Test und Verlässlichkeit (F2)
Kapitel 2: Zufallstest, Verteilungen

Prof. G. Kemnitz

Institut für Informatik, Technische Universität Clausthal

2. Juni 2015

Inhalt Foliensatz F2: Zufallstest, Verteilungen

Zufallstest

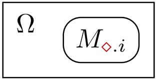
Zufälliger Fehlernachweis

Ein IT-System enthält nach Entwurf und Fertigung statistisch gesehen Fehler. Für die Anzahl ist eine Bereichsangabe möglich (siehe später Abschn. 7), aber welche Fehler vorhanden und wie diese genau nachweisbar sein werden, ist nicht vorhersagbar. Auch wenn es Techniken gibt, gezielt Tests zu suchen, ist der Fehlernachweis immer zu einem gewissen Grad Zufall.

Die zu erwartende Fehleranzahl nimmt mit der Systemgröße zu. Ein Test erkennt nur einen gewissen Anteil der Fehler und nur erkannte Fehler werden beseitigt. Große Systeme enthalten auch im Einsatz noch unerkannte Fehler, die mit gewisser Häufigkeit Fehlfunktionen verursachen.

Nachweiswahrscheinlichkeit

Nachweiswahrscheinlichkeit



Definition 1

Ein beständiger Fehler verursacht bei gleicher Eingabe immer dasselbe Fehlverhalten.

Eine Service-Anforderung hat einen Eingaberaum Ω von Bedatungsmöglichkeiten und jeder permanente Fehler i wird mit einer Teilmenge $M_i \in \Omega$ nachgewiesen. Die Nachweiswahrscheinlichkeit je Service-Anforderung ist die Wahrscheinlichkeit, dass der fehlerhafte Service mit einer Bedatung $\mathbf{x}$ aus der Nachweismenge M_i angefordert wird:

$$p_i = P\left(\mathbf{x} \in M_i\right)$$

Wenn alle Eingabewerte mit gleicher Häufigkeit auftreten:

$$p_i = \frac{|M_i|}{|\Omega|}$$

($|\ldots|$– Anzahl der Elemente der Menge).

Unbeständige Fehler haben auch eine Nachweismenge, werden aber bei einer Service-Anforderung mit einer Bedatung $M_i \in \Omega$ nur mit einer Wahrscheinlichkeit kleiner eins nachgewiesen.

Die Wahrscheinlichkeit, dass mindestens einer von n Service-Anforderungen den Fehler i nachgeweist, beträgt, wenn jede Anforderung ihn unabhängig voneinander mit p_i nachweist:

$$p_i(n) = 1 - (1 - p_i)^n$$

- Übergang zur e-Funktion:

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

  mit der Taylor-Reihe

  $$\ln(1 - p_i) = -\sum_{k=1}^{\infty} \frac{p_i^k}{k} = p_i + \frac{p_i^2}{2} + \ldots$$

  und $p_i \ll 1$ (für die Testauswahl interessierender Bereich):

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

Erforderliche Testsatzlänge

Erforderliche Testsatzlänge

$n \cdot p_i$	0,5	1	2	4	8
$p_i(n) = 1 - e^{-n \cdot p_i}$	39%	63%	86%	98%	99,97%

Der nahezu sichere Nachweis eines Fehlers verlangt einen Testsatz mit

$$n \geq \frac{4...8}{p_i}$$

zufällig bedateten Service-Anforderungen. Für die Festlegung der erforderlichen Testsatzlänge genügt es, eine Untergrenze der Fehlernachweiswahrscheinlichkeit p_{min} zu kennen.

Fakt 2

Jeder zufällig bedatete Testsatz der Länge $n \approx 4...8 \cdot p_{\mathrm{min}}^{-1}$ weist praktisch jeden Fehler nach.

Anzahl der Care-Bits

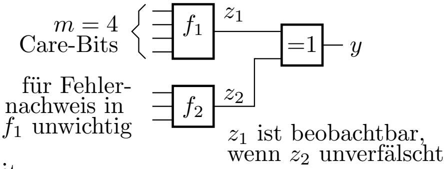
Ein Möglichkeit zur Abschätzung der Untergrenze der Fehlernachweiswahrscheinlichkeit ist das Zählen der Bits, von denen der Fehlernachweis abhängt (Care-Bits[1]). Bei einem Service ohne Gedächtnis mit m Eingabebits beträgt die Größe des Eingaberaums $|\Omega| = 2^m$ und die Größe der Nachweismenge eines Fehlers mindestens $|M_i| \geq 1$. Untergrenze der Fehlernachweiswahrscheinlichkeit bei gleicher Häufigkeit aller Bedatungen:

$$p_{\min} \geq 2^{-m}$$

Ausreichende Testsatzlänge, um nahezu alle Fehler zu erkennen:

$$n \geq 2^{m+3}$$

Die Anzahl der Care-Bits kann deutlich kleiner als die Anzahl der Eingabebits sein.

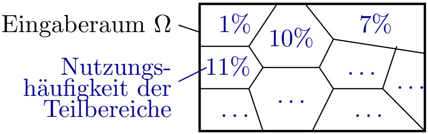


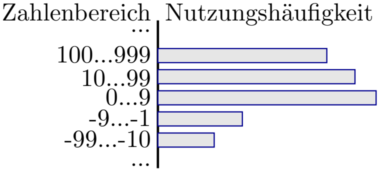
[1] Als Gegenteil von Don't-Care-Bit.

Operationsprofil

Operationsprofil

Der Eingaberaum für einen Service ist in der Regel in Teilbereiche unterteilt, die unterschiedlich häufig genutzt werden. Beispielsweise werden kleine Zahlenwerte häufiger als große und positive häufiger als negative genutzt.



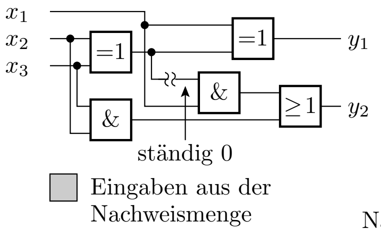


Bei einem menügesteuerten Programm werden die einzelnen Menüeinträge unterschiedlich oft ausgewählt.

Operation	Nutzungshäufigkeit
editieren	35%
löschen	12%
browse	46%
drucken	7%

Operationsprofils und Fehlernachweis

Das Operationsprofil hat erheblichen Einfluss auf die Fehlernachweiswahrscheinlichkeiten. In der Beispielschaltung ist die Verbindung zu einem Gattereingang unterbrochen, der dadurch ständig null führt. Nachweis mit zwei der acht Bedatungsmöglichkeiten. Nachweiswahrscheinlichkeit gleich Summe der Auftrittshäufigkeiten beider Bedatungen aus M_i:



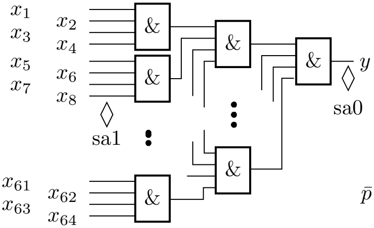
Eingabe x_3	x_2	x_1	Ausgabe y_2	y_1	Auftritts-häufigkeit	
0	0	0	0	0	0,1	0,1
0	0	1	0	1	0,05	0,1
0	1	0	0	1	0,15	0,2
0	1	1	1	0	0,2	0,05
1	0	0	0	1	0,05	0,2
1	0	1	1	0	0,2	0,05
1	1	0	1	0	0,05	0,2
1	1	1	1	1	0,2	0,1
Nachweiswahrscheinlichkeit:					0,4	0,1

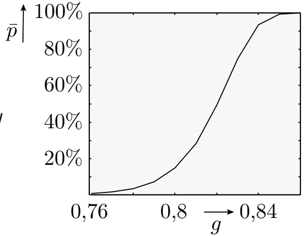
Gewichteter Zufallstest

Ein einfach zu beschreibendes/erzeugendes Operationsprofil für digitale Schaltungen ist die bitweise Wichtung:

- Auftrittswahrscheinlichkeit für Bitwert »1«
$$P\left(x_i = 1\right) = g\left(x_i\right)$$
- Auftrittswahrscheinlichkeit für Bitwert »0«
$$P\left(x_i = 0\right) = 1 - g\left(x_i\right)$$
(g_i – Wichtung).
- Auftrittswahrscheinlichkeit Eingabewert $\mathbf{x}$
$$P\left(\mathbf{x}\right) = \prod_{i=0}^{m-1} \begin{cases} g\left(x_i\right) & \text{wenn} \quad x_i = 1 \\ 1 - g\left(x_i\right) & \text{wenn} \quad x_i = 0 \end{cases}$$
(m – Bitanzahl).

Beispielschaltung:





$\bar{p}$ mittlere Nachweiswahrscheinlichkeit für $n = 10^6$ Testschritte

Angenommene Fehler: Für je einen der 64 Eingänge ständig 1:

$$p_{\mathrm{sa1}} = g^{63} \cdot (1 - g)$$

Für den Ausgang ständig 0:

$$p_{\mathrm{sa0}} = g^{64}$$

Eine Wichtung von 86% verringert die erforderliche Testsatzlänge für den Nachweis aller angenommenen Fehler von $n \approx 2^{67}$ (64 Care-Bits) auf $n \approx 10^6$.

