Klausur Formale Systeme

Universität Karlsruhe

Fakultät für Informatik

WS 2007/2008

Prof. Dr. P. H. Schmitt

18. Februar 2008

Name: _____

Vorname: _____

Matrikel-Nr.: _____

Bitte geben Sie auf jedem benutzten Blatt rechts oben Ihren Namen und Ihre Matrikel-Nummer an!

A1 (11)	A2 (6)	A3 (3)	A4 (7)	A5 (7)	A6 (8)	A7 (8)	A8 (4)	A9 (6)	Σ (60)

Bewertungstabelle bitte frei lassen!

Zum Bestehen der Klausur benötigen Sie 20 der erreichbaren 60 Punkte.

Bonus: _____ **Gesamtpunkte:**

1 Zur Einstimmung (11 Punkte)

Kreuzen Sie in den folgenden Tabellen alles Zutreffende an.

Für jede falsche Antwort wird ein halber Punkt abgezogen!
(Dabei werden jedoch keinesfalls weniger als 0 Punkte für jede der drei Teilaufgaben vergeben.)

Hinweise:

- „PL1“ steht für „Prädikatenlogik erster Stufe (mit Gleichheit $\doteq$)“, wie sie in der Vorlesung vorgestellt wurde. Auf diese beziehen sich in Teilaufgabe a. auch die Begriffe „erfüllbar“, „allgemeingültig“ und „unerfüllbar“.
- In Teilaufgabe a. kann eine Formel mehr als eine der genannten Eigenschaften haben. In Teilaufgabe b. und c. *genau* eine.
- p und q sind Prädikatssymbole, c und f sind Funktionssymbole, und r, t, x, y und z sind Variablen.
- Es gelten die üblichen Klammereinsparungsregeln.

a.

	keine Formel der PL1	erfüllbar	allgemeingültig	unerfüllbar
$\big[\forall x \exists y \big(p(x) \rightarrow q(y)\big)\big] \leftrightarrow \big[(\exists r\ p(r)) \rightarrow (\exists t\ q(t))\big]$		X	X	
$\forall x \big[p(x) \rightarrow p(p(x))\big] \rightarrow p(p(c))$	X			
$\forall x \exists y \big[\neg(x \doteq y)\big]$		X		
$\forall x \forall y \big(p(f(x,y))\big) \wedge \exists z \big(\neg p(f(z,z))\big)$				X

b.

	Richtig	Falsch
Sei $\mathcal{K} = (S, R, I)$ eine Kripkestruktur mit $\mathcal{K} \models \Box p \rightarrow \Box\Box p$. Daraus folgt, dass R transitiv ist.		X
In der Aussagenlogik gilt: $p \wedge q$ ist unerfüllbar, genau dann wenn $p \rightarrow \neg q$ allgemeingültig ist.	X	
Für jede unerfüllbare Klauselmenge M gibt es eine Ableitung der leeren Klausel $M \vdash_{\text{lin.Res}} \square$ mit linearer Resolution.	X	
Das Hinzufügen einer neuen Regel zum Tableaukalkül für die Prädikatenlogik kann sowohl Korrektheit als auch Vollständigkeit verletzen.		X

c.

Sind folgende LTL-Formeln allgemeingültig, d.h. gelten sie in allen omega-Strukturen?

LTL-Formel	Ja	Nein
$((\mathbf{X}\neg p)\ \mathbf{U}\ p)$		X
$\Box(p\ \mathbf{U}\ q) \rightarrow \Box(p \vee q)$	X	
$\mathbf{X}(p\ \mathbf{U}\ q) \rightarrow ((\mathbf{X}p)\ \mathbf{U}\ (\mathbf{X}q))$	X	

2 Formalisieren in Aussagenlogik / Davis-Putnam (3+3 Punkte)

a. Gegeben sei eine Landkarte mit L Ländern, die mit den Zahlen von 0 bis $L-1$ bezeichnet werden. Die binäre Relation $Na(i,j)$ trifft auf zwei Länder i und j zu ($0 \leq i,j < L$), wenn sie benachbart sind. Die Landkarte soll nun mit den **drei** Farben *rot*, *grün* und *blau* so eingefärbt werden, dass keine zwei benachbarten Länder dieselbe Farbe erhalten.

