Test und Verlässlichkeit Grosse Übung zu Foliensatz 2

Prof. G. Kemnitz

13. Juni 2018

Contents

1 Fehlerbeseitigung

Aufgabe 2.1: Test als Filter

Bei einem Software-Test werden

- beim Korrekturlesen (Review) $\varphi_{\text{Erk.Rev}} = 30$ Fehler,
- vom Syntaxtest $\varphi_{\text{Erk.Synt}} = 100$ Fehler,
- vom Test mit Beispieleingaben $\varphi_{\text{Erk.DT}} = 80$ Fehler

von insgesamt schätzungsweise $\varphi \approx 300$ Fehlern erkannt.

1. Wie groß sind die Fehlerüberdeckungen der einzelnen Tests und aller Tests zusammen?
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
$FC_{\text{R}} = \frac{30}{300}$	$FC_{\text{S}} = \frac{100}{300}$	$FC_{\text{D}} = \frac{80}{300}$	$FC_{\text{ges}} = \frac{210}{300}$

2. Für ein hundert mal so großes System:
   - Im Referenzsystem mit $\varphi \approx 300$ Fehlern werden ca. $\varphi_{\text{NErk}} \approx 90$ 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 $\varphi_{\text{NErk}} \approx 9000$ nicht erkannte Fehler.

Aufgabe 2.2: Ersatz

Für ein gefertigtes Gerät ist die zu erwartende Ausbeute $E(Y) = 60\%$ und der Test erkennt $p_{\mathrm{E}} = 90\%$ der fehlerhaften Geräte. Erkannte fehlerhafte Geräte werden ersetzt.

1. Wie groß ist die Wahrscheinlichkeit p_{F}, dass ein gefertigtes Gerät fehlerhaft ist?
2. Wie hoch ist der zu erwartende Fehleranteil nach Ersatz der erkennbar defekten Geräte?

Zur Kontrolle

1. Die Ausbeute ist der Anteil der Objekte ohne erkennbare Fehler:

$$E(Y) = 1 - p_{\mathrm{E}} \cdot E(DL_{\mathrm{EP}})$$

Zu erwartender Fehleranteil:

$$E(DL_{\mathrm{EP}}) = \frac{1 - E(Y)}{p_{\mathrm{E}}} = \frac{1 - 60\%}{90\%} = 44{,}4\%$$

2. Zu erwartender Fehleranteil nach Ersatz der erkennbar defekten Objekte:

$$E(DL_{\mathrm{Ers}}) = \frac{p_{\mathrm{F}} \cdot (1 - p_{\mathrm{E}})}{1 - p_{\mathrm{F}} \cdot p_{\mathrm{E}}} = \frac{44{,}4\% \cdot (1 - 90\%)}{1 - 44{,}4\% \cdot 90\%} = 7{,}4\%$$

($p_{\mathrm{F}} = E(DL_{\mathrm{EP}})$ – Wahrscheinlichkeit, dass ein Objekt vor der Beseitigungsiteration fehlerhaft ist).

Aufgabe 2.3: Fehlerbeseitigung durch Reparatur

Ein Programm von 1.000 NLoc habe abschätzungsweise nach dem Syntaxtest und der erfolgreichen Abarbeitung der ersten Testbeispiele noch 20 Fehler. Der nachfolgende Test habe einer Erkennungswahrscheinlichkeit von $p_{\mathrm{E}} = 60\%$.

1. Wie groß muss die Reparaturgüte Q_{Rep} mindestens sein, damit sich die Anzahl der nicht beseitigten Fehler halbiert?
2. Wie groß darf die Fehlerentstehungsrate η_{Rep} (neu entstehende Fehlern je Reparaturversuch) maximal sein, wenn die Erfolgswahrscheinlichkeit der Reparatur $p_{\mathrm{R}} = 30\%$ beträgt?

