Test und Verlässlichkeit Foliensatz 2: Wahrscheinlichkeiten

Prof. G. Kemnitz

May 27, 2020

Contents

Die Zusammenhänge zwischen den Bedrohungen (Fehler, FF, ...), Gegenmaßnahmen (Kontrollen, Tests und den Kenngrößen zur Beschreibung der Verlässlichkeit (Zuverlässigkeit, Verfügbarkeit, Fehleranzahl, ...) werden durch Zufallsgrößen und Wahrscheinlichkeiten beschrieben,

- über die Annahmen zu treffen sind oder
- die aus experimentellen Ergebnissen abgeschätzt werden.

1 Wahrscheinlichkeit

1.1 Definition, Abschätzung

Zufall, Zufallsexperiment, Zufallsvariable

- Zufälliges Ereignis: Ereignis, dass weder sicher noch unmöglich ist, sondern mit einer gewissen Wahrscheinlichkeit eintritt.
- Zufallsexperiment: Experiment mit mehreren möglichen Ergebnissen und zufälligem Ausgang.
- Zufallsvariable: Veränderliche, die ihre Werte in Abhängigkeit vom Zufall nach einer Wahrscheinlichkeitsverteilung annimmt.

Bernoulli-Versuch

Das einfachste Zufallsexperiment. Zweipunktverteilung:

$$\begin{aligned} \mathbb{P}\{X=0\} &= 1-p \\ \mathbb{P}\{X=1\} &= p \end{aligned}$$

(p – Eintrittswahrscheinlichkeit).

Die beiden mögliche Ergebnisse $\{0,1\}$ können auch $\{\text{nein}, \text{ja}\}$, $\{\text{falsch}, \text{wahr}\}$, ... bedeuten.

Zufallsexperimente mit mehr als zwei möglichen Ergebnissen lassen sich in je einen Bernoulli-Versuch je Ergebnis aufspalten:

$$A_i = \begin{cases} 0 & \text{Ereignis nicht eingetreten} \\ 1 & \text{Ereignis eingetreten} \end{cases}$$

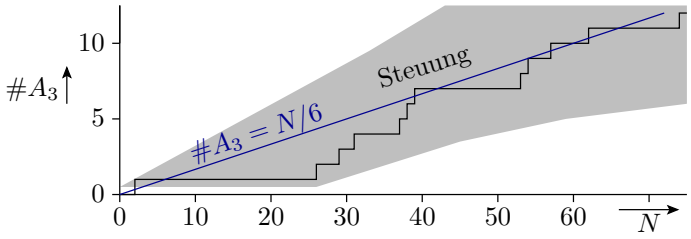
Relative Häufigkeit und Wahrscheinlichkeit

Der Begriff Wahrscheinlichkeit ist aus der Beobachtung und Erfahrung entstanden. Tritt bei N-maliger Durchführung eines Versuches ein bestimmtes zufälliges Ereignis A_i $\#A_i$ mal auf, so bezeichnet man mit $(\#A_i/N)$ die relative Häufigkeit des Ereignisses A_i. Bei gleichbleibenden Versuchsbedingungen schwankt die relative Häufigkeit bei wachsendem N immer weniger um einen bestimmten, praktisch konstanten Wert, die Wahrscheinlichkeit:

$$\mathbb{P}(A_i) = \lim_{N\to\infty} \frac{\#A_i}{N}$$

Beispiel »Würfeln«

- Zufallsexperiment: Würfeln einer 3.
- Mögliche Ergebnisse: 1, 2, ..., 6
- günstiges Ergebnis: 3
- Anzahl der Versuche: N
- Anzahl der Versuche, bei denen eine 3 gewürfelt wird: A_3



$$\mathbb{P}(A_3) = \lim_{N\to\infty} \frac{\#A_3}{N} = \frac{1}{6}$$

1.2 Verkettete Ereignisse

Verkettete Ereignisse

Beschreibung eines Zufallsexperiments durch Teilexperimente mit logischer Ergebnisverknüpfung. 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
$\sum C$	1	1	2	3	3	3	3	3	4	5	6	6	6		11		21
$\sum D$	0	0	0	1	2	2	2	2	2	2	3	3	4		6		9
$\sum E$	0	0	0	1	1	1	1	1	1	1	2	2	2		5		6
$\sum F$	1	1	2	3	4	4	4	4	5	6	7	7	8		13		24

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

Die Wahrscheinlichkeit als Grenzwerte für $N \to \infty$ ergibt sich für jeden Versuch aus dem Verhältnis der günstigen zur Anzahl der möglichen Ergebnisse. Die Würfelexperimente haben 6 mögliche Ergebnisse. Davon sind für die Ereignisse C und D 3 bzw. 2 günstig. Die verketten Ereignisse E und F haben $6^2 = 36$ mögliche Ergebnisse, von denen 6 bzw. 24 günstig sind.

Die Schätzung einer Wahrscheinlichkeit mit weniger als 100 Wiederholungen des Zufallsexperiments ist recht ungenau.

1.3 Bedingte Wahrscheinl.

Bedingte Wahrscheinlichkeit

Bei einer bedingten Wahrscheinlichkeit werden nur die Versuche und Ereignisse gezählt, die die Bedingung erfüllen. Beispiel sei die ODER-Verknüpfung sich ausschließender Ereignisse:

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

																				$\sum$	$\sum$
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 Ergebnisse verringern sich um die vier nicht mitzuzählenden Ergebnisse mit $C \wedge D = 1$. $\Rightarrow$ Geänderte Wahrscheinlichkeit.

Bedingte Wahrscheinlichkeit

Bedingte Wahrscheinlichkeit, dass A unter der Bedingung B eintritt:

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$$

Bedingte Wahrscheinlichkeit, dass B unter der Bedingung A eintritt:

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)}$$

Satz von Bayes:

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

Beispiel: Fehlklassifizierung Corona-Test

- Zufallsgröße A Person infiziert: $\mathbb{P}(A) = 10^{-4}$
- Zufallsgröße B Test positiv: $\mathbb{P}(B) = 10^{-2}$
- Wahrsch. Test positiv, wenn Person infiziert: $\mathbb{P}(B|A) = 99\%$

Mit welcher Wahrsch. Person infiziert, wenn der Test positiv ist?

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

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

Kontrolle mit Beispielzählwerten:

	Test positiv	Test negativ	Summe
infizierte Personen	9.900	100	10.000
nicht infizierte Pers.	≈1 Mio.	99 Mio.	99,99 Mio
Summe	≈1 Mio.	99 Mio.	100 Mio.

- Schätzwerte Wahrsch. Person infiziert und Test positiv:

$$\mathbb{P}(\hat{A}) = \frac{10.000}{1\,\text{Mio.}} \approx 10^{-4} \quad \mathbb{P}(\hat{B}) = \frac{1\,\text{Mio.}}{100\,\text{Mio.}} \approx 1\%$$

- Schätzwert Wahrsch. Test positiv, wenn Person infiziert:

$$\mathbb{P}(\hat{B}|A) = \frac{9.900}{10.000} = 99\%$$

- Schätzwerte Wahrsch. Person infiziert, wenn Test positiv:

$$\mathbb{P}(\hat{A}|B) = \frac{9.900}{1\,\text{Mio.}} \approx 1\%$$

NOT / UND / ODER von Ereignissen

NOT (Nichteintrittswahrscheinlichkeit):

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

UND (gleichzeitiges Eintreten von A und B):

- stochastische Unabhängigkeit:

$$\mathbb{P}(A|B) = \mathbb{P}(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$$
$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B)$$

- sich ausschließende Ereignisse:

$$\mathbb{P}(A \cap B) = 0 \tag{1}$$

ODER (alternatives Eintreten von A und B):

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$$

- stochastische Unabhängigkeit:

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B)$$
$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A) \cdot \mathbb{P}(B)$$

- sich ausschließende Ereignisse:

$$\mathbb{P}(A \cap B) = 0$$
$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$$

Abhängige, sich nicht ausschließende Ereignisse: Ausdruck in UND oder ODER unabhängiger oder sich ausschließender Ereignisse umformen:

$$\begin{aligned}\mathbb{P}(A \oplus B) &= \mathbb{P}\left((A \cap \bar{B}) \cup (\bar{A} \cap B)\right) \\ &= \mathbb{P}\left(A \cap \bar{B}\right) + \mathbb{P}\left(\bar{A} \cap B\right) \quad \text{ausschließend} \\ &= \mathbb{P}(A) \cdot (1 - \mathbb{P}(B)) + (1 - \mathbb{P}(A)) \cdot \mathbb{P}(B)\end{aligned} \tag{2}$$

Beispielaufgabe

In einem System mit drei Fehlern seien diese unabhängig voneinander mit den Wahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$ nachweisbar. Wie groß sind die Wahrscheinlichkeiten der verketten Ereignisse, dass

E_1 : alle Fehler nachweisbar,

E_2 : kein Fehler nachweisbar,

E_3 : mindestens ein Fehler nachwiesbar und

E_4 : genau zwei Fehler nachweisbar?

Hilfestellung:

- Definition von Ereignissen F_i für Fehler i nachweisbar.
- Beschreibung der Ereignisse E_i durch logische Verknüpfungen von Ereignissen F_i bzw. anderer Ereignisse E_i, ...

