Test und Verlässlichkeit
Grosse Übung zu Foliensatz 1

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV-GUe-F1)

28. Juni 2016

Grundbegriffe

Aufgabe 1.1: C-typischer Multiplikationsfehler

Eine Service-Leistung sei definiert durch:

- Eingabeformat: zwei Variablen a und b, 16-Bit vorzeichenfrei
- Ausgabeformat: Rückgabewert 32-Bit vorzeichenfrei
- Sollfunktion: Rückgabe des Produkts a*b
- Implementierung als C-Funktion:

```
uint32_t umult16(uint16_t a, uint16_t b){
 return a*b[1];
}
```

1. Kleinste und größte darstellbare Eingabewerte?
2. Kleinstes und größtes mögliches / darstellbares Produkt?
3. Testbeispiel für den Fehlernachweis.
4. Vorschlag zur Fehlerbehebung.

[1] Der Multiplikationsoperator »*« berechnet zuerst ein uint16_t-Produkt und führt erst danach den Typcast auf den Zieltyp durch.

```
uint32_t umult16(uint16_t a, uint16_t b){
    return a*b
}
```

	Minimalwert	Maximalwert
Operanden a, b		
Produkt, darstellbar		
Produkt, möglich		

4 Testbeispiel für Fehlernachweis:

a=	b=

5 Vorschlag zur Fehlerbehebung:

```
Prog. Zeile 1:
Prog. Zeile 2:
```

Aufgabe 1.2: Fehler und Fehlfunktionen

```
uint32_t umult16(uint16_t a, uint16_t b){
 return a*b;
}
```

Testbeispiele, eines davon für den Fehlernachweis:

a	b	Soll-Ergebnis	Ist-Ergebnis	nachweisbar?

Erläutern Sie an diesem Beispiel

1. was eine Fehlfunktion und
2. was ein Fehler ist.
3. Was sind laut Service-Modell wesentliche Eigenschaften des gegebenen Programms und was vernachlässigbare Details?

Zur Kontrolle

Testbeispiele, eines davon für den Fehlernachweis:

a	b	Soll-Ergebnis	Ist-Ergebnis	nachweisbar?
0x23	0x10	0x230	0x230	nein
0x23FA	0x100	0x23FA00	0xFA00	ja

1. Fehlfunktion: Im Beispiel die abweichende Ausgabe im 2. Testbeispiel.
2. Fehler: Umgangssprachlich würde man hier angeben, wie man die Ursache der FF beseitigt hat und der Fehler wäre die »Nichtbeseitigung«, im Beispiel[2]:
   - vergessener Typcast,
   - falsche Imlementierung des Multiplikationsoperators,
   - ...

[2] Die Beschreibung, was Fehler und potenzielle Fehler sind, ist nicht trivial.

4 Wesentliche Eigenschaften der Service-Modells aus der Sicht von Test- und Verlässlichkeit:

- Zählbare Anzahl der Service-Leistungen.
- Das Ein- und Ausgabeformat.
- Unterscheidbarkeit zwischen korrekten, und falschen Ein- und Ausgaben.

Vernachlässigbare Details: Funktion und Realisierung des Programms.

Aufgabe 1.3: Potenzielle Fehler und Modellfehler

```
uint32_t umult16(uint16_t a, uint16_t b){
 return a*b;
}
```

Versuchen Sie für das Beispiel eine Menge

1. potenzieller Fehler und
2. eine Menge von Modellfehlern

zusammenzustellen.

Zur Kontrolle

1. Potenzielle Fehler:
   - Jede vorhandene Anweisung (Anzahl 3),
   - Jede Variablenzuweisung / -zuordnung: (Anzahl 3),
   - Jeder Operator (Anzahl 1).

   Ohne Zusatzdefinitionen, was genau als potenzieller Fehler zu zählen ist, nicht präzise angebbar.

2. Modellfehler:
   - jede Anweisung einmal weglassen.
   - jedes berechnete Zwischenergebnis einmal +1 und einmal -1, ...

   Verlangt zusätzlich ein Fehlermodell, dass genau vorschreibt, was für (geringfügige)) Änderungen als Fehler einzubauen sind.

Aufgabe 1.4: Determinismus

Das nachfolgende fehlerhafte Unterprogramm soll für das mit einem Zeiger auf den Anfang und der Länge übergebene Feld den kleinsten Wert zurückgeben:

```
int16_t Feld[]= {231, -13, ...}; // Beispiel für ein Feld
...
int16_t kleinsterWert(int16_t *Feld, uint16_t len){
  int16_t tmp, *ptr;
  for (ptr=Feld; ptr < Feld+len; ptr++){
    if (*ptr<tmp) tmp = *ptr;
  }
 }
```

1. Verhält sich das Programm deterministisch? (Begründung)
2. Gibt es ein Testbeispiel, dass den Fehler sicher bei jeder Testwiederholung nachweist?

