Test und Verlässlichkeit 3: Themenspezifische Einführung in die Wahrscheinlichkeitrechnung

Prof. G. Kemnitz

17. Dezember 2024

Inhaltsverzeichnis

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.

1 Wahrscheinlichkeit

1.1 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:

$$\mathbb{P}[A] = \lim_{n\to\infty} \frac{\#A}{n} \tag{3.1}$$

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.

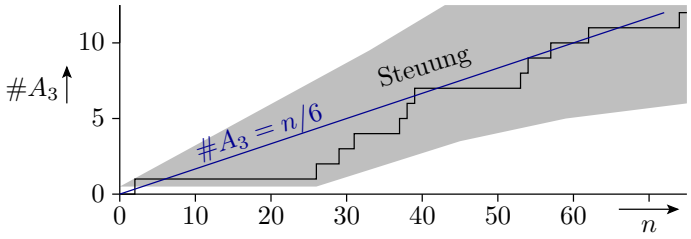
Anschließend speziell Wahrscheinlichkeiten für Fehlernachweis, Fehlerbeseitigung und Fehlerentstehung.

$\mathbb{P}[A]$ 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



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

Satz 1. *Wenn die möglichen Ereignisse eines Zufallsexperiments gleichäufig sind, ist die Wahrscheinlichkeit der Anteil der günstigen Ereignisse.*

1.2 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 $\{1,2,\ldots,6\}$. 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 realtiven 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 verketten Ereignisse E und F haben $6^2 = 36$ gleichwahrscheinliche mögliche Ergebnisse, von denen für $E = C \wedge D$ sechs und für $F = C \wedge D$ 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. 4.2.7).

3.7 Bedingte Wahrscheinlichkeiten

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

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

																				$\sum$	$\sum$
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	16
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:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]} \tag{3.2}$$

Wahrscheinlichkeit, dass B unter Bedingung A eintritt:

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

Satz von Bayes:

$$\mathbb{P}[B|A] = \mathbb{P}[A|B] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]} \tag{3.3}$$

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?

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

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.

Kontrolle mit Beispielwerten:

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

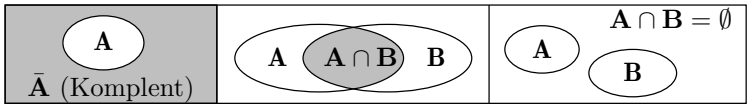
Person infiziert: $\mathbb{P}[A] = \frac{10.000}{100\,\text{Mio.}} \approx 10^{-4}$

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

3.10 NOT / UND / ODER von Ereignissen



- NOT (Nichteintrittswahrscheinlichkeit):

$$\mathbb{P}[\bar{A}] = 1 - \mathbb{P}[A] \tag{3.4}$$

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

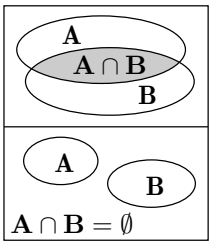
$$\mathbb{P}[A|B] = \mathbb{P}(A) = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]}$$
$$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B] \tag{3.5}$$

  - sich ausschließende Ereignisse:

$$\mathbb{P}[A \wedge B] = 0 \tag{3.6}$$

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

Vereinigungsmenge



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:

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

- sich ausschließende Ereignisse:

$$\mathbb{P}[A \wedge B] = 0$$
$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] \tag{3.8}$$

A, B	Ereignisse.
$\mathbb{P}[\ldots]$	Eintrittswahrscheinlichkeit des Ereignisses ...

3.12 Abhängig, aber nicht ausschließend

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

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

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

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

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).

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:

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

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 de-morganschen Regel in UND unabhängiger Ereignisse:

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

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

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

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

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-verküpften Terme schließen sich gegenseitig aus:

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

$\mathbb{P}[F_i]$ Wahrscheinlichkeit, dass Fehler i nachweisbar ist.
$\mathbb{P}[A]$ Wahrscheinlichkeit, dass alle Fehler nachgewiesen werden.
$\mathbb{P}[B]$ Wahrscheinlichkeit, dass kein Fehler nachgewiesen wird.
$\mathbb{P}[C]$ Wahrscheinlichkeit, dass mindestes ein Fehler nachgewiesen wird.
$\mathbb{P}[D]$ 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?

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:

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

Zwei Fehler sind nachweisbar, wenn beide Fehler nachweisbar sind:

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

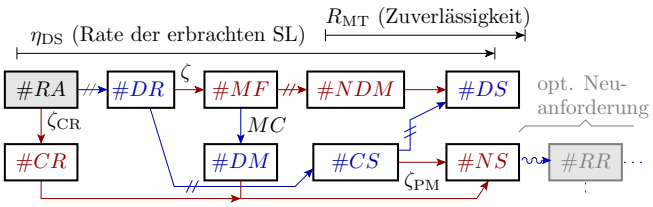
Probe: Die Summe der Wahrscheinlichkeiten der drei möglichen Ergebnisse muss 1 sein:

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

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

1.3 CVA-Graph

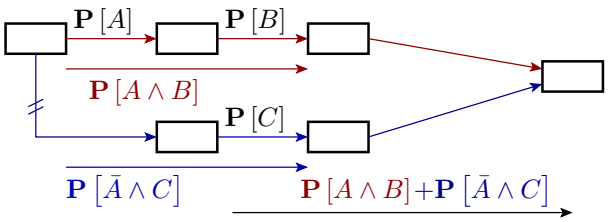
3.15 Beispiel für einen Zählwertzuordnungsgraphen



- 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.
DR, MF	Erbrachtes Ergebnis, Fehlfunktion.
DM,NDM	Erkannte Fehlfunktion, nicht erkannte Fehlfunktion.

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 Zurdnungsereignissen. Bei Unabhängigkeit Wahrscheinlichkeitsprodukt:

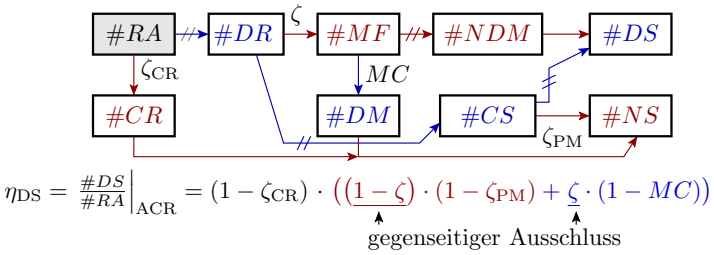
$$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B] \tag{3.5}$$

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

$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] \tag{3.8}$$

.

3.17 Für das Beispiel



Zuordnungsereignisse, für die Unabhängigkeit unterstellt wird:

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

Zusammenführung mit gegenseitigem Ausschluss:

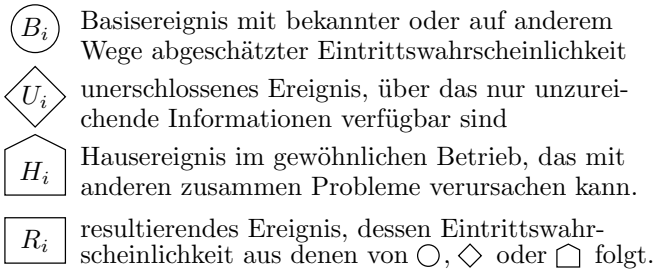
- erkannte Fehlfunktionen (DM) und Phantom-Fehlfunktionen zu nicht erbrachten Leistungen (NS) und
- sonstige korrekte Leistungen und nicht erkannte Fehlfunktionen (NDM) zu erbrachten Leistungen (DS).

1.4 Fehlerbäume

3.18 Fehlerbaumanalyse (FTA – fault tree analysis)

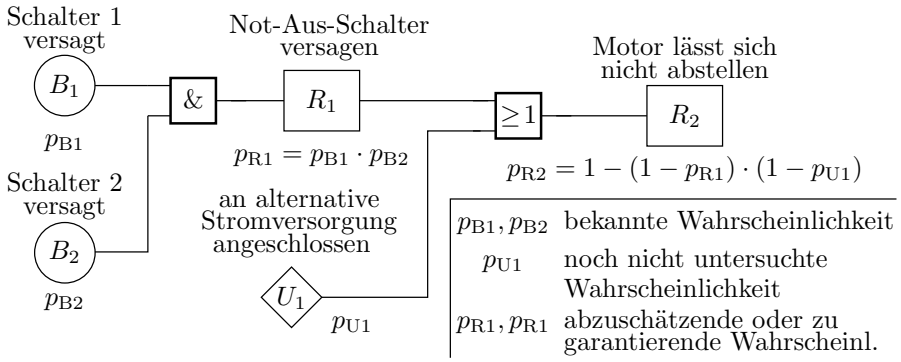
Graphische Darstellung für logische Ereignisbeziehungen (UND, ODER, Nicht*) zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahrensituationen, Ausfälle, Fehlfunktionen, ...

Unterschiedene Ereignistypen:



* 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* $p_{B1} = p_{B2} = 10^{-3}$*?*

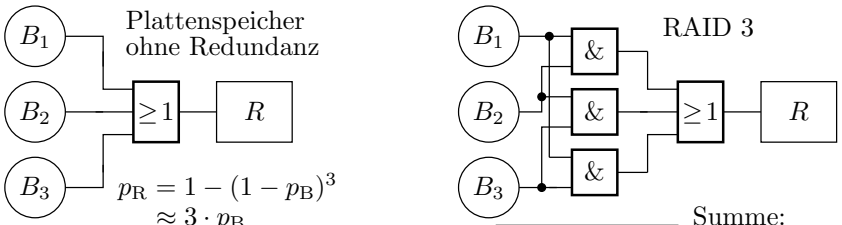
$$p_{R1} = p_{B1} \cdot p_{B2} = 10^{-6}$$
$$p_{R2} = 1 - (1 - p_{R1}) \cdot (1 - p_{U1}) \leq 10^{-6}$$

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

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.

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	$p_B^2 \cdot (1 - p_B)$
1	0	0	0	
1	0	1	1	$p_B^2 \cdot (1 - p_B)$
1	1	0	1	$p_B^2 \cdot (1 - p_B)$
1	1	1	1	p_B^3

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

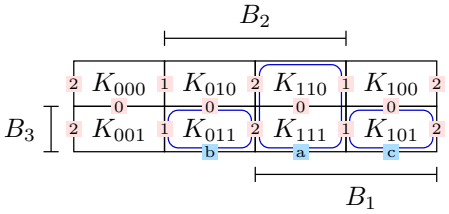
3.21 Rekonvergente Auffächerungen

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

$$R = B_1B_2 \vee B_2B_3 \vee B_1B_3$$

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

Umstellung in Terme sich ausschließender Ereignisse:



Überdeckungsfreie Konjunktionen:
- a: B_1B_2
- b: $\bar{B}_1B_2B_3$
- c: $B_1\bar{B}_2B_3$

$$\begin{aligned} R &= B_1B_2 \vee \bar{B}_1B_2B_3 \vee B_1\bar{B}_2B_3 \\ p_R &= p_B^2 + p_B^2 \cdot (1 - p_B) + p_B^2 \cdot (1 - p_B) = 3 \cdot p_B^2 - 2 \cdot p_B^3 \end{aligned}$$

3.22 Geschichte der Fehlerbaumanalyse

- Einführung 1960: Abschlusssicherheitsbewertung 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, ...

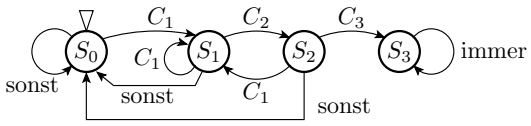
Für Interkontinentalraketen mit Atomsprengköpfen nicht sehr vertrauenserweckend.

1.5 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 $C_1C_2C_3$:



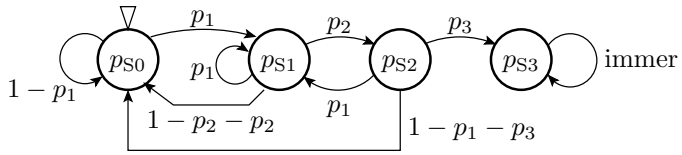
Start im Zustand S_0 »keine richtige Eingabe« und Verbleib nach drei richtigen Eingaben im Zustand S_3 »Fehler nachgewiesen«.

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 $p_{S0} = 1$ und die anderen Zustände haben die Wahrscheinlichkeit $p_{S.i}|_{i\neq 0} = 0$.

