Simple Homomorphism Verification Tool: Konzeption, theoretische Grundlagen, Beispiele

Humboldt-Universität zu Berlin

Andrey Bogdanov

21.04.2004

SHVT

- Inhalt
  - Übersicht
  - Eigenschaften: linear und annähernd erfüllte Lebendigkeits- und Sicherheitseigenschaften
  - Schlichte Homomorphismen
  - Vorgehensweise bei der Verifikation komplizierter Systeme
  - Wie bildet man schlichte Homomorphismen?
  - Asynchrone Produktautomaten (APA)
  - Beispiel
  - Zusammenfassung
  - Literaturliste

SHVT: Übersicht (1)

- S - Systemspezifikation,
- P – Eigenschaft des Systems,
- Q – Anforderung an das System

- LTS = beschriftetes Transitionssystem

SHVT: Übersicht (2)

- *Fragen:*
  - **F1.** Forderungen und Entsprechung ?
  - **F2.** Abstraktion ?
  - **F3.** Genug Information für eine erfolgreiche Verifikation ?

SHVT: Eigenschaften (1)

- Lokale Sprache des Systems
- Eigenschaft des Systems
  - Linear Eigenschaften
    - Definition,
    - Formelle Definition;
  - Annähernd erfüllte Eigenschaften
    - Definition,
    - 2 formale Definitionen,
    - Unformale Definition
  - Bespiel

SHVT: Eigenschaften (2)

- Lebendigkeitseigenschaften
  - Informelle Definition
- Sicherheitseigenschaften
  - Informelle Definition
- Aussage

- **F1** Beantwortet!

SHVT: Homomorphismen (1)

- Homomorphismus
  - Erinnerung,
  - Alphabetische Homomorphismen
  - **F2** beantwortet!
- Schlichte Homomorphismen
  - Linkquotient
  - Definition
  - Erklärung

SHVT: Homomorphismen (2)

- Warum soll der zu bildende Homomorphismus schlicht sein?
- Theorem
- **F3** beantwortet!

SHVT: Vorgehensweise

- Bilde L durch ein Spezifikationsverfahren,
- Wähle P aus,
- Bilde einen schlichten Homomorphismus h(L),
- Bekomme L‘ und P‘
- Prüfe, ob L‘ P‘ (annährend) entspricht

SHVT: Wie sind SH zu bilden?

- Am einfachsten:
  - Bilde einen Homomorphismus h(L),
  - Prüfe, ob h schlicht ist

- Theorem
  (ausreichende Bedingung der Schlichtheit des Homomorphismus)

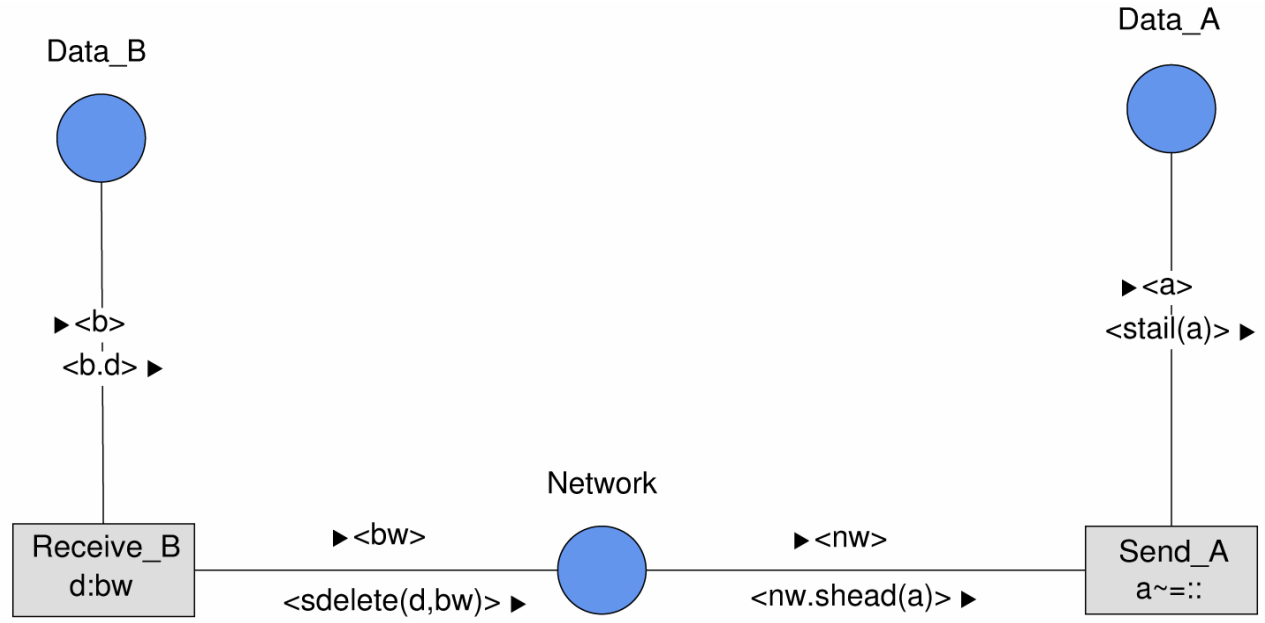
SHVT: APA (1)