Zur Kontrolle

- Erkennungswahrscheinlichkeit des Tests: $p_{\mathrm{E}} = 60\%$
- Halbierung der zu erwartenden Fehleranzahl: $p_{\mathrm{NBes}} = 50\%$.
- Erfolgswahrscheinlichkeit der Reparatur: $p_{\mathrm{R}} = 30\%$

1. Reparaturgüte Q_{Rep}:

$$\begin{aligned} p_{\mathrm{NBes}} &= \left(1 + \frac{p_{\mathrm{E}}}{Q_{\mathrm{Rep}}}\right) \cdot (1 - p_{\mathrm{E}}) \\ Q_{\mathrm{Rep}} &= \frac{p_{\mathrm{E}}}{\frac{p_{\mathrm{NBes}}}{1-p_{\mathrm{E}}} - 1} = \frac{60\%}{\frac{50\%}{1-60\%} - 1} = 2{,}4 \end{aligned}$$

2. Max. zulässige Fehlerentstehungsrate:

$$\begin{aligned} Q_{\mathrm{Rep}} &= \frac{p_{\mathrm{R}}}{(1 - p_{\mathrm{R}}) \cdot \eta_{\mathrm{Rep}}} \geq 2{,}4 \\ \eta_{\mathrm{Rep}} &= \frac{p_{\mathrm{R}}}{(1 - p_{\mathrm{R}}) \cdot Q_{\mathrm{Rep}}} \leq \frac{30\%}{(1 - 30\%_{\mathrm{R}}) \cdot 2{,}4} = 17{,}86\% \end{aligned}$$

Aufgabe 2.4: Kontrollfragen zur Reparatur

1. Angenommen, ein Reparaturmechaniker baut getauschte Teile eines defekten Rechners ohne nachweisbare Fehler in andere Rechner ein. Wie wirkt sich das auf die zu erwartende Fehleranzahl der reparierten Rechner aus?
2. Warum ist das Pareto-Prinzip für Fehler und Fehlfunktionen
   - für den Test ein Nachteil und
   - für die Fehlerlokalisierung ein Vorteil?

Zur Kontrolle

1. Die zu erwartende Fehleranzahl hängt davon ab, ob die vermeindlich ganzen aus anderen Rechnern ausgebauten Teile einen höheren zu erwartenden Fehleranteil als neue Ersatzteile haben. Der Anteil der Herstellungsfehler, die der Herstellertest nicht erkannt hat, erhöht sich nicht, wenn ein Rechnerteil in einem anderen Rechner eingebaut war. Der Fehleranteil durch Ausfälle, die der Testsatz des Mechanikers nicht erkennt, tut das, wenn der Mechanikertestsatz eine geringere Überdeckung als der Herstellertestsatz hat.

2. Das Pareto-Prinzip für Fehler und Fehlfunktionen besagt, dass es rekursiv nach Beseitigung der dominanten Fehler weiterhin eine kleine Menge dominanter Fehler gibt, die die Mehrheit der FF verursacht. Das bedeutet
   - für den Test, dass es nach beliebig aufwändigen Tests immer noch Fehler gibt, deren Entdeckung noch aufwändigere Tests verlangt.
   - für die Lokalisierung, dass es meist Vorzugsfehler gibt, bei denen es Sinn macht, explizit zu testen, ob sie vorhanden sind.

2 Reifeprozesse

Aufgabe 2.5: Zuverlässigkeitswachstum

Ein bei $N_{\mathrm{Nutzer}} = 10^4$ Nutzern eingesetztes Software-System hat nach einer Reifedauer von $t_0 = 100$ Tagen eine fehlerbezogene Teilzuverlässigkeit von $Z_{\mathrm{F}}(t_0) = 10^5\,\frac{\mathrm{SL}}{\mathrm{FF}}$. Die Testdauer vor dem Einsatz sei gegenüber der Summe der Nutzungsdauern bei allen Anwendern vernachlässigbar und die QQ-Funktion sei eine Potenzfunktion mit einem Exponenten $k \geq 0{,}4$.
Nach wie vielen weiteren Tagen

1. verdoppelt,
2. verzehnfacht

sich etwa die fehlerbezogene Teilzuverlässigkeit, wenn sich die Nutzungshäufigkeit und die Wahrscheinlichkeit, dass ein Fehler, wenn er an einer verursachten FF erkannten wird, beseitigt wird, nicht ändert?