Zur Kontrolle

1. Deterministisch: Nein. Ergebnis hängt vom zufälligen Anfangswert »tmp« ab.
2. Sicheres Testbeispiel: Nein. Wenn tmp größer als der kleinste Wert im Eingabefeld ist, was für kein Testbeispiel ausschließbar ist, ist der Fehler nicht nachweisbar.

Wahrscheinlichkeit

Aufgabe 1.5: 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.

1. $X + Y > 8$
   - Anzahl der Möglichkeiten:
   - günstig:

   - Anzahl günstig:
   - Wahrscheinlichkeit:

2. $X > Y$
   - Anzahl der Möglichkeiten:
   - günstig:

   - Anzahl günstig:
   - Wahrscheinlichkeit:

Zur Kontrolle

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

3. $(X = 5) \wedge (Y < 5)$
   - Anzahl der Möglichkeiten:
   - günstig:
   - Anzahl günstig:
   - Wahrscheinlichkeit:

4. $X \cdot Y$ ist durch drei teilbar.
   - Anzahl der Möglichkeiten:
   - günstig:
   - Anzahl günstig:
   - Wahrscheinlichkeit:

Zur Kontrolle

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)
   - Anzahl günstig: 10
   - Wahrscheinlichkeit: 10/36

Verkettete Ereignisse

Aufgabe 1.6: 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 1.7: Fehlfunktionen und Fehlernachweis

Ein System habe vier unabhängig voneinander nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten je Service-Aufruf von $p_1 = 10\%$, $p_2 = 20\%$, $p_3 = 5\%$ und $p_4 = 1\%$.

1. Mit welcher Wahrscheinlichkeit versagt eine einzelne Service-Anforderung?
2. Wie hoch ist die Wahrscheinlichkeit, dass zehn Service-Anforderungen korrekt ausgeführt werden?
3. Wie groß ist die Wahrscheinlichkeit für jeden der vier Fehler, dass er bei mindestens einer der zehn Service-Anforderungen versagt (nachgewiesen wird)?

Basisereignisse F_i Service versagt durch Fehler i
($P(F_1) = p_i$; $p_1 = 10\%$, $p_2 = 20\%$, $p_3 = 5\%$ und $p_4 = 1\%$).

Gesucht:

1. Versagt eine einzelne Service-Anforderung:

$$V_1 =$$

$$P(V_1) =$$

2. Korrekte Ausführung zehn Service-Anforderungen:

$$\overline{V}_{10} =$$

$$P\left(\overline{V}_{10}\right) =$$

Service-Versagen durch jeden der vier Fehler mit mindstens eine von zehn Service-Anforderungen:

$$V_{i.10} \quad =$$

1. Fehler

$$P\left(V_{1.10}\right) =$$

2. Fehler:

$$P\left(V_{2.10}\right) =$$

3. Fehler:

$$P\left(V_{3.10}\right) =$$

4. Fehler:

$$P\left(V_{3.10}\right) =$$

Zur Kontrolle

1. Versagen einzelne Service-Anforderung:

$$\begin{aligned} V_1 &= F_1 \vee F_2 \vee F_3 \vee F_4 \\ V_1 &= \overline{\bar{F}_1 \bar{F}_2 \bar{F}_3 \bar{F}_4} \\ P(V) &= 1 - 0{,}9 \cdot 0{,}8 \cdot 0{,}95 \cdot 0{,}99 = 23{,}3\% \end{aligned}$$

2. Korrekte Ausführung von zehnService-Anforderungen:

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

Service-Versagen durch durch mindstens eine von zehn Service-Anforderungen:

$$\begin{aligned} p_{1.10} &= 1 - (1 - 10\%)^{10} = 65\% \\ p_{2.10} &= 1 - (1 - 20\%)^{10} = 89\% \\ p_{3.10} &= 1 - (1 - 5\%)^{10} = 40\% \\ p_{4.10} &= 1 - (1 - 1\%)^{10} = 9{,}6\% \end{aligned}$$