Lösung

- Alle Fehler nachweisbar:

$$\begin{aligned} E_1 &= F_1 \cap F_2 \cap F_3 \\ \mathbb{P}(E_1) &= \mathbb{P}(F_1) \cdot \mathbb{P}(F_2) \cdot \mathbb{P}(F_3) \\ &= p_1 \cdot p_2 \cdot p_3 = 10\% \cdot 5\% \cdot 20\% = 0{,}1\% \end{aligned}$$

- Kein Fehler nachweisbar:

$$\begin{aligned} E_2 &= \overline{F_1 \cup F_2 \cup F_3} = \bar{F}_1 \cap \bar{F}_2 \cap \bar{F}_3 \\ \mathbb{P}(E_2) &= (1 - \mathbb{P}(F_1)) \cdot (1 - \mathbb{P}(F_2)) \cdot (1 - \mathbb{P}(F_3)) \\ &= (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) = 90\% \cdot 95\% \cdot 80\% = 68{,}4\% \end{aligned}$$

- Mindestens ein (nicht kein) Fehler nachweisbar:

$$\begin{aligned} E_3 &= \bar{E}_2 \\ \mathbb{P}(E_3) &= 1 - \mathbb{P}(E_2) = 1 - 68{,}4\% = 31{,}6\% \end{aligned}$$

- 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 (ausschließendes ODER):

$$\begin{aligned} E_4 &= \left(F_1 \cap F_2 \cap \bar{F}_3\right) \cup \left(\bar{F}_1 \cap F_2 \cap F_3\right) \cup \left(F_1 \cap \bar{F}_2 \cap F_3\right) \\ \mathbb{P}(E_4) &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\ &= 10\% \cdot 5\% \cdot 80\% + 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% = 3{,}2\% \end{aligned}$$

Beispielaufgabe »abhängiger Fehlernachweis«

Wie groß sind die Wahrscheinlichkeiten, dass von zwei Fehlern im System 0, 1 oder 2 Fehler nachweisbar sind, wenn die Nachweiswahrscheinlichkeit für Fehler 1 unabhängig vom Nachweis von Fehler 2 $p_1 = 10\%$ beträgt und für Fehler 2 bei Nachweis von Fehler 1 $p_2 = 20\%$ und sonst 0 beträgt. (Der Nachweis des zweiten Fehler hängt vom Nachweis des ersten ab.)

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

- Kein Fehler ist nachweisbar, wenn der erste Fehler nicht nachweisbar ist[1]:

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

- 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:

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

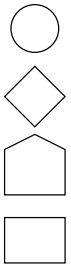
- Probe: Summe der Wahrscheinlichkeiten aller möglichen Ergebnisse muss immer 100% sein:

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

1.4 Fehlerbaumanalyse

Fehlerbaumanalyse (FTA – fault tree analysis)

Verfahren zur Abschätzung der Eintrittswahrscheinlichkeit von Ereignissen in Abhängigkeit vom Eintreten anderer Ereignisse (Gefahrensituationen, Ausfälle, Service-Versagen, ...). Einteilung der Ereignisse:



Ereignis mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit.

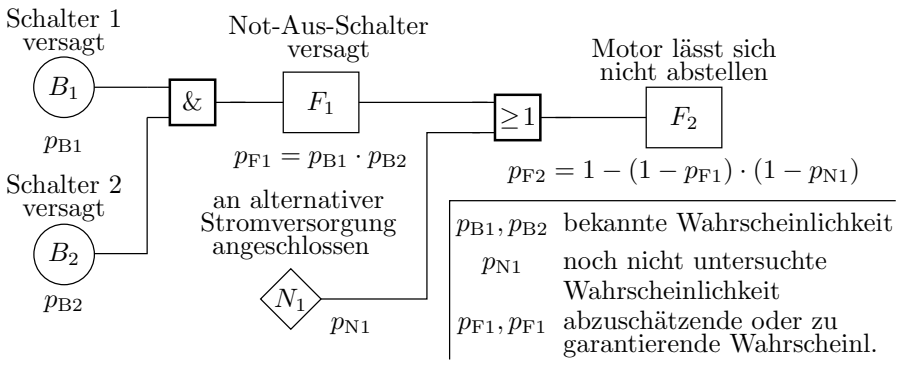
Ereignis, dessen Eintrittswahrscheinlichkeit nicht untersucht wurde.

Ereignis im gewöhnlichen Betrieb, das in Kombination mit anderen Probleme verursachen kann.

Ereignis, dessen Eintrittswahrscheinlichkeit aus denen von ○, ◇ oder ⬠-Ereignissen folgt.

Verknüpfung mit UND, ODER, NICHT.

Beispiel: Motor lässt sich nicht abstellen



[1] Der Fall, Nachweis des zweiten ohne den ersten Fehler ist ausgeschlossen.

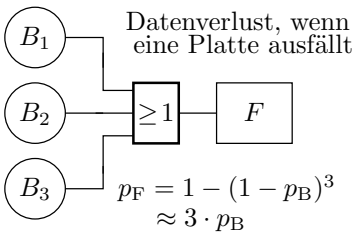
Formulierbare Aufgabe: Wenn $p_{B1} = p_{B2} = 10^{-3}$ ist und $p_{F2} \leq 10^{-6}$ sein darf

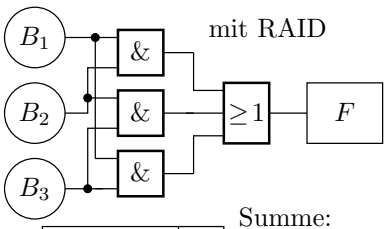
- ist dieses Ziel erreichbar?
- Wie groß darf p_{N1} dann maximal sein?

(Ziel hier nur mit $p_{N1} = 0$ erreichbar. Realistisch/andere Lösung?)

Datenverlust mit RAID

Bei einem RAID 3 tritt nur ein Datenverlust ein, wenn zwei Platten gleichzeitig versagen. Gesucht Wahrscheinlichkeit für Versagen eines Systems mit 3 Festplatten einfach / als Raid 3, wenn alle Platten unabhängig von einander mit derselben Wahrscheinlichkeit p_B versagen.





B_3	B_2	B_1	F	
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:
$p_F = 3 \cdot p_B^2 - 2 \cdot p_B^3$

p_B Wahrscheinlichkeit Plattenversagen
p_F Wahrscheinlichkeit Datenverlust

Rekonvergente Auffächerungen

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

$$F = B_1B_2 \vee B_2B_3 \vee B_1B_3$$

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

Umstellung in Verknüpfung sich ausschließender Ereignisse:

- disjunktive Normalform:

$$\begin{aligned} F &= B_1B_2\bar{B}_3 \vee \bar{B}_1B_2B_3 \vee B_1\bar{B}_2B_3 \vee B_1B_2B_3 \\ p_F &= p_B^2 \cdot (1-p_B) + p_B^2 \cdot (1-p_B) + p_B^2 \cdot (1-p_B) + p_B^3 = 3 \cdot p_B^2 - 2 \cdot p_B^3 \end{aligned}$$

- Alternative Umstellung:

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

Verallgemeinerung auf n Platten

Die Wahrscheinlichkeit, dass mindestens eine von n Platten versagt, ist etwa:

$$p_F \approx n \cdot p_B$$

(p_B – Wahrscheinlichkeit, dass eine Platte versagt). Die Wahrscheinlichkeit, dass mindestens zwei Platten versagen, ist eins abzüglich der Wahrscheinlichkeiten, dass null oder eine Platte versagen:

$$p_F \approx 1 - (1 - p_B)^n - n \cdot p_B \cdot (1 - p_B)^{n-1}$$

Die Anzahl der versagenden Platten ist bei dieser Aufgabenstellung binomialverteilt (siehe Foliensatz 3, Abschnitt »Näherungen für Zählverteilungen, Binomialverteilung«).

Zur 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

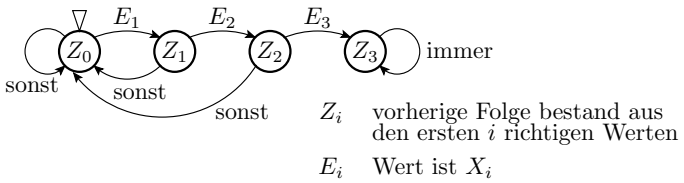
zuvor auf andere Weise abzuschätzen: Vorexperimente, Expertenbefragungen, Ursache-Wirkungs- (Ishikawa-) Diagramme, ...

1.5 Markov-Ketten

Markov-Ketten[2]

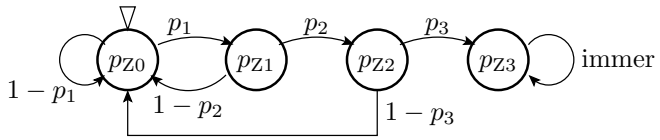
Modellierung eines stochastischen Prozesses durch einen Zustandsautomaten mit Übergangswahrscheinlichkeiten an den Kanten, z.B. zur Bestimmung von Fehlernachweis- und Fehlerbeseitigungswahrscheinlichkeiten.

Fehlernachweis mit einer Eingabefolge $E_1E_2E_3$:



Start im Zustand Z_0 »keine richtige Eingabe« und Verbleib nach drei richtigen Eingaben im Zustand Z_3 »Fehler nachgewiesen«.

Zur Umwandlung in eine Markov-Kette werden die Übergangsbedingungen durch die Übergangswahrscheinlichkeiten p_{E1} bis p_{E3} und die Zustände durch Zustandswahrscheinlichkeiten $p_{\mathrm{Z.i}}$ ersetzt.



Der Anfangszustand hat zu Beginn die Zustandswahrscheinlichkeit $p_{\mathrm{Z0}} = 1$ und die anderen $p_{\mathrm{Z.i}}|_{i\neq 0} = 0$.

[2] Nach Andrej Andreevič Markov, russischer Mathematiker, 1856-1922.

