Test und Verlässlichkeit Foliensatz 2: Wahrscheinlichkeiten

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F2)

May 30, 2022

Inhalt Foliensatz TV_F2 Wahrscheinlichkeiten

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

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

Wahrscheinlichkeit

Definition, Abschätzung

Zufall, Zufallsexperiment, Zufallsvariable

- Zufälliges Ereignis: Ereignis, das 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 {nein, ja}, {falsch, 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

Tritt bei N-maliger Durchführung eines Versuches ein bestimmtes zufälliges Ereignis A_i $\#A_i$ mal auf, so bezeichnet $(\#A_i/N)$ die relative Häufigkeit des Ereignisses A_i. Bei gleichbleibenden Versuchsbedingungen schwankt die relative Häufigkeit bei wachsendem N immer weniger um die Wahrscheinlichkeit:

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

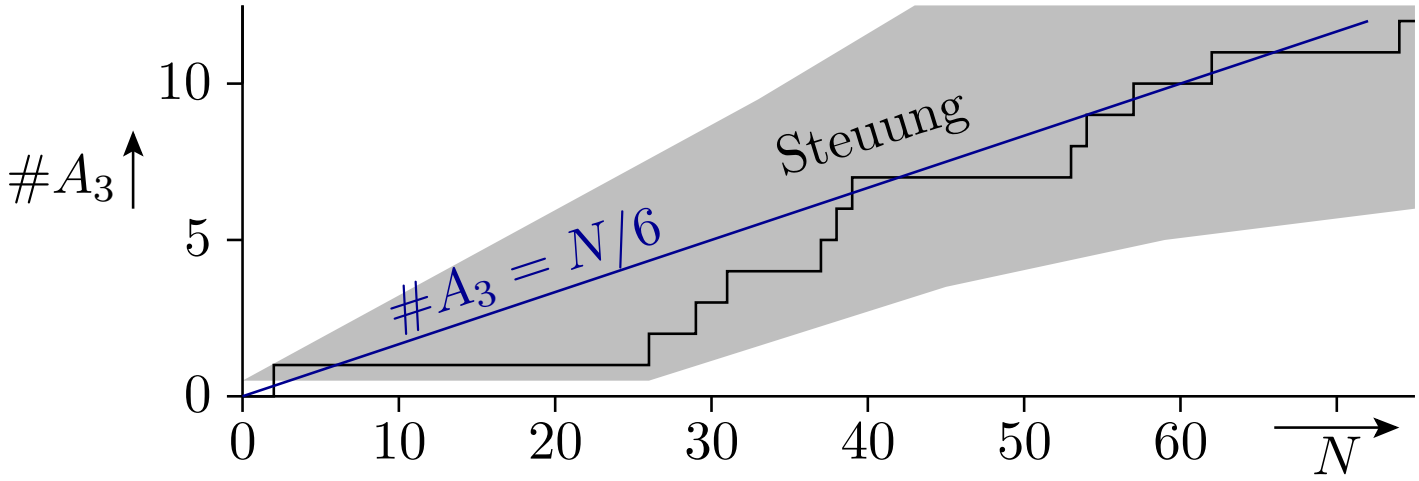
Kenngrößen, die gegen Wahrscheinlichkeiten streben:

Kenngröße	Experiment	günstig
$\lim_{N\to\infty}(DL) = p_\mathrm{F}$	Betrachtung eines Objekts	Objekt fehlerfrei
$\lim_{N\to\infty}(FC) = p_\mathrm{E}$	Test Objekt mit Fehler	Fehler erkennbar
$\lim_{N\to\infty}(Y) = 1 - p_\mathrm{F}\cdot p_\mathrm{E}$	Fertigung eines Objekts	kein erkennb. Fehler

(p_F – Wahrsch. Objekt fehlerhaft; p_E – Erkennungswahrscheinlichkeit).

Beispiel »Würfeln einer 3«

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



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

Wahrscheinlichkeit ist die beste Vorhersage für die zu erwartende relative Häufigkeit.

Verkettete Ereignisse

Verkettete Ereignisse

Beschreibung eines Zufallsexperiments durch Teilexperimente mit 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
$\#C$	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

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

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.

Bedingte Wahrscheinl.

Zusatzbedingungen

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 $C \wedge D = 1$.

Zusatzbedingungen können großen Einfluss auf die möglichen Ergebnisse eines Zufallsexperiments und deren Eintrittswahrsch. haben.

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

- Zufallsvariable A Person infiziert: $\mathbb{P}(A) = 10^{-4}$
- Zufallsvariable 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:

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

Wenn Test anschlägt, dann in 99% der Fälle Fehlalarm.

Kontrollen mit Beispielzählwerten:

	Test positiv	Test negativ	Summe	
		$\mathbf{P}(B\|A)$		
infizierte Personen	9.900	100	10.000	
nicht infiz. Pers.	≈1 Mio.	≈99 Mio.	99,99 Mio.	$\mathbf{P}(A)$
Summe	1 Mio.	99 Mio.	100 Mio.	
	$\mathbf{P}(A\|B)$	$\mathbf{P}(B)$		

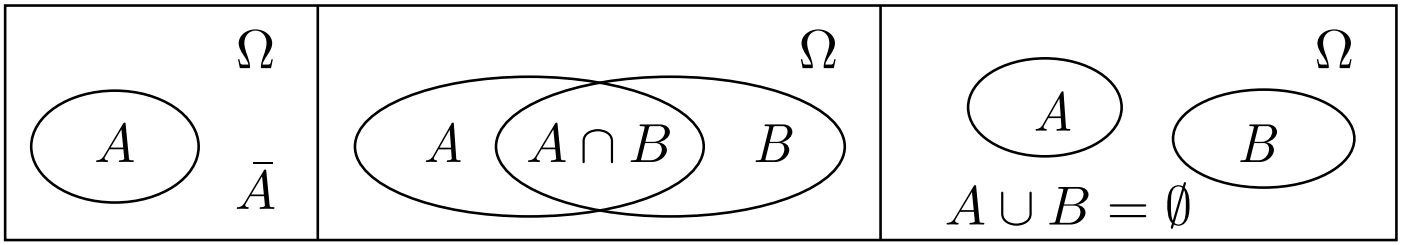
Person infiziert: $\mathbb{P}(A) = \frac{10.000}{1\,\text{Mio.}} \approx 10^{-4}$

Test positiv: $\mathbb{P}(B) = \frac{1\,\text{Mio.}}{100\,\text{Mio.}} \approx 1\%$

Test positiv, wenn Person infiziert: $\mathbb{P}(B|A) = \frac{9.900}{10.000} = 99\%$

Person infiziert, wenn Test positiv: $\mathbb{P}(A|B) = \frac{9.900}{1\,\text{Mio.}} \approx 1\%$

NOT / UND / ODER von Ereignissen



NOT (Nichteintrittswahrscheinlichkeit):

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

UND (gleichzeitiges Eintreten von A und B):

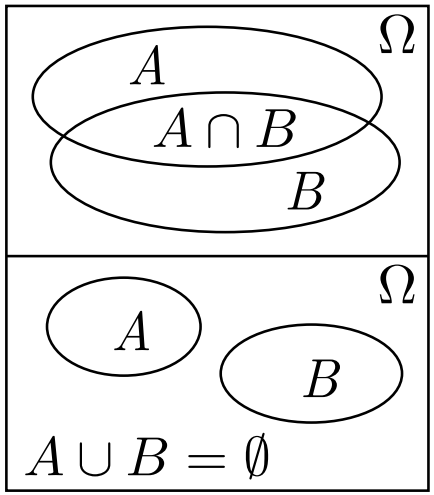
- stochastische Unabhängigkeit:

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

$$\mathbb{P}\left(A \cap B\right) = \mathbb{P}\left(A\right) \cdot \mathbb{P}\left(B\right)$$

- sich ausschließende Ereignisse:

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



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:

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

- sich ausschließende Ereignisse:

$$\begin{aligned} \mathbb{P}(A \cap B) &= 0 \\ \mathbb{P}(A \cup B) &= \mathbb{P}(A) + \mathbb{P}(B) \end{aligned}$$

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

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

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 nachweisbar 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):

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

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]:

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

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

- 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:

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

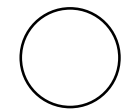
- Probe: Summe der Wahrscheinlichkeiten aller möglichen Ergebnisse muss immer 100% sein:

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

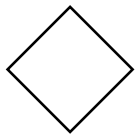
Fehlerbaumanalyse

Fehlerbaumanalyse (FTA – fault tree analysis)

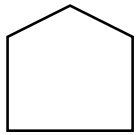
Graphische Darstellung für Ereignisabhängigkeiten zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahrensituationen, Ausfälle, Service-Versagen, ... Ereignissymbole:



Ereignis mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit.



Ereignis, dessen Eintrittswahrscheinlichkeit nicht untersucht wurde.

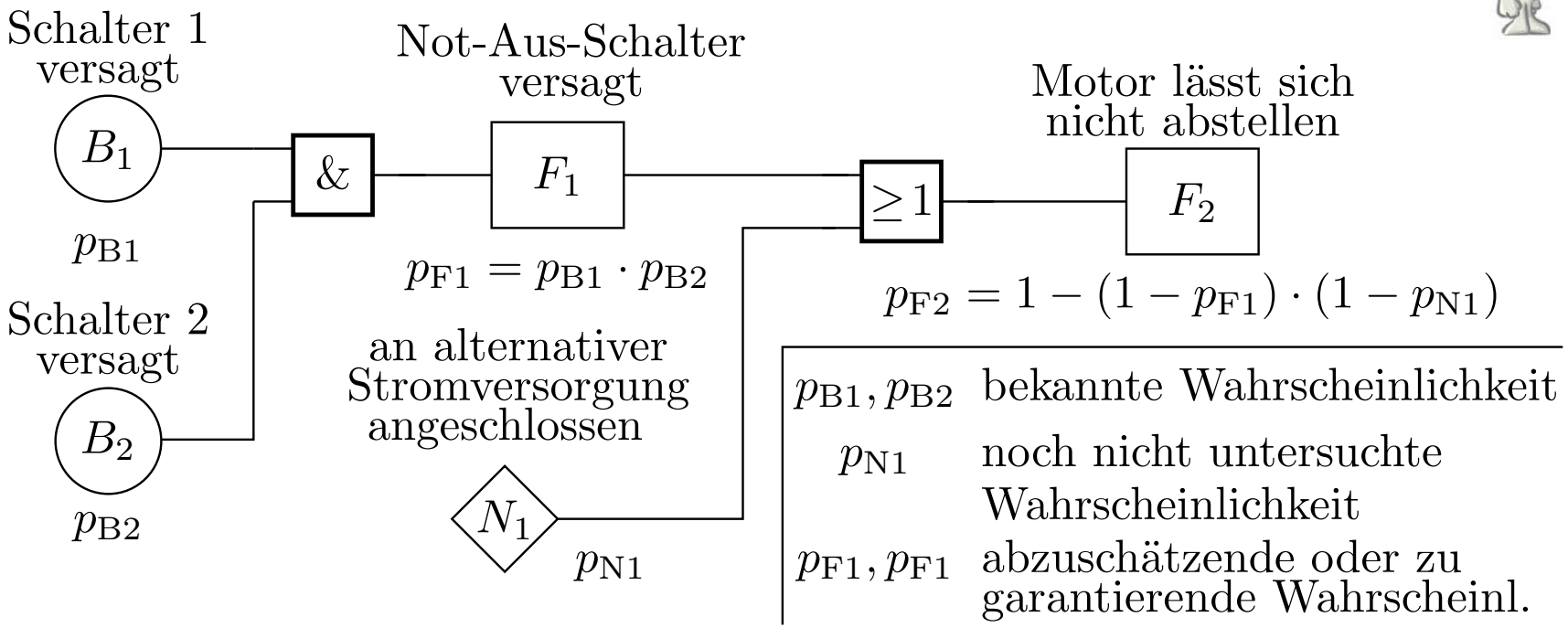


Ereignis im gewöhnlichen Betrieb, das in Kombination mit anderen Probleme verursachen kann.

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

Im Unterschied zur klassischen Fehlerbaumdarstellung verwenden wir für die Darstellung der logische UND-, ODER- und NICHT-Verknüpfungen die Schaltsymbole aus der Digitaltechnik.

Beispiel: Motor lässt sich nicht abstellen



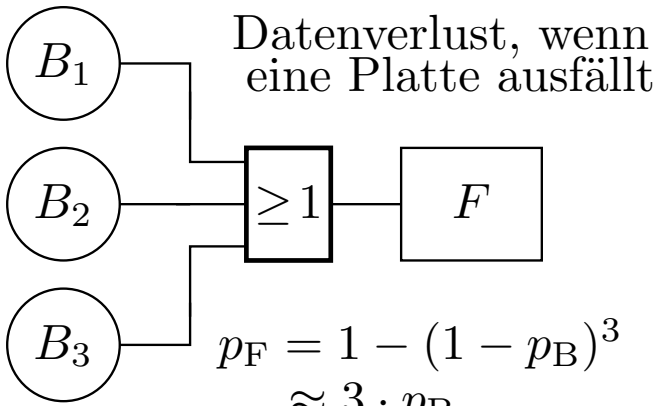
Formulierbare Aufgabe: Wenn $p_{B1} = p_{B2} = 10^{-3}$ ist und $p_{F2} \leq 10^{-6}$ sein darf

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

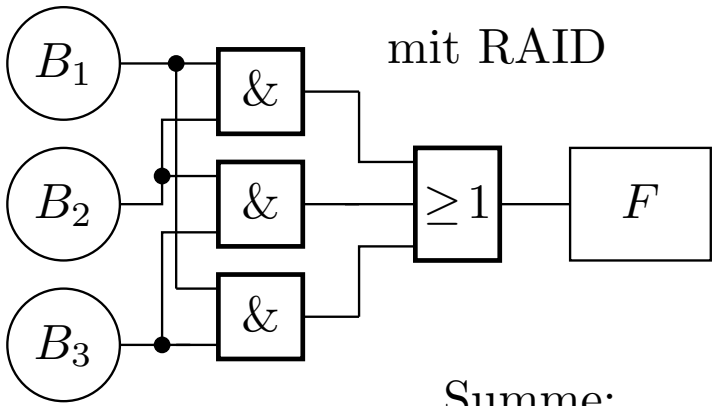
(Ziel hier nur mit $p_{N1} = 0$ erreichbar. Realistisch/andere Lösung?)

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.



$$p_\mathrm{F} = 1 - (1 - p_\mathrm{B})^3 \approx 3 \cdot p_\mathrm{B}$$



B_3	B_2	B_1	F	
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$p_\mathrm{B}^2 \cdot (1 - p_\mathrm{B})$
1	0	0	0	
1	0	1	1	$p_\mathrm{B}^2 \cdot (1 - p_\mathrm{B})$
1	1	0	1	$p_\mathrm{B}^2 \cdot (1 - p_\mathrm{B})$
1	1	1	1	p_B^3

Summe:

$$p_\mathrm{F} = 3 \cdot p_\mathrm{B}^2 - 2 \cdot p_\mathrm{B}^3$$

p_B	Wahrscheinlichkeit Plattenversagen
p_F	Wahrscheinlichkeit Datenverlust

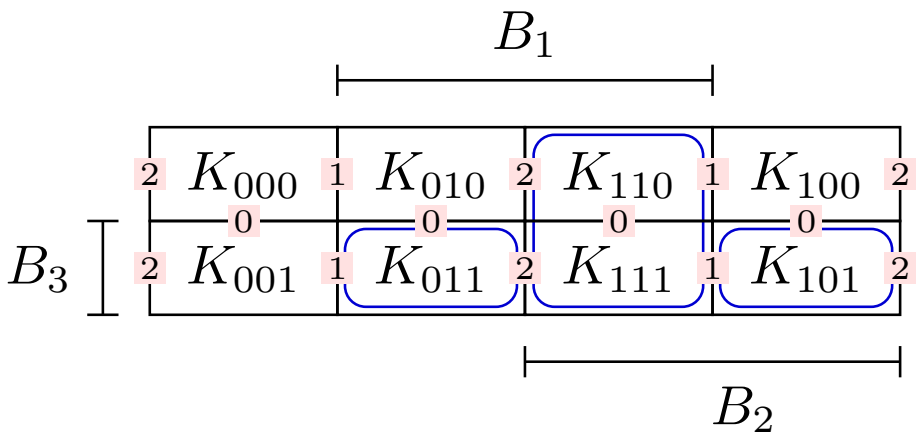
Rekonvergente Auffächerungen

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

$$F = B_1 B_2 \vee B_2 B_3 \vee B_1 B_3$$

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

Umstellung in Verknüpfung sich ausschließender Ereignisse:



$$\begin{aligned} F &= B_1 B_2 \vee \bar{B}_1 B_2 B_3 \vee B_1 \bar{B}_2 B_3 \\ p_F &= p_B^2 + p_B^2 \cdot (1 - p_B) + p_B^2 \cdot (1 - p_B) = 3 \cdot p_B^2 - 2 \cdot p_B^3 \end{aligned}$$

Verallgemeinerung auf n Platten

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

$$p_\mathrm{F} \approx n \cdot p_\mathrm{B}$$

(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:

$$p_\mathrm{F} \approx 1 - \underbrace{\underbrace{\left(\underbrace{(1-p_\mathrm{B})^n}_{\text{keine Platte}} + \underbrace{n \cdot p_\mathrm{B} \cdot (1-p_\mathrm{B})^{n-1}}_{\text{eine Platte}} \right)}_{\text{keine oder eine Platte}}}_{\text{mindestens zwei Platten}}$$

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

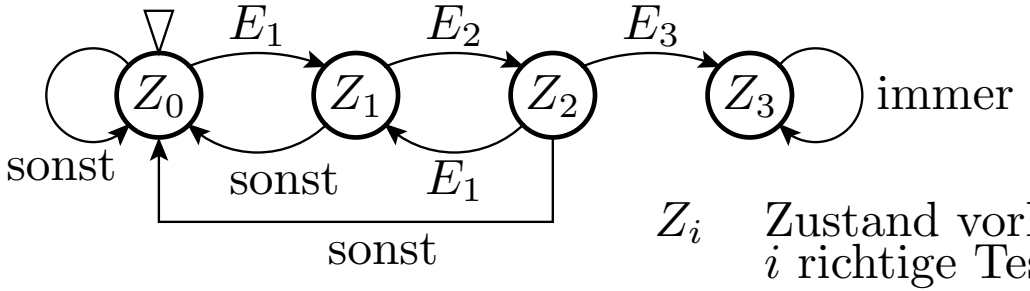
zuvor auf andere Weise abzuschätzen: Vorexperimente, Expertenbefragungen, Ursache-Wirkungs- (Ishikawa-) Diagramme, ...

