Ludwig-Maximilians-Universität München **SoSe 2014**
Institut für Informatik
Dr. M. Hölzl, C. Kroiß

Formale Techniken der Software-Entwicklung
Übungsblatt 4
Besprechung am 23.05.2014

Die Aufgaben 1 und 2 wurden aus [1] übernommen und sind daher auf Englisch.

Aufgabe 1:

Let $F(x, y)$ mean that x is the father of y; $M(x, y)$ denotes x is the mother of y. Similarly, $H(x, y)$, $S(x, y)$, and $B(x, y)$ say that x is the husband/sister/brother of y, respectively. You may also use constants to denote individuals, like 'Ed' and 'Patsy.' However, you are not allowed to use any predicate symbols other than the above to translate the following sentences into predicate logic:

(a) Everybody has a mother.

(b) Everybody has a father and a mother.

(c) Whoever has a mother has a father.

(d) Ed is a grandfather.

(e) All fathers are parents.

(f) All husbands are spouses.

(g) No uncle is an aunt.

(h) All brothers are siblings.

(i) Nobody's grandmother is anybody's father.

(j) Ed and Patsy are husband and wife.

(k) Carl is Monique's brother-in-law.

Aufgabe 2:

The following sentences are taken from the RFC3157 Internet Taskforce Document 'Securely Available Credentials – Requirements.' Specify each sentence in predicate logic, defining predicate symbols as appropriate:

(a) An attacker can persuade a server that a successful login has occurred, even if it hasn't.

(b) An attacker can overwrite someone else's credentials on the server.

(c) All users enter passwords instead of names.

(d) Credential transfer both to and from a device MUST be supported.

(e) Credentials MUST NOT be forced by the protocol to be present in cleartext at any device other than the end user's.

(f) The protocol MUST support a range of cryptographic algorithms, including syymetric and asymmetric algorithms, hash algorithms, and MAC algorithms.

(g) Credentials MUST only be downloadable following user authentication or else only downloadable in a format that requires completion of user authentication for deciphering.

(h) Different end user devices MAY be used to download, upload, or manage the same set of credentials.

Aufgabe 3:

Gegeben sei die Formel $\Phi \stackrel{def}{=} \forall x \forall y.Q(g(x,y), g(y,y), z)$. Finden Sie zwei Modelle $\mathcal{M}$ und $\mathcal{M}'$ so dass $\mathcal{M} \models \Phi$ aber $\mathcal{M}' \not\models \Phi$ gilt.

Aufgabe 4:

Gegeben sei der folgende Satz:

$$\Phi \stackrel{def}{=} \forall x \exists y \exists z (P(x,y) \wedge P(z,y) \wedge (P(x,z) \rightarrow P(z,x)))$$

Welche der folgenden Modelle erfüllen Φ?

(a) Das Modell $\mathcal{M}$ besteht aus den natürlichen Zahlen mit $P^{\mathcal{M}} \stackrel{def}{=} \{(m,n) | m < n\}$.

(b) Das Modell $\mathcal{M}'$ besteht aus den natürlichen Zahlen mit $P^{\mathcal{M}'} \stackrel{def}{=} \{(m, 2 * m) | m \in \mathbb{N}\}$.

(c) Das Modell $\mathcal{M}''$ besteht aus den natürlichen Zahlen mit $P^{\mathcal{M}''} \stackrel{def}{=} \{(m,n) | m < n + 1\}$.

Aufgabe 5:

Geben Sie Beweisbäume im Sequenzkalkül für folgende Formeln an:

(a) $\exists x(P \rightarrow Q(x)) \rightarrow (P \rightarrow \exists z.Q(z))$, wobei P ein aussagenlogisches Symbol und Q ein unäres Predikat ist.

(b) $(\forall x.A) \vee (\forall x.B) \rightarrow \forall x(A \vee B)$, wobei A und B beliebige Formeln seien, in denen x nicht frei vorkommt.

Literatur

[1] Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and reasoning about systems.* Cambridge University Press, 2004.