



Test und Verlässlichkeit 3: Themenspezifische Einführung in die Wahrscheinlichkeitsrechnung

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal
7. Mai 2025



Inhalt Foliensatz 3

Wahrscheinlichkeit

- 1.1 Definition, Abschätzung
- 1.2 Verkettete Ereignisse
- 1.3 CVA-Graph
- 1.4 Fehlerbäume
- 1.5 Markov-Ketten

Fehlernachweis

- 2.1 Nachweis & Zuverlässigkeit
- 2.2 Service mit Gedächtnis
- 2.3 Fehler und Modellfehler

Operationsprofil

- 3.1 Testauswahl
- 3.2 Zuverlässigkeitsgewinn
- 3.3 DIC-Test mit Bitwichtung
- 3.4 Testsuche für Software

Fehlerbeseitigung

- 4.1 Ersatz
- 4.2 Reparatur
- 4.3 Reifeprozesse

Fehlerentstehung



Verlässlichkeit und alle ihre Teilaspekte werden in der Vorlesung durch Zählwerte bzw. Häufigkeiten positiver und negativer Erfahrungen beschrieben. Für große Zählwerte streben Häufigkeiten gegen Wahrscheinlichkeiten.

Für die Arbeit mit Wahrscheinlichkeiten bietet die Mathematik einen großen Werkzeugkasten, von dem wir auch schon einiges genutzt haben.



Wahrscheinlichkeit



Definition, Abschätzung



3.3 Wahrscheinlichkeit

Wird ein Zufallsexperiment unter konstanten Versuchsbedingungen n -mal wiederholt, so strebt die relative Häufigkeit $\#A/n$, dass ein Ereignis A eintritt, gegen die Eintrittswahrscheinlichkeit:

$$\mathbb{P}[A] = \lim_{n \rightarrow \infty} \frac{\#A}{n} \quad (3.1)$$

Viele der bisher eingeführten Kenngrößen streben für große Zählwerte gegen Wahrscheinlichkeiten:

- Anteil der erbrachten Service-Leistungen η_{DS}
- Fehlfunktionsrate ζ ,
- Fehlerabdeckung FC , ...

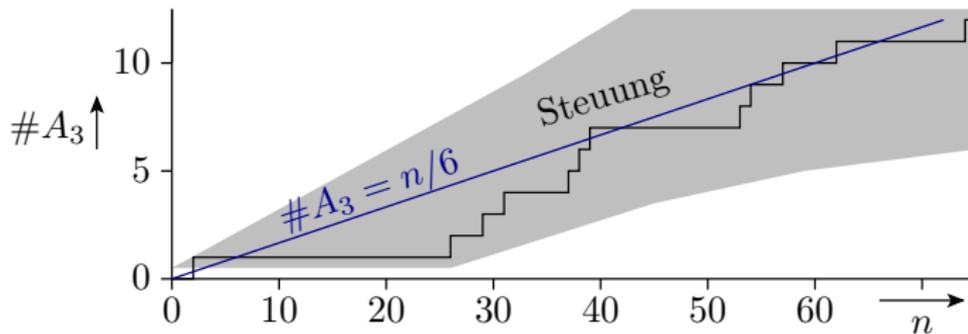
Die Wahrscheinlichkeit ist die beste Vorhersage für die zu erwartende relative Häufigkeit künftiger Versuche. Deshalb hier eine themenspezifische Einführung.

Anschließend speziell Wahrscheinlichkeiten für Fehlernachweis, Fehlerbeseitigung und Fehlerentstehung.

$\mathbb{P}[A]$	Eintrittswahrscheinlichkeit von Ereignis A .
$\#A$	Anzahl, wie oft Ereignis A eingetreten ist.

3.4 Beispiel: Würfeln einer 3

- Mögliche Ergebnisse: 1, 2, ..., 6, günstiges Ergebnis: 3
- Anzahl der Versuche: n



$$\mathbb{P}[A_3] = \lim_{n \rightarrow \infty} \frac{\#A_3}{n} = \frac{1}{6}$$

Satz 1

Wenn die möglichen Ereignisse eines Zufallsexperiments gleichmäßig sind, ist die Wahrscheinlichkeit der Anteil der günstigen Ereignisse.



Verkettete Ereignisse



3.5 Verkettete Ereignisse

Komplexe Ereignisse lassen sich oft durch logische und andere Verknüpfungen einfacher zu untersuchender Ereignisse beschreiben. Im nachfolgenden wird bei jedem Experiment zweimal gewürfelt (Ereignisse A und B , Wertebereich jeweils $\{1, 2, \dots, 6\}$). Daraus werden mit Vergleichsoperatoren die zweiwertigen Ereignisse C und D gebildet und diese einmal UND- und einmal ODER verknüpft und gezählt.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	...	20	...	40
A	6	1	5	4	1	1	2	2	4	6	4	3	1		6		5
B	6	5	6	2	1	3	3	6	4	5	1	3	1		4		3
$C = (A > 3)$	1	0	1	1	0	0	0	0	1	1	1	0	0		1		1
$D = (B < 3)$	0	0	0	1	1	0	0	0	0	0	1	0	1		0		0
$E = (C \wedge D)$	0	0	0	1	0	0	0	0	0	0	1	0	0		0		0
$F = (C \vee D)$	1	0	1	1	1	0	0	0	1	1	1	0	1		1		1
$\#C$	1	1	2	3	3	3	3	3	4	5	6	6	6		11		21
$\#D$	0	0	0	1	2	2	2	2	2	2	3	3	4		6		9
$\#E$	0	0	0	1	1	1	1	1	1	1	2	2	2		5		6
$\#F$	1	1	2	3	4	4	4	4	5	6	7	7	8		13		24



3.6 Abschätzung der relativen Häufigkeiten

Ereignis	rel. Häufigkeit	Wahrscheinlichkeit
$C = (A > 3)$	$21/40 = 53\%$	$3/6 = 50\%$
$D = (B < 3)$	$9/40 = 23\%$	$2/6 = 33\%$
$E = (C \wedge D)$	$6/40 = 15\%$	$6/36 = 17\%$
$F = (C \vee D)$	$24/40 = 60\%$	$24/36 = 67\%$

Von den 6 möglichen gleichwahrscheinlichen Würfelergebnissen sind für $C = (A > 2)$ drei und $D = (A < 3)$ 2 günstig. Die verketteten Ereignisse E und F haben $6^2 = 36$ gleichwahrscheinliche mögliche Ergebnisse, von denen für $E = C \wedge D$ sechs und für $F = C \vee D$ 24 günstig sind.

Fakt

Die Abschätzung über den Anteil der günstigen Ereignisse erscheint im Beispiel deutlich einfacher. Zählversuche mit nur 40 Wiederholung haben Schätzfehlerfehler von im Beispiel $\approx 10\%$ des Wahrscheinlichkeitswerts (siehe später Abschn. 4.2.5).



3.7 Bedingte Wahrscheinlichkeiten

Bei einer bedingten Wahrscheinlichkeit werden nur die Versuche und Ereignisse gezählt, die eine Bedingung erfüllen*, im. Beispiel:

$$E = C \vee D \text{ unter der Bedingung } C \wedge D = 0.$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Σ	Σ
C	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	0	1	1	11	7
D	0	0	0	1	1	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	6	2
$C \vee D$	1	0	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1	0	1	1	13	9

■ nicht mitgezählte Ereignisse bzw. Summe ohne diese Ereignisse

Sowohl die Anzahl der gezählten Versuche als auch die günstigen Ereignisse verringern sich um die vier nicht mitzuzählenden Ereignisse mit $C \wedge D = 1$.

Fakt

Zusatzbedingungen, die die Zählung beeinflussen, sind bei Abschätzungen von Wahrscheinlichkeiten zu berücksichtigen. Dabei ist es unwichtig, ob nicht mitzuzählende Ereignisse eintreten können oder nicht.



3.8 Regeln für bedingte Wahrscheinlichkeit

Wahrscheinlichkeit, dass A unter Bedingung B eintritt:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]} \quad (3.2)$$

Wahrscheinlichkeit, dass B unter Bedingung A eintritt:

$$\mathbb{P}[B|A] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[A]}$$

Satz von Bayes:

$$\mathbb{P}[B|A] = \mathbb{P}[A|B] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]} \quad (3.3)$$

A, B	Ereignisse.
$\mathbb{P}[A B]$	Wahrscheinlichkeit von Ereignis A unter der Bedingung B .
$\mathbb{P}[A \wedge B]$	Wahrscheinlichkeit von Ereignis A und B .
$\mathbb{P}[A \vee B]$	Wahrscheinlichkeit von Ereignis A oder B .

Beispiel 3.1: Fehlklassifizierung Corona-Test

- Zufallsvariable A Person infiziert: $\mathbb{P}[A] = 10^{-4}$
- Zufallsvariable B Test positiv: $\mathbb{P}[B] = 10^{-2}$
- Wahrscheinlichkeit Test positiv, wenn eine Person infiziert ist:
 $\mathbb{P}[B|A] = 99\%$

Mit welcher Wahrscheinlichkeit ist eine Person infiziert, wenn der Test positiv ist?

$$\mathbb{P}[A] = 10^{-4}, \mathbb{P}[B] = 10^{-2}, \mathbb{P}[B|A] = 99\%, \text{ gesucht } \mathbb{P}[A|B]$$



$\mathbb{P}[A] = 10^{-4}$, $\mathbb{P}[B] = 10^{-2}$, $\mathbb{P}[B|A] = 99\%$, gesucht $\mathbb{P}[A|B]$

Die Wahrscheinlichkeit $\mathbb{P}(A|B)$, dass eine Person infiziert, wenn der Test positiv ist:

$$\mathbb{P}[A|B] = \mathbb{P}[B|A] \cdot \frac{\mathbb{P}[A]}{\mathbb{P}[B]} = 99\% \cdot \frac{10^{-4}}{10^{-2}} \approx 1\%$$

Wenn der Test positiv ist, dann ist das mit den gegebenen Wahrscheinlichkeiten in 99% der Fälle ein Fehlalarm.



$$\mathbb{P}[A] = 10^{-4}, \mathbb{P}[B] = 10^{-2}, \mathbb{P}[B|A] = 99\%, \text{ gesucht } \mathbb{P}[A|B]$$

Kontrolle mit Beispielwerten:

		Test positiv	Test negativ	Summe	
infizierte Personen	$0,99\%$	9.900	100	10.000	10^{-4}
nicht infiz. Pers.	$\mathbb{P}(A B)$	≈ 1 Mio.	≈ 99 Mio.	99,99 Mio.	$\mathbb{P}(A)$
Summe		1 Mio.	99 Mio.	100 Mio.	
		1%	$\mathbb{P}(B)$		

Person infiziert:

$$\mathbb{P}[A] = \frac{10.000}{100 \text{ Mio.}} \approx 10^{-4}$$

Test positiv:

$$\mathbb{P}[B] = \frac{1 \text{ Mio.}}{100 \text{ Mio.}} = 0,99\%$$

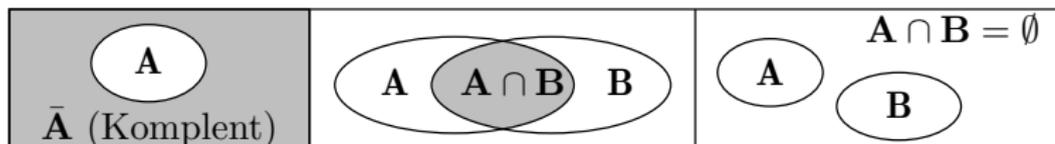
Test positiv, wenn Person infiziert:

$$\mathbb{P}[B|A] = \frac{9.900}{10.000} = 99\%$$

Person infiziert, wenn Test positiv:

$$\mathbb{P}[A|B] = \frac{9.900}{1 \text{ Mio.}} = 0,99\% \checkmark$$

3.10 NOT / UND / ODER von Ereignissen



- NOT (Nichteintrittswahrscheinlichkeit):

$$\mathbb{P}[\bar{A}] = 1 - \mathbb{P}[A] \quad (3.4)$$

- UND (gleichzeitiges Eintreten der Ereignisse A und B)
 - stochastische Unabhängigkeit:

$$\mathbb{P}[A|B] = \mathbb{P}(A) = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]}$$

$$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B] \quad (3.5)$$

- sich ausschließende Ereignisse:

$$\mathbb{P}[A \wedge B] = 0 \quad (3.6)$$

A, B	Ereignismengen.
\cup, \emptyset	Vereinigungsmenge, leere Menge.
A, \bar{A}	Ereignisse.



ODER (alternatives Eintreten von A und B):

$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A \wedge B]$$

- stochastische Unabhängigkeit:

$$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$

$$\mathbb{P}(A \vee B) = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A] \cdot \mathbb{P}[B] \quad (3.7)$$

- sich ausschließende Ereignisse:

$$\mathbb{P}[A \wedge B] = 0$$

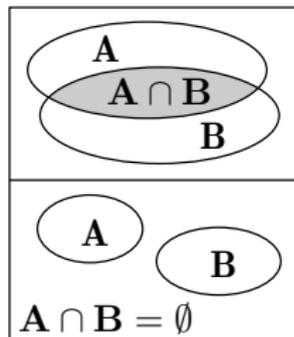
$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] \quad (3.8)$$

- Für mehr als zwei unabhängigen Ereignissen ist es einfacher, zuerst nach DeMorgan ODER auf UND zurückzuführen:

$$A \vee B \vee C = \overline{\overline{A} \wedge \overline{B} \wedge \overline{C}}$$

$$\mathbb{P}[A \vee B \vee C] = 1 - (1 - \mathbb{P}[A]) \cdot (1 - \mathbb{P}[B]) \cdot (1 - \mathbb{P}[C]) \quad (3.9)$$

Vereinigungsmenge



A, B, C

Ereignisse.

$\mathbb{P}[\dots]$

Eintrittswahrscheinlichkeit des Ereignisses ...



3.12 Abhängig, aber nicht ausschließend

Für abhängige, sich nicht ausschließende Ereignisse gibt es keine einfache Abschätzung.

Workaround:

- Umformung der logischen Ausdruck in UND, ODER, Nicht
- unabhängiger oder sich ausschließender Terme, z.B.:

$$A \oplus B = \underbrace{(A \wedge \bar{B})}_{\text{unabhängig}} \vee \underbrace{(\bar{A} \wedge B)}_{\text{unabhängig}}$$

──────────────────
gegenseitig ausschließend

$$\mathbb{P}[A \oplus B] = \mathbb{P}[A] \cdot (1 - \mathbb{P}[B]) + (1 - \mathbb{P}[A]) \cdot \mathbb{P}[B]$$



Beispiel 3.2: Unabhängiger Fehlernachweis

Ein System enthält drei unabhängig nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

Hilfestellung:

- Definition von Ereignissen F_i für Fehler i nachweisbar.
- Definition von Ereignissen A , B , C und D für die günstigen Ereignisse je Aufgabenteil und Beschreibung durch logische Gleichungen.
- Umformung in UND unabhängiger und ODER sich ausschließender Ereignisse. Nutzung Gl. (3.4), (3.5) und (3.8).

- Mit welcher Wahrscheinlichkeit werden alle Fehler nachgewiesen?*
- Mit welcher Wahrscheinlichkeit wird kein Fehler nachgewiesen?*
- Mit welcher Wahrsch. wird mindestens ein Fehler nachgewiesen?*
- Mit welcher Wahrsch. werden genau zwei Fehler nachgewiesen?*

$\mathbb{P}[F_i]$ Wahrscheinlichkeit, dass Fehler i nachweisbar ist.



Ein System enthält drei unabhängig nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

a) *Mit welcher Wahrscheinlichkeit werden alle Fehler nachgewiesen?*

Alle Fehler werden nachgewiesen, wenn der erste und der zweite und der dritte Fehler nachgewiesen wird. UND unabhängiger Ereignisse:

$$\begin{aligned}\mathbb{P}[F_i] &= p_i \\ A &= F_1 \wedge F_2 \wedge F_3 \\ \mathbb{P}[A] &= \mathbb{P}[F_1] \cdot \mathbb{P}[F_2] \cdot \mathbb{P}[F_3] \\ &= p_1 \cdot p_2 \cdot p_3 = 10\% \cdot 5\% \cdot 20\% = 0,1\%\end{aligned}$$

$\mathbb{P}[A]$ Wahrscheinlichkeit, dass alle Fehler nachgewiesen werden.



Ein System enthält drei unabhängig nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

b) *Mit welcher Wahrscheinlichkeit wird kein Fehler nachgewiesen?*

Kein Fehler wird nachgewiesen, wenn nicht der erste oder der zweite oder der dritte Fehler nachgewiesen wird. Umformung nach der demorganschen Regel in UND unabhängiger Ereignisse:

$$\begin{aligned} B &= \overline{F_1 \vee F_2 \vee F_3} = \bar{F}_1 \wedge \bar{F}_2 \wedge \bar{F}_3 \\ \mathbb{P}[B] &= (1 - \mathbb{P}[F_1]) \cdot (1 - \mathbb{P}[F_2]) \cdot (1 - \mathbb{P}[F_3]) \\ &= (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) = 90\% \cdot 95\% \cdot 80\% = 68,4\% \end{aligned}$$

$\mathbb{P}[B]$ Wahrscheinlichkeit, dass kein Fehler nachgewiesen wird.



Ein System enthält drei unabhängig nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

c) *Mit welcher Wahrsch. wird mindestens ein Fehler nachgewiesen?*

Mindestens ein Fehler wird nachgewiesen, wenn nicht kein Fehler nachweisbar ist:

$$\begin{aligned} C &= \bar{B} \\ \mathbb{P}[C] &= 1 - \mathbb{P}[B] = 1 - 68,4\% = 31,6\% \end{aligned}$$

$\mathbb{P}[C]$ Wahrscheinlichkeit, dass mindestes ein Fehler nachgewiesen wird.



Ein System enthält drei unabhängig nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

d) *Mit welcher Wahrsch. werden genau zwei Fehler nachgewiesen?*

Genau 2 Fehler werden nachgewiesen, wenn

- die ersten beiden und der dritte nicht,
- die zweiten beiden und der erste nicht oder
- der erste und der dritte, aber nicht der zweite

nachgewiesen werden. Alle UND-verknüpften Ereignisse sind unabhängig und die ODER-verknüpften Terme schließen sich gegenseitig aus:

$$\begin{aligned} D &= (F_1 \wedge F_2 \wedge \bar{F}_3) \vee (\bar{F}_1 \wedge F_2 \wedge F_3) \vee (F_1 \wedge \bar{F}_2 \wedge F_3) \\ \mathbb{P}[D] &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\ &= 10\% \cdot 5\% \cdot 80\% + 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% = 3,2\% \end{aligned}$$

$\mathbb{P}[D]$ **Wahrscheinlichkeit, dass genau zwei Fehler nachgewiesen werden.**



Beispiel 3.3: Abhängiger Fehlernachweis

Die Nachweiswahrscheinlichkeit für Fehler 1 beträgt unabhängig vom Nachweis von Fehler 2 $p_1 = 10\%$. Die Nachweiswahrscheinlichkeit für Fehler 2 beträgt, wenn Fehler 1 nachgewiesen, $p_2 = 20\%$ und sonst 0, d.h. der Nachweis von Fehler 2 impliziert den Nachweis von Fehler 1.

$p_1 = 10\%$, $p_2 = 20\%$, wenn Fehler 1 nachweisbar, sonst 0

Wie groß sind die Wahrscheinlichkeiten, dass 0, 1 oder 2 Fehler nachweisbar sind?

Hilfestellung: Definition von Ereignissen F_i für Fehler i nachweisbar und E_i für i Fehler nachweisbar.



$p_1 = 10\%$, $p_2 = 20\%$, wenn Fehler 1 nachweisbar, sonst 0

Wie groß sind die Wahrscheinlichkeiten, dass 0, 1 oder 2 Fehler nachweisbar sind?

Kein Fehler ist nachweisbar, wenn Fehler 1 nicht nachweisbar ist.
Nachweis Fehler 2 und nicht Fehler 1 ausgeschlossen:

$$\begin{aligned}E_0 &= \bar{F}_1 \\ \mathbb{P}(E_0) &= 1 - \mathbb{P}[F_1] = 1 - p_1 = 1 - 10\% = 90\%\end{aligned}$$

Ein Fehler ist nachweisbar, wenn der erste Fehler nachweisbar ist und der zweite nicht:

$$\begin{aligned}E_1 &= F_1 \wedge \bar{F}_2 \\ \mathbb{P}(E_1) &= p_1 \cdot (1 - p_2) = 10\% \cdot 80\% = 8\%\end{aligned}$$



$p_1 = 10\%$, $p_2 = 20\%$, wenn Fehler 1 nachweisbar, sonst 0

Wie groß sind die Wahrscheinlichkeiten, dass 0, 1 oder 2 Fehler nachweisbar sind?

Zwei Fehler sind nachweisbar, wenn beide Fehler nachweisbar sind:

$$\begin{aligned} E_2 &= F_1 \wedge F_2 \\ \mathbb{P}(E_2) &= p_1 \cdot p_2 = 10\% \cdot 20\% = 2\% \end{aligned}$$

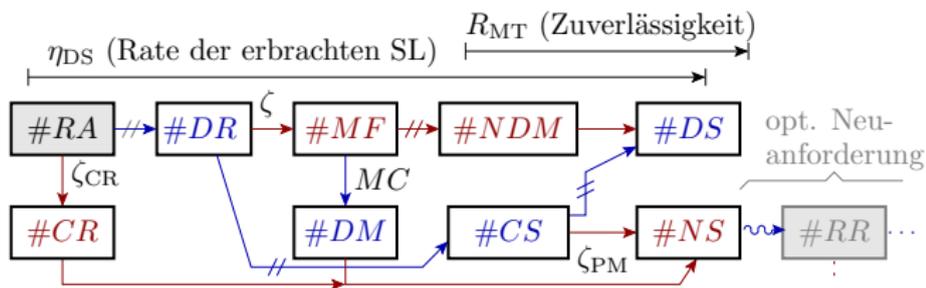
Probe: Die Summe der Wahrscheinlichkeiten der drei möglichen Ergebnisse muss 1 sein:

$$\mathbb{P}[E_0] + \mathbb{P}[E_1] + \mathbb{P}[E_2] = 90\% + 8\% + 2\% = 100\% \checkmark$$



CVA-Graph

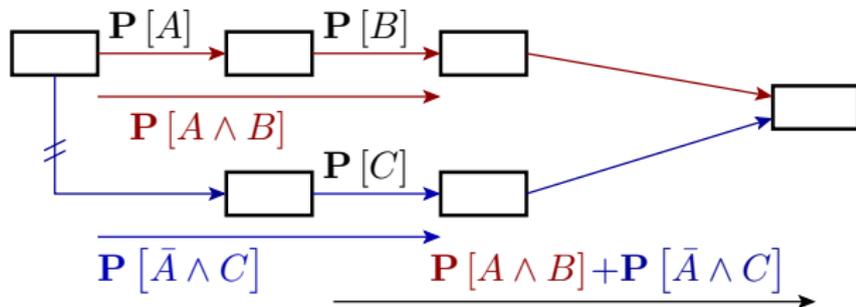
3.15 Beispiel für einen Zählwertzuordnungsgraphen



- Fehlfunktionen (MF) werden mit Häufigkeit MC erkannt (DM) und sonst nicht erkannt (NDM).
- Korrekte Service-Leistungen (CS) werden mit Häufigkeit ζ_{PM} wie Fehlfunktionen behandelt.
- Ohne Tolerierung werden Abstürze (CR), erkannte Fehlfunktionen (DM) und Phantom-MF nicht erbrachte Leistung (NS).

ζ_{CR}, ζ	Absturzrate, Fehlfunktionsrate.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
RA, CR	Akzeptierte Anforderung, Absturz.

3.16 Konstruktions- und Rechenregeln



Gerichteter Graph mit Zählwerten als Knoten und dem zu klassifizierenden Zählwert als Wurzel. Die Zuordnungshäufigkeiten an den Kanten sind Wahrscheinlichkeiten von Zuordnungsereignissen.

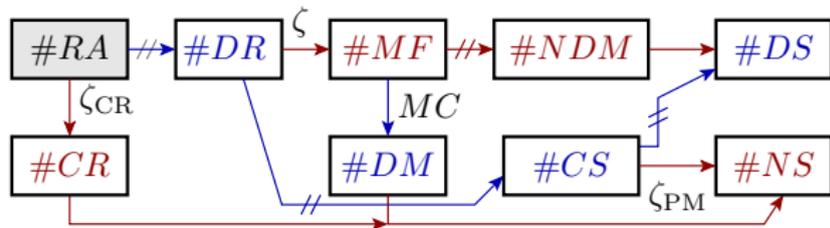
Der Übergang über mehrere Kanten beschreibt ein »UND« von Zuordnungsereignissen. Bei Unabhängigkeit Wahrscheinlichkeitsprodukt:

$$(3.5) \quad \mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$

Bei Zusammenfassung von Pfaden »ODER«. Bei Ausschluss Wahrscheinlichkeitssumme nach

$$(3.8) \quad \mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B]$$

3.17 Für das Beispiel



$$\eta_{DS} = \frac{\#DS}{\#RA} \Big|_{ACR} = (1 - \zeta_{CR}) \cdot \left(\underbrace{(1 - \zeta)}_{\text{gegenseitiger Ausschluss}} \cdot (1 - \zeta_{PM}) + \underbrace{\zeta}_{\text{gegenseitiger Ausschluss}} \cdot (1 - MC) \right)$$

Zuordnungsereignisse, für die Unabhängigkeit unterstellt wird:

- Absturz (ζ_{CR}), Fehlfunktionsentstehung (ζ),
- Fehlernachweis (MC), Phantomfehler (ζ_{Phan}).

Zusammenführung mit gegenseitigem Ausschluss:

- erkannte Fehlfunktionen (DM) und Phantom-Fehlfunktionen zu nicht erbrachten Leistungen (NS) und
- sonstige korrekte Leistungen und nicht erkannte Fehlfunktionen (NDM) zu erbrachten Leistungen (DS).



Fehlerbäume

3.18 Fehlerbaumanalyse (FTA – fault tree analysis)

Graphische Darstellung für logische Ereignisbeziehungen (UND, ODER, Nicht*) zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahrensituationen, Ausfälle, Fehlfunktionen, ...

Unterschiedene Ereignistypen:



B_i Basisereignis mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit



U_i unerschlossenes Ereignis, über das nur unzureichende Informationen verfügbar sind



H_i Hausereignis im gewöhnlichen Betrieb, das mit anderen zusammen Probleme verursachen kann.

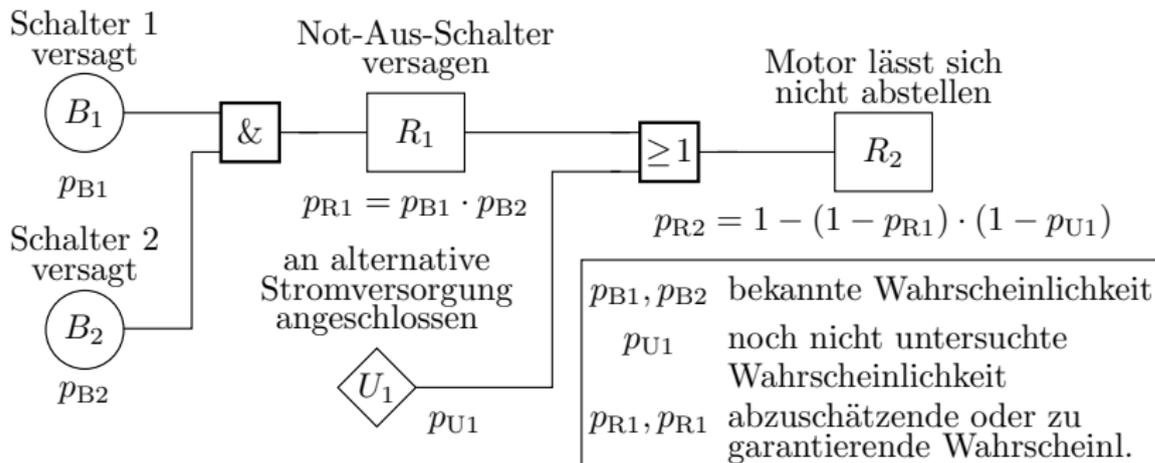


R_i resultierendes Ereignis, dessen Eintrittswahrscheinlichkeit aus denen von \circ , \diamond oder \square folgt.