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.

Zustandsautomat Fehlernachweis mit Eingabefolge $E_1 E_2 E_3$:

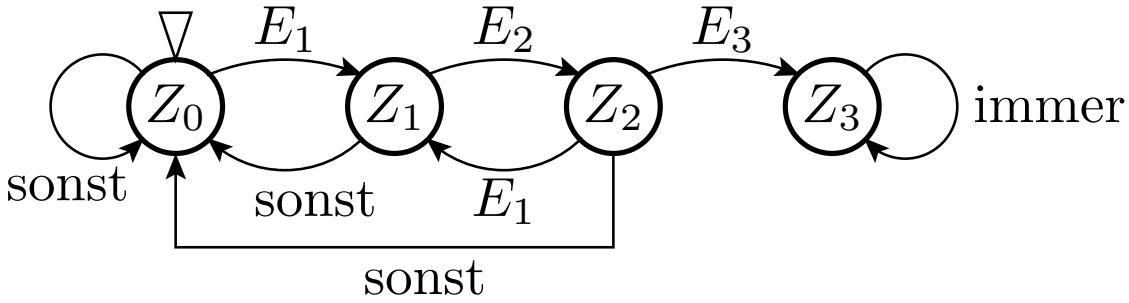


Z_i Zustand vorherige Folge i richtige Testeingaben

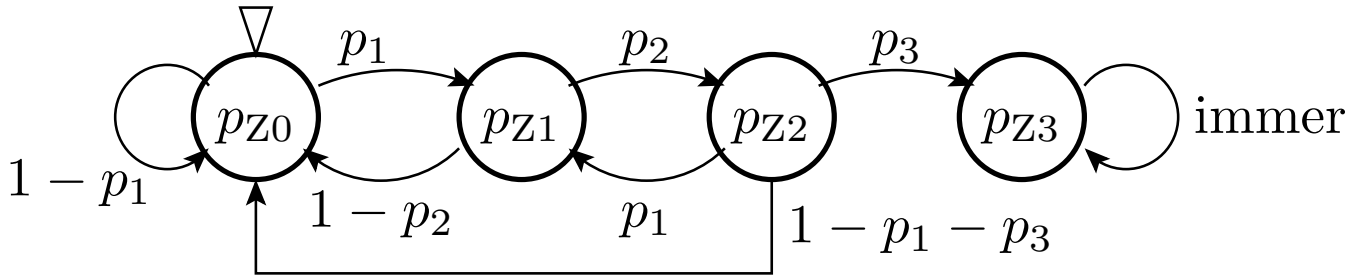
E_i richtige Eingabe i

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

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

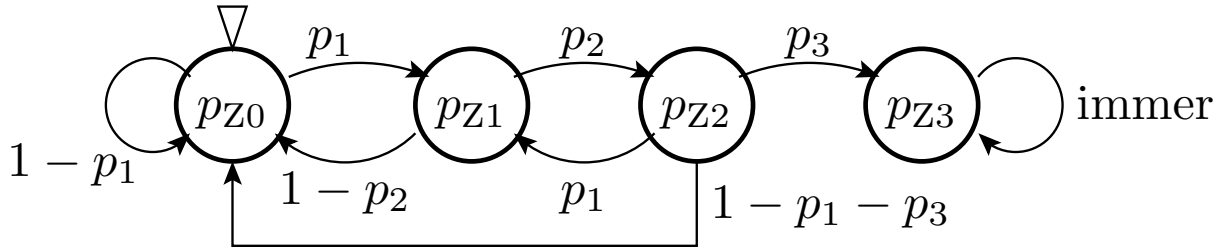


Zur Umwandlung in eine Markov-Kette werden die Übergangsbedingungen durch die Übergangswahrscheinlichkeiten p_1 bis p_3 und die Zustände durch Zustandswahrscheinlichkeiten $p_{\mathrm{Z.i}}$ ersetzt.



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

Simulation von Markov-Ketten



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

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

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

Kontrollkriterien für Gleichungssystem und Simulationsergebnis:

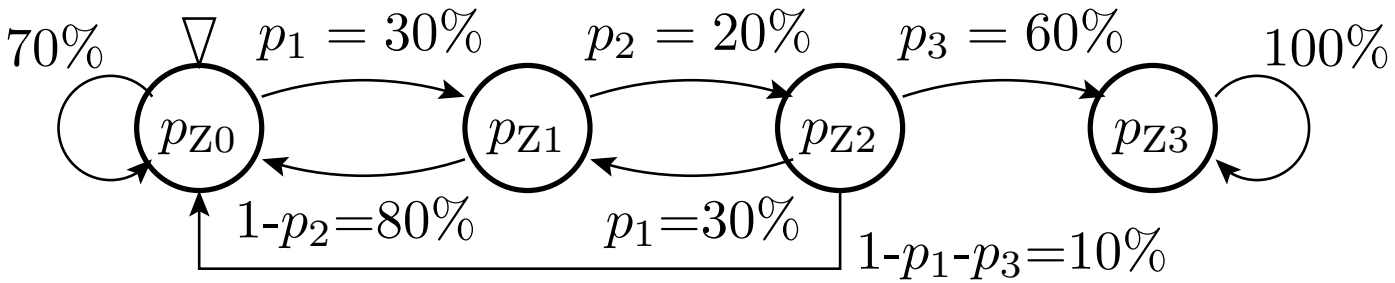
- Summe der Wahrscheinlichkeiten je Matrixspalte eins.
- Summe $p_{Z.i}$ in jedem Schritt eins.

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

Simulation mit Octave bzw. Matlab:

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

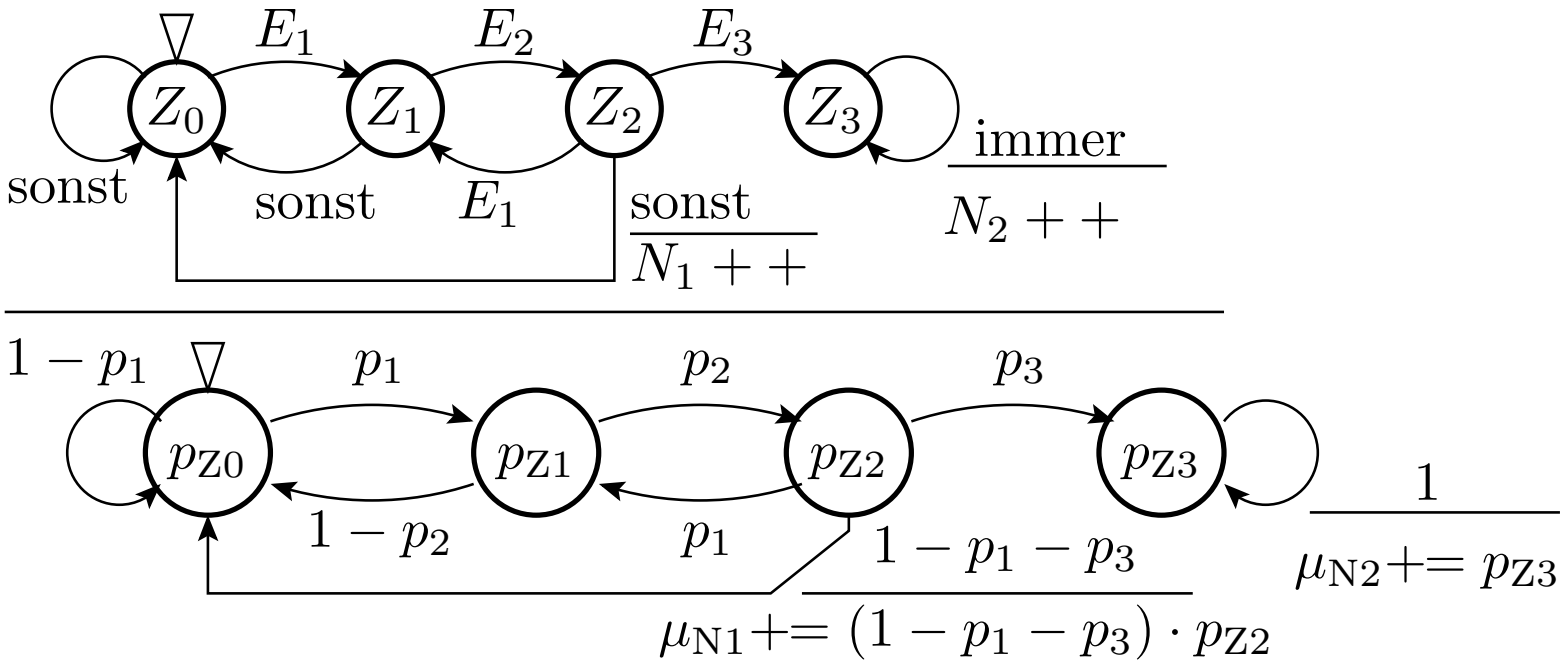
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	p_{Z0}	p_{Z1}	p_{Z2}	p_{Z3}	Summe
0	100,00%	0	0	0	100%
1	70,00%	30,00%	0	0	100%
2	73,00%	21,00%	6,00%	0	100%
3	68,50%	21,90%	6,00%	3,60%	100%
4	66,07%	20,55%	6,18%	7,20%	100%
...	...	...	...	...	...
10	51,52%	16,11%	4,88%	27,49%	100%
...	...	...	...	...	...
50	9,89%	3,09%	0,94%	86,08%	100%
...	...	...	...	...	...
100	1,26%	0,39%	0,12%	98,23%	100%

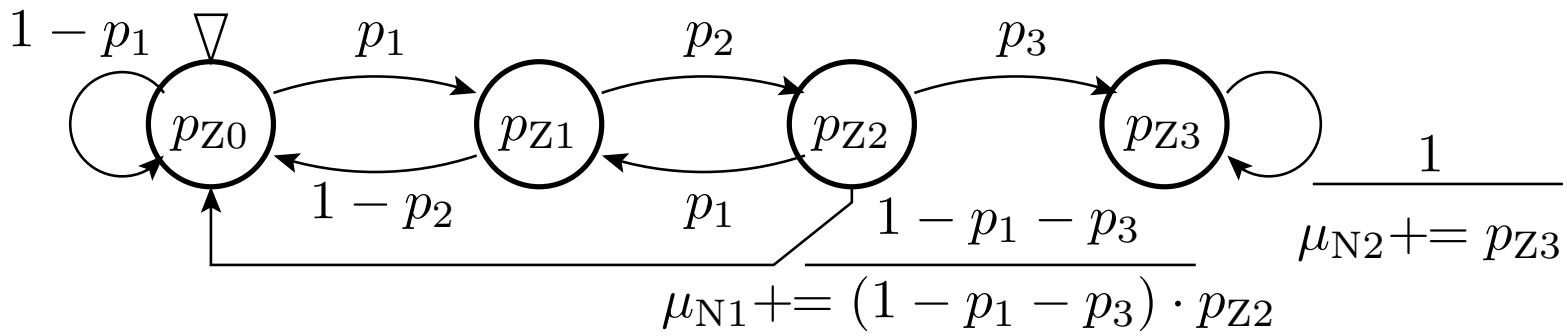
Kantenkosten

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



Zähler N_1 zählt, wie oft nach zwei richtigen Eingaben eine falsche folgt, Zähler N_2 die Anzahl der Eingaben im Zustand Z_3; n – Gesamtzahl der Schritte; $n - N_2$ Schritte bis Fehlernachweis.

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

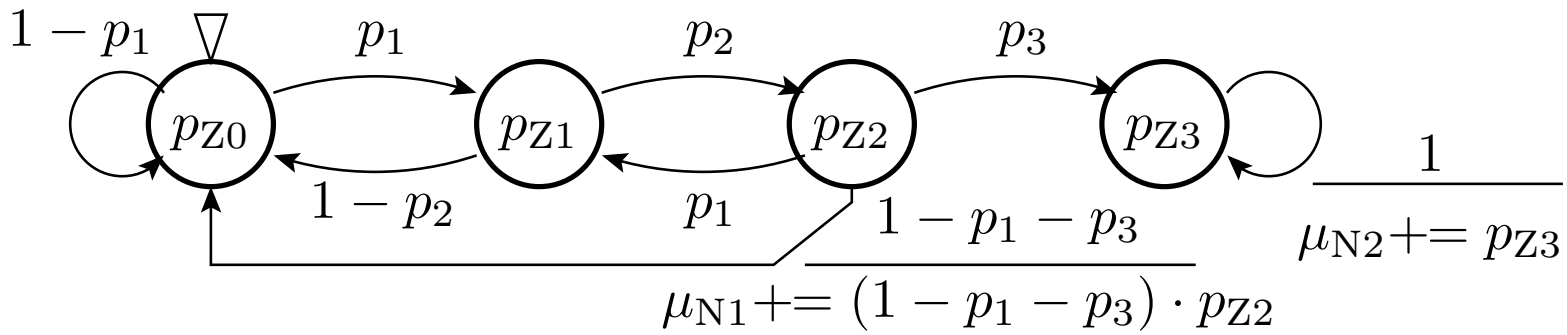


Erweiterung des Simulationsprogramms:

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

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

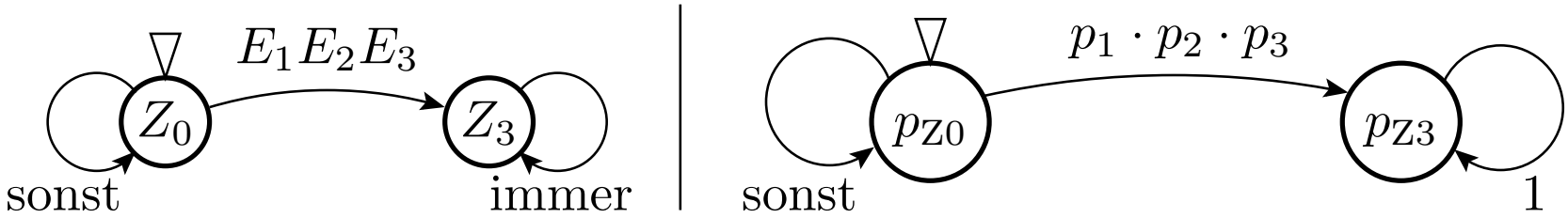
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	p_{Z0}	p_{Z1}	p_{Z2}	p_{Z3}	μ_{N1}	μ_{N2}
1	70,00%	30,00%	0	0	0	0
2	73,00%	21,00%	6,00%	0	0,01	0
3	68,50%	21,90%	6,00%	3,60%	0,01	0,04
4	66,07%	20,55%	6,18%	7,20%	0,02	0,11
...	...	...	...	...	...	...
10	51,52%	16,11%	4,88%	27,49%	0,05	1,27
...	...	...	...	...	...	...
50	9,89%	3,09%	0,94%	86,08%	0,14	27,36
...	...	...	...	...	...	...
100	1,26%	0,39%	0,12%	98,23%	0,16	74,48

Die zu erwartende Anzahl der Schritte bis zum Nachweis $n - N_2$ (n – Anzahl der simulierten Schritte) ist etwa 25.