Zur Kontrolle

Wenn sich die Nutzungshäufigkeit und die Wahrscheinlichkeit, dass ein Fehler, wenn er an einer verursachten FF erkannten wird, beseitigt wird, nicht ändert, ist das Verhältnis $\frac{t}{t_0}$ (t – Nutzungsdauer insgesamt) etwa das Verhältnis $\frac{n}{n_0}$ der überwachten Service-Leistungen:

$$\frac{Z_{\mathrm{F}}(n)}{Z_{\mathrm{F}}(n_0)} = \left(\frac{n}{n_0}\right)^{k+1} \approx \left(\frac{t}{t_0}\right)^{k+1}$$

Aufgelöst nach der Gesamtnutzungsdauer:

$$t \approx t_0 \cdot \left(\frac{Z_{\mathrm{F}}(n)}{Z_{\mathrm{F}}(n_0)}\right)^{\frac{1}{k+1}} \leq 100 \cdot \left(\frac{Z_{\mathrm{F}}(n)}{Z_{\mathrm{F}}(n_0)}\right)^{\frac{1}{1,4}}$$

beträgt die zusätzlich erforderliche Reifedauer:

$\frac{Z_F(n)}{Z_F(n_0)}$	2	10
$t-t_0$	$\leq$64 Tage	$\leq$418 Tage

Aufgabe 2.6: Modell von Musa und Goel-Okumoto

Das am häufigsten zitiertes Zuverlässigkeitswachstumsmodell[1] unterstellt für den Zusammenhang zwischen der Anzahl der nicht beseitigten Fehler und der Reifezeit t folgende Funktion

$$\varphi(t) = a \cdot e^{-bt}$$

(a, b – experimentell zu bestimmende Parameter). Welche QQ-Funktion $h(x)$ liegt dieser Annahme zugrunde?

Ansatz: Ersatz der Parameter $a = c_1$ und $t = \frac{c_2}{b} \cdot n$ sowie der Fehleranzahl durch die zu erwartende Fehleranzahl der nicht beseitigten Fehler:

$$E(\varphi(n)) = c_1 \cdot e^{-c_2 \cdot n}$$

und suche einer QQ-Funktion $h(x)$, die das bewirkt:

$$E(\varphi(n)) = c_1 \cdot e^{-c_2 \cdot n} = \int_0^\infty h(x) \cdot e^{-\frac{p_{\text{Bes}} \cdot n}{x}} \cdot dx$$

Zur Kontrolle

Ein $h(x)$, dass die Gleichung

$$c_1 \cdot e^{-c_2 \cdot n} = \int_0^\infty h(x) \cdot e^{-\frac{p_{\text{Bes}} \cdot n}{x}} \cdot dx$$

erfüllt, darf nur für einen Wert x_0 ungleich 0 sein:

$$\begin{aligned} h(x) &= \begin{cases} a & \text{für } x = x_0 \\ 0 & \text{sonst} \end{cases} \\ c_1 \cdot e^{-c_2 \cdot n} &= a \cdot e^{-\frac{p_{\text{Bes}} \cdot n}{x_0}} \cdot dx \end{aligned}$$

mit $c_1 = a \cdot dx$ und $c_2 = \frac{p_{\text{Bes}}}{x_0}$.

Das Musa-Goel-Okumoto-Modell beschreibt den Sonderfall, dass alle Fehler dieselbe Nachweiswahrscheinlichkeit haben.

3 Ausfälle

Aufgabe 2.7: Überlebenswahrscheinlichkeit

1. Wie groß ist die Überlebenswahrscheinlichkeit eines zum Zeitpunkt $t = 0$ funktionierenden Systems mit einer über die Zeit konstanten Ausfallraten von $\lambda = 1000\,\text{fit}$ nach einer Nutzungsdauer von 100 Tagen?
2. Wie lang darf das Zeitinvall T_w sein, in dem das System gewartet wird[2], damit die Überlebenswahrscheinlichkeit nicht kleiner als 99,9% wird?

Zur Kontrolle

Bei einer konstanten Ausfallrate gilt für die Überlebenswahrscheinlichkeit:

$$\begin{aligned} \lambda &= -\frac{1}{R(t)} \cdot \frac{d\,R(t)}{dt} \\ R(t) &= \text{const.} \cdot e^{-\lambda \cdot t} \end{aligned}$$

Aus der Zusatzbedingung $R(0) = \text{const.} \cdot e^{-\lambda \cdot 0} = 1$ folgt $R(t) = e^{-\lambda \cdot t}$.