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

---

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

p_j Wahrscheinlichkeit von Zustandsübergang C_j.

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

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

mit $\begin{pmatrix} p_{S0} & p_{S1} & p_{S2} & p_{S3} \end{pmatrix}_0^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$.

Kontrollkriterien für Gleichungssystem und Simulationsergebnis:

- Summe der Wahrscheinlichkeiten je Matrixspalte eins.
- Summe aller $p_{S.i}$ nach jedem Schritt eins.

$(\ldots)^T$ Transponierte Matrix (Tausch von Zeilen und Spalten).

n Schrittnummer der Simulation der Markov-Kette.

Simulation mit Octave bzw. Matlab:

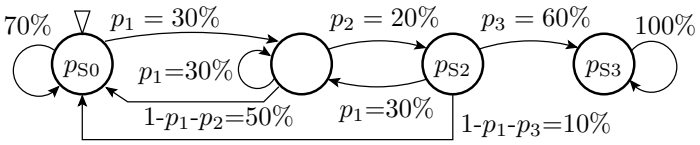
```
p1=...; p2=...; p3=...;

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;
```

3.26 Beispielsimulation

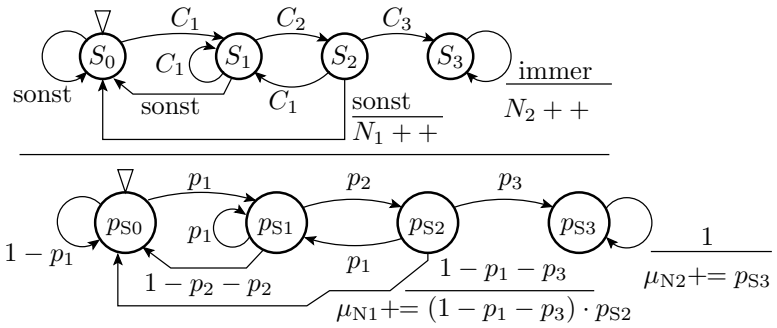
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



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%

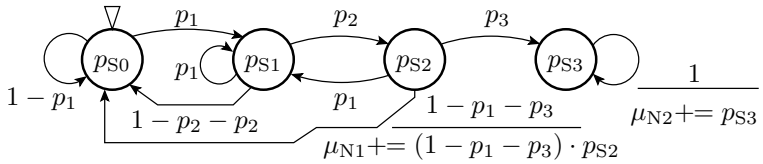
3.28 Kantenzähler

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



n	Schrittnummer der Simulation 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_{Ni}	Zu erwartende Kantenübergangsanzahl.
$n-\mu_{N2}$	Zu erwartende Schrittanzahl bis zum Fehlernachweis.

In den Variablen $\mu_{...}$ werden die Wahrscheinlichkeiten der Kantenübergänge aufsummiert. Wie später gezeigt, sind das die Erwartungswerte der Anzahl der Übergänge. Analog auch Erwartungswert, wie oft System in eine Zustand ist, bestimmbar.



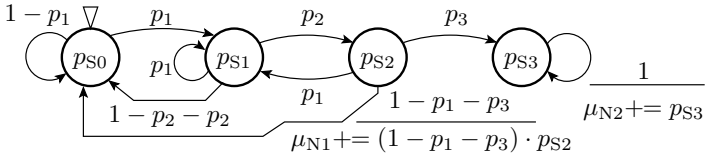
Erweiterung des Simulationsprogramms:

```
...
N1=0; N2=0;

for idx=1:100
 Z = M * Z;
 N1 = N1+Z(3)*(1-p1-p3);
 N2 = N2+Z(4);
 printf('%3i %6.2f%% %6.2f%% %6.2f%% %6.2f%%',idx,100*Z);
 printf('%6.2f %6.2f\n', N1, N2);
end;
```

3.29 Beispielsimulation

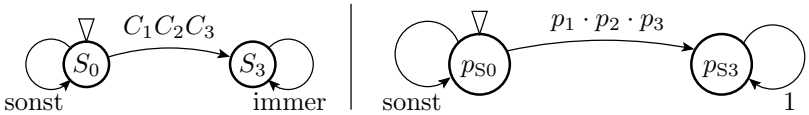
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$



Schritt	p_{S0}	p_{S1}	p_{S2}	p_{S3}	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: $n - \mu_{N2} \approx 20$

3.30 Drei richtige Eingaben als Einzelereignis



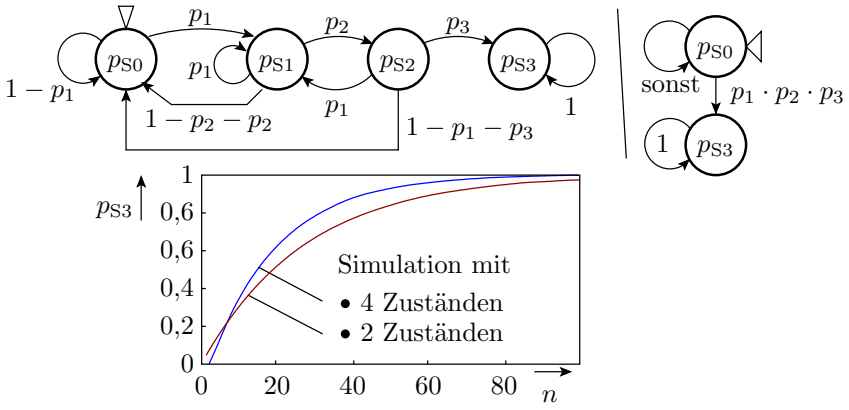
Gleichungssystem
der modifizierten Markov-Kette:

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

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

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

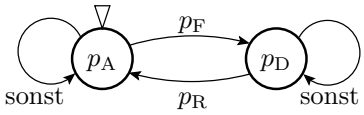
3.31 Unterschied zwischen den Markov-Ketten



Offenbar doch nicht ganz identisches Verhalten, aber sehr ähnliches.

3.32 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):



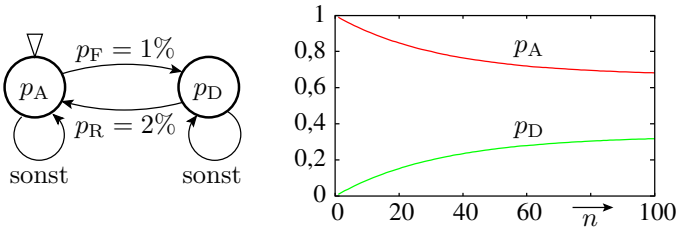
Modellierung als simulierbares Gleichungssystem:

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

---

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 Schrittnummer der Simulation der Markov-Kette.

3.33 Beispielsimulation



Stationärer Zustand:

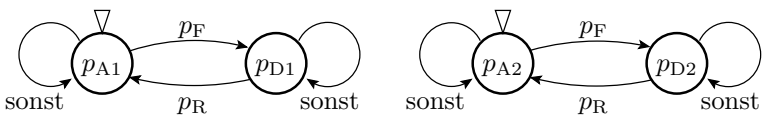
$$p_A \cdot p_F = p_D \cdot p_R \quad \text{mit } p_A + p_D = 1$$
$$p_A = \frac{p_R}{p_R+p_F} = \frac{2\%}{1\%+2\%} = 66{,}7\%$$
$$p_D = \frac{p_F}{p_R+p_F} = \frac{1\%}{1\%+2\%} = 33{,}3\%$$

---

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.

Reparaturprozess für ein 1oo2 System

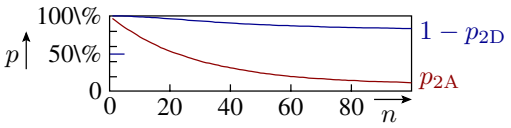
System aus zwei gleichartigen Teilsystemen, das solange funktioniert, wie 1 von (**o**ut **o**f) 2 Teilsystemen funktioniert:




```
pF=0.01; pR=0.02;
M=[1-pF  pR; pF  1-pR];
S=[1; 0];
for n=1:100
```

```
    S = M * S;
    p2A(n)=S(1)**2; % beide Einheiten ganz
    p2D(n)=S(2)**2; % beide Einheiten defekt
end;
plot(1:100, p2A, 1:100, 1-p2D)
```

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



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

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

n	Schrittnummer der Simulation 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

3.35 Wahrscheinlichkeit

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

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

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

3.36 Verketteter Ereignisse

Bedingte Wahrscheinlichkeit:

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

Satz von Bayes:

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

Gegenwahrscheinlichkeit:

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

UND unabhängiger Ereignisse:

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

UND sich ausschließerder Ereignisse:

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

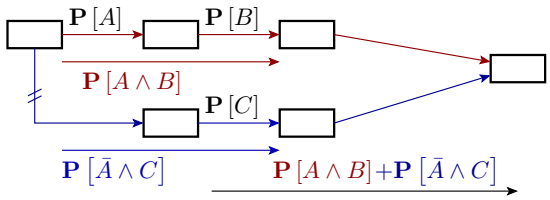
ODER unabhängiger Ereignisse:

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

Oder sich ausschließender Ereignisse:

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

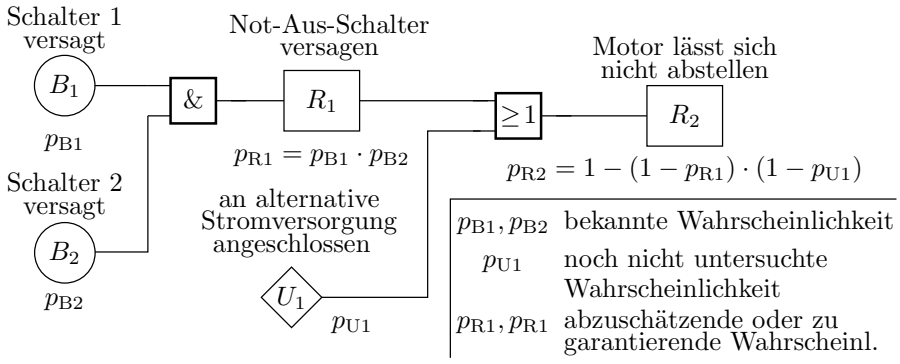
3.37 Zählwertzuordnungsgraph



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

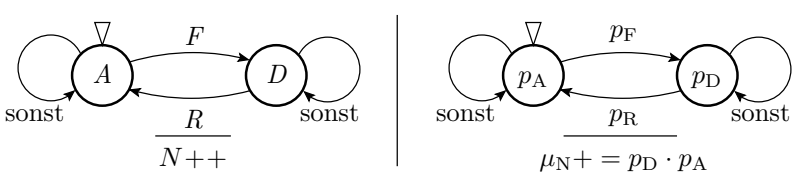
- eine Zuordnung über mehrere Kante eine »UND« unabhängiger Ereignisse und
- Zusammenführungen ein »ODER« sich ausschließender Ereignisse beschreiben.

3.38 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.

3.39 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:

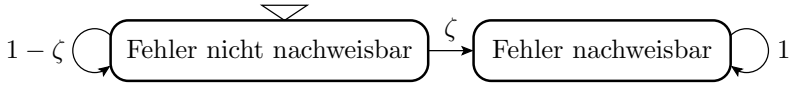
- Fehlernachweis,
- Fehlerentstehung,
- Verfügbarkeit, ...

Kantenzähler für die zu erwartende Anzahl der Übergänge.

2 Fehlernachweis

2.1 Nachweis & Zuverlässigkeit

3.40 Nachweiswahrscheinlichkeit



Ein Fehler verursacht mit einer Rate ζ Fehlfunktionen, an denen er erkannt wird:

$$p_{FD}(\zeta, N) = 1 - (1-\zeta)^N = 1 - e^{\ln(1-\zeta)\cdot N}$$
$$\approx^* 1 - e^{-\zeta \cdot n} \quad \text{für } \zeta \ll 1$$

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:

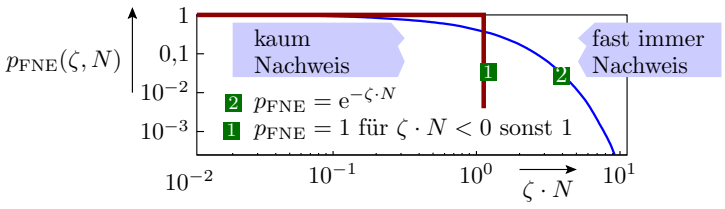
$$p_{FD}(\zeta, N) = 1 - e^{-\zeta \cdot N} \tag{3.9}$$

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

ζ Fehlfunktionsrate des Fehlers.

