Test und Verlässlichkeit Grosse Übung zu Foliensatz 1

Prof. G. Kemnitz

31. Mai 2018

Contents

1 Modelle und Begriffe

1.1 Service-Modell

Aufgabe 1.1: Service-Modell, Sicherung der Verl.

1. Was besagt das in der Vorlesung definierte Service-Modell und welche Eigenschaften von Systemen vernachlässigt es als unwesentlich.
2. Wie lauten die drei Ebenen zur Sicherung der Verlässlichkeit?

Zur Kontrolle

1. Ein Service ist eine Vorgang, der in zeitdiskreten Schritten aus Eingaben Ausgaben erzeugt, die richtig oder FFs sein können. Als unwesentlich vernachlässigt werden Funktion und Realisierung.
2. Die drei Ebenen zur Sicherung der Verlässlichkeit:
   - Fehlervermeidung während der Entstehungsprozesse durch Prozessüberwachung und Beseitigung von Ursachen für die Fehlerentstehung,

- Test und Fehlerbeseitigung vor und während des Einsatzes und
- während des Einsatzes Überwachung von Service- und Teil-Service-Leistungen + Schadesbegrenzung, Wiederholung, ... bis zur Ergebniskorrektur bei nicht erbrachten SL und erkannten Fehlfunktionen.

Aufgabe 1.2: Determinismus, Gedächtnis

1. Was ist die Grundregel des prüfgerechten Entwurfs für eine nicht-deterministische Zielfunktion?
2. Welche Maßnahmen sich erforderlich, damit ein System mit Gedächtnis wie eines ohne Gedächtnis getestet werden kann.

Zur Kontrolle

1. Überwiegende Nachbildung auf separat testbare deterministische SL. Beschränkung von Zufallsentscheidungen auf eine Initialisierung.
2. Mit einem Lese- und Schreibzugriff auf alle Zustandsdaten kann eine Funktion mit Gedächtnis wie eine ohne getestet werden.

Aufgabe 1.3: Initialisierungsfehler

Das nachfolgende Programm zur Aufsummierung von »len« Werten hat einen Initialisierungsfehler:

```
int bilde_summe(int *dat, uint8_t len){
 int sum;
 while(len){
  sum += *dat;
  dat++; len--;
 }
 return sum;
}
```

1. Arbeitet das Programm deterministisch?
2. Hat das Programm ein Gedächtnis?

Zur Kontrolle

Programm zur Summenbildung:

1. Die Soll-Funktion arbeitet deterministisch, das fehlerhafte Programm nicht.
2. Laut Soll-Funktion ist das Ergebnis nur eine Funktion der Eingabe, d.h. kein Gedächtnis.

1.2 Fehler und Fehlfunktionen

Aufgabe 1.4: Fehlfunktionen, Fehler, Hierarchie

1. Wie lauten die Definitionen für Fehlfunktion und Fehler?
2. Was steckt hinter der Redensart »It not a Bug, it is a Feature!« in Bezug die Beriffsdefinition für Fehlfunktionen.
3. Warum haben IT-Systeme i. Allg. eine hierarchische Struktur?

Zur Kontrolle

1. Definitionen für Fehler und FF:
   - Eine FF ist eine fehlerhaft ausgeführte SL.
   - Fehler sind beseitigbare Ursache für das Entstehen von FF.
2. Die Redensart »It not a Bug, it is a Feature!« deutet darauf hin, dass es in der Praxis oft Interpretationsspielraum gibt, was als richtige/fehlerhafte Ausführung einer SL zählt.
3. Gründe für die hierarchische Struktur von IT-Systemen:
   - Verkleinert die Beschreibungsgröße auf die der Komponenten und Verbindungen.
   - Verringerung des Entwurfsaufwands durch Mehrfachnutzung von Teilentwürfen und deren Testlösungen und Testsätzen.
   - Verringerter Entwurfsaufwand verringert die zu erwartende Anzahl der entstehenden Fehler.
   - Fehlerbeseitigung durch Komponentenaustausch, ...

Aufgabe 1.5: Nicht gefundene Fehler, Pareto-Prinzip

1. Was soll in der Vorlesung im Weiteren als potentielle Fehler gezählt werden?
2. Wie groß ist die zu erwartende Fehleranzahl in einem Programm mit 10^5 NLOC (Netto Lines of Code) bei einer Fehlerentstehungsrate von 40 Fehlern je 1000 NLOC mindestens, wenn der Test 80% der Fehler erkennt?
3. Was besagt das Pareto-Prinzip für nicht beseitigte Fehler?

Zur Kontrolle

1. Potentielle Fehler können in der Vorlesung Entstehungs-SL oder Reperaturmöglichkeiten sein.
2. Von der zu erwartenden Anzahl der entstehenden Fehler
   $$10^5\,\text{NLOC} \cdot 40\,\frac{\text{Fehler}}{\text{NLOC}} = 4000\,\text{Fehler}$$
   startet nur für die 80% der erkannten Fehler ein Beseitigungsversuch. Mindestens die 20% unentdeckte Fehler bleiben im System. Zu erwartende Fehleranzahl im Einsatz ≥ 800.
3. Das Pareto-Prinzip besagt, dass ein kleiner Teil der nicht beseitigten Fehler den größten Teil der FF im Einsatz verursacht.

1.3 Modellfehler

Aufgabe 1.6: Potenzielle und Modellfehler

Was sind die wesentlichen Unterschiede zwischen Modellfehlern und potentiellen Fehlern?

Zur Kontrolle

- Potentielle Fehler sind eine abzählbare Menge von Fehlermöglichkeiten
  - Entstehungsschritte (die Herstellung eines Schaltkreises und das Schreiben einer Programmanweisung, ...) oder
  - kleinste lokalisierbare Fehlermöglichkeiten (Schaltkreis defekt, Anweisung falsch, ...)

  Ein potentieller Fehler kann die unterschiedlichsten Wirkungen haben.
- Modellfehler sind (simulierbare) Fehlermöglichkeiten mit exakt beschriebenem Fehlverhalten.

Aufgabe 1.7: Fehlermodell

Fehlermodell: Jeder variable Operand eines Ausdrucks soll einmal um eins erhöht (Modellfehlertyp »+1«) und einmal um eins verringert sein (Modellfehlertyp »-1«). Für dereferenzierte Zeiger sind beide Modellfehler je für den Wert und die Adresse zu unterstellen.

```
Z1: int bilde_summe(int *dat, uint8_t len){
Z2:  int sum = 0;
Z3:  while(len){
Z4:   sum = sum + *dat;
Z5:   dat = dat + 1;
Z6:   len = len -1;
     }
Z7:  return sum;
    }
```

1. Auflisten der verfälschten Programmzeilen für alle Modellfehler.
2. Welche dieser Modellfehler sind identisch nachweisbar?