»Drei richtige Eingaben« als Einzelereignis



Gleichungssystem der modifizierten Markov-Kette:

$$\begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_1 \cdot p_2 \cdot p_3 & 0 \\ p_1 \cdot p_2 \cdot p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

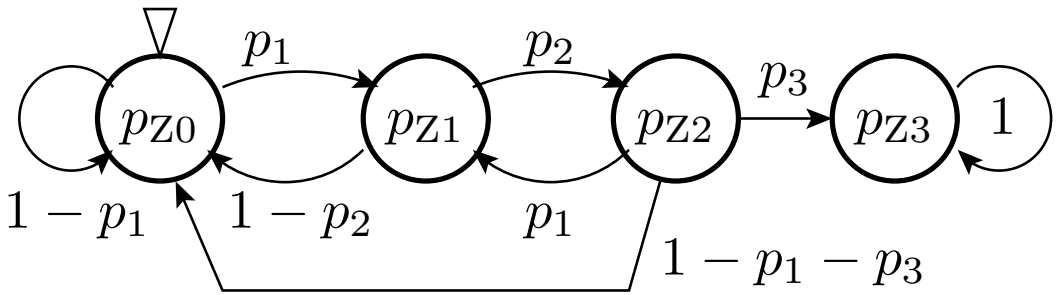
$$\begin{aligned} p_{Z0}(n) &= (1 - p_1 \cdot p_2 \cdot p_3) \cdot p_{Z0}(n-1) = (1 - p_1 \cdot p_2 \cdot p_3)^n \\ &= \mathrm{e}^{\ln(1-p_1 \cdot p_2 \cdot p_3) \cdot n} \approx \mathrm{e}^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \quad \text{für } p_1 \cdot p_2 \cdot p_3 \ll 1^* \\ p_{Z3}(n) &= 1 - p_{Z0}(n) = 1 - (1 - p_1 \cdot p_2 \cdot p_3)^n \\ &\approx 1 - \mathrm{e}^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \quad \text{für } p_1 \cdot p_2 \cdot p_3 \ll 1^* \end{aligned}$$

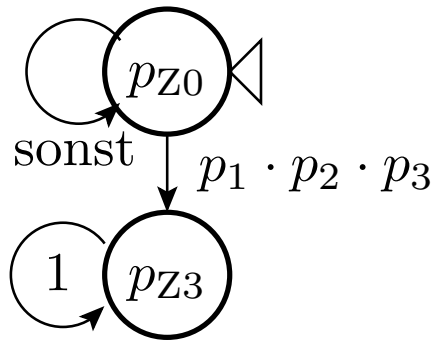
---

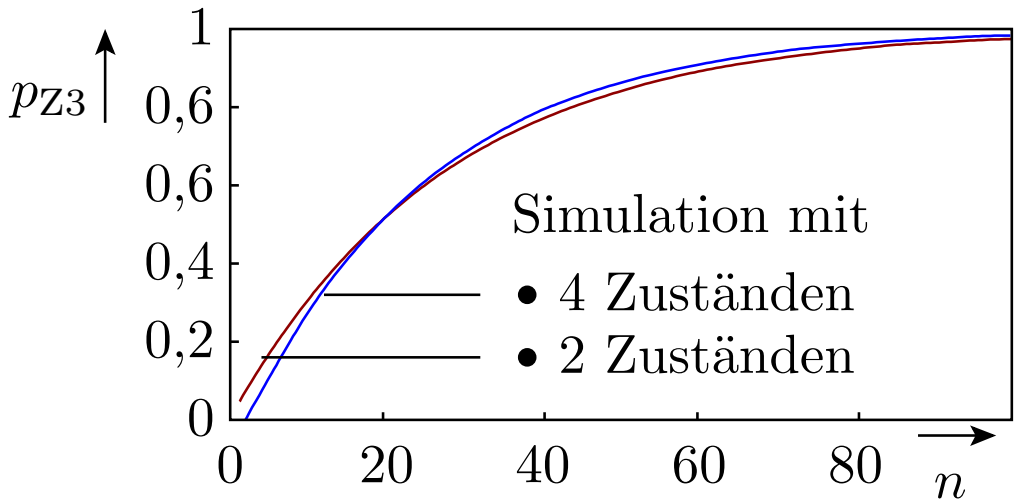
* Annäherung durch das erste Glied der Taylor-Reihe:

$$\ln(1-x) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots\right)$$

Abweichung $p_{Z3}\,(n)$ beider Markov-Ketten





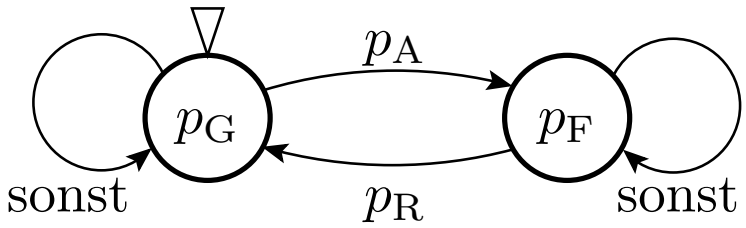


Offenbar doch nicht identisches Verhalten:

- In der linken MK fehlt Kante $Z_1 \overset{E_1}{\to} Z_1$.
- Rechte MK ignoriert Abhängigkeiten $E_iE_jE_k,\ E_jE_kE_l, \ldots,$ ...

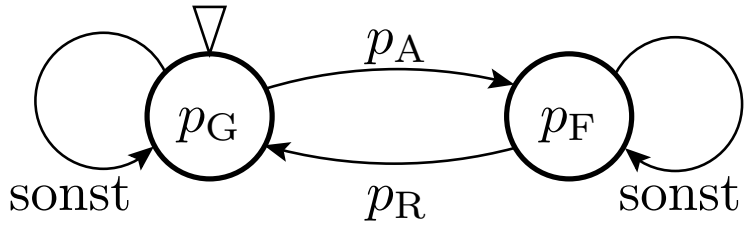
Abschätzung der Verfügbarkeit

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):

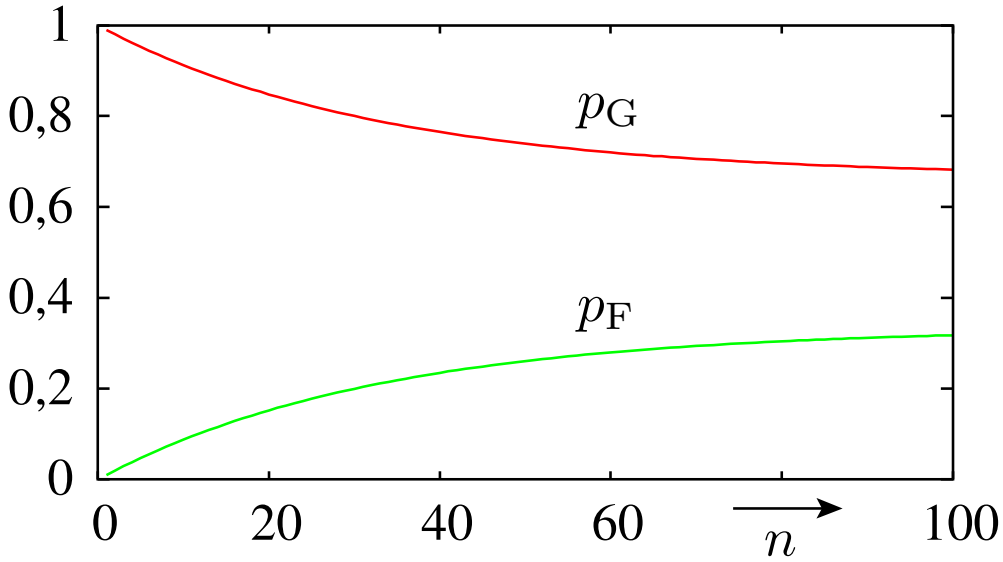


Beschreibung als simulierbares Gleichungssystem:

$$\begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_\mathrm{A} & p_\mathrm{R} \\ p_\mathrm{A} & 1-p_\mathrm{R} \end{pmatrix} \cdot \begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$



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

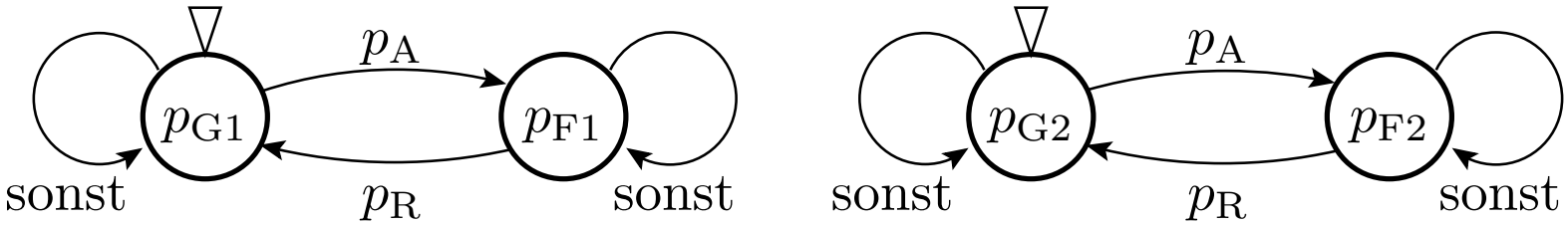


Für große n strebt der Reparaturprozess gegen den stationären Zustand:

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

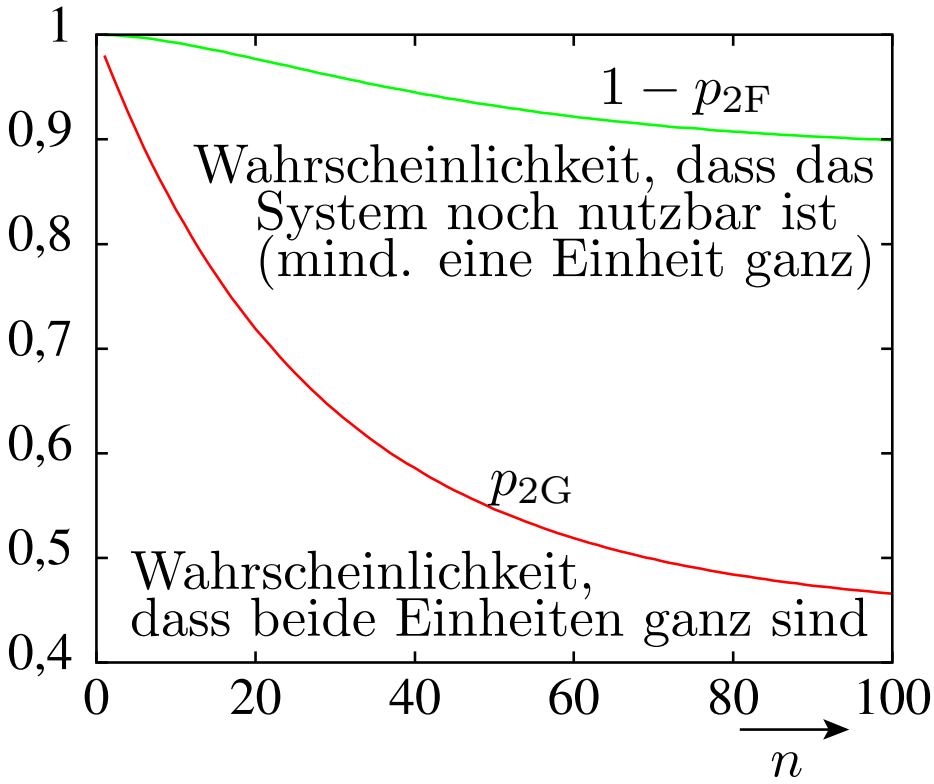
Reparatur mit Redundanz

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 $p_R = 2\%$:

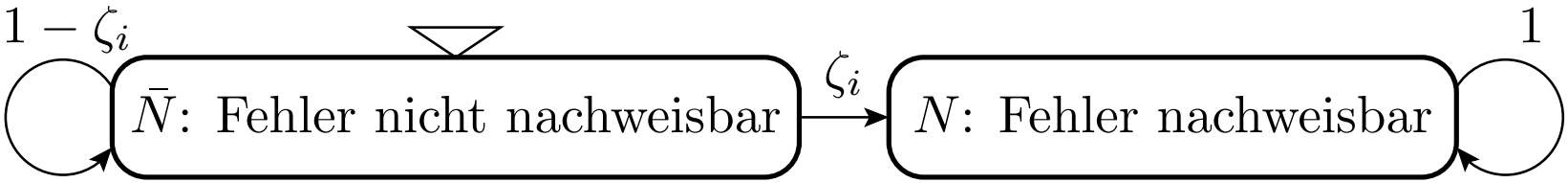


n Anzahl der Simulationsschritte

Fehlernachweis

Ohne Gedächtnis

Nachweiswahrscheinlichkeit für einen Fehler



Ein Fehler i wird nachgewiesen, wenn er eine FF verursacht. Nachweiswahrscheinlichkeit je Service-Anforderung $\zeta_i \left[\cdot 1\,\mathrm{FF/SL}\right]$ (ohne Masseinheit). Wahrscheinlichkeit Nichtnachweis mit n SL bzw. Tests:

$$\mathbb{P}\left(\bar{N}_i, \zeta_i, n\right) = (1-\zeta_i)^n = \mathrm{e}^{\ln(1-\zeta_i)\cdot n}$$

Für $\zeta \ll 1$ nach Tailor-Reihe $\ln(1-\zeta) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots\right) \approx -\zeta$:

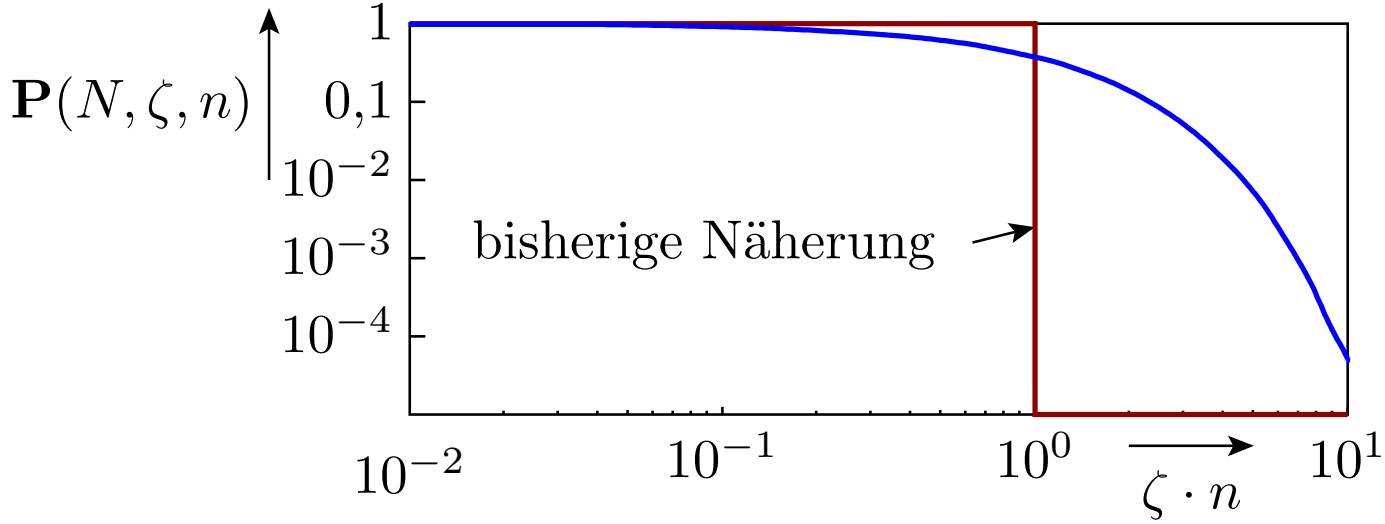
$$\mathbb{P}\left(\bar{N}_i, \zeta_i, n\right) = \mathrm{e}^{-\zeta_i \cdot n}$$

Nachweiswahrscheinlichkeit:

$$p_i(n) = \mathbb{P}\left(N_i, \zeta_i, n\right) = 1 - \mathbb{P}\left(\bar{N}_i, \zeta_i, n\right) = 1 - \mathrm{e}^{-\zeta_i \cdot n}$$

Voraussetzung: ζ_i bleibt während des Tests konstant:

- fehlerunabhängige Testauswahl, keine Gedächtinis,
- keine Änderung des Operationsprofils, ...



Auf Foliensatz F1, Abschnitt Test und Zuverlässigkeit wurde unterstellt:

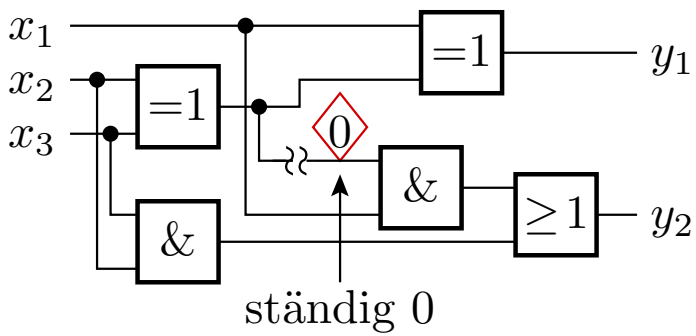
- Fehler mit $\zeta \cdot n \geq 1$ werden nachgewiesen und beseitigt und
- Fehler mit $\zeta \cdot n < 1$ verursachen FF.