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

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

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

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

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

3.42 Abnahme Fehleranzahl mit Testanzahl

(2.13) $$\mu_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \mathrm{d}\zeta$$

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

Nichtbeseitigungswahrscheinlichkeit als Gegenwahrscheinlichkeit der Nachweiswahrscheinlichkeit (Gl. 3.9):

$$p_{\mathrm{FNE}}(\zeta, N) = 1 - p_{\mathrm{FD}}(\zeta, N) = \mathrm{e}^{-\zeta \cdot N} \tag{3.10}$$

Alles eingesetzt:

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

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

$$\mu_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^N \underbrace{\mathrm{e}^{-z}}_{p_{\mathrm{FNE}}(\zeta,N)} \cdot \underbrace{K \cdot \left(\tfrac{z}{N}\right)^{K-1}}_{h(\zeta)} \cdot \tfrac{\mathrm{d}z}{N} = \tfrac{\mu_{\mathrm{F}} \cdot K}{N^K} \cdot \underbrace{\int_0^N \mathrm{e}^{-z} \cdot z^{K-1} \cdot \mathrm{d}z}_{*}$$

$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$p_{\mathrm{FNE}}(\zeta, N)$	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 $\int_0^\infty \ldots \mathrm{d}z$.

3.43 Gammafunktion

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

$$\Gamma(K) = \int_0^\infty \mathrm{e}^{-z} \cdot z^{K-1} \cdot \mathrm{d}z \approx \tfrac{1}{K} \tag{3.11}$$

- Für $0 < K < 1$ gilt:

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

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:

$$\Gamma(K+1) = K \cdot \Gamma(K) \tag{3.12}$$

$\Gamma(\ldots)$	Gamma-Funktion.
K	Parameter der Gamma-Funktion und Formfaktor der Verteilung der Fehlfunktionsrate.

3.44 Verbleibende Fehleranzahl (Fortsetzung)

$$\mu_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}} \cdot K \cdot \Gamma(K)}{N^K} \tag{3.13}$$

Für die Abnahme der zu erwartenden Fehleranzahl mit der effektiven Testanzahl gilt auch mit der genauer abgeschätzten Nachweiswahrscheinlichkeit (Gl. 3.9) das Potenzgesetz:

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

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

$$\mu_{\mathrm{FC}}(N) = 1 - \left(\tfrac{N}{N_0}\right)^{-K} \tag{3.14}$$

3.45 Dieselbe Kontrolle für die Fehlfunktionsrate

(2.14)
$$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \mu_{\mathrm{F}} \cdot \underbrace{\int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \zeta \cdot \mathrm{d}\zeta}_{\text{mittlere Fehlfunktionsrate je Fehler}}$$

$$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^1 \mathrm{e}^{-\zeta \cdot N} \cdot K \cdot \zeta^{K-1} \cdot \zeta \cdot \mathrm{d}\zeta$$

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

$$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \mu_{\mathrm{F}} \cdot \int_0^N \underbrace{\mathrm{e}^{-z}}_{p_{\mathrm{FNE}}(\zeta,N)} \cdot \underbrace{K \cdot \left(\tfrac{z}{N}\right)^{K-1}}_{h(\zeta)} \cdot \tfrac{z}{N} \cdot \tfrac{\mathrm{d}z}{N} = \tfrac{\mu_{\mathrm{F}} \cdot K}{N^{K+1}} \cdot \int_0^N \mathrm{e}^{-z} \cdot z^K \cdot \mathrm{d}z$$

$$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \tfrac{\mu_{\mathrm{F}} \cdot K \cdot \Gamma(K+1)}{N^{K+1}} = \tfrac{\mu_{\mathrm{F}} \cdot K^2 \cdot \Gamma(K)}{N^{K+1}} \tag{3.15}$$

Für die Abnahme der MF-Rate mit der effektiven Testanzahl gilt auch mit Fehlernachweiswahrscheinlichkeit (Gl. 3.9) das Potenzgesetz

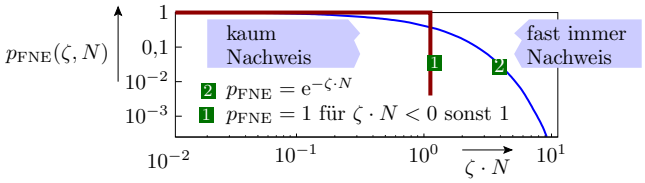
(2.22)
$$\zeta_{\mathrm{F}}(N_2) \overset{(\leq 1)}{=} \zeta_{\mathrm{F}}(N_1) \cdot \left(\tfrac{N_2}{N_1}\right)^{-(K+1)}$$

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

$\zeta_{\mathrm{F}}(N)$ Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.

(≥ 1) Der errechnete Wert ist eine Obergrenze. Der tatsächliche Wert ist max. eins.

3.46 Vergleich mit bisherigem Modell



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

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

   (2.20)
   $$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \mu_{\mathrm{F}} \cdot \tfrac{K}{K+1} \cdot N^{-(K+1)}$$

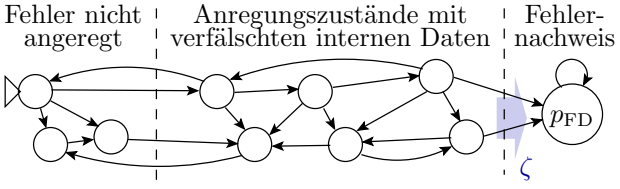
2. Mit $p_{\mathrm{FNE}}(\zeta, N) = \mathrm{e}^{-\zeta \cdot N}$:

   (2.23)
   $$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \tfrac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

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

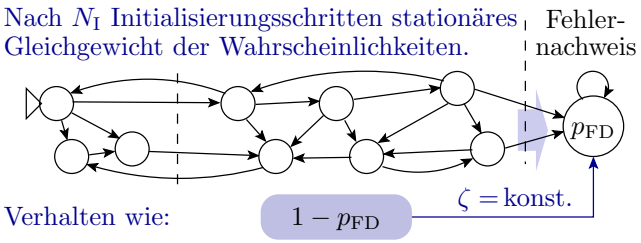
2.2 Service mit Gedächtnis

3.47 Service mit Gedächtnis



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

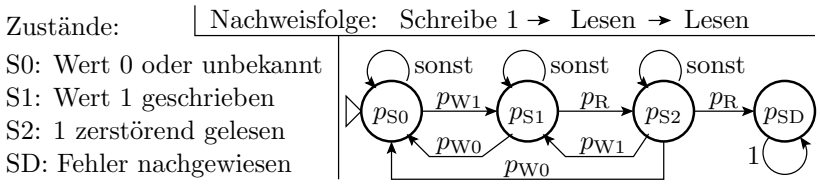
Eine genaue Modellierung des Zusammenhangs zwischen Nachweiswahrscheinlichkeit und Testanzahl verlangt für jeden Fehler einen individuellen Beobachterautomaten, aus dem sich eine fehlerspezifische Markov-Kette ableitet. Oft mehr als zwei Zustände, testschrittabhängige Fehlfunktionsrate ζ.



An einem Beispielfehler wird gezeigt, dass solche Beobachterautomaten dazu tendieren, sich für lange Testsätze nahzu wie der Zweizustands-Beobachterautomat 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.

3.49 Beispiel: RAM-DR1-Fehler

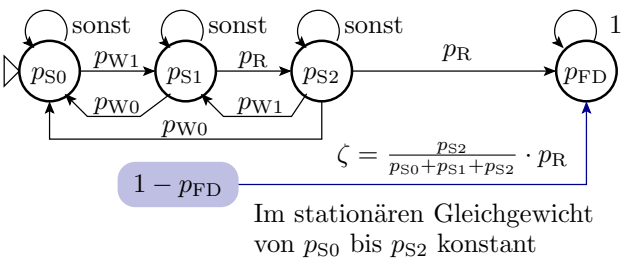


Im RAM wird beim Lesen der fehlerhaften Speicherzelle mit Adresse a eine gespeicherte 1 in eine 0 verfälscht. Der Nachweis erfordert:

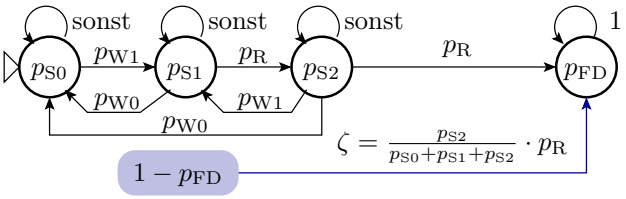
- Schreibe 1 auf Adresse a (Übergang in Zustand S1),
- Lese Wert von Adresse a (Übergang in Anregungszustand S2),
- Lese von Adresse a ohne zwischenzeitlichen Schreibzugriff auf a (Übergang in den Nachweiszustand SD).

---

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.



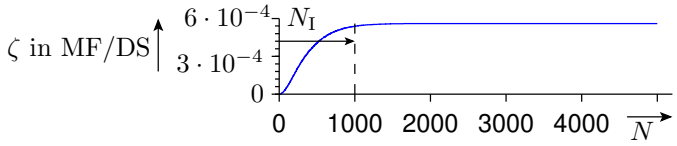
Die äquivalente Fehlfunktionsrate für die Zweizustands-Markov-Kette ist hier die bedingte Wahrscheinlichkeit, dass der Beobachterautomat im Zustand S2 ist, wenn er nicht im Zustand FD, also in einem der Zustande S1, S2 oder S3 ist, und die defekte Speicherzelle gelesen wird.




```
pS0=1; pS1=0; pS2=0; pSD(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW0 = pW1 = 1/(4*NA);
for n=1:N
  p0   = pS0 * (1-pW1) + pS1*pW0         + pS2*pW0;
  p1   = pS0 *    pW1  + pS1*(1-pW0-pR) + pS2*pW1;
  p2   = pS1 *    pR   + pS2*(1-pW1+pW0-pR);
  pFD   = pSD(n) + pS2 * pR;
  zeta  = pS2*pR / (pS0+pS1+pS2); % MF rate
  pS0 = p0; pS1 = p1; pS2 = p2;
end
plot(1:N, zeta);
```

p_{Si}	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.

3.50 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:

$$p_{FD}(\zeta, N) \geq 1 - e^{-\zeta \cdot (N - N_I)} \tag{3.16}$$

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

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

$p_{FD}(N)$	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.

2.3 Fehler und Modellfehler

3.51 Fehler und Modellfehler (Abschn. 2.1.5)

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

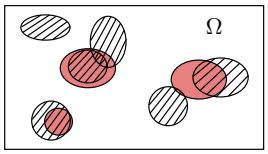
Testauswahl und Testbewertung verwenden Modellfehler.

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?

3.52 Nachweismengen, Nachweisbeziehungen

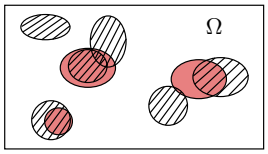


Ω Ereignisraum, hier Menge der möglichen Eingaben bzw. Eingabefolgen.
Nachweismenge eines Modellfehlers
Nachweismenge eines tatsächlichen Fehlers

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.

3.53 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:

(3.14)
$$\mu_{\mathrm{FC}}(N) = 1 - \left(\frac{N}{N_0}\right)^{-K}$$

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.

3.54 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):

(2.37)
$$N = c \cdot N_{\mathrm{MF}} \quad \text{für } \mu_{\mathrm{FC}}(N) = \mu_{\mathrm{FCM}}(N_{\mathrm{MF}})$$

- $c < 1$: Modellfehler tendentiell strengere Nachweisbedingungen,

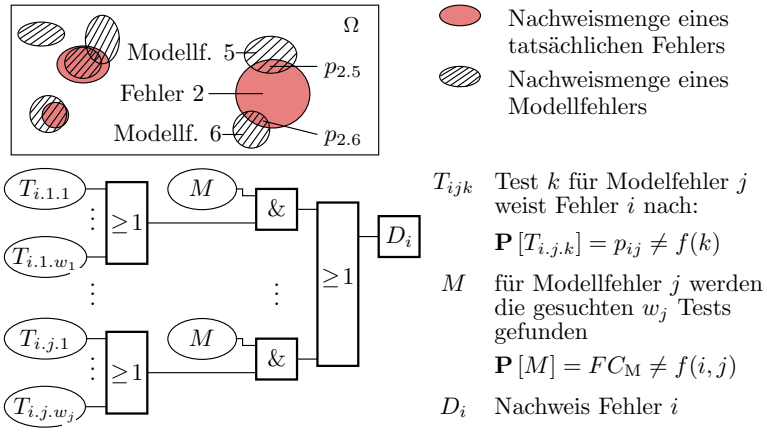
- $c > 1$: Modellfehler tendentiell einfachere Nachweisbedingungen.

