

# Formalisierung von Sicherheitseigenschaften im $\mu$ -Kalkül

Hauptseminar: Nachweis von Sicherheitseigenschaften  
für JavaCard durch approximative Programmauswertung

Michael Wahler (wahler@in.tum.de)

## Überblick

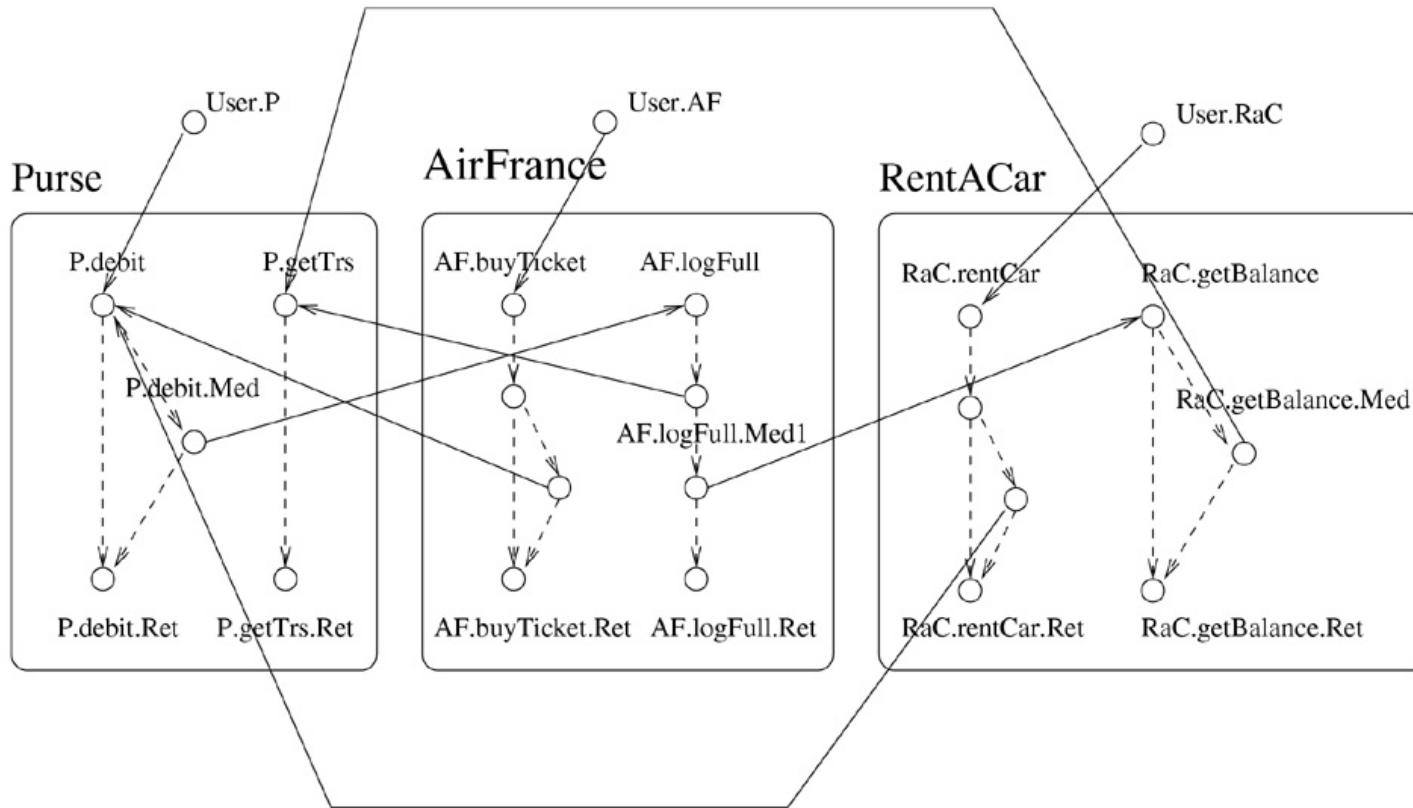
- Einführungsbeispiel: Elektronische Geldbörse
- Zustandsübergangsautomaten
- Fixpunkttheorie
- $\mu$  und  $\nu$  - Formeln im  $\mu$ -Kalkül
- Semantik