Zufallstest: $\mathbb{P}\left(N_i, \zeta_i, n\right) = 1 - \mathrm{e}^{-\zeta_i \cdot n}$

- $n = {}^1/_{\zeta}$ ist nur die mittlere, nicht die garantierte Testsatzlänge, ab der Fehler nachgewiesen werden.
- Praktisch sicher nachgewiesen erst ab $\zeta \cdot n \geq 5 \ldots 10$.
- Genaue Rechnung erst auf Foliensatz F3 nach Einführung der Gamma-Verteilung. Die bisherigen Abschätzungen ändern sich nur unerheblich.

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.

Mit Gedächtnis

Service mit Gedächtnis

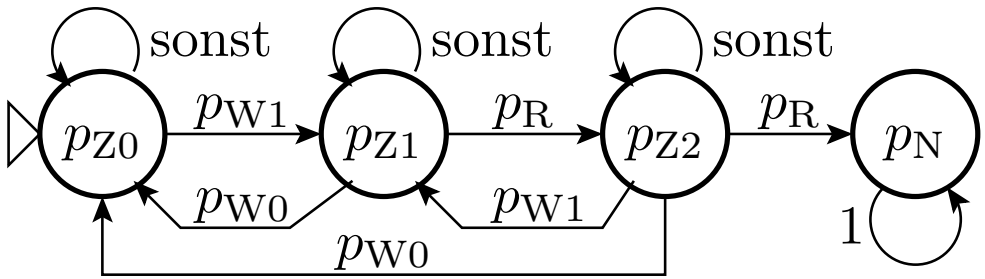
Der Fehlernachweis in einem Service mit Gedächtnis kann auch eine Folgen von mehreren Service-Anforderungen erfordern. Der Nachweis des Fehlertyps »zerstörendes Lesen einer Eins«[3] erfordert z.B.:

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

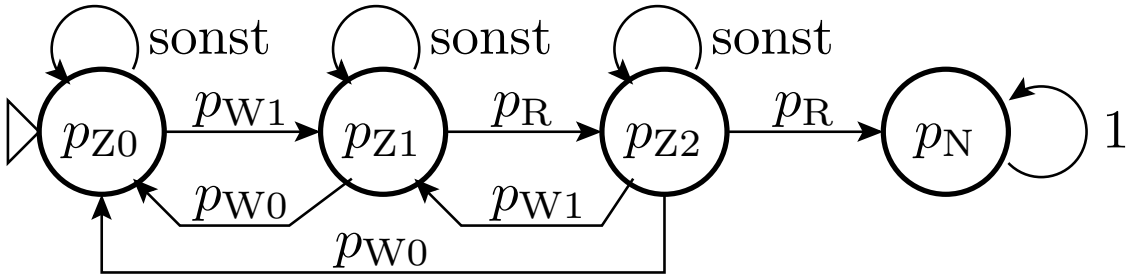
Markov-Kette zur Modellierung des zufälligen Fehlernachweises:

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



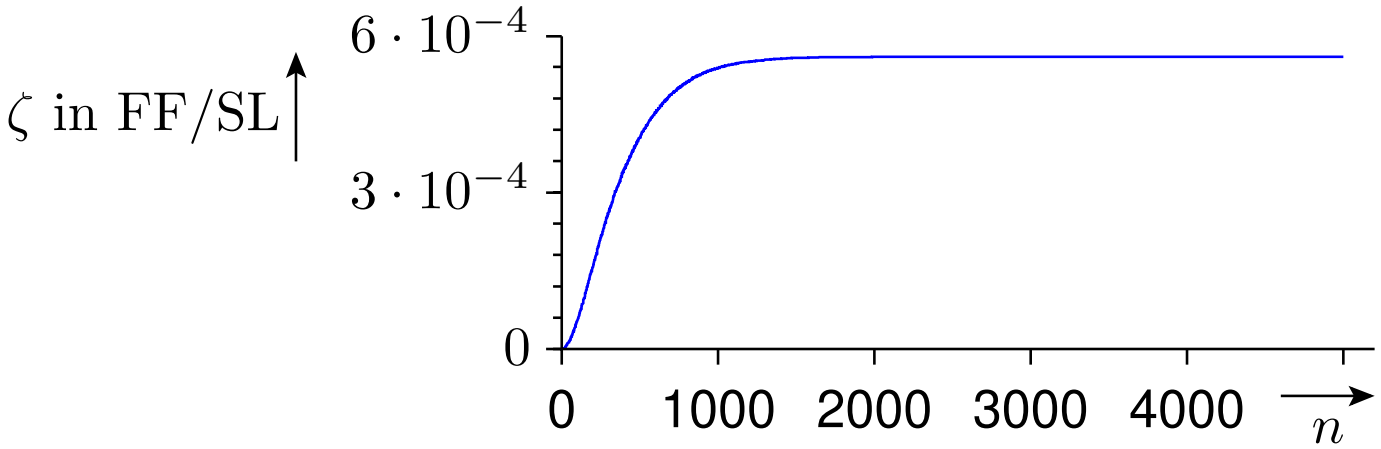
p_{W0}, p_{W1} – Wahrscheinlichkeit, dass in die Speicherzelle eine null bzw. eine eins geschrieben wird; p_R – Wahrscheinlichkeit, dass die Speicherzelle gelesen wird.

```
pZ0=1; pZ1=0; pZ2=0; pN(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW0 = pW1 = 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    = pN(n) + pZ2 * pR;
  zeta  = pZ2*pR / (pZ0+pZ1+pZ2); % FF-Rate gleich Nachweiswahrsch.,
end                               % wenn noch nicht nachgewiesen
plot(1:N, zeta);
```

Vermeidung kleiner Differenzen großer Zahlen:

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

FF-Rate in Abhängigkeit von der Testsatzlänge:



Die FF-Rate nimmt anfangs mit der Testsatzlänge zu und bleibt ab $n_{\mathrm{K}} \approx 1000$ konstant $\zeta \approx 5{,}7 \cdot 10^{-4}$.

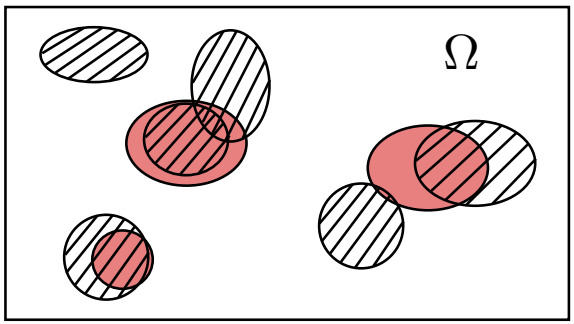
Für lange Zufallstests kann in der Regel auch die FF-Rate eines Fehlers in Systemen mit Gedächtnis wie bei Systemen ohne Gedächtnis als konstant betrachtet und die Nachweiswahrscheinlichkeit wie die für Systeme ohne Gedächtnis abgeschätzt werden:

$$1 - e^{-(n-n_{\mathrm{K}})\cdot\zeta} < p\,(n) < 1 - e^{-n\cdot\zeta}$$

Fehler und Modellfehler

Fehler und Modellfehler

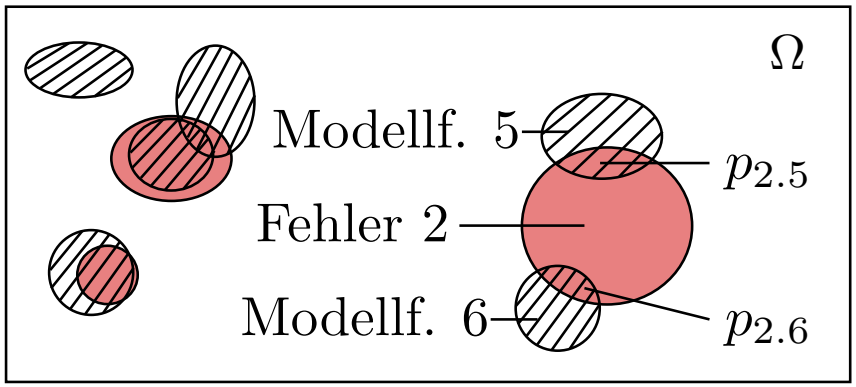
Die zu findenden Fehler sind zum Zeitpunkt der Testauswahl unbekannt. Die Suche von Tests für den Fehlernachweis, die Abschätzung der Fehlerüberdeckung, der FFR-Dichte und der erforderlichen Testsatzlänge erfolgt mit Modellfehlermengen. Ein Fehlermodell generiert für ein Testobjekt eine große Menge von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



Ω	Menge der Eingabewerte / Teilfolgen die einen Fehler nachweisen können
	Nachweismenge eines Modellfehlers
	Nachweismenge eines tatsächlichen Fehlers

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

Fehlerorientierte Testauswahl



Nachweismenge eines tatsächlichen Fehlers

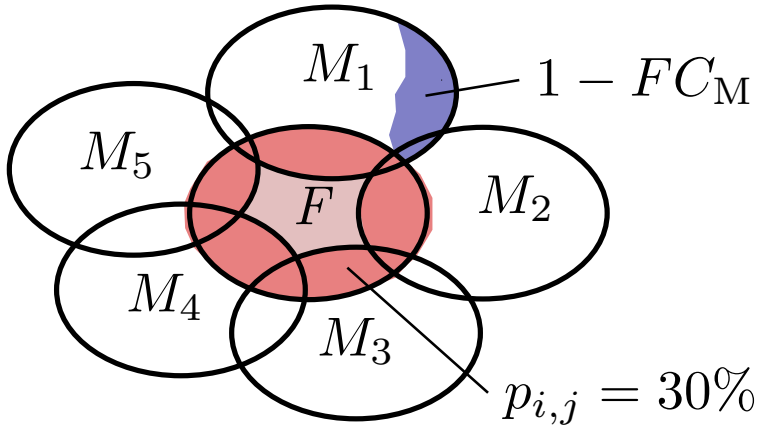
Nachweismenge eines Modellfehlers

Bei fehlerorientierter Testauswahl werden für jeden Modellfehler $m \geq 1$ gesucht, die ihn nachweisen. Ein tatsächlicher Fehler i wird von jedem für einen ähnlich nachweisbaren Modellfehler gefundenen Test j mit einer Wahrscheinlichkeit p_{ij} nachgewiesen:

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

$\#MF_i$ – Anzahl der ähnlich nachweisbaren Modellfehler für Fehler i;
m_j – Anzahl der gefundenen Tests für Modellfehler j.

Modellrechnung



Nachweismenge

M_j	Modellfehler j
F	Fehler i

- $\#MF_i = 5$ ähnlichnachweisbare Modellfehler.
- Wahrsch., dass ein Test, der einen der ähnlich nachweisbaren Modellfehler j nachweist, auch Fehler i nachweist, sei $p_{ij} = 30\%$.
- Modellfehlerüberdeckung $FC_{\mathrm{M}} \in \{90\%, 95\%\}$.
- Anzahl der gesuchten Tests je Modellfehler $m \in \{1, 2, \ldots, 5\}$.
- Für Modellfehler, für die überhaupt ein Test gefunden wird, werden auch die weiteren $m - 1$ angestrebten Tests gefunden.

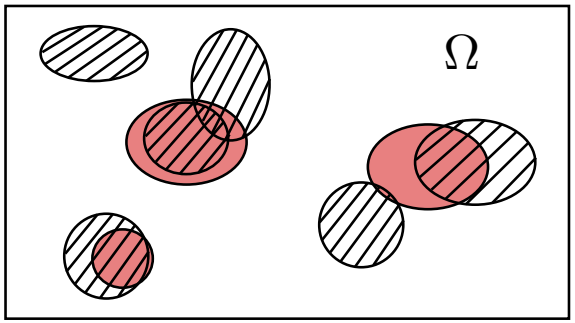
Geschätzte Nachweiswahrscheinlichkeit:

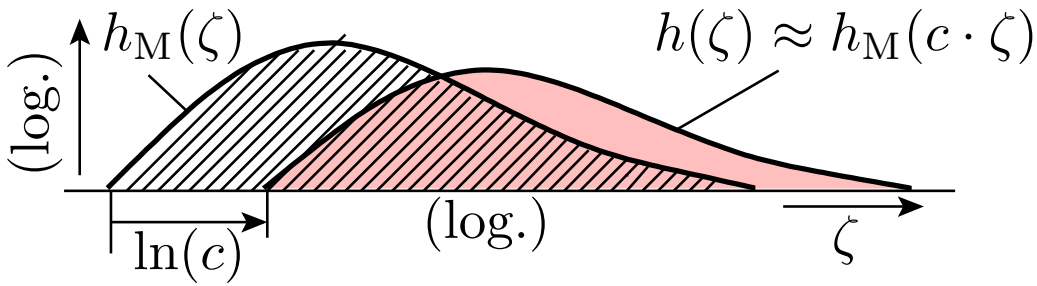
$$p_i = 1 - (1 - 30\%)^{5 \cdot FC_{\mathrm{M}} \cdot m} = 1 - 0{,}168^{FC_{\mathrm{M}} \cdot m}$$

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

Die Nachweiswahrscheinlichkeit des tatsächlichen Fehlers und damit auch FC hängt weniger von FC_{M}, dafür aber erheblich von der Anzahl der Tests m, die für jeden Modellfehler gesucht werden, ab.

Zufälliger Fehlernachweis





Nachweismenge eines tatsächlichen Fehlers

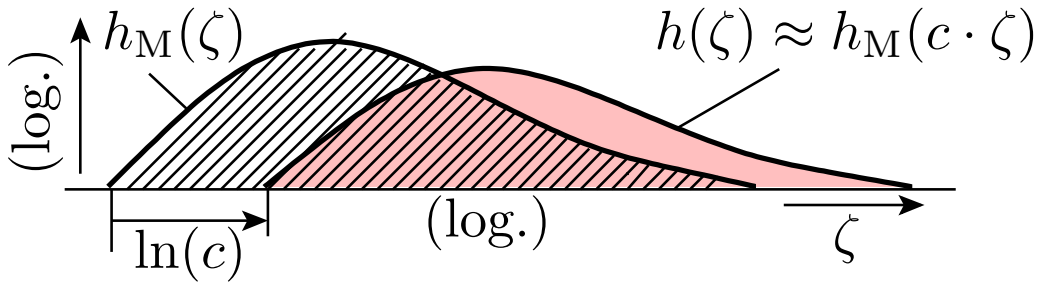
Nachweismenge eines Modellfehlers

Nachweiswahrscheinlichkeiten der Modell- und der tatsächlichen Fehler gleich der FF-Rate der Fehler.
Annahme: Dichte der FF-Rate der tatsächlichen Fehler proportional zur Dichte der FF-Rate der Modellfehler für die c-fache FF-Rate:

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

Tatsächliche FC abschätzungsweise Modellfehlerüberdeckung der c–fachen Testsatzlänge:

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



$$h\left(\zeta\right) \sim h_{\mathrm{M}}\left(c \cdot \zeta\right) \quad \rightarrow \quad FC\left(n\right) \approx FC_{\mathrm{M}}\left(c \cdot n\right)$$

Für $FC \approx FC_{\mathrm{M}}$ muss,

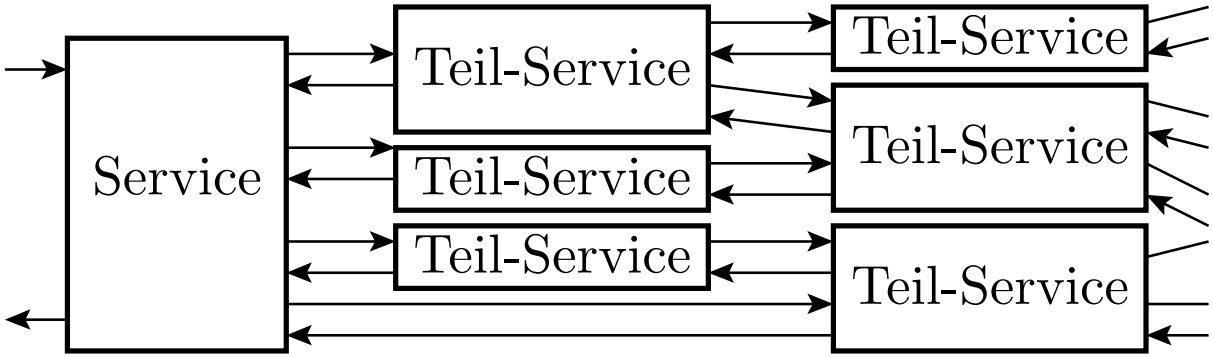
- wenn die Modellfehler im Mittel schlechter nachweisbar sind ($c > 1$), der Modellfehlertest und
- wenn die Modellfehler besser nachweisbar sind ($c < 1$), der tatsächliche Test

um Faktor c länger sein.