Simulation von Markov-Ketten

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

$$\begin{pmatrix} p_{Z0} \\ p_{Z1} \\ p_{Z2} \\ p_{Z3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_3 & 0 \\ p_1 & 0 & 0 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{Z0} \\ p_{Z1} \\ p_{Z2} \\ p_{Z3} \end{pmatrix}_{n-1}$$

mit $\begin{pmatrix} p_{Z0} & p_{Z1} & p_{Z2} & p_{Z3} \end{pmatrix}^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$.

$$\begin{pmatrix} p_{Z0} \\ p_{Z1} \\ p_{Z2} \\ p_{Z3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_3 & 0 \\ p_1 & 0 & 0 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{Z0} \\ p_{Z1} \\ p_{Z2} \\ p_{Z3} \end{pmatrix}_{n-1}$$

Zur Kontrolle:

- Die Summe der Wahrscheinlichkeiten in jeder Spalte muss eins sein.
- Die Summe der Zustandswahrscheinlichkeiten $p_{Z.i}$ muss in jedem Schritt eins sein.

Simulation mit Octave bzw. Matlab:

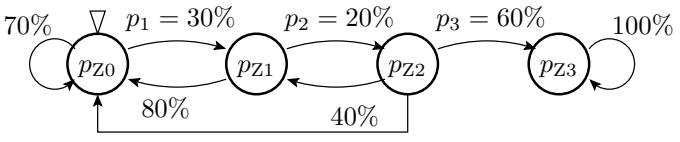
```
p1=...; p2=...; p3=...;

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

for idx=1:100
 Z = M * Z;
 printf('%3i %6.2f%% %6.2f%% %6.2f%% %6.2f%%\n', ...
         idx, 100*Z);

end;
```

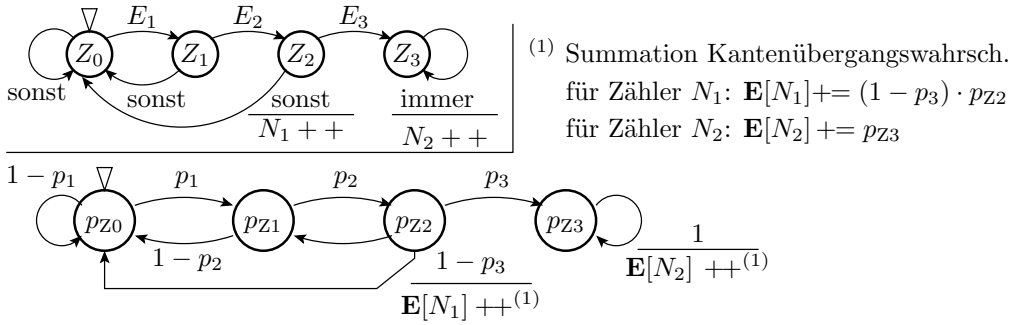
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	p_{Z0}	p_{Z1}	p_{Z2}	p_{Z3}	Summe
0	100,00	0,00	0,00	0,00	100,00
1	70,00	30,00	0,00	0,00	100,00
2	73,00	21,00	6,00	0,00	100,00
3	70,30	21,90	4,20	3,60	100,00
4	68,41	21,09	4,38	6,12	100,00
...	...	...	...	...	...
10	59,43	18,34	3,77	18,46	100,00
...	...	...	...	...	...
50	19,27	5,95	1,22	73,56	100,00
...	...	...	...	...	...
100	4,73	1,46	0,30	93,53	100,00

Kantenkosten

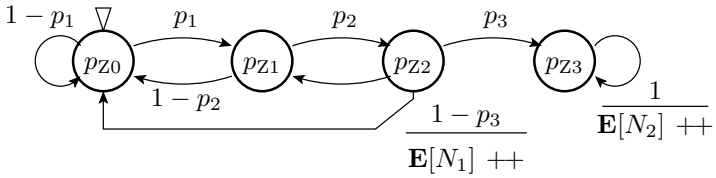
Mit Zählern an den Kanten lässt sich im Automat die Anzahl und in der Markov-Kette die zu erwartende Anzahl der Kantenübergänge, bestimmen:



(1) Summation Kantenübergangswahrsch.
für Zähler N_1: $\mathbf{E}[N_1]\mathrel{+}= (1-p_3)\cdot p_{Z2}$
für Zähler N_2: $\mathbf{E}[N_2]\mathrel{+}= p_{Z3}$

Der Zähler N_1 zählt, wie oft nach zwei richtigen Eingaben eine falsche folgt, der Zähler N_2 die Anzahl der Eingaben im Zustand Z_3 (Fehler nachgewiesen). Die Wahrscheinlichkeiten der Kantenübergange summiert. Die zu erwartende Anzahl der Schritte bis zum Nachweis ist $n - N_2$ (n – Anzahl simulierter Schritte).

Die korrespondierenden Zähler in der Markov-Kette berechnen die Erwartungswerte der Zählgrößen.

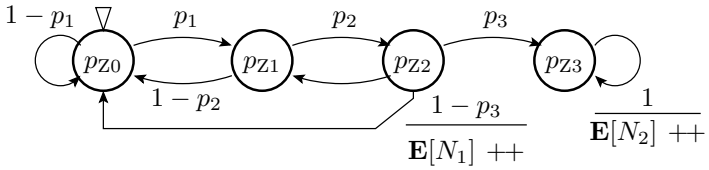


Erweiterung des Simulationsprogramms:

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

for idx=1:100
 Z = M * Z;
 N1 = N1+Z(3)*(1-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;
```

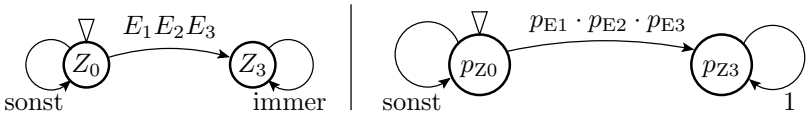
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



n	p_{Z0}	p_{Z1}	p_{Z2}	p_{Z3}	$\mathbf{E}[N_1]$	$\mathbf{E}[N_2]$
1	70,00%	30,00%	0,00%	0,00%	0,00	0,00
2	73,00%	21,00%	6,00%	0,00%	0,02	0,00
3	70,30%	21,90%	4,20%	3,60%	0,04	0,04
4	68,41%	21,09%	4,38%	6,12%	0,06	0,10
...	...	...	...	...	...	...
10	57,78%	17,83%	3,67%	20,73%	0,15	0,99
...	...	...	...	...	...	...
50	18,74%	5,78%	1,19%	74,29%	0,50	22,23
...	...	...	...	...	...	...
100	4,59%	1,42%	0,29%	93,71%	0,63	65,43

Die zu erwartende Anzahl der Schritte bis zum Nachweis $n - N_2$ (n – Anzahl der simulierten Schritte) ist etwa 35.

»Drei richtige Eingaben« als Einzelereignis



Gleichungssystem der modifizierten Markov-Kette:

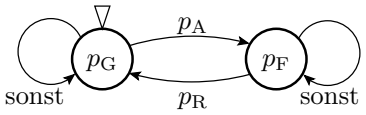
$$\begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_{E1} \cdot p_{E2} \cdot p_{E3} & 0 \\ p_{E1} \cdot p_{E2} \cdot p_{E3} & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{aligned} p_{Z0}(n) &= (1 - p_{E1} \cdot p_{E2} \cdot p_{E3}) \cdot p_{Z0}(n-1) = (1 - p_{E1} \cdot p_{E2} \cdot p_{E3})^n \\ p_{Z3}(n) &= 1 - p_{Z0}(n) = 1 - (1 - p_{E1} \cdot p_{E2} \cdot p_{E3})^n \end{aligned}$$

Wie stark werden $p_{Z0}(n)$ und $p_{Z3}(n)$ von den Ergebnissen der Simulation mit allen vier Zuständen auf den Folien zuvor abweichen?

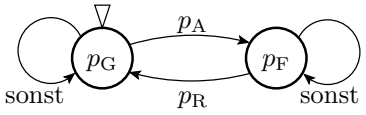
Reparaturprozess als Markov-Kette

Ein System sei zu Beginn funktionsfähig (Zustand G), fällt in jedem Zeitschritt, wenn es ganz ist, mit einer Wahrscheinlichkeit p_A aus (Übergang in Zustand F) und wird, wenn es kaputt ist, mit einer Wahrscheinlichkeit p_R repariert (Übergang in Zustand G):

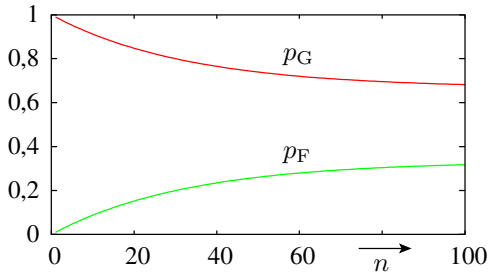


Beschreibung als simulierbares Gleichungssystem:

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



Simulation mit $p_A = 1\%$ und $p_R = 2\%$:

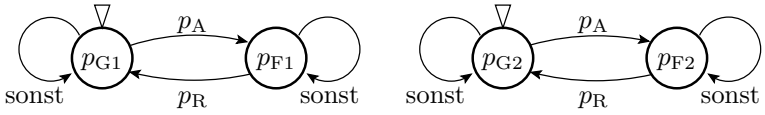


Für große n strebt der Reparaturprozess gegen den stationären Zustand:

$$p_G = \frac{p_R}{p_R + p_A};\ p_F = \frac{p_A}{p_R + p_A}$$

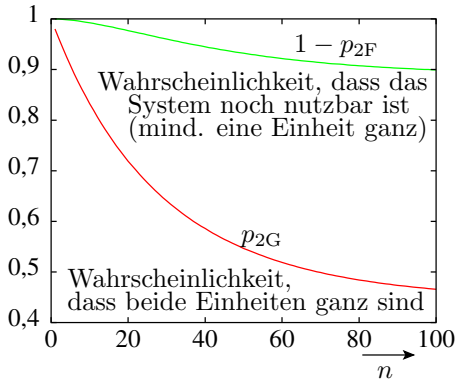
Reparatur mit Redundanz

System aus zwei gleichartigen Teilsystemen, das solange funktioniert, wie ein Teilsystem funktioniert:




```
pA=0.01; pR=0.02;
M=[1-pA  pR; pA  1-pR];
Z=[1; 0];
for n=1:100
  Z = M * Z;
  p2G(n)=Z(1)**2; % beide Einheiten ganz
  p2F(n)=Z(2)**2; % beide Einheiten defekt
end;
plot(1:100, p2G, 1:100, 1-p2F)
```

Simulation mit $p_A = 1\%$ und $p_R = 2\%$:

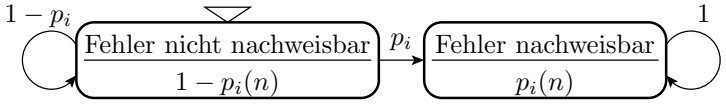


n Anzahl der Simulationsschritte

2 Fehlernachweiswahrscheinlichkeit

2.1 Ohne Gedächtnis

Nachweiswahrscheinlichkeit für Fehler



Ein Fehler i wird nachgewiesen, wenn er eine FF verursacht. Nachweiswahrscheinlichkeit je Service-Anforderung $p_i = \zeta_i \cdot 1\,^{\mathrm{SL}}/_{\mathrm{FF}}$. Mindestens eine FF bei n Service-Anforderungen:

$$1 - p_i\,(n) = (1 - p_i) \cdot (1 - p_i\,(n-1)) = (1 - p_i)^n$$
$$p_i\,(n) = 1 - (1 - p_i)^n$$

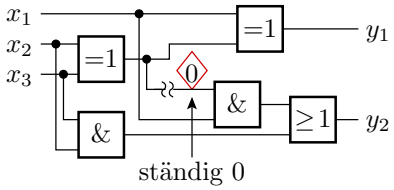
Für kleine $p_i \ll 1$ ist $\ln(1 - p_i) = -p_i$:

$$\boxed{p_i\,(n) = 1\text{-}\mathrm{e}^{-n \cdot p_i}} \tag{3}$$

Die Voraussetzung, dass Fehler i bei allen Service-Anforderungen unabhängig voneinander mit derselben FF-Raten eine FF verursacht, gilt genau genommen nur für ein Service ohne Gedächtnis und fehlerunabhängig ausgewählte Eingabedaten.

Nachweiswahrscheinlichkeit eines Haftfehlers

Die Beispielschaltung enthält einen sa0-Fehler (Gattereingang ständig 0). Nachweis mit zwei der acht Eingabemöglichkeiten. Nachweiswahrscheinlichkeit gleich Summe der Auftrittshäufigkeiten beider Eingaben:



Eingaben die den Fehler nachweisen

Eingabe x_3	x_2	x_1	Ausgabe y_2	y_1	Auftrittshäufigkeit		
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

Nachweiswahrscheinlichkeiten hängen offenbar nicht nur vom Fehler, sondern auch von den Auftrittshäufigkeiten der Eingaben ab.

2.2 Mit Gedächtnis

Service mit Gedächtnis

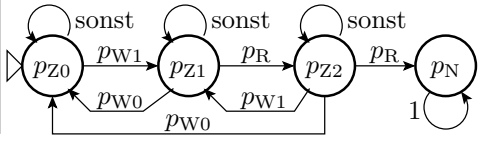
Der Fehlernachweis in einem Service mit Gedächtnis kann auch eine Folgen von mehreren Service-Anforderungen erfordern. Der Nachweis des Fehlertyps »zerstörendes Lesen einer Eins«[3] erfordert z.B.:

- Schreibe 1 auf Adresse a,
- Lese Wert von Adresse a,
- Lese von Adresse a ohne zwischenzeitlichen Schreibzugriff auf a.

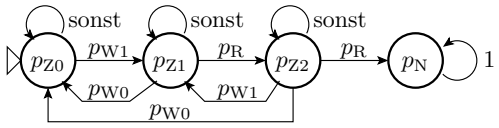
Markov-Kette zur Modellierung des zufälligen Fehlernachweises:

Nachweisfolge: Schreibe 1 → Lesen Lesen

Z0: Wert 0 oder unbekannt
Z1: Wert 1 geschrieben
Z2: 1 zerstörend gelesen
N: Fehler nachgewiesen



[3] Eine 1 in Speicherzelle i wird beim Lesen in eine 0 verändert



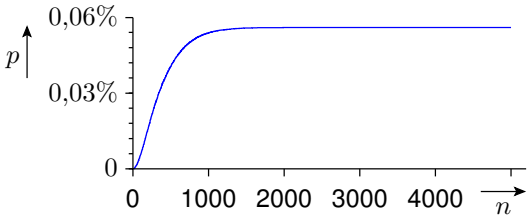
p_{W0}, p_{W1} – Wahrscheinlichkeit, dass in die Speicherzelle eine null bzw. eine eins geschrieben wird; p_R – Wahrscheinlichkeit, dass die Speicherzelle gelesen wird.