Fakt 3

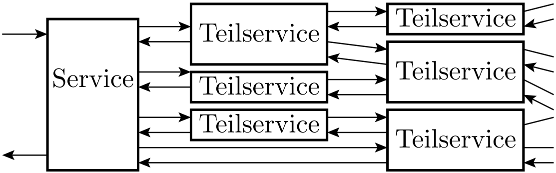
Bei gleichem Operationsprofil ist die Fehlernachweiswahrscheinlichkeit eines Fehlers je Service-Anforderung gleich der Wahrscheinlichkeit, dass der Service wegen diesem Fehler versagt.

Über diesen Zusammenhang korreliert die Testdauer und auch die bisherige Betriebsdauer, in der die erkannten Fehler beseitigt wurden, mit der fehlerfreien Betriebsdauer während des weiteren Einsatzes.

Der Test sollte idealerweise mit unterschiedlichen Operationsprofilen erfolgen. Dazu gehört auch ein Test durch einen »inkompetenten Nutzer«, der ganz andere Eingaben bevorzugt als ein normaler oder gar erfahrender Nutzer und dabei andere Fehler aufdeckt.

Steuer- und Beobachtbarkeit

Hierarchie



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

- die übergeordnete Service-Leistung den Teilservice nutzt,
- der Teil-Service mit einer Bedatung aus der Nachweismenge angefordert wird und
- das Ergebnis der Teilleistung das Gesamtergebnis verfälscht.

Der Nachweis lokaler Fehler kann entsprechend in drei Teilaspekte aufgeteilt werden:

- Nutzungshäufigkeit bzw. -wahrscheinlichkeit (Steuerbarkeit),
- Nachweiswahrscheinlichkeit bei seperatem Test und
- Beobachtbarkeit.

Die Mindestnachweiswahrscheinlichkeit $p_{\mathrm{MTS}.i}$ für Fehler in einem Teilservice i bei Anforderung der übergeordneten Service-Leistung ist abschätzungsweise:

$$p_{\mathrm{MTS}.i} \approx 1 - e^{-h \cdot p_{\mathrm{MTS}} \cdot b} \tag{2}$$

(h – Nutzungshäufigkeit von Teilservice i; $p_{\min .i}$ – minimale Nachweiswahrscheinlichkeit bei seperatem Test von Service i; b_i – Wahrscheinlichkeit, dass verfälsche Ergebnisse von Service i die Ergebnisse der übergeordneten Service-Leistung verfälschen).

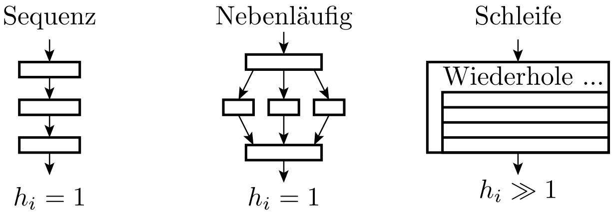
Fehler von Anweisungen in Schleifenkörpern, deren Ergebnisse direkt beobachtbar sind $(h_i \cdot p_{\mathrm{MTS}.i} \cdot b_i \gg 1)$, sind im übergeordneten Service fast sicher nachweisbar. Für schlecht nachweisbare Fehler $(h_i \cdot p_{\mathrm{MTS}.i} \cdot b_i \ll 1$ in selten genutzten und schlecht beobachtbaren Systembestandteilen vereinfacht sich Gl. 2 zu:

$$p_{\mathrm{MTS}.i} \approx h_i \cdot p_{\min .i} \cdot b_i$$

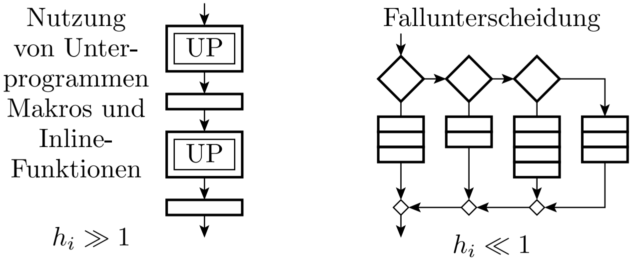
Verarbeitungsfluss und Nutzungshäufigkeit

Nutzungshäufigkeit h_i einer Teilleistung i im übergeordneten Service hängt vom Verarbeitungsfluss ab. Für Programm wird unterschieden zwischen:

- Sequenz: Eine Teil-Service-Leistung nach der anderen.
- Nebenläufig: Zeitlich unabhängige Abarbeitung mehrerer Service-Leistung und Zusammfassung der Ergebnisse.
- Schleife: Mehrfache Abarbeitung der Teil-Service-Leistungen im Schleifenkörper.



- Unterprogramme, Makros: Mehrfache Nutzung derselben Service-Leistung an unterschiedlichen Programmstellen[2].
- Fallunterscheidung: Auswahl zwischen unterschiedlichen Teilleistungen[3].

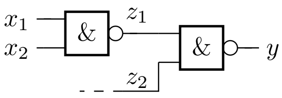


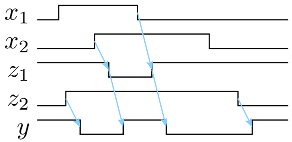
[2] Bei Makros und Include-Funktionen hat jede Instanz eigenen Code, aber der Code jeder Instanz hat dieselben Fehler, so dass es aus Sicht des Fehlernachweises egal ist, ob eine Code-Folge mehrfach aufgerufen oder mehrfach eingefügt wird.

[3] Schlecht nachweisbare Fehler sind vorrangig in Fallunterscheidungen zu erwarten.

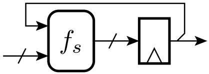
Der Verarbeitungsfluss in Schaltungen:

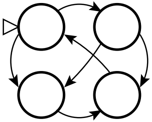
- In einer kombinatorischen Schaltung arbeiten alle Teilbausteine nebenläufig. Jede Eingabeänderung bildet sich mit einer gewissen Verzögerung auf eine Ausgabeänderung ab. Nutzungshäufigkeit der Teilschaltungen: $h_i = 1$.



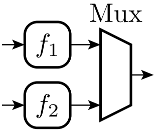


- Das Äquivalent zu eine Schleife ist ein Automat. Eine Service-Anforderung an einen Automaten erfordert i.Allg. mehrere Zustandsübergänge, für die Service-Leistungen der Übergangsfunktion und des Zustandsregisters angefordert werden. Nutzungshäufigkeit f_s: $h_i \gg 1$.



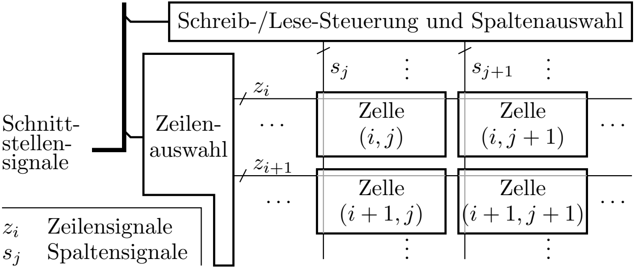


- Die Auswahl in einem Berechungsschritt erfolgt über Multiplexer. Nebenläufige Berechnung mehrer Ergebnisse und Weiterleitung nur von einem. Nutzungshäufigkeit f_i: $h_i \ll 1$.



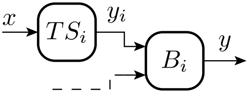
- Die geringste Nutzungshäufigkeit haben die Teil-Service-Leistungen in Speichern Lesen von und Schreiben auf eine Adresse (A – Anzahl der Adressen; $^{(*)}$ – Nur-Lese-Speicher):

$$h_i \approx \frac{1}{1^{(*)} \dots 2 \cdot A}$$



Beobachtbarkeit

Die Ergebnisse einer genutzten Teil-Service-Leistung y_i werden im Allg. mit einer Funktion B_i auf die Ergebnisse y der Gesamt-Service-Leistung abgebildet. Die Beobachtbarkeit b_i, das Verfälschungen von y_i das Gesamtergebnis y verfälschen, hängt von der Art der Verfälschung und der Funktion B_i ab.



TS_i	Teil-Service i
y_i	Ergebnisse von Teil-Service i
B_i	Beobachterfunktion für y_i

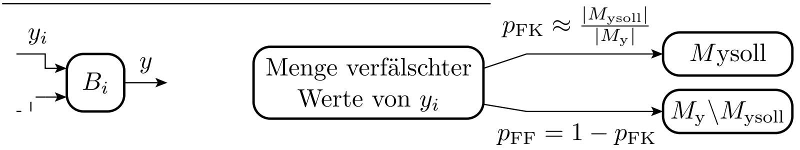
Fehlerhafte Ergebnisse einer Teil-Service-Leistung i sind immer beobachtbar ($b_i = 1$), wenn sie

- gleichzeitig Ergebnisse der Gesamt-Service-Leistung sind,
- linear oder
- mit einer umkehrbaren Funktion auf das Gesamtergebnis abgebildet werden.