Zufällige Testauswahl stellt weniger Anforderungen an das Fehlermodell (nicht für jeden zu erwartenden tatsächlichen Fehler mehrere ähnlich nachweisbare Fehler mit $p_{ij} > 10\%$) und erlaubt eine vertrauenswürdigere Abschätzung der tatsächlichen Fehlerüberdeckung.

Isolierter Test

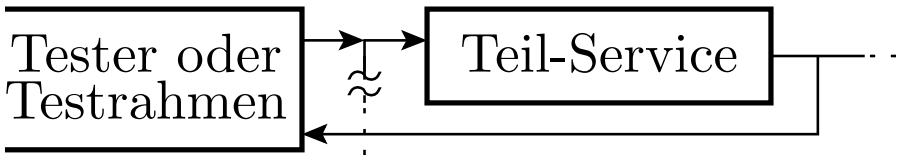
Isolierter Test



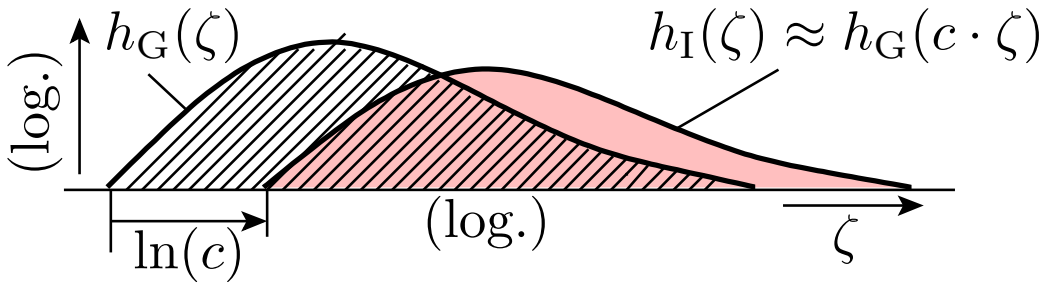
In einem hierarchischen System verursacht ein Fehler in einem Teil-Service nur dann ein Versagen der übergeordneten Service-Leistung, wenn

- 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 $c \gg 1$:

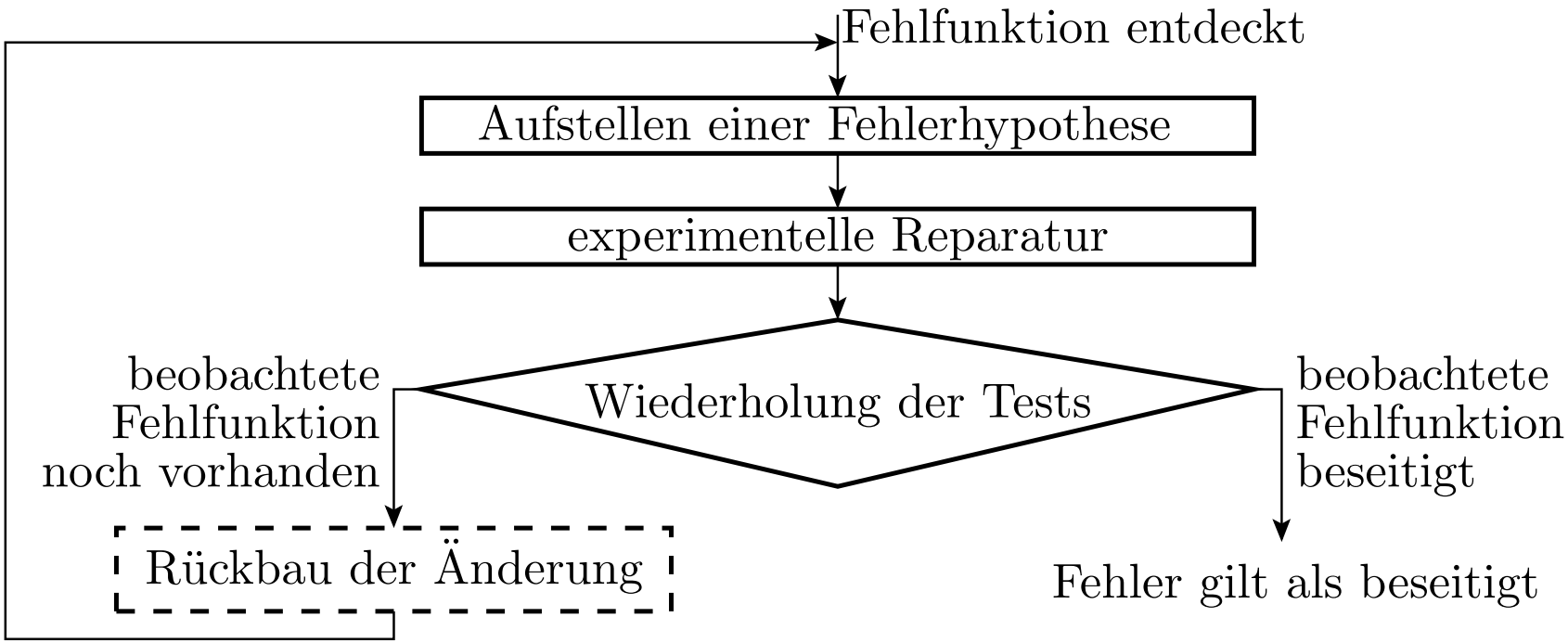


(h_{G} – FFR-Dichte der betrachteten Teil-SL beim eingebetteten Test im Gesamtsystem; h_{I} – FFR-Dichte der betrachteten Teil-SL beim isolierten Test; $c \gg 1$ – Skalierungsfaktor).

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.

Fehlerbeseitigung

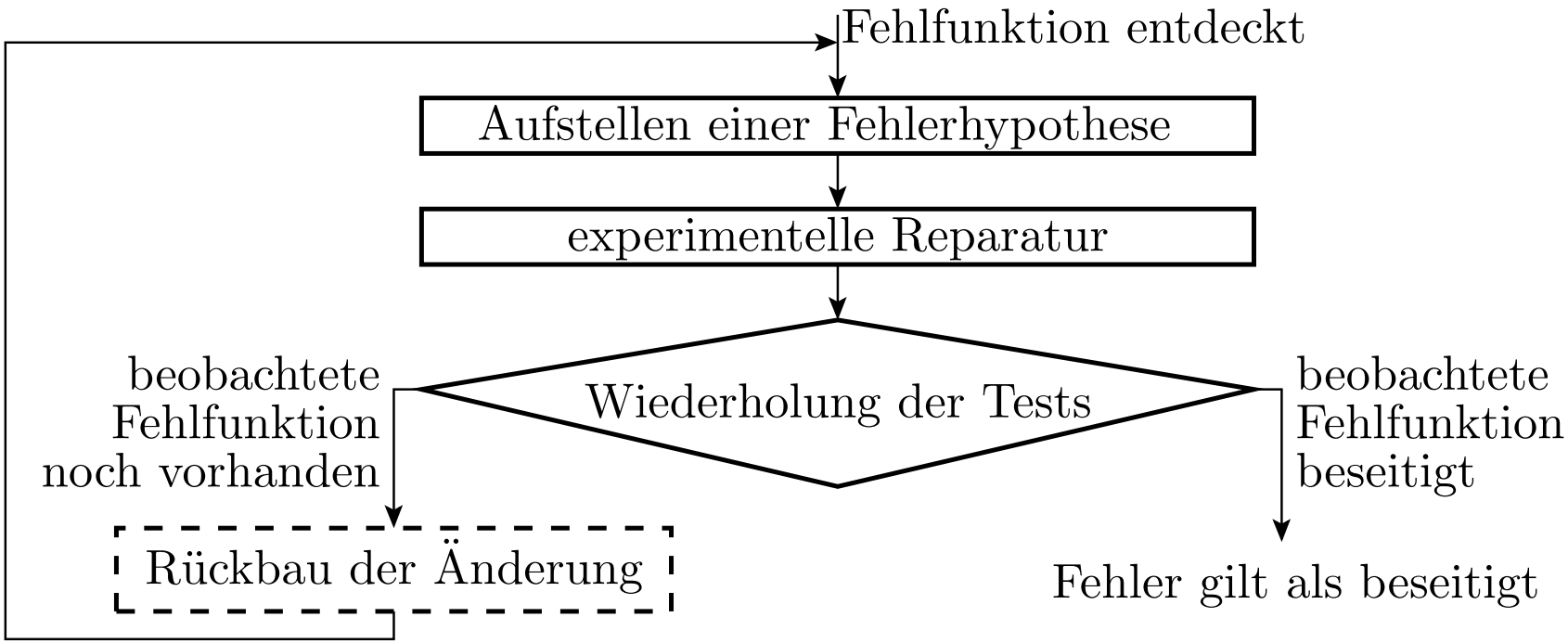
Wiederholung Experimentelle Reparatur



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

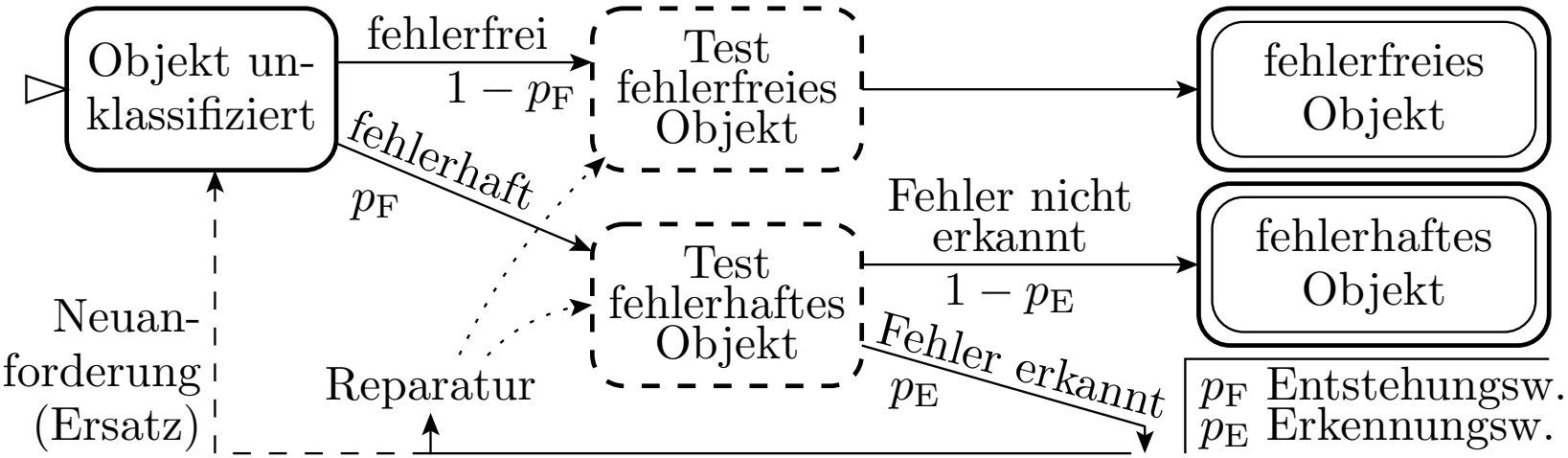
Diese Iteration beseitigt jeden erkennbaren Fehler.

3. Fehlerbeseitigung



- 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.
- Phantomfehler, im Bild vernachlässigt, würden einer Zusatzkante von »Test fehlerfreies Objekt« zu Reparatur oder Ersatz erfordern.

Für die Fehlerbeseitigung selbst sind zwei Ansätze zu unterscheiden:

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

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 $Y \ll 50\%$.

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

Beispiel Schaltkreiskosten ohne Reparatur

- Zu erwartenden Fehlerzahl: $\#F \approx 10^{-5} \cdot \#T$ ($\#T$ – Anz. Trans.).
- Fertigungskosten in Geldeinheiten je Schaltkreis: $K_\mathrm{F} \approx 10^{-5} \cdot \#T$.
- Ausbeute[5]: $Y \approx \mathrm{e}^{-\#F}$.

Fertigungskosten je als gut befundener Schaltkreis:

$$K \approx \frac{\#K_\mathrm{F}}{\mathrm{e}^{-\#F}} = \underbrace{10^{-5} \cdot \#T}_{\#K_\mathrm{F}} \cdot \mathrm{e}^{\underbrace{10^{-5} \cdot \#T}_{\#F}}$$

$\#T$	10^4	10^5	10^6
K	$10^{-1} \cdot \mathrm{e}^{0,1} \approx 0{,}11$	$1 \cdot \mathrm{e}^{1} \approx 2{,}72$	$10 \cdot \mathrm{e}^{10} \approx 2{,}2 \cdot 10^5$

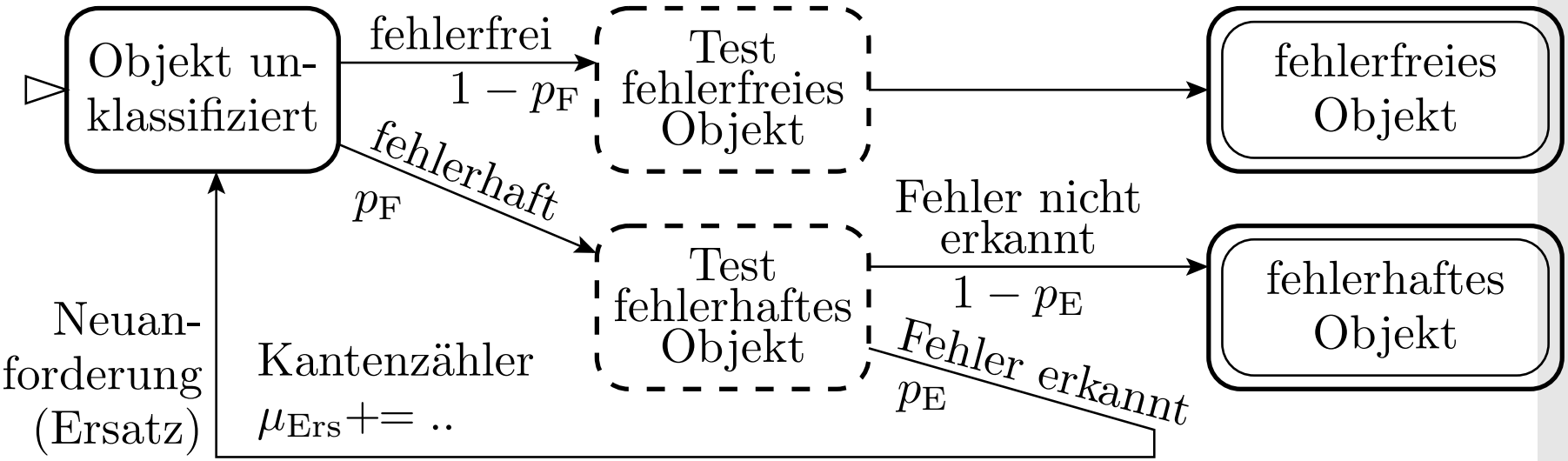
Ab $\#F \approx 2$ zu erwartenden Fehlern pro Schaltkreis ist ein reparaturgerechter Entwurf zwingend:

- deaktivieren / Ersatz defekter Funktionsblöcke,
- Verkauf z.B. als Prozessoren mit weniger Cache, ...

[5] Vorgriff auf Foliensatz F3, Poisson-Verteilung

Ersatziteration

Experimentelle Reparatur durch Ersatz

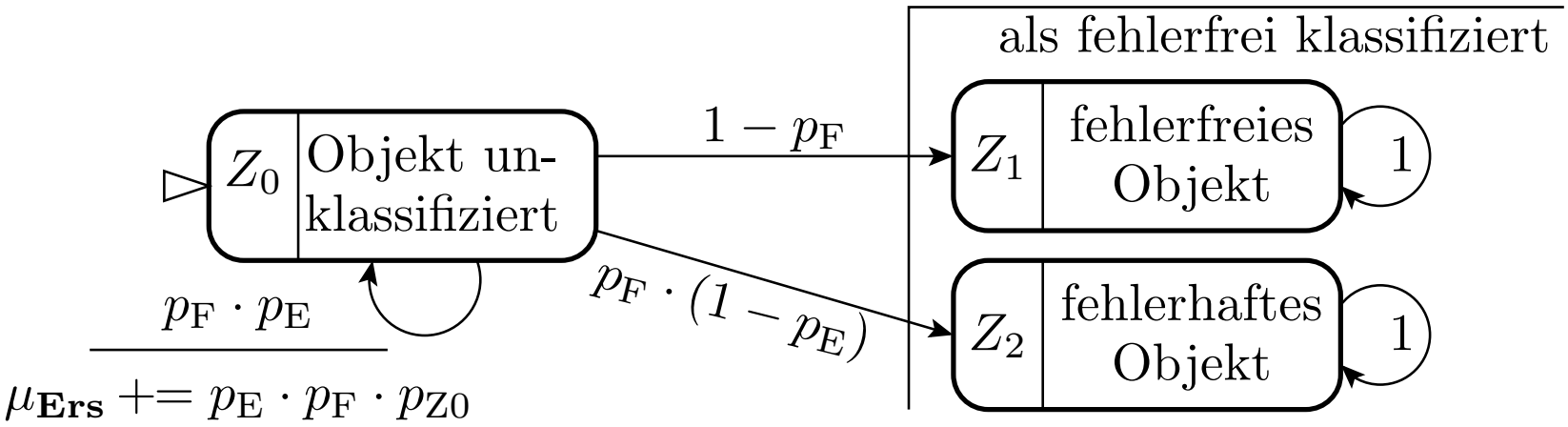


- Ersatzobjekte haben auch mit Wahrscheinlichkeit p_F Fehler.
- Diese entstehen unabhängig und sind unabhängig nachweisbar.