## Einführungsbeispiel: Elektronische Geldbörse

Treueprogramm; realisiert mit drei Applets:

- **P**
  - Auszahlungen
  - Speicherung der letzten getätigten Transaktionen
  - *logFull*-Service (kostenpflichtig)
- **AF**
  - Treue-Applet
  - Teilnehmer am *logFull*-Service
  - Partner von **RaC**
- **RaC**
  - Treue-Applet
  - **kein** Teilnehmer am *logFull*-Service

# Aufrufgraph der Elektronischen Geldbörse



## Spezifikation der einzelnen Applets

SPEC\_P (P) =

ALWAYS.

WITHIN (P.getTrs).

P CALLS {}

SPEC\_AF (AF, P, RaC) =

ALWAYS.

WITHIN (AF.logFull).

AF CALLS (P.getTrs, RaC.getBalance)

SPEC\_RaC (RaC) =

ALWAYS.

WITHIN (RaC.getBalance).

RaC CALLS {}

## Spezifikation der Interaktion der Applets

```
SPEC_EP (P, AF, RaC) =  
  ALWAYS.  
  WITHIN (AF.logFull)  
    NOT (RaC CALLS {P.getTrs})
```

Beweis, dass die Spezifikation eingehalten wird:

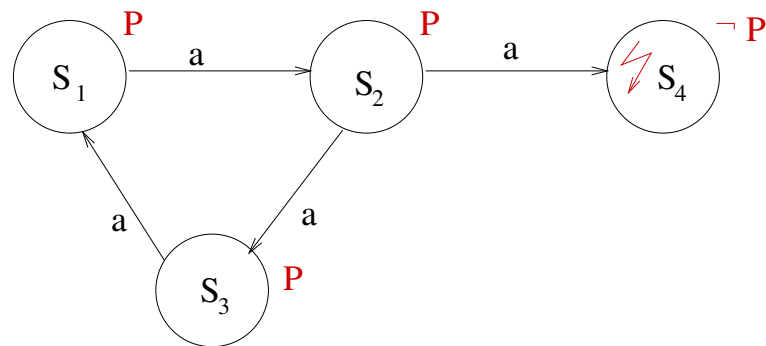
- Umwandlung in Zustandsautomat (Kripke-Struktur)
- Formulierung der Spezifikationen im  $\mu$ -Kalkül

# Kripke-Strukturen

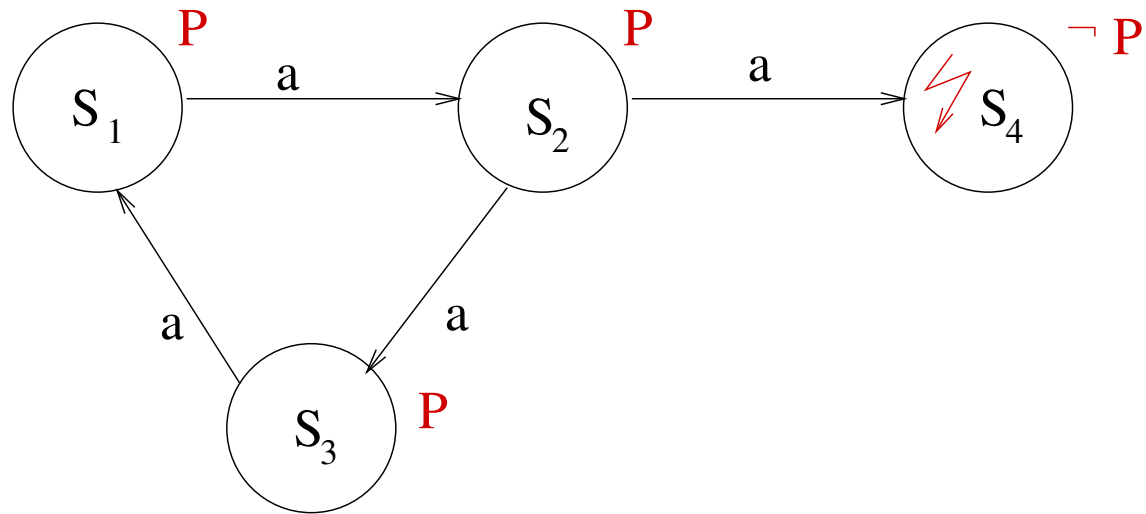
Kripke-Strukturen bestehen aus

- einer Menge von Zuständen
- eine Menge von Übergängen zwischen den Zuständen
- eine Funktion, die jedem Zustand  $S$  eine Menge von Eigenschaften zuweist, die in  $S$  gelten

*Pfade* modellieren Berechnungen eines Systems.