*

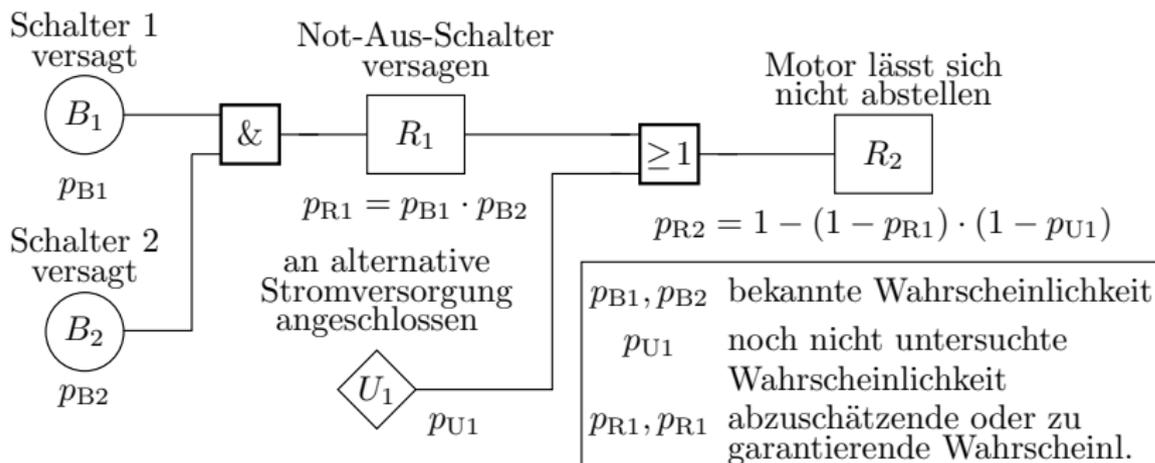
Abweichend von der klassischen Fehlerbaumdarstellung verwenden wir für logische UND-, ODER- und NICHT die Schaltsymbole aus der Digitaltechnik.

Beispiel 3.4: Motor lässt sich nicht abstellen



Ist $p_{R2} \leq 10^{-6}$ erzielbar mit $p_{B1} = p_{B2} = 10^{-3}$?

- B_i Basisereignis mit bekannter oder auf anderem Weg geschätzter Wahrscheinlichkeit.
- R_i Resultierendes Ereignis, dessen Eintrittswahrscheinlichkeit geschätzt werden soll.
- U_i Unerschlossenes Ereignis, über das unzureichende Information vorliegt.



Ist $p_{R2} \leq 10^{-6}$ erzielbar mit $p_{B1} = p_{B2} = 10^{-3}$?

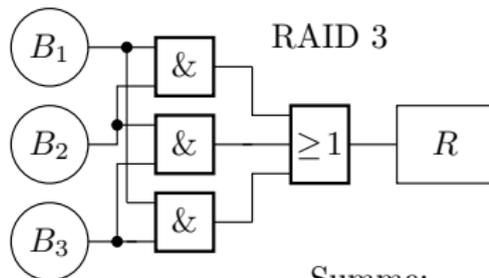
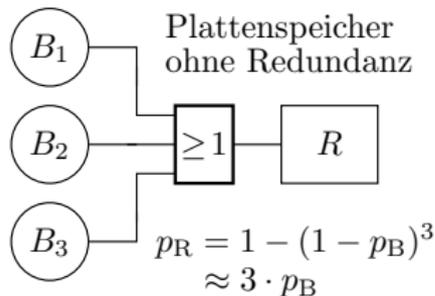
$$p_{R1} = p_{B1} \cdot p_{B2} = 10^{-6}$$

$$p_{R2} = 1 - (1 - p_{R1}) \cdot (1 - p_{U1}) \leq 10^{-6}$$

Es gibt nur die Lösung mit $p_{U1} = 0$. Lässt sich das Risiko einer alternativen Stromversorgung ausschließen oder muss die Gesamtlösung nachgebessert werden?

3.20 Datensicherheitsverbesserung durch ein RAID

Ein redundanzfreies Speichersystem aus drei Festplatten verliert Daten, wenn eine der drei Festplatten ausfällt, ein RAID 3 erst, wenn gleichzeitig zwei Platten ausfallen.



- B_i Ausfall Platte i
- R Datenverlust (result. Ereignis)
- p_B Ausfallwahrscheinlichkeit je Zeitschritt für eine Festplatte
- p_R Wahrscheinlichkeit Datenverlust je Zeitschritt Gesamtsystem

B_3	B_2	B_1	R
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Summe:

$$p_R = 3 \cdot p_B^2 - 2 \cdot p_B^3$$

$$p_B^2 \cdot (1 - p_B)$$

$$p_B^2 \cdot (1 - p_B)$$

$$p_B^2 \cdot (1 - p_B)$$

$$p_B^3$$

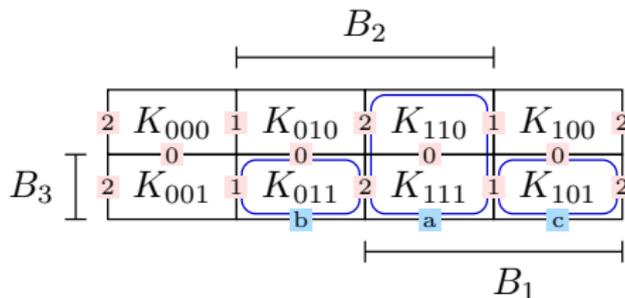
3.21 Rekonvergente Auffächerungen

Wenn sich der Bedingungsfluss verzweigt und wieder zusammentrifft, werden zum Teil abhängige Ereignisse verknüpft. Im Beispiel

$$R = B_1 B_2 \vee B_2 B_3 \vee B_1 B_3$$

haben die ODER-verknüpften UND-Terme jeweils eine gemeinsame Ereignisvariable. Für Wahrscheinlichkeitsabschätzung ungeeignet.

Umstellung in Terme sich ausschließender Ereignisse:



Überdeckungsfreie
Konjunktionen:

$$a: B_1 B_2$$

$$b: \bar{B}_1 B_2 B_3$$

$$c: B_1 \bar{B}_2 B_3$$

$$R = B_1 B_2 \vee \bar{B}_1 B_2 B_3 \vee B_1 \bar{B}_2 B_3$$

$$p_R = p_B^2 + p_B^2 \cdot (1 - p_B) + p_B^2 \cdot (1 - p_B) = 3 \cdot p_B^2 - 2 \cdot p_B^3$$

3.22 Geschichte der Fehlerbaumanalyse

- Einführung 1960: Abschluss sicherheitsbewertung von Interkontinentalraketen vom Typ LGM-30 Minuteman.
- Folgejahre: Auch für Sicherheitsbewertung kommerzieller Flugzeuge.
- Ab 70er bis 80er Jahre: Sicherheitsbewertung Atomkraftwerke.
- Später auch Automobilindustrie und deren Zulieferer.

Beim Einsatz zur Sicherheitsbewertung

- sind die sicherheitsrelevanten Ereignisse,
- die Basisereignisse und
- deren Wahrscheinlichkeiten

zuvor auf andere Weise abzuschätzen: Vorexperimente, Expertenbefragungen, Ursache-Wirkungs- (Ishikawa-) Diagramme, ...

Schätzfehler: unberücksichtigte Schadensereignisse, Einflüsse, ...
Für Interkontinentalraketen mit Atomsprengeköpfen nicht sehr vertrauenserweckend.

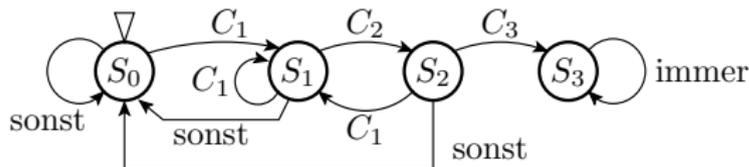


Markov-Ketten

3.23 Markov-Ketten

Eine Markov-Kette* (MC) ist ein stochastisches Modell für Ereignisfolgen, deren Verarbeitung sich durch einen endlichen Automaten beschreiben lässt.

Zustandsautomat Fehlernachweis mit Eingabefolge $C_1C_2C_3$:

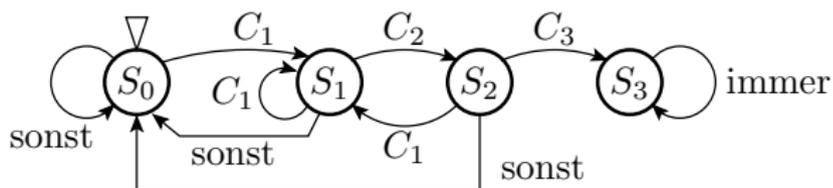


Start im Zustand S_0 »keine richtige Eingabe« und Verbleib nach drei richtigen Eingaben im Zustand S_3 »Fehler nachgewiesen«.

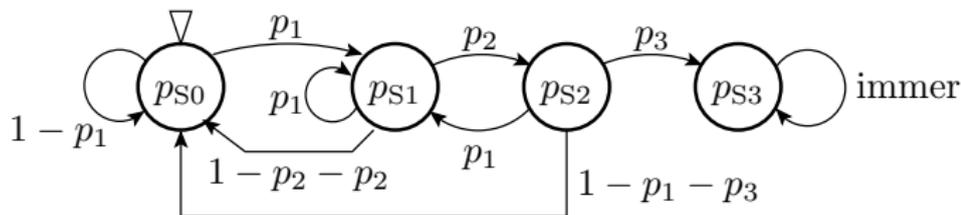
S_i Zustand i der Markov-Kette (State i of Markov chain).

C_j Übergangsbedingung j (Transitional condition j).

* Andrej Andreevič Markov, russischer Mathematiker, 1856-1922 (Andrej Andreevič Markov, Russian mathematician, 1856-1922).



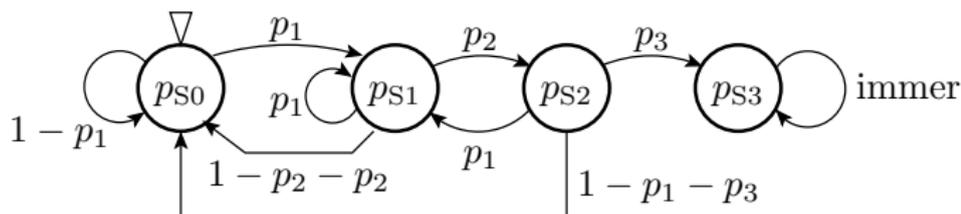
In der Markov-Kette werden Übergangsbedingungen durch die Übergangswahrscheinlichkeiten und Zustände durch Zustandswahrscheinlichkeiten ersetzt.



Zu Beginn hat der Startzustand S_0 die Wahrscheinlichkeit $ps_0 = 1$ und die anderen Zustände haben die Wahrscheinlichkeit $ps_{S_i} |_{i \neq 0} = 0$.

In jedem Schritt verteilt jeder Knoten seine Wahrscheinlichkeit über seine abgehenden Kanten auf Zielknoten. $\sum ps_{S_i}$ bleibt immer 100%.

- ps_i Wahrscheinlichkeit, dass die Markov-Kette im Zustand S_i ist.
- p_j Wahrscheinlichkeit von Zustandsübergang C_j .



Eine Markov-Kette beschreibt ein lineares Gleichungssystem zur Berechnung der Zustandswahrscheinlichkeiten für den Folgeschritt:

$$\begin{pmatrix} ps_0 \\ ps_1 \\ ps_2 \\ ps_3 \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & p_1 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} ps_0 \\ ps_1 \\ ps_2 \\ ps_3 \end{pmatrix}_{n-1}$$

mit $\begin{pmatrix} ps_0 & ps_1 & ps_2 & ps_3 \end{pmatrix}_0^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$.

Kontrollkriterien für Gleichungssystem und Simulationsergebnis:

- Summe der Wahrscheinlichkeiten je Matrixspalte eins.
- Summe aller $ps_{s,i}$ nach jedem Schritt eins.

$(\dots)^T$
 n Transponierte Matrix (Tausch von Zeilen und Spalten).
 Simulationsschrittnummer der Markov-Kette.

$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & p_1 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_{n-1}$$

Simulation mit Octave bzw. Matlab:

```
p1 = ...; p2 = ...; p3 = ...;
```

```
M=[1-p1 1-p1-p2 1-p1-p3 0;
    p1    p1    0    0;
    0    p2    p1    0;
    0    0    p3    1];
```

```
S=[1; 0; 0; 0];
```

```
for idx=1:100
```

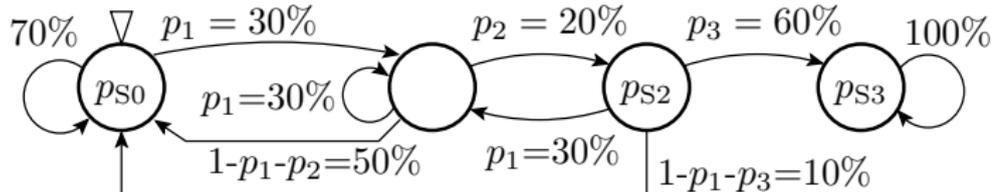
```
    S = M * S;
```

```
    printf ( '%3i  %6.2f%%  %6.2f%%  %6.2f%%  %6.2f%%\n' , idx , 100*S);
```

```
end;
```

3.27 Beispielsimulation

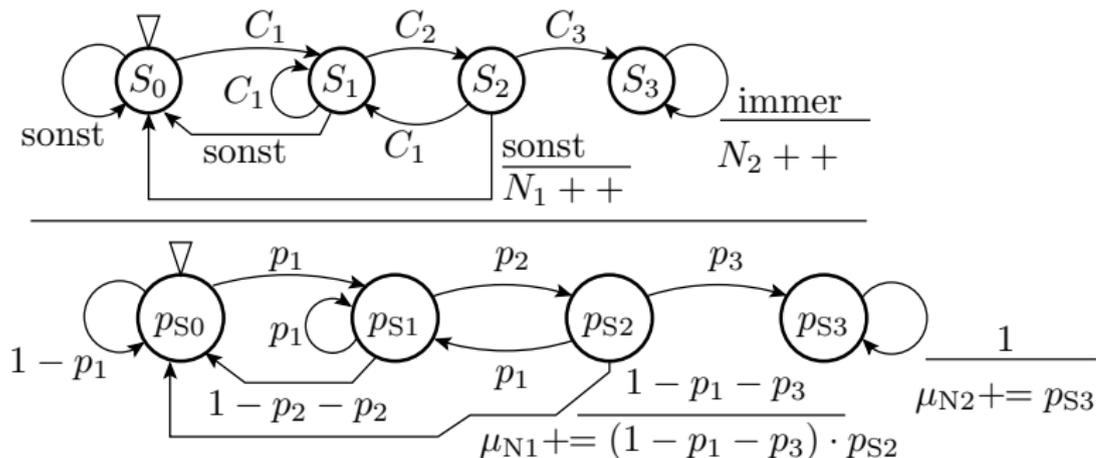
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	p_{S0}	p_{S1}	p_{S2}	p_{S3}	$\sum_{i=0}^3 p_{Si}$
0	100,00%	0	0	0	100%
1	70,00%	30,00%	0	0	100%
2	64,00%	30,00%	6,00%	0	100%
3	60,40%	28,20%	7,80%	3,60%	100%
4	57,16%	26,58%	7,89%	8,28%	100%
...
10	41,08%	19,06%	5,90%	33,96%	100%
...
50	4,54%	2,11%	0,65%	92,71%	100%
...
100	0,29%	0,13%	0,04%	99,44%	100%

3.29 Kantenzähler

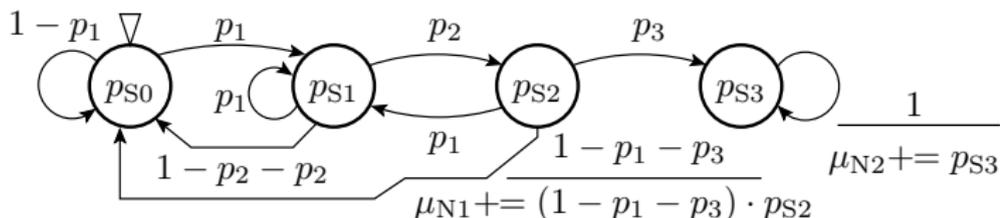
Mit Zählern an den Kanten lässt sich die Anzahl bzw. die zu erwartende Anzahl der Kantenübergänge, bestimmen:



- n Simulationsschrittnummer der Markov-Kette.
- N_1 Zähler, wie oft nach zwei richtigen Eingaben eine falsche folgt.
- N_2 Zähler für die Anzahl der Schritte nach dem Fehlernachweis.
- μ_{N_i} Zu erwartende Kantenübergangsanzahl.
- $n - \mu_{N_2}$ Zu erwartende Schrittzahl bis zum Fehlernachweis.

3.31 Beispielsimulation

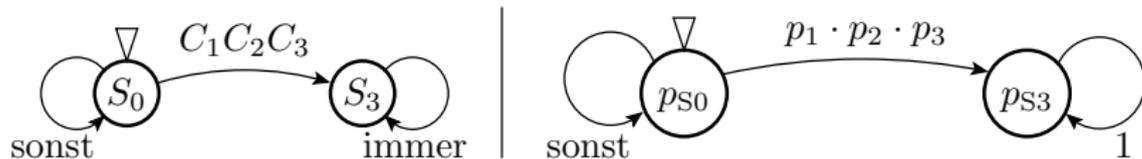
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$



Schritt	ps_0	ps_1	ps_2	ps_3	μ_{N1}	μ_{N2}
1	70,00%	30,00%	0	0	0	0
2	64,00%	30,00%	6,00%	0	0,01	0
3	60,40%	28,20%	7,80%	3,60%	0,01	0,04
4	57,16%	26,58%	7,89%	8,28%	0,02	0,12
...
10	41,08%	19,06%	5,90%	33,96%	0,06	1,55
...
50	4,54%	2,11%	0,65%	92,71%	0,16	31,18
...
100	0.29%	0,13%	0,04%	99,44%	0,17	79,79

Zu erwartende Anzahl der Schritte bis zum Nachweis: $n - \mu_{N2} \approx 20$

3.32 Drei richtige Eingaben als Einzelereignis



Gleichungssystem
der modifizierten Markov-Kette:

$$\begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1 - p_1 \cdot p_2 \cdot p_3 & 0 \\ p_1 \cdot p_2 \cdot p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_n \quad \text{mit} \quad \begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

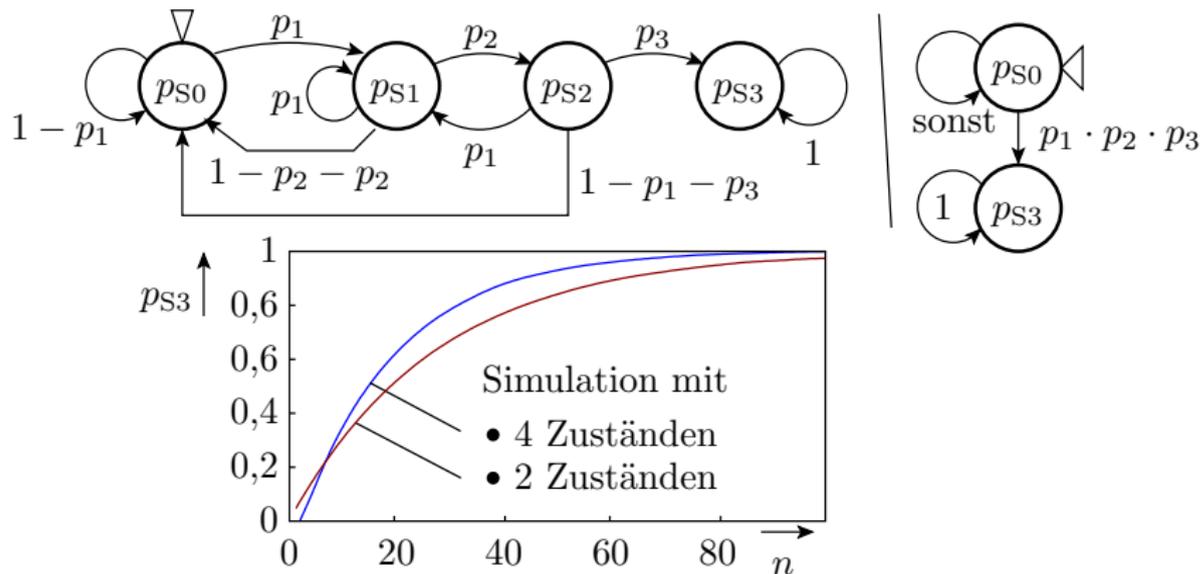
$$\begin{aligned} p_{S0}(n) &= (1 - p_1 \cdot p_2 \cdot p_3) \cdot p_{S0}(n-1) = (1 - p_1 \cdot p_2 \cdot p_3)^n \\ &= e^{\ln(1 - p_1 \cdot p_2 \cdot p_3) \cdot n} \approx e^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \quad \text{für } p_1 \cdot p_2 \cdot p_3 \ll 1^* \end{aligned}$$

$$\begin{aligned} p_{S3}(n) &= 1 - p_{S0}(n) = 1 - (1 - p_1 \cdot p_2 \cdot p_3)^n \\ &\approx 1 - e^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \quad \text{für } p_1 \cdot p_2 \cdot p_3 \ll 1^* \end{aligned}$$

*

Annäherung durch erste Glied Taylor-Reihe: $\ln(1-x) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \dots\right)$.

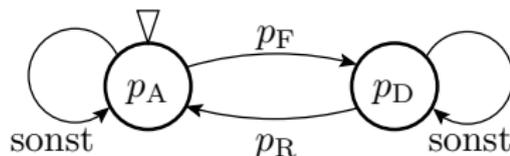
3.33 Unterschied zwischen den Markov-Ketten



Offenbar doch nicht ganz identisches Verhalten, aber sehr ähnliches.

3.34 Abschätzung einer Verfügbarkeit

Ein System sei zu Beginn funktionsfähig (Zustand A), fällt in jedem Zeitschritt, wenn es ganz ist, mit einer Wahrscheinlichkeit p_F aus (Übergang in Zustand D) und wird, wenn es kaputt ist, innerhalb des Zeitschritts mit einer Wahrscheinlichkeit p_R repariert (Übergang in Zustand A):

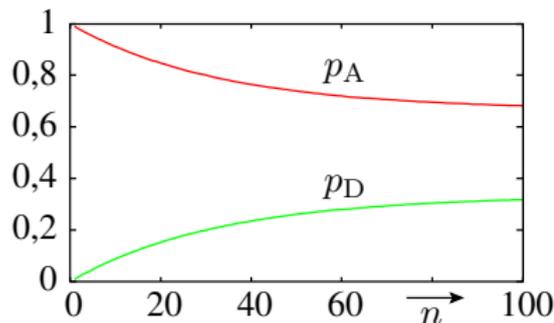
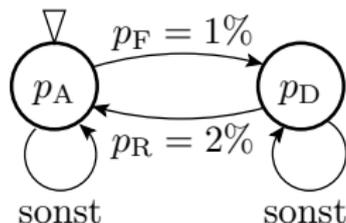


Modellierung als simulierbares Gleichungssystem:

$$\begin{pmatrix} p_A \\ p_D \end{pmatrix}_{n+1} = \begin{pmatrix} 1 - p_F & p_R \\ p_F & 1 - p_R \end{pmatrix} \cdot \begin{pmatrix} p_A \\ p_D \end{pmatrix}_n \quad \text{mit} \quad \begin{pmatrix} p_A \\ p_D \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

p_A	Wahrscheinlichkeit, dass das System verfügbar (available) ist.
p_D	Wahrscheinlichkeit, dass das System defekt ist.
p_F	Wahrscheinlichkeit, dass das System im Zeitschritt ausfällt.
p_R	Wahrscheinlichkeit, dass das System im Zeitschritt repariert wird.
n	Simulationsschrittnummer der Markov-Kette.

3.35 Beispielsimulation



Stationärer Zustand:

$$p_A \cdot p_F = p_D \cdot p_R \quad \text{mit } p_A + p_D = 1$$

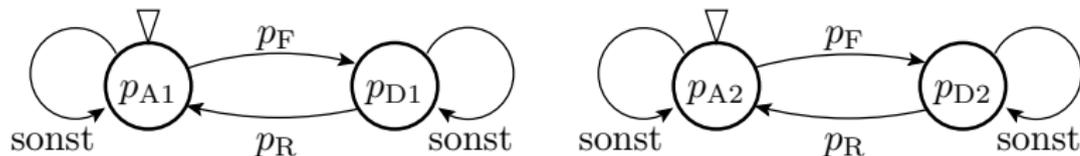
$$p_A = \frac{p_R}{p_R + p_F} = \frac{2\%}{1\% + 2\%} = 66,7\%$$

$$p_D = \frac{p_F}{p_R + p_F} = \frac{1\%}{1\% + 2\%} = 33,3\%$$

p_A	Wahrscheinlichkeit, dass das System verfügbar (available) ist.
p_D	Wahrscheinlichkeit, dass das System defekt ist.
p_F	Wahrscheinlichkeit, dass das System im Zeitschritt ausfällt.
p_R	Wahrscheinlichkeit, dass das System im Zeitschritt repariert wird.

3.36 Reparaturprozess für ein 1oo2 System

System aus zwei gleichartigen Teilsystemen, das solange funktioniert, wie 1 von (out of) 2 Teilsystemen funktioniert:



$$p_F = 0.01; \quad p_R = 0.02;$$

$$M = \begin{bmatrix} 1-p_F & p_R \\ p_F & 1-p_R \end{bmatrix};$$

$$S = [1; 0];$$

for n=1:100

$$S = M * S;$$

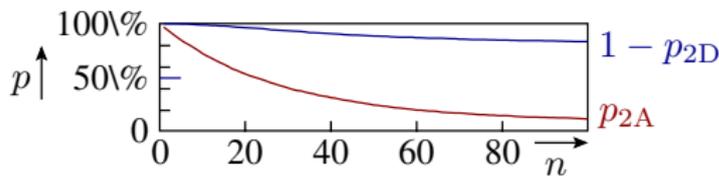
$$p_{2A}(n) = S(1) ** 2; \quad \% \text{ beide Einheiten ganz}$$

$$p_{2D}(n) = S(2) ** 2; \quad \% \text{ beide Einheiten defekt}$$

end;

plot(1:100, p2A, 1:100, 1-p2D)

3.37 Beispielsimulation mit $p_F = 1\%$ und $p_R = 2\%$



beide Systeme verfügbar	$p_{2D} = p_D^2$	$\lim_{n \rightarrow \infty} (p_{2D}) = (1/3)^2$
kein System verfügbar	$p_{2A} = p_A^2$	$\lim_{n \rightarrow \infty} (p_{2A}) = (2/3)^2$
mindestens ein System verfügbar	$1 - p_{2D}$	$\lim_{n \rightarrow \infty} (\dots) = 1 - (1/9)$

- 1oo2-Reserve nur bei hoher Verfügbarkeit je Systeme sinnvoll.
- Im Beispiel wäre ein $p_R \gg p_F$ zielführender.

n	Simulationsschrittnummer der Markov-Kette.
p_F	Wahrscheinlichkeit, dass das System im Zeitschritt ausfällt.
p_R	Wahrscheinlichkeit, dass das System im Zeitschritt repariert wird.
$1 - p_{2D}$	Wahrscheinlichkeit, daß mindestens ein System verfügbar ist.
p_{2A}	Wahrscheinlichkeit, daß beide Systeme verfügbar sind.