[1] Benedikte Elbel, Zuverlässigkeitsorientiertes Testmanagement (2003)

[2] Wartung hier im Sinne von Test und Ersatz oder Repartur ausgefallener Systeme.

1. Überlebenswahrscheinlichkeit nach $t = 100\,\text{Tage} = 2400\,\text{h}$ bei $\lambda = 1000\,\text{fit} = 10^{-9}\,\text{h}^{-1}$:

$$R(t) = e^{-10^{-6}\,\text{h}^{-1}\cdot 2400\,\text{h}} = 99{,}76\%$$

2. Wartungsintervall T_w für $R(t = T_\text{w}) \geq 99{,}9\%$:

$$T_\text{w} \leq -\frac{\log(R(T_\text{w}))}{\lambda} = -\frac{\log(99{,}9\%)}{10^{-6}\,\text{h}^{-1}} = 1.000\,\text{h} = 41{,}7\,\text{Tage}$$

Aufgabe 2.8: Mittlere Lebensdauer

Wie groß ist die mittlere Lebensdauer eines Rechners aus

- 30 Schaltkreisen mit einer Ausfallrate von 150 fit,
- 100 diskreten Bauteilen mit einer Ausfallrate von 30 fit und
- 500 Lötstellen mit einer Ausfallrate von 0,5 fit?

Zur Kontrolle

Die Ausfallraten addieren sich. Gesamtausfallrate:

$$30 \cdot 150\,\text{fit} + 100 \cdot 30\,\text{fit} + 500 \cdot 0{,}5\,\text{fit} = 7750\,\text{fit}$$

Zu erwartende (mittlere) Lebensdauer:

$$\begin{aligned} E(t_\text{L}) &= \int_0^\infty R(t) \cdot dt \\ &= \int_0^\infty e^{-\lambda \cdot t} \cdot dt \\ &= \frac{1}{\lambda} = \frac{1}{7750 \cdot 10^{-9}\,\text{h}^{-1}} = 129 \cdot 10^3\,\text{h} = 14{,}7\,\text{Jahre} \end{aligned}$$

Aufgabe 2.9: Ausfall vs. Entwurfsfehler

Warum verursacht ein durch Ausfall während der Nutzung entstandener Fehler im Mittel viel mehr Fehlfunktionen als ein nicht beseitigter Entwurfsfehler?

Zur Kontrolle

Für die Fehlfunktionen durch Ausfälle und Entwurfsfehler gilt gleichermaßen das Pareto-Prinzip. Ein kleiner Anteil der entstehenden Fehler verursacht die Mehrheit der Fehlfunktionen. Der Unterschied ist, dass die dominaten Entwurfsfehler, die viele FF verursachen, im Einsatz beseitigt und die dominaten Ausfälle, die viele FF verursachen, bis zur nächsten Reparatur noch vorhanden sind.

Aufgabe 2.10: Frühausfälle, Voralterung

1. Was ist Voralterung und wie erhöht sich durch sie die mittlere Lebensdauer der vorgealterten Objekte?
2. Ein Rechner wird zum Nutzungsbeginn einen Monat lang mit erhöhter Betriebsspannung und übertaktet betrieben. Mindert oder erhöht das die Ausfallrate innerhalb der nachfolgenden ein bis zwei Jahre[3]?
3. Verkürzt oder verlängert ein zeitlich begrenzter übertakteter Betrieb mit erhöhter Betriebsspannung die mittlere Lebensdauer?

---

[3] Die Ermügungsphase beginnt erst nach mehreren Jahren, in der Regel mit dem Austrocknen der Elektrolytkondensatoren in den Netzteilen.