Insgesamt wird aus jedem unklassifizierten Objekt je Schritt mit Wahrscheinlichkeit:

- $1 - p_F$ ein fehlerfreies Objekt,
- $p_F \cdot (1 - p_E)$ ein nicht erkanntes fehlerhaftes Objekt,
- $p_F \cdot p_E$ bleibt es unklassifiziert.

Vereinfachte Markov-Kette



Nach Ersatz aller erkennbar defekten Objekte[6] :

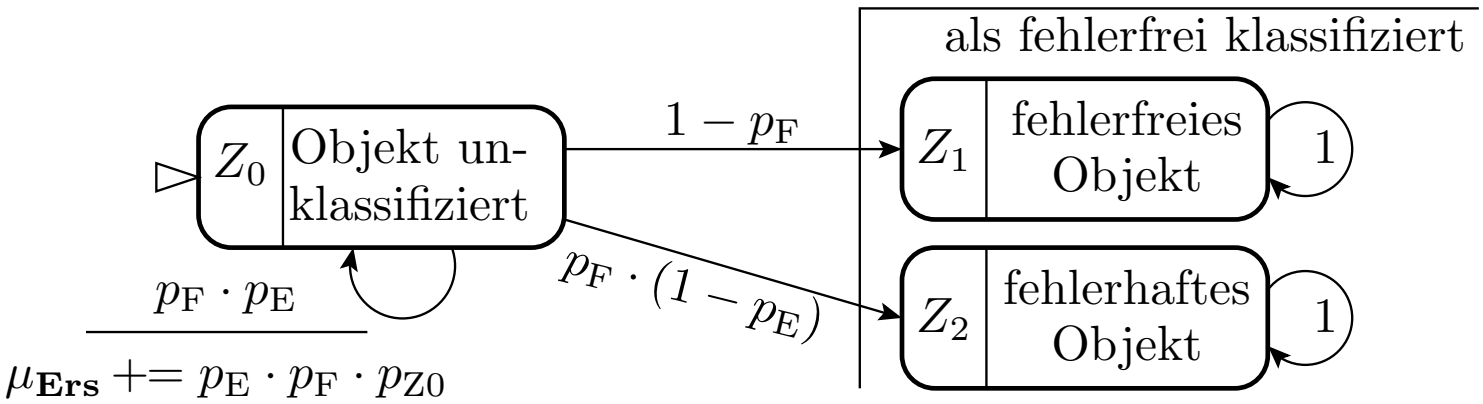
$$\lim_{n\to\infty}(p_{Z0}) = \lim_{n\to\infty}(p_F \cdot p_E)^n = 0$$

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

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

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

Abschätzbare Kenngrößen



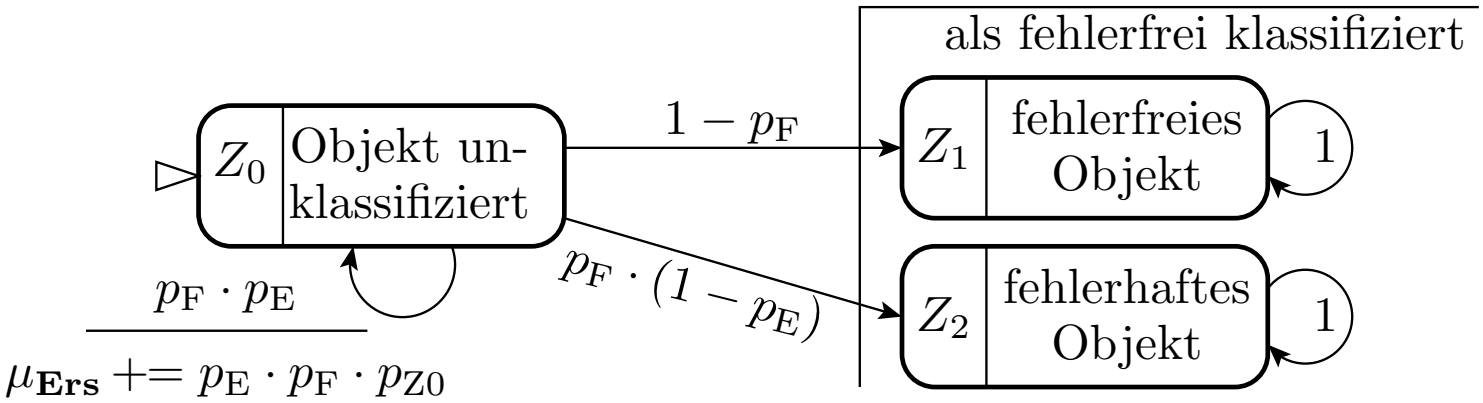
Wahrscheinlichkeit, dass ein als fehlerfrei ausgewiesenes Objekt fehlerhaft ist:

$$p_{FT} = \lim_{n \to \infty} (p_{Z2}) = \frac{p_F \cdot (1 - p_E)}{1 - p_F \cdot p_E} \approx DL_{Ers} \tag{3}$$

Wahrscheinlichkeit, dass ein Fehler nicht beseitigt wird:

$$p_{NBes} = \frac{p_{FT}}{p_F} = \frac{\frac{p_F \cdot (1 - p_E)}{1 - p_F \cdot p_E}}{p_F} = \frac{1 - p_E}{1 - p_F \cdot p_E} \approx \frac{DL_{Ers}}{DL_{EP}}$$

DL_{EP} – Fehleranteil nach Entstehungsprozess; DL_{Ers} – Fehleranteil nach Ersatz aller erkennbar defekten Objekte.



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

$$\mu_{\mathrm{Ers}} = \sum_{n=1}^{\infty} (p_F \cdot p_E)^n = \frac{p_F \cdot p_E}{1 - p_F \cdot p_E} \tag{4}$$

Zu erwartende Ausbeute[7]:

$$Y = \frac{1}{\mu_{\mathrm{Ers}} + 1} = 1 - p_F \cdot p_E \tag{5}$$

[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.

Beispielaufgabe

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

1. die zu erwartende Anzahl der Ersetzungen μ_{Ers}, bis der ausgewählte Schaltkreis durch den Test kommt und
2. die Wahrscheinlichkeit p_{F}, dass ein Schaltkeis vor dem Aussortieren fehlerhaft ist?
3. Wie groß ist die Wahrscheinlichkeit p_{FT}, dass ein nach der Fehlerbesitigung 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. 5:

$$\mu_{\mathrm{Ers}} = \frac{1}{Y} - 1$$

Y	10%	30%	50%	80%	90%
μ_{Ers}	9	2,33	1	0,25	0,11

2. Die Wahrscheinlichkeit p_{F}, dass ein Schaltkeis vor dem Aussortieren fehlerhaft ist, beträgt nach Gl. 5:

$$p_{\mathrm{F}} = \frac{1 - Y}{p_{\mathrm{E}}}$$

p_{E}	$Y = 10\%$	...=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%

Für $Y = 1 - p_{\mathrm{E}}$ sind alle gefertigten Schaltkreise defekt.

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. 3:

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

	$p_{\mathrm{E}} = 90\%$	$p_{\mathrm{E}} = 99\%$	$p_{\mathrm{E}} = 99{,}9\%$
$p_{\mathrm{F}} = 100\%$	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

Für den Fehleranteil getesteter Schaltkreise $DL_{\mathrm{T}} \approx p_{\mathrm{FT}}$ findet man in der Literatur die Größenordnung 100 ... 300 dpm. Für $Y = 30\%..80\%$ leiten sich daraus Fehlerüberdeckungen $FC \approx p_{\mathrm{E}} > 99{,}9\%$ ab.

Reparaturiteration

Fehlerbeseitigung durch Reparatur

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

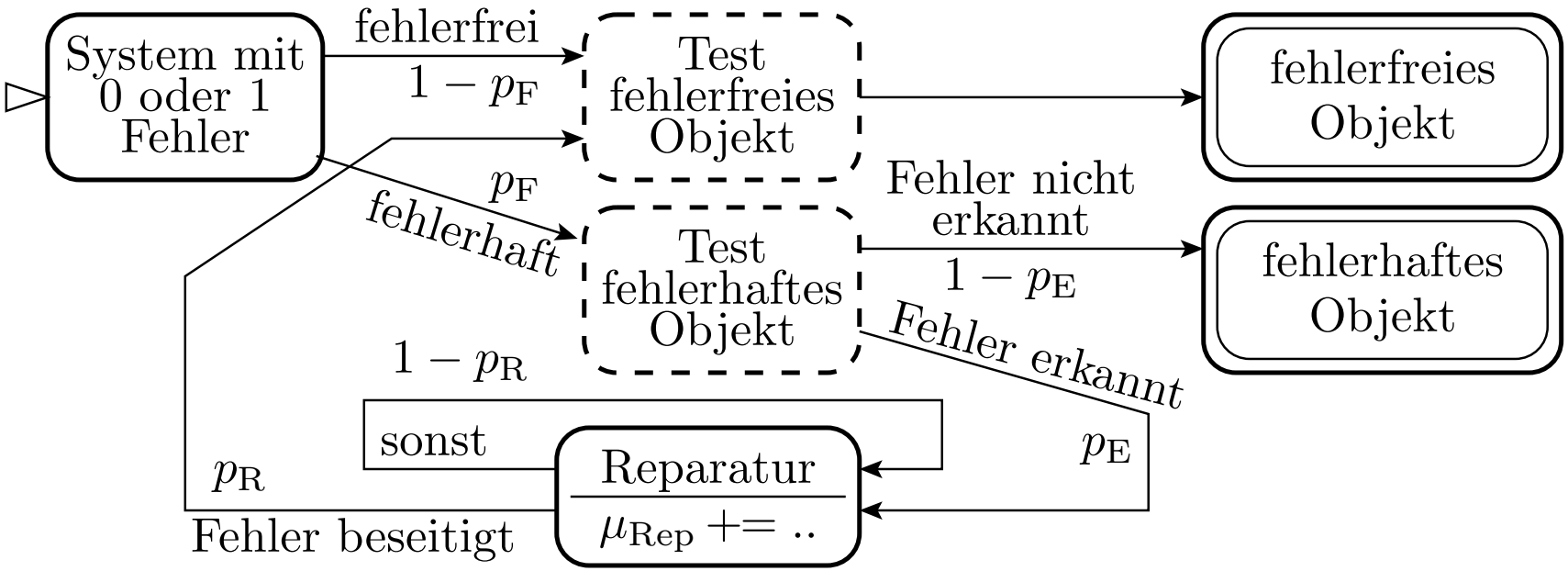
- sind billiger als zu ersetzende Gesamtsysteme und
- haben einen kleineren Fehleranteil (weniger Mehrfachersetzungen).

Dafür verlangt Reparatur Zusatzaufwändungen:

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

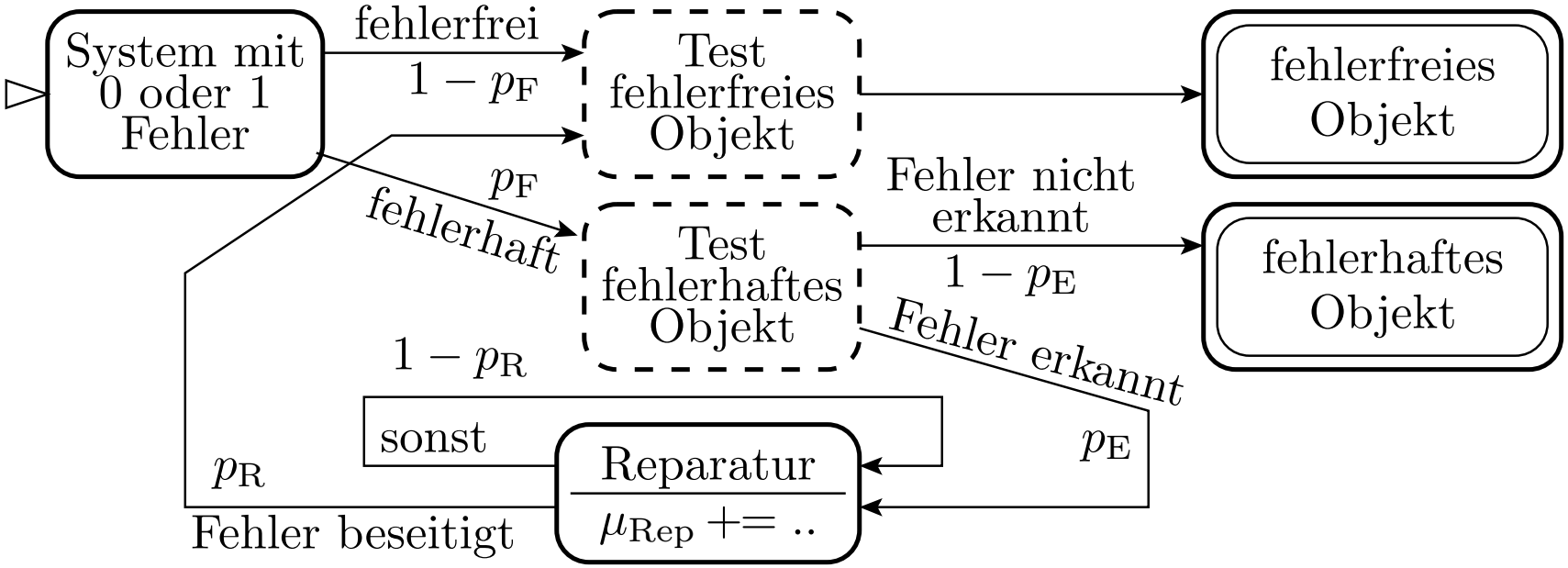
Für Systeme mit Ausbeute $Y > 50$ unrentabel.

Beseitigungsiteration für einen Fehler



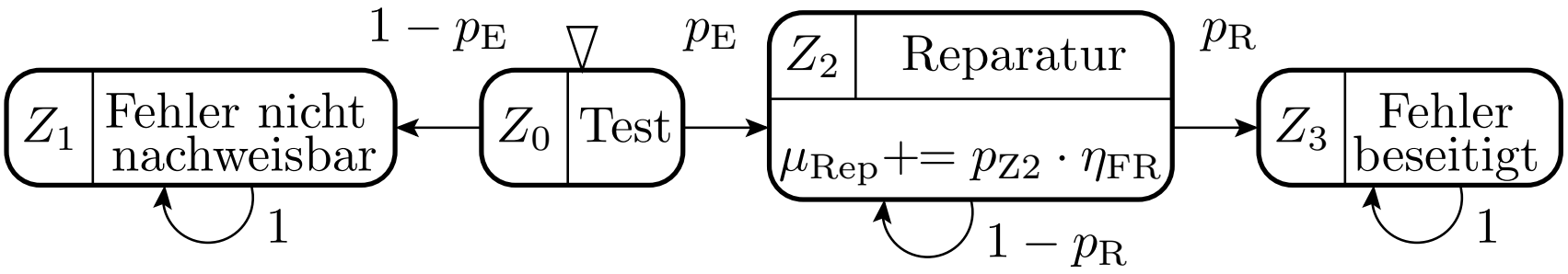
- Bei einem erkennbaren Fehler wird solange mit einer Erfolgswahrscheinlichkeit p_R repariert, bis das vom Test nachweisbare Fehlverhalten beseitigt ist.

μ_{Rep}+= .. Aufsummieren der Wahrscheinlichkeiten, dass ein neuer Fehler entsteht.