Zur Kontrolle

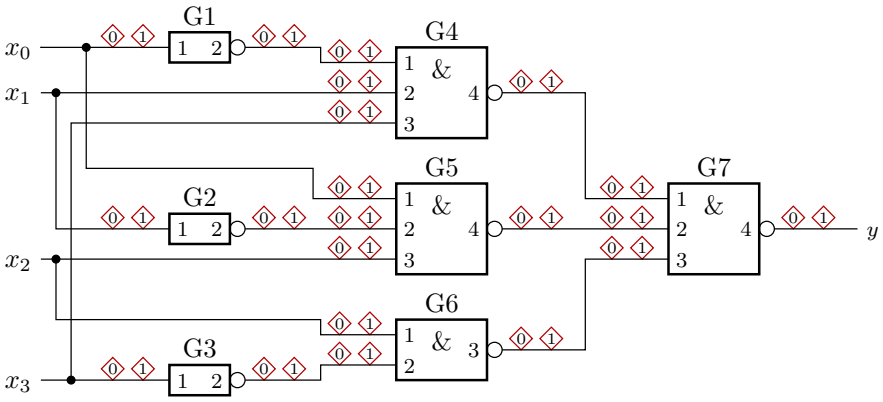
1. Modellfehler und verfälschte Programmzeilen:

	Modellfehlertyp »-1«	Modellfehlertyp »+1«
Z2 sum	sum = -1	sum = 1
Z3 len	while(len-1){	while(len+1){
Z4 sum	sum = (sum-1) + *dat;	sum = (sum+1) + *dat;
Z4 dat val	sum = sum + (*dat-1);	sum = sum + (*dat+1);
Z4 dat ref	sum = sum + *(dat-1);	sum = sum + *(dat+1);
Z5 dat	dat = (dat-1) + 1;	dat = (dat+1) + 1;
Z6 len	len = (len-1) - 1	len = (len+1) - 1
Z7 sum	return (sum-1);	return (sum+1);

2. Identisch nachweisbar sind »Z4 (sum-1)« und »Z4 (dat-1)« sowie »Z4 (sum+1)« und »Z4 (dat+1)«.

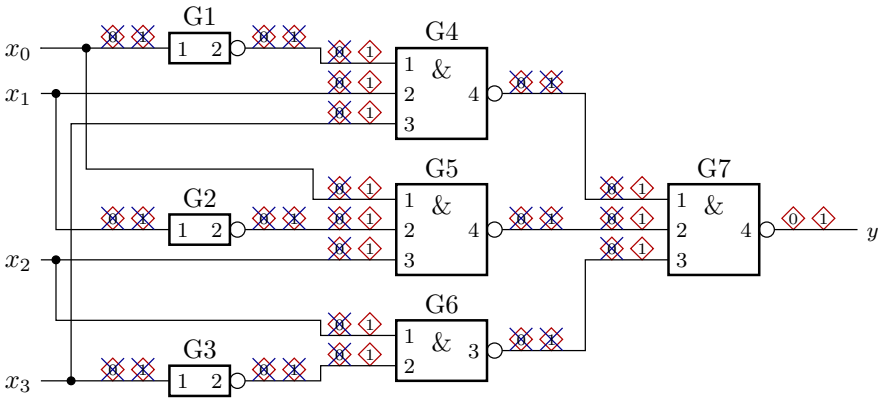
1.4 Haftfehlermodell

Aufgabe 1.8: Vereinfachung Haftfehlermenge



1. Streichen Sie alle identisch nachweisbaren Haftfehler.
2. Streichen Sie anschließend alle implizit nachweisbaren Haftfehler.

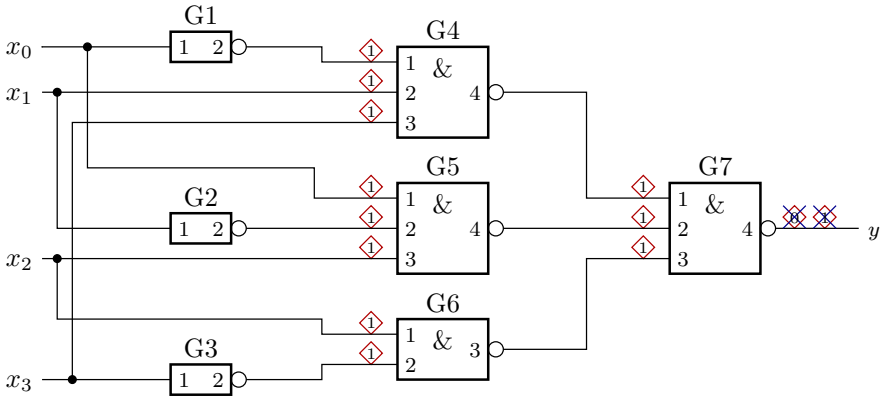
Zur Kontrolle Aufgabenteil 1



Identisch nachweisbare Haftfehler:

- sa0(G1-1), sa1(G1-2), sa1(G4-1)
- sa1(G1-1), sa0(G1-2), sa0(G4-1), sa1(G4-4), sa1(G7-1)
- ...

Zur Kontrolle Aufgabenteil 2



Impliziter Nachweis:

- sa0(G7-4): sa1(G7-1), sa1(G7-2), sa1(G7-3)
- sa1(G7-4): sa1(G4-1), sa1(G4-2), sa1(G4-3), sa1(G5-1), ...

2 Wahrscheinlichkeiten

2.1 Zufallsexperiment

Aufgabe 1.9: Zufallsexperiment

1. Was ist ein Zufallsexperiment?
2. Welchen Wertebereich haben die Ergebnisse nachfolgender Zufallsexperimente:
   - Ergebniskontrolle,
   - Korrektur falscher Ergebnisse,
   - Aufdecken eines Fehlers mit einem Test,
   - Messen der Zeit bis zum Ausfall?
3. Welche dieser Zufallsexpermente sind Bernoulli-Versuche?

Zur Kontrolle Aufgabenteil 1 und 2

1. Ein Zufallsexperiment ist ein Experiment mit mehreren möglichen Ergebnissen und zufälligem Ausgang.
2. Wertebereich der Zufallsexperimente:
   (a) Ergebniskontrolle {richtig, falsch, ...}.
   (b) Korrektur falscher Ergebnisse {erfolgreich, ...}.
   (c) Aufdecken eines Fehlers mit einem Test {ja, nein}.
   (d) Messen der Zeit bis zum Ausfall {Zeit größer null}.
3. Bernoulli Versuche sind die ersten 3 (a bis c), falls die Menge der möglichen Ergebnisse aus zwei begrenzt ist. Wenn der WB z.B. um ein dritte mögliches Ergebnis »nicht entscheidbar« erweitert wird, sind es keine Bernoulli-Versuche mehr.

Aufgabe 1.10: Würfelexperiment

X und Y seien die zufälligen Augenzahlen bei der Durchführung des Versuchs »würfeln mit zwei Würfeln«:

1. $X + Y > 8$
2. $X > Y$
3. $(X = 5) \wedge (Y < 5)$
4. $X \cdot Y$ ist durch drei teilbar.

Bestimmen Sie jeweils

- die möglichen Ergebnisse und deren Anzahl,
- die günstigen Ergebnisse und deren Anzahl,
- die Wahrscheinlichkeit bei gleicher Auftrittshäufigkeit aller möglichen Ergebnisse.