Geben Sie eine Menge F von aussagenlogischen Formeln an, so dass F genau dann erfüllbar ist, wenn eine Färbung der geforderten Art möglich ist.

Gefragt ist eine Formalisierung in **Aussagenlogik**, nicht in **Prädikatenlogik**. Für jedes Land i gibt es drei AL-Variablen R_i, G_i, B_i. Nun muss für einen gegebenen Graphen formalisiert werden, dass

1. Jedes Land mindestens 1 Farbe hat,
2. jedes Land höchstens 1 Farbe hat und
3. benachbarte Länder nicht diesselbe Farbe haben.

$$\begin{aligned} F = \quad & \{R_i \vee G_i \vee B_i : 0 \leq i < L\} \\ \cup \quad & \{(\neg R_i \vee \neg G_i) \wedge (\neg G_i \vee \neg B_i) \wedge (\neg B_i \vee \neg R_i) : 0 \leq i < L\} \\ \cup \quad & \{(\neg R_i \vee \neg R_j) \wedge (\neg G_i \vee \neg G_j) \wedge (\neg B_i \vee \neg B_j) : 0 \leq i,j < L, Na(i,j)\} \end{aligned}$$

b.

$$M := \big\{\{A, \neg B, C, \neg D\}, \{B, \neg D\}, \{C, D\}, \{\neg A, \neg D\}, \{\neg C, D\}, \{A, \neg C\}, \{A, B, \neg C\}\big\}$$

Zeigen Sie mit Hilfe des Davis-Putnam-Loveland-Algorithmus, dass die Menge M an aussagenlogischen Klauseln unerfüllbar ist.

Fallunterscheidung nach A.
1. $A = 0$

	$\{A,\neg B,C,\neg D\}$,	$\{B,\neg D\}$,	$\{C,D\}$,	$\{\neg A,\neg D\}$,	$\{\neg C,D\}$,	$\{A,\neg C\}$,	$\{A,B,\neg C\}$
$A=0$	$\{\neg B,C,\neg D\}$,	$\{B,\neg D\}$,	$\{C,D\}$,	$-$,	$\{\neg C,D\}$,	$\{\neg C\}$,	$\{B,\neg C\}$
$\Rightarrow C=0$	$\{\neg B,\neg D\}$,	$\{B,\neg D\}$,	$\{D\}$,	$-$,	$-$,	$-$,	$-$
$\Rightarrow D=1$	$\{\neg B\}$,	$\{B\}$,	$-$,	$-$,	$-$,	$-$,	$-$
$\Rightarrow B=1$	$\square$,	$-$,	$-$,	$-$,	$-$,	$-$,	$-$

2. $A = 1$

	$\{A,\neg B,C,\neg D\}$,	$\{B,\neg D\}$,	$\{C,D\}$,	$\{\neg A,\neg D\}$,	$\{\neg C,D\}$,	$\{A,\neg C\}$,	$\{A,B,\neg C\}$
$A=1$	$-$,	$\{B,\neg D\}$,	$\{C,D\}$,	$\{\neg D\}$,	$\{\neg C,D\}$,	$-$,	$-$
$\Rightarrow D=0$	$-$,	$-$,	$\{C\}$,	$-$,	$\{\neg C\}$,	$-$,	$-$
$\Rightarrow C=1$	$-$,	$-$,	$-$,	$-$,	$\square$,	$-$,	$-$

Nur eine Fallunterscheidung (ein „choose“) ist notwendig, ab dann benötigt der Algorithmus wegen der Unit-Elimination keine Entscheidungen mehr.

