1 Bounded-Model-Checking:

eine Anwendung der Aussagenlogik

Ziel: Model-Checking

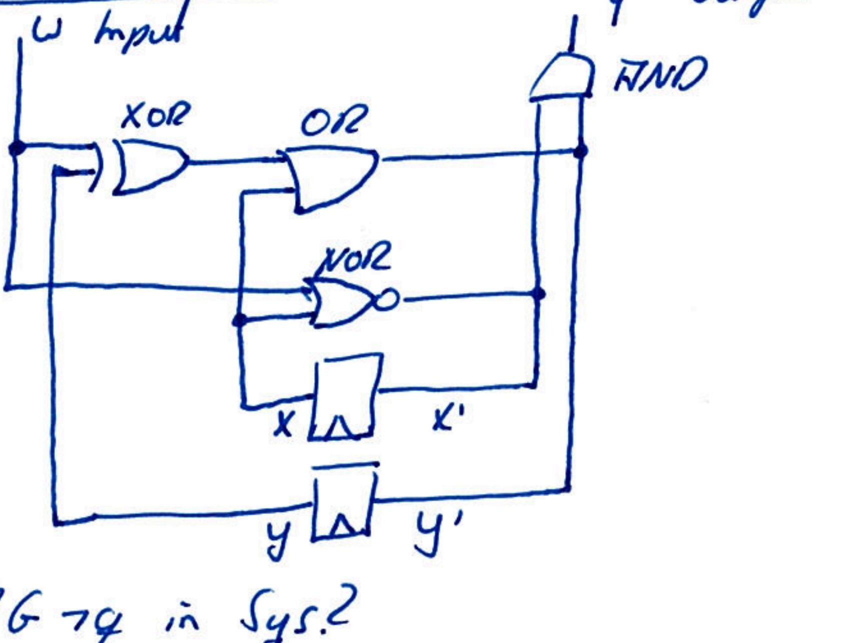
- Prüfe die Korrektheit von Schaltkreisen / Chips, seit 2000 auch Software
- Zwei Varianten:
  - ↳ Nachweis der Korrektheit (hier nicht)
  - ↳ Finden von Bugs

Ein Ansatz: Bounded-Model-Checking

- Zum Bug-Handling
- Finde Bugs in Ausführungen beschränkter Länge (erziele Vollständigkeit durch Iteration)
- Basierend auf SAT-Solvern (Erfüllbarkeitschecker für Aussagenlogik) (Wir entwickeln SAT-Solver in dieser Vorlesung.)
- Nicht zum Nachweis der Korrektheit gedacht.

Beispiel zum (iterativen) Bounded-Model-Checking:

Gegeben: Sys =



Initial:
$x = 0$
$y = 0$

Eigenschaft: $AG\neg q$

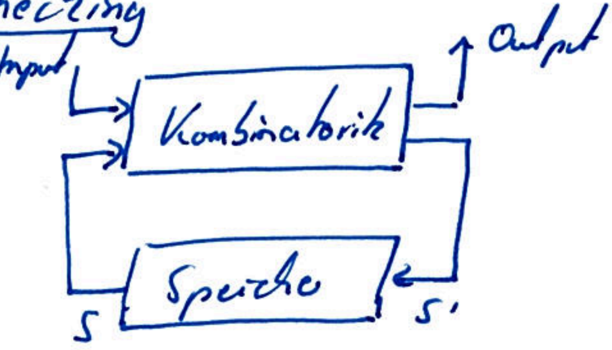
Frage: Gilt $AG\neg q$ in Sys?

Antwort: Nein, sehe in Takt 1 $w = 1$
und in Takt 2 $w = 0$.

Ziel: Bestimme solche Gegenbeispiele automatisch.