```
pZ0=1; pZ1=0; pZ2=0; pN(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW = 1/(4*NA);
for n=1:N
  pZ0     = pZ0 * (1-pW1) + pZ1*pW0          + pZ2*pW0;
  pZ1     = pZ0 *    pW1  + pZ1*(1-pW0-pR) + pZ2*pW1;
  pZ2     = pZ1 *    pR   + pZ2*(1-pW1+pW0-pR);
  pN(n+1) = pN(n) + pZ2 * pR;
  p(n)    = pZ2*pR / (pZ0+pZ1+pZ2); % Nachweisw., wenn noch
end                                 % nicht nachgewiesen
plot(1:N, p);
```

Vermeidung kleiner Differenzen großer Zahlen:

$$p(n) = \frac{p_N(n+1) - p_N(n)}{1 - p_N(n)} = \frac{p_{Z2} \cdot p_R}{p_{Z0} + p_{Z1} + p_{Z2}}$$

FF-Rate in Abhängigkeit von der Testsatzlänge:



Die FF-Rate nimmt anfangs mit der Testsatzlänge zu und bleibt ab $n_K \geq 2000$ konstant $p \approx 0,057\%$.

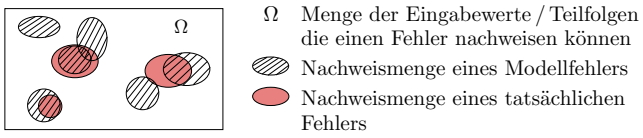
Für lange Zufallstests kann in der Regel auch die FF-Rate eines Fehlers in Systemen mit Gedächtnis wie bei Systemen ohne Gedächtnis als konstant betrachtet und die Nachweiswahrscheinlichkeit über Gl. 3 abgeschätzt werden:

$$1 - e^{-(n-n_K)\cdot p} < p(n) < 1 - e^{-n\cdot p}$$

2.3 Fehler- und Modellfehler

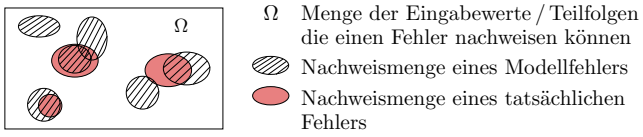
Fehler und Modellfehler

Die zu findenden Fehler sind zum Zeitpunkt der Testauswahl unbekannt. Die Suche von Tests für den Fehlernachweis, die Abschätzung der Fehlerüberdeckung, der FFR-Dichte und der erforderlichen Testsatzlänge erfolgt mit Modellfehlermengen. Ein Fehlermodell generiert für ein Testobjekt eine große Menge von Modellfehlern.



Die meisten tatsächlichen Fehler teilen sich mit mehreren Modellfehlern Nachweisbedigungen und Nachweismengen.

Fehlerorientierte Testauswahl



Bei fehlerorientierter Testauswahl wird für jeden Modellfehler mindestens ein Test gesucht, der ihn nachweist. Ein tatsächlicher Fehler i wird von jedem für einen ähnlich nachweisbaren Modellfehler gefundenen Test j mit einer Wahrscheinlichekit p_{ij} nachgewiesen:

$$p_i = 1 - \prod_{j=1}^{\#j} (1 - p_{ij})$$

($\#j$ – Anzahl der ähnlich nachweisbaren Modellfehler).

Nicht für alle Modellfehler werden Tests gefunden, weil

- sie entweder redundant sind (FF-Rate null) oder
- der Rechenaufwand zu groß ist.

Man findet aber für Modellfehler, für die ein Test gefunden wurde, in der Regel mit dem m-fachen Aufwand m weitere zufällige Tests aus seiner Nachweismenge.

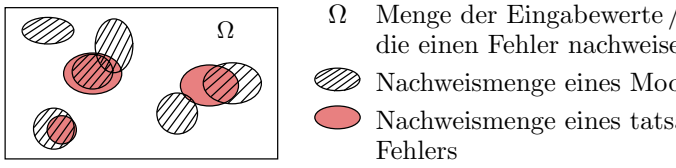
Modellrechnung: Fehler i mit 5 ähnlich nachweisbare Modellfehlern und $p_{ij} = 30\%$. Für FC_{M} der Modellfehler wurden im Mittel m Tests gesucht und gefunden:

$$p_i = 1 - (1 - 30\%)^{5 \cdot FC_{\mathrm{M}} \cdot m} = 1 - 0{,}168^{FC_{\mathrm{M}} \cdot m}$$

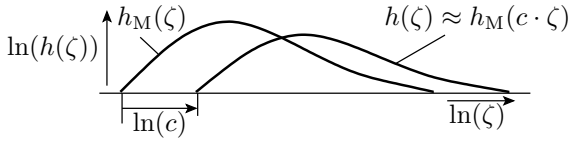
	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$
$FC_{\mathrm{M}} = 90\%$	79,9%	95,9%	99,19%	99,84%	99,97%
$FC_{\mathrm{M}} = 95\%$	81,6%	96,6%	99,38%	99,88%	99,97%

Bei gezielter Testsuche hängt die tatsächliche Fehlerüberdeckung weniger von der Modellfehlerüberdeckung ab, sondern mehr davon, wie viele Tests je Modellfehler gesucht werden, wie viel ähnlich nachweisbare Modellfehler die Fehlermenge enthält und den bedingten Nachweiswahrscheinlichkeiten, dass Modellfehlertests tatsächliche Fehler nachweisen.

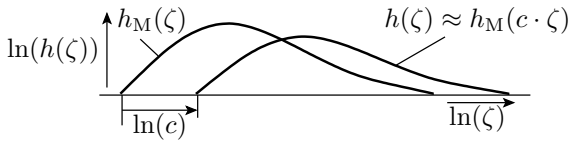
Zufälliger Fehlernachweis



Bei fehlerunabhängiger (zufälliger) Testauswahl sind die Wahrscheinlichkeiten das die Nachweismenge eines Fehlers oder Modellfehlers »getroffen« wird, von der Größer der Nachweismengen und den Wahrscheinlichkeiten, mit denen die einzelen Eingaben ausgewählt werden ab.



Die FF-Dichten der Fehler und Modellfehler sind tendentiell um einen Faktor c zueinander verschoben:



$$h\left(\zeta\right) \sim h_{\mathrm{M}}\left(c \cdot \zeta\right)$$

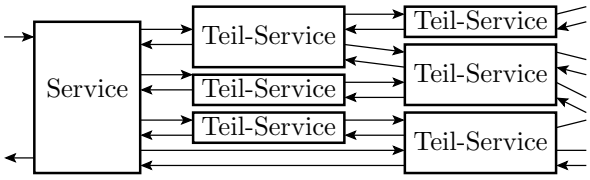
- $c > 1$: Modellfehler schlechter nachweisbar
- $c < 1$: Modellfehler besser nachweisbar.

Die zu erwartende Fehlerüberdeckung ist abschätzungsweise die Modellüberdeckung der c-fachen Testsatzlänge:

$$FC\left(n\right) \approx FC_{\mathrm{M}}\left(c \cdot n\right)$$

2.4 Isolierter Test

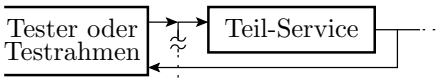
Isolierter Test



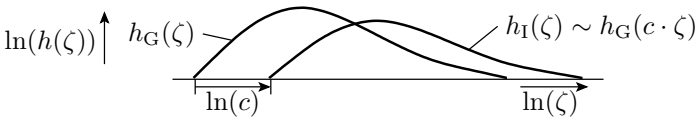
In einem hierarchischen System verursacht ein Fehler in einem Teil-Service nur dann ein Versagen der übergeordneten Service-Leistung, wenn

- die übergeordnete Service-Leistung den Teil-Service nutzt,
- der Fehler dabei lokal nachweisbar ist und
- die lokale Verfälschung am Gesamtergebnis beobachtbar ist.

Der isolierte Test von jedem Teil-Service verringert bei gezielter Suche den Rechenaufwand und beim Zufallstest die erforderliche Testsatzlänge erheblich.



Der Isolierte Test eines Teilsystems verbessert die Wahrscheinlichkeit der Steuer- und Beobachtbarkeit um einen Faktor $c \ll 1$:



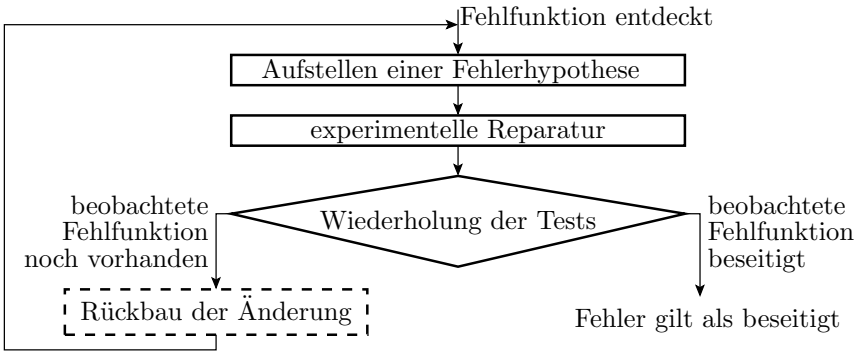
(h_{G} – FFR-Dichte der betrachteten Teil-SL beim eingebetteten Test im Gesamtsystem; h_{I} – FFR-Dichte der betrachteten Teil-SL beimisolierten Test; $c \gg 1$ – Skalierungsfaktor).

Ein isolierter Test der Länge n weist ähnlich viele Fehler in einem betrachteten Systembaustein nach, wie ein $n \cdot c$ langer Test in der Systemumgebung.

3 Fehlerbeseitigungswahrscheinlichkeit

3.1 Markov-Kette

Wiederholung Experimentelle Reparatur

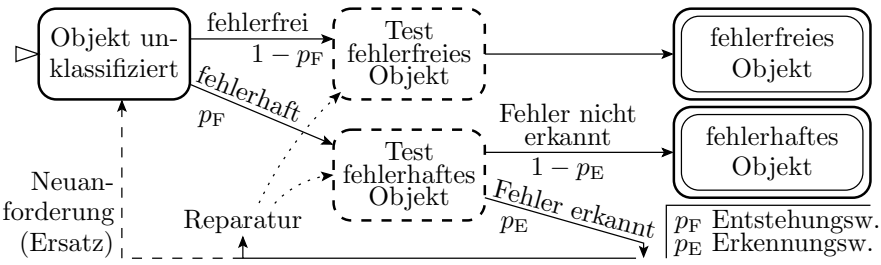


- Deterministische Sollfunktion.
- Der Test weist den Fehler bei jeder Testwiederholung nach.
- Beseitigung durch »intelligentes Probieren«
- Fehlerbeseitigungskontrolle durch Testwiederholung.

Diese Iteration beseitigt jeden erkennbaren Fehler.

- Nicht beseitigt werden nicht erkennbare Entwurf-, Fertigungs- und bei der Reparatur entstehende Fehler.
- Die Fehlerbeseitigungswahrscheinlichkeit hängt hauptsächlich von der Erkennungswahrscheinlichkeit der Tests ab.
- Die Erfolgsrate der Reparaturversuche hat nur mittelbar über die Anzahl der bei der Reparatur entstehenden Fehler Einfluss.
- »Rückbau« mindert die Fehlerentstehung bei der Reparatur.

Experimentelle Reparatur als Markov-Kette



Ein potentieller Fehler i