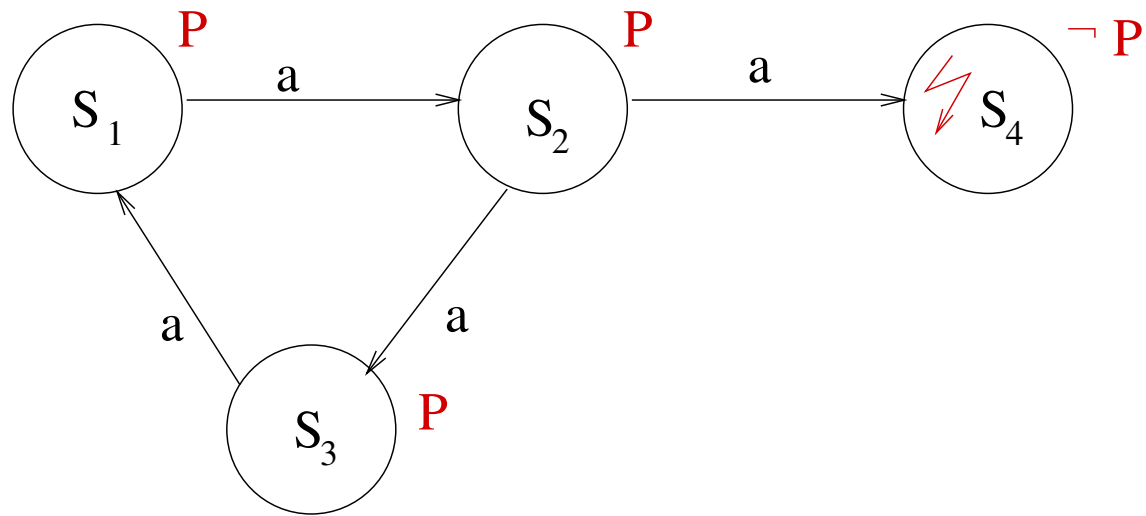


## Aussagen über Aktionen und Zustände



- $[-]P$  – "Für alle Aktionen gilt nach Ausführung  $P$ "
- $[a]P$  – "Für alle  $a$ -Aktionen gilt nach Ausführung  $P$ "
- $\langle - \rangle P$  – "Es gibt eine Aktion, nach deren Ausführung  $P$  gilt"
- $\langle a \rangle P$  "Es gibt eine  $a$ -Aktion, nach deren Ausführung  $P$  gilt"

## Aussagen "immer ..."



- **Frage:** Wie lässt sich ausdrücken: " $P$  muss immer gelten."?
- **Antwort:**  $P \wedge [-]Z$

wobei  $Z$  eine Menge von Zuständen ist, in denen  $P$  immer gilt.

⇒ Das ist ein rekursiver Ausdruck!

⇒ Jetzt muss ein bisschen Theorie sein (nur ein kleiner Ausschnitt aus der sehr komplexen Theorie)!

## Definition Fixpunkt

Annäherungsweise Definition des Begriffs "Fixpunkt":

**Theorem** (nach Knaster-Tarski): Ist  $f$  eine monotone Abbildung über einer geordneten, vollständigen Menge  $A$  mit kleinstem Element, so ist die Gleichung

$$x = f(x)$$

lösbar und es existiert ein eindeutig bestimmter kleinster Fixpunkt von  $f$ .