- Definition
  - Zustandsmengen,
  - Elementarautomaten,
  - Nachbahrenrelation,
  - Startzustand;

- Erreichbarkeitsgraph des APA

SHVT: APA (2)

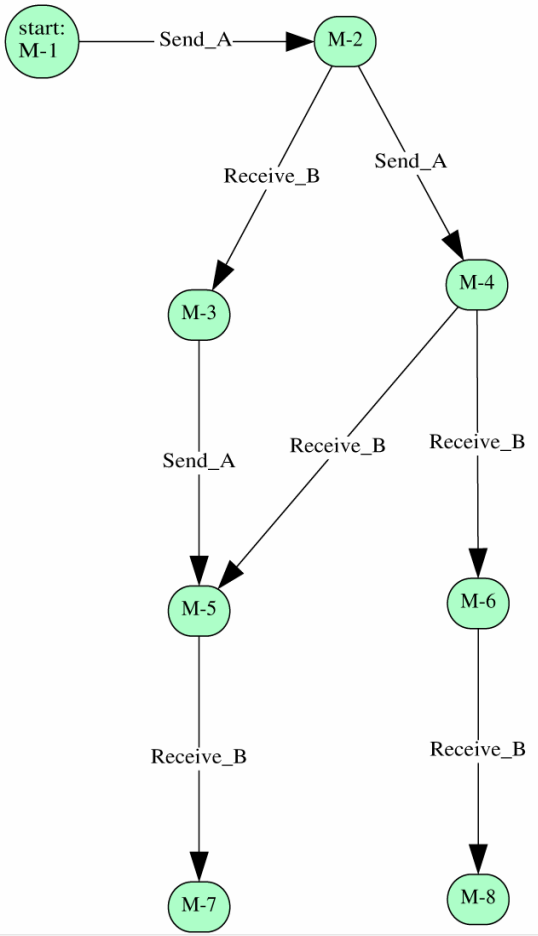
- Beispiel der Spezifizierung - APA