Bei nicht umkehrbaren Beobachterfunktion liefert eine Mengenbetrachtung einen ersten Richtwert für die Beobachtbarkeit. Angenommen, der richtige Wert von y_i und alle Verfälschungen werden gleichwahrscheinlich auf Werte von y abgebildet. Dann ist die Beobachtbarkeit die Wahrscheinlichkeit, das ein verfälschtes y_i auf ein falsches y abgebildet wird:

$$b_i \approx p_{\mathrm{FK}} \approx 1 - \frac{|M_{\mathrm{ysoll}}|}{|M_{\mathrm{y}}|}$$

($|M_{\mathrm{y}}|$ – Anzahl der unterschiedlichen mit y darstellbaren Werte).



p_{FK}	Wahrscheinlichkeit der Klassifizierung fehlerhafter Werte als korrekt
p_{FF}	Wahrscheinlichkeit der Klassifizierung fehlerhafter Werte als fehlerhaft
M_{y}	Menge der mit y darstellbaren Werte
M_{ysoll}	Menge der zulässigen mit y darstellbaren Werte

Am schlechtesten sind tendentiell Verfälschungen bei Beobachterfunktionen mit zweiwertiger Ausgabe $|M_{\mathrm{y}}| = 2$ beobachtbar.

Für die Testauswahl und die vom Test nicht gefundenen Fehler, die die Verlässlichkeit im Einsatz beeinträchtigen, ist vor allem Kenntnis über die schwer nachzuweisenden und damit die schwer zu beobachtenden Fehler wichtig[4].

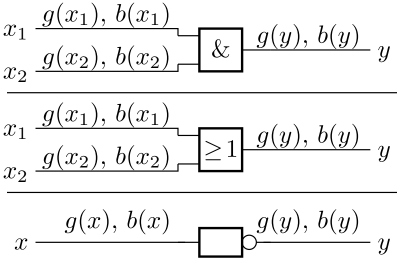
Am schlechtesten beobachtbar sind Fehler, deren Verfälschungen binär weiterverarbeitet werden:

- Fehler in digitalen Schaltungen und
- Fehler bei der Berechnung von Verzweigungsbedingungen.

[4]Die einfacher nachzuweisenden Fehler werden automatisch mit gefunden.

Beobachtbarkeit in logischen Funktionen

Die Eingabe einer UND-Operation ist beobachtbar, wenn die andere Eingabe eins, bei einer ODER-Operation, wenn die andere Eingabe null ist. Die Auftrittshäufigkeit einer Eins ist die Wichtung g und einer Null Gegenwahrscheinlichkeit $1 - g$.

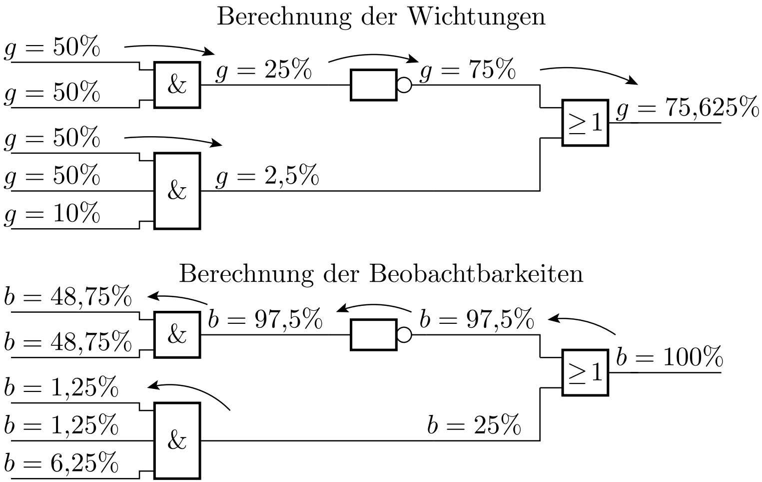


$$b(x_2) = b(y) \cdot g(x_1)$$
$$b(x_1) = b(y) \cdot g(x_2)$$
$$g(y) = g(x_1) \cdot g(x_2)$$

$$b(x_1) = b(y) \cdot (1 - g(x_2))$$
$$b(x_2) = b(y) \cdot (1 - g(x_1))$$
$$g(y) = 1 - (1 - g(x_1)) \cdot (1 - g(x_2))$$

$$b(x) = b(y)$$
$$g(y) = (1 - g(x))$$

Die Wichtungen werden in und die Beobachtbarkeiten entgegen dem Berechnungsfluss bestimmt.



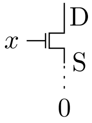
Die Beobachtbarkeit kann selbst bei wenigen logischen Operationen lokal sehr kleine Werte annehmen. Probleme bereiten rekonvergente Auffächerung (siehe Foliensatz F1, Abschn. 2.2).

Transistor- und Gatterfehler

Transistorfehler

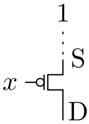
Die kleinsten in der Vorlesung betrachteten Teilsysteme sind Transistorschalter. NMOS-Transistoren können bei einer Eins am Gate eine Verbindung nach Masse[5]. PMOS-Transistoren bei einer Null am Gate eine Verbindung nach U_V schalten.

NMOS-Transistor



x	D→S
0	0 (aus)
1	1 (ein)

PMOS-Transistor



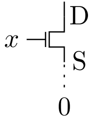
x	D→S
1	0 (aus)
0	1 (ein)

permanente Fehler:
- ständig ein (stuck-at 1)
- ständig aus (stuck-at 0)

unbeständige Fehler:
- verzögertes Einschalten
- verzögertes ausschalten

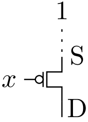
[5] Eins ist in der Vorlesung »groß« und Null »klein. Das niedrigste Potential hat Masse und das höchste U_V.

NMOS-Transistor



x	D→S
0	0 (aus)
1	1 (ein)

PMOS-Transistor



x	D→S
1	0 (aus)
0	1 (ein)

permanente Fehler:
- ständig ein (stuck-at 1)
- ständig aus (stuck-at 0)

unbeständige Fehler:
- verzögertes Einschalten
- verzögertes ausschalten

Mögliche permanente Fehlverhalten sind, dass der Transistor ständig ein- oder ausgeschaltet (Haftfehler). Mögliche unbeständige Fehlverhalten sind, das diese Fehlverhalten nur kurz nach Schaltvorgängen zu beobachten ist (Verzögerungsfehler). Unterbrechungen und Kurzschlüsse der Transistoranschlussleitungen sind ähnlich nachweisbar.

Nachweiswahrscheinlichkeiten bei einem seperaten Test mit gleichwahrscheinlicher Bedatung ist $p_i \approx 25 \ldots 50\%$.

Speicherzellen und Speicher

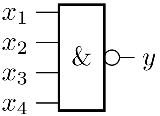
Eine Speicherzelle stellt die Service-Leitungen Schreiben, Speichern und Lesen bereit. Fehlernachweis ist nur beim Lesen möglich und erfordert allgemein eine vorherige Schreiboperation mit einem bestimmten Wert und Speichern, während andere Zellen beschrieben oder gelesen werden.
Nachweiswahrscheinlichkeit je Leseoperation $p_i = 1 \ldots 50\%$, bei Fehlern in Festwertspeichern bis 100%.

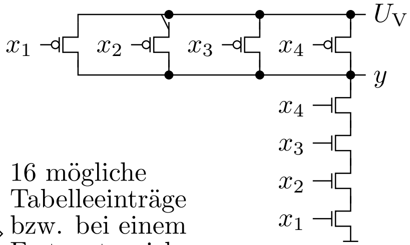
Der Service »Lesen von einem Speicherplatz« nutzt den Lese-Service der einzelnen Zellen im Mittel mit der Häufigkeit $h_i \approx 1/A$ (A – Anzahl der Adressen). Gelesene Werte sind immer beobachtbar. Nachweiswahrscheinlichkeit von Speicherfehlern je Blockspeicherzugriff:

$$p_i = \frac{1}{1 \ldots 100 \cdot A}$$

Gatterfehler

Eine logische Funktion kann unterschiedlich realisiert sein, z.B. mit Transistorschaltern oder als Blockspeicher mit einprogrammierter Wertetabelle.



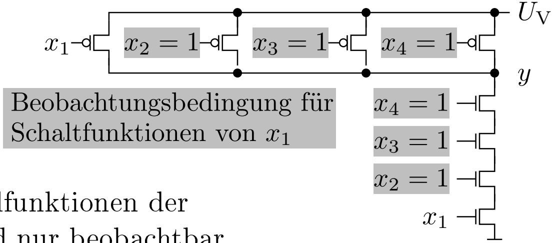


x_4	x_3	x_2	x_1	y
0	0	0	0	1
0	0	0	1	1
0	0	1	0	1
...	...	...	...	...
1	1	1	1	0

16 mögliche Tabelleeinträge bzw. bei einem Festwertspeicher Speicherplätze

Als Blockspeicher mit einer defekten Zelle: $p_i \approx \frac{1}{1\ldots100\cdot16}$

Bei Realisierung mit Transistorschaltern wird jeder Schalter bei jeder Gatter-Service-Leistung genutzt. Fehlfunktionen der Transistorschalter sind nur beobachtbar, wenn die parallelen Transistoren sperren und die Transistoren in Reihe leiten.



Verlangt im Beispiel drei definierte Bitwerte (Care-Bits), bei gleichwahrscheinlicher Bedatung: $b_i \approx 2^{-3}$.
Nachweiswahrscheinlichkeit eines Transistorfehlern bei einem seperaten Gattertest:

$$p_i \approx 2^{-4\ldots5}$$

Die Realisierung mit Transistorschaltern hat deutlich weniger und besser im Verbund testbare Teilsysteme als die Realisierung als Blockspeicher.

