der Parallelklasse: „In Lusanien steht der Borken“.
> Claudia ist erleichtert.
> Wie heißen die vier Berge, wie hoch sind sie, in welchem Land sind sie, und welche Besonderheit findet man auf den vier Gipfeln?

Man kann die Frage noch erweitern: Gibt es nur eine Lösung? Gibt es mehrere Lösungen, wenn die Tafel geputzt gewesen wäre?

7. Das Zebra-Rätsel

Folgendes Rätsel (siehe Wikipedia) wird Einstein zugeschrieben, obwohl es keinerlei Hinweis darauf gibt, dass Einstein etwas damit zu tun hat.

Es geht so:

1 Es gibt fünf Häuser.

2 Der Engländer wohnt im roten Haus.

3 Der Spanier hat einen Hund.

4 Kaffee wird im grünen Haus getrunken.

5 Der Ukrainer trinkt Tee.

6 Das grüne Haus ist direkt links vom weißen Haus.

7 Der Raucher von Old-Gold-Zigaretten hält Schnecken als Haustiere.

8 Die Zigaretten der Marke Kools werden im gelben Haus geraucht.

9 Milch wird im mittleren Haus getrunken.

10 Der Norweger wohnt im ersten Haus.

11 Der Mann, der Chesterfields raucht, wohnt neben dem Mann mit dem Fuchs.

12 Die Marke Kools wird geraucht im Haus neben dem Haus mit dem Pferd.

13 Der Lucky-Strike-Raucher trinkt am liebsten Orangensaft.

14 Der Japaner raucht Zigaretten der Marke Parliaments.

15 Der Norweger wohnt neben dem blauen Haus.

16 Der Chesterfields-Raucher hat einen Nachbarn, der Wasser trinkt.

Dabei setzen wir voraus, dass jedes Haus genau eine der möglichen Eigenschaften hat und dass das verbleibendw Haustier das Zebra ist.

Die Frage ist dann:

„Wer trinkt Wasser und wem gehört das Zebra?“

Lösen Sie das Rätsel mit Alloy.

8. Das Damenproblem

Das Damenproblem besteht darin, n (üblicherweise 8) Damen so auf einem Schachbrett aufzustellen, dass sie sich nicht gegenseitig schlagen können.

Formulieren Sie das Damenproblem in Alloy und generieren Sie Lösungen dafür.

Hinweis: Wenn man in Alloy `Int` verwendet, dann muss man beachten, dass ganze Zahlen in Alloy explizit als Atome im untersuchten Universum erzeutg werden und zwar soviele wie die Anzahl der verwendeten Bits (`Bitwidth`) angibt. Bei arithmetischen Operationen mit `Int`s muss man beachten, dass `Int` *einstellige Relationen* sind und nicht *Zahlen*, siehe https://alloy.readthedocs.io/en/latest/modules/integer.html.

9. Kartenfärbungen

Planare Karten sollen so gefärbt werden, dass zwei benachbarte Länder nicht diesselbe Farbe haben.

(a) Erstellen Sie eine Spezifikation für Kartenfärbungen und lassen Sie den Alloy Analyzer beispielhafte Konfigurationen konstruieren.

(b) Zeigen Sie mittels dieser Spezifikation, dass die Karte der Staaten und Territorien Australiens mit drei Farben gefärbt werden kann.

(c) Geben Sie eine Konfiguration vor, bei der vier Farben erforderlich sind.

(d) Könnte es eine Karte geben, bei der man mehr als vier Farben benötigt?

10. Formeln der Aussagenlogik

Gesucht ist eine Alloy-Spezifikation, die Formeln der Aussagenlogik spezifiziert. Wir wollen voraussetzen, dass wir unsere Sprache der Aussagenlogik die Operatoren `Not`, `And`, `Or` sowie `Impl` hat.

11. Erfüllbare Formeln der Aussagenlogik

Erweitern Sie die Spezifikation der vorherigen Aufgabe so, dass nur erfüllbare Formeln erzeugt werden.