Zur Kontrolle Aufgabenteil 1 und 2

1. $X + Y > 8$
   - Anzahl der Möglichkeiten: 36
   - günstig: 3+6, 4+5, 4+6, 5+4, bis 5+6, 6+3 bis 6+6
   - Anzahl günstig: 1+2+3+4=10
   - Wahrscheinlichkeit: 10/36
2. $X > Y$
   - Anzahl der Möglichkeiten: 36
   - günstig: 2>1, 3>1, 3>2, 4>1 bis 4>3, 5>1 bis 5>4, 6>1 bis 6>5
   - Anzahl günstig: 1+2+3+4+5=15
   - Wahrscheinlichkeit: 15/36

Zur Kontrolle Aufgabenteil 3 und 4

3. $(X = 5) \wedge (Y < 5)$
   - Anzahl der Möglichkeiten: 36
   - günstig: (5,1) bis (5,4)
   - Anzahl günstig: 4
   - Wahrscheinlichkeit: 4/36

4. $X \cdot Y$ ist durch drei teilbar.
   - Anzahl der Möglichkeiten: 36
   - günstig: (3,1) bis (3,6), (1,3), (2,3), (4,3), (5,3), (6,1) bis (6,6), (1,6), (2,6), (4,6), (5,6)
   - Anzahl günstig: 20
   - Wahrscheinlichkeit: 20/36

2.2 Erwartungswert

Aufgabe 1.11: Erwartungswert, lin. Transformation

1. Die Fehler $i = 1$ bis 5 seien mit folgenden Wahrscheinlichkeiten nachweisbar:

Fehler	1	2	3	4	5
p_i	10%	20%	40%	50%	30%

   wie groß ist die zu erwartende Anzahl der nachweisbaren Fehler.

2. Kontrollieren Sie die Gleichungen zur linearen Transformation für den Erwartungswert:

$$E(a \cdot X + b) = a \cdot E(X) + b$$

Zur Kontrolle

1. Der Fehlernachweis wird durch je einen Bernoulli-Versuch mit der dem Erwartungswert $E(X_i) = p_i$ beschrieben. Der gesamte Erwartungswert ist die Summe der einzelnen Erwartungswerte:

$$E(X) = \sum_{i=1}^{5} p_i = 10\% + 20\% + 40\% + 50\% + 30\% = 1{,}5$$

2. Zu zeigen ist $E(a \cdot X + b) \stackrel{!}{=} a \cdot E(X) + b$. Kontrolle:

$$\begin{aligned} E(a \cdot X + b) &= \sum_{i=1}^{N} p_i \cdot (a \cdot x_i + b) \\ &= a \cdot \underbrace{\sum_{i=1}^{N} p_i \cdot x_i}_{E(X)} + b \cdot \underbrace{\sum_{i=1}^{N} p_i}_{1} \\ &= a \cdot E(X) + b \surd \end{aligned}$$

Aufgabe 1.12: Erwartungswert Datenstichprobe

Für eine Modellfehlermenge von 1000 Fehlern wurden für 10 verschiedene Zufallstestsätze derselben Länge die Anzahl der nicht nachweisbaren Fehler bestimmt:

Versuch i	1	2	3	4	5	6	7	8	9	10
Ergebnis $\varphi_{\mathrm{NErk}.i}$	58	49	40	54	67	35	34	57	47	66

Schätzen Sie den Erwartungswert der Datenstichprobe.

Zur Kontrolle

Erwartungswert der Datenstichprobe:

$$\begin{aligned} E(X) \approx \bar{x} &= \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \\ &= 50{,}7 \end{aligned}$$

2.3 Verkettete Ereignisse

Aufgabe 1.13: Verkettete Würfelereignisse

- Welche möglichen Ergebnisse hat das Zufallsexperiment »auswürfeln einer Zahl, bei einer Sechs darf ein zweites Mal gewürfelt werden«?
- Mit welcher Wahrscheinlichkeit tritt jedes der möglichen Ergebnisse ein?

Zur Kontrolle

mögliche Ergebnisse	Wahrscheinlichkeit
1 bis 5,	6^{-1}
6+1 bis 6+5	6^{-2}
6+6+1 bis 6+6+5	6^{-3}
...	...

Summe der Wahrscheinlichkeiten aller Möglichkeiten:

$$\frac{5}{6} + \frac{5}{6^2} + \frac{5}{6^3} + \ldots = 5 \cdot \sum_{i=1}^{\infty} 6^{-i} = 5 \cdot \frac{\frac{1}{6}}{1 - \frac{1}{6}} = 1 \surd$$

Aufgabe 1.14: Fehlfunktionen und Fehlernachweis

Ein System habe vier Fehler, die unabhängig von einander mit den Wahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 20\%$, $p_3 = 5\%$ und $p_4 = 1\%$ eine Fehlfunktion je Service-Leistung verursachen.

1. Wie hoch ist die Wahrscheinlichkeit p_{FFF} einer durch Fehler verursachten Fehlfunktion je SL?
2. Wie hoch ist die Wahrscheinlichkeit, dass zehn Service-Leistungen korrekt ausgeführt werden?
3. Wie groß ist die Wahrscheinlichkeit für jeden der vier Fehler, dass er bei mindestens einer der zehn Service-Anforderungen eine FF verursacht?

Zur Kontrolle

1. Versagen einer einzelnen Service-Anforderung:

$$\begin{aligned} B &= A_1 \vee A_2 \vee A_3 \vee A_4 \\ B &= \overline{\bar{A}_1 \bar{A}_2 \bar{A}_3 \bar{A}_4} \\ P(B) &= 1 - 0{,}9 \cdot 0{,}8 \cdot 0{,}95 \cdot 0{,}99 = 23{,}3\% \end{aligned}$$

2. Korrekte Ausführung von zehn Service-Leistungen:

$$P(C) = (1 - P(B))^{10} = (1 - 23{,}3\%)^{10} = 2\%$$

3. Mindestens eine durch Fehler i verursachte FF bei zehn Service-Anforderungen:

$$\begin{aligned} P(D_1) &= 1 - (1 - 10\%)^{10} = 65\% \\ P(D_2) &= 1 - (1 - 20\%)^{10} = 89\% \\ P(D_3) &= 1 - (1 - \ 5\%)^{10} = 40\% \\ P(D_4) &= 1 - (1 - \ 1\%)^{10} = 9{,}6\% \end{aligned}$$

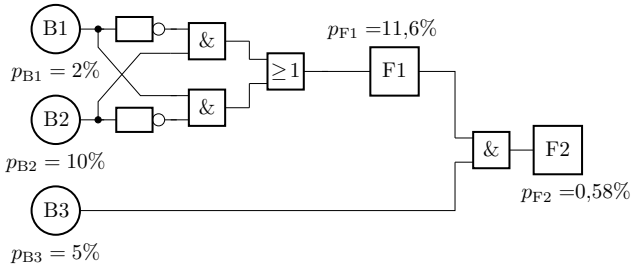
2.4 Fehlerbaumanalyse

Aufgabe 1.15: Fehlerbaumanalyse

1. Entwickeln Sie den Fehlerbaum für folgenden Zusammenhang:
   - Ereignis F_1 tritt ein, wenn entweder B_1 und nicht B_2 oder nicht B_1 und B_2 eintritt.
   - Das Ereignis F_2 tritt nur ein, wenn F_1 und B_3 eintreten.