Das Haftfehlermodell

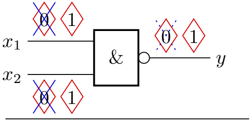
Fehlermodell

- Ein Modellfehler ist eine Beispielfehler mit exakt vorgegebenem Fehlverhalten.
- Ein Fehlermodell ist ein Algorithmus für die Berechnung von Modellfehlermengen für die Suche und Bewertung von Testsätzen.
- Das wichtigstes Fehlermodell ist das Haftfehlermodell: Annahme, dass logische Werte (binärer Signale, Entscheidungen, ...) ständig null oder ständig eins sind.
- Gut geeignet für Fehlersimulation, Testberechung, Bewertung von Zufallstestsätzen, ... für Systeme mit vielen tausend logische Operationen.
- Auch die in der Praxis genutzten Techniken für Software binarisieren die Systeme. Auswahl/Bewertung wie für Haftfehler.

Haftfehler für Logikgatter

Für jeden Gatteranschluss wird unterstellt:

- ein sa0 (stuck-at-0) Fehler
- ein sa1 (stuck-at-1) Fehler



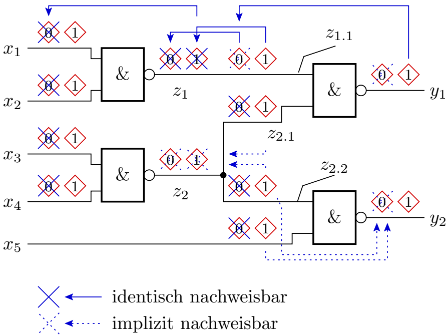
x_2	x_1	$\overline{x_2 \wedge x_1}$	sa0(x_1)	sa1(x_1)	sa0(x_2)	sa1(x_2)	sa0(y)	sa1(y)
0	0	1	1	1	1	1	0	1
0	1	1	1	1	1	0	0	1
1	0	1	1	0	1	1	0	1
1	1	0	1	0	1	0	0	1

Nachweisidentität (gleiche Nachweismenge)

- 0 sa0-Modellfehler
- 1 sa1-Modellfehler
- × identisch nachweisbar
- ⁙ implizit nachweisbar
- ⋯→ Nachweisimplikation
- ■ zugehörige Eingabe ist Element der Nachweismenge

Zusammenfassung identisch nachweisbarer Fehler. Optionale Streichung redundanter und implizit nachweisbarer Modellfehler. Modellierte Fehler sind ähnlich wie Transistorfehler in Gattern nachweisbar. Nicht für Gatter aus Blockspeichern geeignet.

Streichen identisch implizit nachweisbarer Fehler



Größe der Anfangsfehlermenge:	24
Anzahl der nicht identisch nachweisbaren Fehler:	14
ohne implizit nachgewiesene Fehler:	10

	Mengen von identisch nachweisbaren Fehlern	Nachweis impliziert durch
1	sa0(x_1), sa0(x_2), sa1(z_1), sa1($z_{1.1}$)	
2	sa1(x_1)	
3	sa1(x_2)	
4	sa0(x_3), sa0(x_4), sa1(z_2)	9, 12
5	sa1(x_3)	
6	sa1(x_4)	
7	sa0(z_2)	5, 6, 8, 11
8	sa0(z_1), sa0($z_{1.1}$), sa0($z_{2.1}$), sa1(y_1)	2, 3
9	sa1($z_{2.1}$)	
10	sa0(y_1)	1, 9
11	sa0($z_{2.2}$), sa0(x_5), sa1(y_2)	
12	sa1($z_{2.2}$)	
13	sa1(x_5)	
14	sa0(y_2)	12, 13

Redundante Fehler

Definition 4

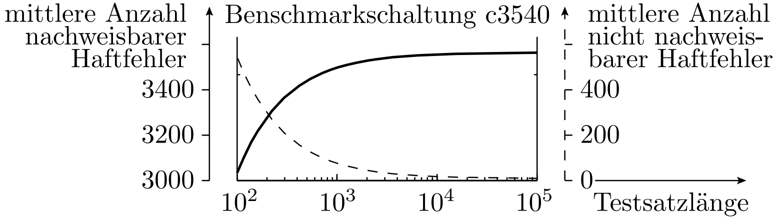
Ein redundanter (Modell-) Fehler ist ein Fehler in einem Teilsystem, der die Funktion des Gesamtsystems nicht beeinträchtigt.

- Der Gatteranschluss kann mit »0« (sa0 Fehler nicht nachweisbar) bzw. »1« (sa1-Fehler nicht nachweisbar) verbunden sein, ohne dass sich die Funktion ändert.
- Umformungen zur Beseitigung redundanter Modellfehler dient auch zur Systemoptimierung.

Typische Beobachtung für große Systeme

Fakt 5

Kurze Zufallstests finden die überwiegende Mehrheit der Haftfehler. Wenige Fehler verlangen sehr lange Testsätze.



- Bestimmt durch Fehlersimulation mit 1000 verschiedenen Zufallstestsätzen.
- Das Experiment erlaubt Rückschlüsse auf Nachweiswahrscheinlichkeit und Fehlernachweisprofil (siehe später).

Fehler in komplexen Funktionen

Fehler in komplexen Funktionen

- Die Anzahl der Care-Bits einer komplexen Funktion ist im ungünstigsten Fall die Anzahl der Eingabebits plus die Anzahl der gespeicherten Bits. Hunder Care-Bits $\Rightarrow$ $p_i \geq 2^{-100}$ ...
- Die unteren Grenzen für Nachweiswahrscheinlichkeiten sind so gering, dass es Fehler geben kann, in Millionen von Jahren mit fast absoluter Sicherheit nie eine Fehlfunktion verursachen.
- Aber auch hier lässt sich vielfach aus der Struktur auf im Mittel viel häufigere Fehlfunktionen bzw. viel größere Nachweiswahrscheinlichkeiten schließen.

Test mit alle Bedatungsvarianten

Die nachfolgende Tabelle zeigt, dass komplexe Funktionen mit vielen Eingabebits selbst ohne Gedächtnis nur mit einer winzigen Stichprobe von Bedatungsvarianten getestet werden können.

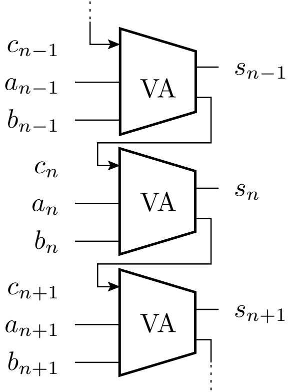
	m	2^m	t^*	$p_{\min}$
Gatter mit 4 Eingängen	4	16	16 µs	$10^{1\ldots2}$
ALU mit 68 Eingängen	68	$3 \cdot 10^{20}$	10^7 Jahre	$10^{-21\ldots22}$
vier Eingabevariablen vom Typ int32_t	128	$3 \cdot 10^{38}$	10^{25} Jahre	$10^{-39\ldots40}$

(m – Anzahl der Eingabebits; 2^m – Anzahl der Bedatungsmöglichkeiten; t^* Testdauer bei einer Service-Ausführungszeit von 1µs; $p_{\min}$ – minimale Nachweiswahrscheinlichkeit bei Realisierung mit einem Blockspeicher oder einer Tabellenfunktion).

Komplexe Funktionen sind so realisiert, dass fast alle Fehler mit sehr vielen unterschiedlichen Bedatungen nachweisbar sind.

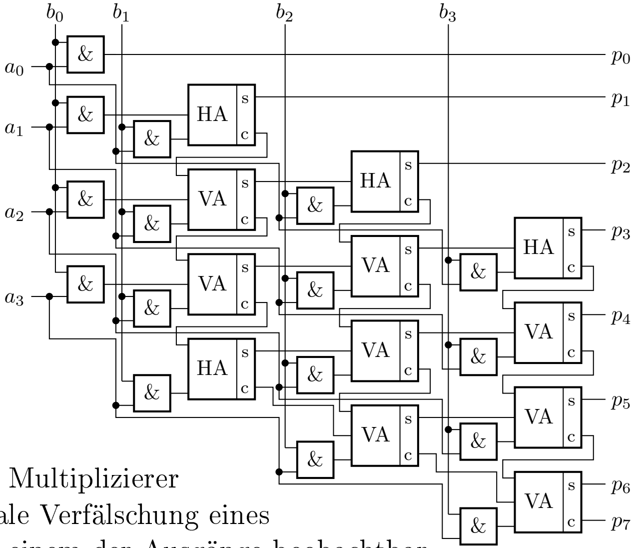
Beispiel Ripple-Addierer

- Jede Addition von zwei Datenworten nutzt jeden der Volladdierer.
- Fehlerhafte Ausgaben am Summenbit sind direkt beobachtbar.
- fehlerhafte Überträge invertieren das nächst höhere Summenbit.



Beobachtbarkeit der Service-Leistungen der einzelnen Volladdierer ist eins, die Nachweiswahrscheinlichkeit von Haftfehlern auf den Verbindungen ist etwa 50%, ein Volladdierer hat drei Care-Bits, ... $p_{\min} \approx 2^{-4\dots6}$ und nicht wie bei einer Tabellenrealisierung mit $p_{\min} \approx 2^{2\cdot n+1\dots2}$.