- entsteht mit einer Wahrscheinlichkeit p_F und
- wird mit einer Wahrscheinlichkeit p_E erkannt.

Für die Fehlerbeseitigung selbst sind zwei Ansätze zu unterscheiden:

- Ersatz des Gesamtsystems (Wiederholung des Entstehungsprozesses) und
- Reparatur, Lokalisierung und Tausch defekter Teilsysteme..

3.2 Ersatz oder Reparatur?

Ersatz vs. Reparatur

Beim Ersatz erkannter defekter Systeme vor dem Einsatz aus demselben Fertigungsprozess

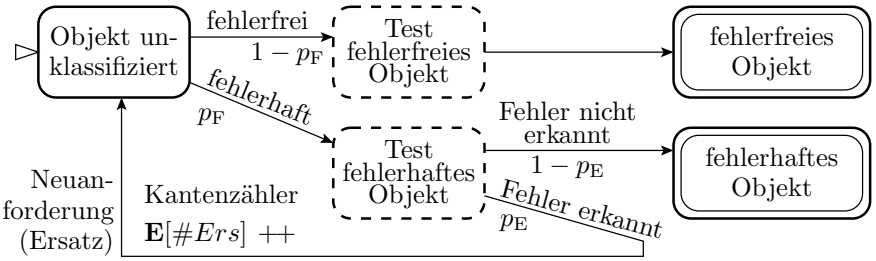
- haben Orginal- und Ersatzsystem dieselbe zu erwartende Ausbeute Y,
- müssen im Mittel $\frac{1}{Y}$ mal so viele Systeme gefertigt oder entworfen, wie am Ende eingesetzt werden.

Aus diesem modellhaften Überschlag leitet sich ab:

- Die Fertigungskosten pro verkauftes System sind $\approx \frac{1}{Y}$ mal so hoch wie die Kosten für die Fertigung eines Systems.
- Ersatz ist die kostengünstigste Fehlerbeseitigung bei hoher Ausbeute[4] und unbezahlbar für Ausbeuten $Y \ll 50\%$.

3.3 Ersatziteration

Experimentelle Reparatur durch Ersatz



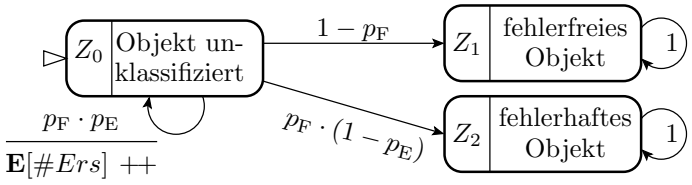
- Ersatzobjekte haben auch mit Wahrscheinlichkeit p_F Fehler.
- Diese entstehen unabhängig und sind unabhängig nachweisbar.

Insgesamt ist das Ergebnis jeder Entstehungsanforderung mit

- $1 - p_F$ ein fehlerfreies Objekt,
- $p_F \cdot (1 - p_E)$ ein nicht erkanntes fehlerhaftes Objekt,
- $p_F \cdot p_E$ eine Wiederhol- (Ersatz-) Anforderung.

$\mathbb{E}[\#Ers]$ ++ Aufsummieren der Kantenübergangswahrscheinlicheiten.

Vereinfachte Markov-Kette



Nach Ersatz aller erkennbar defekten Objekte[5] :

$$\lim_{n\to\infty}(p_{Z0}) = \lim_{n\to\infty}(p_F \cdot p_E)^n = 0$$

$$\lim_{n\to\infty}(p_{Z1}) = (1-p_F)\cdot\sum_{n=0}^{\infty}(p_F \cdot p_E)^n = \frac{1-p_F}{1-p_F \cdot p_E}$$

$$\lim_{n\to\infty}(p_{Z2}) = 1 - \lim_{n\to\infty}(p_{Z1}) = 1 - \frac{1-p_F}{1-p_F \cdot p_E} = \frac{p_F \cdot (1-p_E)}{1-p_F \cdot p_E}$$

[4] Spart Aufwändungen für prüf- und reparaturgerechten Entwurf, Lokalisierung und Vorratshaltung von Reparaturkapazitäten.

[5] Summenformel der geometrischen Reihe: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$

Abschätzbare Kenngrößen

Wahrscheinlichkeit, dass ein als fehlerfrei ausgewiesenes Objekt fehlerhaft ist:

$$p_{\mathrm{FT}} = \lim_{n\to\infty}(p_{\mathrm{Z2}}) = \frac{p_{\mathrm{F}}\cdot(1-p_{\mathrm{E}})}{1-p_{\mathrm{F}}\cdot p_{\mathrm{E}}} \tag{4}$$

Wahrscheinlichkeit, dass der Fehler nicht beseitigt wird[6]:

$$p_{\mathrm{NBes}} = \frac{p_{\mathrm{FT}}}{p_{\mathrm{F}}} = \frac{\frac{p_{\mathrm{F}}\cdot(1-p_{\mathrm{E}})}{1-p_{\mathrm{F}}\cdot p_{\mathrm{E}}}}{p_{\mathrm{F}}} = \frac{1-p_{\mathrm{E}}}{1-p_{\mathrm{F}}\cdot p_{\mathrm{E}}}$$

Die zu erwartende Anzahl der Ersetzungen je als fehlerfrei befundenes Objekt:

$$\mathbb{E}\left[\#Ers\right] \quad = \quad \sum_{n=1}^{\infty}(p_{\mathrm{F}}\cdot p_{\mathrm{E}})^n = \frac{p_{\mathrm{F}}\cdot p_{\mathrm{E}}}{1-p_{\mathrm{F}}\cdot p_{\mathrm{E}}} \tag{5}$$

Zu erwartende Ausbeute[7]:

$$\mathbb{E}\left[Y\right] = \frac{1}{\mathbb{E}\left[\#Ers\right]+1} = 1-p_{\mathrm{F}}\cdot p_{\mathrm{E}} \tag{6}$$

Beispielaufgabe

Wie groß ist für zu die erwartenden Schaltkreisausbeuten von
$\mathbb{E}\left(Y\right) = 10\%$, 30%, 50%, 80% und 90% und eine Fehlererkennungswahrscheinlichkeit von $p_{\mathrm{E}} = 90\%$, 99% und 99,9%

1. die zu erwartende Anzahl der Ersetzungen je als gut befundener Schaltkreis $\mathbb{E}\left[\#Ers\right]$ und
2. die Wahrscheinlichkeit p_{F}, dass ein Schaltkeis vor dem Aussortieren fehlerhaft ist?
3. Wie groß ist die Wahrscheinlichkeit p_{FT}, dass ein als fehlerfrei ausgewiesener Schaltkreis fehlerhaft ist, für $p_{\mathrm{F}} = 100\%$, 90%, 70%, 50%, 20% und 10% und die Werte der Erkennungswahrscheinlichkeit p_{E} oben?

Lösung Aufgabenteile 1 und 2

1. Die zu erwartende Anzahl der Ersetzungen je guter Schaltkreis ist nach Gl. 6:

$$\mathbb{E}\left[\#Ers\right] = \frac{1}{\mathbb{E}\left[Y\right]} - 1$$

Y	10%	30%	50%	80%	90%
$\mathbb{E}\left[\#Ers\right]$	9	2,33	1	0,25	0,11

2. Die Wahrscheinlichkeit p_{F}, dass ein Schaltkeis vor dem Aus- sortieren fehlerhaft ist, beträgt nach Gl. 6:

$$p_{\mathrm{F}} = \frac{1-\mathbb{E}\left[Y\right]}{p_{\mathrm{E}}}$$

p_{E}	$\mathbb{E}\left(Y\right)=10\%$	...=30%	...=50%	...=80%	...=90%
90%	100,0%	77,8%	55,6%	22,2%	11,1%
99%	90,9%	70,7%	50,50%	20,2%	10,1%
99,9%	90,1%	70,1%	50,1%	20,0%	10,0%

[6] Verhältnis des zu erwartenden Fehleranteils DL_{Ers} nach dem Ersatz erkennbar defekten Objekte und DL_{EP} nach Entstehung (vor dem Ersatz).

[7] Die zu erwartende Anzahl der pro funktionierendes System zu fertigenden Systeme ist um eins größer als zu erwartende Anzahl der Ersetzungen und gleich dem Kehrwert der zu erwartenden Ausbeute.

Lösung Aufgabenteil 3

4. Die Wahrscheinlichkeit p_{FT}, dass ein als gut befundenen Schaltkreise nach Ersatz aller erkennbar fehlerhaften Schaltkreise fehlerhaft ist, beträgt nach Gl. 4:

$$p_{\mathrm{FT}} = \frac{p_{\mathrm{F}} \cdot (1 - p_{\mathrm{E}})}{1 - p_{\mathrm{F}} \cdot p_{\mathrm{E}}}$$

	$p_{\mathrm{E}} = 90\%$	$p_{\mathrm{E}} = 99\%$	$p_{\mathrm{E}} = 99{,}9\%$
$p_{\mathrm{F}} = 100\%$	100,0%	100,0%	100,0%
$p_{\mathrm{F}} = 90\%$	47,4%	8,26%	8920 dpm
$p_{\mathrm{F}} = 70\%$	18,9%	2,28%	2328 dpm
$p_{\mathrm{F}} = 50\%$	9,09%	9901 dpm	999 dpm
$p_{\mathrm{F}} = 20\%$	2,43%	2494 dpm	250 dpm
$p_{\mathrm{F}} = 10\%$	1,10%	1110 dpm	111 dpm

3.4 Reparaturiteration

Fehlerbeseitigung durch Reparatur

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

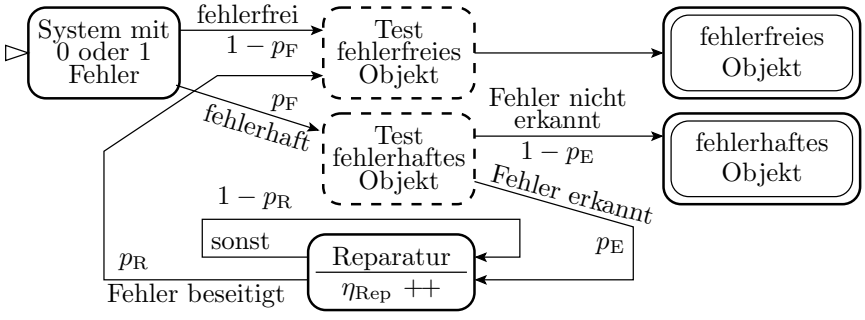
- sind billiger als zu ersetzende Gesamtsysteme und
- haben einen kleinerer Fehleranteil (weniger Mehrfachersetzungen).

Dafür verlangt Reparatur Zusatzaufwändungen:

- Reparaturgerechter Entwurf (modulare Austauschbarkeit),
- Fehlerlokalisierung und
- Organisationseinheiten + Personalkapazität für Reparatur (bei Software für Wartung).

Für Systeme mit Ausbeute $\mathbb{E}[Y] \gg 50$ unrentabel.

Beseitigungsiteration für einen Fehler