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.

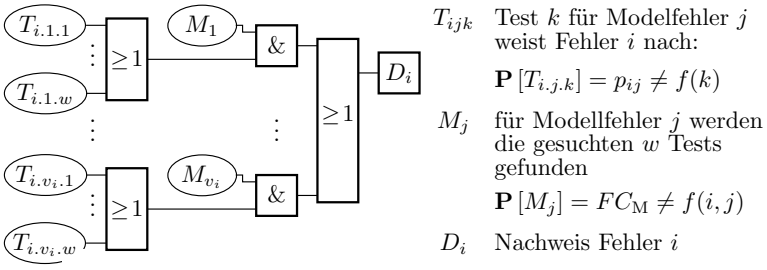
Ähnlich gut zu befriedigene Nachweisbedingungen ist umgekehrt die Anforderung des Zufallstests an ein Fehlermodell.

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

3.55 Gezielte Testsuche



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 $\mathbb{P}[M] = FC_{\mathrm{M}}$ gefunden werden.



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:

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

$$p_{\mathrm{FD}.i} = \mathbb{P}(D_i) = 1 - \prod_{j=1}^{v_i} (1 - (FC_{\mathrm{M}} \cdot (1 - (1 - p_{ij})^w))) \tag{3.17}$$

w	Anzahl der je Modellfehler gesuchten Tests. Gefunden werden alle oder keiner.

3.57 Zahlenbeispiel

$$p_i = 1 - \prod_{j=1}^{v_i} (1 - (FC_{\mathrm{M}} \cdot (1 - (1 - p_{ij})^w)))$$

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

$p_i\,(w,\, FC_{\mathrm{M}})$	$w=1$	$w=2$	$w=3$	$w=4$	$w=5$
$FC_{\mathrm{M}} = 90\%$	72,0%	91,8%	97,5%	99,15%	99,70%
$FC_{\mathrm{M}} = 95\%$	74,2%	93,2%	98,1%	99,47%	99,84%

Tatsächlich haben Fehler weder gleich viele ähnlich nachweisbare Modellfehler noch ähnlich große p_{ij} (Pareto-Prinzip vernachlässigt), ...

Vorsichtige Schlussfolgerungen:

- Abschätzung der Fehler- aus der Modellfehlerabdeckung unsicher.
- Es ist nützlich, für jeden Modellfehler mehrere Tests zu suchen.
- Suche kurzer Testsätze mit ausreichender FC_{M} schlechte Idee.

---

p_i Nachweiswahrscheinlichkeit Fehler i.

v_i AnzahIl der ähnlich nachweisbaren Modellfehler für Fehler i.

FC_{M} Modellfehlerabdeckung.

w Anzahl der je Modellfehler gesuchten Tests. Gefunden werden alle oder keiner.

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

3.58 Anforderungen an das Fehlermodell

$p_i\,(w,\, FC_{\mathrm{M}})$	$w=1$	$w=2$	$w=3$	$w=4$	$w=5$
$FC_{\mathrm{M}} = 90\%$	72,0%	91,8%	97,5%	99,15%	99,70%
$FC_{\mathrm{M}} = 95\%$	74,2%	93,2%	98,1%	99,47%	99,84%

Fehlermodelle für geziele Testauswahl

1. Das Fehlermodell muss für jeden zu erwartenden Fehler (mehrere) ähnlich nachweisbare Modellfehler generieren.
2. Die Anzahl zu suchende Tests je Modellfehler sollte Größenordnung »Kehrwerts der kleinsten p_{ij}« haben.
3. Testauswahl je Modellfehler muss Zufallscharakter haben.

Erst wenn Fehlermodell und Auswahltechniken das leistet, lohnen weiterführende Gedanken zur gezielten Testauswahl.

2.4 Operationsprofil

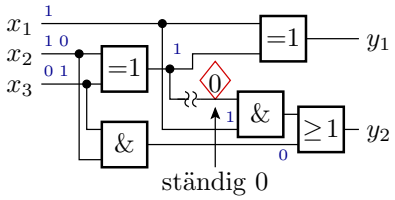
3.59 Operationsprofil, Test und Zuverlässigkeit

Das Operationsprofil beschreibt die Art der Systemnutzung, genauer die relative Nutzungshäufigkeit der Eingaben. Erheblicher Einfluss auf die Nachweiswahrscheinlichkeiten und Fehlfunktionsraten jedes einzelnen vorhandenen und modellierten Fehlers.

- Die Sicherung der Zuverlässigkeit erfolgt bisher durch Test und Fehlerbeseitigung mit dem Operationprofil der Anwendung.
- Ein Wechsel des Operationsprofils im Einsatz bewirkt, dass plötzlich andere Probleme dominieren und der Nutzer erneut mit der Suche von Workarround beschäftigt ist (Abschn. 2.2.8).
- In der Iteration aus Test und Fehlerbeseitigung bewirken Wechsel des Operationsprofils sprunghafte Anstiege der Anzahl der erkennbaren und zu beseitigenden Fehler.

Der Test mit mehreren Operationsprofilen ist zwingend für die Sicherung der Zuverlässigkeit für alle zu erwartenden Arten der Nutzung und hilfreich, um viele Fehler zu finden.

3.60 Nutzung und Nachweiswahrscheinlichkeit



Eingaben die den Fehler nachweisen

Eingabe x_3	x_2	x_1	Ausgabe y_2	y_1	Nutzungshäufigkeit der Eingabewerte		
0	0	0	0	0	0,125	0,1	0,1
0	0	1	0	1	0,125	0,05	0,1
0	1	0	0	1	0,125	0,15	0,2
0	1	1	1	0	0,125	0,2	0,05
1	0	0	0	1	0,125	0,05	0,2
1	0	1	1	0	0,125	0,2	0,05
1	1	0	1	0	0,125	0,05	0,2
1	1	1	1	1	0,125	0,2	0,1
Nachweiswahrscheinlichkeit:						0,25	0,4	0,1

Fehler haben eine Nachweismenge von Eingaben. Die

- Nachweiswahrscheinlichkeit während des Tests und
- die Fehlfunktionsraten im Einsatz

hängen von den Nutzungshäufigkeiten dieser Eingaben ab.

Der eingezeichnete Haftfehler ist mit zwei der acht möglichen Eingaben nachweisbar.

3.61 Operationsprofil und Nachweiswahrsch.

Das Operationsprofil legt die Auftrittshäufigkeiten der Eingaben fest. Bevorzugung der Eingaben der Nachweismenge verbessert und Benachteiligung mindert die Nachweiswahrscheinlichkeit.

Ein Wechsel des Operationsprofils kann vorher gut nachweisbare in danach schlecht nachweisbare Fehler und umgekehrt umwandeln.

3.62 Unterschiedliche Operationsprofile

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

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

Nach einem Vortest mit N_0 dynamischen Tests bewirkt eine Testverlängerung auf $N \gg N_0$ Tests mit dem Operationsprofil der Anwendung eine Abnahme der zu erwartenden Fehleranzahl und eine Zunahme der fehlerbezogenen Teilzuverlässigkeit auf:

$$\mu_{F.1}(N) = \mu_F(N_0) \cdot \left(\frac{N}{N_0}\right)^{-K}$$

$$R_{F.1}(N) \overset{(\geq 1)}{=} \frac{N}{K \cdot \mu_F(N_1) \cdot \left(\frac{N}{N_0}\right)^{-K}} \sim N^{1+K}$$

Bei eine Fortsetzung mit weiteren $N - N_0$ Tests mit einem zweiten Operationsprofil sind andere Fehler gut nachweisbar.

N_0, N	Anzahl Vortests, Anzahl der Tests je Operationsprofil incl. N_0.
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).
(≤ 1)	Der errechnete Wert ist eine Untergrenze. Der tatsächliche Wert ist mindestens eins.

Abnahme der zu erwartenden Fehleranzahl durch Testverlängerung gegenüber Vortest von $N/N_0 \gg 2$ statt durch Testverlängerung gegenüber allen bisherigen Tests von nur $(N - N_0 + N)/N \approx 2$:

$$\mu_{F.2}(N) = \mu_F(N_0) \cdot \left(\frac{N}{N_0}\right)^{-K} \cdot \left(\frac{N}{N_0}\right)^{-K}$$

$$R_{F.2}(N) = \frac{N}{K \cdot \mu_F(N_0) \cdot \left(\frac{N}{N_0}\right)^{-K} \cdot \left(\frac{N}{N_0}\right)^{-K}} \sim N^{1+2K}$$

Für $\#OP$ Operationsprofile mit je Testanzahl N nimmt unter der gleichbleibenden Annahme, dass

- für jedes neue Operationsprofil andere Fehler in den Bereich der mit N Tests nachweisbaren Fehler rücken,
- die Tests für das neue Operationsprofil dadurch den Anteil der nicht beseitigten Fehler immer um $(N/N_0)^K$ verringern,
- die zusätzlichen Tests im ungünstigsten Fall nicht zur effektiven Testanzahl anderer Operationsprofile beitragen ...

$\mu_{\mathrm{F.i}}(N)$ Anzahl nicht nachweisbarer Fehler nach Test mit i Operationsprofilen, je Länge N.
$R_{\mathrm{F.i}}(N)$ Fehlerbezogene Teilzuverlässigkeit nach Test mit i Operationsprofilen, je Länge N.
N_0, N Anzahl Vortests, Anzahl der Tests je Operationsprofil incl. N_0.

... die Fehleranzahl mit der $\#OP \cdot K$-ten Potenz ab und die Zuverlässigkeit mit der $1 + \#OP \cdot K$-ten Potenz zu:

$$\mu_{\mathrm{F.\#OP}}(N) = \mu_{\mathrm{F}}(N_0) \cdot \left(\tfrac{N}{N_0}\right)^{-\#OP \cdot K} \tag{3.18}$$

$$R_{\mathrm{F.\#OP}}(N) = R_{\mathrm{F}}(N_0) \cdot \left(\tfrac{N}{N_0}\right)^{1+\#OP \cdot K} \tag{3.19}$$

Die Modellannahmen und Ergebnis sind Spekulationen. Gesichert gilt:

- Ausreichend viele Tests mit allen für die Anwendung zu erwartenden Operationsprofile zwingend (Mindestzuverlässigkeit).
- Zusätzlichen Tests mit anderen Operationsprofilen finden mehr Fehler, als weitere Tests mit demselben Operationsprofil.
- Das auswürfeln der Tests für ein Operationsprofil muss Zufallscharakter haben.

Opertionsprofil-basierten Testauswahl ist auf jeden Fall für die Praxis interessant. Wie weit das hier skizziert Potential praktisch nutzbar ist, wird künftige Forschung zeigen.

$\mu_{\mathrm{F.i}}(N)$ Anzahl nicht nachweisbarer Fehler nach Test mit i Operationsprofilen, je Länge N.
$R_{\mathrm{F.i}}(N)$ Fehlerbezogene Teilzuverlässigkeit nach Test mit i Operationsprofilen, je Länge N.
N_0, N Anzahl Vortests, Anzahl der Tests je Operationsprofil incl. N_0.
$\#OP$ Anzahl der unterschiedlichen Operationsprofile, mit denen getestet wird.

3.65 Fehlerorientierte Operationsprofilauswahl

Nutzung von Modellfehlermengen zur Operationsprofilauswahl (statt zur Testauswahl). Erlaubt sehr lange Tests je Modellfehler und kommt mit einem Fehlermodell »mit sehr kleinen p_{ij}'s« aus:

Pragmatischer Ansatz für die praktische Testauswahl:

- Aufstellung einer Menge simulierbarerer Modellfehler. Entfernen erkennbar identisch nachweisbarer und redundanter Fehler.
- Fehlersimulation mit z.B. $N = 10^4$ Tests mit Standardoperationsprofil. Entfernen aller nachweisbaren Modellfehler.
- Wiederhole, bis alle Modellfehler nachweisbar:
  - Errate günstiges Operationsprofil für den Rest der Modellfehler.
  - Fehlersimulation wieder mit N Tests, aber dem neuen Operationsprofil. Entfernen aller nachweisbaren Modellfehler.