2. Berechnen Sie die Wahrscheinlichkeit für F_1 und F_2 für den Fall, dass die Wahrscheinlichkeiten der Basisereignisse $p_{\mathrm{B1}} = 2\%$, $p_{\mathrm{B2}} = 10\%$ und $p_{\mathrm{B3}} = 5\%$ betragen.

Zur Kontrolle

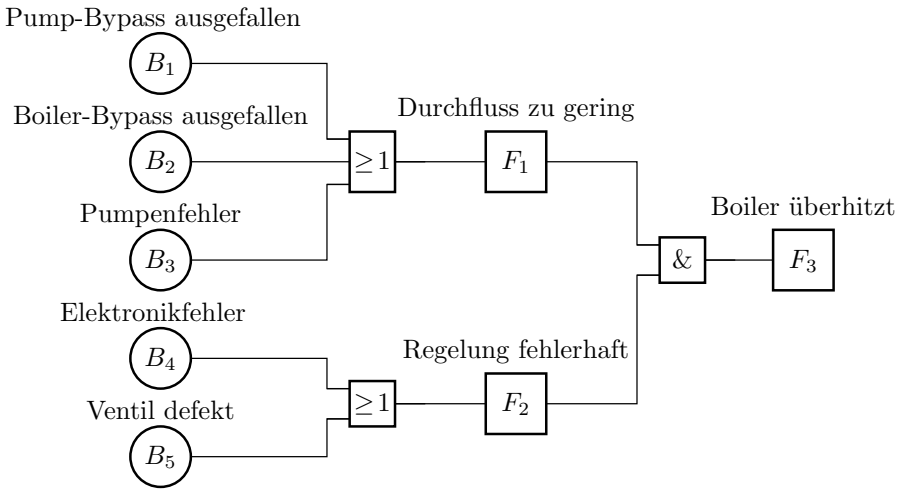


$$\begin{aligned} P\left(\mathrm{B1} \wedge \overline{\mathrm{B2}}\right) &= p_{\mathrm{B1}} \cdot (1 - p_{\mathrm{B2}}) = 2\% \cdot 90\% = 1{,}8\% \\ P\left(\mathrm{B2} \wedge \overline{\mathrm{B1}}\right) &= p_{\mathrm{B2}} \cdot (1 - p_{\mathrm{B1}}) = 10\% \cdot 98\% = 9{,}8\% \\ p_{\mathrm{F1}} &= P\left(\mathrm{B1} \wedge \overline{\mathrm{B2}}\right) + P\left(\mathrm{B2} \wedge \overline{\mathrm{B1}}\right)^{*} = 1{,}8\% + 9{,}8\% = 11{,}6\% \\ p_{\mathrm{F2}} &= P\left(\mathrm{F1} \wedge \mathrm{B3}\right) = 11{,}6\% \cdot 5\% = 0{,}58\% \end{aligned}$$

(* Die Bedingungen $\mathrm{B1} \wedge \overline{\mathrm{B2}}$ und $\mathrm{B2} \wedge \overline{\mathrm{B1}}$ schließen sich gegenseitig aus.)

Aufgabe 1.16: Auswerten eines Fehlerbaums

In dem nachfolgenden Fehlerbaum haben die Basisereignisse B_1 bis B_5 die geschätzen Wahrscheinlichkeiten $p_{\mathrm{B}i} \approx 0{,}1\%$ pro Tag.



Bestimmen Sie die Wahrscheinlichkeiten $p_{\mathrm{F}i}$ der Fehlerereignisse F_1 bis F_3 pro Tag.

Zur Kontrolle

$$
\begin{aligned}
p_{\mathrm{F1}} &= 1-(1-P(B_1))\cdot(1-P(B_2))\cdot(1-P(B_3)) \\
&\approx P(B_1)+P(B_2)+P(B_3) = 0,3\frac{\%}{\mathrm{Tag}} \\
p_{\mathrm{F2}} &= 1-(1-P(B_4))\cdot(1-P(B_5)) \approx 0,2\,\frac{\%}{\mathrm{Tag}} \\
p_{\mathrm{F3}} &= p_{\mathrm{F1}}\cdot p_{\mathrm{F2}} \approx 6\cdot 10^{-6}\,\mathrm{Tag}^{-1}
\end{aligned}
$$

2.5 Markov-Ketten

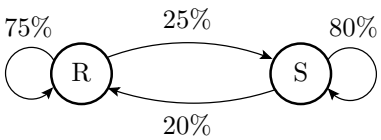
Aufgabe 1.17: Wettervorhersage mit Markov-Kette

Für ein Gebiet mit längeren Regen- und Trockenzeiten soll die Wettervorhersage für den nächsten Tag durch eine Markov-Kette mit den zwei Zuständen R – »Regen« und S – »Sonnenschein« beschrieben werden. Die Wahrscheinlichkeit, dass auf einen Regentag wieder ein Regentag folgt, sei 75% und die Wahrscheinlichkeit, dass auf einen Sonnentag wieder ein Sonnentag folgt, sei 80%.

1. Beschreiben Sie den Sachverhalt als Markov-Kette mit dem Startzustand »Regentag«.
2. Stellen Sie die Übergangsfunktion auf.
3. Wenn es am Tag $i = 0$ regnet, wie groß ist für die Tage $i = 1$ bis 4 die Wahrscheinlichkeit, dass die Sonne scheint?

Zur Kontrolle

1. Markov-Kette:



2. Übergangsfunktion:

$$\begin{pmatrix} P(R) \\ P(S) \end{pmatrix}_{n+1} = \begin{pmatrix} 0{,}75 & 0{,}2 \\ 0{,}25 & 0{,}8 \end{pmatrix} \cdot \begin{pmatrix} P(R) \\ P(S) \end{pmatrix}_{n}$$

$P(R)_0 = 100\%$, $P(S)_0 = 0$

Simulationsergebnisse für die Tage 1 bis 4

Tag	0	1	2	3	4
$P(R)$	1	0,75	0,6125	0,53687	0,49528
$P(S)$	0	0,25	0,3875	0,46313	0,50472

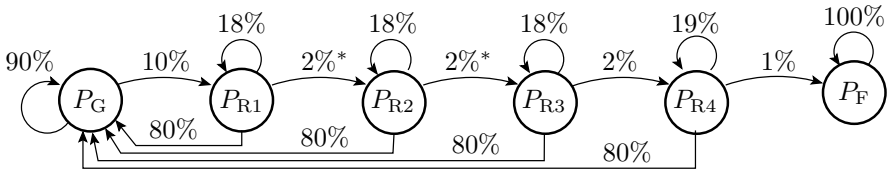
Aufgabe 1.18: Risikoanalyse

Eine schwerwiege Fehlfunktion bei einer Maschine kann nur auftreten, wenn sie vom Grundzustand G nacheinander in höhere Riskozustände R_1 bis R_4 übergeht. Das Bedienpersonal erkennt erhöhte Risikozustände mit einer Wahrscheinlichkeit von 80% und initialisiert das System dann neu (Rückkehr in den Grundzustand G). Die Wahrscheinlichkeit für den Übergang von einem in den nächsten Risikozustand betrage in jedem Zeitschritt, wenn nicht neuinitialisiert wird, 10%. In Risikozustand R_4 tritt ohne rechtzeitige Neuinitialisierung mit 5% die schwerwiegende Fehlersituation F ein.