Hinweis: Das Modul `util/boolean` könnte hilfreich sein.

12. ⋆ Natürliches Schließen in der Aussagenlogik

Ausgehend von der Spezifikation von Formeln der Aussagenlogik ist es möglich, das natürliche Schließen in der Aussagenlogik in Alloy zu spezifizieren. Was ist zu tun?

(a) Man muss die Regeln des natürlichen Schließens als Prädikate formulieren.

(b) Für die Herleitung muss man eine rekursive Struktur vorsehen, deren Knoten jeweils einen Schritt der Herleitung beschreiben mit

- Verwendeter Regel,
- Voraussetzungen,
- Folgerung, und
- den verwendeten Teil-Herleitungen.

13. Gruppen

Eine Gruppe G ist ein Tupel $(G, *, 1)$ bestehend aus einer Menge von Elementen G, einer Funktion $* : G \times G \to G$ und einem ausgezeichneten Element $1 \in G$, so dass gilt:

(1) Inverse Elemente: zu jedem $x \in G$ gibt es ein $y \in G$ so dass gilt: $x * y = y * x = 1$

(2) Assoziativgesetz: für alle $x, y, z \in G$ gilt: $x * (y * z) = (x * y) * z$

(3) Neutrales Element: für alle $x \in G$ gilt: $1 * x = x * 1 = x$.

(a) Spezifizieren Sie die Struktur einer Gruppe in Alloy.

(b) Lassen Sie den Alloy Analyzer eine Gruppe mit drei Elementen generieren.

(c) Überprüfen Sie die Aussage, dass jedes Element einer Gruppe ein *eindeutiges* inverses Element hat mittels des Alloy Analyzers.

(d) Schreiben Sie eine `assert`-Anweisung zur Überprüfung, ob eine Gruppe *kommutativ* ist, d.h. ob für alle $x, y \in G$ gilt: $x * y = y * x$. Überprüfen Sie die Anweisung mit steigendem *Scope* beginnend bei 1.

14. Projektive Ebenen

Eine projektive Ebene ist eine Menge von Punkten und Geraden mit folgenden Eigenschaften:

(1) Zu je zwei verschiedenen Punkten gibt es genau eine Gerade, auf der die Punkte liegen.

(2) Zu je zwei verschiedenen Geraden gibt es genau einen Punkt, in dem sich die Geraden schneiden.

(3) Auf jeder Geraden liegen wenigstens 3 Punkte.

(4) Durch jeden Punkt gehen mindestens 3 Geraden.

- Spezifizieren Sie die Struktur einer (endlichen) projektiven Ebene in Alloy.
- Zeigen Sie mit Alloy, dass die kleinste endliche projektive Ebene 7 Punkte und 7 Geraden hat.

15. Königsberger Brücken

Die Stadt Königsberg wird durch den Fluss Pregel mit seinen beiden Inseln geteilt. Die beiden Stadthälften sind durch je drei Brücken mit den Inseln verbunden. Die Inseln sind untereinander durch eine weitere Brücke verbunden, wie in Abb. 1 dargestellt.

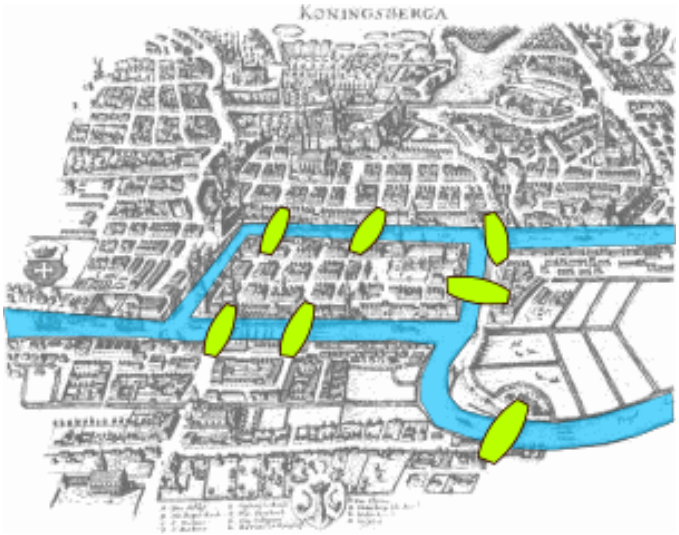

Abbildung 1: Königsberger Brücken

Leonhard Euler bewies, dass es keinen Weg gibt, auf dem man alle sieben Brücken genau einmal überquert.