3 Formalisieren in Prädikatenlogik (3 Punkte)

Gegeben ist die prädikatenlogische Signatur $\Sigma_{\mathbb{N}}$, die das Konstantensymbol *eins*, das zweistellige Funktionszeichen *mul* und das binäre Relationszeichen *kl* enthält. Die Interpretation $(\mathbb{N}, I_{\mathbb{N}})$ ist gegeben durch

$$\begin{aligned} I_{\mathbb{N}}(eins) &= 1 \\ I_{\mathbb{N}}(mul)(a,b) &= a \cdot b \\ I_{\mathbb{N}}(kl) &= \{(a,b) \in \mathbb{N} \times \mathbb{N} : a < b\} \end{aligned}$$

Hinweis: 1 ist keine Primzahl.

a. Geben Sie eine prädikatenlogische Formel φ_{pr}, die eine freie Variable x enthält und für die gilt:

$$(\mathbb{N}, I_{\mathbb{N}}, \beta_x^p) \models \varphi_{pr} \iff p \text{ ist Primzahl}$$

$$\forall y \forall z(mul(y,z) \doteq x \rightarrow (y \doteq eins \vee z \doteq eins)) \wedge kl(eins, x)$$

oder

$$\forall y \forall z(mul(y,z) \doteq x \rightarrow (y \doteq x \vee z \doteq x)) \wedge \neg eins \doteq x$$

b. Geben Sie eine Formel an, die folgenden Sachverhalt formalisiert:

Es gibt unendlich viele Primzahlen in $\mathbb{N}$.

Sie können dafür die Formel φ_{pr} aus Teilaufgabe a. als Abkürzung verwenden.

$$\forall y \exists x(kl(y,x) \wedge \varphi_{pr})$$

4 Skolemnormalform (5+2 Punkte)

a. Transformieren Sie folgende Formel K der Prädikatenlogik schrittweise in Skolemnormalform.

$$K := \Big[\exists x\big((\forall y\ p(x,y)) \rightarrow \forall y\ q(y,x)\big)\Big] \rightarrow \forall u \exists w\ p(f(u,w),u)$$

Hinweis: Bei einer Formel in Skolemnormalform ist die Matrix in konjunktiver Normalform.

i. Allabschluss: K ist geschlossen, nichts zu tun

ii. Bereinigen:

$$\Big[\exists x\big((\forall y_1\ p(x,y_1)) \rightarrow \forall y_2\ q(y_2,x)\big)\Big] \rightarrow \forall u \exists w\ p(f(u,w),u)$$

iii. Pränexnormalform:

$$\begin{aligned} & \big[\exists x \forall y_2 \exists y_1 (p(x,y_1) \rightarrow q(y_2,x))\big] \rightarrow \forall u \exists w\ p(f(u,w),u) \\ \leftrightarrow\ & \forall x \exists y_2 \forall y_1 \forall u \exists w (p(x,y_1) \rightarrow q(y_2,x)) \rightarrow p(f(u,w),u) \end{aligned}$$

iv. Skolemisieren: $y_2 \mapsto g(x), w \mapsto h(x,y_1,u)$

$$\forall x \forall y_1 \forall u [(p(x,y_1) \rightarrow q(g(x),x)) \rightarrow p(f(u,h(x,y_1,u)),u)]$$

v. Matrix in KNF transformieren:

$$\begin{aligned} & \forall x \forall y_1 \forall u [\neg(p(x,y_1) \rightarrow q(g(x),x)) \vee p(f(u,h(x,y_1,u)),u)] \\ \leftrightarrow\ & \forall x \forall y_1 \forall u [(p(x,y_1) \wedge \neg q(g(x),x)) \vee p(f(u,h(x,y_1,u)),u)] \\ \leftrightarrow\ & \forall x \forall y_1 \forall u [(p(x,y_1) \vee p(f(u,h(x,y_1,u)),u)) \wedge (\neg q(g(x),x) \vee p(f(u,h(x,y_1,u)),u))] \end{aligned}$$

b. Geben Sie eine Skolemnormalform für K an, die sich von Ihrer Lösung zu a. nicht nur durch Umbenennung und Äquivalenzumformung unterscheidet.