1. Beschreiben Sie den Sachverhalt mit einer Markov-Kette.
2. Simulation der Markov-Kette für 10 Schritte.
3. Wie hoch ist die Wahrscheinlichkeit, dass nach $n = 10^6$ Zeitschritten die schwerwiegende Fehlersituation mindestens einmal eingetreten ist?

Zur Kontrolle

1. Beschreiben des Sachverhalts als Markov-Kette:



2. Simulationsprogramm:

```
PN = 100; PR1 = 0; PR2=0; PR3=0; PR4=0; PF=0;
fprintf('  n|  P(N)|  P(R1)| P(R2)| P(R3)| P(R4)  |  P(F)\n');
for n = 1:10
 PN  = PN *0.9 + PR1*0.8 + PR2*0.8 + PR3*0.8 + PR4*0.8;
 PR1 = PN *0.10 + PR1*0.18;
 PR2 = PR1*0.02 + PR2*0.18;
 PR3 = PR2*0.02 + PR3*0.18;
 PR4 = PR3*0.02 + PR4*0.19;
 PF  = PR4*0.01 + PF;
 fprintf('%3i|%6.3f| %6.3f|%6.3f|%6.3f|%8.6f|%8.6f\n',
           n, PN, PR1, PR2, PR3, PR4, PF);
end;
```

Simulationsergebnis:

n	P(N)	P(R1)	P(R2)	P(R3)	P(R4)	P(F)
1	90.000	9.000	0.180	0.004	0.000072	0.000001
2	88.347	10.455	0.241	0.005	0.000123	0.000002
3	88.074	10.689	0.257	0.006	0.000146	0.000003
4	88.029	10.727	0.261	0.006	0.000154	0.000005
5	88.021	10.733	0.262	0.006	0.000157	0.000007
6	88.020	10.734	0.262	0.006	0.000157	0.000008
7	88.020	10.734	0.262	0.006	0.000158	0.000010
8	88.020	10.734	0.262	0.006	0.000158	0.000011
9	88.020	10.734	0.262	0.006	0.000158	0.000013
10	88.020	10.734	0.262	0.006	0.000158	0.000014
10^6	86.491	10.548	0.257	0.006	0.000155	1.562945

Wahrscheinlichkeit, dass nach $n = 10^6$ Zeitschritten die schwerwiegende Fehlersituation mindestens einmal eingetreten ist:

$$P\,(F)_{10^6} = 1{,}58\%$$

Aufgabe 1.19: Speicherfehlernachweis

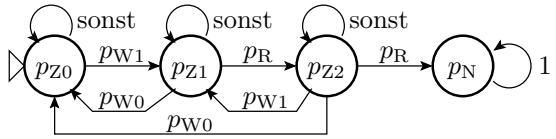
Beschreiben Sie den Fehlernachweis der nachfolgenden Speicherfehler durch Markov-Ketten:

1. zerstörendes Lesen einer 1: Der Inhalt von Speicherzelle i wird beim Lesen verändert, nachweisbar durch eine Folge
   - Schreibe 1 in Zelle i,
   - Lese Zelle i,
   - Lese Zelle i ohne zwischenzeitlichen Schreibzugriff auf i.
2. Kopplungsfehler: Schreiben einer 1 in Zelle i verändert Zelle j von 0 nach 1, nachweisbar durch folgende Folge:
   - Schreibe 0 in Zelle j
   - Schreibe eine 1 in Zelle i
   - Lese Zelle j ohne zwischenzeitlichen Schreibzugriff auf Zelle j.

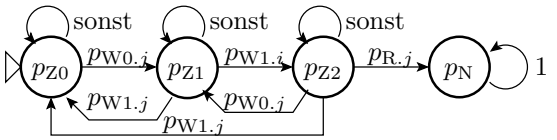
Wahrscheinlichkeit: $p_{\mathrm{W0}} = \frac{1}{4 \cdot N_{\mathrm{A}}}$, $p_{\mathrm{W1}} = \frac{1}{4 \cdot N_{\mathrm{A}}}$ – Schreiben einer 0 bzw. 1 auf einen Speicherplatz; $p_{\mathrm{R}} = \frac{1}{2 \cdot N_{\mathrm{A}}}$ – Lesen eines Speicherplatzes; N_{A} – Anzahl der Speicherplätze.

Zur Kontrolle

Zerstörendes Lesen einer 0:



Kopplungsfehler:



p_{Z0}	Fehler nicht anregbar	p_{Z2}	Zustand kontaminiert
p_{Z1}	Fehler anregbar	p_{N}	Fehler nachgewiesen

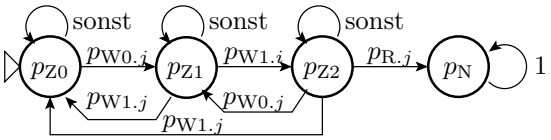
Aufgabe 1.20: Speicherfehlernachweis Fortsetzung

1. Schreiben Sie für die erste Markov-Ketten ein Simulationsprogramm zur Bestimmung der Zustandswahrscheinlichkeiten.
2. Stellen Sie die Nachweiswahrscheinlichkeit je Testschritt als die bedingte Wahrscheinlichkeit, dass der Fehler in Schritt n nachgewiesen wird, wenn er in Schritt $n-1$ noch nicht nachgewiesen war

$$p\left(n\right)=\frac{p_{\mathrm{N}}\left(n+1\right)-p_{\mathrm{N}}\left(n\right)}{1-p_{\mathrm{N}}\left(n\right)}$$

   für n im Bereich von 1 bis 5000 graphisch dar.
3. Stellt sich für die Nachweiswahrscheinlichkeit je Testschritt ein konstanter Wert ein und wie groß ist dieser?

Zur Kontrolle Aufgabenteil 1



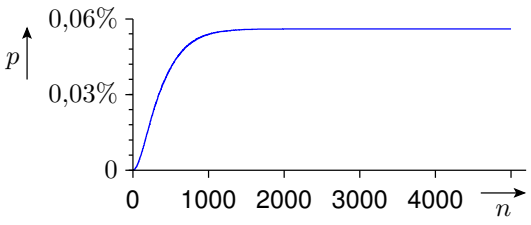

```
pZ0=1; pZ1=0; pZ2=0; pN(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW = 1/(4*NA);
for n=1:N
  pZ0     = pZ0 * (1- pW) + pZ1 * pW + pZ2 * pW;
  pZ1     = pZ0 *     pW  + pZ1 * (1-2*pW) + pZ2 * pw;
  pZ2     = pZ1 *     pR  + pZ2 * (1-pW-pR);
  pN(n+1) = pN(n) + pZ2 * pR;
  p(n)    = pZ2*pR / (pZ0+pZ1+pZ2); % Vermeidung kleiner Differenzen ...
end
plot(1:N, p);
```