Für digitaler Schaltungen kann man auf diese Weise sog. Wichtungen als Operationsprofil berechnen und sogar für Selbsttests nutzen (Abschn. 6.3.4 *Fehlerorientierte Wichtung*).

3.66 Nutzungsfälle, symbolische Tests, Fuzzing

Im modernen Softwareentwurf werden die Anforderungen in Form typischen Nutzungsfällen (Use cases), Grenzfälle, symbolischen Tests*, ... skizziert (Abschn. 7.2.3 *Testbare Anforderungen*). Jede Anforderung ist zu testen, und zwar mit viele (tausenden) Tests mit einem zur Testabsicht passendem Operationsprofil.

Für Software ist vor wenigen Jahren der Begriff Fuzz-Tests aufgetaucht. Das waren lange Zufallstests zur Attakierung von Systemen zur Suche von Einfallstoren und Sicherheitslücken. Die Entwicklung ging von »Dump-Fuzzing« einfach nur viele Zufallswerte zu »smart Fuzzing« mit »angriffwirksameren« Operationsprofilen. Später taucht der Begriff auch bei der Testauswahl auf, »Dump-Fuzzing« als langer Zufallstets mit typischen Systemeingaben und »Smart-Fuzzing« mit zielgenaueren Operationsprofilen.

Ähnliche Idee, andere Namen.

---

* Symbolische Tests beschreiben, was, wie, warum und wie gründlich zu überprüfen ist.

Zusammenfassung

3.67 Nachweiswahrscheinlichkeit, R-Wachstum

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

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

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

(2.23) $$\zeta_{\mathrm{F}}(N) \overset{(\leq 1)}{=} \frac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

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

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.

3.68 Fehler- und Modellfehlerabdeckung

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

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

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

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

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

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.

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

3.70 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:

$$\mu_{\mathrm{F}.\#\mathrm{OP}}(N) = \mu_{\mathrm{F}}(N_0) \cdot \left(\frac{N}{N_0}\right)^{-\#OP \cdot K} \tag{3.18}$$

$$R_{\mathrm{F}.\#\mathrm{OP}}(N) = R_{\mathrm{F}}(N_0) \cdot \left(\frac{N}{N_0}\right)^{1+\#OP \cdot K} \tag{3.19}$$

Wie weit dieses Potential nutzbar ist, wird die zukünftige Forschung zeigen.

3.71 Testauswahl, Fuzzifizierung

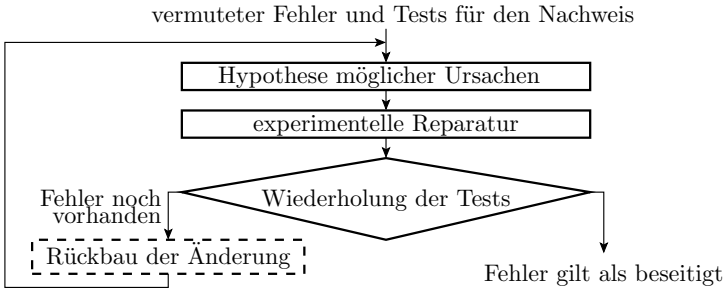
Systeme, die mit unterschiedlichen Opertionsprofilen genutzt werden, sind mit allen Opertionsprofilen der Nutzung und weiteren für den Fehlernachweis günstigen Opertionsprofilen (Grenzwerte) zu testen.

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 Zufallszahlgeneratoren 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.

3 Fehlerbeseitigung

3.72 Experimentelle Reparatur nach Absch. 2.1.1

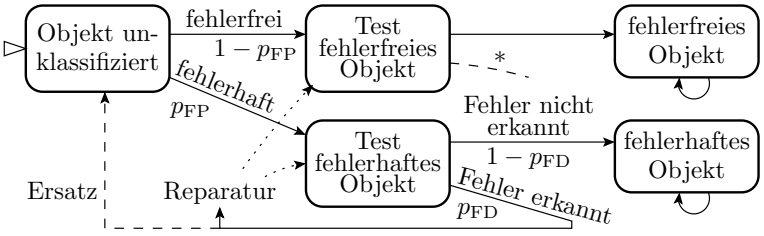


- Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung.
- Beseitigt alle vom Test nachweisbaren Fehler.

- Zur Vermeidung neu entstehender Fehler bei der Reparatur, Rückbau nach erfolglosen Reparaturversuchen.

Voraussetzung: deterministische Fehlerwirkung (Abschn. 2.3.2).

3.73 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.

3.74 Ersatz oder Reparatur

Beim Ersatz erkannter defekter Systeme vor dem Einsatz aus demselben Fertigungsprozess

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

$$\mu_{Repl} = \frac{1}{Y} - 1 \tag{3.20}$$

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

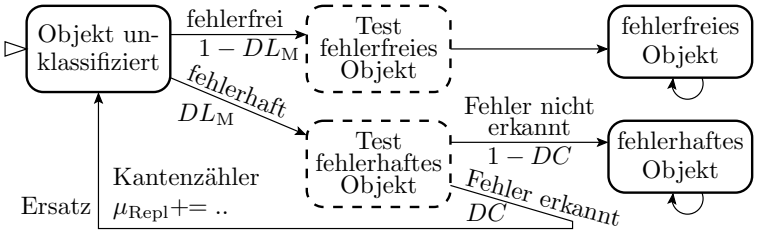
Reparatur: Tausch kleinerer Bausteine, die mit geringerem Risiko defekt sind. Dafür Zusatzaufwand für Lokalisierung, Reparatur, Ersatzteile, ...

Ersatz ist kostengünstigster bei hoher und Reparatur bei geringer Ausbeute.

μ_{Repl} Zu erwartende Anzahl der Ersetzungen.
Y Ausbeute (Yield).

3.1 Ersatz

3.75 Fehlerbeseitigung durch Ersatz



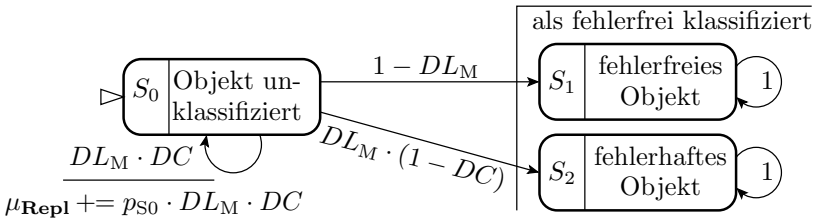
Original- und Ersatzobjekte sind mit Wahrscheinlichkeit DL_M defekt.

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	Defektabdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
μ_{Repl}	Kantenzähler für die zu erwartende Anzahl der Ersetzungen.

3.76 Vereinfachte Markov-Kette



Nach Ersatz aller erkennbar defekten Objekte:

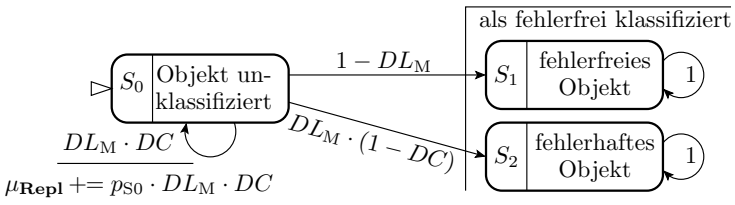
$$\lim_{\#Repl\to\infty}(p_{S0}) = \lim_{\#Repl\to\infty}(DL_M \cdot DC)^{\#Repl} = 0$$

$$\lim_{\#Repl\to\infty}(p_{S1}) = (1 - DL_M) \cdot \sum_{\#Repl=0}^{\infty}(DL_M \cdot DC)^{\#Repl} \overset{(SGS)}{=} \frac{1-DL_M}{1-DL_M \cdot DC}$$

$$\lim_{\#Repl\to\infty}(p_{S2}) = DL = 1 - \lim_{\#Repl\to\infty}(p_{S1}) = \frac{DL_M \cdot (1-DC)}{1-DL_M \cdot DC}$$

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: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.77 Defektanteil



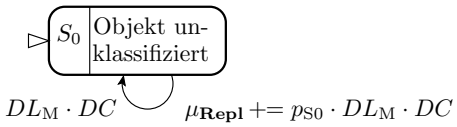
Der Defektanteil nach Aussortieren als Wahrscheinlichkeit, dass ein als fehlerfrei ausgewiesenes Objekt fehlerhaft ist $\lim_{\#Repl\to\infty}(p_{S2})$ wurde in Abschn. 2.1.6 durch Subtraktion der Anzahl der erkannten defekten Produkte von der Anzahl der defekten und aller Produkte in Zähler und Nenner hergeleitet:

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

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.

3.78 Zu erwartende Anzahl der Ersetzungen



$$\mu_{\text{Repl}} = DL\cdot DC\cdot\sum_{n=0}^{\infty}\underbrace{(DL\cdot DC)^n}_{p_{S0}()} = \frac{DL_M\cdot DC}{1-DL_M\cdot DC} \tag{3.21}$$

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

(3.20) $$\mu_{\text{Repl}} = \tfrac{1}{Y} - 1$$
(2.6) $$Y = 1 - DL_M\cdot DC$$

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

Auch hier vorherige Abschätzung aus Abschn. 2.1.6 bestätigt.

Beispiel 3.5 Ausbeute und Defektanteil nach Ersatz

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) $$Y = 1 - DL_M\cdot DC$$

Umstellung nach dem Defektanteil DL_M vor dem Aussortieren der als derfekt 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%

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

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

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

	$DC = 90\%$	$DC = 99\%$	$DC = 99,5\%$	$DC = 99,9\%$
$Y = 10\%$	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

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

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 Defektabdeckungen von $DC \gtrsim 99{,}9\%$.

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

Diese Frage wird uns weiter begleiten.

Y Ausbeute (Yield).
DC Defektabdeckung (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.
100% Für $Y = 1 - DC$ sind alle gefertigten Schaltkreise defekt.
dpm Anzahl der defekten Produkte von einer Million (defecs per million).

3.2 Reparatur

3.80 Fehlerbeseitigung durch Reparatur

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

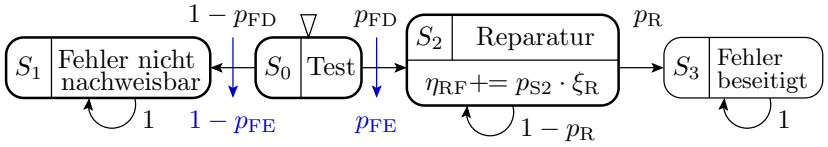
- sind billiger als zu ersetzende Gesamtsysteme und
- haben einen kleineren Defektanteil (weniger Mehrfachersetzungen durch defekte Ersatzteile).

Dafür verlangt Reparatur Zusatzaufwändungen:

- 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.

3.81 Markov-Kette für einen vorhandenen Fehler



Jeder erkannte Fehler wird beseitigt:

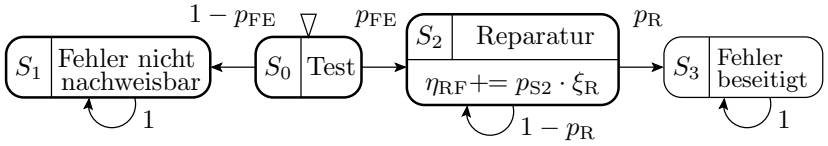
$$p_{FE} = p_{S3} = p_{FD} \cdot p_R + p_{FD} \cdot (1-p_R) \cdot p_R + p_{FD} \cdot (1-p_R)^2 \cdot p_R + \ldots$$

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

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_{Si}	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.
SGS	Summe einer geometrischen Reihe: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.