Fehlerbaumanalyse

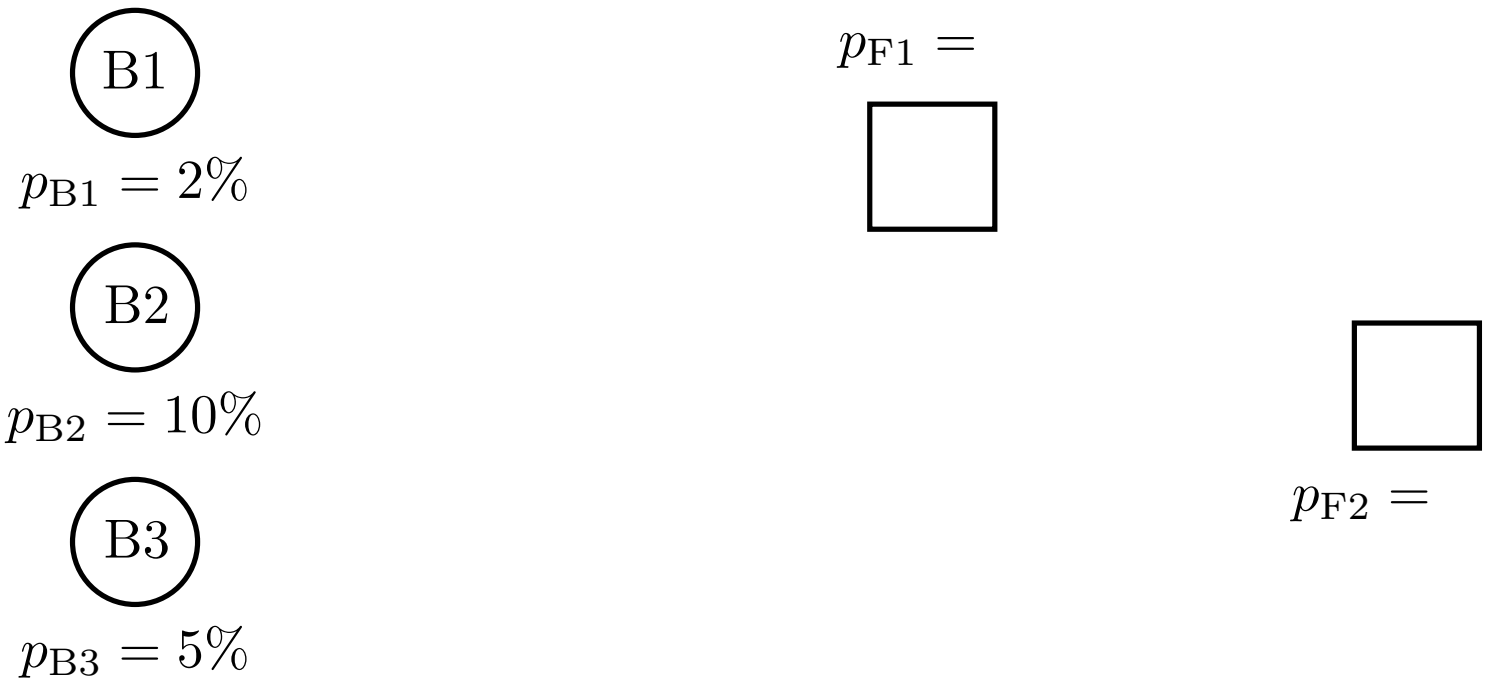
Aufgabe 1.8: Fehlerbaumanalyse

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.

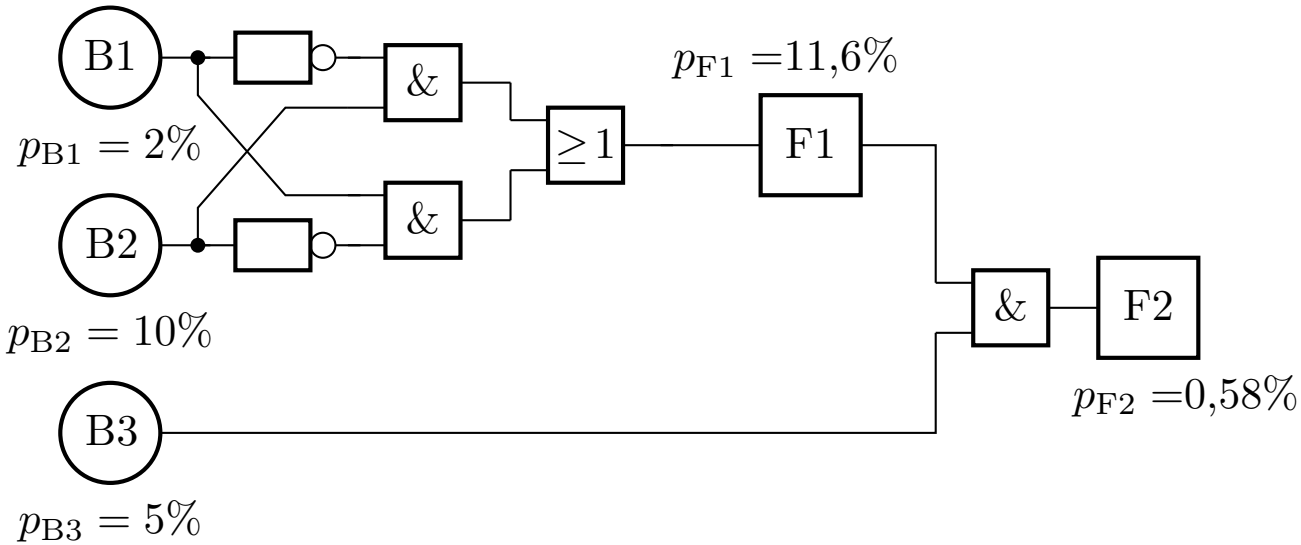
2. Berechnen Sie die Wahrscheinlichkeit für F_1 und F_2 für den Fall, dass die Wahrscheinlichkeiten der Basisereignisse $p_{\mathrm{B1}} = 2\%$, $p_{\mathrm{B2}} = 10\%$ und $p_{\mathrm{B3}} = 5\%$ betragen.