Data_A:
<(t1,data).(t2,data)>
Data_B:<::>
Network: <::>

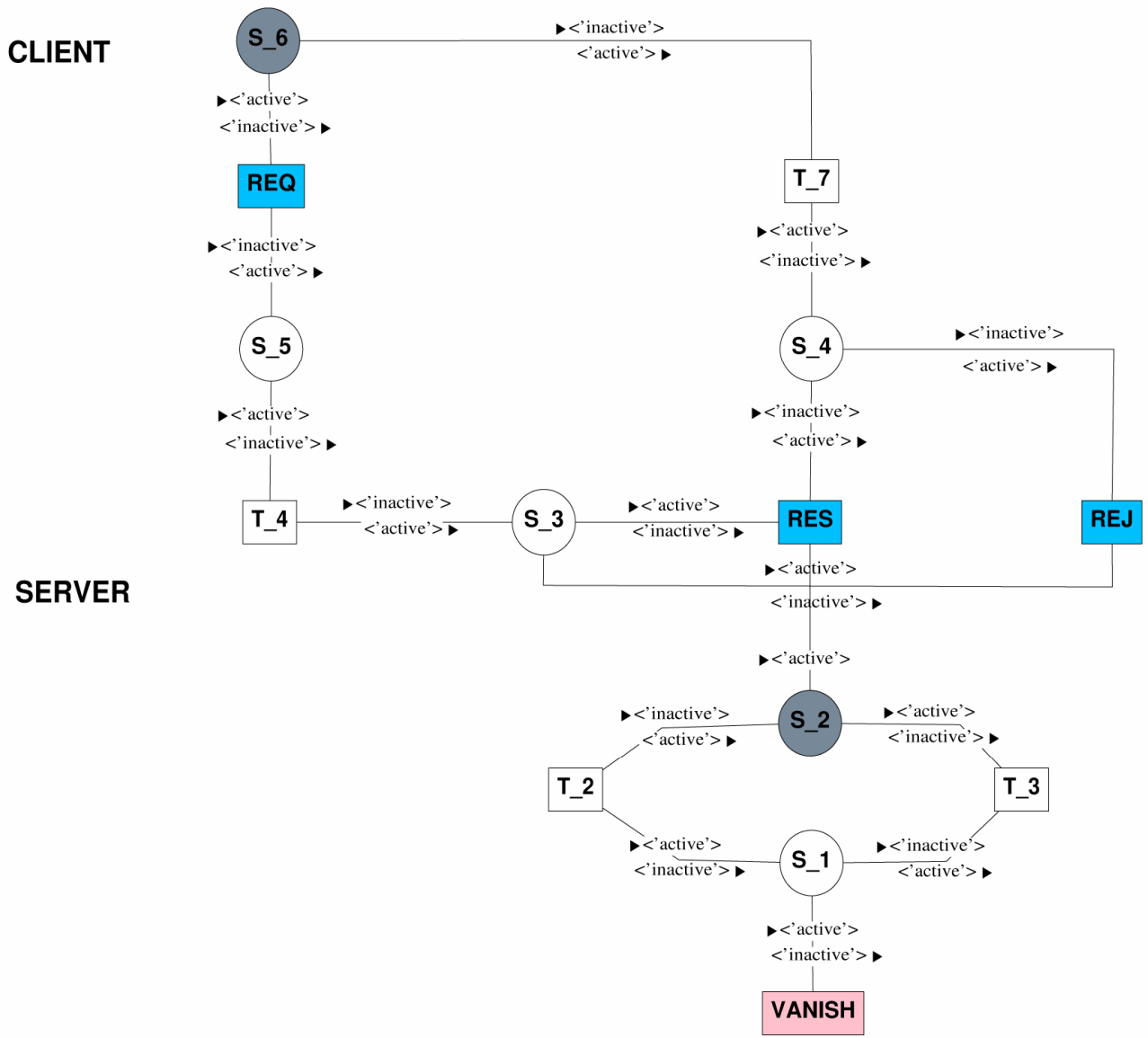
SHVT: APA (3)

- Beispiel der Spezifizierung - Erreichbarkeitsgraph



SHVT: Beispiel (1)