Zur Kontrolle

1. Voralterung erhöht die Ausfallrate auch für die potentiellen Schwachstellen, die Frühausfälle verursachen. Die kränklichen Bauteile sterben und werden vor dem Einsatz ersetzt. Unter normalen Betriebsbedingungen ist die Ausfallrate vorgealterter Bauteile geringer und die mittlere Lebensdauer höher.
2. Der übertaktete Betrieb mit erhöhter Betriebsspannung ist eine Voralterung. Überleben tun die Systeme ohne Kinderkrankheiten. Die Ausfallrate innerhalb der nachfolgenden ein bis zwei Jahre ist geringer.
3. Alle Ausfälle eingerechnet verkürzt Stress die mittlere Lebensdauer. Werden nur die Ausfälle nach dem Stressbetrieb vor der Verschleißphase betrachtet, erhöht sich die mittlere Lebensdauer. Stress führt natürlich auch dazu, dass die Verschleißphase eher beginnt.

Aufgabe 2.11: Kalte, und heiße Reserve

1. Wie hoch ist die mittlere Lebensdauer $E(t_{\mathrm{L.ges}})$ einer Lichterkette in Form einer Reihenschaltung aus 10 Lampen, wenn jede Lampe einzeln eine mittlere Lebensdauer von $E(t_{\mathrm{L.L}}) = 1000\,\mathrm{h}$ besitzt?
2. Auf welchen Wert erhöht sich die mittlere Lebensdauer, wenn eine zusätzlich kalte Reserve von 2 Ersatzlampen existiert, die zum Beanspruchungsbeginn noch funktionieren und die ersten zwei ausfallenden Lampen ersetzen.

Zur Kontrolle

1. Die Ausfallrate ist der Kehrwert der mittleren Lebsdauer. Eine Reihenschaltung fällt aus, wenn mindestens eine Lampe ausfällt, d.h. die Ausfallraten und die Kehrwerte der mittleren Lebensdauern addieren sich:
$$\frac{1}{E(t_{\mathrm{L.ges}})} = 10\cdot\frac{1}{E(t_{\mathrm{L.L}})};\ E(t_{\mathrm{L.ges}}) = \frac{E(t_{\mathrm{L.L}})}{10} = 100\,\mathrm{h}$$
2. Das Gesamtsystem mit zwei Lampen als kalte Reserve fällt aus, wenn dreimal eine von zehn Lampen ausgefallen ist. Die mittlere Lebensdauer verdreifacht sich:
$$E(t_{\mathrm{L.2KR}}) = 3\cdot E(t_{\mathrm{L.ges}}) = 300\,\mathrm{h}$$

Aufgabe 2.12: Dauerbetrieb oder Ausschalten

Das Netzteil eines Rechners habe im normalen Betrieb eine Ausfallrate $\lambda = 9000$ fit. Im ausgeschalteten Zustand sei die Ausfallrate 0. Bei einem Einschaltvorgang werden die Bauteile des Netzteils stärker belastet, so dass das Netzteil mit einer Wahrscheinlichkeit von 0,01% ausfällt. Ab welcher Ausschaltdauer verringert das Ausschalten die Ausfallwahrscheinlichkeit des Rechners?

Zur Kontrolle

Die gesuchte Ausschaltdauer t_{AD} ist die Zeit, ab der die Wahrscheinlichkeit eines Ausfalls im normalen Betrieb größer als die Ausfallwahrscheinlichkeit p_{ES} beim Einschalten ist:

$$\begin{aligned} 1 - R(t_{\mathrm{AD}}) &= 1 - e^{-\lambda\cdot t_{\mathrm{AD}}} < p_{\mathrm{ES}} \\ t_{\mathrm{AD}} &> -\frac{\ln(1-p_{\mathrm{ES}})}{\lambda} = -\frac{\ln(1-0{,}01\%)}{9000\cdot 10^{-9}\mathrm{h}^{-1}} \approx 11\,\mathrm{h} \end{aligned}$$

4 Umgang mit FF

Aufgabe 2.13: Beispiele für die Fehlerbehandlung

Nennen Sie Beispiele (Ihnen bekannte Programme und Geräte) die folgende Techniken nutzen:

1. Zeitüberwachung mit Service-Abbruch bei Zeitüberschreitung.
2. Wiederholungsanforderung nach fehlerhaftem Datenempfang.
3. Systemen, bei denen sich Fehlverhalten durch andere Eingabereihenfolgen, Nutzung andere Eingabemenüs etc. umgehen lassen.
4. Systeme, die vor dem Ausschalten automatisch ihre Bearbeitungszustand sichern.
5. Systeme, die nach einer Fehlfunktion vom letzten gesicherten Zustand starten.
6. Versenden von Fehlerinformationen an die Firma, die das System entwickelt hat.