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

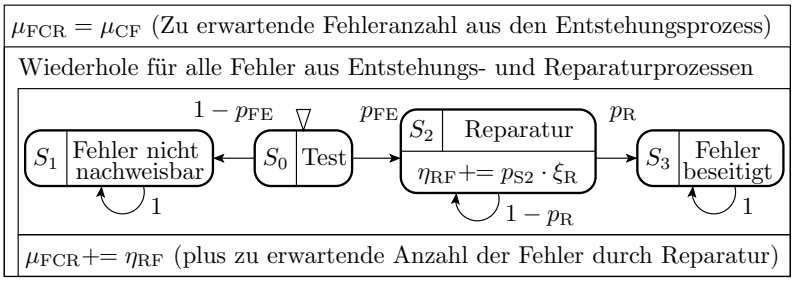
$$\eta_{RF} = p_{FE} \cdot \sum_{n=0}^{\infty} \xi_R \cdot (1-p_R)^n \overset{(SGS)}{=} p_{FE} \cdot \frac{\xi_R}{p_R} \tag{3.22}$$

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

$$\eta_{RE} = \frac{\eta_{RF}}{p_{FE}} = \frac{\xi_R}{p_R} < 1 \tag{3.23}$$

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: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.83 Mehrere zu beseitigende Fehler



- 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:

$$\eta_{\mathrm{RER}} = \eta_{\mathrm{RE}} \cdot (1 + \eta_{\mathrm{RE}} \cdot (1 + \ldots)) = \sum_{i=1}^{\infty} (\eta_{\mathrm{RE}})^i \overset{(\mathrm{SGS})}{=} \tfrac{1}{1-\eta_{\mathrm{RE}}} - 1$$

$$\eta_{\mathrm{RER}} = \tfrac{1}{1-\eta_{\mathrm{RE}}} - 1 = \tfrac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}} \tag{3.24}$$

Neuentstehungsrate je vorhandener ursprünglicher Fehler:

$$\eta_{\mathrm{RFR}} = p_{\mathrm{FE}} \cdot \eta_{\mathrm{RER}} = p_{\mathrm{FE}} \cdot \left(\tfrac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}}\right) \text{ für } \eta_{\mathrm{RE}} < 1 \tag{3.25}$$

Ersatz der Entstehungsrate je vorhandener Fehler in (Gl. 3.25) durch:

(3.23) $$\eta_{\mathrm{RE}} = \tfrac{\eta_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \tfrac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1$$

$$\eta_{\mathrm{RFR}} = p_{\mathrm{FE}} \cdot \left(\tfrac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}-\xi_{\mathrm{R}}}\right) \text{ für } p_{\mathrm{R}} > \xi_{\mathrm{R}} \tag{3.26}$$

Zu erwartende Anzahl der nicht beseitigten Fehler:

$$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + \eta_{\mathrm{RFR}}) \tag{3.27}$$

$$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot \left(1 + p_{\mathrm{FE}} \cdot \left(\tfrac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}}\right)\right) \text{ für } \eta_{\mathrm{RE}} < 1 \tag{3.28}$$

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.

3.85 Fallunterscheidung nach η_{RE} in (Gl. 3.28)

(3.28) $$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot \left(1 + p_{\mathrm{FE}} \cdot \left(\tfrac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}}\right)\right) \text{ für } \eta_{\mathrm{RE}} < 1$$

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

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

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

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

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

  Kontrolle:

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

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: $\frac{1}{2-p_{\mathrm{FE}}} < \eta_{\mathrm{RE}} < 1$
- Mehr neu entstehende als beseitigte Fehler ($\eta_{\mathrm{RE}} \geq 1$): 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 $\eta_{\mathrm{RE}} < 0{,}1$ in neue je beseitigte Fehler

anstreben.

η_{RE} Fehlerentstehungsrate in neue Fehler je beseitigter Fehler.
p_{FE} Fehlernachweis- und Beseitigungswahrscheinlichkeit.

3.87 Gute studentische Programmierleistung

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

Gl. 3.26:	η_{RFR}	$= \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}} - \xi_{\mathrm{R}}}$	$= \frac{0{,}5 \cdot 0{,}1}{0{,}4 - 0{,}1}$	$= 0{,}167$
Gl. 3.27:	μ_{F}	$= \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + \eta_{\mathrm{RFR}})$	$= 5 \cdot (1 - 50\%) \cdot 1{,}167$	$= 2{,}92$
Gl. 2.23:	ζ_{F}	$\overset{(\leq 1)}{=} \frac{K \cdot \mu_{\mathrm{F}}(N)}{N}$	$= \frac{0{,}4 \cdot 2{,}92}{10}$	$= 0{,}11$

- 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.

3.88 Schlechte Programmierleistung

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

Gl. 3.26:	η_{RFR}	$= \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}} - \xi_{\mathrm{R}}}$	$= \frac{0{,}3 \cdot 0{,}2}{0{,}25 - 0{,}2}$	$= 1{,}2$
Gl. 3.27:	μ_{F}	$= \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + \eta_{\mathrm{RFR}})$	$= 7 \cdot (1 - 30\%) \cdot 2{,}2$	$= 10{,}8$
Gl. 2.23:	ζ	$\overset{(\leq 1)}{=} \frac{K \cdot \mu_{\mathrm{F}}(N)}{N}$	$= \frac{0{,}4 \cdot 10{,}8}{5}$	$\to 1$

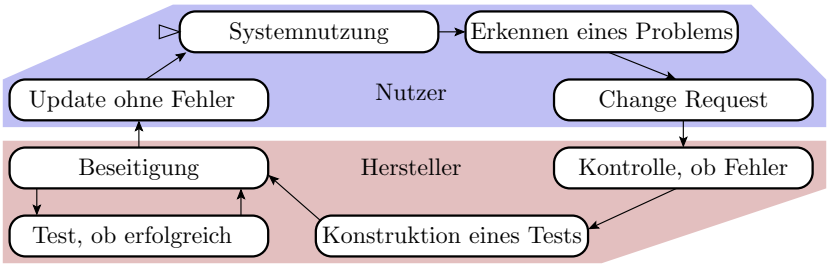
- Im Mittel 4,9 ursprüngliche plus 5,9 bei der Reparatur entstehende nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel liefert garantiert MF.

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.
p_{FE}	Fehlernachweis- und Beseitigungswahrscheinlichkeit.
N	Anzahl der Tests.
p_R	Erfolgswahrscheinlichkeit der Reparatur.
ξ_R	Fehlerentstehungsrate in neue Fehler je Reparaturversuch.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
η_{RF}	Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.

3.3 Reifeprozesse

3.89 Reifen von Produkten (Abschn. 2.2.7)



- Bei einer vermuteten Fehlfunktion stellt der Nutzer eine Änderungsanforderung (Change Request). Alternativ sendet das System einer 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.

3.90 Effektive Testanzahl, Abnahme Fehleranzahl

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

$$N = \underbrace{p_{FE} \cdot \mu_{NU} \cdot \eta_{SU} \cdot t_{VR}}_{N_{MV}} \cdot (u + u_{V0}) \quad \text{mit} \quad u_{V0} = \frac{N_{V0}}{N_{VM}} \tag{2.39}$$

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

$$\mu_F(u) = \mu_F(v) \cdot \left(\frac{u+u_{V0}}{v+u_{V0}}\right)^{-K} \tag{2.41}$$

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 **n**umber of **u**ser).
η_{SU}	Mittlere Anzahl der **S**ervice-Leistungen pro Nutzer (**u**ser) 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 $(0 < K < 1)$.

3.91 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:

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

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

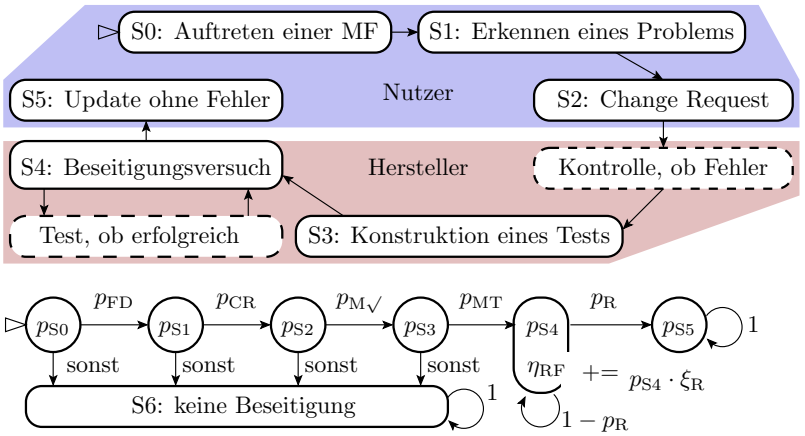
(2.47) $$\frac{S(u)}{S(v)} = \frac{R_{\mathrm{MT}}(u)}{R_{\mathrm{MT}}(v)} = \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{K+1}$$

$R_{[\mathrm{MT}]}$ 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 ($0 < K < 1$).

3.92 Fortsetzung / Modellerweiterung

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

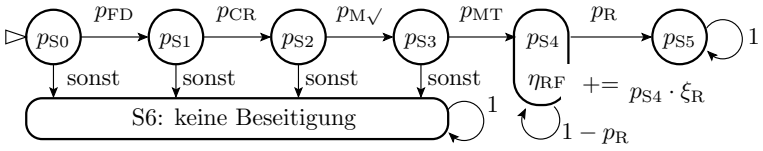
3.93 Reifeprozess als Markov-Kette



---

p_{Si} Wahrscheinlichkeit, dass die Markov-Kette im Zustand S_i ist.
η_{RF} Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.
p_{FD} Fehlernachweiswahrscheinlichkeit (Probability of fault detection).
p_{CR} Wahrscheinlichkeit einer Änderungsanforderung (change request) bei beobachteter MF.
$p_{\mathrm{M}\surd}$ Wahrscheinlichkeit, dass der Hersteller (manufacturer) die MF rekonstruieren kann.
p_{MT} Wahrscheinlichkeit, dass ein Test für den Fehlernachweis gefunden wird.
η_{RF} Fehlerentstehungsrate in neue Fehler je vorhandener Fehler.
p_{R} Erfolgswahrscheinlichkeit der Reparatur.

3.95 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:

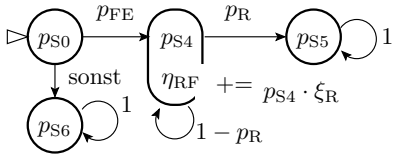
$$p_{\mathrm{FE}} = \lim_{n\to\infty} p_{\mathrm{S5}}(n) = p_{\mathrm{FD}} \cdot p_{\mathrm{CR}} \cdot p_{\mathrm{M}\surd} \cdot p_{\mathrm{MT}} \tag{3.29}$$

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.

3.96 Fehlerentstehungsrate



Dieselbe Markov-Kette wie für die Fehlerbeseitigung durch Reparatur (Abschn. 3.3.2). Neue je vorhandenerer und je beseitigter Fehler:

$$\eta_{\mathrm{RF}} = p_{\mathrm{FE}} \cdot \sum_{n=0}^{\infty} \xi_{\mathrm{R}} \cdot (1 - p_{\mathrm{R}})^n \overset{(\mathrm{SGS})}{=} p_{\mathrm{FE}} \cdot \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} \tag{3.22}$$

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

$$\eta_{\mathrm{RE}} = \frac{\eta_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1 \tag{3.23}$$

Rekursiv unter Berücksichtigung »neuer Fehler durch neue Fehler«

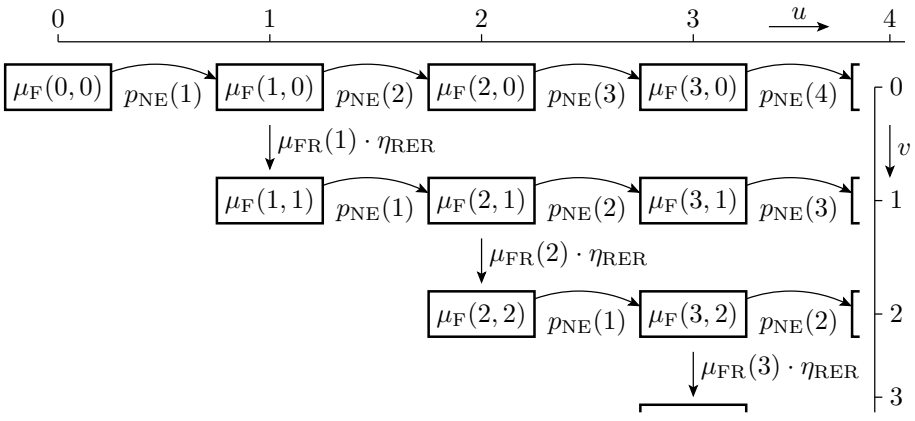
$$\eta_{\mathrm{RER}} = \frac{1}{1-\eta_{\mathrm{RE}}} - 1 = \frac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}} \tag{3.24}$$

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_{RER} Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

3.98 Reifeprozess mit Fehlerneuentstehung



- Version 0 enthält $\mu_{\mathrm{F}}(0,0)$ Fehler. Diese Zahl reduziert sich mit jeder Folgeversionen $u > 0$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{\mathrm{NE}}(u)$ auf $\mu_{\mathrm{F}}(u,0)$.