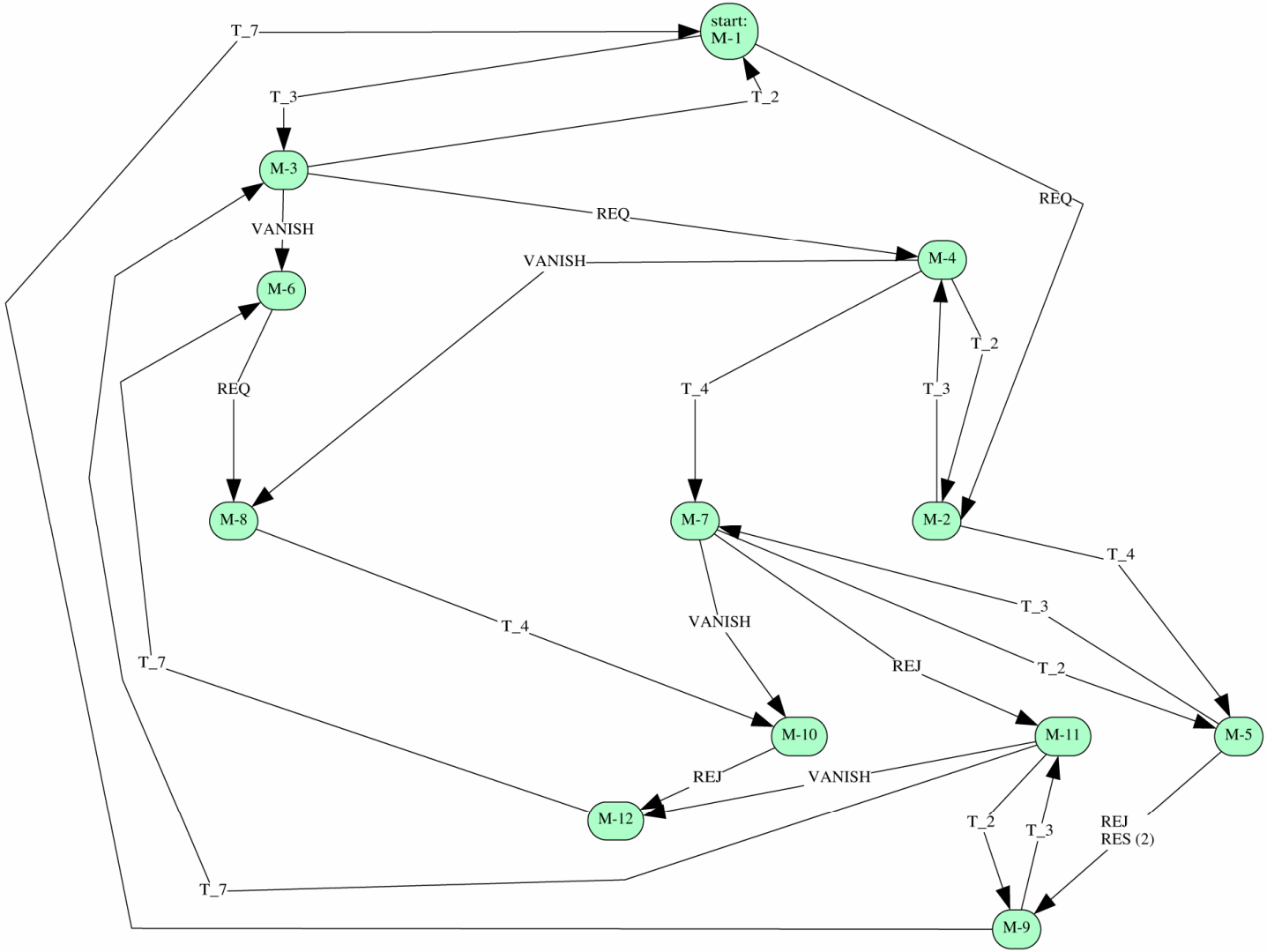
- Spezifikation durch APA



S_1:<inactive>
S_2:<*active*>
S_3:<inactive>
S_4:<inactive>
S_5:<inactive>
S_6:<*active*>