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

Verbesserte Markov-Kette je Fehler



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

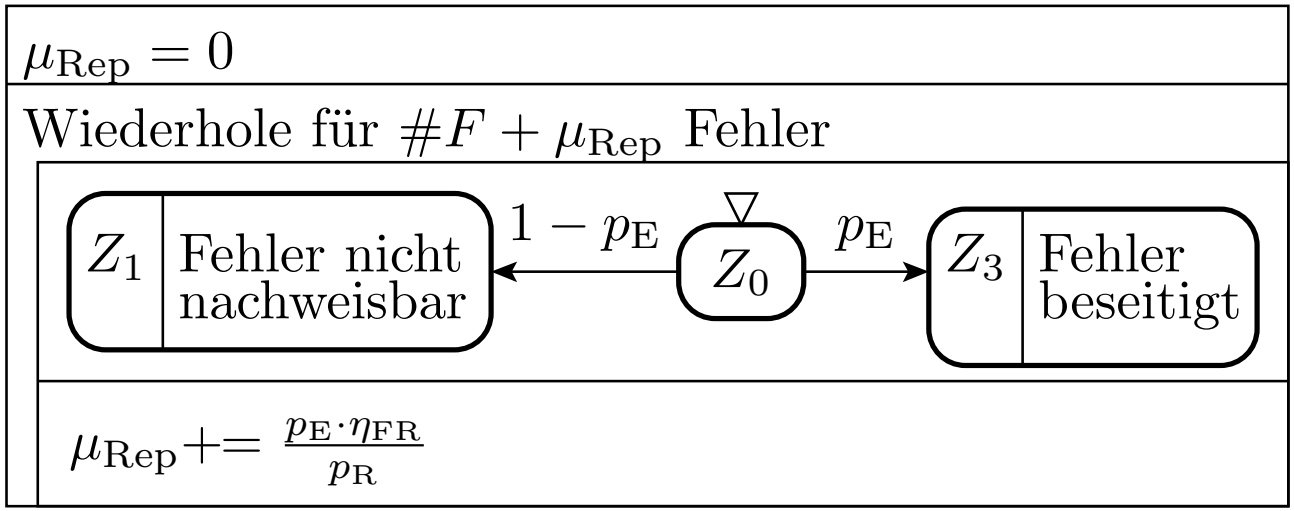
$$p_B = p_{Z3} = p_E \cdot p_R \cdot \sum_{n=0}^{\infty} (1 - p_R)^n = p_E \tag{6}$$

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

$$\mu_{Rep} = p_E \cdot \eta_{FR} \cdot \sum_{n=0}^{\infty} (1 - p_R)^n = \frac{p_E \cdot \eta_{FR}}{p_R} \tag{7}$$

η_{FR} – Anz. entstehende Fehler je Reparaturversuch.

Systeme mit $\#F$ potentiellen Fehlern



- Je eine Markov-Kette für die Beseitigungsiteration eines Fehlers.
- Jeder erkennbare Fehler wird beseitigt: $p_{\text{B}} = p_{\text{E}}$
- Anzahl der neuen Fehler je beseitigter Fehler: $\mu_{\text{Rep}} = \frac{p_{\text{E}} \cdot \eta_{\text{FR}}}{p_{\text{R}}}$

Gesamtanzahl der entstehenden Fehler für $\mu_{\text{Rep}} < 1$:

$$\#F_{\text{ges}} = \#F \cdot (1 + \mu_{\text{Rep}} \cdot (1 + \mu_{\text{Rep}} \cdot (1 + \ldots)))$$

$$= \#F \cdot \sum_{i=0}^{\infty} (\mu_{\text{Rep}})^i = \frac{\#F}{1 - \mu_{\text{Rep}}}$$

Zu erwartende Fehleranzahl nach der Beseitigungsiteration:

$$\#F_{\mathrm{TB}} = \#F_{\mathrm{ges}} \cdot (1 - p_{\mathrm{E}}) = \frac{\#F \cdot (1 - p_{\mathrm{E}})}{1 - \mu_{\mathrm{Rep}}} = \frac{\#F \cdot (1 - p_{\mathrm{E}})}{1 - \frac{p_{\mathrm{E}} \cdot \eta_{\mathrm{FR}}}{p_{\mathrm{R}}}}$$

Fälle:

1. $\mu_{\mathrm{Rep}} < 0{,}1$: Verringerung der Fehleranzahl nahezu um die Fehlernichterkennungswahrscheinlichkeit $1 - p_{\mathrm{E}}$:

$$\#F_{\mathrm{TB}} = \frac{\#F \cdot (1 - p_{\mathrm{E}}) \cdot (1 + \mu_{\mathrm{Rep}})}{(1 - \mu_{\mathrm{Rep}}) \cdot (1 + \mu_{\mathrm{Rep}})} = \frac{\#F \cdot (1 - p_{\mathrm{E}}) \cdot (1 + \mu_{\mathrm{Rep}})}{1 - \mu_{\mathrm{Rep}}^2}$$
$$\approx \#F \cdot (1 - p_{\mathrm{E}}) \cdot (1 + \mu_{\mathrm{Rep}})$$

2. $\eta_{\mathrm{FR}} = p_{\mathrm{R}}$: Die Fehleranzahl bleibt konstant. Alle erkennbaren Fehler werden zwar beseitigt, aber bei der Beseitigung von jedem erkennbaren Feher entsteht im Mittel ein neuer nicht erkennbarer Fehler. Die Iteration endet, wenn alle erkennbaren Fehler beseitigt sind mit $\#F_{\mathrm{TB}} = \#F$.
3. $\eta_{\mathrm{FR}} > p_{\mathrm{R}}$: Es entstehen mehr neue Fehler als beseitigt werden. Für $\frac{p_{\mathrm{E}} \cdot \eta_{\mathrm{FR}}}{p_{\mathrm{R}}} < 1$ endet der Reparaturprozess mit »kein weiterer nachweisbarer Fehler«, sonst auch Zunahme der Anzahl der nachweisbaren Fehler.

Gute studentische Programmierarbeit

- Fehlerarme Programmierung: $\#F = 5$ Fehler (ohne Syntaxfehler).
- Gründlicher Test, z.B.: $p_\mathrm{E} = 50\%$ mit $n = 10$ Tests.
- Brauchbare Fehlerbeseitigung: 2 bis 3 Reparaturversuche je Fehler ($p_\mathrm{R} = 40\%$), ein neuer Fehler je 10 Reparaturversuche, der nicht durch Rückbau beseitigt wird ($\eta_\mathrm{Rep} = 0{,}1$).
- Abnahmeexponent der $\#F_\mathrm{TB}\,(n)$ mit Testsatzlänge $k = 0{,}5$:

$$\#F_\mathrm{TB} \approx \#F \cdot \frac{(1 - p_\mathrm{E})}{1 - \frac{p_\mathrm{E} \cdot \eta_\mathrm{FR}}{p_\mathrm{R}}} = 5 \cdot \frac{(1 - 50\%)}{1 - \frac{50\% \cdot 0{,}1}{40\%}} = 3{,}75$$

$$\zeta_\mathrm{F} \approx \frac{k \cdot \#F_\mathrm{TB}}{(k+1) \cdot n} = \frac{0{,}5 \cdot 3{,}75}{1{,}5 \cdot 10} = \frac{1\,\mathrm{FF}}{8\,\mathrm{SL}}$$

- Im Mittel 2,5 ursprüngliche plus 1,25 bei der Reparatur entstandene nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel wird mit einer Wahrscheinlichkeit von $\approx 7/8$ korrekt abgearbeitet. Für eine studentische Leistung gut genug.

Schlechte studentische Programmierarbeit

- Doppelte Fehleranzahl: $\#F = 10$ Fehler (ohne Syntaxfehler).
- Weniger Tests: $p_{\mathrm{E}} = 30\%$ mit $n = 5$ Tests.
- Schlechtere Fehlerbeseitigung: im Mittel 3 bis 4 Reparaturversuche je Fehler ($p_{\mathrm{R}} = 30\%$), kein Rückbau nach erfolglosen Reparaturversuchen, angenommen $\eta_{\mathrm{Rep}} = 0{,}5$.
- Abnahmeexponent der $\#F_{\mathrm{TB}}\,(n)$ mit Testsatzlänge $k = 0{,}5$:

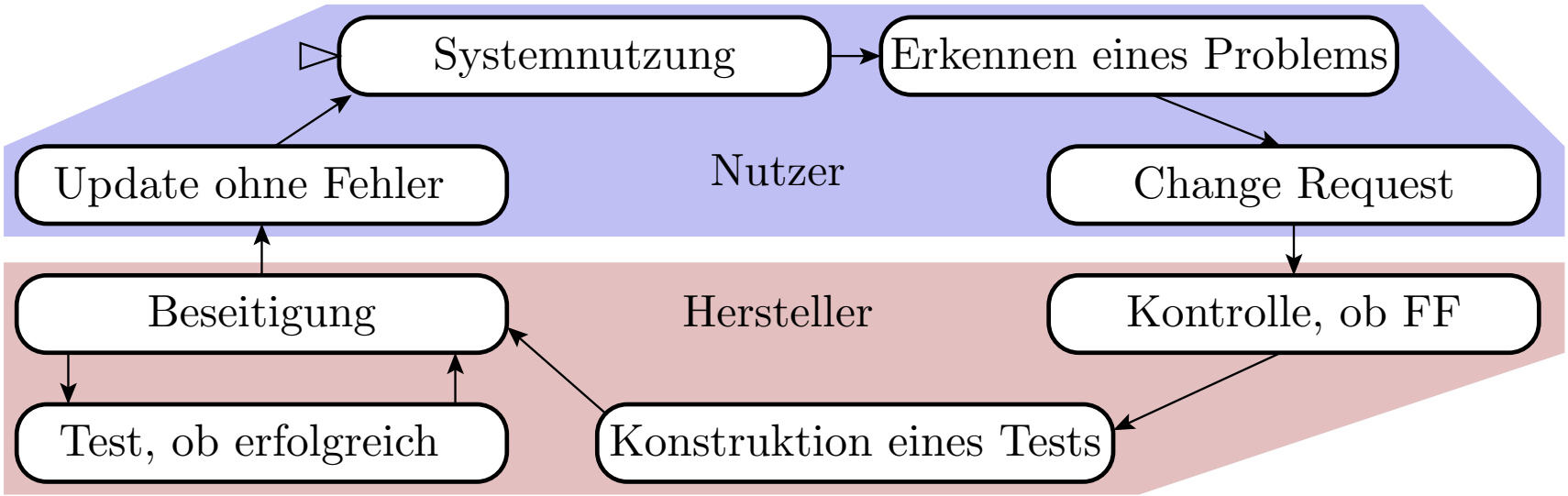
$$\#F_{\mathrm{TB}} \approx \#F \cdot \frac{(1 - p_{\mathrm{E}})}{1 - \frac{p_{\mathrm{E}} \cdot \eta_{\mathrm{FR}}}{p_{\mathrm{R}}}} = 10 \cdot \frac{(1 - 30\%)}{1 - \frac{30\% \cdot 0{,}5}{30\%}} = 14\,\mathrm{Fehler}$$

$$\zeta_{\mathrm{F}} \approx \frac{k \cdot \#F_{\mathrm{TB}}}{(k+1) \cdot n} = \frac{0{,}5 \cdot 14}{1{,}5 \cdot 5} = \frac{14\,\mathrm{FF}}{15\,\mathrm{SL}}$$

- Im Mittel 7 ursprüngliche plus 7 bei der Reparatur entstandene nicht erkannte Fehler.
- Ein weiteres zufälliges Testbeispiel wird nur mit Wahrscheinlichkeit nahe null korrekt abgearbeitet.
- Wie Prüfung bestehen? Erhöhung auf $n = 10$ Tests plus Rückbau nach erfolglosen Fehlerbeseitigungsversuchen ($\eta_{\mathrm{Rep}} = 0{,}2$).

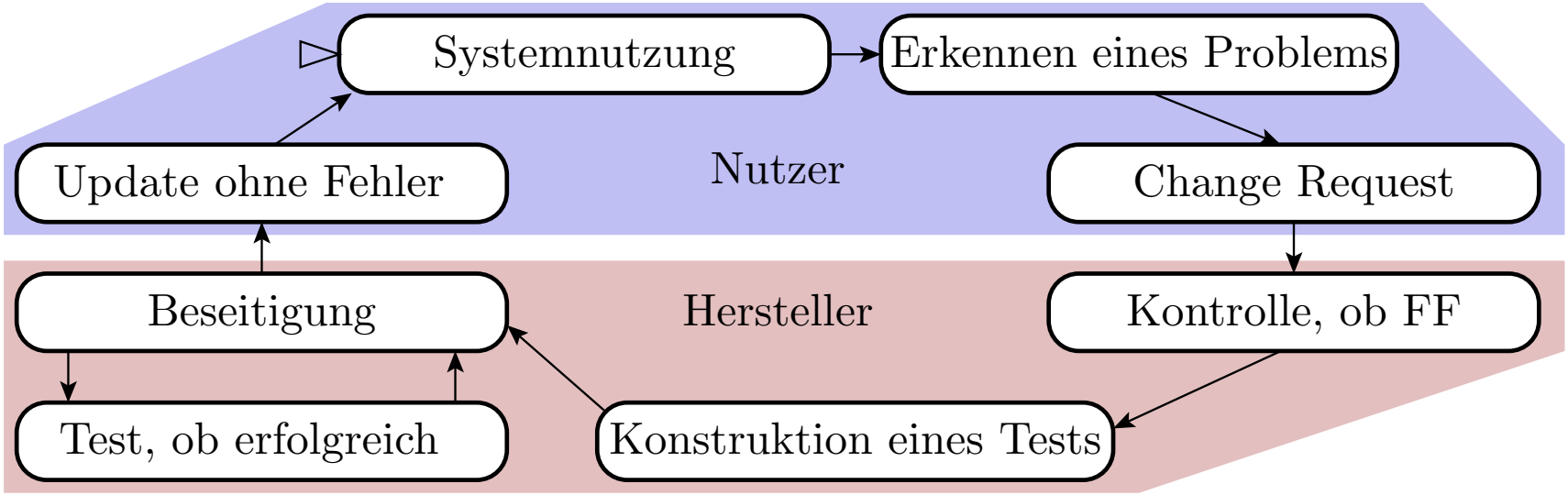
Reifeprozesse

Beseitigung in einem Reifeprozess (Wiederholung)



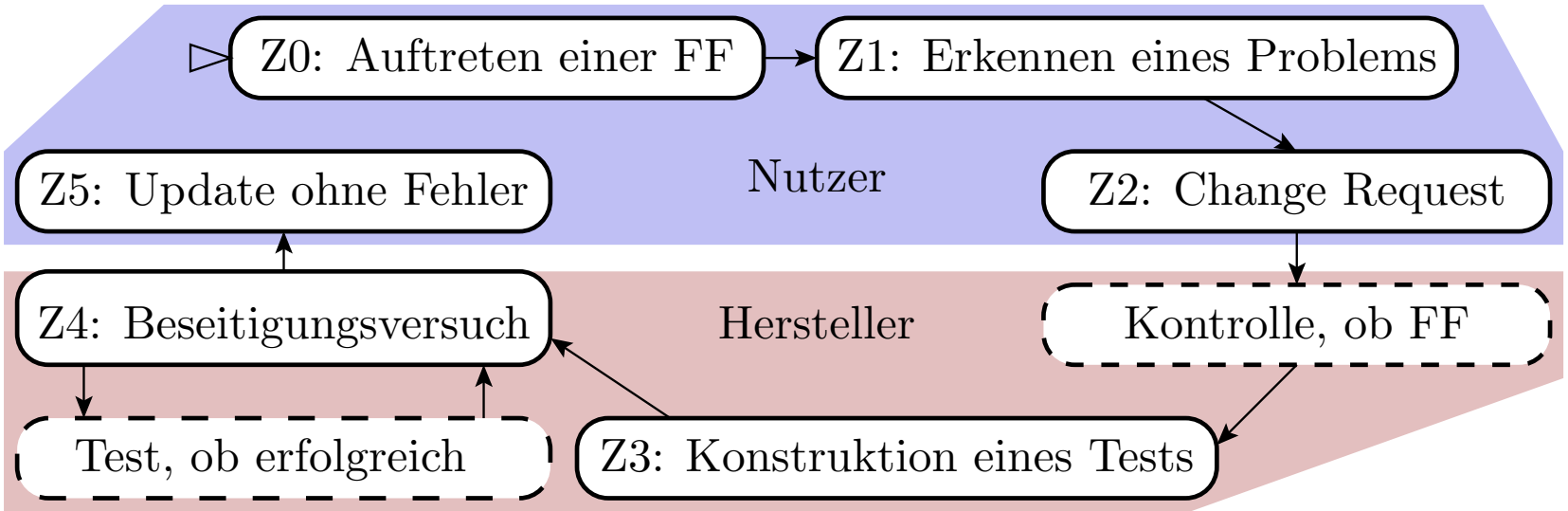
Fehlerbeseitigungsiteration für von Anwendern beobachtete FF:

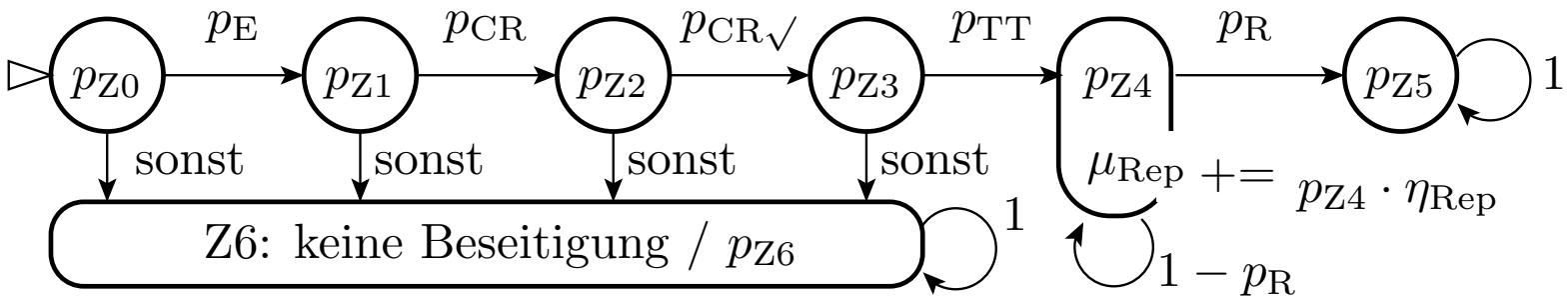
- Erfassen der FF mit allen Daten, um die FF nachzustellen,
- Übermittlung an den Hersteller,
- Priorisierung, Fehlersuche und Beseitigung,
- Herausgabe und Einspielung von Updates.