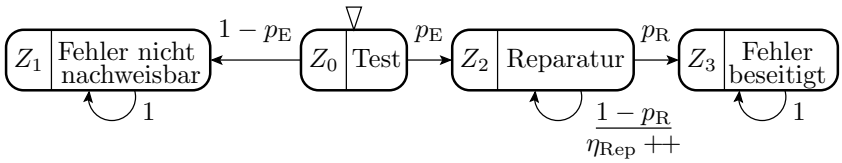


- Bei einem erkennbaren Fehler wird solange mit einer Erfolgswahrscheinlichkeit p_{R} repariert, bis das vom Test nachweisbare Fehlverhalten beseitigt ist.

η_{Rep} ++ Aufsummieren der Zustandswahrscheinlicheiten.

- Bei den Reparaturversuchen können jedoch neue Fehler entstehen, modelliert durch einen Fehlerzähler, der bei jedem Reparaturversuch um die mittlere Anzahl der neu entstehenden Fehler je Reparaturversuch η_{FR} erhöht wird.
- Für den parktisch interessanten Fall $\eta_{\mathrm{FR}} \ll 1$ ist die zu erwartende Anzahl der entstehenden Fehler gleich der Wahrscheinlichkeit, dass ein neuer Fehler entsteht.

Markov-Kette je Fehler



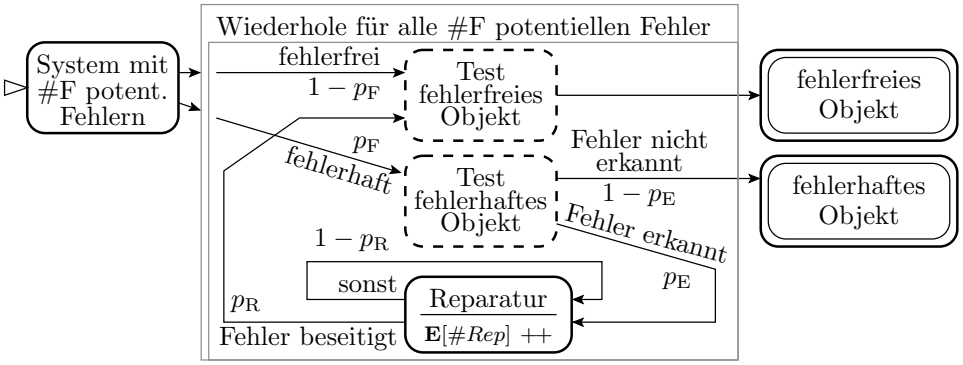
- Wahrscheinlichkeit der Beseitigung eines vorhandenen Fehlers ist gleich der Erkennungswahrscheinlichkeit:

$$p_B = p_{Z3} = p_E \cdot p_R \cdot \sum_{n=0}^{\infty} (1 - p_R)^n = p_E \tag{7}$$

- Zu erwartende Anzahl der neu entstehenden Fehler je vorhandener Fehler beträgt:

$$\eta_{Rep} = p_E \cdot \eta_{FR} = \sum_{n=0}^{\infty} (1 - p_R)^n \cdot \frac{p_E \cdot \eta_{FR}}{p_R} \tag{8}$$

Systeme mit $\#F$ poteniellen Fehlern



- Je eine Markov-Kette für die Beseitigungsiteration eines potentiellen Fehlers.
- Jeder erkannte Fehler wird beseitigt.

Dabei entstehen je ursprünglicher Fehler im Mittel $\eta_{Rep} = \frac{p_E \cdot \eta_{FR}}{p_R}$ neue Fehler, für die in der Beseitigungsiteration wiederum im Mittel η_{Rep} neue Fehler entstehen, ... Anzahl aller entstehenden Fehler:

$$\begin{aligned}\mathbb{E}[\#F_{ges}] &= \mathbb{E}[\#F] \cdot (1 + \eta_{Rep} \cdot (1 - \eta_{Rep}) \cdot \ldots) \\ &= \mathbb{E}[\#F] \cdot \sum_{i=0}^{\infty} (\eta_{Rep})^i = \frac{\mathbb{E}[\#F]}{1 - \eta_{Rep}}\end{aligned}$$

mit $\eta_{Rep} = \frac{p_E \cdot \eta_{FR}}{p_R}$ nach Gl. 8 und $Q_{Rep} = \frac{p_R}{\eta_{FR}}$:

$$\begin{aligned}\mathbb{E}[\#F_{TB}] &= \mathbb{E}[\#F_{ges}] \cdot (1 - p_E) = \frac{\mathbb{E}[\#F] \cdot (1 - p_E)}{1 - \eta_{Rep}} \\ &= \frac{\mathbb{E}[\#F] \cdot (1 - p_E)}{1 - \frac{p_E \cdot \eta_{FR}}{p_R}} = \frac{\mathbb{E}[\#F] \cdot (1 - p_E)}{1 - \frac{p_E}{Q_{Rep}}}\end{aligned}$$

$$\begin{aligned}\mathbb{E}[\#F_{TB}] &= \frac{\mathbb{E}[\#F] \cdot (1 - p_E)}{1 - \frac{p_E}{Q_{Rep}}} \\ \frac{\mathbb{E}[\#F_{TB}]}{\mathbb{E}[\#F]} &= \frac{(1 - p_E)}{1 - \frac{p_E}{Q_{Rep}}}\end{aligned} \tag{9}$$

(p_E – Fehlererkennungswahrscheinlichkeit; η_{FR} – zu erwartende Anzahl der neu entstehenden Fehler je Reparaturversuch; p_R – Erfolgswahrscheinlichkeit der Reparatur; $Q_{Rep} = \frac{p_R}{\eta_{FR}}$ – Reparaturgüte in beseitigte Fehler je neu entstehender Fehler.)

Sonderfälle:

- $\eta_{\mathrm{Rep}} = \frac{p_{\mathrm{E}}}{Q_{\mathrm{Rep}}} > 1$: Es entstehen mehr Fehler als beseitigt werden. Gl. 8 hat keine Summe. Die Fehleranzahl strebt gegen unendlich.
- $p_{\mathrm{E}} < Q_{\mathrm{Rep}} \leq 1$: Die Anzahl der erkennbaren Fehler nimmt ab, aber die tatsächliche Fehleranzahl nimmt zu oder bleibt konstant. Die Fehler werden »vor dem Testsatz versteckt«.
- $Q_{\mathrm{Rep}} \gg 1$: Bei der Fehlerbeseitigung entsteht kein signifikanter nicht erkennbarer neuer Fehler.

Typische studentische Programmierarbeiten

1. Wenige Testbeispiele, brauchbarer Reparaturprozess, z.B. $p_{\mathrm{E}} = 30\%$ erkennbare Fehler, $Q_{\mathrm{Rep}} = 2$ beseitigte Fehler je neu entstehender Fehler. Verringerungsfaktor der Fehleranzahl:

$$\frac{\mathbb{E}\left[\#F_{\mathrm{TB}}\right]}{\mathbb{E}\left[\#F\right]} = \frac{(1-30\%)}{1-\frac{30\%}{2}} = \left(1+\frac{30\%}{2,5}\right)\cdot(1-30\%) = 82{,}4\%$$

   Es werden 30% der ursprünglichen Fehler beseitigt. Vergrößerung $\mathbb{E}\left[\#F_{\mathrm{TB}}\right]$ gegenüber einem idealen Reparaturprozess mit $Q_{\mathrm{Rep}} \to \infty$ ${}^{82{,}4\%}/_{70\%} = 1{,}18$.

2. Weniger Testbeispiele, grenzwertiger Reparaturprozess, z.B. $p_{\mathrm{E}} = 25\%$ erkennbare Fehler, $Q_{\mathrm{Rep}} = 0,5$ beseitigte Fehler je je neu entstehender Fehler. Vergrößerungsfaktor der Fehleranzahl:

$$\frac{\mathbb{E}\left[\#F_{\mathrm{TB}}\right]}{\mathbb{E}\left[\#F\right]} = \frac{(1-25\%)}{1-\frac{25\%}{0,5}} = 150\%$$

   Es werden 25% der ursprünglichen Fehler beseitigt. Vergrößerung $\mathbb{E}\left[\#F_{\mathrm{TB}}\right]$ gegenüber einem idealen Reparaturprozess ${}^{150\%}/_{75\%} = 2$.

Erkannt und beseitigt werden die am meisten störenden Fehler (siehe Zufallstest).

Auch wenn nur wenige Tests erfolgreich durchlaufen, bestehen Chancen, dass das System einen Abnahmetest mit 1 bis 2 neuen zufälligen Testbeispielen passiert.

Während im 1. Beispiel der Reparaturprozess die Anzahl der nicht beseitigten Fehler und damit auch die FF-Rate im Einsatz nur um 18% erhöht, verdoppelt der schlechtere 2. Reparaturprozess die Anzahl der nicht beseitigten Fehler und die FF-Rate durch Fehler im Einsatz.

Wegen der tendentiell mehr als doppelt so großen FF-Rate sind die Chancen, dass ein zufälliger Abnahmetest erfolgreich passiert wird, weniger als halb so groß wie im ersten Beispiel.

Als Studienleistung ok.. Für den praktischen Einsatz sind Programme aus unausgereiften Entstehungs- und Reparaturprozessen zu unzuverlässig.

Zufallstest mit Fehlerbesitigungsiteration

Für einen Zufallstest gilt nach Foliensatz 1, Abschn. »Test und Zuverlässigkeit« für den Anteil der nicht beseitigten Fehler und damit auch für die Nichterkennungswahrscheinlichkeit:

$$1 - FC\,(n) = 1 - p_{\mathrm{E}} = \left(\frac{n}{n_0}\right)^{-k} \quad \text{mit } 0 < k < 1 \tag{10}$$

Eingesetzt in Gl. 9 für Anzahl der Fehler nach der Fehlerbeseitigung in einem nicht idealen Reparaturprozess:

$$\mathbb{E}\left[\#F_{\mathrm{TB}}\right] = \frac{\mathbb{E}\left[\#F\right]\cdot(1-p_{\mathrm{E}})}{1-\frac{p_{\mathrm{E}}}{Q_{\mathrm{Rep}}}} = \frac{\mathbb{E}\left[\#F\right]\cdot\left(\frac{n}{n_0}\right)^{-k}}{1-\frac{1-\left(\frac{n}{n_0}\right)^{-k}}{Q_{\mathrm{Rep}}}} \leq \frac{\mathbb{E}\left[\#F\right]\cdot\left(\frac{n}{n_0}\right)^{-k}}{1-Q_{\mathrm{Rep}}^{-1}} \tag{11}$$