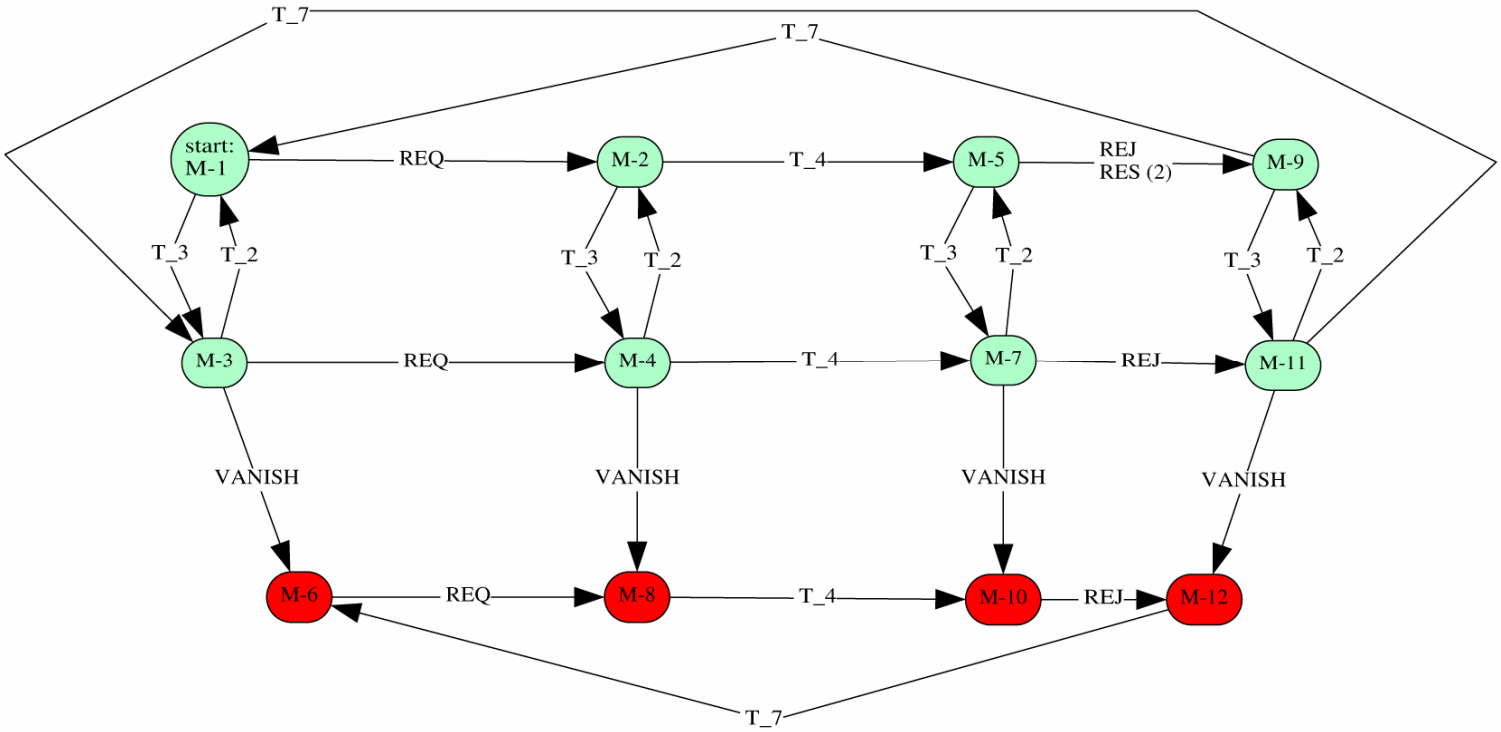
SHVT: Beispiel (2)

- LTS (raw!)


start:
M-1
M-2
M-3
M-4
M-5
M-6
M-7
M-8
M-9
M-10
M-11
M-12
T_7
T_3
T_2
REQ
VANISH
T_4
REJ
RES (2)

SHVT: Beispiel (3)

- LTS (umgestaltet!)



SHVT: Beispiel (4)

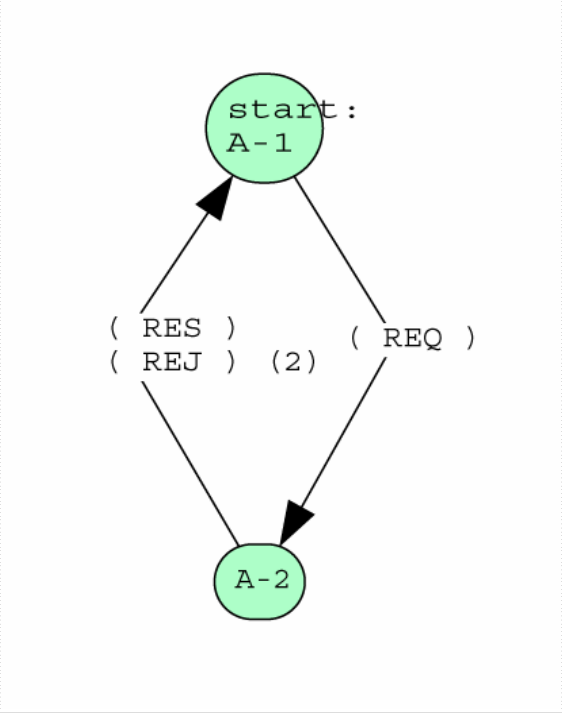
- „Falscher“ Homomorphismus
  - RES -> RES,
  - REQ -> REQ,
  - REJ -> REJ;
  - VANISH, T2, T3, T4, T7 -> ε

SHVT: Beispiel (5)

- Warum ist h(L) nicht als schlicht anerkannt?