Zur Kontrolle

1. Zeitüberwachung mit Abbruch bei Zeitüberschreitung: Lesezugriffe auf Laufwerke. Lesezugriffe auf Daten im Internet. ...
2. Wiederholung nach fehlerhaftem Datenempfang: Standardreaktion auf Prüfsummenfehler beim Datenempfang, Buskollisionen CAN-Bus, Ethernet, ...
3. Beseitigung des Fehlverhalten durch geänderte Eingabereihenfolge: XFig, Textbearbeitung. Beim Löschen vorwärts Programmabsturz, beim Löschen rückwärts kein Absturz.
4. Automatische Sicherung des Bearbeitungszustands beim Ausschalten: Handys, Tablets, ...
5. Start vom letzten gesicherten Zustand: Typisch für Textverarbeitungssysteme.
6. Versenden von Fehlerberichten: Windows, Linux, ...

Aufgabe 2.14: Fail-Safe/-Fast/-Slow

1. Was besagt das Ruhestromprinzip?
2. Eine Software sei so programmiert, dass mit einem Compieler-Schalter zwischen Fail-Fast und Fail-Slow umgeschalten werden kann. Wann wird es wie übersetzt und warum?

Zur Kontrolle

1. Das System wird so aufgebaut, dass bei Ausfall der Kontrollfunktion die Notfallbehandlung eingeleitet wird.
2. Fail-Fast für den Test und Probebetrieb, um möglichst viele Probleme zu erkennen und Fehler zu finden. Fail-Slow für den Einsatz, weil so die Zuverlässigkeit höher ist.

Aufgabe 2.15: Fehlerisolation

1. Welche Konzepte dienen in modernen Betriebssystemen zur Fehlerisolation zwischen nebenläufig auf Rechner abzuarbeitenden Prozessen?
2. Welche Hardware-Funktionen stellen dafür moderne Prozessoren zur Verfügung?

Zur Kontrolle

1. Welche Konzepte dienen in modernen Betriebssystemen zur Fehlerisolation zwischen nebenläufig auf Rechner abzuarbeitenden Prozessen:
   - Virtuelle Adressierung, die jedem Prozess nur Zugriff auf eigene Daten erlaubt.
   - Zugriff auf Betriebssystemdienste (Bereitstellung von physikalischem Speicher, Zugriff auf EA-Geräte, ...) über Systemrufe, ...
2. Hardware-Funktionen für die Fehlerisolation:
   - Adressrecheneinheit, TLB (Übersetzungs-Cache zwischen virtuellen und physikalischen Adressen, Cache-Controller, ...;
   - Systemrufe: Software-Interrupts, privelegierte Befehle z.B. zur Umprogrammierung der TLB- und Cache-Speicher, ...

Aufgabe 2.16: 3-Versionssystem

Für ein 3-Versionssystem mit folgenden Wahrscheinlichkeiten je SL:

- $p_{\mathrm{FF}} = 10^{-5}$ zufällige Fehlfunktion in einem Teilsystem
- $p_{\mathrm{FA}} = 10^{-1}$ wenn die erste SL eine FF ist, sind die beiden anderen dieselbe FF.

wie groß sind unter der Annahme, dass zwei zufällige Verfälschungen praktisch nie übereinstimmen, die Wahrscheinlichkeiten:

1. p_{NFF} keine Fehlerfunktion (alle 3 SL korrekt),
2. p_{FK} falsche Korrektur (übereinstimmende FF),
3. p_{KFF} korrigierbare FF (zwei SL korrekt, eine FF, keine »falsche Korrektur«),
4. p_{ENK} erkennbare, aber nicht korrigierbare FF (mindestens zwei FF).