Zusammenfassung



3.38 Wahrscheinlichkeit

Unter konstanten Versuchbedingungen strebt die Eintrittshäufigkeit von Zählversuchen gegen die Eintrittswahrscheinlichkeit:

$$(3.1) \quad \mathbb{P}[A] = \lim_{n \rightarrow \infty} \frac{\#A}{n}$$

Die Wahrscheinlichkeit ist die beste Vorhersage der zu erwartenden relativen Häufigkeit künftiger Versuche.

Bei gleichhäufigen möglichen Ereignissen ist die Wahrscheinlichkeit der Anteil der günstigen Ereignisse.

Komplexe Ereignisse lassen sich oft durch logische Verknüpfungen einfacher zu untersuchender Ereignisse beschreiben.

Zusatzbedingungen mit Einfluss auf die Eintrittshäufigkeit sind zu berücksichtigen.

Für logische Ereignisverknüpfungen bietet die Mathematik nur Lösungen für Unabhängigkeit und gegenseitigen Ausschluss. Für andere Abhängigkeiten müssen die logischen Beziehungen entsprechend umgestellt werden.

3.39 Verketteter Ereignisse

Bedingte Wahrscheinlichkeit:

$$(3.2) \quad \mathbb{P}[A|B] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]}$$

Satz von Bayes:

$$(3.3) \quad \mathbb{P}[B|A] = \mathbb{P}[A|B] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]}$$

Gegenwahrscheinlichkeit:

$$(3.4) \quad \mathbb{P}[\bar{A}] = 1 - \mathbb{P}[A]$$

UND unabhängiger Ereignisse:

$$(3.5) \quad \mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$

UND sich ausschließender Ereignisse:

$$(3.6) \quad \mathbb{P}[A \wedge B] = 0$$

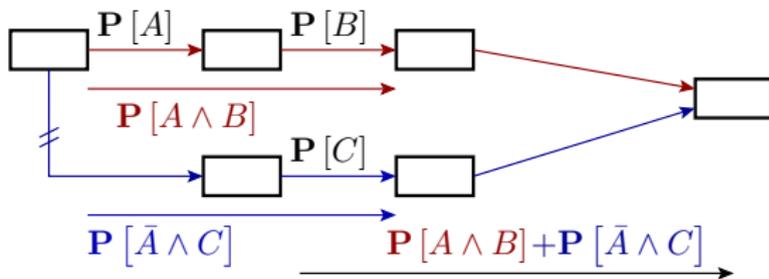
ODER unabhängiger Ereignisse:

$$(3.7) \quad \mathbb{P}(A \vee B) = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A] \cdot \mathbb{P}[B]$$

Oder sich ausschließender Ereignisse:

$$(3.8) \quad \mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B]$$

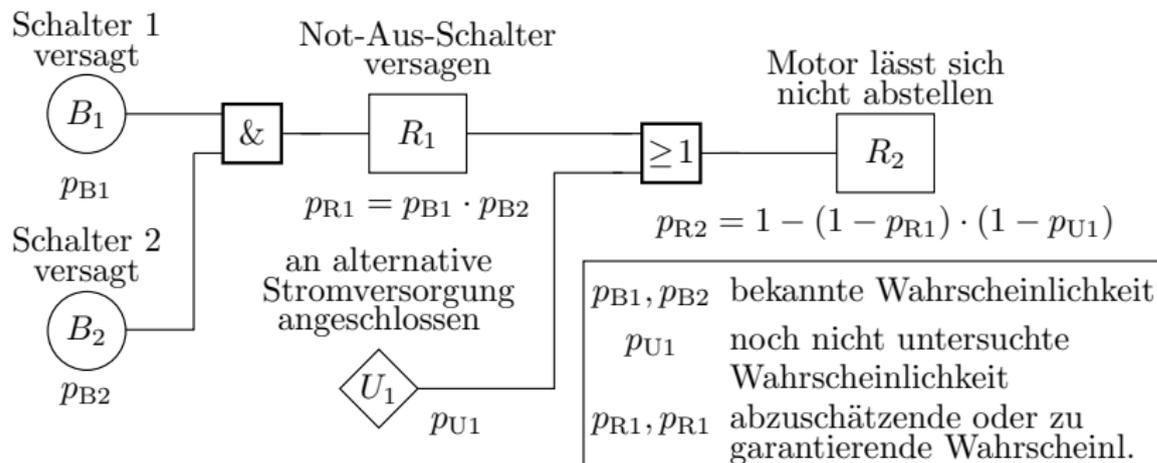
3.40 Zählwertzuordnungsgraph



Zuordnungsgraph zur Definition unserer Kenngrößen zur Beschreibung der Verlässlichkeit: Verfügbarkeit, Fehlfunktionsrate, ... Zuordnung von Zählwerte über Zufallsereignisse zu Teilaspekten so, dass

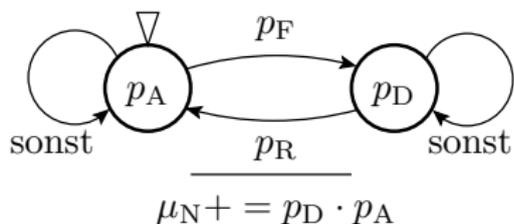
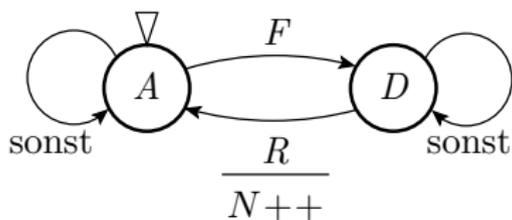
- eine Zuordnung über mehrere Kante eine »UND« unabhängiger Ereignisse und
- Zusammenführungen ein »ODER« sich ausschließender Ereignisse beschreiben.

3.41 Fehlerbäume



- Graphische Darstellung logisch verketteter Ereignisse zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahrensituationen, Ausfällen, Fehlfunktionen,
- Zulässige Ereignisverknüpfungen: NOT, UND und ODER.
- Wenn »Abhängigkeit, aber nicht Ausschluss« Gleichungsumstellung.

3.42 Markov-Ketten



$$\begin{pmatrix} p_A \\ p_D \end{pmatrix}_{n+1} = \begin{pmatrix} 1 - p_F & p_R \\ p_F & 1 - p_R \end{pmatrix} \cdot \begin{pmatrix} p_A \\ p_D \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_A \\ p_D \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mu_N = \mu_N + p_D \cdot p_A$$

Berechnung von Zustandswahrscheinlichkeit für stochastische Prozesse, die sich durch endliche Automaten beschrieben lassen:

- Fehlernachweis,
- Fehlerentstehung,
- Verfügbarkeit, ...

Kantenzähler für die zu erwartende Anzahl der Übergänge.

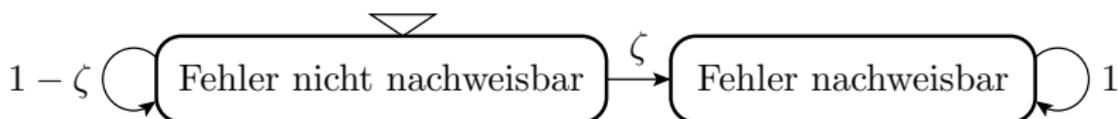


Fehlernachweis



Nachweis & Zuverlässigkeit

3.43 Nachweiswahrscheinlichkeit



Ein Fehler verursacht mit einer Rate ζ Fehlfunktionen, an denen er erkannt wird. Mindestens ein Nachweis bei N Tests:

$$p_{\text{FD}}(\zeta, N) = 1 - (1 - \zeta)^N = 1 - e^{\ln(1-\zeta) \cdot N}$$

$$\approx^* 1 - e^{-\zeta \cdot n} \quad \text{für } \zeta \ll 1$$

Für den Zusammenhang zwischen Test und Verlässlichkeit interessieren nur Fehler mit $\zeta \ll 1$, weil nur diese nach längerer Iteration aus Test und Fehlerbeseitigung noch im System sind:

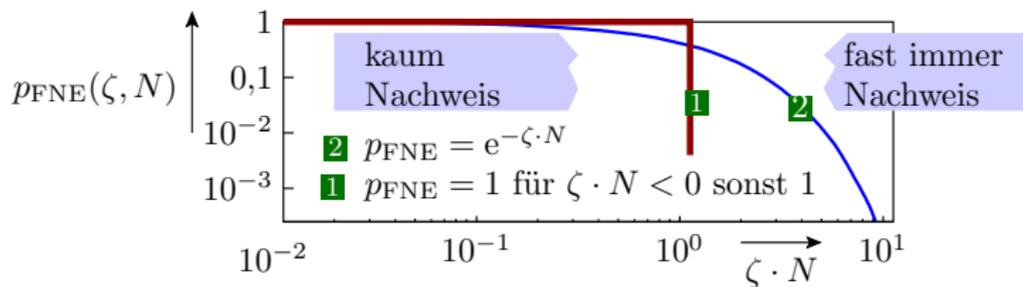
$$p_{\text{FD}}(\zeta, N) = 1 - e^{-\zeta \cdot N} \quad (3.10)$$

$p_{\text{FD}}(\zeta, N)$ Nachweiswahrscheinlichkeit des Fehlers mit N Tests.

ζ Fehlfunktionsrate des Fehlers.

* Annäherung durch erste Glied Taylor-Reihe: $\ln(1 - x) = - \left(x + \frac{x^2}{2} + \frac{x^3}{3} + \dots \right)$.

3.44 Rückblick (Abschn. 2.2.2)



Für die Abnahme der Fehleranzahl mit der Testanzahl bei Beseitigung aller erkannten Fehler hatten wir unter der Vereinfachung, dass Fehler ab $\zeta \cdot N \geq 1$ beseitigt werden und sonst nicht (Kurve 1), abgeschätzt

$$(2.16) \quad \mu_F(N_2) = \mu_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1$$

$$(2.13) \quad \mu_F(N) = \mu_F \cdot \int_0^1 p_{FNE}(\zeta, N) \cdot h(\zeta) \cdot d\zeta$$

$$(2.19) \quad h(\zeta) = K \cdot \zeta^{K-1} \quad \text{mit } 0 < K < 1 \quad \text{und } 0 < \zeta \leq 1$$

Gilt das auch mit der ablingenden Exponentialfunktion (Kurve 2)?

3.45 Abnahme Fehleranzahl mit Testanzahl

$$(2.13) \quad \mu_F(N) = \mu_F \cdot \int_0^1 p_{FNE}(\zeta, N) \cdot h(\zeta) \cdot d\zeta$$

$$(2.19) \quad h(\zeta) = K \cdot \zeta^{K-1} \quad \text{mit } 0 < K < 1 \quad \text{und } 0 < \zeta \leq 1$$

Nichtbeseitigungswahrscheinlichkeit als Gegenwahrscheinlichkeit der Nachweiswahrscheinlichkeit (Gl. 3.10):

$$p_{FNE}(\zeta, N) = 1 - p_{FD}(\zeta, N) = e^{-\zeta \cdot N} \quad (3.11)$$

Alles eingesetzt:

$$\mu_F(N) = \mu_F \cdot \int_0^1 e^{-\zeta \cdot N} \cdot K \cdot \zeta^{K-1} \cdot d\zeta$$

Substitution: $\zeta = \frac{z}{N}$, $d\zeta = \frac{dz}{N}$:

$$\mu_F(N) = \mu_F \cdot \int_0^N \underbrace{e^{-z}}_{p_{FNE}(\zeta, N)} \cdot \underbrace{K \cdot \left(\frac{z}{N}\right)^{K-1}}_{h(\zeta)} \cdot \frac{dz}{N} = \frac{\mu_F \cdot K}{N^K} \cdot \underbrace{\int_0^N e^{-z} \cdot z^{K-1} \cdot dz}_*$$

$\mu_F(N)$ Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.

$p_{FNE}(\zeta, N)$ Wahrscheinlichkeit, dass Fehler mit MF-Rate ζ nach N Tests nicht beseitigt sind.

$h(\zeta)$ Dichtefunktion der Fehlfunktionsrate vor der Fehlerbeseitigung.

K Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).

*

Anteil für $z \gg 1$ vernachlässigbar, also fast bestimmtes Integral $\int_0^\infty \dots dz$.



3.46 Gammafunktion

Das verbleibende bestimmte Integral ist für $N \gg 1$ die Gamma-Funktion $\Gamma(K)$. Für $0 < K \leq 1$ beträgt diese:

$$\Gamma(K) = \int_0^{\infty} e^{-z} \cdot z^{K-1} \cdot dz \approx \frac{1}{K} \quad (3.12)$$

- Für $0 < K < 1$ gilt:

$$\Gamma(K) \approx \frac{1}{K}$$

K	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
$\Gamma(K)$	9,51	4,59	2,99	2,22	1,77	1,49	1,30	1,16	1,07

- Für $K > 1$ gilt:

$$\Gamma(K+1) = K \cdot \Gamma(K) \quad (3.13)$$

 $\Gamma(\dots)$

Gamma-Funktion.

 K

Parameter der Gamma-Funktion und Formfaktor der Verteilung der Fehlfunktionsrate.

3.47 Verbleibende Fehleranzahl (Fortsetzung)

$$\mu_F(N) = \frac{\mu_F \cdot K \cdot \Gamma(K)}{N^K} \quad (3.14)$$

Für die Abnahme der zu erwartenden Fehleranzahl mit der effektiven Testanzahl gilt auch mit der genauer abgeschätzten Nachweiswahrscheinlichkeit (Gl. 3.10) das Potenzgesetz:

$$(2.16) \quad \mu_F(N_2) = \mu_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1$$

Zu erwartende Fehlerabdeckung als die mittlere Fehlernachweiswahrscheinlichkeit für eine Testverlängerung von N_0 auf $N > N_0$:

$$\mu_{FC}(N) = 1 - \left(\frac{N}{N_0}\right)^{-K} \quad (3.15)$$

3.48 Dieselbe Kontrolle für die Fehlfunktionsrate

$$(2.14) \quad \zeta_F(N) \stackrel{(\leq 1)}{=} \underbrace{\mu_F \cdot \int_0^1 p_{\text{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \zeta \cdot d\zeta}_{\text{mittlere Fehlfunktionsrate je Fehler}}$$

$$\zeta_F(N) = \mu_F \cdot \int_0^1 e^{-\zeta \cdot N} \cdot K \cdot \zeta^{K-1} \cdot \zeta \cdot d\zeta$$

Substitution $\zeta = \frac{z}{N}$, $d\zeta = \frac{dz}{N}$:

$$\zeta_F(N) \stackrel{(\leq 1)}{=} \mu_F \cdot \int_0^N \underbrace{e^{-z}}_{p_{\text{FNE}}(\zeta, N)} \cdot \underbrace{K \cdot \left(\frac{z}{N}\right)^{K-1}}_{h(\zeta)} \cdot \frac{z}{N} \cdot \frac{dz}{N} = \frac{\mu_F \cdot K}{N^{K+1}} \cdot \int_0^N e^{-z} \cdot z^K \cdot dz$$

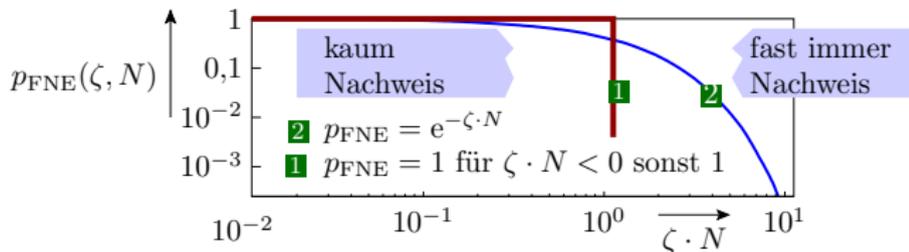
$$\zeta_F(N) \stackrel{(\leq 1)}{=} \frac{\mu_F \cdot K \cdot \Gamma(K+1)}{N^{K+1}} = \frac{\mu_F \cdot K^2 \cdot \Gamma(K)}{N^{K+1}} \quad (3.16)$$

Für die Abnahme der MF-Rate mit der effektiven Testanzahl gilt auch mit Fehlernachweiswahrscheinlichkeit (Gl. 3.10) das Potenzgesetz

$$(2.22) \quad \zeta_F(N_2) \stackrel{(\leq 1)}{=} \zeta_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)}$$

$h(\zeta)$	Dichtefunktion der Fehlfunktionsrate vor der Fehlerbeseitigung.
$\zeta_F(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
(≥ 1)	Der errechnete Wert ist eine Obergrenze. Der tatsächliche Wert ist max. eins.

3.49 Vergleich mit bisherigem Modell



Alles gleich, außer geringfügige Abweichung im Verhältnis zwischen Fehlfunktionsrate und zu erwartenden Fehleranzahl:

1 Mit Sprungfunktion für $p_{\text{FNE}}(\zeta, N)$:

$$(2.20) \quad \zeta_{\text{F}}(N) \stackrel{(\leq 1)}{=} \mu_{\text{F}} \cdot \frac{K}{K+1} \cdot N^{-(K+1)}$$

2 Mit $p_{\text{FNE}}(\zeta, N) = e^{-\zeta \cdot N}$:

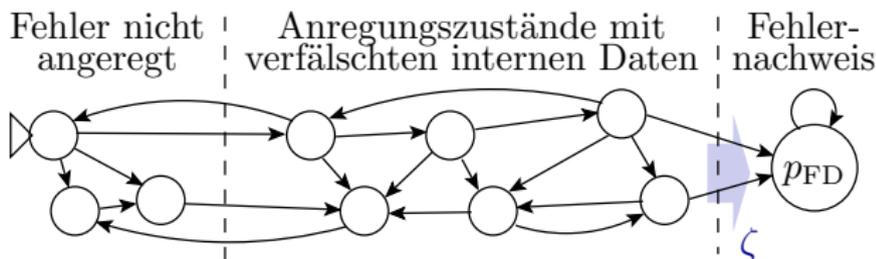
$$(2.23) \quad \zeta_{\text{F}}(N) \stackrel{(\leq 1)}{=} \frac{\mu_{\text{F}}(N) \cdot K}{N}$$

Der Term $K + 1$ unter dem Bruchstrich in (Gl. 2.20) wurde bereits in Abschnitt 2.2.2 unter Verweis auf diesen Abschnitt vernachlässigt.



Service mit Gedächtnis

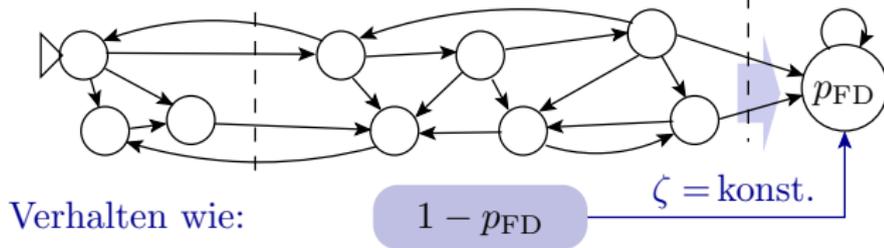
3.50 Service mit Gedächtnis



In Systemen mit internen Speicherzuständen (Gedächtnis) verlangt der Fehlernachweis zum Teil mehrere Zustandsübergänge über Anregungszustände mit verfälschten internen Daten bis zum Nachweis.

Eine genaue Modellierung des Zusammenhangs zwischen Nachweiswahrscheinlichkeit und Testanzahl verlangt für jeden Fehler einen individuellen Beobachterautomaten, aus dem sich eine fehlerspezifische Markov-Kette ableitet. Oft mehr als zwei Zustände, testschrittabhängige Fehlfunktionsrate ζ .

Nach N_I Initialisierungsschritten stationäres Gleichgewicht der Wahrscheinlichkeiten. Fehler-nachweis



An einem Beispielfehler wird gezeigt, dass solche Beobachterautomaten dazu tendieren, sich für lange Testsätze nahezu wie der Zweizustands-Beobachteraautomat mit der abklingenden Exponentialfunktion als Nachweiswahrscheinlichkeit zu verhalten.

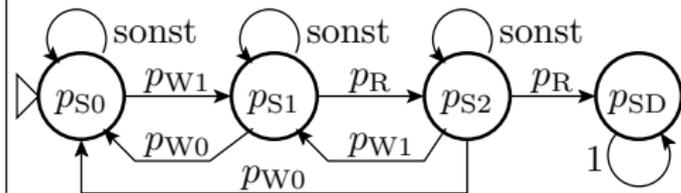
Und zwar stellt sich nach N_I Initialisierungsschritten ein stationäres Gleichgewicht zwischen den Zustandswahrscheinlichkeiten der linken Zustände und darüber eine konstante Fehlfunktionsrate ζ für den Abfluss von Wahrscheinlichkeit in den Zustand »Fehlernachweis« ein.

3.52 Beispiel: RAM-DR1-Fehler

Zustände:

- S0: Wert 0 oder unbekannt
- S1: Wert 1 geschrieben
- S2: 1 zerstörend gelesen
- SD: Fehler nachgewiesen

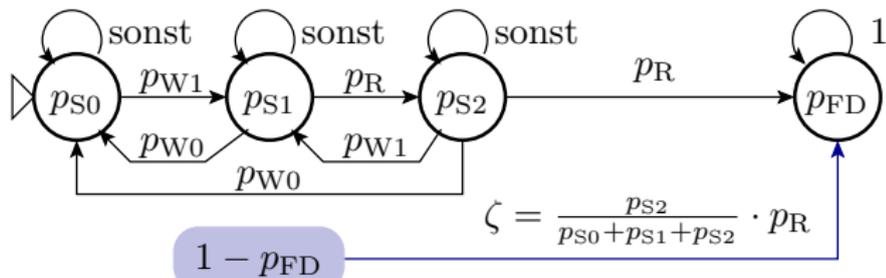
Nachweisfolge: Schreibe 1 → Lesen → Lesen



Im RAM wird beim Lesen der fehlerhaften Speicherzelle mit Adresse a eine gespeicherte 1 in eine 0 verfälscht. Der Nachweis erfordert:

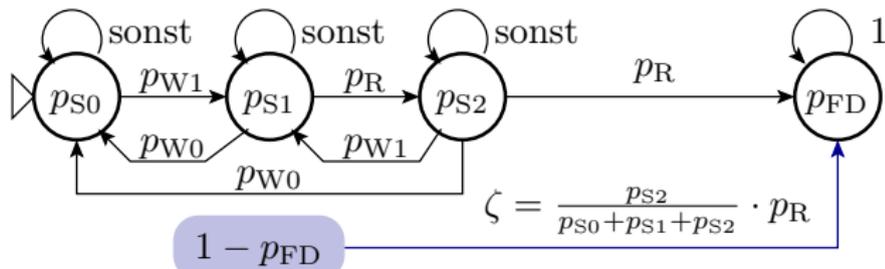
- Schreibe 1 auf Adresse a (Übergang in Zustand S1),
- Lese Wert von Adresse a (Übergang in Anregungszustand S2),
- Lese von Adresse a ohne zwischenzeitlichen Schreibzugriff auf a (Übergang in den Nachweiszustand SD).

p_{W0}	Wahrscheinlichkeit, dass eine 0 in die Speicherzelle geschrieben wird.
p_{W1}	Wahrscheinlichkeit, dass eine 1 in die Speicherzelle geschrieben wird.
p_R	Wahrscheinlichkeit, dass die Speicherzelle gelesen wird.
p_{FD}	Fehlernachweiswahrscheinlichkeit (Probability of fault detection).
DR1	Zerstörendes Lesen einer eins.



Im stationären Gleichgewicht von p_{S0} bis p_{S2} konstant

Die äquivalente Fehlfunktionsrate für die Zweizustands-Markov-Kette ist hier die bedingte Wahrscheinlichkeit, dass der Beobachterautomat im Zustand S2 ist, wenn er nicht im Zustand FD, also in einem der Zustände S1, S2 oder S3 ist, und die defekte Speicherzelle gelesen wird.



$p_{S0}=1$; $p_{S1}=0$; $p_{S2}=0$; $p_{SD}(1)=0$; $N=5000$;
 $NA=128$; $p_R = 1/(2 \cdot NA)$; $p_{W0} = p_{W1} = 1/(4 \cdot NA)$;

for n=1:N

$p_0 = p_{S0} \cdot (1 - p_{W1}) + p_{S1} \cdot p_{W0} + p_{S2} \cdot p_{W0}$;

$p_1 = p_{S0} \cdot p_{W1} + p_{S1} \cdot (1 - p_{W0} - p_R) + p_{S2} \cdot p_{W1}$;

$p_2 = p_{S1} \cdot p_R + p_{S2} \cdot (1 - p_{W1} + p_{W0} - p_R)$;

$p_{FD} = p_{SD}(n) + p_{S2} \cdot p_R$;

$zeta = p_{S2} \cdot p_R / (p_{S0} + p_{S1} + p_{S2})$; % MF rate

$p_{S0} = p_0$; $p_{S1} = p_1$; $p_{S2} = p_2$;

end

plot(1:N, zeta);

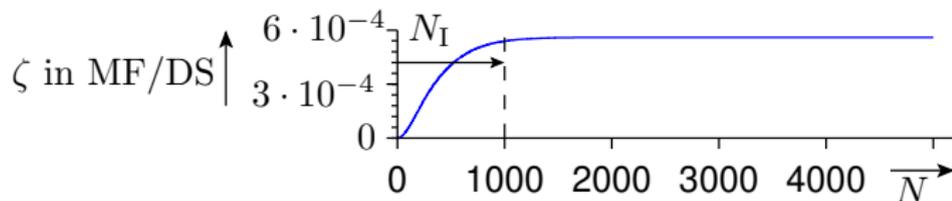
p_{S_i} Wahrscheinlichkeit, dass die Markov-Kette im Zustand S_i ist.

p_R Wahrscheinlichkeit, dass die Speicherzelle gelesen wird.

ζ MF-Rate des DR1-Fehlers.

N Anzahl der Tests.

3.55 Simulation



Die durch den Fehler verursachte MF-Rate ζ nimmt anfangs mit der Testanzahl N zu und bleibt ab $N_I \approx 1000$ konstant $\zeta \approx 5,7 \cdot 10^{-4}$. Ab $N > N_I$ beträgt die Nachweiswahrscheinlichkeit mindestens:

$$p_{\text{FD}}(\zeta, N) \geq 1 - e^{-\zeta \cdot (N - N_I)} \quad (3.17)$$

und für lange Zufallstests $N \gg N_I$ gilt wie für Systeme ohne Gedächtnis:

$$(3.10) \quad p_{\text{FD}}(\zeta, N) = 1 - e^{-\zeta \cdot N}$$

$p_{\text{FD}}(N)$	Nachweiswahrscheinlichkeit des DR1-Fehlers als Funktion der Anzahl der Tests.
ζ	MF-Rate des DR1-Fehlers.
N_I	Anzahl der Initialisierungsschritte.
N	Testanzahl, für Worst-Case-Abschätzungen ohne die N_I Initialisierungsschritte.



Fehler und Modellfehler



3.56 Fehler und Modellfehler (Abschn. 2.1.5)

Man kennt nie die Fehler, die man sucht, sondern nur die, die man gefunden hat.

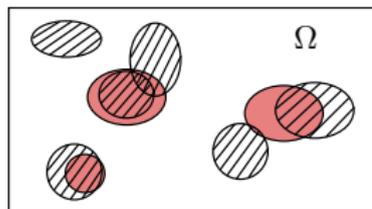
Testauswahl und Testbewertung verwenden Modellfehler.

Modellfehler: Angenommener Fehler, in der Regel eine kleine Änderungen der Testobjektbeschreibung, z.B. Haftfehler
»Gateranschluss ständig null oder ständig eins«.