Es können z.B. y_1 und y_2 in anderer Reihenfolge nach außen gezogen werden:

$$\forall x \forall y_1 \exists y_2 \forall u \exists w (p(x,y_1) \rightarrow q(y_2,x)) \rightarrow p(f(u,w),u)$$

Damit ergäbe sich für die Skolemisierung: $y_2 \mapsto g'(x,y_1)$
Insgesamt also:

$$\forall x \forall y_1 \forall u [(p(x,y_1) \vee p(f(u,h(x,y_1,u)),u)) \wedge (\neg q(g'(x,y_1),x) \vee p(f(u,h(x,y_1,u)),u))]$$

5 Tableaubeweis (7 Punkte)

Beweisen Sie im Tableau-Kalkül:

$$\left\{ \begin{array}{l} \exists x\ p(x), \\ \forall x(p(x) \rightarrow p(f(x))), \\ \forall x(\neg p(x) \leftrightarrow r(x)) \end{array} \right\} \vdash\ \exists x\ \neg r(f(f(x)))$$

Verwenden Sie ausschließlich die im Skript angegebenen Tableauregeln und die folgenden Regeln für die Äquivalenz:

$1\ A \leftrightarrow B$	
$1\ A$	$0\ A$
$1\ B$	$0\ B$

$0\ A \leftrightarrow B$	
$0\ A$	$1\ A$
$1\ B$	$0\ B$

$1\,\exists x\ p(x)$ (0)

$1\,\forall x(p(x) \rightarrow p(f(x)))$ (1)

$1\,\forall x(\neg p(x) \leftrightarrow r(x))$ (2)

$0\,\exists x\ \neg r(f(f(x)))$ (4)

$0\,\neg r(f(f(X_1)))$ (5)[4]

$1\,r(f(f(X_1)))$ (6)[5]

$1\,p(c_1)$ (7)[0]

$1\,p(X_2) \rightarrow p(f(X_2))$ (8)[1]

$0\,p(X_2)$ (9)[8] | $1\,p(f(X_2))$ (10)[8]

$1\,p(X_3) \rightarrow p(f(X_3))$ (11)[1]

$0\,p(X_3)$ (12)[11] | $1\,p(f(X_3))$ (13)[11]

$1\,\neg p(X_4) \leftrightarrow r(X_4)$ (14)[2]

$1\,\neg p(X_4)$ (15)[14] | $0\,\neg p(X_4)$ (17)[14]

$1\,r(X_4)$ (16)[14] | $0\,r(X_4)$ (18)[14]

$0\,p(X_4)$ (19)[15]

$\sigma = \{X_1/c_1, X_2/c_1, X_3/f(c_1), X_4/f(f(c_1))\}$ schließt das Tableau

6 Modallogik (7+1 Punkte)

Definition Ein Kripkerahmen (S, R) heißt *schwach konfluent*, wenn er die Formel

$$\forall x \forall y (R(x, y) \rightarrow \exists z (R(x, z) \wedge R(y, z)))$$

erfüllt.

a. Zeigen Sie, dass die modallogische Formel $\Diamond\Box p \rightarrow \Diamond p$ die Klasse der schwach konfluenten Rahmen charakterisiert.

Wir zeigen, dass $\Diamond\Box p \rightarrow \Diamond p$ die Klasse der schwachkonfluenten Rahmen charakterisiert.

Teil 1 Sei $\mathcal{K} = (S, R, I)$ eine Kripke-Struktur mit schwach konfluentem Rahmen. Für $s \in S$ haben wir $s \models \Diamond\Box p \rightarrow \Diamond p$ zu zeigen. Nehmen wir also die linke Seite der Implikation an, $s \models \Diamond\Box p$, und versuchen $s \models \Diamond p$ zu zeigen. Aus $s \models \Diamond\Box p$ folgt die Existenz einer Welt $s_1 \in S$ mit $R(s, s_1)$ und $s_1 \models \Box p$. Wegen der schwachen Konfluenzeigenschaft existiert eine Welt s_2 mit $R(s, s_2)$ und $R(s_1, s_2)$. Aus $s_1 \models \Box p$ folgt also auch $s_2 \models p$. Da auch $R(s, s_2)$ gilt haben wir $s \models \Diamond p$ gezeigt, wie gewünscht.