SHVT: Beispiel (6)

- Abstraktion nach h

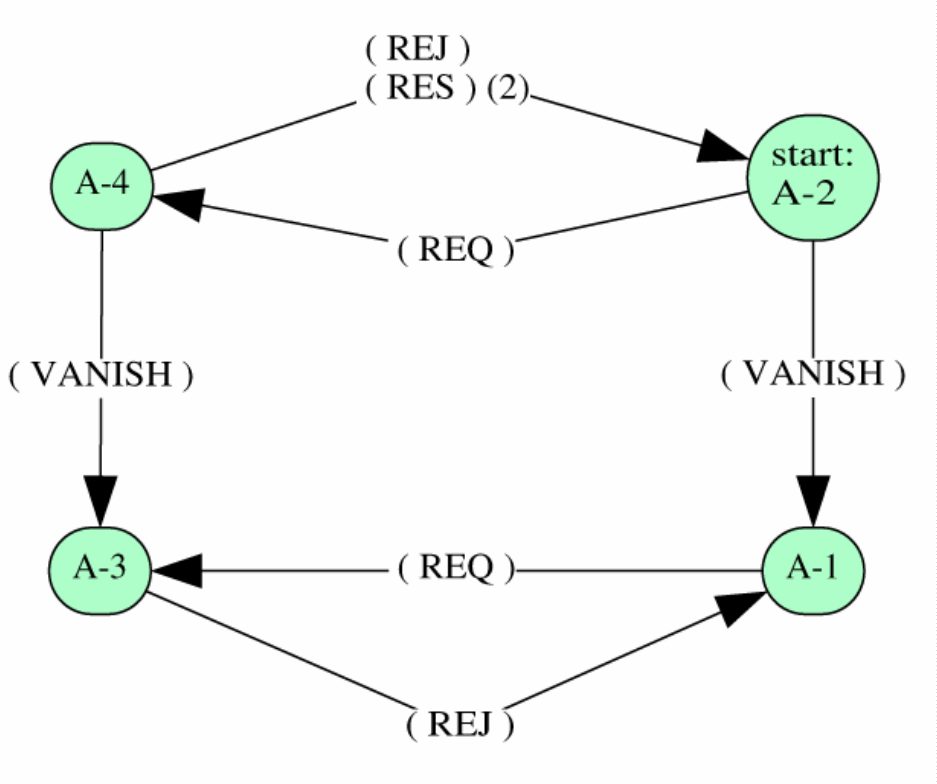


SHVT: Beispiel (7)

- „Richtiger“ Homomorphismus
  - RES -> RES,
  - REQ -> REQ,
  - REJ -> REJ,
  - VANISH -> VANISH;
  - T2, T3, T4, T7 -> ε

SHVT: Beispiel (8)

- „Richtige“ Abstraktion



SHVT: Zusammenfassung

+ Die Verifikationsmethode ist vom Spezifikationsverfahren unabhängig (*LTS*!)
+ Die Abstraktionsmethode ermöglicht die vollständige Analyse des Systems durch die erhebliche Reduzierung des Zustandsraums (*Homomorphismus*!)
- Dem Forscher steht nur eine begrenzte Klasse der Eigenschaften zur Verfügung (*annähernde Erfüllung der Eigenschaften*!)

SHVT: Literaturliste

- Fraunhofer Institute for Secure Telecooperation. SHVT Manual, 2003
- U.Nitsche, P.Ochsenschläger. Approximately satisfied properties of systems and simple language homomorphisms., 1995
- P.Ochsenschläger, R.Prinoth. Modellierung verteilter Systeme, 1995
- P.Ochsenschläger, J.Repp, R.Rieke. The SHVT – A Tutorial, 2002
- P.Ochsenschläger, J.Repp, R.Rieke. Abstraction and composition - a verification method for cooperation systems, 2002