Fehlermodell: Algorithmus zur Erzeugung einer Modellfehlermenge aus einer Testobjektbeschreibung.

Wie und wie gut kann man von der Modellfehlerabdeckung oder anderen »messbaren« Kenngrößen für einen Testsatz auf die tatsächliche Fehlerabdeckung schließen?

3.57 Nachweismengen, Nachweisbeziehungen

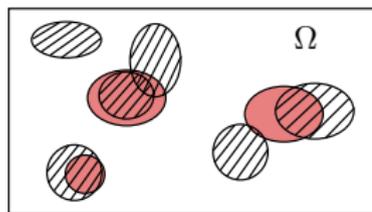


- Ω Ereignisraum, hier Menge der möglichen Eingaben bzw. Eingabefolgen.
-  Nachweismenge eines Modellfehlers
-  Nachweismenge eines tatsächlichen Fehlers

Die Nachweisbeziehungen zwischen Fehlern und Modellfehlern lassen sich über die Mengenbeziehungen veranschaulichen:

- Der Ereignisraum Ω umfasst alle Möglichkeiten der Eingaben bzw. der Eingabefolgen.
- Günstig sind die, die einen betrachteten Fehler bzw. Modellfehler nachweisen.
- Idealerweise generiert ein Fehlermodell für alle tatsächlichen Fehler mehrere Modellfehler mit ähnlichen Anregungs- und Beobachtungsbedingungen.
- Gemeinsame Nachweisbedingungen bilden sich auf mehr oder weniger große Schnittmengen der Nachweismengen ab.

3.58 Zufallstest



- Ω Ereignisraum, hier Menge der möglichen Eingaben bzw. Eingabefolgen.
-  Nachweismenge eines Modellfehlers
-  Nachweismenge eines tatsächlichen Fehlers

Zufallstests sind »Blindschüsse« in den Ereignisraum. Jede Nachweismenge hat eine »Trefferwahrscheinlichkeit« die komplett unabhängig von Treffern für anderen Nachweismengen ist. Relative Zunahme der Fehlerabdeckung unter Annahme »gleicher Formfaktor K der Dichten der MF-Rate« für Modellfehler und tatsächliche Fehler:

$$(3.15) \quad \mu_{FC}(N) = 1 - \left(\frac{N}{N_0}\right)^{-K}$$

Für einen Zufallstest lassen sich unter den getroffenen Annahmen

- Testverlängerung N_2/N_1 für eine Fehlerabdeckung,
- Fehlerabdeckung μ_{FC} für Testverlängerung N_2/N_1 und
- Formfaktor K

mit Modellfehlern bestimmen und auf tatsächliche Fehler anwenden.



3.59 Zufallstest, absolute Testanzahl

Die Unterschiede der Nachweiseigenschaften zwischen tatsächlichen und Modellfehlermengen spielen erst bei absoluten Testsatzlängen eine Rolle. Die Modellfehlerabdeckung tendiert hier gegen die Fehlerabdeckung der c -fachen Testanzahl (Abschn. 2.2.4):

$$(2.38) \quad N = c \cdot N_{MF} \quad \text{für} \quad \mu_{FC}(N) = \mu_{FCM}(N_{MF})$$

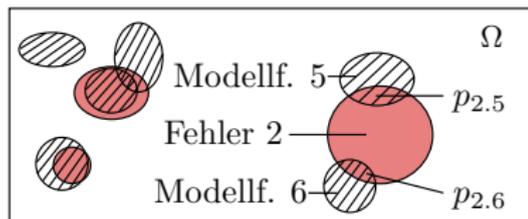
- $c < 1$: Modellfehler tendentiell strengere Nachweisbedingungen,
- $c > 1$: Modellfehler tendentiell einfachere Nachweisbedingungen.

Für Abschätzungen der Fehlerabdeckung bzw. der erforderlichen Testanzahl für tatsächliche Fehler mit Modellfehlern gut handhabbar, insbesondere für Fehlermodelle, für die sich c auf Werte nahe eins beschränken lässt, d.h. wenn die Modellfehler ähnlich gut zu befriedigene Nachweisbedingungen wie die zu erwartenden Fehler haben.

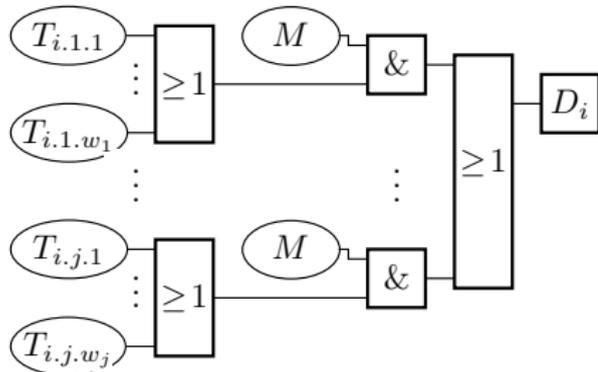
Ähnlich gut zu befriedigene Nachweisbedingungen ist umgekehrt die Anforderung des Zufallstests an ein Fehlermodell.

N, c	Effektive Testanzahl, Testskalierung.
N_{MF}	Testanzahl, mit der die Modellfehlerabdeckung bestimmt wird.
μ_{FCM}, μ_{FC}	Zu erwartende Modellfehlerabdeckung und tatsächliche Fehlerabdeckung.

3.60 Gezielte Testsuche



- Nachweismenge eines tatsächlichen Fehlers
- Nachweismenge eines Modellfehlers



T_{ijk} Test k für Modellfehler j weist Fehler i nach:

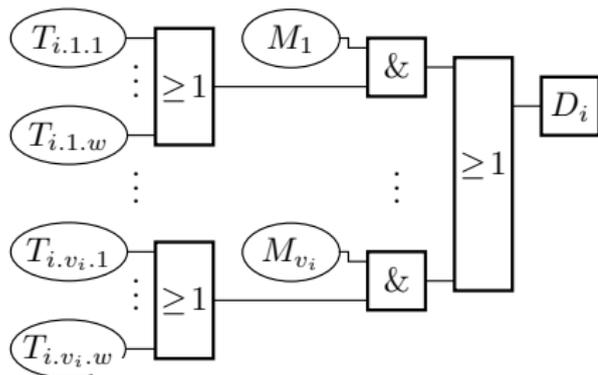
$$\mathbf{P}[T_{i,j,k}] = p_{ij} \neq f(k)$$

M für Modellfehler j werden die gesuchten w_j Tests gefunden

$$\mathbf{P}[M] = FC_M \neq f(i, j)$$

D_i Nachweis Fehler i

Für jeden Fehler i enthält die Modellfehlermenge $j = 1$ bis v_i ähnlich nachweisbare Modellfehler, für die jeweils $w \geq 1$ Tests gesucht und mit Wahrscheinlichkeit $\mathbf{P}[M] = FC_M$ gefunden werden.



T_{ijk} Test k für Modellfehler j weist Fehler i nach:

$$\mathbf{P}[T_{i.j.k}] = p_{ij} \neq f(k)$$

M_j für Modellfehler j werden die gesuchten w Tests gefunden

$$\mathbf{P}[M_j] = FC_M \neq f(i, j)$$

D_i Nachweis Fehler i

Testsuche ist schwierig und nur für FC_M Modellfehler erfolgreich (Abschn. 6.2). Wenn sich ein Test finden lässt, werden in der Regel auch $w \geq 1$ »zufällige« Tests aus der Nachweismenge gefunden:

$$D_i = \bigvee_{j=1}^{v_i} \left(\left(\bigvee_{k=1}^w T_{ijk} \right) \wedge M_j \right) = \bigwedge_{j=1}^{v_i} \left(\left(\bigwedge_{k=1}^w \bar{T}_{ijk} \right) \wedge M_j \right)$$

$$p_{\text{FD}.i} = \mathbb{P}(D_i) = 1 - \prod_{j=1}^{v_i} (1 - (FC_M \cdot (1 - (1 - p_{ij})^w))) \quad (3.18)$$

3.62 Zahlenbeispiel

$$(3.18) \quad p_{\text{FD}.i} = \mathbb{P}(D_i) = 1 - \prod_{j=1}^{v_i} (1 - (FC_M \cdot (1 - (1 - p_{ij})^w)))$$

Beispielwerte: $p_{ij} = 25\%$, $v_i = 5$ und $w = 1 \dots 5$:

$p_{\text{FD}.i}(w, FC_M)$	$w = 1$	$w = 2$	$w = 3$	$w = 4$	$w = 5$
$FC_M = 90\%$	72,0%	91,8%	97,5%	99,15%	99,70%
$FC_M = 95\%$	74,2%	93,2%	98,1%	99,47%	99,84%

Die Anzahl der Tests w , die für jeden Modellfehler gesucht werden, hat viel größeren Einfluss auf die Nachweiswahrscheinlichkeiten $p_{\text{FD}.i}$ der tatsächlichen Fehler als die Modellfehlerüberdeckung.

p_i Nachweiswahrscheinlichkeit Fehler i .

v_i Anzahl der ähnlich nachweisbaren Modellfehler für Fehler i .

FC_M Modellfehlerabdeckung.

w Nachweisanzahl, Anzahl der je Nachweismenge zufällig auszuwählender Tests.

p_{ij} Wahrscheinlichkeit, dass ein Test, der Modellfehler j nachweist, auch Fehler i findet.



3.63 Modellfehlerabdeckung $FC_M = 100\%$

Modellfehlerabdeckung $FC_M = 100\%$ vereinfacht (Gl. 3.18):

$$p_{\text{FD},i} = 1 - \prod_{j=1}^{v_i} (1 - p_{ij})^w \geq 1 - e^{-w \cdot \sum_{j=1}^{v_i} p_{ij} v_i}$$

Zu erwartende Anzahl der nicht nachweisbaren Fehler:

$$\mu_F(w) \leq \frac{1}{\#F} \cdot \sum_{i=1}^{\#F} (e^{-w \cdot \zeta_i}) \quad \text{mit } \zeta_i = \sum_{j=1}^{v_i} p_{ij} v_i$$

Wird analog zum Zufallstest für die Dichte der Fehlfunktionsrate während des Tests eine Potenzfunktion unterstellt, ergibt sich analog zu (Gl. 2.16) eine Potenzfunktion für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der gesuchten Testanzahl w je Modellfehler:

$$\mu_F(w) \leq \mu_F(w=1) \cdot w^{-K}$$

ζ_i Fehlfunktionsrate von Fehler i während des Tests.

$\mu_F, \#F$ Zu erwartende Anzahl nachweisbare Fehler, Anzahl vorhandene Fehler.

3.64 Nachweisstärke

Die Nachweisstärke DS eines Fehlermodells sei die zu erwartende tatsächliche Fehlerabdeckung für Modellfehlerabdeckung 100%, wenn ein Test je Modellefehler gesucht wird:

$$DS = 1 - \frac{\mu_F(w=1)}{\mu_F}$$

Zu erwartende tatsächliche Fehlerüberdeckung:

$$\mu_{FC} \geq 1 - (1 - DS) \cdot w^{-K} \quad (3.19)$$

Erforderliche Anzahl der zu suchenden Tests je Modellfehler:

$$w = \left(\frac{1 - DS}{1 - FC_{TRG}} \right)^{\frac{1}{K}} \quad (3.20)$$

$\mu_F, \#F$	Zu erwartende Anzahl nachweisbare Fehler, Anzahl vorhandene Fehler.
w	Nachweisanzahl, Anzahl der je Nachweismenge zufällig auszuwählender Tests.
DS, K	Nachweisstärke und Formfaktor des Fehlermodells (bzw. der Abdeckungskriterien).
FC_{TRG}	Angestrebte Fehlerüberdeckung (Erwartungswert).



Zusammenfassung

3.65 Nachweiswahrscheinlichkeit, R-Wachstum

In der Regel strebt die Nachweiswahrscheinlichkeit mit der Testanzahl mit einer abfallenden Exponentialfunktion gegen eins:

$$(3.10) \quad p_{\text{FD}}(\zeta, N) = 1 - e^{-\zeta \cdot N}$$

Genaugenommen gilt das nur für Systeme und Fehler ohne Gedächtnis, ist aber für sehr lange Zufallstests auch sonst brauchbar.

Mit dieser erst hier hergeleiteten Beziehung gelten weiterhin die zuvor mit einfacheren Modellannahmen hergeleiteten Beziehungen zwischen Fehlfunktionsrate, Fehleranzahl, Zuverlässigkeit und Testanzahl:

$$(2.16) \quad \mu_{\text{F}}(N_2) = \mu_{\text{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1$$

$$(2.23) \quad \zeta_{\text{F}}(N) \stackrel{(\leq 1)}{=} \frac{\mu_{\text{F}}(N) \cdot K}{N}$$

$$(2.29) \quad R_{\text{F}}(N) \stackrel{(\geq 1)}{=} \frac{1}{\zeta_{\text{F}}(N)} = R_{\text{F}}(N_0) \cdot \left(\frac{N}{N_0}\right)^{K+1}$$

Die Kernthese der Vorlesung, dass in Iterationen aus Zufallstests und Beseitigung aller nachweisbaren Fehler die Fehleranzahl mit Exponent $0 < K < 1$ ab- und die Zuverlässigkeit mit Exponent $K + 1$ zunehmen, steht nach diesem Abschnitt auf einem festeren Fundament.

3.66 Fehler- und Modellfehlerabdeckung

Fehlernachweis ist Zufall. Für die Bewertung und gezielte Auswahl dienen Fehlerannahmen (Modellfehler).

Gut beschreibbar ist die Beziehung zwischen Fehler- und Modellfehler nachweis für Zufallstest. Die Fehlerabdeckung in Abhängigkeit von der relativen Testsatzverlängerung ist unter sehr allgemeinen Bedingungen für Modellfehler und tatsächliche Fehler gleich:

$$(3.15) \quad \mu_{\text{FC}}(N) = 1 - \left(\frac{N}{N_0}\right)^{-K}$$

Bei der absoluten Testsatzlänge tendiert die Modellfehlerabdeckung gegen die der tatsächlichen Fehlerabdeckung für die c -fache Testanzahl.

$$(2.38) \quad N = c \cdot N_{\text{MF}} \quad \text{für} \quad \mu_{\text{FC}}(N) = \mu_{\text{FCM}}(N_{\text{MF}})$$

Die Testlängenskalierung c hängt vom Fehlermodell ab. Am vertrauenswürdigsten erscheinen Abschätzungen, für die sich c auf Werte nahe eins beschränken lässt, d.h. für Fehlermodelle, die Modellfehler generieren, die sich ähnlich gut wie die tatsächlich zu erwartenden Fehler nachweisen lassen.

3.67 Gezielte Testauswahl

Das Versuchsschema ist anders als beim Zufallstest. Statt blinder Auswahl werden für v_i ähnlich nachweisbare Modellfehler je w Tests gesucht, die mit Wahrscheinlichkeiten p_{ij} auch den tatsächlichen Fehler nachweisen.

Man braucht ein Fehlermodell, das für jeden zu erwartenden Fehler ähnlich nachweisbare Modellfehler generiert. Das ist viel schwerer zuzusichern als die für den Zufallstest geforderten »ähnlich gut nachweisbaren« Modellfehler.

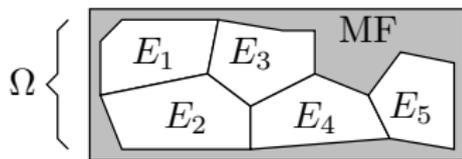
Damit von den w Tests mit hinreichender Wahrscheinlichkeit mindestens einer zufällig den Fehler nachweist, muss w mindestens die Größenordnung des Kehrwerts der schlechtesten p_{ij} haben.

Eine Beispielrechnung hat gezeigt, dass die Modellfehlerabdeckung bei gezielter Testauswahl offenbar kein allzu nützliches Mass für die Abschätzung der tatsächlichen Fehlerabdeckung ist.



Operationsprofil

3.68 Operationsprofil



- Ω Eingaberaum
- E_i Äquivalenzklasse i
- MF** unzulässige Eingaben (Fehlfunktion)

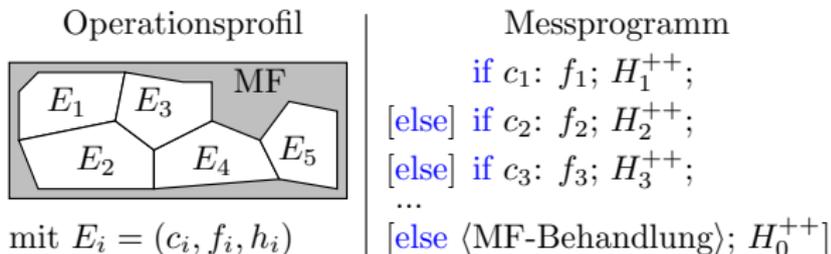
Der **Eingaberaum** Ω eines IT-Systems umfasst viele Funktionen, die für unterschiedliche Aufgaben unterschiedlich häufig mit unterschiedlichen Daten und Datenbereichen genutzt werden.

Komplexe Systeme bieten sogar für viele Aufgaben mehrere Eingabe- und Lösungsmöglichkeiten (verg. Folie 1.101).

Äquivalenzklassen sind Eingabebereiche mit ähnlicher Verarbeitung und Nutzung.

Ein **Operationsprofil** beschreibt die relative Nutzungshäufigkeit der Äquivalenzklassen und hat erheblichen Einfluss auf die Nachweiswahrscheinlichkeiten und Fehlfunktionsraten der vorhandenen und modellierten Fehler.

3.69 Messen von Operationsprofilen



Eine Äquivalenzklasse hat eine Funktion f_i die unter Bedingung c_i mit einer Nutzungshäufigkeit h_i ausgeführt wird. Die Nutzungshäufigkeiten h_i lassen sich durch Einbau* von Ausführungszählern H_i messen:

$$h_i = \frac{H_i}{N}$$

Die Ausführungsbedingungen müssen sich gegenseitig ausschließen, bzw. Modellierung wie im Bild durch »else if«.

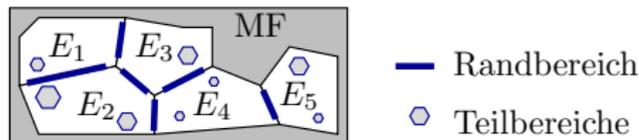
Für unzulässige Eingaben, also solche, die zu keiner Äquivalanzklasse gehören, ist das Sollverhalten eine Fehlfunktionsbehandlung.

* Bei Software als Instrumentierung bezeichnet, vergl. Folie 2.40).



Testauswahl

3.70 Test mit mehreren Operationsprofilen



Systeme, die mit unterschiedlichen Operationsprofilen genutzt werden, sind zur Zusicherung einer ausreichenden Zuverlässigkeit nach

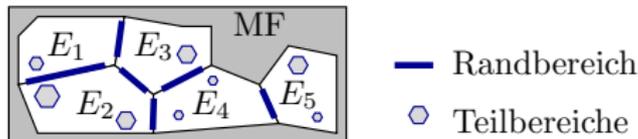
$$(2.30) \quad R_F(N) \stackrel{(\geq 1)}{=} \frac{N}{K \cdot \mu_F(N)}$$

mit jedem Operationsprofil mit ausreichender Testanzahl N zu testen.

Die initialen Operationsprofile beschreiben die Nutzersicht. Nach dem Pareto-Prinzip nimmt die Häufigkeit der Fehler mit der verursachten Fehlfunktionsrate, an der sie nachweisbar sind ab (vergl. Gl. 2.19).

Das deutet darauf, dass die mit zunehmender Testanzahl noch nicht nachweisbaren Fehler von immer kleineren Äquivalenzklassen gehören, die immer seltener zufällig ausgewählt werden.

3.71 Bereichsgrenzen und Wichtung



Bekannte Bereiche mit üblicherweise schlecht nachweisbaren Fehlern sind Bereichsgrenzen. Eine Beschränkung auf Werte nahe an den Bereichsgrenzen erhöhen deren Auftrittshäufigkeit und darüber die Nachweiswahrscheinlichkeiten der dort verorteten Fehler erheblich.

Die fehlerorientierte Bevorzugung von Eingabebereichen wird im weiteren als Wichtung bezeichnet.

Für unbekannte Unterbereiche schlecht nachweisbarer Fehler lassen sich nur Abdeckungskriterien bzw. Modellfehler angeben, die sich Nachweisbedingungen teilen.

Statt einer expliziten Suche der Unterbereiche genügt die Suche von Wichtungen, die den Kriteriennachweis soweit verbessern, dass diese mit akzeptabler Testanzahl ausreichend abgedeckt werden.

3.72 Suche Eingabebedingungen bzw. Eingaben

Die Abdeckungskriterien, bzw. Modellfehler für die unbekanntenen Unterbereiche mit schlecht nachweisbaren Fehlern werden über eine einfache Siebmethode bestimmt, die gleichzeitig die Tests für die Anwenderoperationsprofile und Äquivalenzklassenränder auswählt:

Zusammenstellen aller Abdeckungskriterien. Streichen alle mit

- den Tests der Anwenderoperationsprofile und
- den Tests für die Bereichsgrenzen

ausreichend abgedeckter Kriterien. Für die Suche der Tests bzw. Wichtungen für die restlichen Abdeckungskriterien gibt es zwei Wege:

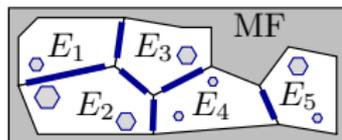
- 1 Suche von Eingabebedingungen für den Kriteriennachweis anhand der Testobjektbeschreibung und
- 2 Eingabesuche durch Ausführung, Bewertung, Mutation und Kombination gut bewerteter Eingaben (genetische Algorithmen).

Ersteres hat sich für Hardware bewährt, für zweites gibt es erste Erfahrungen für Software, auch große Systeme.



Zuverlässigkeitsgewinn

3.73 Test mit mehreren Operationsprofilen



- Randbereich
- ⬡ Teilbereiche

$$(2.27) \quad \mu_F(N) = \mu_F(N_0) \cdot \left(\frac{N}{N_0}\right)^{-K} \quad \text{mit } 0 < K < 1$$

$$(2.30) \quad R_F(N) \stackrel{(\geq 1)}{=} \frac{N}{K \cdot \mu_F(N)}$$

Modellannahme: Test mit $\#OP$ verschiedenen Operationsprofilen, mindestens ein Nutzungsoperationsprofil, der Rest fehlerorientiert gesuchte Operationsprofile. Jedes Operationsprofil weist andere Fehler bevorzugt nach.

N_0, N	Bezugstestsanzahl, Anzahl der Tests incl. N_0 .
$\mu_F(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$R_F(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.
(≤ 1)	Der errechnete Wert ist eine Untergrenze. Der tatsächliche Wert ist mindestens eins.
$\#OP$	Anzahl der unterschiedlichen Operationsprofile, mit denen getestet wird.



3.74 Modellrechnung für den Idealfall

... andere Fehler gut nachweisbar bedeutet im Idealfall, dass jedes Operationsprofil die Fehleranzahl unabhängig von allen anderen um einen Faktor N_i/N_0 verringert:

$$\mu_F = \mu_F(N_0) \cdot \prod_{i=1}^{\#OP} \left(\frac{N_i}{N_0}\right)^K$$

Für übereinstimmende Testanzahl $N_i = N$:

$$\mu_F = \mu_F(N_0) \cdot \left(\frac{N}{N_0}\right)^{\#OP \cdot K} \quad (3.21)$$

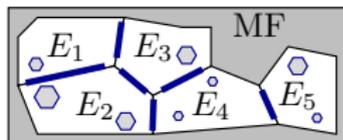
Für die Zuverlässigkeit in (Gl. 2.30) ist N die Anzahl der Tests mit dem Anwendungsoperationsprofil:

$$R_F(\#OP \cdot N) = \frac{N}{K} \cdot \left(\frac{N}{N_0}\right)^{\#OP \cdot K} \sim N^{1+\#OP \cdot K} \quad (3.22)$$

Die Anzahl der Operationsprofile erhöht im Idealfall den Exponenten.

N_0, N	Bezugstestsanzahl, Anzahl der Tests je Operationsprofil incl. N_0 .
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).
$\#OP$	Anzahl der unterschiedlichen Operationsprofile, mit denen getestet wird.

3.75 Abdeckungsanzahl



- Randbereiche
- Teilbereiche

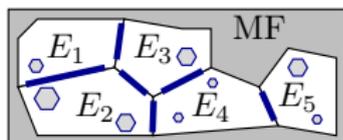
```

if  $c_1: f_1; H_1^{++}$ ;
[else] if  $c_2: f_2; H_2^{++}$ ;
[else] if  $c_3: f_3; H_3^{++}$ ;
...
[else] ⟨MF-Behandlung⟩;  $H_0^{++}$ ;]
    
```

Die erforderliche Abdeckungsanzahl für Kriterien, Äquivalanzklassen, Anweisungen, Zweige oder Bedingungen (vergl. Abschn. ###), ..., ist über das Modell »gezielte Suche von $\geq w$ Tests je Modellfehler« abschätzbar. Zu erwartenden Fehlerabdeckung mindestens:

$$(3.19) \quad \mu_{FC} \geq 1 - (1 - DS) \cdot w^{-K}$$

$\mu_F, \#F$	Zu erwartende Anzahl nachweisbare Fehler, Anzahl vorhandene Fehler.
w	Nachweisanzahl, Anzahl der je Nachweismenge zufällig auszuwählender Tests.
DS, K	Nachweisstärke und Formfaktor des Fehlermodells (bzw. der Abdeckungskriterien).
FC_{TRG}	Angestrebte Fehlerüberdeckung (Erwartungswert).



- Randbereiche
- Teilbereiche

```

if  $c_1: f_1; H_1^{++}$ ;
[else] if  $c_2: f_2; H_2^{++}$ ;
[else] if  $c_3: f_3; H_3^{++}$ ;
...
[else <MF-Behandlung>;  $H_0^{++}$ ;]
    
```

Ausreichende Abdeckungsanzahl je Kriterium:

$$(3.20) \quad w = \left(\frac{1-DS}{1-FC_{TRG}} \right)^{\frac{1}{K}}$$

Beispielabschätzungen für die erforderliche Kriterienabdeckung für $DS = 60\%$ bis 90% und $K = 0,5$:

$K = 0,5$	$FC_{TRG} = 90\%$	$= 95\%$	$= 99\%$	$= 99,5\%$
$DS = 60\%$	$w = 16$	$w = 64$	$w = 256$	$w = 1024$
$DS = 90\%$	$w = 1$	$w = 4$	$w = 16$	$w = 64$

- w Nachweisanzahl, Anzahl der je Nachweismenge zufällig auszuwählender Tests.
- DS, K Nachweisstärke und Formfaktor des Fehlermodells (bzw. der Abdeckungskriterien).
- FC_{TRG} Angestrebte Fehlerüberdeckung (Erwartungswert).



DIC-Test mit Bitwichtung

3.77 Bitweise Wichtung

Für integrierte Digitalschaltungen (DIC) hat sich fehlerorientierte Wichtung als verlässlich einfach erwiesen. In [HaK93] konnte gezeigt werden, dass bitweise Wichtung ausreicht, um auch für große Benchmarks alle Haftfehler nachzuweisen.

Bei digitale Schaltungen haben alle Signalwerte den Wertebereich $\{0, 1\}$. Die Bitwichtung ist die Wahrscheinlichkeit »Bitwert eins«:

$$g(x_i) = \mathbb{P}(x_i = 1)$$

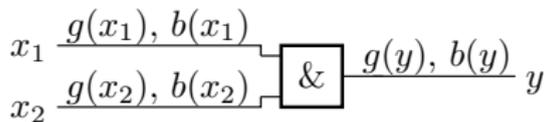
Daran angelehnt ist die Beobachtbarkeit eines Bits die Wahrscheinlichkeit, dass eine Invertierung mindestens ein Ausgabebit invertiert.