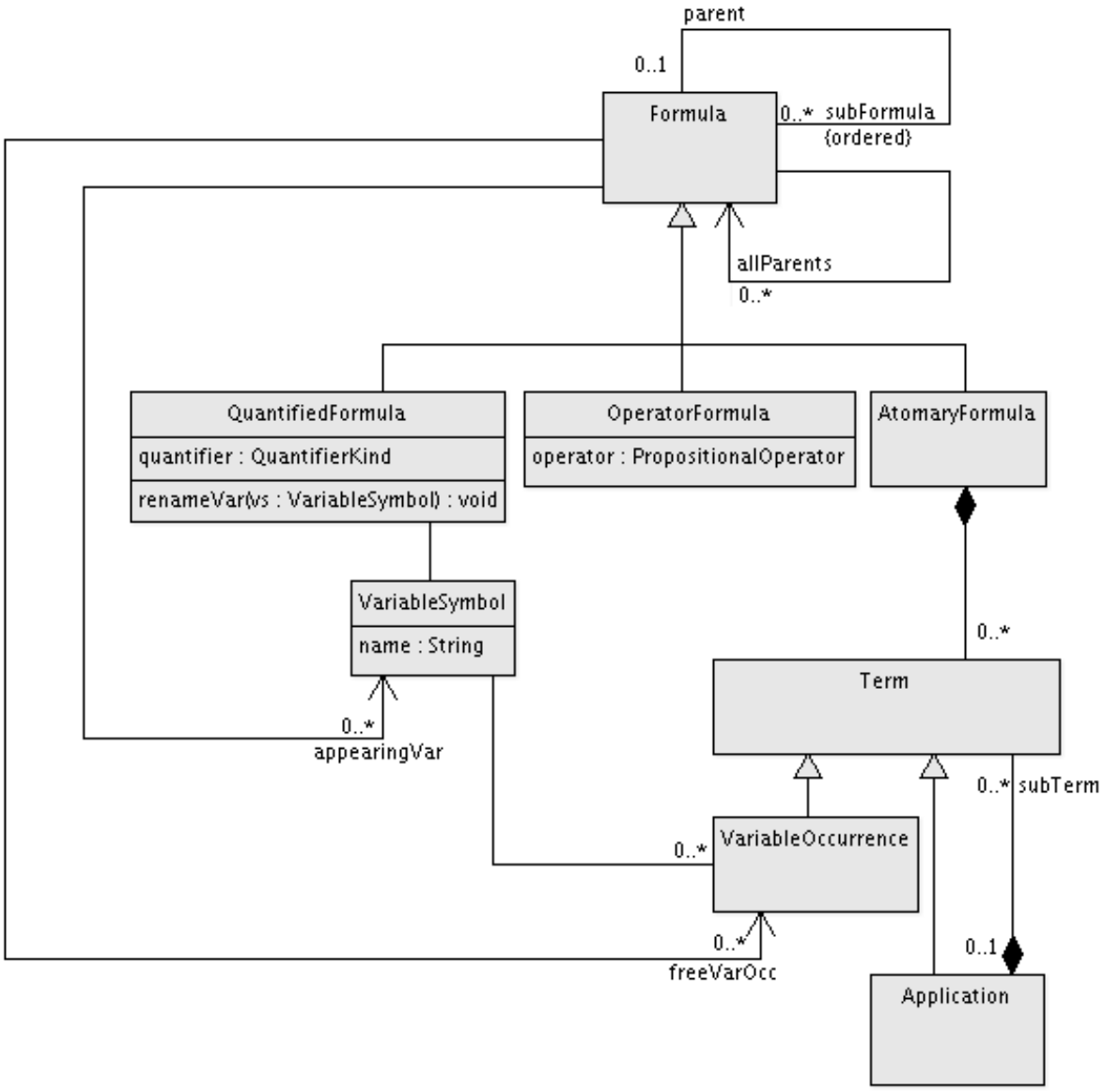
Teil 2 Angenommen der Rahmen (S, R) ist nicht schwach konfluent. Dann gibt es $s_1, s_2 \in S$ mit $R(s_1, s_2)$, so daß für alle $t \in S$ gilt $\neg R(s_1, t)$ oder $\neg R(s_2, t)$. Wir definieren eine Interpretationsfunktion I durch:

$$I(p, t) = \begin{cases} W & \text{falls } R(s_2, t) \\ F & \text{sonst} \end{cases}$$

Nach Definition von I gilt in der Kripke Struktur $\mathcal{K} = (S, R, I)$ auf jeden Fall $s_2 \models \Box p$ und auch $s_1 \models \Diamond\Box p$. Wäre auch $s_1 \models \Diamond p$ wahr, so würde es ein $t \in S$ geben mit $R(s_1, t)$ und $t \models p$. Was nach Definition von I zu $R(s_2, t)$ führt. Ein solches t sollte es aber nach Annahme nicht geben. Der Widerspruchsbeweis ist damit erfolgreich abgeschlossen.

b. Begründen Sie kurz, warum jeder reflexive, symmetrische Kripkerahmen auch schwach konfluent ist.