Sein Argument geht so: Zu jedem Gebiet gibt es eine ungerade Zahl von Brücken. Damit es einen Weg gibt, der alle Brücken genau einmal überquert, dürfte es maximal 2 Gebiete mit einer ungeraden Anzahl von Brücken geben, nämlich das, wo der Weg beginnt und das, wo er endet. Die anderen Gebiete müssten eine gerade Anzahl von Brücken haben, weil man ja auf zwei verschiedenen Brücken das Gebiet betreten und wieder verlassen muss.

Wie kann man das Problem in Alloy formulieren und dann zeigen, dass ein „Eulerscher“ Weg nicht existiert?

C Spezifikation von Dynamik

16. Uhr in Alloy

Spezifizieren Sie ein Uhr, die die Stunden 1 bis 12 anzeigen kann und lassen Sie sie laufen.

17. Flussüberquerungsrätsel

Ein Bauer steht mit einem Wolf, einer Ziege und einem Kohlkopf auf einer Seite eines Flusses und möchte auf die andere Seite mit einem Boot übersetzen. Das Boot kann aber außer ihm selbst nur noch einen weiteren Passagier aufnehmen. Das Problem: Wolf und Ziege können nicht unbeaufsichtigt bleiben, der Wolf würde die Ziege fressen. Genausowenig können Ziege und Kohlkopf unbeaufsichtigt bleiben, weil die Ziege dann den Kohl verschlingen würde.

Wie gelingt es dem Bauern, den Fluss zu überqueren, ohne dass ein Unglück passiert? Lösen Sie das Rätsel mit dem Alloy Analyzer.

18. Tic-Tac-Toe — Drei Gewinnt

Auf einem quadratischen 3×3 Felder großen Spielfeld setzen zwei Spieler abwechselnd ihr Zeichen (ein Spieler Kreuze, der andere Kreise) in ein freies Feld. Der Spieler, der als Erster drei Zeichen in eine Zeile, Spalte oder Diagonale setzen kann, gewinnt.

Spezifizieren Sie das Spiel in Alloy.

Zusatzaufgabe: Zeigen Sie, dass es möglich ist, dass das Spiel unentschieden endet. Das heißt, alle neun Felder sind gefüllt, ohne dass ein Spieler die erforderlichen Zeichen in einer Reihe, Spalte oder Diagonalen setzen konnte.

19. Variante des Echo-Algorithmus

In Erste Begegnung mit Alloy 6 haben wir gesehen, wie man mit dem Echo-Algorithmus den aufspannenden Baum eines Graphen konstruieren kann.

In dieser Spezifikation haben wir ein Feld `color` verwendet, das `Green` wird, wenn ein Knoten sein Echo zurückgesandt hat. In der Visualisierung kann man eine Funktion spezifizieren, mit der man die Knoten auch entsprechend im Visualisierungsfenster grün anzeigen kann.

Das geht aber auch anders: Verändern Sie den Algorithmus aus Abschnitt 6 von Erste Begegnung mit Alloy 6 so, dass man die Knoten tatsächlich in der Visualisierung grün anzeigen kann, jedoch nicht durch eine Funktion. Tipp: Die Spezifikation einer Teilmenge der Knoten, die ihr Echo geschickt haben, könnte dabei helfen.