- In jeder Version $u > 0$ entstehen neue Fehler. Deren zu erwartende Anzahl nimmt mit jeder Folgeversionen $u > v$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{\mathrm{NE}}(u-v)$ ab auf $\mu_{\mathrm{F}}(u,v)$.

3.99 Nichtbeseitigungswahrscheinlichkeit

Für gleichlange Update-Intervalle beträgt die effektive Testanzahl für Fehler in Version u, die in Version v entstanden sind, nach (Gl. 2.39):

$$N(u,v) = N_{\mathrm{VM}} \cdot (u - v + u_{\mathrm{V0}}) \tag{3.30}$$

Die zu erwartende Fehleranzahl aus jeder Version v nimmt mit Version $u \geq v$ seit der Vorversion $u-1$ nach (Gl. 2.41) ab:

$$\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K} \tag{3.31}$$

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

$$p_{\mathrm{NE}}(u-v) = \frac{\mu_{\mathrm{F}}(u,v)}{\mu_{\mathrm{F}}(u-1,v)} = \left(\frac{u-v+u_{\mathrm{V0}}}{u-v-1+u_{\mathrm{V0}}}\right)^{-K} \tag{3.32}$$

$N(u,v)$	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.
$p_{\mathrm{NE}}(u-v)$	Nichtbeseitigungswahrscheinlichkeit für Fehler aus Version v in der Folgeversion von u.
K	Formfaktor der Dichte der Fehlfunktionsrate ($0 < K < 1$).

3.100 Neu entstehende Fehler

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

$$\mu_{\mathrm{FR}}(u) = \sum_{v=0}^{u-1} \left(\mu_{\mathrm{F}}(u-1,v) - \mu_{\mathrm{F}}(u,v)\right) \tag{3.33}$$

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

$$\mu_{\mathrm{F}}(u,u) = \eta_{\mathrm{RER}} \cdot \mu_{\mathrm{FR}}(u) \tag{3.34}$$

η_{RER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

3.101 Zu erwartende Fehleranzahlen insgesamt

$\mu_{\mathrm{F}}(0,0)$ 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:

    (3.31) $\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K}$

- Erwartete Zahl der beseitigten und neu entstehenden Fehler:

  (3.33) $\mu_{\mathrm{FR}}(u) = \sum_{v=0}^{u-1} \left(\mu_{\mathrm{F}}(u-1,v) - \mu_{\mathrm{F}}(u,v)\right)$

  (3.34) $\mu_{\mathrm{F}}(u,u) = \eta_{\mathrm{RER}} \cdot \mu_{\mathrm{FR}}(u)$

- Alle Fehler:

$$\mu_{\mathrm{F}}(u) = \sum_{v=0}^{u} \mu_{\mathrm{F}}(u,v) \tag{3.35}$$

$\mu_{\mathrm{F}}(u,v)$	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.
$\mu_{\mathrm{FE}}(u)$	Erwartete Anzahl der in Version u aus Version $u-1$ beseitigten Fehler.
η_{RER}	Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

3.102 Fehlfunktionsrate durch Fehler

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

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

$$\zeta_{\mathrm{F}}(u) = K \cdot \sum_{v=0}^{u} \frac{\mu_{\mathrm{F}}(u,v)}{N(u,v)} \tag{3.36}$$

$\zeta_{\mathrm{F}}(u)$ 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

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

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

(3.31) $$\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K}$$

(3.33) $$\mu_{\mathrm{FR}}(u) = \sum_{v=0}^{u-1} \left(\mu_{\mathrm{F}}(u-1,v) - \mu_{\mathrm{F}}(u,v)\right)$$

(3.34) $$\mu_{\mathrm{F}}(u,u) = \eta_{\mathrm{RER}} \cdot \mu_{\mathrm{FR}}(u)$$

Tabelle $\mu_{\mathrm{F}}(u,v)$:

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	$2{,}37 \cdot 10^{-1}$
$\mu_{\mathrm{F}}(u)$	100	44,49	33,21	28,18	25,13	22,99

b) *MF-Raten $\zeta_{\mathrm{F}}(u,v)$ einzeln und Summe $\zeta_{\mathrm{F}}(u)$?*

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

(3.36) $$\zeta_{\mathrm{F}}(u) = K \cdot \sum_{v=0}^{u} \frac{\mu_{\mathrm{F}}(u,v)}{N(u,v)}$$

Tabelle $\zeta_{\mathrm{F}}(u,v) = \frac{\mu_{\mathrm{F}}(u,v)}{N(u,v)}$:

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	$9{,}48{\cdot}10^{-7}$
$\zeta_{\mathrm{F}}(u)$	$4{\cdot}10^{-4}$	$3{,}86{\cdot}10^{-5}$	$1{,}15{\cdot}10^{-5}$	$6{,}02{\cdot}10^{-6}$	$3{,}92 \cdot 10^{-6}$	$2{,}83{\cdot}10^{-6}$

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	$4{,}80\cdot10^{-1}$	$3{,}71\cdot10^{-1}$	$3{,}17\cdot10^{-1}$
$v=3$	0	0	0	$5{,}58\cdot10^{-1}$	$2{,}14\cdot10^{-1}$	$1{,}65\cdot10^{-1}$
$v=4$	0	0	0	0	$3{,}40\cdot10^{-1}$	$1{,}30\cdot10^{-1}$
$v=5$	0	0	0	0	0	$2{,}37\cdot10^{-1}$
$\mu_F(u)$	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 enstehende Fehler je beseitigter Fehler.

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	$9{,}48{\cdot}10^{-7}$
$\zeta_F(u)$	$4{\cdot}10^{-4}$	$3{,}86{\cdot}10^{-5}$	$1{,}15{\cdot}10^{-5}$	$6{,}02{\cdot}10^{-6}$	$3{,}92\cdot10^{-6}$	$2{,}83{\cdot}10^{-6}$
$\frac{\zeta_F(u)}{\zeta_F(u,0)}$		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}.

$\mu_F(0,0)$ 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.

$\zeta_F(u,v)$ MF-Rate in Version u verursacht von Fehlern die in Version v entstanden sind.
$\zeta_F(u)$ Gesamte Fehlfunktionsrate in Version u.
$\mu_F(u,0)$ Zu erwartende Fehleranzahl aus Version 0, die in Version u nicht beseitigt sind.
$\zeta_F(u,0)$ MF-Rate in Version u durch Fehlern aus Version 0 (erste freigegebene Version).

Zusammenfassung

3.104 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. 2.1.6):

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

(3.21) $$\mu_{Repl}=DL\cdot DC\cdot\sum_{n=0}^{\infty}\underbrace{(DL\cdot DC)^n}_{p_{S0}()}=\frac{DL_M\cdot DC}{1-DL_M\cdot DC}$$

(3.20) $$\mu_{Repl}=\frac{1}{Y}-1$$

3.105 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:

(3.22) $$\eta_{\mathrm{RF}} = p_{\mathrm{FE}} \cdot \sum_{n=0}^{\infty} \xi_{\mathrm{R}} \cdot (1-p_{\mathrm{R}})^n \overset{(\mathrm{SGS})}{=} p_{\mathrm{FE}} \cdot \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}}$$

- Fehlerentstehungsrate je beseitigter Fehler:

(3.23) $$\eta_{\mathrm{RE}} = \frac{\eta_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1$$

- Fehlerentstehungsrate je beseitigter ursprünglicher Fehler:

(3.24) $$\eta_{\mathrm{RER}} = \frac{1}{1-\eta_{\mathrm{RE}}} - 1 = \frac{\eta_{\mathrm{RE}}}{1-\eta_{\mathrm{RE}}}$$

- Fehlerentstehungsrate je vorhandener ursprünglicher Fehler:

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

Zu erwartende Anzahl der nicht beseitigten Fehler:

(3.27) $$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1-p_{\mathrm{FE}}) \cdot (1+\eta_{\mathrm{RFR}})$$

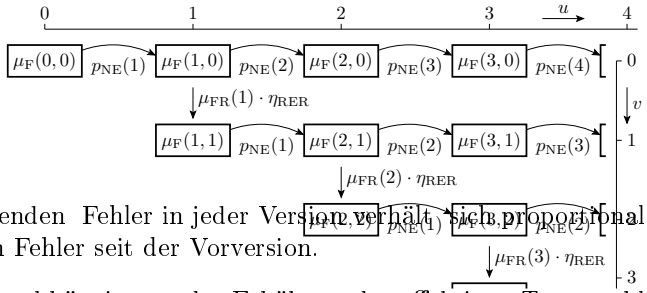
Bei geringer Fehlerentstehungsrate (z.B. $\eta_{\mathrm{RE}} \lesssim 0{,}1$ neuer je beseitigter Fehler) und hoher Fehlererkennungswahrscheinlichkeit p_{FD} erhöht »Reparatur« die Fehleranzahl gegenüber der Anzahl der ursprünglichen nicht erkennbaren Fehler nur prozentual um $p_{\mathrm{FD}} \cdot \eta_{\mathrm{RE}}$.

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

3.107 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.

3.108 Simulation mit Beispielwerten

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

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

Aufgrund der $\leq u_{\mathrm{V0}}$-fachen Reifedauer gegenüber Fehlern früherer Versionen, haben die neuen Fehler die $\geq 1/u_{\mathrm{V0}}$-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_{RER} Fehlerentstehungsrate in neue Fehler je beseitigter ursprünglicher Fehler.

4 Fehlerentstehung

3.109 Erwartete Fehleranzahl (Abschn. 2.3.1)

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

- Programmgröße: $C = 800\,\mathrm{NLOC}$
- Fehlerentstehungsrate: $\xi = 20 \ldots 80\,\frac{\mathrm{F}}{1.000\,\mathrm{NLOC}}$
- 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:

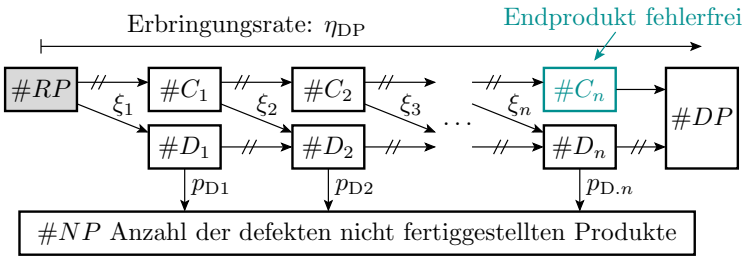
- Modellierung einer linearen Folge von Entstehungsschritten mit einem Zählwertzuordnungsgraphen.
- Modellierung von Phasenmodellen durch Markov-Ketten mit Kantenzählern für die Fehlerentstehung.

μ_{CF} Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.

ξ Fehlerentstehungsrate.

C Metrik für den Entstehungsaufwand oder die Größe des Produkts.

3.110 Entstehungsprozesse mit Kontrollen

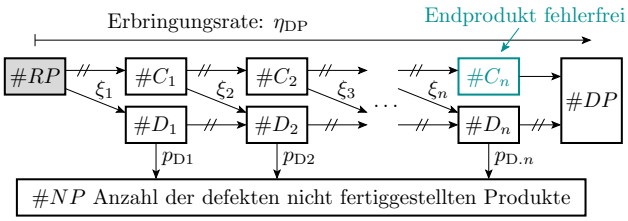


Lineare Folge von Entstehungsschritten. In jedem Schritt

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

$\#\ldots$	Anzahl (Zählwert) der Ereignisse ...
RP	Beauftragung, ein Produkt herzustellen.
C_i, D_i	Schritt 1 bis i korrekt ausgeführt, Produkt nach Schritt i fehlerhaft.
PD, NP	Produkt erzeugt, kein Produkt erzeugt.
ξ_i, $p_{\mathrm{D}.i}$	Fehlerentstehungsrate und Fehlernachweiswahrscheinlichkeit Schritt i.