$f$  heißt *monoton*, wenn gilt:

$$x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$$

# Algorithmische Charakterisierung des Fixpunkts

## Kleinster Fixpunkt

- Iterieren von  $f$  über  $\emptyset$
- das ergibt eine aufsteigende Kette von Approximanten
- $\mu f = \bigcup_{\alpha < \kappa} f^\alpha(\emptyset)$  ist kleinster Fixpunkt von  $f$

## Größter Fixpunkt

- Iterieren von  $f$  über  $\Sigma$  (die Menge der Zustände)
- das ergibt eine absteigende Kette von Approximanten
- $\nu f = \bigcap_{\alpha < \kappa} f^\alpha(\Sigma)$  ist größter Fixpunkt von  $f$

## Beispiel: Natürliche Zahlen

Die Funktion

$$f(M) = \{0\} \cup M \cup \{n+1 \mid n \in M\}$$

definiert die natürlichen Zahlen.  $N_0$  ist  $\emptyset$ , und die Menge  $\mathbb{N}$  wird erzeugt, indem man  $f$  immer wieder auf  $N_0$  iteriert:

$$N_0 = \emptyset$$

$$N_1 = \{0\}$$

$$N_2 = \{0, 1\}$$

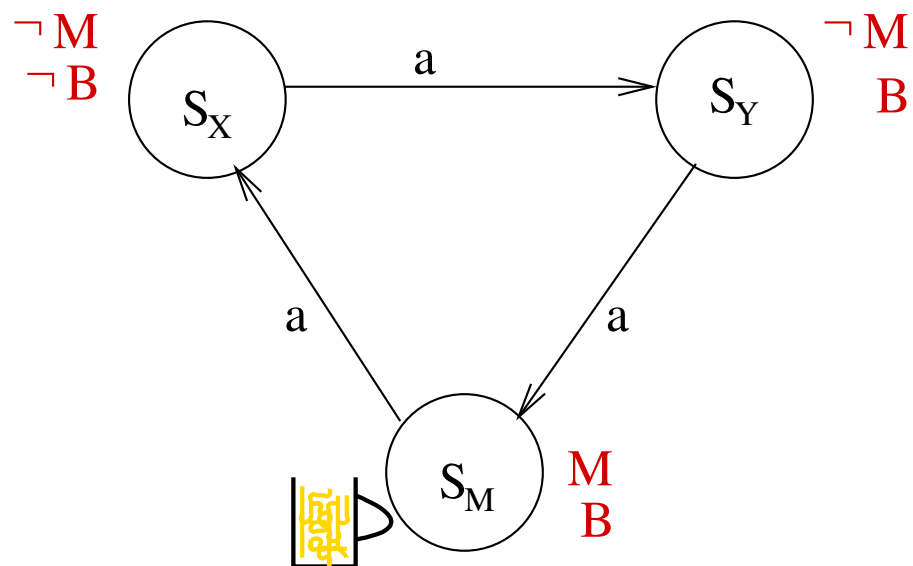
$$N_3 = \{0, 1, 2\}$$

$\vdots$

$$N_\omega = \mathbb{N}$$

□

## Der Weg zum Oktoberfest (I)



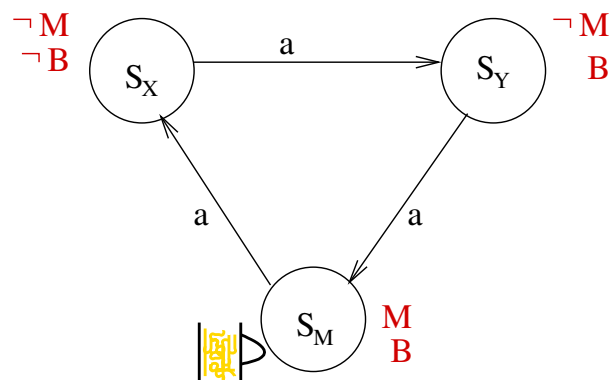
**Frage:** Von welchen Orten kann ich das Oktoberfest erreichen?

- $M$ : Der Ort/Zustand ist München.
- $B$ : Der Ort/Zustand hat einen Bahnhof.

**Antwort:** Von München aus oder von einem Ort aus, von dem ich per Zug nach München komme!

$$\Phi(Z) := M \vee (B \wedge \langle a \rangle Z)$$

## Der Weg zum Oktoberfest (II)



$$\Phi(Z) := M \vee (B \wedge \langle a \rangle Z)$$

1.  $Z_0 = \emptyset$
2.  $\Phi(Z_0) = \{S_M\} = Z_1$
3.  $\Phi(Z_1) = \{S_M, S_Y\} = Z_2$
4.  $\Phi(Z_2) = \{S_M, S_Y\} = Z_2$

$\Rightarrow Z_2 = \{S_M, S_Y\}$  ist die Lösung!