Konstruktion des Fehlerbaums

- 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.



Zur Kontrolle

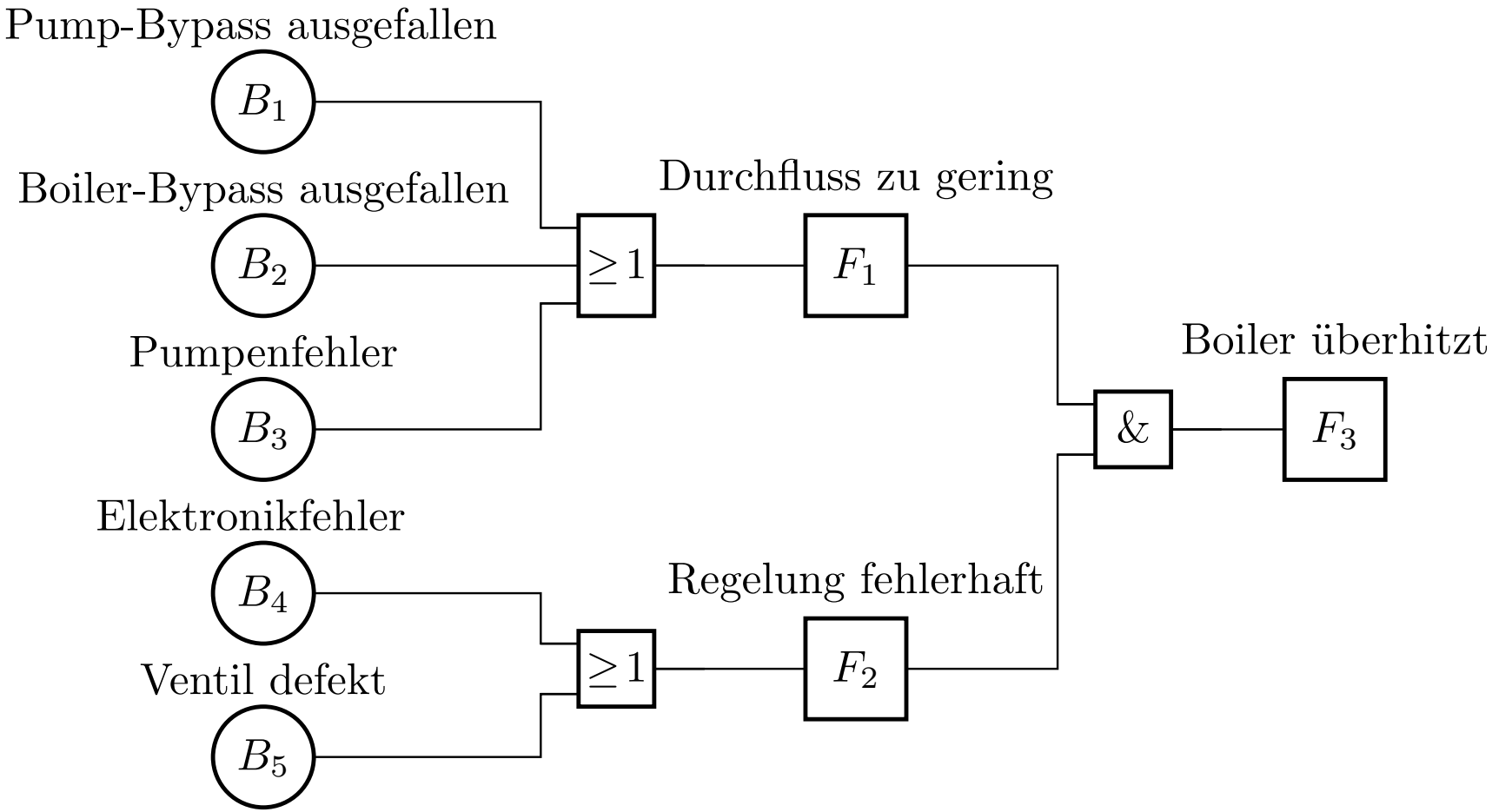


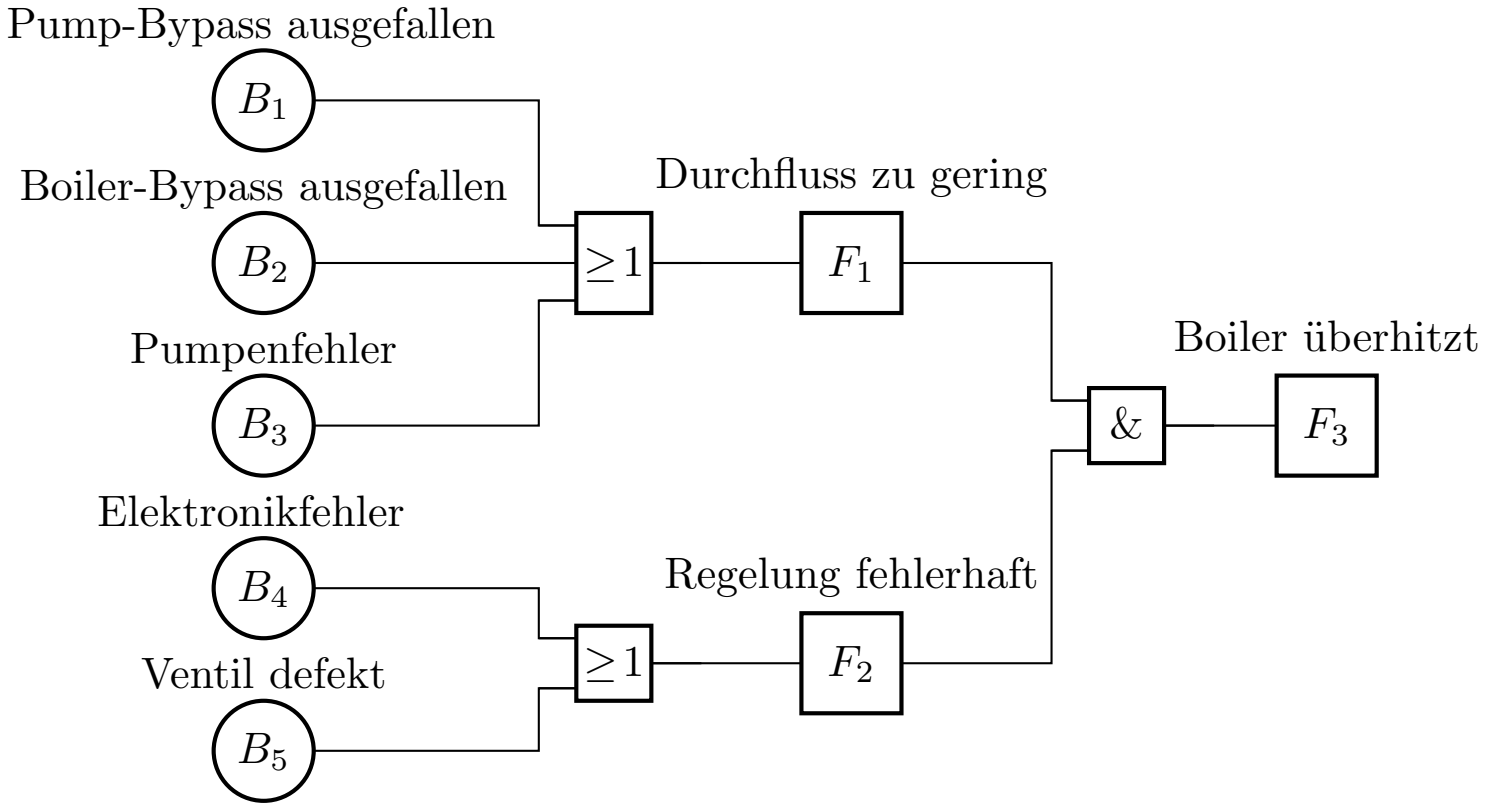
$$
\begin{aligned}
P\left(\mathrm{B1} \wedge \overline{\mathrm{B2}}\right) &= p_{\mathrm{B1}} \cdot (1 - p_{\mathrm{B2}}) = 2\% \cdot 90\% = 1{,}8\% \\
P\left(\mathrm{B2} \wedge \overline{\mathrm{B1}}\right) &= p_{\mathrm{B2}} \cdot (1 - p_{\mathrm{B1}}) = 10\% \cdot 98\% = 9{,}8\% \\
p_{\mathrm{F1}}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

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

Aufgabe 1.9: 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.