Multiplizierer



Auch bei einem Multiplizierer
ist fast jede lokale Verfälschung eines
Signalwertes an einem der Ausgänge beobachtbar.

Programmbausteinen

- Kleine Programmbausteine werden oft nur mit einem oder wenigen zufällig bedateten Beispielen getestst.
- Für nicht sicherheitskritische Software gilt in der Praxis ein Test mit 100% Anweisungsüberdeckung als ausreichend.
- Im Standard RTCA DO-178 B wird erst ab Level C (Software, die bedeutende Ausfälle verursachen kann) gefordert, dass jeder mögliche Kontollflusspfad mindestens vom Test einmal abgearbeitet werden kann.
- Die meisten Anweisungs- und Kontrollflussfehler haben, wenn ein einziger Test als ausreichend betrachtet wird, offenbar Nachweiswahrscheinlichkeiten deutlich größer 50%.

Zusammenfassung

Alle durchgeführten strukturellen Betrachtungen:

- Analyse der Steuer- und Beobachtbarkeiten,
- Untersuchung realer Schaltungen mit Haftfehlern und
- die Strukturbetrachtungen für große Systeme

zeigen, dass in der Regel

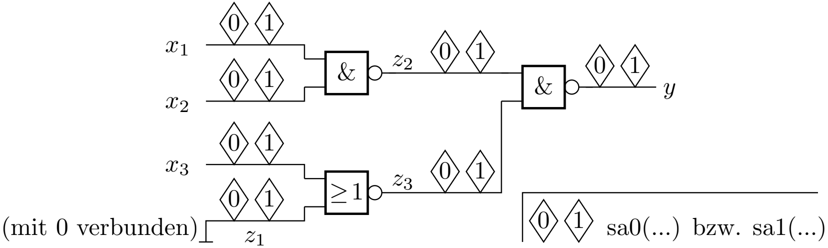
- die meisten potentiellen Fehler häufig Fehlfunktionen verursachen und somit gut nachzuweisen sind,
- es aber auch Fehlermöglichkeiten gibt, die erst nach einer sehr langen Nutzungsdauer oder nie erstmalig eine Fehlfunktion verursachen.

Für den Test und die Verlässlichkeit interessieren vor allem die schlecht nachweisbaren Fehler, weil die anderen alle bei deren Suche mit gefunden und beseitigt werden.

Aufgaben

Aufgabe 1.1: Haftfehlermenge

Gegeben ist die nachfolgende Schaltung mit 12 eingezeichneten Haftfehlern.



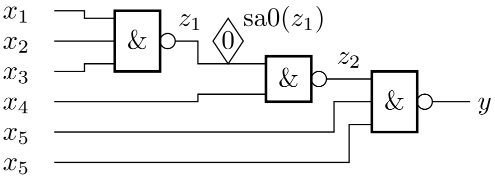
Welche der Haftfehler sind

1. redundant, d.h. mit keiner Eingabebelegung nachweisbar,
2. identisch nachweisbar,
3. implizit durch die Tests anderer Haftfehler nachweisbar?

Aufgabe 1.2: Nachweiswahrscheinlichkeit

Berechnen Sie für den in der nachfolgenden Abbildung eingezeichneten Haftfehler sa0(z_1) die Nachweiswahrscheinlichkeit

1. für gleichwahrscheinliche Eingaben und
2. mit Eingabefolgen mit Auftrittshäufigkeit für Einsen als Bitwerte von $g(x_i) = 60\%$.



Verteilungen

Eine Verteilung weist möglichen Werten einer Zufallsvariablen Wahrscheinlichkeiten zu. Es wird unterschieden zwischen

- Häufigkeitsverteilungen, die empirisch durch Zählen, Messen oder aus Umfragedaten erstellt und als Tabelle, Grafiken oder modellhaft durch eine Funktion dargestellt werden, und
- Wahrscheinlichkeitsverteilungen als mathematisches Gegenstück und als Vorhersage für Häufigkeitsverteilungen.

Häufigkeitsverteilungen

Verteilungen besprochener Experimente

- Zählen Service-Ergebnisse:

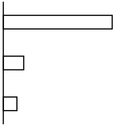
SK	Service-Ergebnis korrekt
SF	Service-Ergebnis fehlerhaft
SN	kein Service-Ergebnis
n	Anzahl der Service-Anfragen

Häufigkeitsverteilung

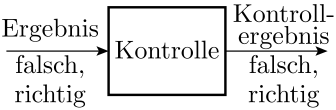
Tabelle

Wert	Häufigkeit
SK	$\frac{\mathrm{Anz}(SK)}{n}$
SF	$\frac{\mathrm{Anz}(SF)}{n}$
SN	$\frac{\mathrm{Anz}(SN)}{n}$

Säulen-diagramm

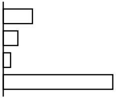


- Zählen der Kontrollergebnisse:



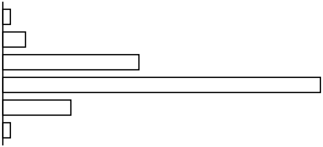
Ergebnis	Kontroll-ergebnis	Kontroll-aussage
falsch	falsch	FF
falsch	richtig	FR
richtig	falsch	RF
richtig	richtig	RR

Verteilung

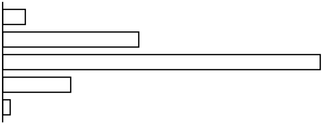


Empirische Einschätzungen

- Einschätzen von Sicherheitsrisiken:

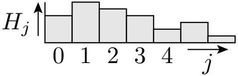
Einschätzung	O*	Häufigkeit Umfrageergebnis
vernachlässigbar	1	
gering	2	
vertretbar	3	
hoch	4	
sehr hoch	5	
unakzeptabel	6	

- Benotung von Prüfungsleistungen:

Einschätzung	O*	Häufigkeit Umfrageergebnis
sehr gut	1	
gut	2	
befriedigend	3	
ausreichend	4	
nicht bestanden	5	

O* Operationalisierung

Fehlernachweishäufigkeit



- Die Fehlernachweishäufigkeit, die die Häufigkeit der Fehler in einem System in Abhängigkeit von ihrer Nachweiswahrscheinlich- keit beschreibt. Zu ihrer empirischen Abschätzung wurden die Nachweiswahrscheinlichkeiten in Intervalle
$$I_j = \left[v^{-j}, v^{-(j+1)}\right)$$
($j \in \{0, 1, 2, \ldots\}$ – Intervallnummer; v – Parameter für die Intervallgröße) unterteilt, z.B. für $v = 2$ in $\left[1, \frac{1}{2}\right)$, $\left[\frac{1}{2}, \frac{1}{4}\right)$, ... und für jedes Intervall der Anteil der erkannten Fehler mit einen Nachweiswahrscheinlichkeit in diesem Bereich gezählt.
- Beispiel einer Verteilung, die sich praktisch nur indirekt über andere Experimente, z.B. Zählen der nachweisbaren Fehler in Abhängigkeit von der Testsatzlänge eines Zufallstests schätzen lässt.

Wahrscheinlichkeitsverteilungen

Wahrscheinlichkeitsverteilungen

Bei einer Wahrscheinlichkeitsverteilung sind die möglichen Ergebnisse ein Zahlenbereich (abzählbar oder stetig). Jedem Wert dieses Bereiches ist eine Wahrscheinlichkeit zugeordnet.

mögliche Ergebnisse x_i	2	3	4	5	...
Wahrscheinlichkeit p_i	3%	5%	2%	3%	...

Mit Wahrscheinlichkeitsverteilungen lassen sich Häufigkeitsverteilungen annähern, vorhersagen, auf ähnliche Sachverhalte übertragen, ...

Erwartungswert, Varianz und Standardabweichung

Der Erwartungswert μ, $E(X)$ (X – Zufallsgröße) ist der Mittelwert der zu erwartenden Realisierungen:

$$E(X) = \sum_{i=1}^{n} p_i \cdot x_i \tag{3}$$

Die Varianz σ^2, $D^2(X)$ ist die mittlere quadratische Abweichung vom Erwartungswert:

$$D^2(X) = \sum_{i=1}^{n} p_i \cdot (x_i - E(X))^2 \tag{4}$$

Die Standardabweichung σ, $\sqrt{D^2(X)}$ ist die Wurzel aus der Varianz und ein Maß dafür, wie stark die Ergebnisse eines Zufallsexperiments um ihren Erwartungswert streuen.

Verschiebungssatz

Vereinfachung der Berechnung der Varianz[6]:

$$D^2(X) = E\left(X^2\right) - (E(X))^2 \tag{5}$$

Herleitung:

$$\sum_{i=1}^{n} p_i \cdot (x_i - E(X))^2 = \sum_{i=1}^{n} p_i \cdot \left(x_i^2 - 2 \cdot x_i \cdot E(X) + E(X)^2\right)$$

$$\underbrace{\sum_{i=1}^{n} p_i \cdot x_i^2}_{E(X^2)} + E(X) \cdot \left(E(X) \cdot \underbrace{\sum_{i=1}^{n} p_i}_{1} - 2 \cdot \underbrace{\sum_{i=1}^{n} p_i \cdot x_i}_{E(X)} \right)$$

[6] Bei begrenzter Rechengenauigkeit numerisch problematisch.