Geänderte Eingabewichtungen ändern die Wichtungen und Beobachtbarkeiten interner Signale und darüber die Nachweiswahrscheinlichkeiten und Fehlfunktionsraten der einzelnen Fehler zum Teil erheblich.

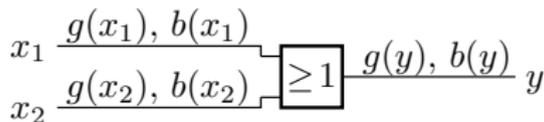
DIC	Integrierter digitaler Schaltkreis (Integrated digital circuit).
$g(\dots)$	Wichtung, Auftrittshäufigkeit des Signalwerts 1.
$b(\dots)$	Beobachtbarkeit, Wahrscheinlichkeit, das eine Invertierung ein Ausgabebit ändert.

3.78 Wichtungen und Beobachtbarkeit

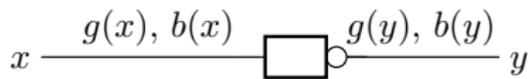
Die Wichtung einer UND-Verknüpfung ist das Produkt der Wichtungen der Operanden. ... Die Eingabe einer UND-Operation ist beobachtbar, wenn die andere Eingabe eins ist, ...



$$\begin{aligned}
 b(x_2) &= b(y) \cdot g(x_1) \\
 b(x_1) &= b(y) \cdot g(x_2) \\
 g(y) &= g(x_1) \cdot g(x_2)
 \end{aligned}$$



$$\begin{aligned}
 b(x_1) &= b(y) \cdot (1 - g(x_2)) \\
 b(x_2) &= b(y) \cdot (1 - g(x_1)) \\
 g(y) &= 1 - (1 - g(x_1)) \cdot (1 - g(x_2))
 \end{aligned}$$



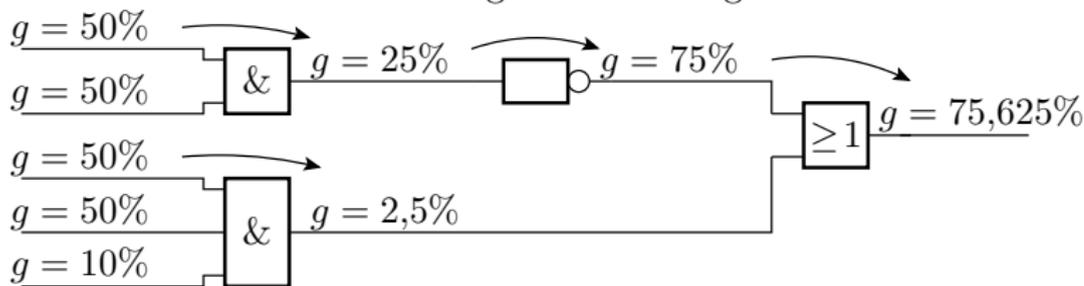
$$\begin{aligned}
 b(x) &= b(y) \\
 g(y) &= 1 - g(x)
 \end{aligned}$$

Wichtungen werden in Richtung und Beobachtbarkeiten entgegen der Richtung des Berechnungsflusses bestimmt.

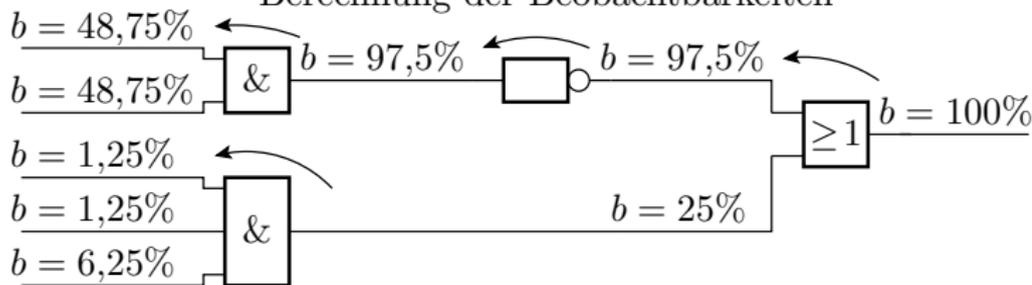
$g(\dots)$ Wichtung, Auftrittshäufigkeit des Signalwerts 1.

$b(\dots)$ Beobachtbarkeit, Wahrscheinlichkeit, das eine Invertierung ein Ausgabebit ändert.

Berechnung der Wichtungen



Berechnung der Beobachtbarkeiten



Berechnung der Nachweiswahrscheinlichkeiten:

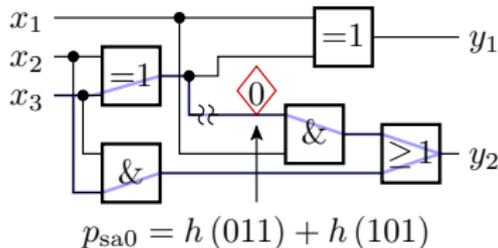
$$p_{\text{sa}0}(x_i) = b(x_i) \cdot g(x_i)$$

$$p_{\text{sa}1}(x_i) = b(x_i) \cdot (1 - g(x_i))$$

3.80 Rekonvergente Auffächerung

Bei rekonvergenter Auffächerung werden abhängige Zufallswerte log. verknüpft, so dass die einfachen Regel für $\mathbb{P}(A \wedge B)$ etc. nicht gelten.

Berechnung der Nachweiswahrscheinlichkeiten über Wertetabellen:



— rekonvergente
Auffächerung

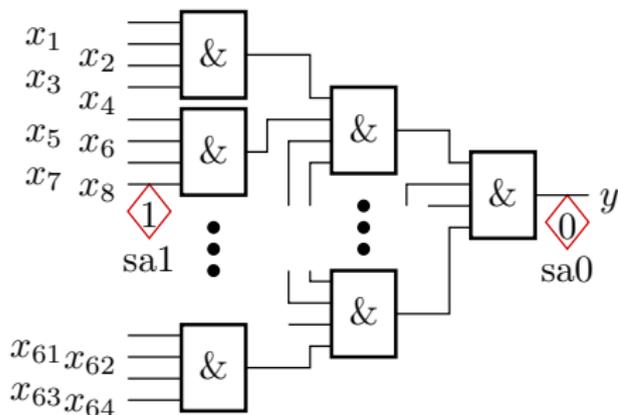
■ Eingaben die den
Fehler nachweisen

Eingabe			Ausg.		$h(\mathbf{x})$ für $g(x_i) = g$		
x_3	x_2	x_1	y_2	y_1	$g=0,5$	$g=0,3$	$g=0,7$
0	0	0	0	0	0,125	0,343	0,027
0	0	1	0	1	0,125	0,147	0,036
0	1	0	0	1	0,125	0,147	0,036
0	1	1	1	0	0,125	0,036	0,147
1	0	0	0	1	0,125	0,147	0,036
1	0	1	1	0	0,125	0,036	0,147
1	1	0	1	0	0,125	0,036	0,147
1	1	1	1	1	0,125	0,027	0,343

$$p_{\text{sa}0} : 0,25 \quad 0,072 \quad 0,294$$

- x_i, y_i Eingabe- und Ausgabesignale.
- g Wichtung der Eingabesignale x_1, x_2 und x_3 .
- $h(\mathbf{x})$ Auftrittshäufigkeit des Eingabevektors $x_3x_2x_1$.

3.81 Fehlerabdeckung und Wichtung



Nachweiswahrscheinlichkeiten für $g(x_i) = g$:

- der 64 sa1-Fehler

$$p_{\text{sa1}}(1) = g^{63} \cdot (1 - g)$$

$$p_{\text{sa1}}(N) = 1 - e^{-g^{63} \cdot (1-g) \cdot N}$$

- des einen sa0-Fehlers

$$p_{\text{sa0}}(1) = g^{64}$$

$$p_{\text{sa0}}(N) = 1 - e^{-g^{64} \cdot N}$$

Zu erwartende Fehlerabdeckung als Mittelwert der Nachweiswahrscheinlichkeiten aller 65 Haftfehler:

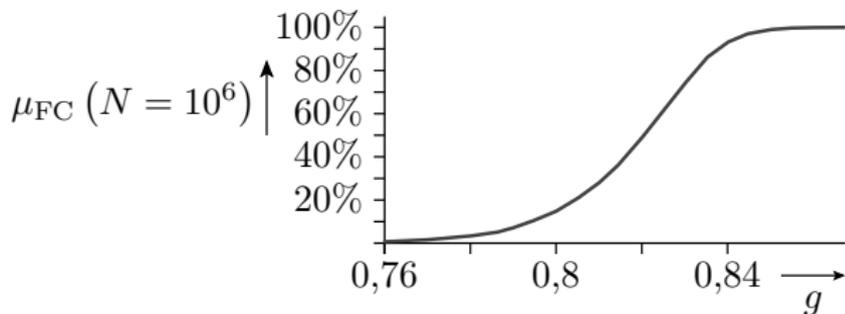
$$\mu_{\text{FC}}(N) = 1 - \frac{64 \cdot e^{-g^{63} \cdot (1-g) \cdot N} + e^{-g^{64} \cdot N}}{65}$$

g Wichtung der Eingabesignale x_1 bis x_{64} .

N Anzahl der Tests.

$\mu_{\text{FC}}(N)$ Zu erwartende Fehlerabdeckung in Abhängigkeit von der Testanzahl.

$$\mu_{FC}(N = 10^6) = 1 - \frac{64 \cdot e^{-g^{63} \cdot (1-g) \cdot 10^6} + e^{-g^{64} \cdot 10^6}}{65}$$



Eine Erhöhung der Wichtung an allen Eingängen von $g \leq 76\%$ auf $g \geq 86\%$ erhöht die Fehlerabdeckung für $N = 10^6$ Tests von 0 auf 1.

Allgemein sind zur Erzielung einer hohen Fehlerabdeckung die Wichtungen $g(x_i)$ für alle Eingänge x_i individuell anzupassen.

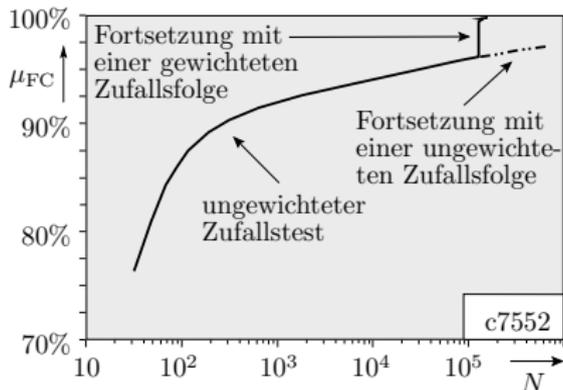
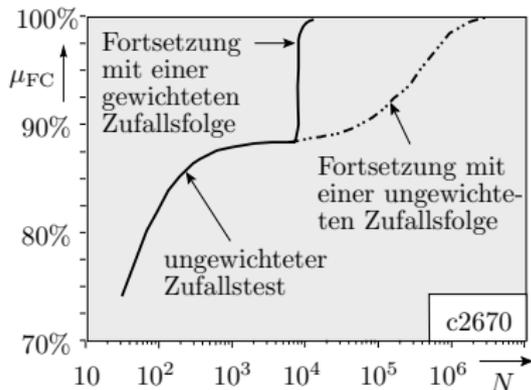
g Wichtung der Eingabesignale x_1 bis x_{64} .

N Anzahl der Tests.

$\mu_{FC}(N)$ Zu erwartende Fehlerabdeckung in Abhängigkeit von der Testanzahl.

3.83 Anwendung auf reale Schaltungen

- Test mit 10^4 bzw. 10^5 ungewichteten Zufallsmustern, die 90% bzw. 95% der Haftfehler nachweisen.
- Gezielte Testberechnung für die restlichen Haftfehler.
- Änderung der Bitwichtung zur Erhöhung der Nachweiswahrscheinlichkeiten noch nicht erfasster Haftfehler (siehe nächste Folie).
- Weitere 10^4 bzw. 10^5 gewichtet Zufallstests weisen alle verbleibenden nichtredundanten Modellfehler nach.



μ_{FC}, N Zu erwartende Haftfehlerabdeckung, Testanzahl.

3.84 Bestimmung der Wichtungen

Testvektor:		1	2	3	4	5	6	7	8	9	10	11	$g(x_i)$
Eingabebit	x_1	1	X	0	1	0	0	X	1	0	1	1	0,5
	x_2	1	1	X	1	1	X	1	X	X	X	X	1
	x_3	0	0	1	0	0	X	0	X	1	0	0	2^{-3}
	x_4	1	0	X	0	X	0	1	X	1	X	0	0,5
	x_5	1	1	1	X	0	1	1	1	X	0	1	$1-2^{-3}$

Suche einer Testeingabe für jeden nicht abgedeckten Modellfehler mit möglichst wenig Care-Bits. Beschränkung auf nur 5 verschiedene Wichtungswerte:

- $g(x_i) = 0$, wenn alle Tests $x_i = 0$ oder X verlangen,
- $g(x_i) = 1$, wenn alle Tests $x_i = 1$ verlangen,
- $g(x_i) = 2^{-a}$ mit $a \in \{3, 4, ..\}$ bei viel häufiger 0 als 1,
- $g(x_i) = 1 - 2^{-a}$ mit $a \in \{3, 4, ..\}$ bei viel häufiger 1 als 0 und
- sonst $g(x_i) = 50\%$ (ungewichtet).

X

Signalwert ungültig oder für den Fehlernachweis ohne Bedeutung.

a

Anzahl der UND- oder ODER- zu verknüpfenden ungewichteten Bits.



Testvektor:		1	2	3	4	5	6	7	8	9	10	11	$g(x_i)$
Eingabebit	x_1	1	X	0	1	0	0	X	1	0	1	1	0,5
	x_2	1	1	X	1	1	X	1	X	X	X	X	1
	x_3	0	0	1	0	0	X	0	X	1	0	0	2^{-3}
	x_4	1	0	X	0	X	0	1	X	1	X	0	0,5
	x_5	1	1	1	X	0	1	1	1	X	0	1	$1-2^{-3}$

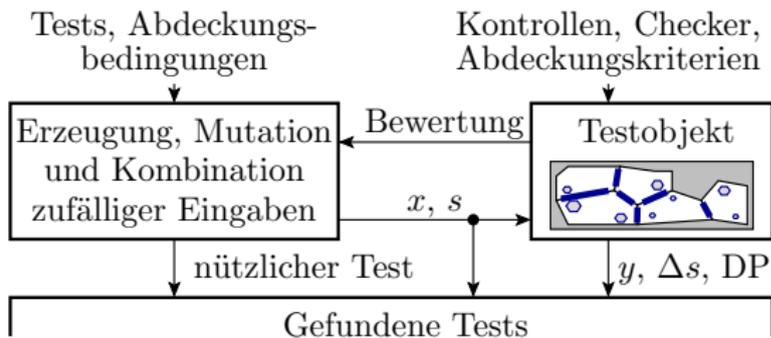
- Eine größere Wertevielfalt und genauere Berechnungen haben sich mit den gewählten Testlängen als unnötig erwiesen.
- Die Beschränkungen auf fünf Wichtungswerte vereinfacht die Implementierung als Selbsttesttests (####).
- Für Schaltkreisselbsttests sind Testlängen $N \leq 10^9$, auch einige Zehnerpotenzen mehr, kein wichtiger Kostenfaktor.
- Zur Erhöhung der Abdeckungsanzahl auf $w > 1$ genügt eine proportionale Erhöhung der Testanzahl.

Lange Zufallstests mit 100% Haftfehlerabdeckung und Abdeckungsanzahl $w > 1$ versprechen sehr hohe Abdeckungen für tatsächliche Fehler und einen hohen Zuverlässigkeitsgewinn.



Testsuche für Software

3.86 Testsuche für Software

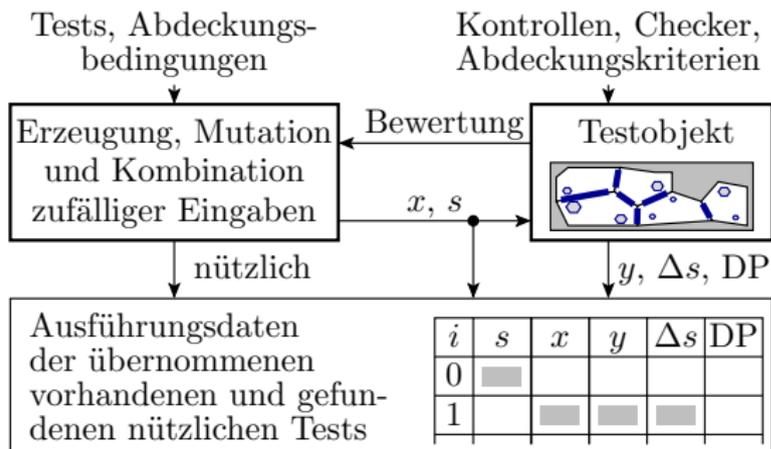


Testsuche für Software umfasst

- das mit Abdeckungszählern, Bewertungsberechnungen und internen Kontrollen instrumentierte Testobjekt und
- ein Rahmenprogramm, das unter Nutzung bekannter Eingaben und Abdeckungsbedingungen über Auswürfeln, Mutation und Kombination nützliche Eingaben sucht.

Ergebnis sind gefundene Test mit allen Infos zur Abarbeitung.

x, y, DP Eingaben, Ausgaben, erkannte Probleme.
 $s, \Delta s$ Objektraum, Änderungen des Objektraums.



Vorgegebene Tests werden übernommen, Test für Vorgabeoperationsprofile und Bereichsgrenzen ausgewürfelt, bevor die zielgerichtete Suche beginnt. Erst dann werden Abdeckungsbedingungen für unzureichend abgedeckte Kriterien gesucht bzw. Bewertungsberechnungen instrumentiert (Folie 2.40).

Ergebnis der Testberechnung sind »nützliche Tests« die

- die Kriterienabdeckung erhöhen oder
- Fehler nachweisen.

Fortsetzung siehe Abschnitt 7.3.



3.88 Querverbindung Fuzz-Tests

Fuzz-Tests bezeichnen den Software-Test mit zufälligen Eingaben, vornehmlich zur Provokation von Abstürze zur Suche von Sicherheitslücken.

- **Ursprung:** Ein Professor hatte die Idee, die Aufgabe zu stellen, UNIX-Werkzeuge mit unsinnigen Eingaben zum Absturz zu bringen. Ergebnis überwältigend. Am erfolgreichsten war ein Zufallsfolge von 1024 Zeichen, die über ein nicht abgefangenen Pufferüberlauf bei den meisten Werkzeugen interne Daten mit unsinnigen Werten überschrieben und die Programme darüber zum Absturz gebracht hat.
- **American Fuzzy Loop (AFL):** Veränderung bestehender legaler Eingaben mit Überwachung und Speicherung, welche Änderungen in der Eingabe welche Änderungen in der Programmausführung bewirken. Dadurch werden Tests gefunden, die nicht nur verschiedenste Bereiche zulässiger Eingaben, sondern auch verschiedenste Programmausführung abdecken.



- Holler : Grammatik-basierter Würfel für zulässige, meist sinnlose Java-Programme für den Test des Java-Script-Interpretes, auch geeignet zur Aufspaltung gültige Java-Scripte in mutierbare Teile und Mutation.
- Microsoft hat mit SAGE sein eigenen Fuzzer für den Test auf Sicherheitslücken
- Google gibt für den Test ihres Chrome-Browsers mit ClusterFuzz $5 \cdot 10^7$ untersuchten Fuzz-Tests pro Tag zur Suche von Sicherheitslücken an und auch, dass zusätzlich zur Kontrolle auf Abstürze mit SANITY zahlreiche Plausibilitätstests instrumentiert werden.

Die in der Vorlesung angedachte operationsprofilorientierte Testauswahl ist im Grunde eine Fuzz-Testsuche für eine größere Vielfalt an Abdeckungskriterien und Kontrollen, bzw. der Vorschlag, Fuzz-Tests mit erweiterter Zielstellung weiterzuentwickeln.

Im weiteren wird davon ausgegangen, dass es in Zukunft unter welchen Namen auch immer Werkzeuge für eine automatische Testsuche mit vorgebbaren Abdeckungs- und Überwachungskriterien geben wird.



Zusammenfassung



3.90 Operationsprofil

Ein Operationsprofil beschreibt die Nutzungshäufigkeiten der einzelnen Eingaben und hat erheblichen Einfluss auf die Nachweiswahrscheinlichkeiten der Fehler. Für jedes neue Operationsprofil rücken andere Fehler in den Bereich der mit $N \gg 1$ Tests zufällig nachweisbaren Fehler.

Im günstigsten Fall nimmt die Fehleranzahl mit der $\#OP \cdot K$ -ten Potenz ab und die Zuverlässigkeit mit der $1 + \#OP \cdot K$ -ten Potenz zu: Wie weit dieses Potential nutzbar ist, wird die zukünftige Forschung zeigen.



3.91 Testauswahl, Fuzzifizierung

Systeme, die mit unterschiedlichen Operationsprofilen genutzt werden, sind mit allen Operationsprofilen der Nutzung und weiteren für den Fehlernachweis günstigen Operationsprofilen (Grenzwerte) zu testen.

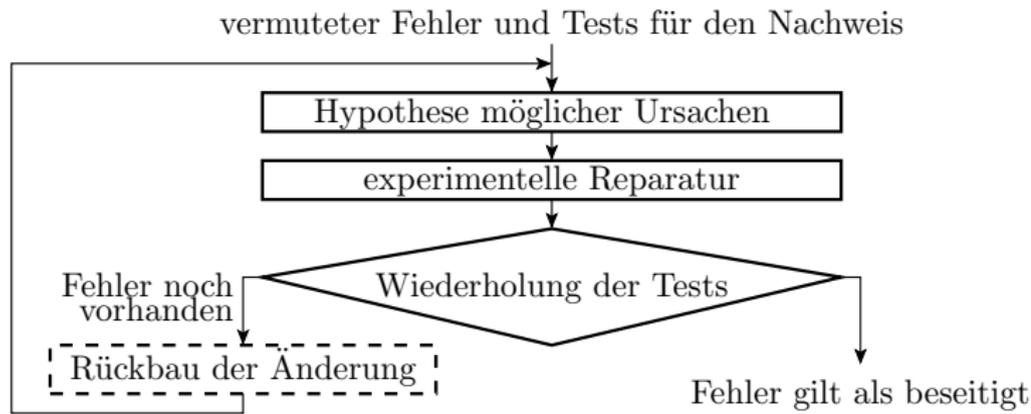
Im modernen Softwareentwurf werden entwurfsbegleitend typische Nutzungsfälle, Grenzfälle, sicherheitskritische Betriebsfälle, ... als Entwurfsziele und symbolische Test gesammelt. Der folgerichtige Weg für die Testauswahl ist die Konfiguration von Zufallszahlengeneratoren mit allen aus der Spezifikation ableitbaren »typischen« Operationsprofilen und Operationsprofilen für »spezielle Testabsichten«, mit denen dann für jedes Operationsprofil ausreichend viele Beispiele generiert werden.

Für Software findet man operationsprofilorientierte Testauswahl eher unter dem Suchbegriff Fuzz-Tests.



Fehlerbeseitigung

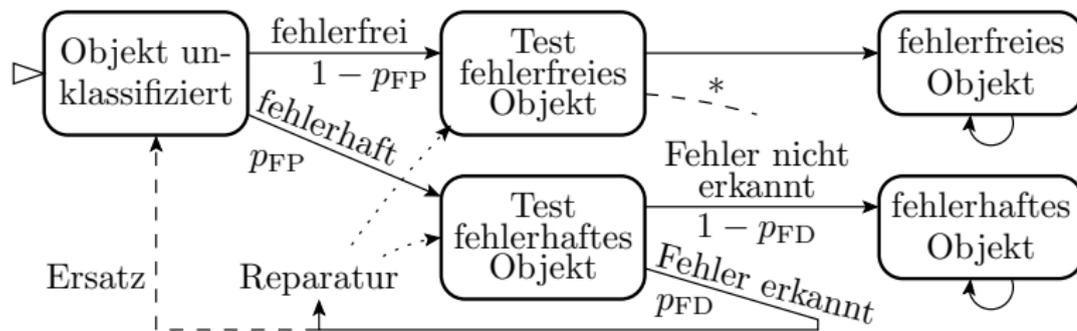
3.92 Experimentelle Reparatur nach Abschn. 2.1.1



- Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung.
- Beseitigt alle vom Test nachweisbaren Fehler.
- Zur Vermeidung neu entstehender Fehler bei der Reparatur, Rückbau nach erfolglosen Reparaturversuchen.

Voraussetzung: deterministische Fehlerwirkung (Abschn. 2.3.2).

3.93 Beseitigung eines Fehlers als Markov-Kette



Ein Fehler i

- ist mit einer Wahrscheinlichkeit p_{FP} vorhanden und
- wird mit einer Wahrscheinlichkeit p_{FD} erkannt.

Für die Fehlerbeseitigung sind zwei Ansätze zu unterscheiden:

- Ersatz Gesamtsystem,
- Reparatur z.B. durch Ersatz fehlerhafter Teilsysteme.

p_{FP}	Wahrscheinlichkeit, dass der Fehler vorhanden (present) ist.
p_{FD}	Fehlernachweiswahrscheinlichkeit (Probability of fault detection).
*	Zusatzkante für Phantomfehler zur Vereinfachung vernachlässigt.



3.94 Ersatz oder Reparatur

Beim Ersatz erkannter defekter Systeme vor dem Einsatz aus demselben Fertigungsprozess

- haben Original- und Ersatzteile dieselbe Ausbeute Y und
- muss das Originalteil im Mittel μ_{Repl} mal ersetzt werden:

$$\mu_{\text{Repl}} = \frac{1}{Y} - 1 \quad (3.23)$$

- Fertigungskosten pro verkauftes System $\approx \frac{1}{Y}$ mal so hoch wie die Kosten für die Fertigung eines einzelnen Systems.

Reparatur: Tausch kleinerer Bausteine, die mit geringerem Risiko defekt sind. Dafür Zusatzaufwand für Lokalisierung, Reparatur, Ersatzteile, ...

Ersatz ist kostengünstigster bei hoher und Reparatur bei geringer Ausbeute.

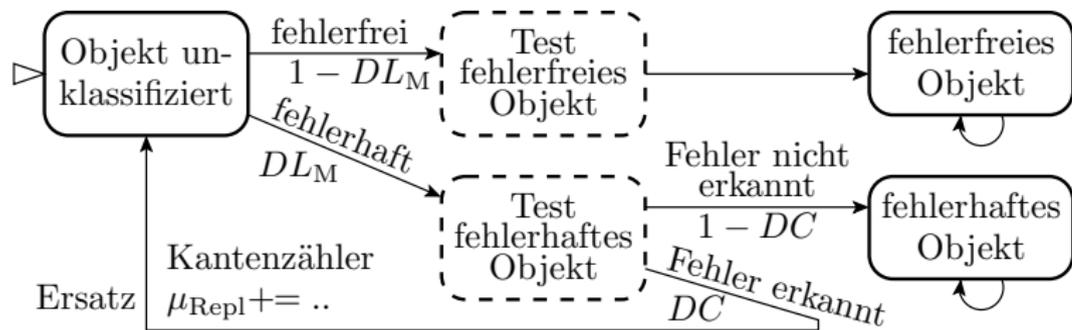
μ_{Repl}
 Y

Zu erwartende Anzahl der Ersetzungen.
Ausbeute (Yield).