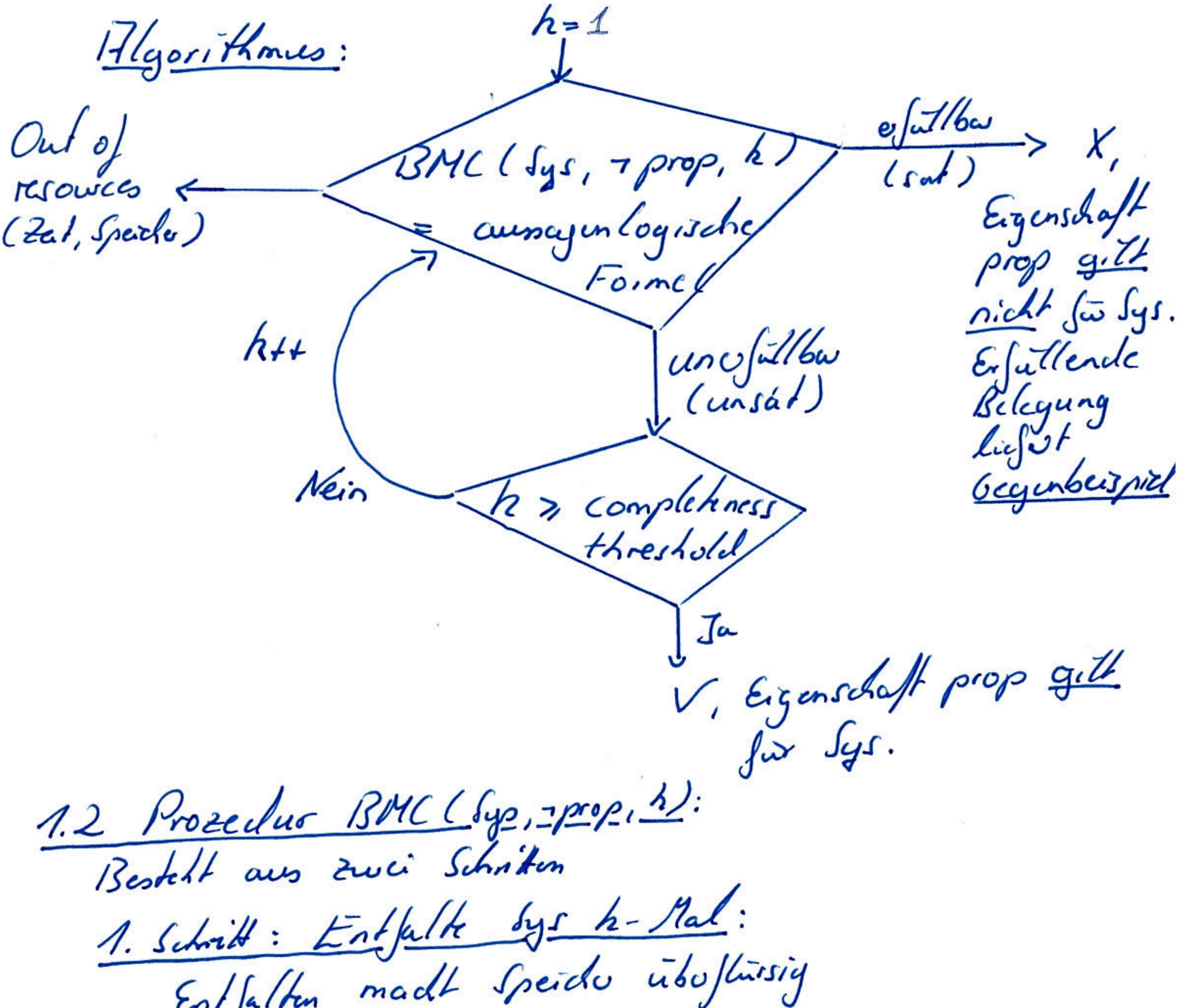
1.1 Iteratives Bounded-Model-Checking

Gegeben: · Schaltkreis Sys =



· Gewünschte Eigenschaft prop.

Algorithmus:

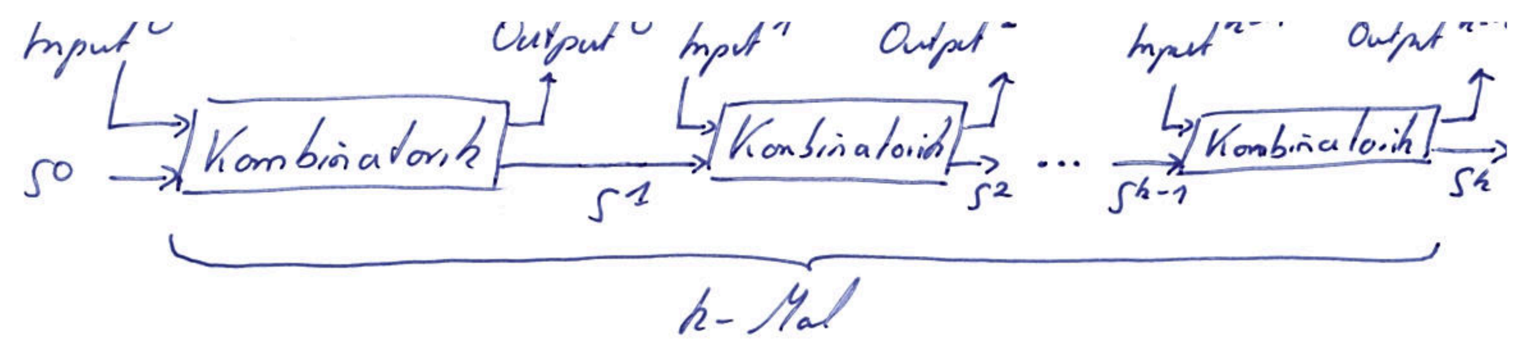


1.2 Prozedur BMC(Sys, ¬prop, h):

Besteht aus zwei Schritten

1. Schritt: Entfalte Sys h-Mal:

Entfalten macht Speicher überflüssig

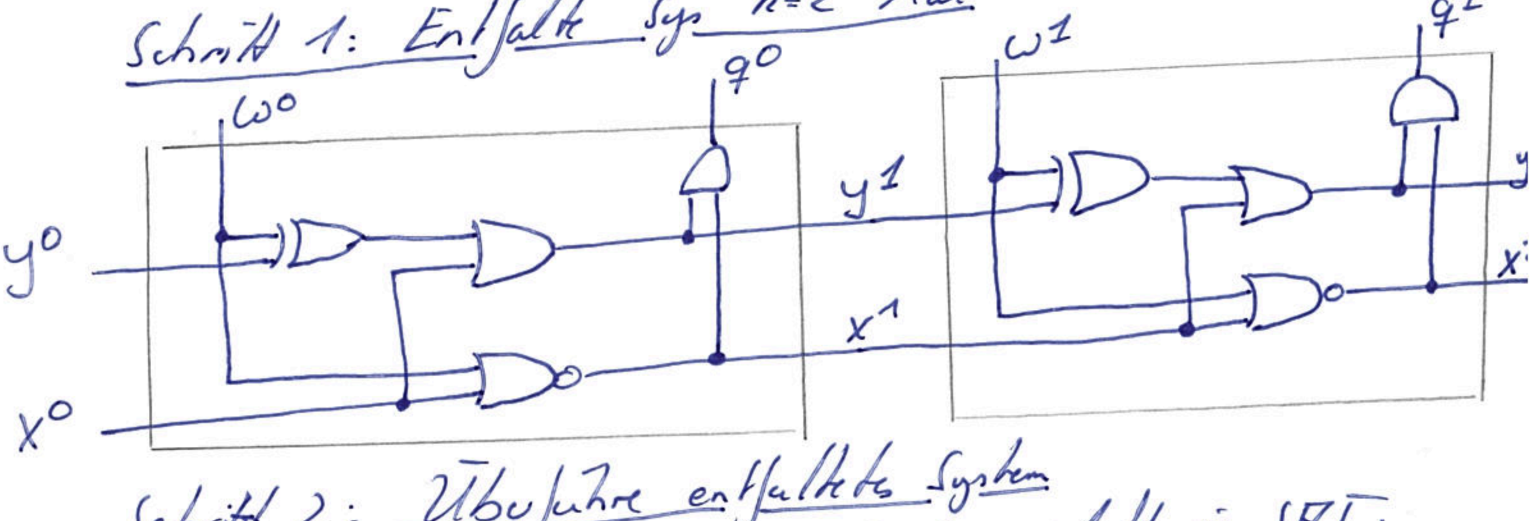


2. Schritt: Überführe entfaltetes System und negierte Eigenschaft in SAT (in aussagenlogische Formel)

- Jedes Eingabesignal, Ausgabesignal und jeder Speicherwert pro Takt ergibt eine aussagenlogische Variable
- Der kombinatorische Schaltkreis ist eine aussagenlogische Formel
- Die Negation der Eigenschaft wird als Konjunktion zur Formel hinzugefügt

Prozedur BMC am Beispiel:

Schritt 1: Entfalte Sys $k=2$-Mal



Schritt 2: Überführe entfaltetes System mit negierter Eigenschaft in SAT:

Initialwert des Speichers:
$$\neg y^0$$
$$\land \neg x^0$$

Erste Kopie des Schaltwerks:
$$\land\ y^1 \Leftrightarrow (w^0 \oplus y^0) \lor x^0$$
$$\land\ x^1 \Leftrightarrow \neg(x^0 \lor w^0)$$
$$\land\ q^0 \Leftrightarrow x^1 \land y^1$$

Zweite Kopie:
$$\land\ y^2 \Leftrightarrow (w^1 \oplus y^1) \lor x^1$$
$$\land\ x^2 \Leftrightarrow \neg(x^1 \lor w^1)$$
$$\land\ q^1 \Leftrightarrow x^2 \land y^2$$

Negation der Eigenschaft:
$$\land\ (q^0 \lor q^1)$$

Prüfe resultierende Formel auf Erfüllbarkeit
im iterativen Bounded-Model-Checking-Algorithmus:

- Wähle (das erledigt der SAT-Solver):

  $\omega^0 = 1$ und $\omega^1 = 0$

  Dann:

  $y^1 = 1$ $\qquad$ $y^2 = 1$

  $x^1 = 0$ $\qquad$ $x^2 = 1$

  $q^0 = 0$ $\qquad$ $q^1 = 1$

  Die Formel BMC(Sys, $\neg$prop, 2) ist erfüllbar,
  also ist die Eigenschaft $AG \neg q$ verletzt.

- Beachte: Die erfüllende Belegung liefert
  ein Gegenbeispiel für $AG \neg q$:
  - wähle im ersten Takt $\omega = 1$, denn $\omega^0 = 1$
  - wähle im zweiten Takt $\omega = 0$, denn $\omega^1 = 0$.