$p_{\mathrm{F1}} =$

$p_{\mathrm{F2}} =$

$p_{\mathrm{F3}} =$

Zur Kontrolle

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

Markov-Ketten

Aufgabe 1.10: Wettervorhersage mit Markov-Kette

Für ein Gebiet mit längeren Regen- und Trockenzeiten soll die Wettervorhersage für den nächsten Tag durch einen Markov-Prozess 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?

Simulationsergebnisse Aufgabenteil c

1. Markov-Kette:

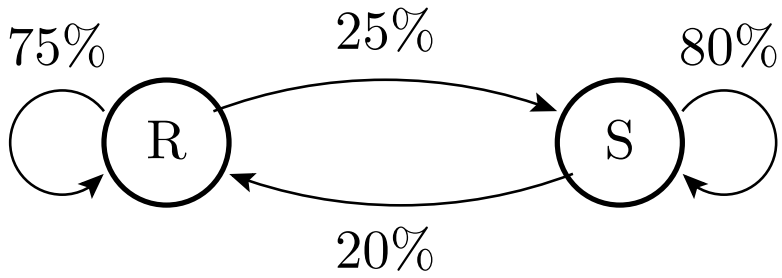
2. Übergangsfunktion:

$$\begin{pmatrix} P(R) \\ P(S) \end{pmatrix}_{n+1} = \begin{pmatrix} \ldots\ldots\ldots & \ldots\ldots\ldots \\ \ldots\ldots\ldots & \ldots\ldots\ldots \end{pmatrix} \cdot \begin{pmatrix} P(R) \\ P(S) \end{pmatrix}_{n}$$

$P(R)_0 =$
$P(S)_0 =$

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

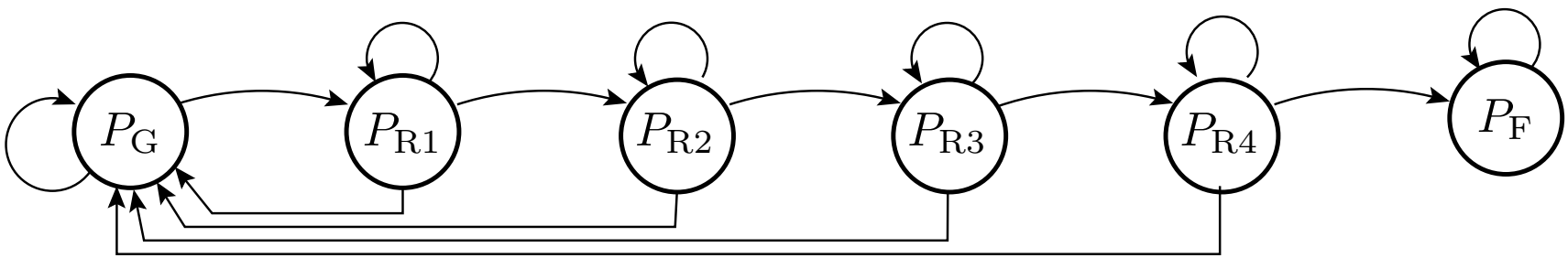
Aufgabe 1.11: Risikoanalyse

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.

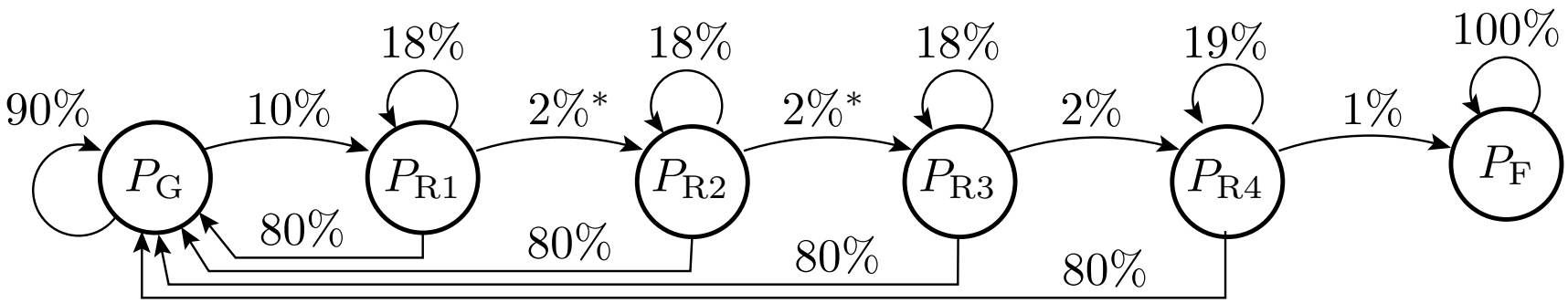
1. Beschreiben Sie den Sachverhalt mit einer Markov-Kette.
2. Simulation der Markov-Kette für 10 Schritte.
3. Wie hoch ist die Wahrscheinlichkeit, dass nach $n = 10^6$ Zeitschritten die schwerwiegende Fehlersituation mindestens einmal eingetreten ist?