Es gilt in refl. symm. Rahmen: $\forall x \forall y (R(x, y) \rightarrow R(x, x) \wedge R(y, x))$. Das x selbst erfüllt die Aufgabe des z.


parent
0..1
Formula
0..* subFormula
{ordered}
allParents
0..*
QuantifiedFormula
quantifier : QuantifierKind
renameVar(vs : VariableSymbol) : void
OperatorFormula
operator : PropositionalOperator
AtomaryFormula
VariableSymbol
name : String
0..*
appearingVar
0..*
Term
0..* subTerm
VariableOccurrence
0..*
0..*
freeVarOcc
0..1
Application

7 OCL (2+3+3) Punkte

Auf der linken Seite (auf der Rückseite zu Aufgabe 6) finden Sie einen Ausschnitt aus einer modifizierten Version des UML-Metamodels der Prädikatenlogik als Klassendiagramm.

Insbesondere verknüpft die Assoziation `appearingVar` eine Formel mit allen Variablensymbolen, die in ihr vorkommen.

Die Assoziation `freeVarOcc` verknüpft eine Formel mit allen Variablenvorkommen (Instanzen eines Variablensymbols), die in ihr frei, also nicht durch einen Quantor gebunden, auftreten.

a. Geben Sie für die folgende OCL-Invariante die Bedeutung in natürlicher Sprache an.

```
context Formula
inv:    allParents = parent.allParents->including(parent)
```

Die Relation `allParents` ist die transitive Hülle der Relation `parent`. *oder*

Die Menge aller Oberformeln (allParents) einer Formel besteht aus der direkten Oberformel (parent) sowie deren Oberformeln (parent.allParents). *oder*

Die Menge aller Eltern einer Formel entspricht der Menge aller Eltern des direkten Elternteils einschließlich des direkten Elternteils selbst.

b. Geben Sie eine OCL-Invariante für die Klasse `QuantifiedFormula` an, die besagt, dass die freien Variablenvorkommen einer quantifizierten Formel gerade die freien Vorkommen der direkten Unterformeln sind, ohne die, die sich auf das quantifizierte Variablensymbol beziehen.

```
context QuantifiedFormula
inv: subFormula.freeVarOcc->select(not variableSymbol = self.variableSymbol)
= freeVarOcc
oder
inv: subFormula->collect(freeVarOcc)->reject(vo|vo.variableSymbol = self.variableSymbol)
= freeVarOcc
```

c. Die Methode `QuantifiedFormula::renameVar(vs: VariableSymbol)` benennt eine quantifizierte Variable um. Schreiben sie einen OCL-Methodenvertrag, der folgendes formalisiert.

> Die Methode darf nur angewendet werden, wenn das neue Variablensymbol `vs` vom bisherigen verschieden ist.
>
> Dann hat nach der Ausführung der Methode das alte Symbol keine freien Vorkommen mehr in den Unterformeln.

```
context QuantifiedFormula::renameVar(vs: VariableSymbol)
pre: not variableSymbol = vs
post: not subFormula.freeVarOcc.variableSymbol->includes(variableSymbol@pre)
oder
post: subFormula.freeVarOcc.variableSymbol->excludes(variableSymbol@pre)
```

8 LTL (3+1 Punkte)

a. Finden Sie eine LTL-Formel F, die genau dann in einer omega-Struktur wahr ist, wenn für jeden Zeitpunkt t_p, in dem p wahr ist, gilt:

i. Es gibt Zeitpunkte t_q und t_r, die nicht vor t_p liegen und in denen q bzw. r wahr ist.