## Syntax und Monotonie von $\Phi(Z)$

- $P$  ist eine Formel (atomare Aussage).
- $Z$  ist eine Formel (Variable).
- $\neg\Phi$  ist eine Formel, wenn  $\Phi$  eine Formel ist (Negation).
- $\Phi_1 \wedge \Phi_2$  ist eine Formel, wenn  $\Phi_1$  und  $\Phi_2$  Formeln sind (Konjunktion).
- $\Phi_1 \vee \Phi_2$  ist eine Formel, wenn  $\Phi_1$  und  $\Phi_2$  Formeln sind (Disjunktion).
- $[a]\Phi$  ist eine Formel, wenn  $\Phi$  eine Formel ist ( $\Phi$  gilt nach jeder  $a$ -Aktion).
- $\langle a \rangle \Phi$  ist eine Formel, wenn  $\Phi$  eine Formel ist ( $\exists$  Aktion  $a$ , nach der  $\Phi$  gilt).
- $\nu Z.\Phi$  ist eine Formel, wenn  $\Phi$  eine Formel ist (größter Fixpunkt).
- $\mu Z.\Phi$  ist eine Formel, wenn  $\Phi$  eine Formel ist (kleinster Fixpunkt).

$\Phi(Z)$  ist monoton  $\Leftrightarrow Z$  kommt in  $\Phi$  unter einer geraden Anzahl von Negationen vor  
(sonst:  $Z$  oszilliert während der Iteration)

## Semantik der Formeln im $\mu$ -Kalkül

$$\|P\| = V(P)$$

$$\|Z\| = V(Z)$$

$$\|\neg\Phi\| = \Sigma - \|\Phi\|$$

$$\|\Phi_1 \wedge \Phi_2\| = \|\Phi_1\| \cap \|\Phi_2\|$$

$$\|\Phi_1 \vee \Phi_2\| = \|\Phi_1\| \cup \|\Phi_2\|$$

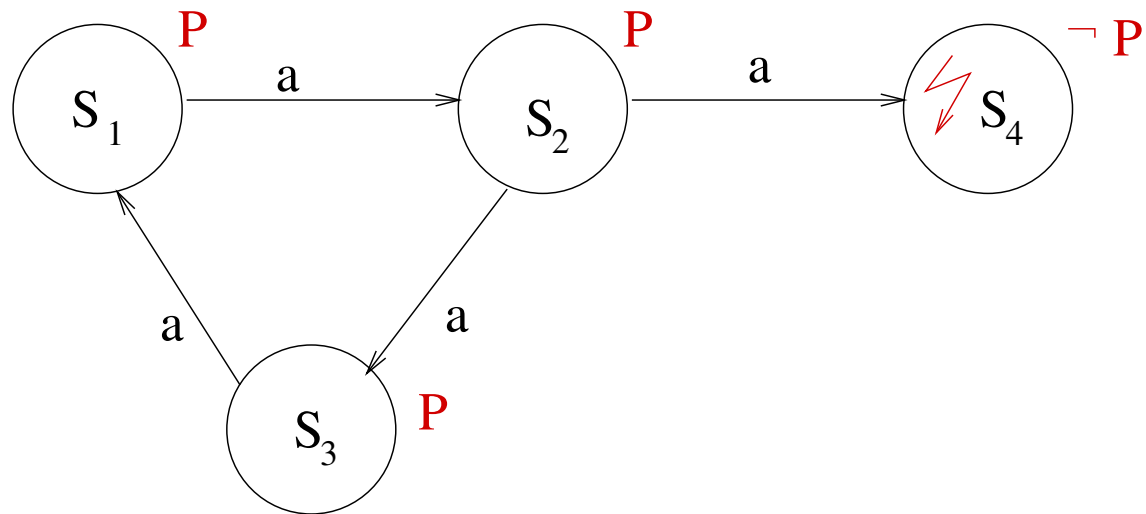
$$\|[a]\Phi\| = \{s \mid \forall t. s \xrightarrow{a} t \Rightarrow t \in \|\Phi\|\}$$

$$\|\langle a \rangle \Phi\| = \{s \mid \exists t. s \xrightarrow{a} t \wedge t \in \|\Phi\|\}$$

$$\|\nu Z. \Phi\| = \bigcup \{s \subseteq \Sigma \mid s \subseteq \|\Phi\|_{[Z:=s]}\}$$