3.111 Prozesserbringungsrate



Der skizzierte Entstehungsprozess bricht bei erkannten Fehler ab. Erbringungsrate korrekter Produkte:

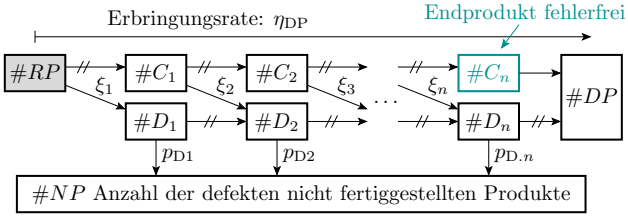
$$\eta_{\mathrm{CP}} = \left.\frac{\#C_n}{\#RP}\right|_{\mathrm{ACR}} = \prod_{i=1}^{n}(1-\xi_i)$$

Erbringungsrate gefertigter fehlerhafter Produkte:

$$\eta_{\mathrm{NDP}} = \xi_1 \cdot \prod_{i=1}^{n}(1-p_{\mathrm{D}.i}) + \sum_{i=1}^{n-1}\left(\prod_{j=1}^{i}(1-\xi_j)\cdot\xi_{i+1}\cdot\prod_{j=i+1}^{n}(1-p_{\mathrm{D}.i})\right) \tag{3.37}$$

η_{DP}	Erbringungsrate fertiger Produkte.
ξ_i, $p_{\mathrm{D}.i}$	Fehlerentstehungsrate und Fehlernachweiswahrscheinlichkeit Schritt i.

Fehleranteil nach der Fertigung



Die Erbringungsrate des Entstehungsprozesses insgesamt:

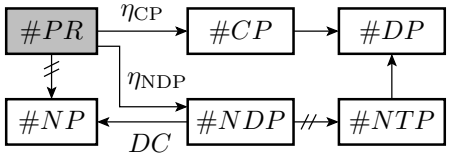
$$\eta_{\mathrm{DP}} = \left.\frac{\#DP}{\#RP}\right|_{\mathrm{ACR}} = \eta_{\mathrm{CP}} + \eta_{\mathrm{NDP}}$$

Fehleranteil der fertiggestellten Produkte:

$$DL_{\mathrm{M}} = \left.\frac{\#NDP}{\#DP}\right|_{\mathrm{ACR}} = \frac{\eta_{\mathrm{NDP}}}{\eta_{\mathrm{CP}}+\eta_{\mathrm{NDP}}}$$

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

Ausbeute und Fehleranteil nach Test



Ein Test mit einer Defektüberdeckung DC reduziert die Erbringungsrate auf die Ausbeute:

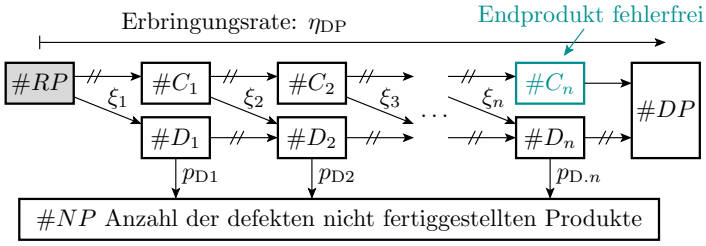
$$Y = \left.\frac{\#DP}{\#PR}\right|_{\mathrm{ACR}} = \eta_{\mathrm{CP}} + (1 - DC) \cdot \eta_{\mathrm{NDP}}$$

und den Defektanteil auf den der ausgelieferten Produkte:

$$DL = \left.\frac{\#NTP}{\#DP}\right|_{\mathrm{ACR}} = \frac{(1-DC)\cdot\eta_{\mathrm{NDP}}}{\eta_{\mathrm{CP}}+(1-DC)\cdot\eta_{\mathrm{NDP}}}$$

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

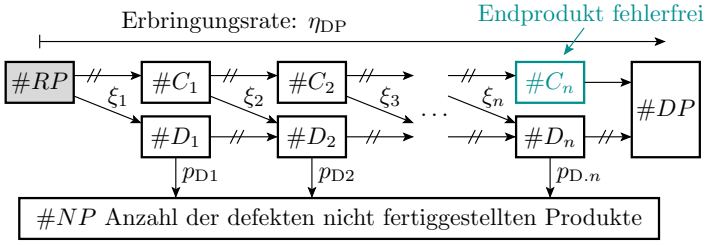
3.113 Fehleranteil



Von den $\#DP$ fertig gestellten Produkten sind $\#C_n$ Produkte fehlerfrei. Fehleranteil als Anteil der fertiggestellten Produkte mit Fehlern (Gl. 2.4):

$$DL_{\mathrm{M}} = 1 - \left.\frac{\#C_n}{\#DP}\right|_{\mathrm{ACR}} = \frac{1 - \prod_{i=1}^{n}(1-\xi_i)}{\eta_{\mathrm{DP}}} \tag{3.38}$$

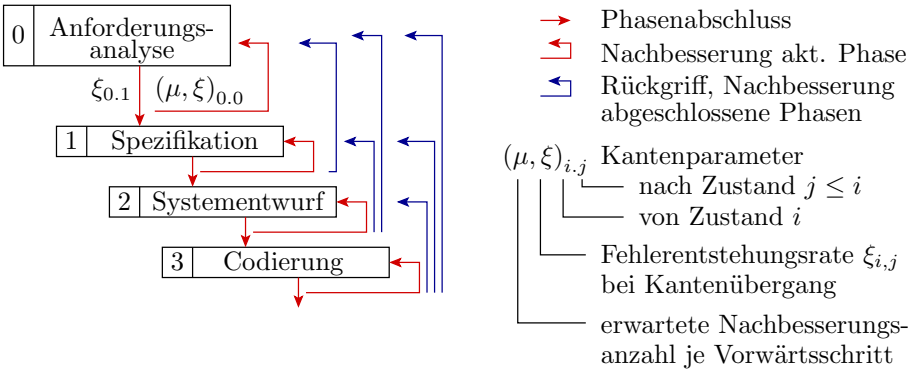
DL_{M}	Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.
ξ_i, $p_{\mathrm{D}.i}$	Fehlerentstehungsrate und Fehlernachweiswahrscheinlichkeit Schritt i.



Ein geringer Fehleranteil fertig gestellter Produkte verlangt geringe Fehlerentstehungsraten und gute Kontrollen. Eine Kontrolle nach jedem Schritt erspart unnütze Arbeit an ohnehin defekten Produkten. Das ist auch ein Grund, Systeme dem Entstehungsfluss folgend, vielen Kontrollen zu unterziehen sind (Abschn. 2.1.4 *Vielfalt der Test*).

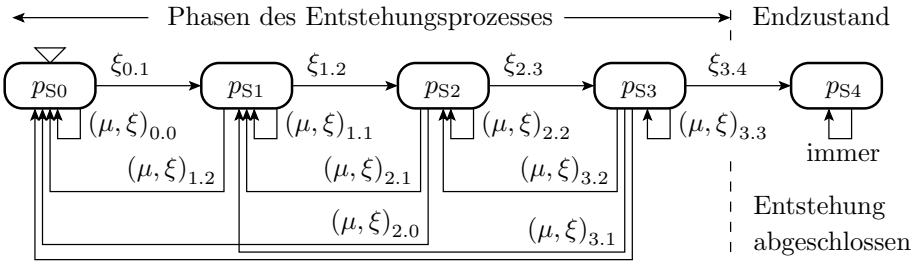
RP	Beauftragung, ein Produkt herzustellen.
C_i, D_i	Schritt 1 bis i korrekt ausgeführt, Produkt nach Schritt i fehlerhaft.
PD, NP	Produkt erzeugt, kein Produkt erzeugt.

3.115 Entstehungsprozesse mit Rückgriffen



- 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.

3.116 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.

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

- 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):

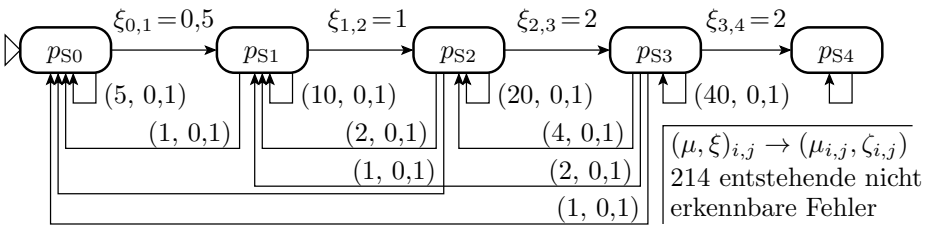
$$p_{i,i+1} = \frac{1}{1+\sum_{j=0}^{i}\mu_{i,j}}$$

- Anzahl der in Simulationsschritt n entstehenden Fehler:

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

$p_{i.j}$ Übergangswahrscheinlichkeit von Phase i nach Phase j.
μ_{FS} Zu erwartende Anzahl aller im aktuellen Simulationsschritt entstehenden Fehler.
$\xi_{i,j}$ Erzeugungsrate nicht erkennbarer Fehler beim Kantenübergang $i \rightarrow j$.
$\#Phs$ Anzahl der abzuarbeitenden Prozessphasen.

3.118 Beispiel



Übergangsmatrix der Markov-Kette und Zunahme der Fehleranzahl:

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

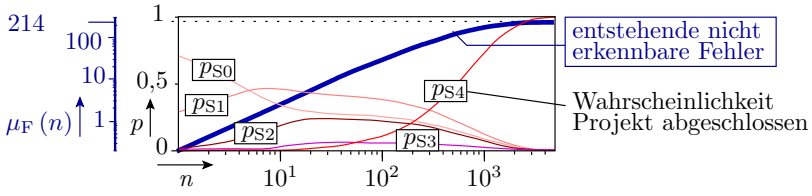
$$\mu_{\mathrm{F}}(n) = \mu_{\mathrm{F}}(n-1) + \mu_{\mathrm{FS}}$$

$p_{\mathrm{S}.i}$ Wahrscheinlichkeit, dass Prozessphase i abgearbeitet wird.
$\mu_{\mathrm{F}}(n)$ Akkumulierte Anzahl aller bis Simulationsschritt n entstehender Fehler.
n Schrittnummer der Simulation der Markov-Kette.

3.119 Ergebnis der Beispielsimulation

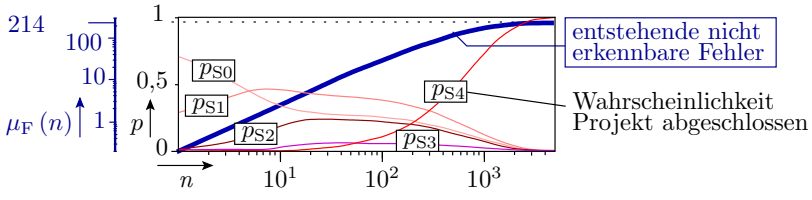
$$\begin{pmatrix} p_{\mathrm{S0}} \\ p_{\mathrm{S1}} \\ p_{\mathrm{S2}} \\ p_{\mathrm{S3}} \\ p_{\mathrm{S4}} \end{pmatrix}_{n+1} = \begin{pmatrix} \frac{5}{6} & \frac{1}{12} & \frac{1}{24} & \frac{1}{48} & 0 \\ \frac{1}{6} & \frac{10}{12} & \frac{2}{24} & \frac{2}{48} & 0 \\ 0 & \frac{1}{12} & \frac{20}{24}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

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



$p_{\mathrm{S}i}$ Wahrscheinlichkeit, dass sich der Entstehungsprozess in Phase i befindet.
$\mu_{\mathrm{F}}(n)$ Akkumulierte Anzahl aller bis Simulationsschritt n entstehender Fehler.
n Schrittnummer der Simulation der Markov-Kette.

3.120 Ergebnis der Beispielsimulation

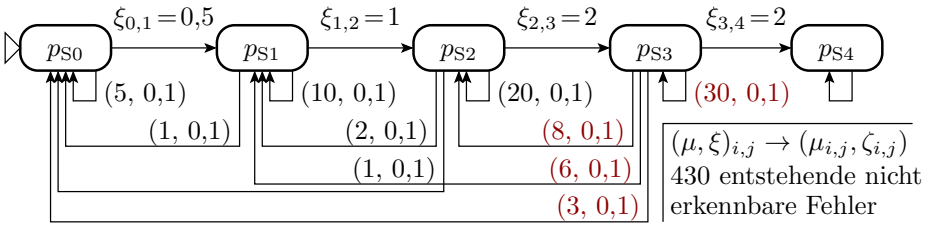


Der zu erwartende Phasenfortschritt und die stetige Zunahme der zu erwartenden Fehleranzahl sind gut zu erkennen.

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.

Die Fehlerentstehungsrate als bedingte Wahrscheinlichkeit für den Übergang in S_4 wenn noch nicht in S_4 scheint recht konstant zu sein und am Ende sind 214 Fehler zu erwarten.

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



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.

3.122 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 parametrierten 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.