Beispielrechnung

Gegeben ist die Verteilung in der nachfolgenden Tabelle:

Wert	5	6	8	11	22
Wahrscheinlichkeit	0,1	0,2	0,4	0,2	0,1

Wie groß sind der Erwartungswert μ, die Varianz σ^2 und die Standardabweichung σ?

- Erwartungswert:

$$\mu = 0{,}1 \cdot 5 + 0{,}2 \cdot 6 + 0{,}4 \cdot 8 + 0{,}2 \cdot 11 + 0{,}1 \cdot 22 = 9{,}3$$

- Varianz nach Gleichung 4:

$$\begin{aligned} \sigma^2 &= 0{,}1 \cdot (5 - 9{,}3)^2 + 0{,}2 \cdot (6 - 9{,}3)^2 + 0{,}4 \cdot (8 - 9{,}3)^2 \\ &+ 0{,}2 \cdot (11 - 9{,}3)^2 + 0{,}1 \cdot (22 - 9{,}3)^2 = 21{,}4 \end{aligned}$$

Wert	5	6	8	11	22
Wahrscheinlichkeit	0,1	0,2	0,4	0,2	0,1

- Varianz nach dem Verschiebungssatz:

$$\begin{aligned}\sigma^2 &= 0{,}1 \cdot 5^2 + 0{,}2 \cdot 6^2 + 0{,}4 \cdot 8^2 + 0{,}2 \cdot 11^2 \\ &+ 0{,}1 \cdot 22^2 - 9{,}3^2 = 21{,}4\end{aligned}$$

- Standardabweichung:

$$\sigma = \sqrt{21{,}4} = 4{,}63$$

Lineare Transformation

Lineare Transformationen sind die Multiplikation und Addition einer Zufallsgröße mit reellen Zahlen. Der Erwartungswert vergrößert und verschiebt sich um dieselben Werte:

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

Bei der Varianz entfällt die Verschiebung und der Skalierungsfaktor geht im Quadrat ein[7]:

$$D^2(a \cdot X + b) = a^2 \cdot D^2(X) \tag{6}$$

Die Varianz ist insbesondere verschiebungsinvariant und bleibt bei einer Spiegelung der Verteilung gleich:

$$D^2(-X) = D^2(X)$$

[7] Kontrolle der Gleichung siehe Aufgabe 2.1

Kontrolle am Beispiel

X	1	2	3
$Y=5-2X$	3	1	-1
$P(Y)=P(X)$	0,3	0,5	0,2

$$\begin{aligned}
E(X) &= 0{,}3+1+0{,}6=1,9 \\
D^2(X) &= 0{,}3+2+1{,}8-1{,}9^2=0{,}49 \\
E(Y) &= 0{,}9+0{,}5-0,2=1{,}2 \\
D^2(Y) &= 2{,}7+0{,}5+0{,}2-0{,}2^2=1{,}96 \\
E(Y) &= 5-2\cdot E(X) \\
D^2(Y) &= (-2)^2\cdot D^2(X)
\end{aligned}$$

Summe von Zufallsgrößen

Die Verteilung der Summe von Zufallsgrößen ordnet jedem möglich Wert der Summe die Wahrscheinlichkeit zu, dass die Summe diesen Wert hat:

X	1	3	4
$P(X)$	0,1	0,4	0,5

Y	2	3	4
$P(Y)$	0,3	0,6	0,1

$$\begin{aligned}
P(X+Y=3) &= P(X=1)\cdot P(Y=2)\\
P(X+Y=4) &= P(X=1)\cdot P(Y=3)\\
P(X+Y=5) &= P(X=1)\cdot P(Y=4)+P(X=3)\cdot P(Y=2)\\
P(X+Y=6) &= P(X=3)\cdot P(Y=3)+P(X=4)\cdot P(Y=2)\\
P(X+Y=7) &= P(X=3)\cdot P(Y=4)+P(X=4)\cdot P(Y=3)\\
P(X+Y=8) &= P(X=4)\cdot P(Y=4)
\end{aligned}$$

Für die Summe von Zufallsgrößen ist der Erwartungswert gleich der Summe der Erwartungswerte:

$$E(X+Y) = E(X) + E(Y)$$

Die Varianz ist die Summe der Varianzen plus doppelte Kovarianz:

$$D^2(X+Y) = D^2(X) + D^2(Y) + 2 \cdot \mathrm{Cov}(X,Y) \tag{7}$$

mit der Kovarianz[8]:

$$\mathrm{Cov}(X,Y) = E((X - E(X)) \cdot (Y - E(Y))) \tag{8}$$

Für unabhängige Zufallsgrößen ist die Kovarianz null und die Varianz die Summe der Varianzen der Summanden:

$$D^2(X+Y) = D^2(X) + D^2(Y)$$

[8] Kontrolle der Gleichungen siehe Aufgabe 2.1

Anwendung auf die Messung eines Widerstands

Der Wert eines (zufällig ausgewählten) Widerstands habe einen Erwartungswert von $E(R) = 1\,\mathrm{k}\Omega$ und einer Standardabweichung von $\sqrt{D^2(R)} = 10\,\Omega$. Das Messgerät habe einen systematischen Fehler von $E(M) = 2\,\mathrm{Ohm}$ und eine Standardabweichung von $\sqrt{D^2(M)} = 5\,\Omega$. Welchen Erwartungswert und welche Standardabweichung hat das Messergebnis?

Ein Messergebnis ist die Summe aus zu messendem Wert und Messfehler. Der Erwartungswert beträgt im Beispiel:

$$E(R+M) = 1010\,\Omega$$

Unter Annahme der Unabhängigkeit zwischen Widerstandsauswahl und Messdurchführung addieren sich auch die Varianzen nur:

$$D^2(R+M) = D^2(R) + D^2(M) = (10\,\Omega)^2 + (5\,\Omega)^2 = 125\,\Omega^2$$

Die Standardabweichung ist $\sqrt{D^2(R+M)} \approx 11,2\,\Omega$.

Verteilung von Zählwerten

Verteilung von Zählwerten

Zählwerte sind eine Summe von Einzelereignissen (z.B. Anzahl der korrekt ausgeführten oder fehlerhaft ausgeführten Service-Leistungen). Die Einzelereignisse können null oder eins sein und haben die Verteilung:

k	0	1
$P(X_i = k)$	$1 - p_i$	p_i

(X_i – Zufallsgröße Einzelereignis i; p_i – Eintrittswahrscheinlichkeit $X_i = 1$). Für N Versuche ist die Anzahl der eingetretenen Ereignisse die Summe der Zufallsgrößen X_i:

$$X = \sum_{i=1}^{N} X_i$$

k	0	1
$P(X_i = k)$	$1 - p_i$	p_i

Der Erwartungswert der Einzelereignisse ist

$$E(X_i) = (1 - p_i) \cdot 0 + p_i \cdot 1 = p_i$$

und die Varianz der Einzelereignisse beträgt:

$$D^2(X_i) = (1 - p_i) \cdot (0 - p_i)^2 + p_i \cdot (1 - p_i)^2 = p_i \cdot (1 - p_i)$$

Der Erwartungswert der Summe ist die Summe der Erwartungswerte

$$E(X) = \sum_{i=1}^{N} p_i \tag{9}$$

Für die Varianz wird unterstellt, das die zu zählenden Ereignisse, wie das Auftreten einer Fehlfunktion, nicht voneinander abhängen, so dass die Varianz der Summe gleich der Summe der Varianzen der Summanden ist (Kovarianz null):

$$D^2(X) = \sum_{i=1}^{N} p_i \cdot (1 - p_i) \tag{10}$$

Für die Verteilung gilt, dass bei Hinzunahme eines weiteren Experiments i sich mit Wahrscheinlichkeit p_i der Zählwert um eins erhöht und mit der Wahrscheinlichkeit $1-p_i$ gleich bleibt:

$$P_i\left(X=k\right)=p_i\cdot P_{i-1}\left(X=k-1\right)+\left(1-pi_j\right)\cdot P_{i-1}\left(X=k\right)$$

i	p_i	$X=0$	$X=1$	$X=2$	$X=3$	$X=4$
1	30%	70%	30%			
2	50%	35%	50%	15%		
3	40%	21%	44%	29%	6%	
4	10%	18,9%	41,7%	30,5%	8,3%	0,6%

Berechnung der Verteilung:

$$P_1\left(X=0\right)=1-p_1$$
$$P_1\left(X=1\right)=p_1$$

`Wiederhole für` $j=2$ `bis` N

$$P_i\left(X=0\right)=P_{i-1}\left(X=0\right)\cdot\left(1-p_i\right)$$
$$P_i\left(X=k\right)=P_{i-1}\left(X=k-1\right)\cdot p_i$$

`Wiederhole für` $i=1$ `bis` $j-1$

$$P_i\left(X=k\right)=P_{i-1}\left(X=k\right)\cdot\left(1-p_i\right)+P_{i-1}\left(X=k-1\right)\cdot p_i$$

(i – Anzahl der berücksichtigten Summanden; k – Zählwert).