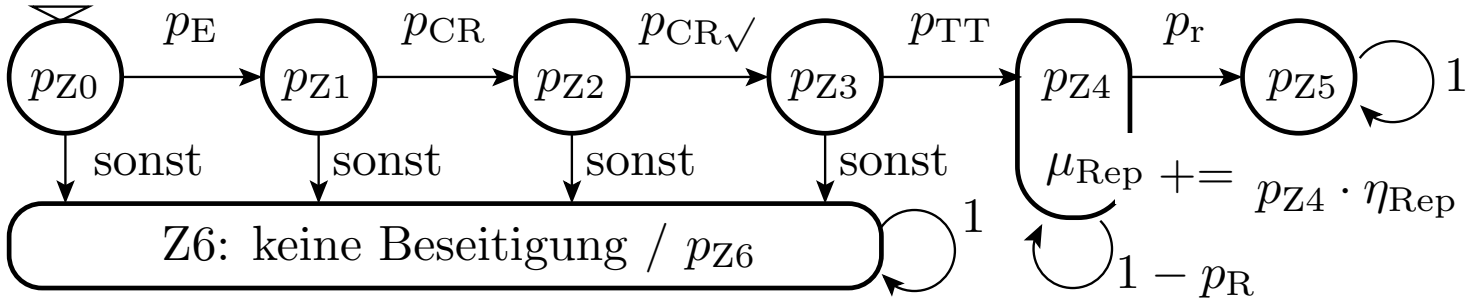
- Bei einer vermuteten Fehlfunktion stellt der Nutzer einen Änderungsanforderung (Change Request).
- Der Hersteller prüft diese, selektiert daraus FFs und versucht, für jede FF reproduzierbare Testbeispiele zu finden.
- Die Testbeispiele dienen zur Fehlerlokalisierung und zur Erfolgskontrolle nach jedem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

Modellierung als Markov-Kette





μ_{Rep}+= .. Aufsummieren der Wahrscheinlichkeiten, dass ein neuer Fehler entsteht.



Wahrscheinlichkeiten:

- p_E: Erkennungswahrscheinlichkeit je SL, Zufallstest
- p_{CR}: Änderungsanforderung wird gestellt
- $p_{CR\surd}$: 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:

$$p_B = p_E \cdot p_{CR} \cdot p_{CR\surd} \cdot p_{TT}$$

Mit dem Kantenzähler μ_{Rep} wird wie bei »Fehlerbeseitigung durch Reparatur« die zu erwartende Anzahl der Fehler abgeschätzt, die während des Reifeprozesses neu entstehen. Diese kommen mit in den Reifeprozess, aber mit einer vom Entstehungszeitpunkt abhängigen Reifedauer ... Kann kompliziert werden.

Fehlerentstehung

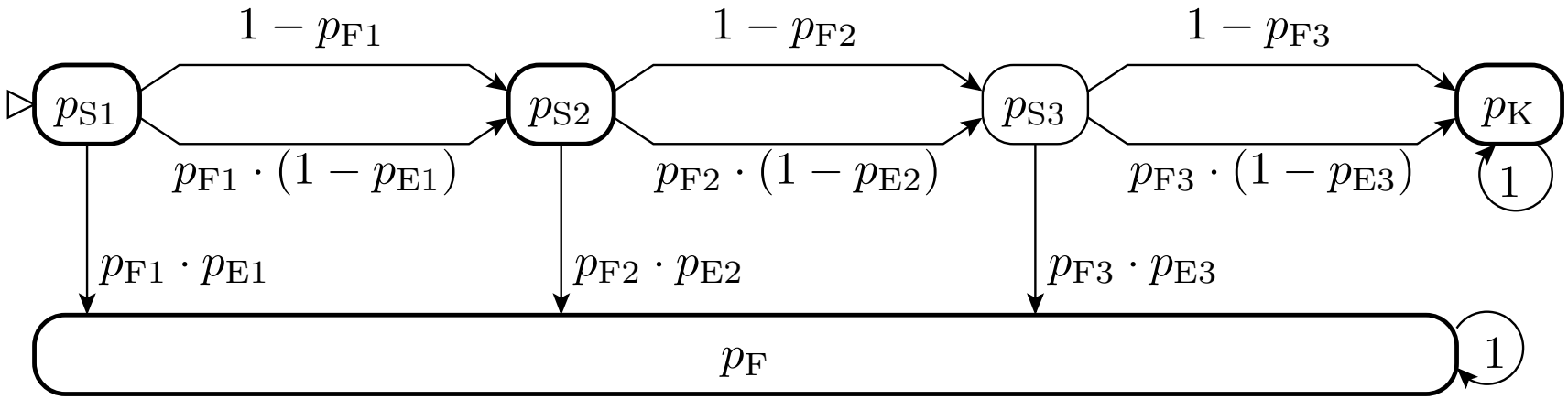
Fehlerentstehung

- Einfaches Abschätzungsmodell über Metriken, z.B. »Anz_NLOC * Fehler_je_NLOC«.
- Näher am Entstehungsprozess »Anz_Prozessschritte * Prozessgüte«
- Beschreibung der Fehlerentstehung durch Markov-Ketten (einer Markov-Kette je Fehler). [8]
- Beschreibung der Produktentstehung durch Markov-Ketten mit Kantenzählern für die zu erwartende Anzahl der entstehenden Fehler.

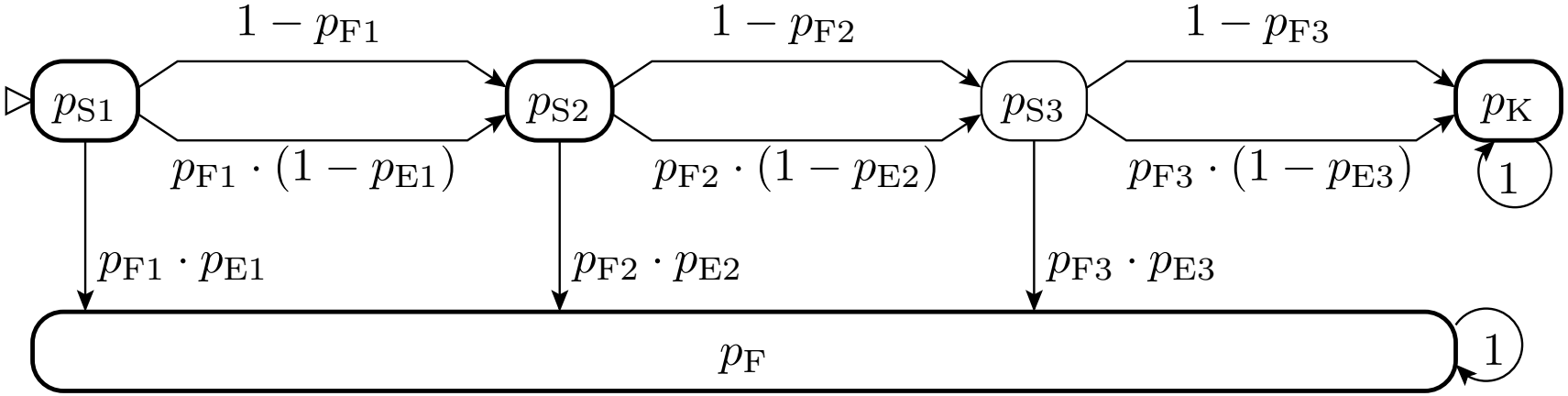
[8] Auf dem nächsten Foliensatz werden wir hierzu lernen, dass die zu erwartende Fehleranzahl gleich der Summe der Entstehungswahrscheinlichkeiten aller potentiellen Fehler ist.

Entstehungsprozesse mit Kontrollen

Lineare Folge von Entstehungsschritten. Wenn die Kontrolle i einen Fehler erkennt, wird das Objekt aussortiert, sonst Übergang zum nächsten Schritt ohne oder mit nicht erkennbarem entstandenen Fehler:



p_{Si} Wahrscheinlichkeit, dass Schritt i abgearbeitet wird.
p_{Fi} Wahrscheinlichkeit, dass in Schritt i ein Fehler entsteht.
p_{Ei} Fehlererkennungswahrscheinlichkeit der Kontrolle nach Schritt i.
p_K Wahrscheinlichkeit, dass Objekt nicht wegen Fehlers aussortiert.
p_F Wahrscheinlichkeit, dass das Objekt als fehlerhaft aussortiert wird.



Wahrscheinlichkeit, dass ein fehlerfreies Objekt entsteht:

$$p_{NF} = \prod_{i=1}^{3} (1 - p_{Fi})$$

Wahrscheinlichkeit, dass das Objekt nicht aussortiert wird:

$$p_K = \prod_{i=1}^{3} (1 - p_{Ei} \cdot p_{Fi})$$

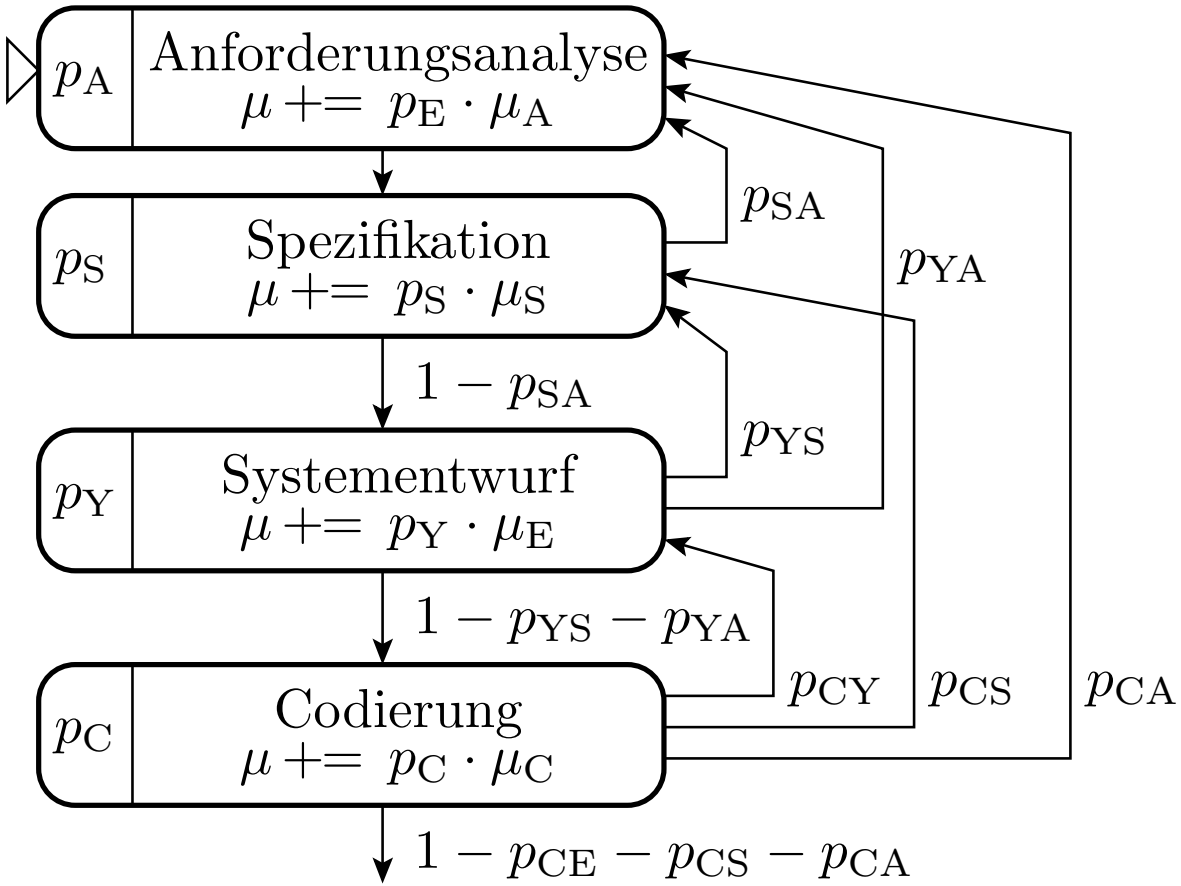
Fehleranteil, geschätzt als Wahrsch. »nicht aussortiert und fehlerhaft«:

$$DL \approx p_{FT} = 1 - \frac{p_{NF}}{p_K}$$

Ausbeute, geschätzt als Wahrscheinlichkeit »nicht aussortiert«:

$$Y = p_K$$

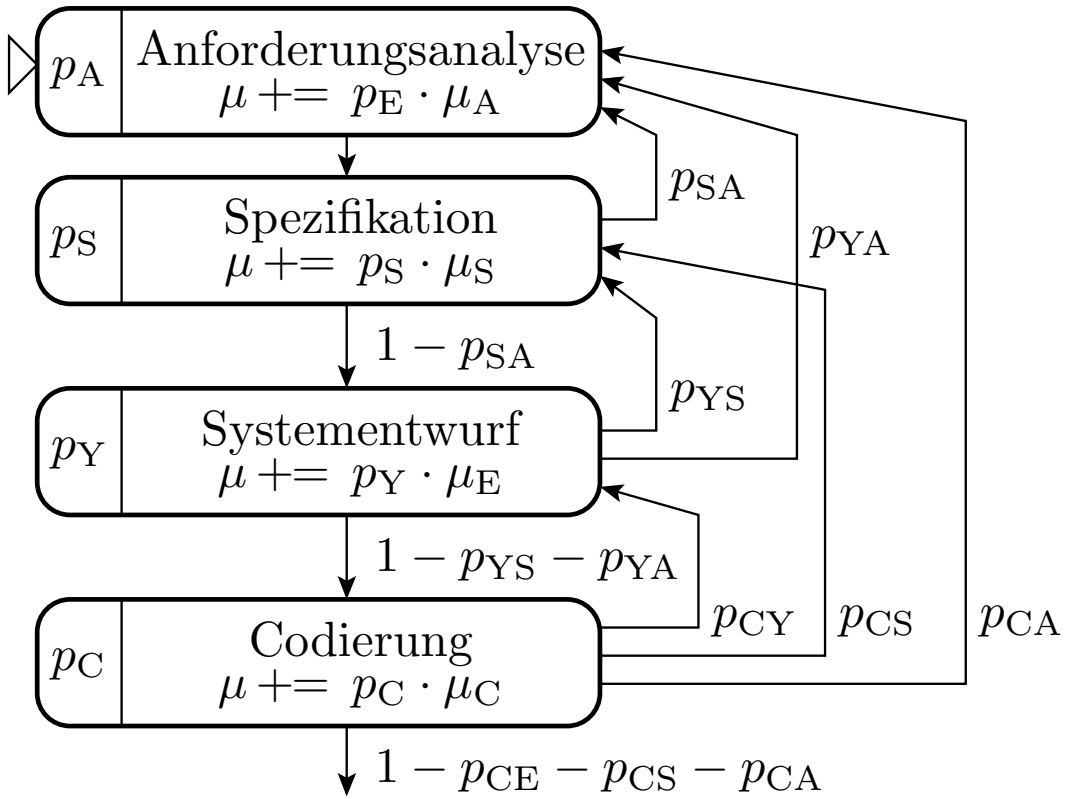
Entstehungsprozesse mit Rückgriffen



μ – Zähler für die zu erwartende Anzahl der entstehenden Fehler; μ_i – zu erwartende Anzahl entstehender Fehler in Entwurfsphase i;
p_{ij} – Rückgriffswahrscheinlichkeiten[9] von i nach j.

[9] Rückgriff: Wiederholung von Entwurfsschritten vorheriger Entwurfsphasen, wenn in späteren Phasen Fehler (oder Unschönheiten) erkannt werden.

Eine Simulation dieser vereinfachten Markov-Kette eines Phasenmodells wird zeigen, dass eine Erhöhung der Rückgriffwahrscheinlichkeiten insbesondere über mehrere Entwurfsphasen die zu erwartende Anzahl der entstehenden Fehler ab einem bestimmten Punkt explosionsartig in die Höhe schnellen lassen.



Dabei haben wir noch nicht berücksichtigt, dass die Rückgriffwahrscheinlichkeiten mit der Anzahl der entstehenden Fehler zunehmen. Vorgehensmodelle schränken deshalb Rückgriffsmöglichkeiten ein (vergl. TV_F1, Abschn. 4.3 Projekte, Vorgehensmodelle).