Für $n \gg n_0$ und $Q_{\mathrm{Rep}} > 1$ erhöht ein nicht idealer Reparaturprozess die Fehleranzahl nach der Beseitigungsiteration maximal um den Faktor:

$$\mathbb{E}\left[\#F_{\mathrm{TB}}\right] \leq \frac{1}{1-Q_{\mathrm{Rep}}^{-1}} \cdot \mathbb{E}\left[\#F_{\mathrm{TB}}|_{Q_{\mathrm{Rep}}\to\infty}\right]$$

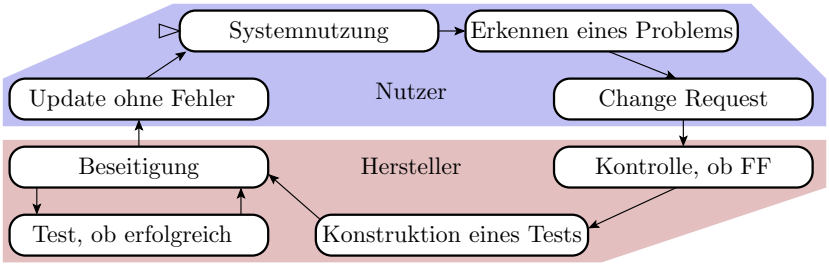
Um denselben Faktor erhöht sich die FF-Rate durch nicht beseitigten

$$\zeta_{\mathrm{F}} = \frac{k}{k+1} \cdot \frac{\mathbb{E}\left[\#F_{\mathrm{TB}}\right]}{n} \left[\cdot \frac{\mathrm{FF}}{\mathrm{F} \cdot \mathrm{SL}}\right]$$
$$\leq \frac{1}{1-Q_{\mathrm{Rep}}^{-1}} \cdot \frac{k}{k+1} \cdot \frac{\mathbb{E}\left[\#F_{\mathrm{TB}}|_{Q_{\mathrm{Rep}}\to\infty}\right]}{n} \left[\cdot \frac{\mathrm{FF}}{\mathrm{F} \cdot \mathrm{SL}}\right]$$

(n – Testsatzlänge; n_0 – Mindesttestsatzlänge, ab der die Abschätzung gilt; $\left[\cdot\frac{\mathrm{FF}}{\mathrm{F}\cdot\mathrm{SL}}\right]$ – Korrekturterm, damit die Maßeinheit stimmt).

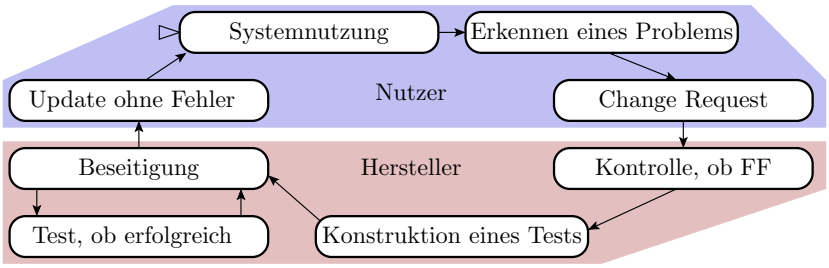
4 Fehlerbeseitigungswahrscheinlichkeitin Reifeprozessen

Beseitigung in einem Reifeprozess (Wiederholung)



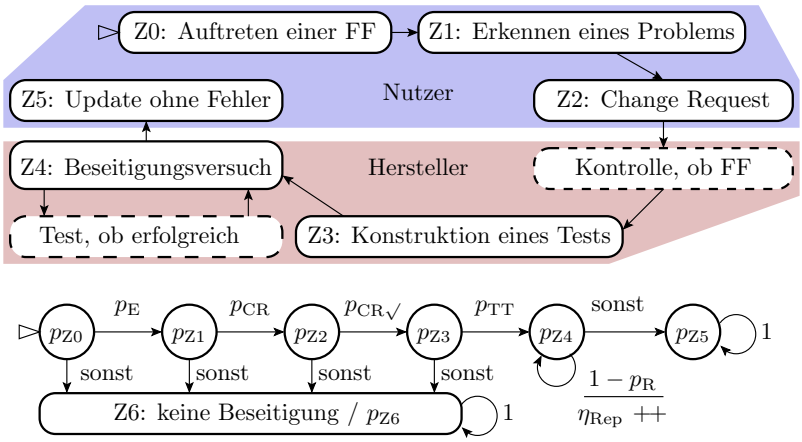
Fehlerbeseitigungsiteration für von Anwendern beobachtete FF:

- Erfassen der FF mit allen Daten, um die FF nachzustellen,
- Übermittlung an den Hersteller,
- Priorisierung, Fehlersuche und Beseitigung,
- Herausgabe und Einspielung von Updates.

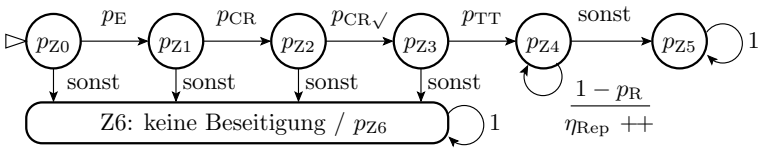


- Bei einer vermuteten Fehlfunktion stellt der Nutzer einen Änderungsanforderung (Change Request).
- Der Hersteller prüft diese, selektiert daraus FFs und versucht, für jede FF reproduzierbare Testbeispiele zu finden.
- Die Testbeispiele dienen zur Fehlerlokalisierung und zur Erfolgskontrolle nach jedem Beseitigungsversuch.
- Fehlerbeseitigung beim Nutzer erfolgt über Einspielen von Updates, in seltenen Ausnahmen über eine Rückrufaktion für Hardware oder komplette Geräte.

Modellierung als Markov-Kette



η_{Rep} ++ Aufsummieren der Übergangswahrscheinlicheiten.



Wahrscheinlichkeiten:

- p_{E}: Erkennungswahrscheinlichkeit je SL, Zufallstest
- p_{CR}: Änderungsanforderung wird gestellt
- $p_{\mathrm{CR}\surd}$: Hersteller kann die Fehlersituation nachstellen
- p_{TT}: Hersteller findet Test für den Fehlernachweis
- p_{R}: Reparaturversuch beseitigt Fehler.

Beseitigungswahrscheinlichkeit des zugrunde liegenden Fehlers für eine beim Anwender beobachtete FF:

$$p_{\mathrm{B}} = p_{\mathrm{E}} \cdot p_{\mathrm{CR}} \cdot p_{\mathrm{CR}\surd} \cdot p_{\mathrm{TT}}$$

Zu erwartende Anzahl der der neu entstehenden Fehler je vorhandener Fehler analog zu Gl. 8:

$$\eta_{\mathrm{Rep}} = p_{\mathrm{B}} \cdot \eta_{\mathrm{FR}} \cdot \sum_{n=0}^{\infty} (1-p_{\mathrm{R}})^n = \frac{p_{\mathrm{B}} \cdot \eta_{\mathrm{FR}}}{p_{\mathrm{R}}}$$

Von der Erkennungswahrsch. unter Testbedingungen nach Gl. 10

$$1 - p_{\mathrm{E}} = \left(\frac{n}{n_0}\right)^{-k} \quad \text{mit } 0 < k < 1$$

zur Beseitigungswahrscheinlichkeit in einem Reifeprozess:

- Die Beseitigingswahrscheinlichkeit, ist die Erkennungswahrscheinlichkeit unter der Bedingung, eine Änderungsanforderung gestellt wird, ...
- Berücksichtigbar, in dem nur ein Anteil von $p_{\mathrm{CR}} \cdot p_{\mathrm{CR}\surd} \cdot p_{\mathrm{TT}}$ von SL als Beitrag zum Reifeprozess gezählt wird:

$$1 - p_{\mathrm{B}} = \left(\frac{p_{\mathrm{CR}} \cdot p_{\mathrm{CR}\surd} \cdot p_{\mathrm{TT}} \cdot n}{n_0}\right)^{-k} \quad \text{mit } 0 < k < 1$$

Anzahl der nicht beseitigten Fehler in Anlehnung an Gl. 9:

$$\mathbb{E}\left[\#F_{\mathrm{RP}}\right] \leq \frac{\mathbb{E}\left[\#F_{\mathrm{TB}}\right]}{1-Q_{\mathrm{Rep}}^{-1}} \cdot \left(\frac{p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}} \cdot n}{n_0}\right)^{-k}$$

Die FF-Rate ist proportional zur Anzahl der nicht beseitigten Fehler und umgekehrt proportional zur gesamten effektiven Testsatzlänge:

$$\zeta_{\mathrm{F}} = \frac{k}{k+1} \cdot \frac{\mathbb{E}\left[\#F_{\mathrm{Rep}}\right]}{n_0 + p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}} \cdot n} \left[\cdot \frac{\mathrm{FF}}{\mathrm{F} \cdot \mathrm{SL}}\right]$$

($\#F_{\mathrm{TB}}$ – Anzahl der nicht beseitigten Fehler nach Test und Fehlerbeseitigung vor dem Einsatz; n_0 – Anzahl der Tests vor dem Einsatz; Q_{Rep} – Reparaturgüte in beseitigten Fehlern je neu entstehender Fehler im Reifeprozess; $p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}}$ – Wahrscheinlichkeit, dass bei einer FF bei einem Anwender beim Hersteller eine Änderungsanforderung eingeht und es dem Hersteller gelingt, für die beobachtet FF einen Test zu finden, mit der sich die FF reproduzierbar anregen lässt.

$$\zeta_{\mathrm{F}} = \frac{k}{k+1} \cdot \frac{\mathbb{E}\left[\#F_{\mathrm{Rep}}\right]}{n_0 + p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}} \cdot n} \left[\cdot \frac{\mathrm{FF}}{\mathrm{F} \cdot \mathrm{SL}}\right] \tag{12}$$

- Das Produkt $p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}}$ lässt sich groß halten, wenn das System seine FF selbst erkennt und an den Hersteller alle Daten für die Aufstellung eines Tests für den zugrundeliegenden Fehler übermittelt.
- Die Testanzahl n ist die Anzahl alle genutzten SL bei allen Anwendern von denen beobachtete FF an den Hersteller übermittet werden. Potentiell um viele Zehnerpotenzen größer als die Anzahl der Herstellertests.
- Die FF-Rate durch Fehler lassen sich so auf um Zehnerpotenzen niedrigere Werte absenken als durch Herstellertests allein.
- Gl. 12 enthält Ungenauigkeiten. Die durch Beseitigungsiterationen neu entstehenden Fehler waren nicht der kompletten effektiven Testsatzlänge von $n_0 + p_{\mathrm{CR}} \cdot p_{\mathrm{CR}_{\surd}} \cdot p_{\mathrm{TT}} \cdot n$ ausgesetzt und haben entsprechend eine höhere zu erwartenen FF-Rate als die nicht beseitigten Fehler aus dem Herstellungsprozess, ...