Zur Vermeidung kleiner Differenzen großer Zahlen, Ersatz von $p_{\mathrm{N}}\left(n\right)-p_{\mathrm{N}}\left(n-1\right)$ durch $p_{\mathrm{Z2}}\cdot p_{\mathrm{R}}$ und $1-p_{\mathrm{N}}$ durch $p_{\mathrm{Z0}}+p_{\mathrm{Z1}}+p_{\mathrm{Z2}}$:

$$p\left(n\right)=\frac{p_{\mathrm{N}}\left(n+1\right)-p_{\mathrm{N}}\left(n\right)}{1-p_{\mathrm{N}}\left(n\right)}=\frac{p_{\mathrm{Z2}}\cdot p_{\mathrm{R}}}{p_{\mathrm{Z0}}+p_{\mathrm{Z1}}+p_{\mathrm{Z2}}}$$

Zur Kontrolle Aufgabenteil 2 und 3

Nachweiswahrscheinlichkeit in Abhängigkeit von der Testsatzlänge:



Die Nachweiswahrscheinlichkeit je Testschritt

$$p=\frac{p_{\mathrm{Z2}}\cdot p_{\mathrm{R}}}{p_{\mathrm{Z0}}+p_{\mathrm{Z1}}+p_{\mathrm{Z2}}}$$

bleibt ab $n\geq 2000$ konstant $p\approx 0,057\%$. Für n Testschritte wie Funktion ohne Gedächtnis

$$p\left(n\right)\approx 1-e^{-n\cdot p}$$

.

2.6 Fehlernachweis

Aufgabe 1.21: Nachweiswahrscheinlichkeit

Ein System hat im Mittel bei jeder 10^4-ten Service-Leistung eine Fehlfunktion. 70% der FF werden einem ersten, 20% einem zweiten und die restlichen 10% nicht lokalisierbaren Fehler zugeordnet.

1. Welche Nachweiswahrscheinlichkeiten p_1 und p_2 haben die beiden zugeordneten Fehler?
2. Wie lang muss ein Zufallstest mindestens sein, damit der schlechter nachweisbare zugeordnete Fehler mindestens mit einer Wahrscheinlichkeit von 99% nachgewiesen wird?
3. Welche Zuverlässigkeit ist für das System zu erwarten, wenn die beiden zugeordneten Fehler beseitigt sind?

Zur Kontrolle

1. Nachweiswahrscheinlichkeiten der beiden zugeordneten Fehler:
$$p_1 = 0{,}7 \cdot 10^{-4}; \quad p_2 = 0{,}2 \cdot 10^{-4}$$
2. Testsatzlänge für den Nachweis von Fehler 2:
$$\begin{aligned} 99\% \geq p_2(n) &= 1 - e^{-n \cdot p_2} \\ n &\geq -\frac{\ln(1-99\%)}{p_2} = 2{,}3 \cdot 10^5 \end{aligned}$$
3. Nach Beseitigung der zugeordneten Fehler ist eine Verringerung der Häufigkeit der FF auf 10% und damit eine Verzehnfachung der Zuverlässigkeit zu erwarten:
$$Z = 10^5 \frac{\text{SL}}{\text{FF}}$$

3 Kenngrößen der Verlässlichkeit

3.1 Anzahl Fehler und FF

Aufgabe 1.22: Software-Fehler im Einsatz

Wie viele Fehler sind in einem Software-System mit 10^5 NLOC zu erwarten, wenn nach dem Entwurf 3% der Nettocodezeilen fehlerhaft sind und der Test 60% der Fehler erkennt?

Zur Kontrolle

Zu erwartende Anzahl der

- entstehenden Fehler: 3000
- gefundenen Fehler: 1800
- nicht gefundenen Fehler: 1200

Aufgabe 1.23: Pareto-Prinzip

1. Was besagt das Pareto-Prinzip für Fehler und Fehlfunktionen?
2. Gilt das Pareto-20%-80%-Prinzip[1], wenn alle Fehler mit derselben Häufigkeit FF erzeugen:
$$h(x) = \begin{cases} c & \text{für } x = x_0 \\ 0 & \text{sonst} \end{cases}$$
3. Gibt es für die nachfolgende QQ-Funktion
$$h(x) = \begin{cases} c & \text{für } x_0 \leq x \leq x_1 \\ 0 & \text{sonst} \end{cases}$$
Kombinationen der Parameter c, x_0 und x_1, mit denen das Pareto-20%-80%-Prinzip gilt?

[1] Gibt es ein d für das gilt, das die 20% der Fehler mit maximal $x \leq d$ SL je FF 80% der FF verursachen?

Zur Kontrolle

1. Die Mehrheit der Fehlfunktionen werden durch einen kleinen Anteil der Fehler verursacht.
2. Wenn alle Fehler mit derselben Wahrscheinlichkeit Fehlfunktionen verursachen, gibt es keine dominanten Fehler, die häufiger als die anderen Fehlfunktionen verursachen. Folglich gilt das Pareto-Prinzip nicht.
3. Für
$$h(x) = \begin{cases} c & \text{für } x_0 \le x \le x_1 \\ 0 & \text{sonst} \end{cases}$$
beträgt Anteil der dominanten Fehler in Abhängigkeit von $x_0 \le d \le x_1$:
$$\frac{E(\varphi(d))}{E(\varphi)} = \frac{\int_0^d h(x)\cdot dx}{\int_0^\infty h(x)\cdot dx} = \frac{\int_{x_0}^d c\cdot dx}{\int_{x_0}^{x_1} c\cdot dx} = \frac{c\cdot(d-x_0)}{c\cdot(x_1-x_0)}$$
... (Fortsetzung nächste Folie)

Der Anteil der FF durch die dominanten Fehler beträgt:

$$\frac{p_{\mathrm{FFF}}(d)}{p_{\mathrm{FFF}}} = \frac{\int_0^d \frac{h(x)}{x}\cdot dx}{\int_0^\infty \frac{h(x)}{x}\cdot dx} = \frac{\int_{x_0}^d \frac{c}{x}\cdot dx}{\int_{x_0}^{x_1} \frac{c}{x}\cdot dx} = \frac{c\cdot\ln\left(\frac{d}{x_0}\right)}{c\cdot\ln\left(\frac{x_1}{x_0}\right)}$$

Für das Pareto-20%-80%-Prinzip müsste gelten:

$$\begin{aligned} \frac{E(\varphi(d))}{E(\varphi)} &= \frac{d-x_0}{x_1-x_0} \stackrel{!}{=} 20\% \\ d &= 0{,}8\cdot x_0 + 0{,}2\cdot x_1 \\ \frac{p_{\mathrm{FFF}}(d)}{p_{\mathrm{FFF}}} &= \frac{\ln\left(\frac{d}{x_0}\right)}{\ln\left(\frac{x_1}{x_0}\right)} \stackrel{!}{=} 80\% \\ 0 &= \left(\frac{x_1}{x_0}\right)^{0{,}8} - 0{,}2\cdot\frac{x_1}{x_0} - 0{,}8 \end{aligned}$$

Die einzige Lösung $x_1 = x_0$ ist ausgeschlossen wegen $E(\varphi) \neq 0$. Folglich gibt es keine Kombination der Parameter c, x_0 und x_1, mit der das Pareto-20%-80%-Prinzip gilt.