Ersatz

3.95 Fehlerbeseitigung durch Ersatz

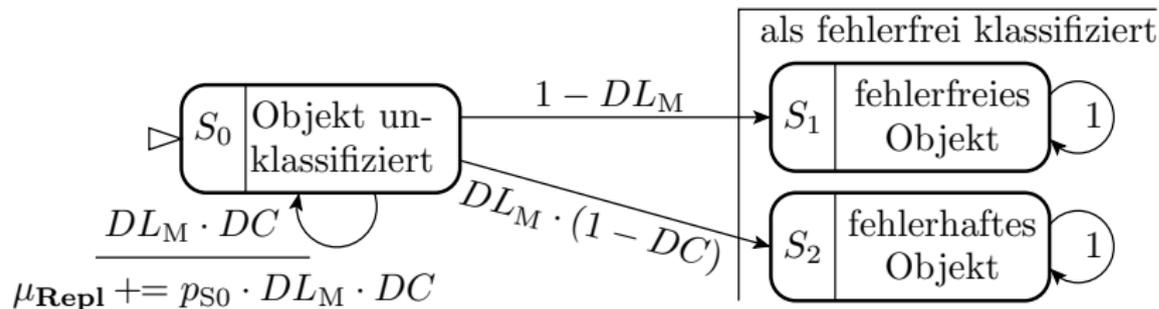


Original- und Ersatzobjekte sind mit Wahrscheinlichkeit DL_M defekt. Je Schritt wird aus unklassifizierten Objekten mit Wahrscheinlichkeit

- $1 - DL_M$ ein fehlerfreies Objekt oder
- $DL_M \cdot (1 - DC)$ ein nicht erkanntes defektes Objekt,
- sonst wird es ersetzt und ist damit wieder unklassifiziert.

DL_M	Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.
DC	Defektdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
μ_{Repl}	Kantenzähler für die zu erwartende Anzahl der Ersetzungen.

3.96 Vereinfachte Markov-Kette



Nach Ersatz aller erkennbar defekten Objekte:

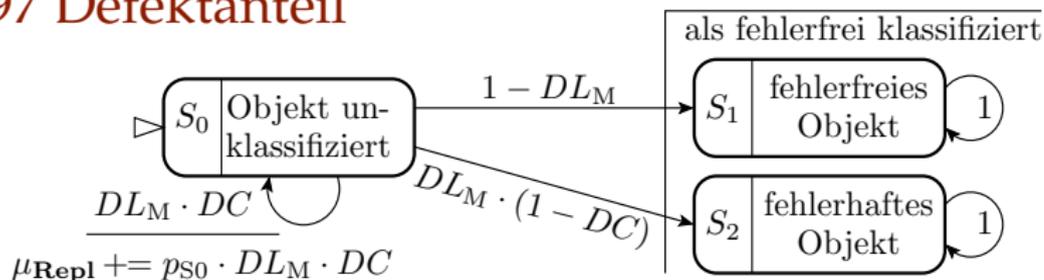
$$\lim_{\#Repl \rightarrow \infty} (p_{S_0}) = \lim_{\#Repl \rightarrow \infty} (DL_M \cdot DC)^{\#Repl} = 0$$

$$\lim_{\#Repl \rightarrow \infty} (p_{S_1}) = (1 - DL_M) \cdot \sum_{\#Repl=0}^{\infty} (DL_M \cdot DC)^{\#Repl} \stackrel{\text{SGS}}{=} \frac{1 - DL_M}{1 - DL_M \cdot DC}$$

$$\lim_{\#Repl \rightarrow \infty} (p_{S_2}) = DL = 1 - \lim_{\#Repl \rightarrow \infty} (p_{S_1}) = \frac{DL_M \cdot (1 - DC)}{1 - DL_M \cdot DC}$$

- DC Defektabdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
- DL_M Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.
- $\#Repl$ Anzahl der Ersetzungen.
- SGS Summe einer geometrischen Reihe: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.97 Defektanteil



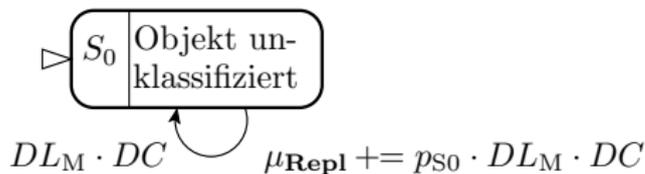
Der Defektanteil nach Aussortieren als Wahrscheinlichkeit, dass ein als fehlerfrei ausgewiesenes Objekt fehlerhaft ist $\lim_{\#Repl \rightarrow \infty} (p_{S_2})$ wurde in Abschn. 2.1.7 durch Subtraktion der Anzahl der erkannten defekten Produkte von der Anzahl der defekten und aller Produkte in Zähler und Nenner hergeleitet:

$$(2.7) \quad DL = \frac{DL_M \cdot (1 - DC)}{1 - DL_M \cdot DC}$$

Vorherige Abschätzung hier mit Markov-Kette bestätigt.

DC	Defektabdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
DL_M	Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.
DL	Defektanteil nach Aussortieren oder Ersatz erkannter defekter Produkte.

3.98 Zu erwartende Anzahl der Ersetzungen



$$\mu_{\text{Repl}} = DL \cdot DC \cdot \sum_{n=0}^{\infty} \underbrace{(DL \cdot DC)^n}_{p_{S_0}()} = \frac{DL_M \cdot DC}{1 - DL_M \cdot DC} \quad (3.24)$$

(n – Nummer der Ersetzung). Zur Kontrolle, es muss gelten:

$$(3.21) \quad \mu_{\text{Repl}} = \frac{1}{Y} - 1$$

$$(2.6) \quad Y = 1 - DL_M \cdot DC$$

$$Y = \frac{1}{\mu_{\text{Repl}} + 1} = \frac{1}{\frac{DL_M \cdot DC}{1 - DL_M \cdot DC} + 1} = 1 - DL \cdot DC \checkmark$$

Auch hier vorherige Abschätzung aus Abschn. 2.1.7 bestätigt.



Beispiel 3.5: Ausbeute und Defektanteil nach Ersatz

Schaltkreisausbeuten Y : 10%, 30%, 50%, 80% und 90%, Defektdeckung DC : 90%, 99%, 99,5% und 99,9%.

- Wie groß ist der Defektanteil DL_M der Schaltkreise nach der Fertigung vor dem Aussortieren?
- Wie groß ist der Defektanteil DL nach Aussortieren (Ersatz) der erkannten fehlerhaften Schaltkreise in Abhängigkeit von der Ausbeute und der Defektdeckung?

Y	Ausbeute (Yield).
DC	Defektdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
μ_{Repl}	Zu erwartende Anzahl der Ersetzungen.
DL_M	Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.
DL	Defektanteil nach Aussortieren oder Ersatz erkannter defekter Produkte.



Schaltkreisausbeuten Y : 10%, 30%, 50%, 80% und 90%, Defektabdeckung DC : 90%, 99%, 99,5% und 99,9%.

a) *Wie groß ist der Defektanteil DL_M der Schaltkreise nach der Fertigung vor dem Aussortieren?*

$$(2.6) \quad Y = 1 - DL_M \cdot DC$$

Umstellung nach dem Defektanteil DL_M vor dem Aussortieren der als defekt erkannten Schaltkreise:

$DL_M = \frac{1-Y}{DC}$	$Y = 10\%$...=30%	...=50%	...=80%	...=90%
$DC = 90,0\%$	100,0%	77,8%	55,6%	22,2%	11,1%
$DC = 99,0\%$	90,9%	70,7%	50,50%	20,2%	10,1%
$DC = 99,9\%$	90,1%	70,1%	50,1%	20,0%	10,0%

100% Für $Y = 1 - DC$ sind alle gefertigten Schaltkreise defekt.



Schaltkreisausbeuten Y : 10%, 30%, 50%, 80% und 90%, Defektabdeckung DC : 90%, 99%, 99,5% und 99,9%.

b) *Wie groß ist der Defektanteil DL nach Aussortieren (Ersatz) der erkannten fehlerhaften Schaltkreise in Abhängigkeit von der Ausbeute und der Defektabdeckung?*

$$(2.7) \quad DL = \frac{DL_M \cdot (1 - DC)}{1 - DL_M \cdot DC}$$

$$DL_M = \frac{1 - Y}{DC}; \quad DL = \frac{\frac{1 - Y}{DC} \cdot (1 - DC)}{1 - \frac{1 - Y}{DC} \cdot DC} = \frac{(1 - Y) \cdot (1 - DC)}{Y \cdot DC}$$

	$DC = 90\%$	$DC = 99\%$	$DC = 99,5\%$	$DC = 99,9\%$
$Y = 10\%$	100%	9,09%	4,52%	9.009 dpm
$Y = 30\%$	25,9%	2,36%	1,17%	2.336 dpm
$Y = 50\%$	11,1%	1,01%	5.025 dpm	1.001 dpm
$Y = 80\%$	2,78%	2.525 dpm	1.256 dpm	250 dpm
$Y = 90\%$	1,23%	1.122 dpm	558 dpm	111 dpm

100%
dpm

Für $Y = 1 - DC$ sind alle gefertigten Schaltkreise defekt.
Anzahl der defekten Produkte von einer Million (defecs per million).



Schaltkreisausbeuten Y : 10%, 30%, 50%, 80% und 90%, Defektdeckung DC : 90%, 99%, 99,5% und 99,9%.

$$DL_M = \frac{1-Y}{DC}; \quad DL = \frac{\frac{1-Y}{DC} \cdot (1-DC)}{1 - \frac{1-Y}{DC} \cdot DC} = \frac{(1-Y) \cdot (1-DC)}{Y \cdot DC}$$

DC	90%	99%	99,5%	99,9%
$Y = 30\%$	25,9%	2,36%	1,17%	2.336 dpm
$Y = 50\%$	11,1%	1,01%	5.025 dpm	1.001 dpm
$Y = 80\%$	2,78%	2.525 dpm	1.256 dpm	250 dpm
$Y = 90\%$	1,23%	1.122 dpm	558 dpm	111 dpm

Für den Defektanteil getesteter Schaltkreise DL findet man in der Literatur die Größenordnung 100 ... 1000 dpm. Für $Y = 30\%..80\%$ folgen daraus Defektdeckungen von $DC \gtrsim 99,9\%$.

- Sind die Defektdeckungen wirklich so hoch oder
- sind die Literaturangaben zum Defektanteil zu niedrig?

Diese Frage wird uns weiter begleiten.



Reparatur

3.100 Fehlerbeseitigung durch Reparatur

Bei Reparatur werden nur die als defekt diagnostizierten Teile getauscht oder modifiziert. Zu ersetzende Teilsysteme:

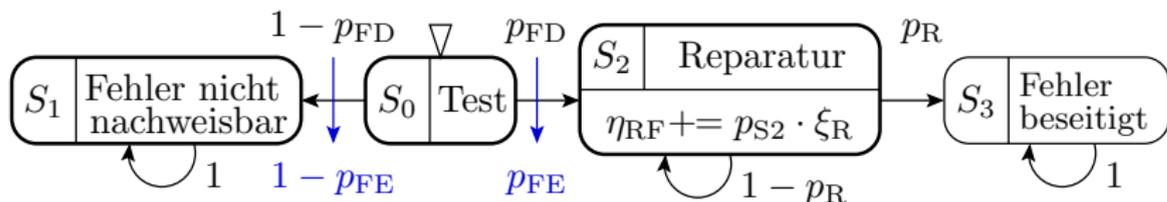
- sind billiger als zu ersetzende Gesamtsysteme und
- haben einen kleineren Defektanteil (weniger Mehrfachersetzungen durch defekte Ersatzteile).

Dafür verlangt Reparatur Zusatzaufwendungen:

- Vorhaltung von Organisationseinheiten + Personalkapazität für Wartung und Reparatur.
- Reparaturgerechter Entwurf (modulare Austauschbarkeit),
- aufwändigere Fehlerlokalisierung und mehr Reparaturversuche durch Fehldiagnose.

Bei hoher Ausbeute $Y \gg 50\%$ unrentabel.

3.101 Markov-Kette für einen vorhandenen Fehler



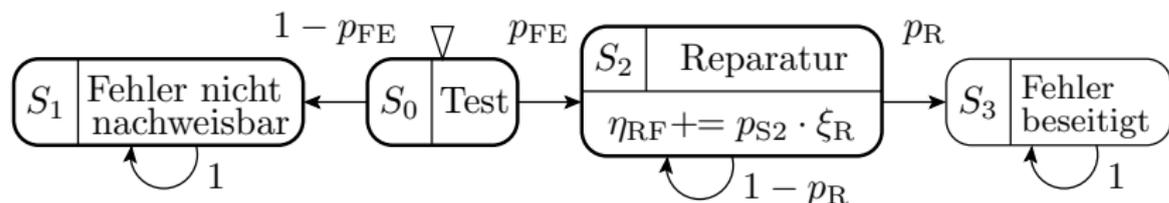
Jeder erkannte Fehler wird beseitigt:

$$p_{FE} = p_{S3} = p_{FD} \cdot p_R + p_{FD} \cdot (1 - p_R) \cdot p_R + p_{FD} \cdot (1 - p_R)^2 \cdot p_R + \dots$$

$$p_{FE} = p_{FD} \cdot p_R \cdot \sum_{n=0}^{\infty} (1 - p_R)^n \stackrel{(SGS)}{=} p_{FD}$$

Bei der Beseitigung können jedoch neue Fehler entstehen ...

p_{FD}	Fehlernachweiswahrscheinlichkeit (Probability of fault detection).
p_{FE}	Fehlernachweis- und Beseitigungswahrscheinlichkeit.
p_R	Erfolgswahrscheinlichkeit der Reparatur.
p_{S_i}	Wahrscheinlichkeit, dass die Markov-Kette im Zustand S_i ist.
η_{RF}	Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.
ξ_R	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.



Im Zustand S_2 werden die Wahrscheinlichkeiten für die Entstehung neuer Fehler für alle Reparaturversuche eines zu beseitigenden Fehlers aufsummiert:

$$\eta_{RF} = p_{FE} \cdot \sum_{n=0}^{\infty} \xi_R \cdot (1 - p_R)^n \stackrel{(SGS)}{=} p_{FE} \cdot \frac{\xi_R}{p_R} \quad (3.25)$$

Die Entstehungsrate je beseitigter Fehler ist um den Kehrwert der Beseitigungswahrscheinlichkeit größer:

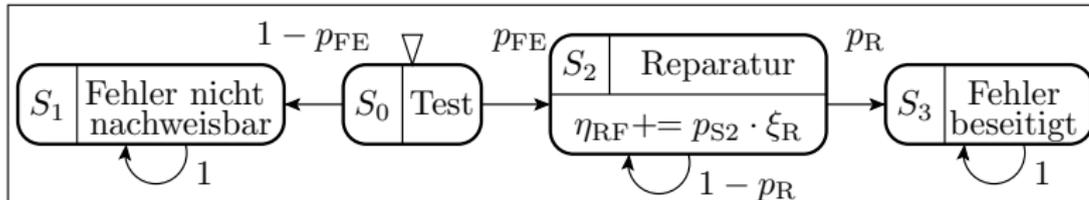
$$\eta_{RE} = \frac{\eta_{RF}}{p_{FE}} = \frac{\xi_R}{p_R} < 1 \quad (3.26)$$

η_{RF}	Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.
p_{FE}	Fehlernachweis- und Beseitigungswahrscheinlichkeit.
p_R	Erfolgswahrscheinlichkeit der Reparatur.
ξ_R	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.
η_{RE}	Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.
SGS	Summe einer geometrischen Reihe: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.103 Mehrere zu beseitigende Fehler

$\mu_{FCR} = \mu_{CF}$ (Zu erwartende Fehleranzahl aus den Entstehungsprozess)

Wiederhole für alle Fehler aus Entstehungs- und Reparaturprozessen



$\mu_{FCR} += \eta_{RF}$ (plus zu erwartende Anzahl der Fehler durch Reparatur)

- Je zu beseitigender Fehler eine Markov-Kette.
- Jeder erkennbare Fehler wird beseitigt.

Beim Beseitigung eines Fehler entstehen im Mittel η_{RE} neue Fehler, bei deren Beseitigung wieder im Mittel η_{RE} neue Fehler entstehen, ...
Entstehungsrate in »neue Fehler« je beseitigter ursprünglicher Fehler:

$$\eta_{RER} = \eta_{RE} \cdot (1 + \eta_{RE} \cdot (1 + \dots)) = \sum_{i=1}^{\infty} (\eta_{RE})^i \stackrel{(SGS)}{=} \frac{1}{1 - \eta_{RE}} - 1$$



$$\eta_{\text{RER}} = \frac{1}{1-\eta_{\text{RE}}} - 1 = \frac{\eta_{\text{RE}}}{1-\eta_{\text{RE}}} \quad (3.27)$$

Neuentstehungsrate je vorhandener ursprünglicher Fehler:

$$\eta_{\text{RFR}} = p_{\text{FE}} \cdot \eta_{\text{RER}} = p_{\text{FE}} \cdot \left(\frac{\eta_{\text{RE}}}{1-\eta_{\text{RE}}} \right) \quad \text{für } \eta_{\text{RE}} < 1 \quad (3.28)$$

Ersatz der Entstehungsrate je vorhandener Fehler in (Gl. 3.26) durch:

$$(3.24) \quad \eta_{\text{RE}} = \frac{\eta_{\text{RF}}}{p_{\text{FE}}} = \frac{\xi_{\text{R}}}{p_{\text{R}}} < 1$$

$$\eta_{\text{RFR}} = p_{\text{FE}} \cdot \left(\frac{\xi_{\text{R}}}{p_{\text{R}} - \xi_{\text{R}}} \right) \quad \text{für } p_{\text{R}} > \xi_{\text{R}} \quad (3.29)$$

Zu erwartende Anzahl der nicht beseitigten Fehler:

$$\mu_{\text{F}} = \mu_{\text{CF}} \cdot (1 - p_{\text{FE}}) \cdot (1 + \eta_{\text{RFR}}) \quad (3.30)$$

$$\mu_{\text{F}} = \mu_{\text{CF}} \cdot (1 - p_{\text{FE}}) \cdot \left(1 + p_{\text{FE}} \cdot \left(\frac{\eta_{\text{RE}}}{1-\eta_{\text{RE}}} \right) \right) \quad \text{für } \eta_{\text{RE}} < 1 \quad (3.31)$$

η_{RFR}	Fehlerentstehungsrate in neue Fehler je vorhandener ursprünglicher Fehler.
η_{RER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.
η_{RE}	Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.
p_{R}	Erfolgswahrscheinlichkeit der Reparatur.
ξ_{R}	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.
μ_{F}	Zu erwartende Fehleranzahl nach Test und Beseitigung aller erkennbaren Fehler.
μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.

3.105 Fallunterscheidung nach η_{RE} in (Gl. 3.29)

$$(3.29) \quad \mu_F = \mu_{CF} \cdot (1 - p_{FE}) \cdot \left(1 + p_{FE} \cdot \left(\frac{\eta_{RE}}{1 - \eta_{RE}} \right) \right) \text{ für } \eta_{RE} < 1$$

- Wenig neu entstehende Fehler: ($1 - \eta_{RE} \rightarrow 1$):

$$\mu_F \approx \mu_{CF} \cdot (1 - p_{FE}) \cdot (1 + p_{FE} \cdot \eta_{RE})$$

Die Fehleranzahl μ_F nach der Beseitigungsiteration erhöht sich nur prozentual um $p_{FE} \cdot \eta_{RE}$.

- Beseitigung aller erkennbaren Fehler, ohne dass sich die zu erwartende Fehleranzahl verringert:

$$(1 - p_{FE}) \cdot \left(1 + p_{FE} \cdot \frac{\eta_{RE}}{1 - \eta_{RE}} \right) = 1 \Rightarrow \eta_{RE} = \frac{1}{2 - p_{FE}}$$

Kontrolle:

$$(1 - p) \cdot \left(1 - p \cdot \frac{\frac{1}{2-p}}{\frac{2-p}{2-p-1}} \right) = (1 - p) \cdot \left(1 - \frac{p}{2-p-1} \right) = (1 - p) \cdot \frac{1-p-p}{1-p} = 1$$

η_{RE}	Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.
μ_F	Zu erwartende Fehleranzahl nach Test und Beseitigung aller erkennbaren Fehler.
p_{FE}	Fehlernachweis- und Beseitigungswahrscheinlichkeit.

Aussprache: ξ : xi, η : eta, μ : my.



- Erhöhung der zu erwartenden Fehleranzahl bei Beseitigung aller erkennbaren Fehler: $\frac{1}{2-p_{FE}} < \eta_{RE} < 1$
- Mehr neu entstehende als beseitigte Fehler ($\eta_{RE} \geq 1$): Das Reparaturziel, die Beseitigung aller erkennbaren Fehler, ist nicht erreichbar.

Einen vernünftiger Reparaturprozess sollte

- alle erkennbaren Fehler beseitigen,
- eine hohe Fehlernachweis- und Beseitigungswahrscheinlichkeit p_{FE} und
- eine geringe Fehlerentstehungsrate $\eta_{RE} < 0,1$ in neue je beseitigte Fehler

anstreben.

η_{RE}

Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.

p_{FE}

Fehlernachweis- und Beseitigungswahrscheinlichkeit.

3.107 Gute studentische Programmierleistung

- Fehlerarme Programmierung, z.B. $\mu_{CF} = 5$ (ohne Syntaxfehler).
- Gründlicher Test, z.B. $p_{FE} = 50\%$ mit $N = 10$ Tests.
- Brauchbare Fehlerbeseitigung: etwa 2,5 Reparaturversuche je Fehler ($p_R = 40\%$), ein neuer Fehler je 10 Reparaturversuche ($\zeta_R = 0,1$).
- Formfaktor der Verteilung der MF-Rate $K = 0,4$.

$$\text{Gl. 3.27: } \eta_{RFR} = \frac{p_{FE} \cdot \zeta_R}{p_R - \zeta_R} = \frac{0,5 \cdot 0,1}{0,4 - 0,1} = 0,167$$

$$\text{Gl. 3.28: } \mu_F = \mu_{CF} \cdot (1 - p_{FE}) \cdot (1 + \eta_{RFR}) = 5 \cdot (1 - 50\%) \cdot 1,167 = 2,92$$

$$\text{Gl. 2.23: } \zeta_F \stackrel{(\leq 1)}{=} \frac{K \cdot \mu_F(N)}{N} = \frac{0,4 \cdot 2,92}{10} = 0,11$$

- Im Mittel 2,5 ursprüngliche plus 0,42 bei der Reparatur entstehende nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel wird mit einer Wahrscheinlichkeit von $1 - \zeta = 89\%$ korrekt abgearbeitet.

Gut genug, um den Abnahmetest zu bestehen.



3.108 Schlechte Programmierleistung

- Mehr Entwurfsfehler: $\mu_{CF} = 7$ Fehler (ohne Syntaxfehler).
- Weniger Tests: $p_{FE} = 30\%$ mit $N = 5$ Tests.
- Etwa 4 Reparaturversuche je Fehler ($p_R = 25\%$), ein neuer Fehler je 5 Reparaturversuche $\xi_R = 0,2$.
- Formfaktor der Verteilung der MF-Rate $K = 0,4$:

$$\begin{aligned} \text{Gl. 3.27: } \eta_{RFR} &= \frac{p_{FE} \cdot \xi_R}{p_R - \xi_R} = \frac{0,3 \cdot 0,2}{0,25 - 0,2} = 1,2 \\ \text{Gl. 3.28: } \mu_F &= \mu_{CF} \cdot (1 - p_{FE}) \cdot (1 + \eta_{RFR}) = 7 \cdot (1 - 30\%) \cdot 2,2 = 10,8 \\ \text{Gl. 2.23: } \zeta &\stackrel{(\leq 1)}{=} \frac{K \cdot \mu_F(N)}{N} = \frac{0,4 \cdot 10,8}{5} \rightarrow 1 \end{aligned}$$

- Im Mittel 4,9 ursprüngliche plus 5,9 bei der Reparatur entstehende nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel liefert garantiert MF.

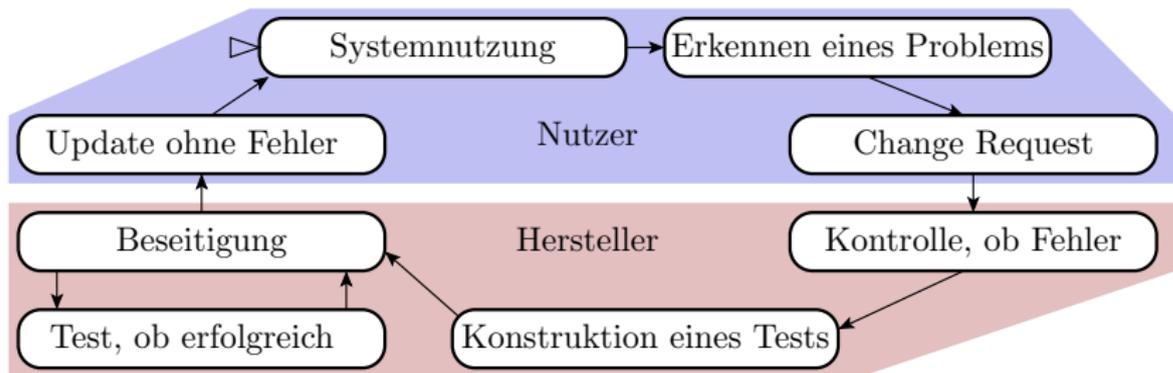
Wie Prüfung bestehen? Mehr Testen und Rückbau!

μ_F, ζ Zu erwartende Fehleranzahl, Fehlfunktionsrate.
 (≥ 1) Der errechnete Wert ist eine Obergrenze. Der tatsächliche Wert ist max. eins.



Reifeprozesse

3.109 Reifen von Produkten (Abschn. 2.2.7)



- Bei einer vermuteten Fehlfunktion stellt der Nutzer eine Änderungsanforderung (Change Request). Alternativ sendet das System einen MF-Report. Vermutete Fehler werden in Schubladen vermuteter gleicher Ursache gesammelt.
- Der Hersteller bevorzugt bei der Beseitigung Schubladen, die Fehler mit häufigen schwerwiegenden MF vermuten lassen.
- Suche von Tests, die den Fehler reproduzierbar nachweisen.
- Experimentelle Reperatur. Installation von Update's.



3.110 Effektive Testanzahl, Abnahme Fehleranzahl

Bei Beobachtung einer MF werden die verursachenden Fehler nur mit einer Wahrscheinlichkeit $p_{FE} \ll 1$ beseitigt. Effektive Testanzahl:

$$(2.40) \quad N = \underbrace{p_{FE} \cdot \mu_{NU} \cdot \eta_{SU} \cdot t_{VR}}_{N_{MV}} \cdot (u + u_{V0}) \quad \text{mit } u_{V0} = \frac{N_{V0}}{N_{VM}}$$

Abnahme der zu erwartenden Fehleranzahl ohne Fehlerneuentstehung, gleichlange Versionsintervalle, ...:

$$(2.42) \quad \mu_F(u) = \mu_F(v) \cdot \left(\frac{u + u_{V0}}{v + u_{V0}} \right)^{-K}$$

N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
p_{FE}	Wahrscheinlichkeit, dass ein Fehler beseitigt wird, wenn er eine MF verursacht.
μ_{NU}	Zu erwartende Nutzeranzahl (Expected number of user).
η_{SU}	Mittlere Anzahl der Service-Leistungen pro Nutzer (user) und Nutzungszeit.
t_{VR}	Versionsintervall, Zeit zwischen der Freigabe aufeinanderfolgender Version.
N_{MV}	Erhöhung der effektive Testanzahl mit jeder Version.
N_{V0}	Effektive Testanzahl von Version 0, d.h. der Fehlerbeseitigungsiteration vor dem Einsatz.
u, v	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
$\mu_F(u)$	Zu erwartende Fehleranzahl in Version u .
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).