20. Aufspannender Baum eines Graphen

In Erste Begegnung mit Alloy 6 haben wir gesehen, wie man mit dem Echo-Algorithmus den aufspannenden Baum eines Graphen konstruieren kann. Dieser Algorithmus endet damit, dass das Echo der Nachrichten zum Initiator zurückgekommen ist. Der aufspannende Baum ist doch dann längst konstruiert.

Passen Sie die Variante der Spezifikation aus Abschnitt 6 von Erste Begegnung mit Alloy 6 so an, dass kein Echo zurückgeschickt wird. Es sollte dann möglich sein, den Spannbaum in $n+1$ Schritten für Graphen mit n Knoten zu konstruieren.

21. Türme von Hanoi

Das Spiel „Türme von Hanoi“ besteht aus drei gleich großen Stäben, den Türmen. Auf die Türmen können mehrere gelochte Scheiben gelegt werden, die alle verschieden groß sind. Zu Beginn liegen alle Scheiben auf dem linken Stab, und zwar der Größe nach geordnet, die kleinste Scheibe oben.

Ziel des Spiels ist es, den kompletten Scheiben-Stapel vom linken Turm auf den rechten Turm zu versetzen. Dabei darf bei jedem Zug die oberste Scheibe eines Turms auf einen anderen Turm befördert werden, allerdings so, dass jeder Turm immer der Größe nach geordnet ist.

Lösen Sie die Aufgabe mit Alloy.

22. Königsberger Brücken mit LTL

Die Aufgabe zu den Königsberger Brücken kann man auch mit LTL lösen. Zeigen Sie damit, (a) dass es keinen Weg gibt, auf dem alle sieben Brücken nur genau einmal

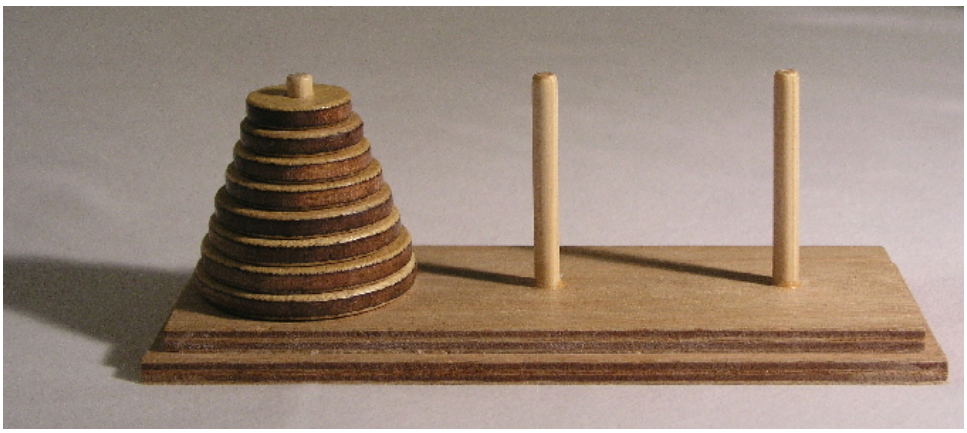

Abbildung 2: Türme von Hanoi, from https://commons.wikimedia.org/wiki/File:Tower_of_Hanoi.jpeg

überquert werden dürfen und (b) dass es natürlich Wege über alle Brücken gibt, wenn man diese Voraussetzung weglässt.

23. Speisende Philosophen

Fünf Philosophen sitzen an einem runden Tisch mit jeweils einer Gabel zwischen ihnen und einem Teller köstlicher Speise vor ihnen. Ein Philosoph darf essen, wenn er beide Gabeln, die linke und die rechte zwischen ihm und seinen beiden Nachbarn in Händen hält (siehe Wikipedia zum Philosophenproblem).

Spezifizieren Sie die Situation und zeigen Sie, dass es (1) eine Verklemmung geben kann, aber auch (2) einen Ablauf, an dem wenigstens ein Philosoph die köstliche Speise zu sich nehmen kann. Können Sie (3) auch einen Ablauf erzeugen, bei dem jeder Philosoph wenigstens einmal zugreifen konnte?