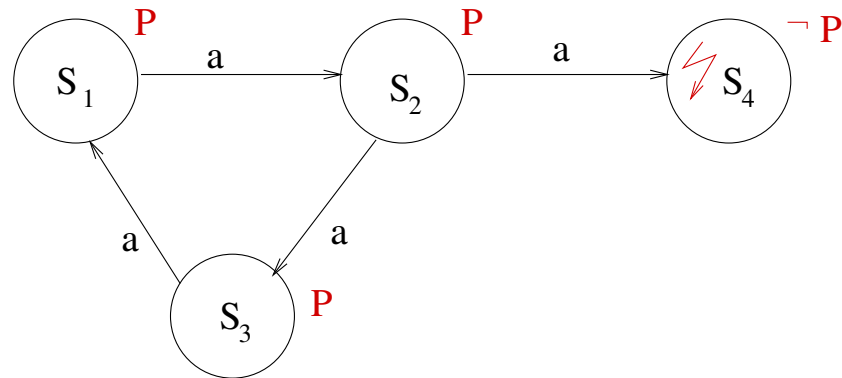
$$\|\mu Z. \Phi\| = \bigcap \{s \subseteq \Sigma \mid s \supseteq \|\Phi\|_{[Z:=s]}\}$$

## Zurück zum Beispiel (I)



- **Frage:** Wie lässt sich ausdrücken: "*P* muss immer gelten"?
- **Antwort:**  $\Phi(Z) = P \wedge [-]Z$
  
- **Frage:** Welche Zustände erfüllen diese Bedingung?
- **Antwort 1:** Der kleinste Fixpunkt macht keinen Sinn wegen  $\wedge$
- **Antwort 2:** Der größte Fixpunkt:  $\nu\Phi(Z)$

## Berechnung des größten Fixpunkts

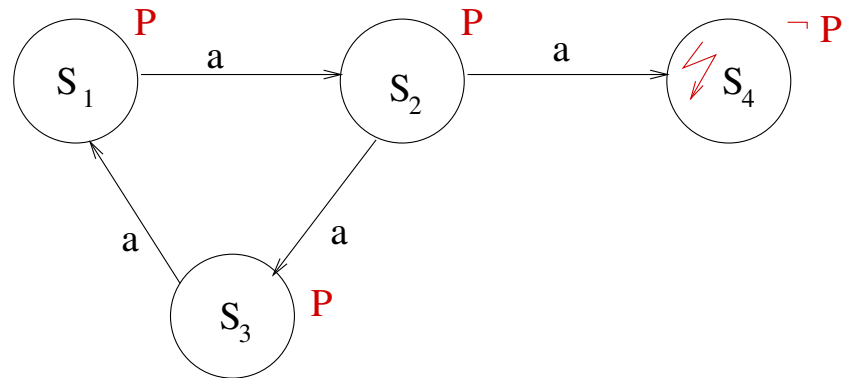


$$\Phi(Z) = P \wedge [-]Z$$

1.  $Z_0 = \Sigma = \{S_1, S_2, S_3, S_4\}$
2.  $\Phi(Z_0) = \{S_1, S_2, S_3\} \cap \{S_1, S_2, S_3, S_4\} = \{S_1, S_2, S_3\} = Z_1$
3.  $\Phi(Z_1) = \{S_1, S_2, S_3\} \cap \{S_1, S_3\} = \{S_1, S_3\} = Z_2$
4.  $\Phi(Z_2) = \{S_1, S_2, S_3\} \cap \{S_3\} = \{S_3\} = Z_3$
5.  $\Phi(Z_3) = \{S_1, S_2, S_3\} \cap \{\} = \{\} = Z_4$

⇒ Es gibt keinen Zustand, von dem aus  $P$  immer gilt!