3.111 Zuverlässigkeit und Sicherheit

Durch digitale Verarbeitung, elektromagnetische Verträglichkeit, Datenübertragung und Speicherung mit Prüfkennzeichen, ... sind Fehlfunktionen durch Störungen oft vernachlässigbar. Wenn das der Fall, ist die Zuverlässigkeit der Kehrwert der Fehlfunktionsrate durch Fehler:

$$(2.46) \quad R_{\text{MT}}(u) = R_{\text{MT}}(v) \cdot \left(\frac{u+u_{\text{V0}}}{v+u_{\text{V0}}} \right)^{K+1}$$

Wird bei allen erkannten Problemen ein sicherer Zustand hergestellt, nimmt auch die Sicherheit mit Exponent $K + 1$ zu:

$$(2.48) \quad \frac{S(u)}{S(v)} = \frac{R_{\text{MT}}(u)}{R_{\text{MT}}(v)} = \left(\frac{u+u_{\text{V0}}}{v+u_{\text{V0}}} \right)^{K+1}$$

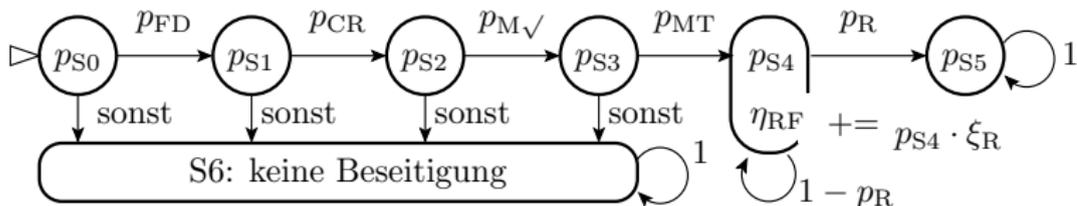
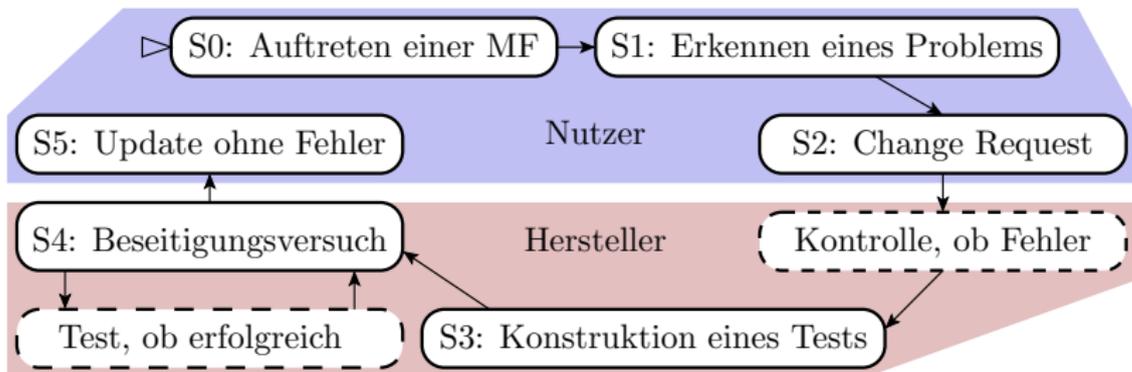
$R_{[\text{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
u, v	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
S_{NDM}	Teilsicherheit bezüglich der nicht erkannten Fehlfunktionen.
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).



3.112 Fortsetzung / Modellerweiterung

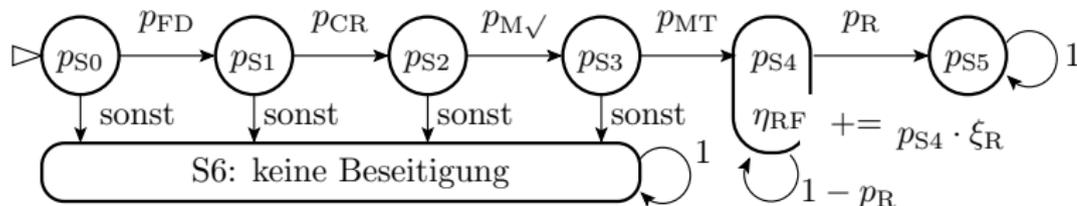
- Reifeprozess als Markov-Kette und
- Berücksichtigung neu entstehender Fehler bei der Fehlerbeseitigung.

3.113 Reifeprozess als Markov-Kette



ps_i Wahrscheinlichkeit, dass die Markov-Kette im Zustand S_i ist.
 η_{RF} Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.

3.115 Fehlerbeseitigungswahrscheinlichkeit



Unter der Annahme, dass so lange repariert wird, bis der Fehler beseitigt ist, beträgt die Wahrscheinlichkeit, dass ein Fehler, wenn er eine Fehlfunktion verursacht, beseitigt wird:

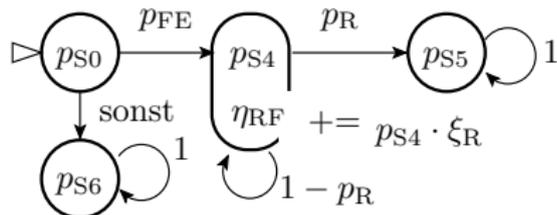
$$p_{FE} = \lim_{n \rightarrow \infty} p_{S5}(n) = p_{FD} \cdot p_{CR} \cdot p_{M\sqrt{}} \cdot p_{MT} \quad (3.32)$$

Bei jedem Reparaturversuch entsteht mit der Rate ξ_R ein neuer Fehler.

p_{FE}	Wahrscheinlichkeit, dass ein Fehler beseitigt wird, wenn er eine MF verursacht.
p_{FD}	Fehlernachweiswahrscheinlichkeit (Probability of fault detection).
p_{CR}	Wahrscheinlichkeit einer Änderungsanforderung (change request) bei beobachteter MF.
$p_{M\sqrt{}}$	Wahrscheinlichkeit, dass der Hersteller (manufacturer) die MF rekonstruieren kann.
p_{MT}	Wahrscheinlichkeit, dass ein Test für den Fehlernachweis gefunden wird.
p_R	Erfolgswahrscheinlichkeit der Reparatur.
ξ_R	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.

3.116 Fehlerentstehungsrate

Dieselbe Markov-Kette wie für die Fehlerbeseitigung durch Reparatur (Abschn. 3.4.2). Neue je vorhandener und je beseitigter Fehler:



$$(3.23) \quad \eta_{RF} = p_{FE} \cdot \sum_{n=0}^{\infty} \xi_R \cdot (1 - p_R)^n \stackrel{(SGS)}{=} p_{FE} \cdot \frac{\xi_R}{p_R}$$

Die Entstehungsrate je beseitigter Fehler ist um den Kehrwert der Beseitigungswahrscheinlichkeit größer:

$$(3.24) \quad \eta_{RE} = \frac{\eta_{RF}}{p_{FE}} = \frac{\xi_R}{p_R} < 1$$

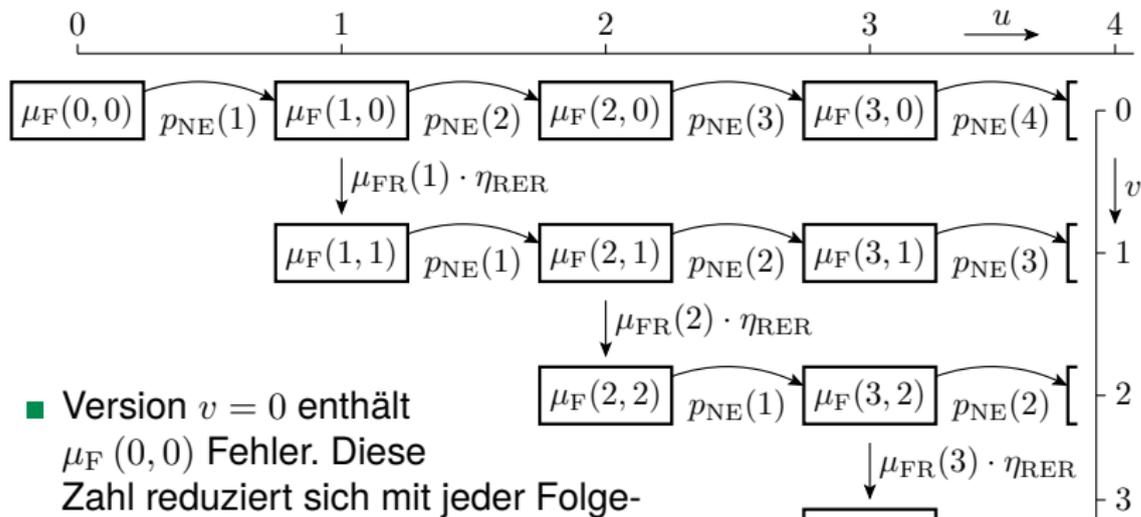
Rekursiv unter Berücksichtigung »neuer Fehler durch neue Fehler«

$$(3.25) \quad \eta_{REER} = \frac{1}{1 - \eta_{RE}} - 1 = \frac{\eta_{RE}}{1 - \eta_{RE}}$$

in neue Fehler je beseitigter Fehler. Anzahl der beseitigten Fehler ...

p_{FE}	Wahrscheinlichkeit, dass ein Fehler beseitigt wird, wenn er eine MF verursacht.
p_R	Erfolgswahrscheinlichkeit der Reparatur.
ξ_R	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.
η_{RF}	Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.
η_{RE}	Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.
η_{REER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

3.118 Reifeprozess mit Fehlerneuentstehung



- Version $v = 0$ enthält $\mu_F(0, 0)$ Fehler. Diese Zahl reduziert sich mit jeder Folgeversionen $u > 0$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{NE}(u - v)$ auf $\mu_F(u, 0)$.
- In jeder Version $u > 0$ entstehen neue Fehler. Deren zu erwartende Anzahl nimmt mit jeder Folgeversionen $u > v$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{NE}(u - v)$ ab auf $\mu_F(u, v)$.

3.119 Nichtbeseitigungswahrscheinlichkeit

Für gleichlange Update-Intervalle beträgt die effektive Testanzahl für Fehler in Version u , die in Version v entstanden sind, nach (Gl. 2.40):

$$N(u, v) = N_{VM} \cdot (u - v + u_{v0}) \quad (3.33)$$

Die zu erwartende Fehleranzahl aus jeder Version v nimmt mit Version $u \geq v$ seit der Vorversion $u - 1$ nach (Gl. 2.42) ab:

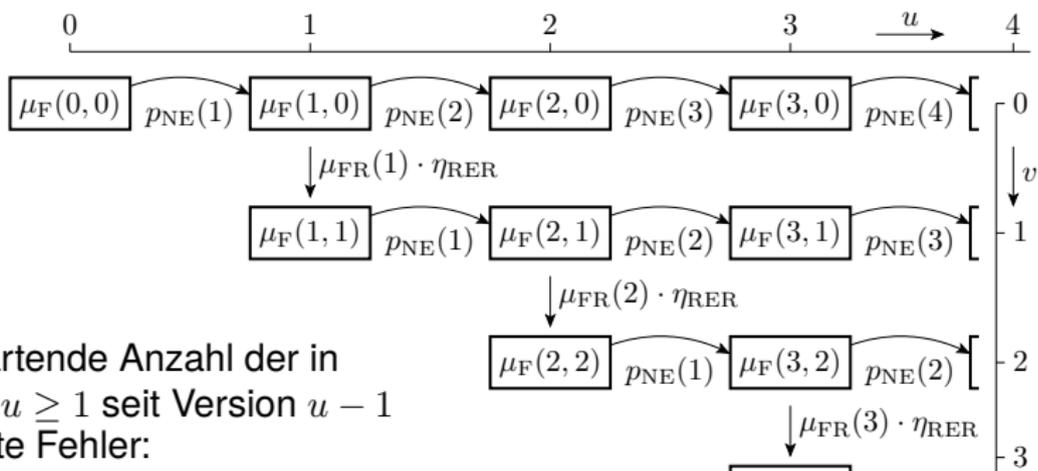
$$\mu_F(u, v) = \mu_F(u - 1, v) \cdot \left(\frac{u - v + u_{v0}}{u - 1 - v + u_{v0}} \right)^{-K} \quad (3.34)$$

Nichtbeseitigungswahrscheinlichkeit $p_{NE}(u)$ als relative Verringerung der zu erwartenden Fehleranzahl gegenüber Vorversion:

$$p_{NE}(u - v) = \frac{\mu_F(u, v)}{\mu_F(u - 1, v)} = \left(\frac{u - v + u_{v0}}{u - v - 1 + u_{v0}} \right)^{-K} \quad (3.35)$$

$N(u, v)$	Effektiven Testanzahl in Version u für Fehler aus Version v .
N_{MV}	Erhöhung der effektive Testanzahl mit jeder Version.
u, v	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_{v0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
$p_{NE}(u - v)$	Nichtbeseitigungswahrscheinlichkeit für Fehler aus Version v in der Folgeversion von u .
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).

3.120 Neu entstehende Fehler



Zu erwartende Anzahl der in Version $u \geq 1$ seit Version $u - 1$ beseitigte Fehler:

$$\mu_{FR}(u) = \sum_{v=0}^{u-1} (\mu_F(u-1, v) - \mu_F(u, v)) \quad (3.36)$$

Die Anzahl der neu entstehenden Fehler ist η_{RER} mal so groß:

$$\mu_F(u, u) = \eta_{RER} \cdot \mu_{FR}(u) \quad (3.37)$$

3.121 Zu erwartende Fehleranzahlen insgesamt

$\mu_F(0, 0)$ gleich erwartetet Fehleranzahl in Version 0

Wiederhole für jede Versionsnummer ab $u = 1$

- Wiederhole für Fehlerentstehungsversion $v = 0$ bis $u - 1$
 - Zu erwartende Anzahl der nicht beseitigten Fehler:

$$(3.32) \quad \mu_F(u, v) = \mu_F(u - 1, v) \cdot \left(\frac{u - v + u_{V0}}{u - 1 - v + u_{V0}} \right)^{-K}$$

- Erwartete Zahl der beseitigten und neu entstehenden Fehler:

$$(3.34) \quad \mu_{FR}(u) = \sum_{v=0}^{u-1} (\mu_F(u - 1, v) - \mu_F(u, v))$$

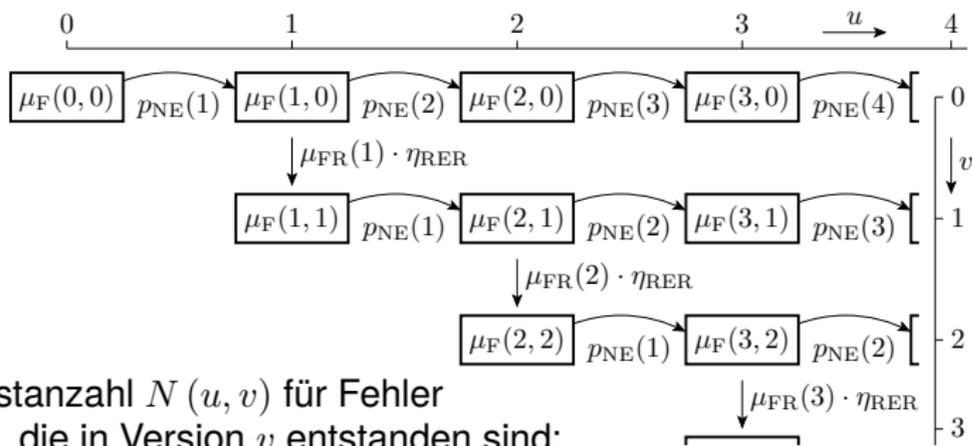
$$(3.35) \quad \mu_F(u, u) = \eta_{RER} \cdot \mu_{FR}(u)$$

- Alle Fehler:

$$\mu_F(u) = \sum_{v=0}^u \mu_F(u, v) \quad (3.38)$$

$\mu_F(u, v)$	Zu erwartende Fehleranzahl in Version u , die in Version v entstanden sind.
u, v	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
$\mu_{FE}(u)$	Erwartete Anzahl der in Version u aus Version $u - 1$ beseitigten Fehler.
η_{RER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

3.122 Fehlfunktionsrate durch Fehler



Effektive Testanzahl $N(u, v)$ für Fehler
in Version u , die in Version v entstanden sind:

$$(3.31) \quad N(u, v) = N_{VM} \cdot (u - v + u_{v0})$$

Wiederhole für jede Versionsnummer ab $u = 0$ (vergl. Gl. 2.23):

$$\zeta_F(u) = K \cdot \sum_{v=0}^u \frac{\mu_F(u, v)}{N(u, v)} \quad (3.39)$$

$\zeta_F(u)$ Gesamte Fehlfunktionsrate durch alle Fehler in Version u .
 K Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).

Beispiel 3.6: Reifeprozess mit neu entstehenden Fehlern

$\mu_F(0, 0) = 100$, $N_{MV} = 10^6$, $u_{V0} = 0,1$, $\eta_{RER} = 0,1$, $K = 0,4$.

- Zu erwartende Fehleranzahlen $\mu_F(u, v)$ für $u = 0$ bis 5 gereifte Versionen je Entstehungsversion v und insgesamt?*
- MF-Raten $\zeta_F(u, v)$ einzeln und Summe $\zeta_F(u)$?*
- Relative Erhöhung der zu erwartenden Fehleranzahl durch die bei der Beseitigung neu entstehenden Fehler?*
- Relative Erhöhung der MF-Rate durch die neuen Fehler?*

$\mu_F(0, 0)$	Erwartete Anzahl Fehler in Version 0 (erste freigegebene Version).
N_{MV}	Erhöhung der effektive Testanzahl mit jeder Version.
u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
η_{RER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).
u, v	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
$\mu_F(u, v)$	Zu erwartende Fehleranzahl in Version u , die in Version v entstanden sind.
$\mu_F(u)$	Gesamte zu erwartende Fehleranzahl in Version u .



$\mu_F(0,0) = 100$, $N_{MV} = 10^6$, $u_{V0} = 0,1$, $\eta_{RER} = 0,1$, $K = 0,4$.

a) *Zu erwartende Fehleranzahlen $\mu_F(u,v)$ für $u = 0$ bis 5 gereifte Versionen je Entstehungsversion v und insgesamt?*

$$(3.32) \quad \mu_F(u, v) = \mu_F(u-1, v) \cdot \left(\frac{u-v+u_{V0}}{u-1-v+u_{V0}} \right)^{-K}$$

$$(3.34) \quad \mu_{FR}(u) = \sum_{v=0}^{u-1} (\mu_F(u-1, v) - \mu_F(u, v))$$

$$(3.35) \quad \mu_F(u, u) = \eta_{RER} \cdot \mu_{FR}(u)$$

Tabelle $\mu_F(u, v)$:

u	0	1	2	3	4	5
$v = 0$	100	38,32	29,59	25,32	22,64	20,75
$v = 1$	0	6,17	2,36	1,82	1,56	1,40
$v = 2$	0	0	1,25	$4,80 \cdot 10^{-1}$	$3,71 \cdot 10^{-1}$	$3,17 \cdot 10^{-1}$
$v = 3$	0	0	0	$5,58 \cdot 10^{-1}$	$2,14 \cdot 10^{-1}$	$1,65 \cdot 10^{-1}$
$v = 4$	0	0	0	0	$3,40 \cdot 10^{-1}$	$1,30 \cdot 10^{-1}$
$v = 5$	0	0	0	0	0	$2,37 \cdot 10^{-1}$
$\mu_F(u)$	100	44,49	33,21	28,18	25,13	22,99



$$\mu_F(0,0) = 100, N_{MV} = 10^6, u_{V0} = 0,1, \eta_{RER} = 0,1, K = 0,4.$$

b) MF-Raten $\zeta_F(u, v)$ *einzeln und Summe* $\zeta_F(u)$?

$$(3.31) \quad N(u, v) = N_{VM} \cdot (u - v + u_{V0})$$

$$(3.37) \quad \zeta_F(u) = K \cdot \sum_{v=0}^u \frac{\mu_F(u, v)}{N(u, v)}$$

Tabelle $\zeta_F(u, v) = \frac{\mu_F(u, v)}{N(u, v)}$:

u	0	1	2	3	4	5
$v = 0$	$4 \cdot 10^{-4}$	$1,39 \cdot 10^{-5}$	$5,64 \cdot 10^{-6}$	$3,27 \cdot 10^{-6}$	$2,21 \cdot 10^{-6}$	$1,63 \cdot 10^{-6}$
$v = 1$	0	$2,47 \cdot 10^{-5}$	$8,59 \cdot 10^{-7}$	$3,48 \cdot 10^{-7}$	$2,02 \cdot 10^{-7}$	$1,36 \cdot 10^{-7}$
$v = 2$	0	0	$5,02 \cdot 10^{-6}$	$1,75 \cdot 10^{-7}$	$7,07 \cdot 10^{-8}$	$4,10 \cdot 10^{-8}$
$v = 3$	0	0	0	$2,23 \cdot 10^{-6}$	$7,78 \cdot 10^{-8}$	$3,14 \cdot 10^{-8}$
$v = 4$	0	0	0	0	$1,36 \cdot 10^{-6}$	$4,73 \cdot 10^{-8}$
$v = 5$	0	0	0	0	0	$9,48 \cdot 10^{-7}$
$\zeta_F(u)$	$4 \cdot 10^{-4}$	$3,86 \cdot 10^{-5}$	$1,15 \cdot 10^{-5}$	$6,02 \cdot 10^{-6}$	$3,92 \cdot 10^{-6}$	$2,83 \cdot 10^{-6}$

$\zeta_F(u, v)$ MF-Rate in Version u verursacht von Fehlern die in Version v entstanden sind.

$\zeta_F(u)$ Gesamte Fehlfunktionsrate in Version u .



$$\mu_F(0,0) = 100, N_{MV} = 10^6, u_{V0} = 0,1, \eta_{RER} = 0,1, K = 0,4.$$

c) *Relative Erhöhung der zu erwartenden Fehleranzahl durch die bei der Beseitigung neu entstehenden Fehler?*

u	0	1	2	3	4	5
$v = 0$	100	38,32	29,59	25,32	22,64	20,75
$v = 1$	0	6,17	2,36	1,82	1,56	1,40
$v = 2$	0	0	1,25	$4,80 \cdot 10^{-1}$	$3,71 \cdot 10^{-1}$	$3,17 \cdot 10^{-1}$
$v = 3$	0	0	0	$5,58 \cdot 10^{-1}$	$2,14 \cdot 10^{-1}$	$1,65 \cdot 10^{-1}$
$v = 4$	0	0	0	0	$3,40 \cdot 10^{-1}$	$1,30 \cdot 10^{-1}$
$v = 5$	0	0	0	0	0	$2,37 \cdot 10^{-1}$
$\mu_F(u)$	100	44,49	33,21	28,18	25,13	22,99
$\frac{\mu_F(u)}{\mu_F(u,0)}$		1,161	1,122	1,113	1,110	1,108

Erhöhung etwa um die zu erwartende Fehlerentstehungsrate η_{RER} in bei der Beseitigung neu entstehende Fehler je beseitigter Fehler.

$\mu_F(u,0)$ Zu erwartende Fehleranzahl aus Version 0, die in Version u nicht beseitigt sind.



$$\mu_F(0,0) = 100, N_{MV} = 10^6, u_{V0} = 0,1, \eta_{RER} = 0,1, K = 0,4.$$

d) *Relative Erhöhung der MF-Rate durch die neuen Fehler?*

u	0	1	2	3	4	5
$v = 0$	$4 \cdot 10^{-4}$	$1,39 \cdot 10^{-5}$	$5,64 \cdot 10^{-6}$	$3,27 \cdot 10^{-6}$	$2,21 \cdot 10^{-6}$	$1,63 \cdot 10^{-6}$
$v = 1$	0	$2,47 \cdot 10^{-5}$	$8,59 \cdot 10^{-7}$	$3,48 \cdot 10^{-7}$	$2,02 \cdot 10^{-7}$	$1,36 \cdot 10^{-7}$
$v = 2$	0	0	$5,02 \cdot 10^{-6}$	$1,75 \cdot 10^{-7}$	$7,07 \cdot 10^{-8}$	$4,10 \cdot 10^{-8}$
$v = 3$	0	0	0	$2,23 \cdot 10^{-6}$	$7,78 \cdot 10^{-8}$	$3,14 \cdot 10^{-8}$
$v = 4$	0	0	0	0	$1,36 \cdot 10^{-6}$	$4,73 \cdot 10^{-8}$
$v = 5$	0	0	0	0	0	$9,48 \cdot 10^{-7}$
$\zeta_F(u)$	$4 \cdot 10^{-4}$	$3,86 \cdot 10^{-5}$	$1,15 \cdot 10^{-5}$	$6,02 \cdot 10^{-6}$	$3,92 \cdot 10^{-6}$	$2,83 \cdot 10^{-6}$
$\frac{\zeta_F(u)}{\zeta_F(u,0)}$		2,78	2,04	1,84	1,77	1,74

Erhöhung um Größenordnung η_{RFR}/u_{V0} . Es sind zwar insgesamt nur grob geschätzt $\eta_{RFR} = 10\%$ mehr Fehler. Aber die jüngsten Fehler davon haben nur eine effektive Testanzahl $N(u,u) = 0,1 \cdot N_{MV}$ und alle anderen Fehler von mindesten von N_{MV} .

$\zeta_F(u,0)$ MF-Rate in Version u durch Fehlern aus Version 0 (erste freigegebene Version).



Zusammenfassung

3.124 Fehlerbeseitigung, Ersatz

Fehlerbeseitigung mit Erfolgskontrolle beseitigt alle erkennbaren Fehler. Bei hoher Ausbeute ist Ersatz und bei geringer Ausbeute Reparatur günstiger.

Für Ersatz ergeben sich über Markov-Ketten dieselben Beziehungen wie über einfache Verhältnisabschätzungen (Abschn. 2.1.7):

$$(2.7) \quad DL = \frac{DL_M \cdot (1 - DC)}{1 - DL_M \cdot DC}$$

$$(3.22) \quad \mu_{\text{Repl}} = DL \cdot DC \cdot \underbrace{\sum_{n=0}^{\infty} (DL \cdot DC)^n}_{p_{\text{So}}()} = \frac{DL_M \cdot DC}{1 - DL_M \cdot DC}$$

$$(3.21) \quad \mu_{\text{Repl}} = \frac{1}{Y} - 1$$

3.125 Reparatur

Bei einer Reparaturiteration bis Erfolg werden auch alle nachweisbaren Fehler beseitigt, aber statt der Reduzierung der Objektanzahl im Nenner um die aussortierten Objekte entstehen neue Fehler.

- Fehlerentstehungsrate je vorhandener Fehler:

$$(3.23) \quad \eta_{RF} = p_{FE} \cdot \sum_{n=0}^{\infty} \xi_R \cdot (1 - p_R)^n \stackrel{(SGS)}{=} p_{FE} \cdot \frac{\xi_R}{p_R}$$

- Fehlerentstehungsrate je beseitigter Fehler:

$$(3.24) \quad \eta_{RE} = \frac{\eta_{RF}}{p_{FE}} = \frac{\xi_R}{p_R} < 1$$

- Fehlerentstehungsrate je beseitigter ursprünglicher Fehler:

$$(3.25) \quad \eta_{RER} = \frac{1}{1 - \eta_{RE}} - 1 = \frac{\eta_{RE}}{1 - \eta_{RE}}$$

- Fehlerentstehungsrate je vorhandener ursprünglicher Fehler:

$$(3.26) \quad \eta_{RFR} = p_{FE} \cdot \eta_{RER} = p_{FE} \cdot \left(\frac{\eta_{RE}}{1 - \eta_{RE}} \right) \text{ für } \eta_{RE} < 1$$

Zu erwartende Anzahl der nicht beseitigten Fehler:

$$(3.28) \quad \mu_F = \mu_{CF} \cdot (1 - p_{FE}) \cdot (1 + \eta_{RFR})$$



Bei geringer Fehlerentstehungsrate (z.B. $\eta_{RE} \lesssim 0,1$ neuer je beseitigter Fehler) und hoher Fehlererkennungswahrscheinlichkeit p_{FD} erhöht »Reparatur« die Fehleranzahl gegenüber der Anzahl der ursprünglichen nicht erkennbaren Fehler nur prozentual um $p_{FD} \cdot \eta_{RE}$.