Markov-Kette

- Schwerwiege Fehlfunktion ..., wenn Übergang vom Grundzustand G nacheinander in höhere Riskozustände R_1 bis R_4 und weiter in den Fehlerzustand F.
- Aus R_1 bis R_4 Übergang mit 80% nach G. Die Übergangswahrscheinlichkeit $G \to R_1$, $R_i \to R_{i+1}$ betrage in jedem Zeitschritt, wenn nicht neuinitialisiert wird, 10%.
- In R_4 tritt wenn nicht neuinitialisiert wird, mit 5% die schwerwiegende Fehlersituation F ein.



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:

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

Zufallsexperimente

Verfügbarkeit

Aufgabe 1.12: 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

$$p_{\mathrm{V}} \geq 1 - 10^{-6}$$

verfügbar ist?

Zur Kontrolle

Mittlere Zeit zwischen zwei Ausfällen:

$$MTBF_{\mathrm{A}} = 2\,\mathrm{Jahre}$$

Geforderte Wahrscheinlichkeit der Verfügbarkeit:

$$1 - 10^{-6} \leq p_{\mathrm{V}} = \frac{MTBF_{\mathrm{A}}}{MTBF_{\mathrm{A}} + MTBF_{\mathrm{R}}}$$

$$MTBF_{\mathrm{R}} = \frac{MTBF_{\mathrm{A}} \cdot (1 - p_{\mathrm{V}})}{p_{\mathrm{V}}} = 2\,\mathrm{Jahre} \cdot 10^{-6} = 61{,}5\,\mathrm{s}$$

Verlangt eine Reparaturtechnologie mit sehr kurzen Reparaturzeiten.

Aufgabe 1.13: Zuverlässigkeit Gesamtsystem

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

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	Z_{R}	Z_{SP}	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

$$Z_{\text{ges}} = \frac{1}{\frac{1}{1000} + \frac{1}{500} + \frac{1}{700} + \frac{1}{2000}} = 203$$

Die Gesamtzuverlässigkeit wird am meisten von den unzuverlässigsten Teilsystemen bestimmt.

Aufgabe 1.14: 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?

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	Z_{R}	Z_{P}	Z_{SV}	Z_{*}
Wert in SL/FF	1000	500	700	2000

Zur Kontrolle

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

$$\begin{aligned} \frac{1}{Z_{\mathrm{RAID}}} &= p_{\mathrm{V.RAID}} = p_{\mathrm{P}}^2 = \frac{1}{Z_{\mathrm{P}}^2} \\ Z_{\mathrm{RAID}} &= 500^2 \end{aligned}$$

Gesamtzuverlässigkeit mit RAID statt Einzelplatte:

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

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

Sicherheit

Aufgabe 1.15: 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.

- Schätzen Sie die Betriebssicherheit für einen Service mit einer Dauer von einer Stunde.

$Z_S \approx 10^5$ SL/FF (SL – Service-Leistungen; FF – Fehlfunktionen)

Kontrollen

Aufgabe 1.16: Sicherheitserhöhung durch Kontrollen

Um die Betriebssicherheit im Beispiel zuvor[3] auf 10^6 zu erhöhen, soll das System um eine Funktionsüberwachung ergänzt werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

1. Wie hoch muss die Erkennungssicherheit abschätzungsweise sein, wenn beim Überführen in den sicheren Zustand keine Fehlfunktionen auftreten können?
2. Wie hoch muss die Erkennungswahrscheinlichkeit sein, wenn zu erwarten ist, dass jeder 20te Versuch, einen sicheren Zustand herzustellen, scheitert?
3. In welchem mittleren zeitlichen Abstand wird überschlagsweise ein sicherer Zustand hergestellt, ohne dass die Betriebssicherheit gefährdet ist?

[3] Zuverlässigkeit 10^3 SL/FF. Jede 100ste Fehlfunktion kritisch für die Betriebssicherheit.

Zur Kontrolle

Zur Erhöhung der Sicherheit von $Z_S \approx 10^5$ SL/FF auf $Z_S \approx 10^6$ SL/FF muss das System im Mittel bei 9 von 10 FF in den sicheren Zustand versetzt werden.