Erwartungswert und Varianz für das Beispiel

i	p_i	$X=0$	$X=1$	$X=2$	$X=3$	$X=4$
1	30%	70%	30%			
2	50%	35%	50%	15%		
3	40%	21%	44%	29%	6%	
4	10%	18,9%	41,7%	30,5%	8,3%	0,6%

Nach Gl. 3 beträgt der Erwartungswert der Summe aller $N = 4$ Summanden:

$$\mu = 18{,}9\% \cdot 0 + 41{,}7\% \cdot 1 \\ +30{,}5\% \cdot 2 + 8{,}3\% \cdot 3 + 0{,}6\% \cdot 4 = 1,3$$

Als Summe aller p_i nach Gl. 9 ist die Berechung kürzer:

$$\mu = 30\% + 50\% + 40\% + 10\% = 1{,}3$$

Die Varianz beträgt nach dem Verschiebesatz Gl. 5:

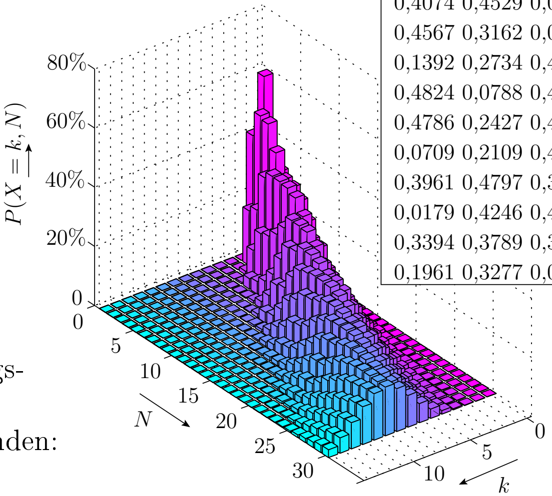
$$18{,}9\% \cdot 0^2 + 41{,}7\% \cdot 1^2 + 30{,}5\% \cdot 2^2 + 8{,}3\% \cdot 3^2 + 0{,}6\% \cdot 4^2 - 1{,}3^2 = 0{,}79$$

Die vereinfachte Berechnung nach Gl. 10 lautet:

$$\sigma^2 = 0{,}3 \cdot 0{,}7 + 0{,}5 \cdot 0{,}5 + 0{,}4 \cdot 0{,}6 + 0{,}1 \cdot 0{,}9 = 0{,}79$$

Mit Matlab berechnete Zählverteilung

Das nachfolgende Säulendiagramm zeigt eine mit Matlab schrittweise berechnete Zählverteilung. Die Eintrittswahrscheinlichkeiten der Zählereignisse siehe Kasten im Bild. Erwartungswert und Varianz für alle 30 Summanden: μ=7,05, $\sigma^2 = 2,19$



p_i für i=1 bis 30		
0,4074	0,4529	0,0635
0,4567	0,3162	0,0488
0,1392	0,2734	0,4788
0,4824	0,0788	0,4853
0,4786	0,2427	0,4001
0,0709	0,2109	0,4579
0,3961	0,4797	0,3279
0,0179	0,4246	0,4670
0,3394	0,3789	0,3716
0,1961	0,3277	0,0856

Binomialverteilung

Binomialverteilung

Für den Sonderfall, dass gleichwahrscheinliche Ereignisse gezählt werden (alle $p_i = \bar{p} = p$) ist die Summe der gezählten Ereignisse binomialverteilt

$$P(X = k) = \left(\begin{array}{c} N \\ k \end{array}\right) \cdot p^k \cdot (1-p)^{N-k}$$

mit dem Erwartungswert

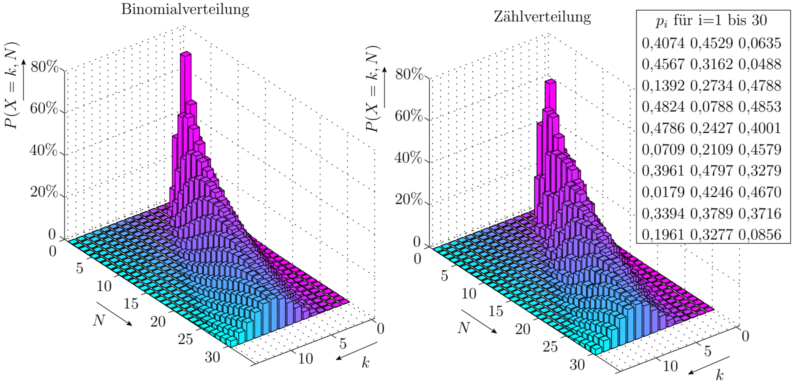
$$E(X)_{\text{Bin}} = N \cdot p$$

und der Varianz

$$D^2(X)_{\text{Bin}} = N \cdot p \cdot (1-p)$$

(N – Anzahl der gezählten Ereignisse, die 1 oder 0 sein können).

Binomialverteilung vs. allgemeine Zählverteilung



p_i für i=1 bis 30		
0,4074	0,4529	0,0635
0,4567	0,3162	0,0488
0,1392	0,2734	0,4788
0,4824	0,0788	0,4853
0,4786	0,2427	0,4001
0,0709	0,2109	0,4579
0,3961	0,4797	0,3279
0,0179	0,4246	0,4670
0,3394	0,3789	0,3716
0,1961	0,3277	0,0856

Eine Binomialverteilung nähert eine allgemeine Zählverteilung gut an und hat den Vorteil, dass sie sich aus nur zwei Parametern N und p, statt aus N Parametern p_i berechnet.

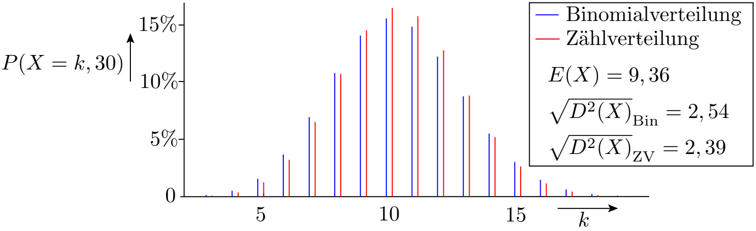
Bei gleichem Erwartungswert

$$E(X)_{\mathrm{Bin}} = N \cdot p = E(X)_{\mathrm{ZV}} = \sum_{i=1}^{N} p_i$$

ist die Varianz einer Binomialverteilung mindestens so groß wie die Varianz einer beliebigen Zählverteilung[9]:

$$D^2(X)_{\mathrm{Bin}} = N \cdot p \cdot (1-p) = E(X) \cdot \left(1 - \frac{E(X)}{N}\right) \geq D^2(X)_{\mathrm{ZV}} \quad (11)$$

Die beiden Verteilungen der Folie zuvor für $N = 30$:



[9] Beweis von Gl. 11 siehe Aufgabe 2.1

Poisson-Verteilung

Poisson-Verteilung

Beim Zählen sehr vieler selten eintretender Ereignisse, z.B. der Fehlfunktionen bei Millionen von Service-Anforderungen eines zuverlässigen Systems, ist die Eintrittswahrscheinlichkeit der Einzelereignisse (im Bsp. fehlerhafter Service-Ergebnisse) nahe null. Die Varianz der zu zählenden Ereignisse strebt gegen den Erwartungswert

$$D^2(X_i) = \lim_{p_i \to 0} (p_i \cdot (1 - p_i)) = p_i$$

und die Varianz der Summe als die Summe der Varianzen auch. Die Verteilung der Zählwerte, im Beispiel die Anzahl der Fehlfunktionen, strebt gegen die Poisson-Verteilung:

$$P(X = k) = \mathrm{Poi}(k,\, E(X)) = e^{-E(X)} \cdot \frac{E(X)^k}{k!}$$

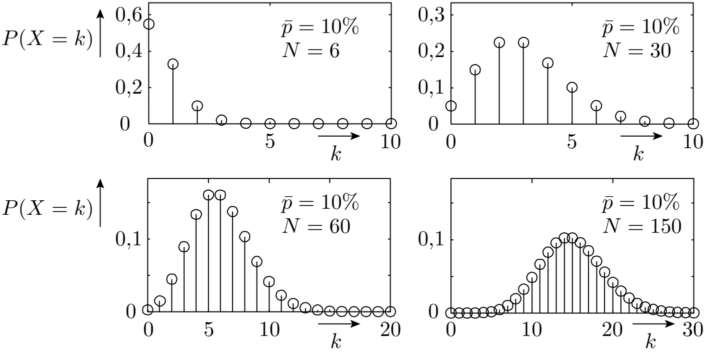
Das ist eine einparametrige Verteilung, die sich allein aus dem Erwartungswert berechnet.