Aufgabe 1.24: Zu erwartende Fehleranzahl und p_{FFF}

Bei einer Verdopplung der Testanzahl von $n_0 = 5\cdot10^3$ auf $n_1 = 10^4$ Zufallstests in einer Iteration aus Test und Fehlerbeseitigung wurden 20 Fehler beseitigt und die Wahrscheinlichkeit einer FF hat sich auf ein Drittel verringert. Schätzen Sie unter der Annahme einer Beseitigungswahrscheinlichkeit von $p_{\mathrm{Bes}} = 80\%$ und
$$h(x) = c\cdot x^{-(k+1)}\cdot e^{-\frac{p_{\mathrm{Bes}}\cdot n}{x}}$$

1. den Parameter k und
2. die zu erwartende Anzahl der nach Verdopplung der Testsatzlänge immer noch nicht beseitigten Fehler.

Zur Kontrolle

1. Bei einer Verdopplung der Testanzahl verringert sich die Wahrscheinlichkeit einer FF auf ein Drittel:
$$\begin{aligned} p_{\mathrm{FFF}}(n_1) &= p_{\mathrm{FFF}}(n_0)\cdot\left(\frac{n_1}{n_0}\right)^{-(k+1)} \\ k &= \frac{\ln\left(\frac{p_{\mathrm{FFF}}(n_0)}{p_{\mathrm{FFF}}(n_1)}\right)}{\ln\left(\frac{n_1}{n_0}\right)} - 1 = \frac{\ln(3)}{\ln(2)} - 1 = 0{,}585 \end{aligned}$$

2. Zu erwartende Fehleranzahl nach Verdopplung der Testsatzlänge:

$$\begin{aligned} p_{\mathrm{FFF}}(n) &= \frac{k \cdot E(\varphi(n))}{p_{\mathrm{Bes}} \cdot n} \\ E(\varphi(n)) &= \frac{p_{\mathrm{Bes}} \cdot n \cdot p_{\mathrm{FFF}}(n)}{k} \end{aligned}$$

$$\begin{aligned} \underbrace{E(\varphi(n_0)) - E(\varphi(n))}_{\text{20 beseitigte Fehler}} &= \frac{p_{\mathrm{Bes}} \cdot n_0 \cdot p_{\mathrm{FFF}}(n_0)}{k} - \frac{p_{\mathrm{Bes}} \cdot n \cdot p_{\mathrm{FFF}}(n)}{k} \\ E(\varphi(n_0)) - E(\varphi(n)) &= \frac{p_{\mathrm{Bes}} \cdot n \cdot p_{\mathrm{FFF}}(n)}{k} \cdot \left(\underbrace{\frac{n_0 \cdot p_{\mathrm{FFF}}(n_0)}{n \cdot p_{\mathrm{FFF}}(n)}}_{\frac{1}{2} \cdot 3} - 1 \right) \\ p_{\mathrm{FFF}}(n) &= \frac{2 \cdot k \cdot (E(\varphi(n_0)) - E(\varphi(n)))}{p_{\mathrm{Bes}} \cdot n} \\ E(\varphi(n)) &= \frac{p_{\mathrm{Bes}} \cdot n \cdot p_{\mathrm{FFF}}(n)}{k} \\ &= 2 \cdot (E(\varphi(n_0)) - E(\varphi(n))) = 40 \end{aligned}$$

Die zu erwartende Anzahl der nicht beseitigten Fehler ist die doppelte Anzahl der beseitigten Fehler.

Aufgabe 1.25: QQ-Potenzfunktion

Gegeben sind die mittlere Anzahl von SL je FF für 24 Modellfehler:

```
x = [10 11 13 15 17 18 21 24 29  31 33 37 40 ...
     52 67 70 83 110 185 217 290 420 850 1730 5870];
```

1. Bestimmen Sie für eine Potenz-QQ-Funktion

$$h(x) = c \cdot x^{-(k+1)}$$

   für $x > x_0$ und $k > 0$ die akkumulierte Funktion $H(x \geq d)$.

2. Stellen Sie die Anzahl der Fehler mit mindestens d SL je FF als Schätzfunktion

$$H_{\mathrm{S}}(x \geq d)$$

   mit doppelt logarithmischer Achsenteilung für d und den Funktionswert dar.

3. Schätzen Sie aus der Darstellung den Exponenten k der QQ-Funktion.

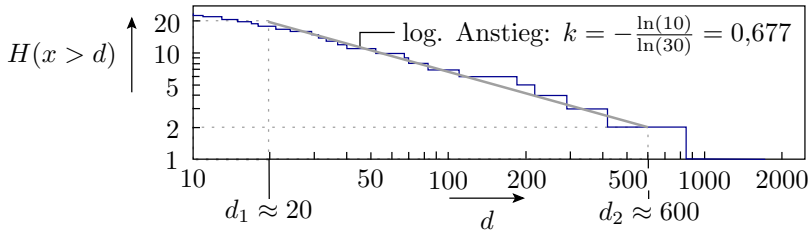
Zur Kontrolle

1. Akumulierte Funktion:

$$H(x \geq d) = \int_d^{\infty} c \cdot x^{-(k+1)} \cdot dx = \frac{c \cdot d^{-k}}{k}$$

2. Octave-Script zur Darstellung der akkumulierten Funktion:

```
x = [10  11  13  15  17  18  21  24  29   31  33  37  40  ...
  52  67  70  83  110  185  217  290  420  850  1730]; %5870
y = [24  23  22  21  20  19  18  17  16  15  14  13  12...
  11  10  9  8  7  6  5  4  3  2  1]; %0
loglog(x,y, '.');
```



3. Abschätzung des Exponenten k der QQ-Funktion aus zwei Punkten der Ausgleichsgeraden:

$$k = \frac{\ln\left(\frac{H(x>d_1)}{H(x>d_2)}\right)}{\ln\left(\frac{d_2}{d_1}\right)} = 0{,}677$$

3.2 Zuverlässigkeit

Aufgabe 1.26: Zuverlässigkeit Gesamtsystem

Ein IT-System bestehe aus Komponenten mit den folgenden Teilzuverlässigkeiten in Form der mittleren Anzahl von Service-Leistungen je Fehlfunktion:

Teilsystem	Rechner	Festplatte	Stromversorgung	sonstiges
Teilzuverlässigkeit	Z_{R}	Z_{FP}	Z_{SV}	Z_{*}
Wert in SL/FF	1000	500	700	2000

Welche Zuverlässigkeit hat das Gesamtsystem, wenn bei jeder Fehlfunktion einer Komponenten auch das Gesamtsystem eine Fehlfunktion hat?

Zur Kontrolle

Gesamtzuverlässigkeit:

$$Z_{\mathrm{ges}} = \frac{1}{\frac{1}{1000}+\frac{1}{500}+\frac{1}{700}+\frac{1}{2000}} = 203\,\frac{\mathrm{SL}}{\mathrm{FF}}$$

Die Gesamtzuverlässigkeit wird am meisten von den unzuverlässigsten Teilsystemen bestimmt.

Aufgabe 1.27: Zuverlässigkeiterhöhung durch Redundanz

Auf welchen Wert erhöht sich die Gesamtzuverlässigkeit, wenn der Speicher durch ein RAID aus zwei Platten vom bisherigen Typ ersetzt wird, und das RAID nur eine Fehlfunktion weitergibt, wenn beide Platten zeitgleich eine Fehlfunktion haben?

Alle Teilzuverlässigkeiten wie Aufgabe zuvor.