Zur Kontrolle

1	K	F	K	F	K	F	K	F	A
2	K	K	F	F	K	K	F	F	A
3	K	K	K	K	F	F	F	F	A
	a	c	c	d	c	d	d	d	b

1. keine Fehlerfunktion:
$$p_{\mathrm{NFF}} = (1 - p_{\mathrm{FF}})^3 \approx 1 - 3 \cdot p_{\mathrm{FF}} = 1 - 3 \cdot 10^{-5}$$
2. falsche Korrektur: eine FF und zwei identische FF
$$p_{\mathrm{AFF}} = p_{\mathrm{FF}} \cdot p_{\mathrm{FA}} = 10^{-5} \cdot 10^{-1} = 10^{-6}$$
3. korrigierbar: 3 Fälle eine FF und zwei korrekte, nicht abhängig
$$p_{\mathrm{KFF}} = 3 \cdot p_{\mathrm{FF}} \cdot (1 - p_{\mathrm{FF}})^2 - p_{\mathrm{AFF}} = 2{,}9 \cdot 10^{-5}$$
4. erkenn-, nicht korrigierbar: 3 Fälle zwei unabhängige FF ...:
$$p_{\mathrm{ENK}} = 3 \cdot p_{\mathrm{FF}}^2 \cdot (1 - p_{\mathrm{FA}})^2 + p_{\mathrm{FF}}^3 = 3 \cdot 10^{-10}$$

5 Fehlervermeidung

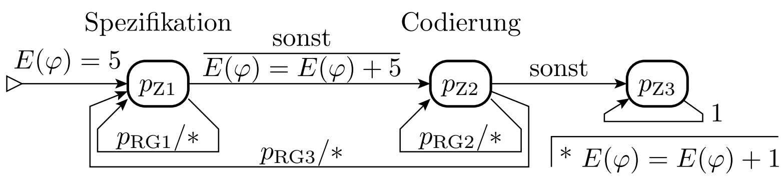
Aufgabe 2.17: Fehlervermeidung allgemein

1. Warum sollten Entstehungsprozesse möglichst deterministisch arbeiten?
2. Wie wird der Reparaturerfolg bei nicht deterministischen Prozessen kontrolliert?
3. Warum ist nach erfolglosen Reparaturversuchen stets ein Rückbau zu empfehlen?
4. Warum hat der Fehleranteil von Produkten typischerweise einen sägezahnförmigen Verlauf mit der Nutzungsdauer?

Zur Kontrolle

1. Determinismus ist Voraussetzung für die Erfolgskontrolle einer Fehlerbeseitigung durch Testwiederholung, d.h. für eine einfache Erfolgskontrolle nach Reparaturversuchen.
2. Bei nicht deterministischen Prozessen wird der Erfolg von Verbesserungen anhand von Erwartungswerten, Varianzen, Verteilungen, ... messbarerer Produkteigenschaften kontrolliert. Verlangt statt einer Prozesswiederholung eine statistisch signifikante Anzahl von sehr viele Wiederholungen.
3. Ein Rückbau beseitigt die möglicherweise bei der Reparatur neu entstandenen Fehler.
4. Innovationen verringern die Streuungen der Zielgrößen. Dabei geht die Zentrierung verloren und der Fehleranteil steigt sprunghaft. Mit der zunehmenden Neuzentrierung verringert sich der Fehleranteil.

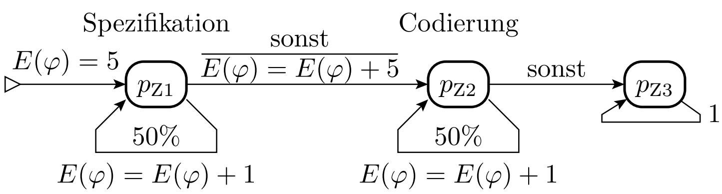
Aufgabe 2.18: Fehlerentstehung, Stufenmodell



In dem vereinfachten Stufenmodell entstehen in den beiden Phasen »Spezifikation« und »Codierung« je im Mittel 5 Fehler. Bei jedem Rückgriff entsteht im Mittel 1 weiterer Fehler. Wie groß ist die zu erwartende Anzahl der entstehenden Fehler

1. bei einer Rückgriffswahrscheinlichkeit von je 50% nach Spezifikation und Codierung ($p_{\mathrm{RG1}} = p_{\mathrm{RG2}} = 50\%$, $p_{\mathrm{RG3}} = 0$),
2. wenn bei der Hälfte der Rückgriffe nach der Codierung die Spezifikation nachgebessert wird ($p_{\mathrm{RG1}} = 50\%$, $p_{\mathrm{RG2}} = p_{\mathrm{RG3}} = 25\%$)?