ii. Der erste Zeitpunkt nach t_p, in dem q wahr ist, liegt nicht nach dem ersten Zeitpunkt, zu dem r wahr ist.

$$\Box(p \rightarrow \Diamond r \wedge (\neg r \,\mathbf{U}\, q))$$

oder

$$\Box(p \rightarrow \Diamond q \wedge \Diamond r) \wedge \Box(p \rightarrow (\neg r \,\mathbf{U}\, q))$$

b. **Definition** Seien P und Q LTL-Formeln. Dann ist die Semantik von $P\,\mathbf{B}\,Q$ ("P begins Q") folgendermaßen definiert:

$$\xi \models P\,\mathbf{B}\,Q :\Longleftrightarrow \text{ Für jedes } n \in \mathbb{N} \text{ für das } \xi_n \models P \text{ gilt, gilt für } k \geq n \text{ die Aussage } \xi_k \models Q$$

Geben Sie einen zu $P\,\mathbf{B}\,Q$ äquivalenten LTL-Ausdruck an, der **B** nicht verwendet.

$$\Box(P \rightarrow \Box Q)$$

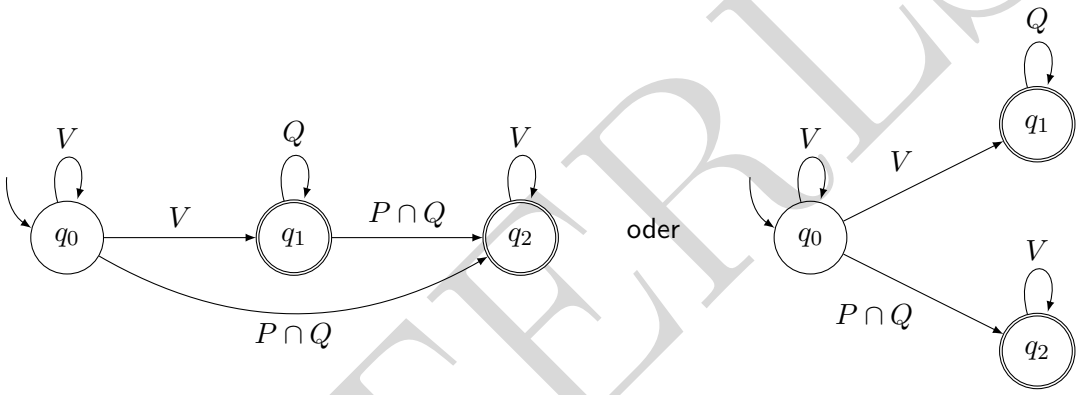
9 Büchi und LTL (3+3 Punkte)

Gegeben ist eine AL-Signatur Σ, die mindestens die beiden von einander verschiedenen Variablen p und q enthält. Für das Vokabular $V = \mathbb{P}(\Sigma)$ (Potenzmenge von Σ) werden die folgenden aus der Vorlesung bekannten Abkürzungen definiert:

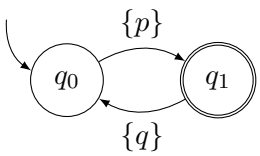
$$\begin{aligned} P &= \{M \in V : p \in M\} \subset V \\ Q &= \{M \in V : q \in M\} \subset V \end{aligned}$$

a. Geben Sie für die LTL-Formel $F = \Diamond(p \,\mathbf{V}\, q)$ einen akzeptierenden Büchi-Automaten $\mathcal{A}$ an, so dass gilt:

$$L(\mathcal{A}) = \{\xi \in V^\omega : \xi \models F\}$$



b. Sei nun $\Sigma = \{p, q\}$. Welche LTL-Formel wird von diesem Büchi-Automaten akzeptiert?



$$p \wedge \neg q \wedge \Box(p \rightarrow \mathbf{X}\neg p \wedge \mathbf{XX}p) \wedge \Box(q \rightarrow \mathbf{X}\neg q \wedge \mathbf{XX}q)$$

oder

$$p \wedge \Box\big((p \rightarrow \mathbf{X}(q \wedge \neg p)) \wedge (q \rightarrow \mathbf{X}(p \wedge \neg q))\big)$$