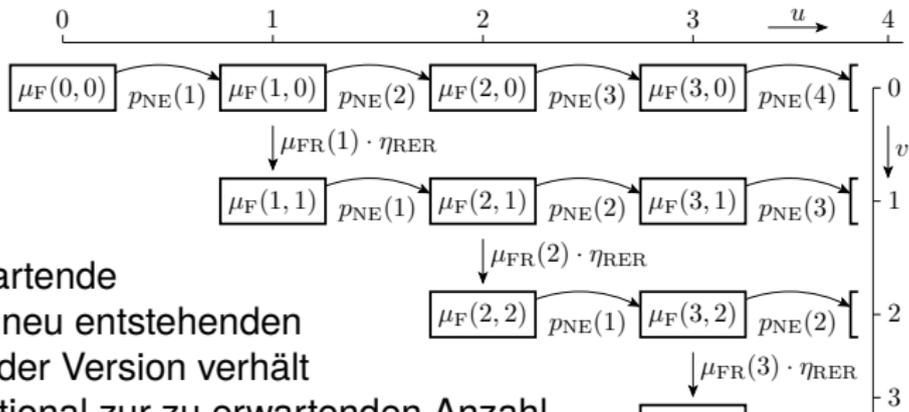
Bei kleiner Erkennungswahrscheinlichkeit p_{FD} und deutlich mehr als ein neu entstehender je 10 beseitigte Fehler kaum Verringerung oder sogar Vergrößerung der Fehleranzahl durch die Reparaturiteration. Deshalb ist Rückbau nach erfolglosen Reparaturversuchen so wichtig.

Wenn die Testanzahl nicht deutlich größer als die zu erwartenden Fehleranzahl nach der Beseitigungsiteration ist, wird oft nicht einmal ein neues zufällig gewähltes Testbeispiel richtig abgearbeitet.

η_{RE}

Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.

3.127 Reifeprozess mit Fehlerentstehung



- Die zu erwartende Anzahl der neu entstehenden Fehler in jeder Version verhält sich proportional zur zu erwartenden Anzahl der beseitigten Fehler seit der Vorversion.
- Die Fehlerbeseitigungswahrscheinlichkeit ist abhängig von der Erhöhung der effektiven Testanzahl seit der Entstehungsversion.
- Die Fehlfunktionrate je noch vorhandener Fehler ist proportional zum Kehrwert der effektiven Testanzahl seit Fehlerentstehung.

Die Modellierung verlangt, dass Fehlerentstehung und Beseitigung für jede Entstehungsversion getrennt berechnet werden.



3.128 Simulation mit Beispielwerten

Die Berücksichtigung, dass bei jeder Beseitigung einer Fehlers von einer zur nächsten Version im Mittel $\eta_{\text{REER}} < 1$ neue Fehler entstehen erhöht grob überschlagen

- die Fehleranzahl anteilmäßig um η_{REER} und
- die Fehlerfunktionsrate um $\approx \eta_{\text{RFR}}/u_{\text{V0}}$.

Aufgrund der $\leq u_{\text{V0}}$ -fachen Reifedauer gegenüber Fehlern früherer Versionen, haben die neuen Fehler die $\geq 1/u_{\text{V0}}$ -fache Fehlfunktionsrate. Bei geringem relativen Testaufwand u_{V0} beobachtet der Nutzer in jeder Version hauptsächlich Fehlfunktionen durch neue Fehler.

Die Wahrnehmung neuer Fehler wird durch die Nutzerlernprozesse verstärkt. Nutzer müssen für die schlimmsten neuen Fehler jeder Version Workarounds suchen, die in der Folgeversion wieder überflüssig sind.

Gute Nutzerakzeptanz von Reifeprozessen verlangt einen angemessener Testaufwand u_{V0} vor jeder Versionsfreigabe.

u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.
η_{REER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.



Fehlerentstehung



3.129 Erwartete Fehleranzahl (Abschn. 2.3.1)

Wir hatten bisher die zu erwartende Anzahl der Fehler über Metriken aus Systemgröße oder Entstehungsaufwand abgeschätzt.

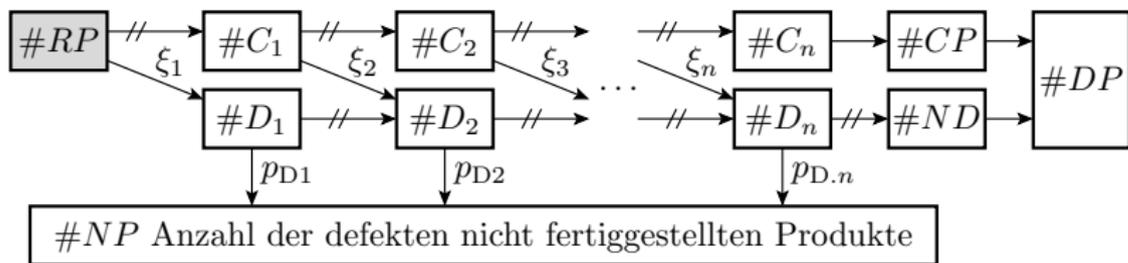
- Programmgröße: $C = 800 \text{ NLOC}$
- Fehlerentstehungsrate: $\xi = 20 \dots 80 \frac{F}{1.000 \text{ NLOC}}$
- zu erwartende Anzahl der entstehenden Fehler: 16 bis 64

In (Abschn. 2.3.1) wurde angedeutet, dass Fehlerentstehung auch als System aus Entstehungsschritten und Beseitigungsiterationen modellierbar ist, was auch Ansatzpunkte für die Fehlervermeidung bietet. Hier folgen zwei Beispiele dazu:

- Modellierung einer linearen Folge von Entstehungsschritten mit einem Zählwertzuordnungsgraphen.
- Modellierung von Phasenmodellen durch Markov-Ketten mit Kantenzählern für die Fehlerentstehung.

μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.
ξ	Fehlerentstehungsrate.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.

3.130 Entstehungsprozesse mit Kontrollen

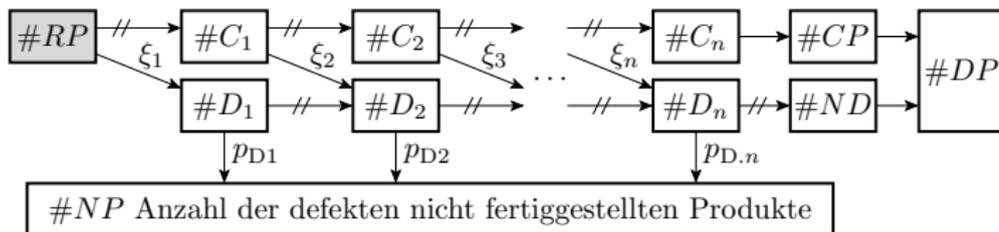


Lineare Folge von Entstehungsschritten. In jedem Schritt

- werden Entstehungsleistungen erbracht, und bei denen mit einer kleinen Rate $\xi_i \ll 1$ Fehler entstehen.
- Entstandene Fehler werden mit Wahrscheinlichkeit $p_{D.i}$ erkannt.

$\#...$	Anzahl (Zählwert) der Ereignisse ...
RP	Bauftragung, ein Produkt herzustellen.
C_i, D_i	Schritt 1 bis i korrekt ausgeführt, Produkt nach Schritt i fehlerhaft.
CP, ND	Fehlerfreies Produkt, Produkt mit nicht erkannten Fehlern.
PD, NP	Produkt erzeugt, kein Produkt erzeugt.
$\xi_i, p_{D.i}$	Fehlerentstehungsrate und Fehlernachweiswahrscheinlichkeit Schritt i .

3.131 Prozesserbringungsrate



Der skizzierte Entstehungsprozess bricht bei erkanntem Fehler ab.
Erbringungsrate für korrekte Produkte:

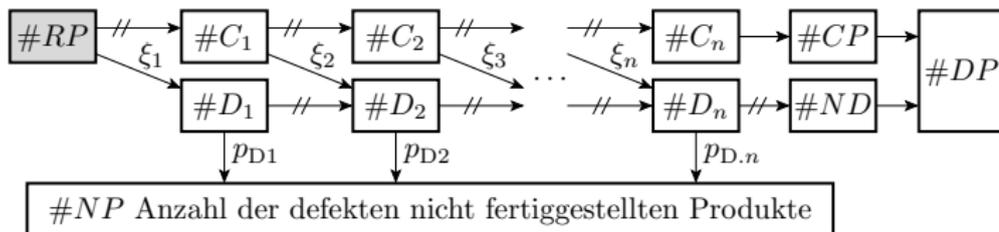
$$\eta_{CP} = \frac{\#C_n}{\#RP} \Big|_{ACR} = \prod_{i=1}^n (1 - \xi_i)$$

Erbringungsrate für Produkte mit nicht erkannten Fehlern:

$$\eta_{ND} = \xi_1 \cdot \prod_{i=1}^n (1 - p_{D.i}) + \sum_{i=1}^{n-1} \left(\prod_{j=1}^i (1 - \xi_j) \cdot \xi_{i+1} \cdot \prod_{j=i+1}^n (1 - p_{D.i}) \right) \quad (3.40)$$

η_{CP}, η_{ND} Erbringungsrate von Produkten ohne und mit nicht erkannten Fehlern.
 $\xi_i, p_{D.i}$ Fehlerentstehungsrate und Fehlernachweiswahrscheinlichkeit Schritt i .

3.132 Erbringungsrate komplett, Fehleranteil



Die Erbringungsrate des Entstehungsprozesses insgesamt:

$$\eta_{DP} = \frac{\#DP}{\#RP} \Big|_{ACR} = \eta_{CP} + \eta_{ND}$$

Fehleranteil der fertiggestellten Produkte:

$$DL_M = \frac{\#ND}{\#DP} \Big|_{ACR} = \frac{\eta_{ND}}{\eta_{CP} + \eta_{ND}}$$

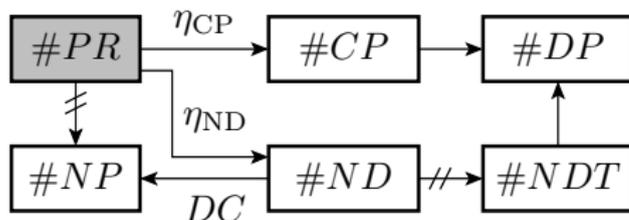
Nach der Fertigung sortiert ein weiterer Test mit einer Defektüberdeckung DC die erkennbar defekten Produkte aus. ...

η_{DP} Erbringungsrate fertiger Produkte.

η_{CP}, η_{ND} Erbringungsrate von Produkten ohne und mit nicht erkannten Fehlern.

DL_M Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.

3.133 Ausbeute und Fehleranteil nach Endtest



Ausbeute bezogen auf Fertigungsaufträge:

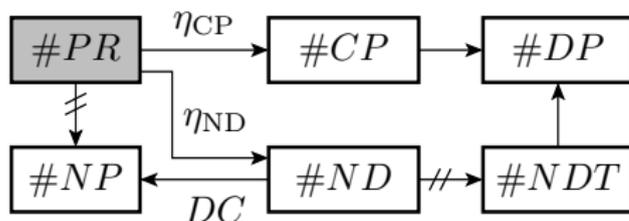
$$Y_{PR} = \frac{\#DP}{\#PR} \Big|_{ACR} = \eta_{CP} + (1 - DC) \cdot \eta_{ND}$$

Defektanteil der als gut befundenen Produkte nach dem Endtest:

$$DL = \frac{\#NDT}{\#DP} \Big|_{ACR} = \frac{(1 - DC) \cdot \eta_{ND}}{\eta_{CP} + (1 - DC) \cdot \eta_{ND}}$$

RP, DP	Fertigungsauftrag, gefertigtes Produkt als gut befundenen.
CP, ND	Fehlerfreies Produkt, Produkt mit nicht erkannten Fehlern.
NDT	Defektes Produkt, das auch vom Endtest als gut befunden wurde.
η_{CP}, η_{ND}	Erbringungsrate von Produkten ohne und mit nicht erkannten Fehlern.
Y_{RP}, DC	Ausbeute bezogen Fertigungsaufträge, Defektabdeckung.

3.134 Rentabilität



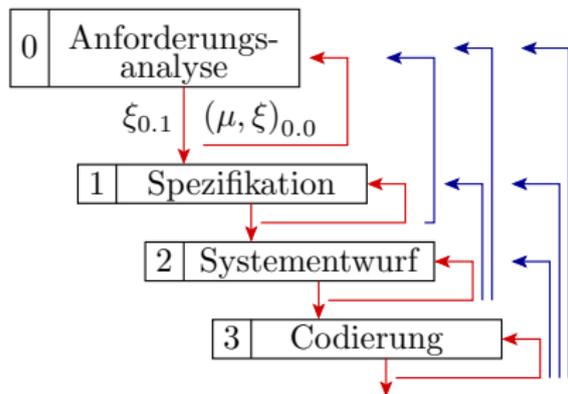
Zu erwartende Anzahl der Versuche je als gut befundenen Produkt.

$$\mu_{PR} = \frac{1}{Y_{PR}}$$

Bei zu geringer Ausbeute können auch schon in den Entstehungsprozess Reparaturiterationen eingebaut werden. Fehlerbeseitigungsiterationen lassen sich allerdings nicht mit Zählwertzuordnungsgraphen beschreiben.

Y_{PR}	Ausbeute in benutzbare Produkte je Fertigungsauftrag.
μ_{PR}	Zu erwartende Anzahl der Beauftragungen je verwendbares Produkt.

3.135 Entstehungsprozesse mit Rückgriffen

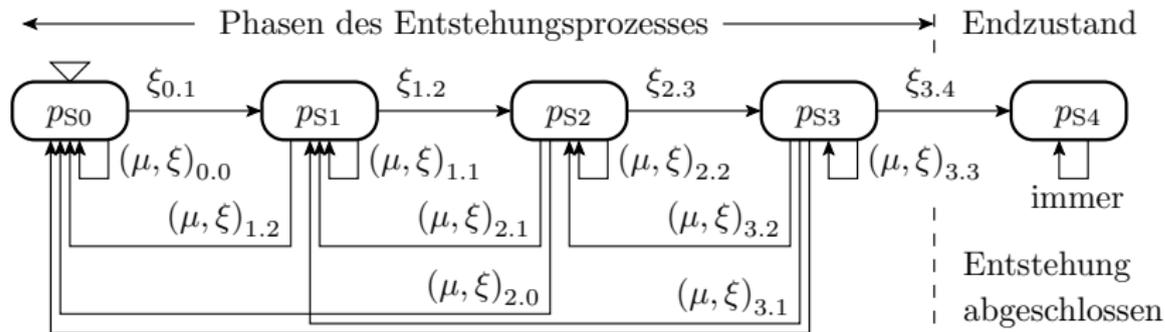


- Phasenabschluss
- ↪ Nachbesserung akt. Phase
- ↩ Rückgriff, Nachbesserung abgeschlossene Phasen

$(\mu, \xi)_{i,j}$ Kantenparameter
 — nach Zustand $j \leq i$
 — von Zustand i
 — Fehlerentstehungsrate $\xi_{i,j}$ bei Kantenübergang
 — erwartete Nachbesserungsanzahl je Vorwärtsschritt

- Entstehungsablauf als Folge von Entstehungsphasen.
- In jeder Phase gibt es Nachbesserungen, in Ausnahmen auch Nachbesserungsrückgriffe auf bereits abgeschlossene Phasen.
- Den Phasenübergängen, Nachbesserungen und Rückgriffen sind Fehlerentstehungsraten $\xi_{i,j}$ zugeordnet.

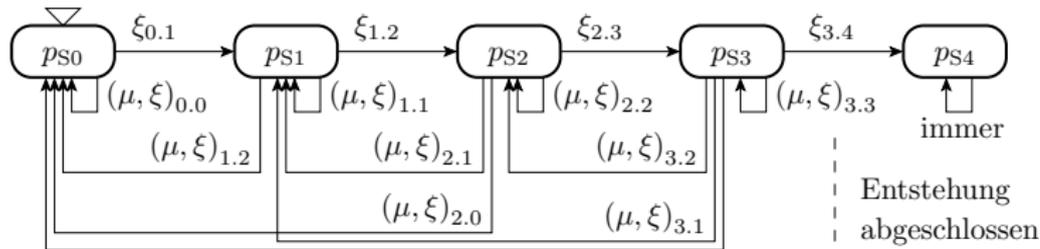
3.136 Modellierung als Markov-Kette



Die Anzahl der erwarteter Rückgriff $\mu_{i,j}$ zur Nachbesserung und Fehlerbeseitigung je Übergang zur nächsten Entwurfsphase ist anschaulicher als die dafür einzusetzenden Übergangswahrscheinlichkeiten.

- ps_i Wahrscheinlichkeit, dass Prozessphase i abgearbeitet wird.
- $(\mu, \xi)_{i,j}$ Erwarteter Übergangszahl $\mu_{i,j}$ und Fehlerentstehungsrate $\xi_{i,j}$.
- $\xi_{i,j}$ Erzeugungsrate nicht erkennbarer Fehler beim Kantenübergang $i \rightarrow j$.
- $\mu_{i,j}$ Erwartete Nachbesserungszahl bzw. Rückgriffanzahl je Vorwärtsschritt.
- $\#PS$ Anzahl der abzuarbeitenden Prozessphasen.

5. Fehlerentstehung



- Übergangswahrscheinlichkeit Nachbesserungen und Rückgriffe:

$$p_{i,j} = \frac{\mu_{i,j}}{1 + \sum_{j=0}^i \mu_{i,j}} \text{ mit } j \leq i$$

- Übergangswahrscheinlichkeit Phasenabschluss (Vorwärtsschritt):

$$p_{i,i+1} = \frac{1}{1 + \sum_{j=0}^i \mu_{i,j}}$$

- Anzahl der in Simulationsschritt n entstehenden Fehler:

$$\mu_{FS}(n) = \sum_{i=0}^{\#PS-1} p_{PS,i}(n) \cdot \left(\xi_{i,i+1} \cdot p_{i,j+1} + \sum_{j=0}^i \xi_{i,j} \cdot p_{i,j} \right)$$

$p_{i,j}$

Übergangswahrscheinlichkeit von Phase i nach Phase j .

μ_{FS}

Zu erwartende Anzahl aller im aktuellen Simulationsschritt entstehenden Fehler.

$\xi_{i,j}$

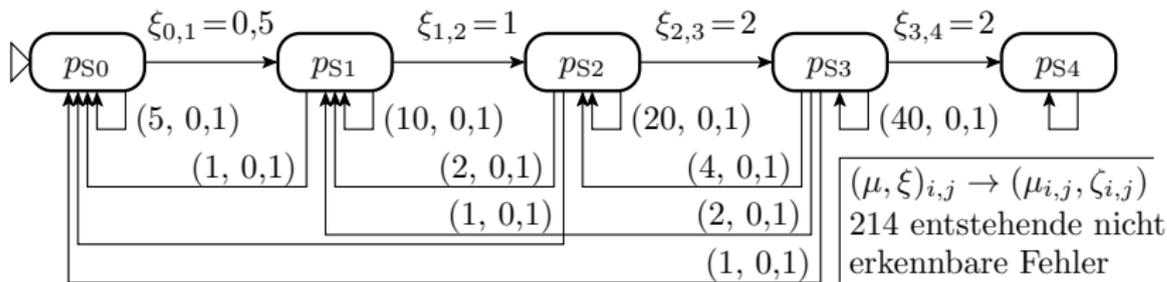
Erzeugungsrates nicht erkennbarer Fehler beim Kantenübergang $i \rightarrow j$.

$\#PS$

Anzahl der abzuarbeitenden Prozessphasen.



3.138 Beispiel



Übergangsmatrix der Markov-Kette und Zunahme der Fehleranzahl:

$$\begin{pmatrix} ps_0 \\ ps_1 \\ ps_2 \\ ps_3 \\ ps_4 \end{pmatrix}_{n+1} = \begin{pmatrix} \frac{5}{6} & \frac{1}{12} & \frac{1}{24} & \frac{1}{48} & 0 \\ \frac{1}{6} & \frac{12}{12} & \frac{24}{24} & \frac{48}{48} & 0 \\ 0 & \frac{1}{12} & \frac{24}{24} & \frac{48}{48} & 0 \\ 0 & 0 & \frac{1}{24} & \frac{40}{48} & 0 \\ 0 & 0 & 0 & \frac{48}{48} & 1 \end{pmatrix} \cdot \begin{pmatrix} ps_0 \\ ps_1 \\ ps_2 \\ ps_3 \\ ps_4 \end{pmatrix}_n$$

$$\mu_F(n) = \mu_F(n-1) + \mu_{FS}(n)$$

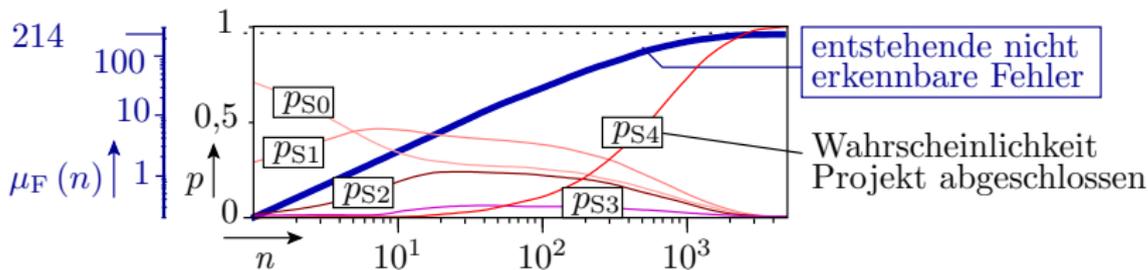
- ps_i Wahrscheinlichkeit, dass Prozessphase i abgearbeitet wird.
- $\mu_F(n)$ Akkumulierte Anzahl aller bis Simulationsschritt n entstehender Fehler.
- n Simulationsschrittnummer der Markov-Kette.



3.139 Ergebnis der Beispielsimulation

$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \\ p_{S4} \end{pmatrix}_{n+1} = \begin{pmatrix} \frac{5}{6} & \frac{1}{12} & \frac{1}{24} & \frac{1}{48} & 0 \\ \frac{1}{6} & \frac{10}{12} & \frac{2}{24} & \frac{2}{48} & 0 \\ 0 & \frac{1}{12} & \frac{20}{24} & \frac{4}{48} & 0 \\ 0 & 0 & \frac{1}{24} & \frac{48}{40} & 0 \\ 0 & 0 & 0 & \frac{1}{48} & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \\ p_{S4} \end{pmatrix}_n$$

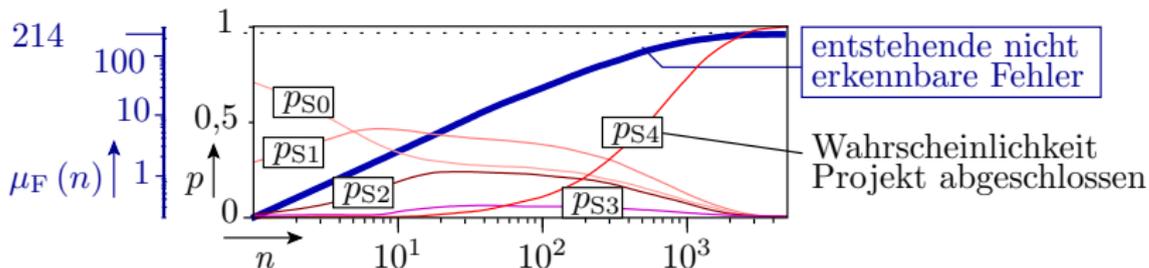
$$\mu_F(n) = \mu_F(n-1) + \mu_{FS}(n)$$



- p_{Si} Wahrscheinlichkeit, dass sich der Entstehungsprozess in Phase i befindet.
- $\mu_F(n)$ Akkumulierte Anzahl aller bis Simulationsschritt n entstehender Fehler.
- n Simulationsschrittnummer der Markov-Kette.



3.140 Ergebnis der Beispielsimulation



Der zu erwartende Phasenfortschritt und die stetige Zunahme der zu erwartenden Fehleranzahl sind gut zu erkennen.

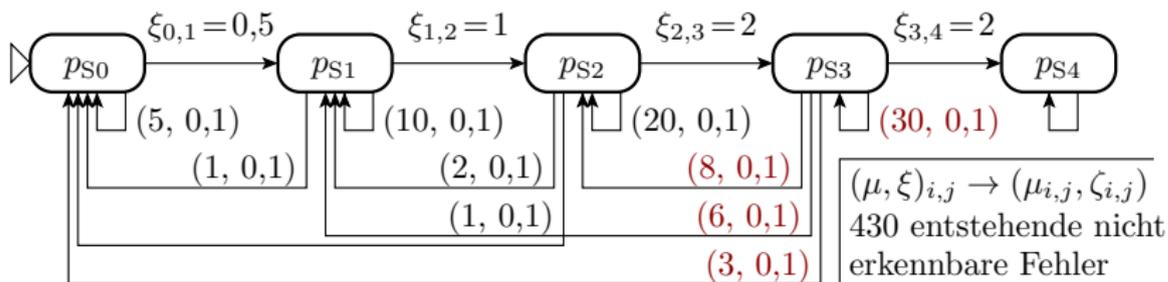
Die Wahrscheinlichkeitsverhältnisse, wie viel Arbeit auf jede Phase entfällt, sind noch nicht typisch, aber man hat die Möglichkeit durch Variation von Modellstruktur und Modellparametern Anpassungen vorzunehmen.

Zu erwartende Anzahl aller entstehenden Fehler: 214.

Bei einer Erhöhung der modellierten Rückgriffhäufigkeit und -tiefe müssten deutlich mehr Fehler entstehen.



5. Fehlerentstehung



Erhöhung der Rückgriffwahrscheinlichkeiten aus Stufe S_3 :

$p_{3.3}$:	$\frac{40}{48}$	\rightarrow	$\frac{30}{48}$	
$p_{3.2}$:	$\frac{4}{48}$	\rightarrow	$\frac{8}{48}$	(verdoppelt)
$p_{3.1}$:	$\frac{2}{48}$	\rightarrow	$\frac{6}{48}$	(verdreifacht)
$p_{3.0}$:	$\frac{1}{48}$	\rightarrow	$\frac{3}{48}$	(verdreifacht)
μ_{CF}	:	214	\rightarrow	450	(mehr als verdoppelt)

Mehr als Verdopplung von Fehleranzahl und Entstehungsaufwand.

Stufenmodelle sollten Rückgriffe über mehrere Stufen beschränken. Nicht verbieten, sondern z.B. Genehmigungsverfahren, die mit der Rückgrifftiefe »undurchlässiger« werden.



3.142 Zusammenfassung

An zwei Beispielen wurde gezeigt, wie sich Wissen über den Entstehungsfluss für eine genauere Modellierung der Fehlerentstehung und letztendlich auch der Fehlervermeidung nutzen lässt.

Für lineare Entstehungsabläufe aus Schritten und Kontrollen eignen sich Zählwertzuordnungsgraphen, aus denen sich die Produkterbringungsrate und der Fehleranteil der entstehenden Produkt ablesen lassen.

Prozesse mit Nachbesserungsiterationen lassen sich durch Markov-Ketten mit Kantenzählern beschreiben. Am Beispiel eines parametrieren Stufenmodells wurde gezeigt, wie sich die Zustandswahrscheinlichkeiten zu immer fortgeschritteneren Phasen verschieben und die zu erwartende Anzahl der entstehenden Fehler zunimmt.

Häufige Rückgriffe über viele Stufen erhöhen den Entstehungsaufwand und die zu erwartende Fehleranzahl erheblich. Deshalb sollten konkrete Stufenmodelle für Rückgriffe über viele Stufen hemmende Maßnahmen vorsehen.