Nur Einfachrückgriff: $p_{\mathrm{RG1}} = p_{\mathrm{RG2}} = 50\%$, $p_{\mathrm{RG3}} = 0$



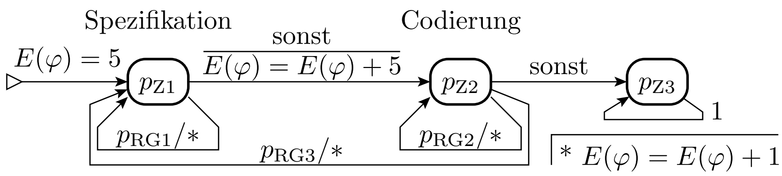
Überschlag:

- je 5 Fehler bei der »Erstspezifikation« und »Erst-Codierung«
- je $\approx \frac{1}{2} + \frac{1}{4} + \ldots$ Fehler bei den Rückgriffen

Simulation als Markov-Kette:

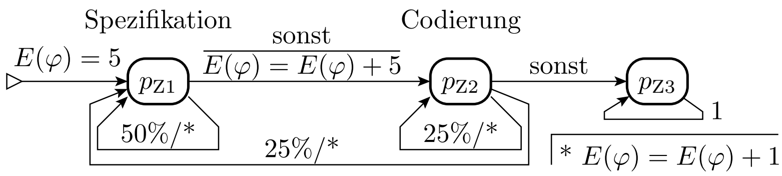
```
 1.0|  50.0%  50.0%   0.0% |   8.00
 2.0|  25.0%  50.0%  25.0% |   9.75
 3.0|  12.5%  37.5%  50.0% |  10.75
 ...
15.0|   0.0%   0.0% 100.0% |  12.00
```

Simulationsprogramm:




```
pRG1 = 0.5; pRG2 = 0.25; pRG3 = 0.25;
pZ = [1; 0; 0]; Ephi = 5;
M = [    pRG1           pRG3   0;
       1-pRG1           pRG2   0;
            0 1-pRG2-pRG3   1];
for idx=1:50
 Ephi += pZ(1)*(1*pRG1 + 5*(1-pRG1)) + ...
         pZ(2)*(1*pRG2 + 1*pRG3);
 pZ = M * pZ;
 printf('%4.1f|%6.1f%%%6.1f%%%6.1f%% |%6.2f\n', ...
         idx, 100*pZ, Ephi);
end
```

50% Spez.-Änderungen nach der Cod.- Rückgriffen




```
 1.0|  50.0%  50.0%   0.0% |   8.00
 2.0|  37.5%  37.5%  25.0% |   9.75
 3.0|  28.1%  28.1%  43.8% |  11.06
 4.0|  21.1%  21.1%  57.8% |  12.05
 5.0|  15.8%  15.8%  68.4% |  12.79
 6.0|  11.9%  11.9%  76.3% |  13.34
 7.0|   8.9%   8.9%  82.2% |  13.75
 8.0|   6.7%   6.7%  86.7% |  14.07
 ...
28.0|   0.0%   0.0% 100.0% |  15.00
```

Aufgabe 2.19: Projekte

1. Welches grundlegende Problem haben Projekte für die Fehlervermeidung?
2. Wie versuchen Vorgehensmodelle dieses Problem zu lösen?
3. Welchen Nachteile hat die Einführung von Vorgehensmodellen für IT-Entwicklungen und akademische Lernprozesse?

Zur Kontrolle

1. Projekte sind einmalige nicht deterministische Abläufe. Damit kann der Fehlerbeseitigungserfolg weder durch Wiederholung von Tests noch durch viele Wiederholungen und statistischer Auswertung der Ergebnisse kontrolliert werden.
2. Vorgehensmodelle vereinheitlichen Abläufe vieler Projekte und schaffen damit die Voraussetzung für eine statistische Erfolgskontrolle für »Verbesserungen im Vorgehen«.
3. Die Erzwingung vereinheitlichter Abläufe schränkt die Kreativität und Innovationsmöglichkeiten ein, was für die IT-Entwicklung nicht immer erwünscht und in der akademischen Ausbildung eher unerwünscht ist.