1. Wenn jeder Versuch erfolgreich ist, genügt es, 9 von 10 (sicherheitskritischen) Fehlfunktionen zu erkennen:
$$p_E = E(EC) \approx 90\%$$
2. Wenn jeder 20-te Versuch scheidert, dann müssen 19 von 20 (sicherheitskritischen) Fehlfunktionen erkannt werden:
$$p_E = E(EC) \approx 95\%$$
3. Ein sicherer Zustand wird etwa aller 1000 h hergestellt. Notwändig ist es aber nur aller 10^5 h. Mittlere Zeit zwischen zwei Phantomfehlern, hier der unnötigen Hergestellung eines sicheren Zustands:
$$\frac{1}{10^{-3}\mathrm{h}^{-1} - 10^{-5}\mathrm{h}^{-1}} \approx 10^3\,\mathrm{h}$$

Aufgabe 1.17: Phantomfehlerwahrscheinlichkeit

Das Erkennen und die Reaktion auf eine nicht sicherkeitskritische Fehlfunktion in der Aufgabe zuvor sei ein Phastomfehler.

- Mit welcher Wahrscheinlichkeit ist bei einem Service ein Phantomfehler zu erwarten?

Ein Phantomfehler aller 1000 SL:

$$p_{\text{Phan}} = \frac{1\,\text{h}}{10^3\,\text{h}} = 0{,}1\%$$

Test

Aufgabe 1.18: Zufallstest

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

1. Wie lange dauert es im Mittel, bis ein Zufallstest jeden dieser Fehler nachgewiesen hat?

1. Fehler	2. Fehler
$E(n_1) =$	$E(n_2) =$

2. Mit welcher Wahrscheinlichkeit werden beide Fehler mit 1000 Testschritten mindestens einmal nachgewiesen?

1. Fehler	2. Fehler
$p_1(1000) =$	$p_2(1000) =$

Beide Fehler:

Zur Kontrolle

1. Mittlere Zeit, bis jeden dieser Fehler nachgewiesen ist?
   Kehrwert der Nachweiswahrscheinlichkeit:

1. Fehler	2. Fehler
$E(n_1) = 10^3$	$E(n_2) = 5 \cdot 10^2$

2. Nachweiswahrscheinlichkeiten mit 1000 Testschritten:

$$p_i(n) = 1 - (1 - p_i)^n \approx 1 - e^{-n \cdot p_i}$$

1. Fehler	2. Fehler
$p_1(10^3) = 1 - e^{-1} = 63{,}2\%$	$p_2(10^3) = 1 - e^{-2} = 86{,}5\%$

Beide Fehler:

$$p_1(10^3) \cdot p_2(10^3) = 54{,}7\%$$

Aufgabe 1.19: Test als Filter

Bei einem Software-Test werden

- beim Review 30 Fehler,
- vom Syntaxtest 100 Fehler,
- von den dynamischen Test 80 Fehler

von insgesamt schätzungsweise 300 Fehlern erkannt.

1. Wie groß sind die Fehlerüberdeckungen der einzelnen Tests und aller Tests zusammen?

Review	Syntaxtest	dyn. Test.	zusammen
$FC_{\mathrm{R}} =$ ——	$FC_{\mathrm{S}} =$ ——	$FC_{\mathrm{D}} =$ ——	$FC_{\mathrm{ges}} =$ ——

2. Wie groß ist abschätzungsweise die Anzahl der nicht erkannten Fehler, wenn ein System mit abschätzungsweise 30.000 Fehlern (hundertfache Systemgröße) in derselben Weise getestet wird?

Zur Kontrolle

1. Fehlerüberdeckungen der einzelnen Tests und aller Tests zusammen:

Review	Syntaxtest	dyn. Test.	zusammen
$FC_{\mathrm{R}} = \frac{30}{300}$	$FC_{\mathrm{S}} = \frac{100}{300}$	$FC_{\mathrm{D}} = \frac{80}{300}$	$FC_{\mathrm{ges}} = \frac{210}{300}$

2. Für ein hundert mal so großes System:
   - Im Referenzsystem mit 300 Fehlern werden ca. 90 nicht erkannt.
   - In einem hundert mal so großen System werden es bei vergleichbarem Entstehungsprozess und gleich guten Tests etwa hundert mal so viele sein, d.h. etwa 9.000 nicht erkannte Fehler.

Fehleranteil, Entstehungspr.

Aufgabe 1.20: Fehleranteil eines Rechners

Ein Steuerrechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerstände, 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.

Aufgabe 1.21: Fehleranzahl in einem Software-System

Wie viele Fehler sind in einem großen Software-System mit 10^5 Programmzeilen zu erwarten, wenn beim Entwurf 3% der Programmzeilen falsch sind und der Test 60% der Fehler erkennt?