Zur Kontrolle

Das RAID versagt, wenn beide Platten (gleichzeitig) versagen:

$$\begin{aligned}\frac{1}{Z_{\mathrm{RAID}}} &= 1 - p_{\mathrm{Z.RAID}} = (1-p_{\mathrm{Z.FP}})^2 = \frac{1}{Z_{\mathrm{FP}}^2}\\ Z_{\mathrm{RAID}} &= 500^2\,\frac{\mathrm{SL}}{\mathrm{NTFF}}\end{aligned}$$

(NTFF – nicht tolerierte FF). Gesamtzuverlässigkeit mit RAID statt Einzelplatte:

$$Z_{\mathrm{ges}} = \frac{1}{\frac{1}{1000}+\frac{1}{500^2}+\frac{1}{700}+\frac{1}{2000}} = 341\,\frac{\mathrm{SL}}{\mathrm{FF}}$$

Mit einem RAID als Festplatte wird die Gesamtzuverlässigkeit von den nun am unzerlässigsten Teilsystemen bestimmt.

Aufgabe 1.28: Fehlerbezogene Zuverlässigkeit

Ein System habe zwei Fehler mit den Nachweiswahrscheinlichkeiten $p_1 = 3 \cdot 10^{-3}$ und $p_2 = 2 \cdot 10^{-3}$ je Service-Leistung.

1. Wie groß ist die fehlerbezogene Zuverlässigkeit[2]?
2. Mit welcher Wahrscheinlichkeit weist ein Zufallstest der Länge $n = 1000$ jeden der beiden Fehler nach?
3. Mit welcher Wahrscheinlichkeit ist mit 1000 Service-Leistungen nachweisbar, dass das System fehlerhaft ist?

Zur Kontrolle

1. Fehlerbezogene Zuverlässigkeit:
   - Wahrscheinlichkeit einer durch Fehler verursache FF/SL:
     $$p_{\mathrm{FFF}} = 1 - (1 - p_1) \cdot (1 - p_2) \approx p_1 + p_2 = 5 \cdot 10^{-3}$$
   - Zuverlässigkeit:
     $$Z = \frac{1}{p_{\mathrm{FFF}}} = 200 \, \frac{\mathrm{SL}}{\mathrm{FF}}$$
2. Nachweiswahrscheinlichkeit mit einem Zufallstest der Länge $n = 1000$:
   - Fehler 1: $p_1\,(1000) = 1 - e^{-1000 \cdot 3 \cdot 10^{-3}} = 1 - e^{-3} = 95{,}02\%$
   - Fehler 2: $p_2\,(1000) = 1 - e^{-1000 \cdot 2 \cdot 10^{-3}} = 1 - e^{-2} = 86{,}47\%$
3. »System fehlerhaft« ist nachweisbar, wenn mindestens ein Fehler nachweisbar ist:
   $$p_{1 \vee 2}\,(1000) = 1 - e^{-1000 \cdot (p_1 + p_2)} = 1 - e^{-5} = 99{,}3\%$$

3.3 Sicherheit

Aufgabe 1.29: Zuverlässigkeit und Sicherheit

Bei einem IT-System mit einer mittleren Zeit zwischen zwei Fehlfunktionen von 10^3 Stunden gefährde abschätzungsweise jede hundertste Fehlfunktion die Betriebssicherheit.

Welche Betriebssicherheit hat ein Service mit einer Dauer von einer Stunde?

Zur Kontrolle: $S \approx 10^5$ SL/GFF (SL – Service-Leistungen; GFF – gefährdende Fehlfunktionen)

3.4 Schadenskosten

Aufgabe 1.30: Produkthaftung und Testauswahl

1. Wie wirkt sich die Produkthaftung auf die Testauswahl aus?
2. Was ist für einen Testfall nach IEEE-Standard 829 zusätzlich zu den Eingaben und Sollausgaben zu dokumentieren?

[2] Mittlere Anzahl der Service-Leistungen zwischen zwei durch Fehler verursachte Fehlfunktionen.

Zur Kontrolle

1. Außer der Sicherung einer ausreichenden Verlässlichkeit muss der Hersteller bei einem durch Fehler verursachten Schadensfall nachweisen, dass er entsprechend Stand der Technik ausreichend getestet hat. Er muss also dokumentieren, was er getestet hat und dass das entsprechend geltender Standards ausreicht.
2. Zusätzlich zur Eingabe und Sollausgabe ist nach geltenden Standards für jeden Testfall zu dokumentieren:
   - Testfall-Identifikation: eindeutiger Bezeichner.
   - Testgegenstand: Referenz auf die Beschreibung, aus der Anforderungen überprüft werden.
   - Zweck: Anforderung, deren Erfüllung der Test bestätigt.
   - Testfallstatus: spezifiziert, durchgeführt, ...

3.5 Verfügbarkeit

Aufgabe 1.31: Reparaturplanung

Für eine Steuerung betrage die mittlere Zeit zwischen zwei Ausfällen mindestens zwei Jahre. Wie groß darf die mittlere Reparaturzeit maximal sein, damit die Steuerung mit einer Wahrscheinlichkeit

$$p_V \geq 1 - 10^{-6}$$

verfügbar ist?

Zur Kontrolle

Mittlere Zeit zwischen zwei Ausfällen:

$$MTBF_V = 2\,\text{Jahre}$$

Geforderte Wahrscheinlichkeit der Verfügbarkeit:

$$1 - 10^{-6} \leq p_V \quad = \quad \frac{MTBF_V}{MTBF_V + MTTR}$$

Zulässige mittlere Reparaturzeit:

$$MTTR \leq \frac{MTBF_A \cdot (1 - p_V)}{p_V} = 2\,\text{Jahre} \cdot 10^{-6} = 61{,}5\,\text{s}$$

Eine so kurze mittlere Reparaturzeit verlangt automatischen Ersatz / Rekonfiguration.

3.6 Fehleranteil

Aufgabe 1.32: Fehleranteil eines Rechners

Ein Steuerrechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerständen, Kondensatoren, ...) und Lötstellen.

Bauteil	Anzahl	Fehleranteil	Produkt
Leiterplatten	2	600 dpm	dpm
Schaltkreise	30	200 dpm	+ dpm
diskrete Bauteile	180	10 dpm	+ dpm
Lötstellen	5000	1 dpm	+ dpm
			= dpm

1. Wie groß ist der zu erwartende Fehleranteil des Rechners, wenn anderen Arten von Fehlern anzahlmäßig vernachlässigbar sind?
2. Auf welchen Wert verringert sich der Fehleranteil, wenn für alle Arten von Bauteilen die Anzahl halbiert wird?

Zu Kontrolle

Bauteil	Anzahl	Fehleranteil	Produkt
Leiterplatten	2	600 dpm	1200 dpm
Schaltkreise	30	200 dpm	+ 6000 dpm
diskrete Bauteile	180	10 dpm	+ 1800 dpm
Lötstellen	5000	1 dpm	+ 5000 dpm
			= 14000 dpm

1. Von 1000 Rechner enthalten im Mittel 14 beim Verkauf einen Bauteilfehler.

2. Bei der halben Bauteilzahl und ansonsten gleichen Werten enthalten im Mittel nur 7 von 1000 Rechnern einen Bauteilfehler.