$\langle - \rangle$  statt  $[-]$



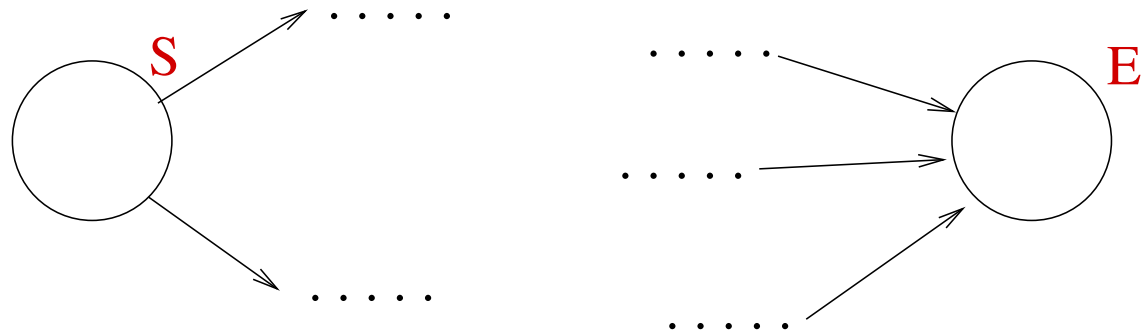
$$\Phi(Z) = P \wedge \langle - \rangle Z$$

1.  $Z_0 = \Sigma = \{S_1, S_2, S_3, S_4\}$
2.  $\Phi(Z_0) = \{S_1, S_2, S_3\} \cap \{S_1, S_2, S_3\} = \{S_1, S_2, S_3\} = Z_1$
3.  $\Phi(Z_1) = \{S_1, S_2, S_3\} \cap \{S_1, S_2, S_3\} = \{S_1, S_2, S_3\} = Z_1$

$\Rightarrow P \wedge \langle - \rangle Z$  bedeutet: alle Zustände, in denen  $P$  gilt und von denen man wieder in einen  $P$ -Zustand kommen kann.

$\Rightarrow$  Hierfür gibt es jetzt eine Lösung! (nämlich  $\{S_1, S_2, S_3\}$ )

## Terminierung eines Programms



Ist der Endzustand  $E$  vom Startzustand  $S$  aus erreichbar?

$$S \wedge (\mu Z. E \vee \langle - \rangle Z)$$

Intuitiv:

- Ausgehend von  $E$  werden alle Zustände "zurückgerechnet", von denen man zu  $E$  gelangt (also eine Art Breitensuche)
- Überprüfung, ob  $S$  in dieser Menge liegt

## Zusammenhang Fixpunktoperatoren – Sicherheitseigenschaften

” $P$  muss immer gelten.”

- Lösung war der größte Fixpunkt  $\nu$  in Kombination mit  $[-]$  (”für alle Aktionen”)
- Intuitiv: Von allen möglichen Zuständen werden ”Fehlerzustände” iterativ entfernt.
- $\nu$  mit  $[-]$  zeigt Sicherheit eines Systems
- $\nu$  mit  $\langle - \rangle$  zeigt Erreichbarkeit von sicheren Zuständen

”Ist der Endzustand  $E$  vom Startzustand  $S$  aus erreichbar?”

- Lösung war der kleinste Fixpunkt  $\mu$  in Kombination mit  $\langle - \rangle$  (”es gibt eine Aktion”)
- Intuitiv: Nacheinander werden alle Zustände ermittelt, bis die Eigenschaft erfüllt ist.
- $\mu$  zeigt Lebendigkeit eines Systems / Erreichbarkeit von Zuständen

## Es bleibt zu sagen, dass

- durch den abwechselnden Einsatz von Fixpunkten ( $\mu X.vY.\mu Z. \dots$ ) die Formeln im  $\mu$ -Kalkül sehr ausdrucksstark sind;
- der Kalkül durch seine Ausdrucksstärke die meisten anderen Logiken subsumiert (z.B. CTL);
- Model-Checking effizient ist (durch die Approximanten-Eigenschaft der Fixpunkte), in der Alternierungstiefe (s.o.) der Fixpunkte aber exponentiell ist;
- die Fragen nach Sicherheit der Elektronischen Geldbörse mit Hilfe des  $\mu$ -Kalküls beantwortet werden können;

## Ende des Vortrags

- Fragen
- Diskussion