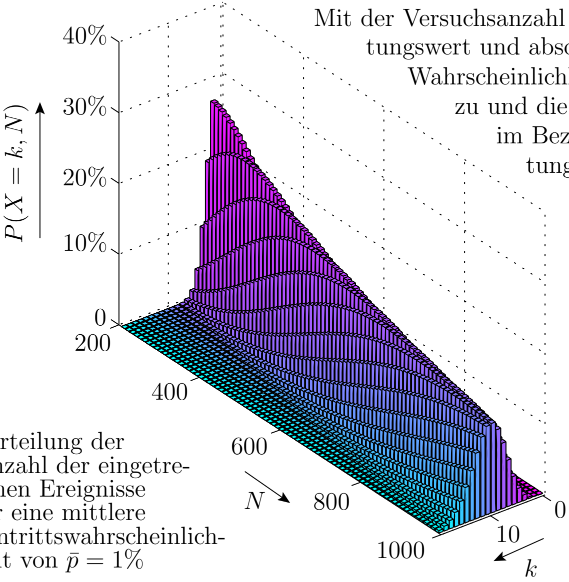
Für Zählprozesse ist der Erwartungswert

$$E(X) = \sum_{i=1}^{N} p_i = N \cdot \bar{p}$$

die mittlere Eintrittswahrscheinlichkeit $\bar{p}$ mal der Versuchsanzahl N:

$$P(X = k) = e^{-\bar{p}\cdot N} \cdot \frac{(\bar{p} \cdot N)^k}{k!}$$





Mit der Versuchsanzahl nehmen Erwartungswert und absolute Breite des Wahrscheinlichkeitsgebirges zu und die relativ Breite im Bezug zum Erwartungswert ab.

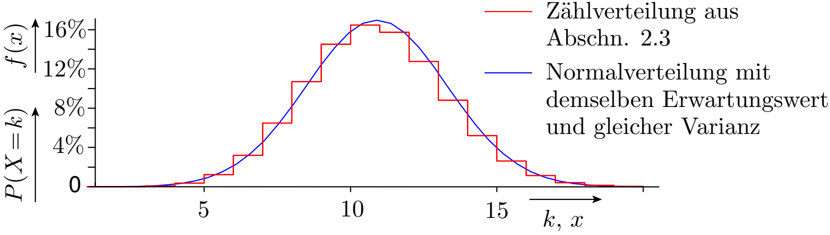
Verteilung der Anzahl der eingetretenen Ereignisse für eine mittlere Eintrittswahrscheinlichkeit von $\bar{p} = 1\%$

Normalverteilung

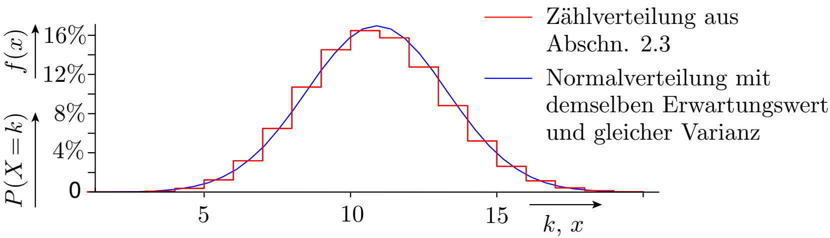
Normalverteilung

Die Summe sehr vieler unabhängiger Zufallsgrößen strebt unter sehr allgemeinen Bedingungen gegen eine Normalverteilung:

- kein Summand hat dominanten Einfluss und
- Erwartungswert deutlich größer als Standardabweichung[10].



[10] Schließt die behandelten Zählverteilungen ein.



Ein Normalverteilung berechnet sich aus den zwei Parametern Erwartungswert μ und Varianz σ^2:

$$f(x) = \frac{1}{\sigma \cdot \sqrt{2\pi}} \cdot e^{-\frac{(x-\mu)^2}{2\cdot\sigma^2}}$$

Die Summe unabhängiger normalverteilter Zufallsgrößen ist wieder normalverteilt. Normalverteilte Zufallsgrößen liegen

- mit 95,45% Wahrscheinlichkeit im Bereich $\mu \pm 2\sigma$
- mit 99,73% Wahrscheinlichkeit im Bereich $\mu \pm 3\sigma$
- praktisch 100% im Bereich $\mu \pm 4\sigma$

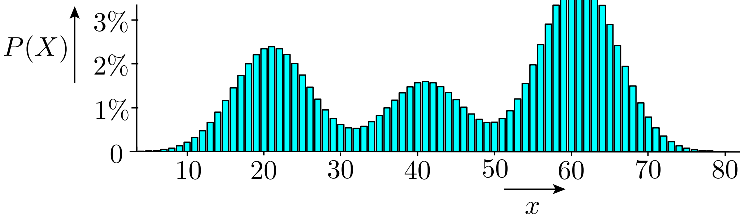
Multimodale Verteilungen

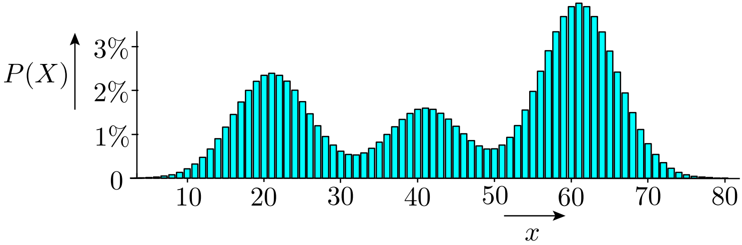
Multimodale (mehrgipflige) Verteilung

Eine multimodale Verteilung ist eine Häufigkeitsverteilung mit mehreren Gipfeln. Sie entsteht durch Mischung unterschiedlich verteilter Grundgesamtheiten, z.B. Normalverteilungen mit unterschiedlichen Erwartungswerten

$$P(X = k) = f(k) = 0,3 \cdot f_1(k) + 0,2 \cdot f_2(k) + 0,5 \cdot f_3(k)$$

($f_i(k)$– diskrete Näherungen einer Normalverteilungen mit Erwartungswerten μ_i und Standardabweichung $\sigma_i = 5$).



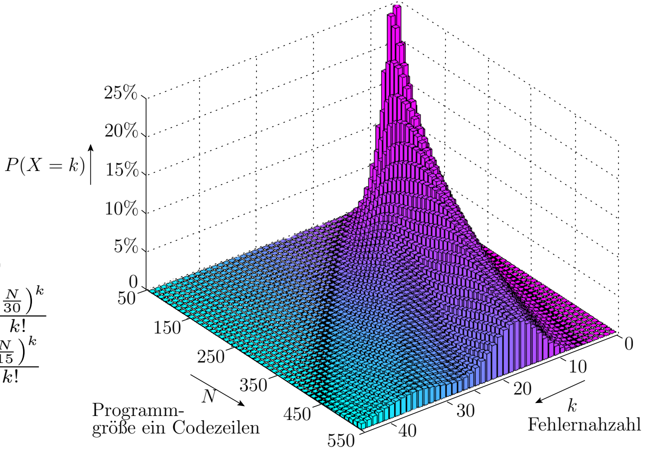


Die Multimodalität deutet auf Polarisierungen der Beobachtungswerte (Zugehörigkeit zu unterschiedlichen Verteilungen). Polarisierungen können wichtige Informationen über die Natur der untersuchten Variablen liefern:

- Abhängigkeiten bei der Fehlerentstehung, bei Ausfällen beim Fehlernachweis, und beim Versagen von Service-Leistungen,
- Vorliebe oder Neigung befragter Experten, z.B. bei der Einschätzung von Gefährdungen und Risiken und
- Probleme beim Messverfahren.

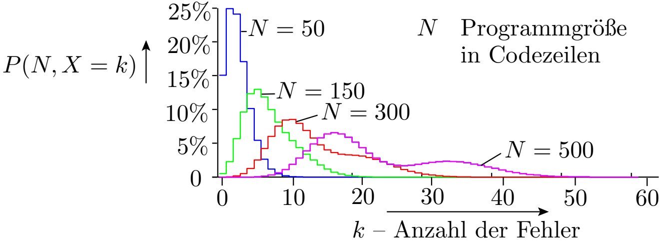
Beispiel sein ein Software-Entstehungsprozess, in dem ein Anfänger und ein Profi Software-Bausteine aus N Code-Zeilen entwickeln, der Profi 66% der Bausteine mit ca. einem Fehler je 30 Codezeilen und der Anfänger 33% der Bausteine mit einem Fehler je 15 Codezeilen.

$$P\left(N, X=k\right) = \frac{2}{3}\cdot e^{-\frac{N}{30}}\cdot\frac{\left(\frac{N}{30}\right)^k}{k!} + \frac{1}{3}\cdot e^{-\frac{N}{15}}\cdot\frac{\left(\frac{N}{15}\right)^k}{k!}$$



Die Wahrscheinlichkeit, dass ein Modul genau k Fehler enthält, ist $2/3$ mal der Wahrscheinlichkeit, das es k Fehler enthält und vom Profi stammt plus $1/3$ mal der Wahrscheinlichkeit, dass es vom Anfänger stammt:

$$P(N, X = k) = \frac{2}{3} \cdot e^{-\frac{N}{30}} \cdot \frac{\left(\frac{N}{30}\right)^k}{k!} + \frac{1}{3} \cdot e^{-\frac{N}{10}} \cdot \frac{\left(\frac{N}{15}\right)^k}{k!} \tag{12}$$



Die Polarisierung nimmt mit der Größe der Software-Bausteine, die vom Profi und vom Anfänger getrennt entwickelt werden, zu.

Aufgaben

Aufgabe 2.1: Kontrolle von Gl. 6, 7 und 11

1. Überprüfen Sie Gl. 6, indem Sie in Gl. 5 als Zufallsgröße $a \cdot X + b$ einsetzen.
2. Überprüfen Sie Gl. 7, indem Sie in Gl. 5 als Zufallsgröße $X + Y$ einsetzen und unter Nutzung der Definition der Kovarianz Gl. 8.
3. Zeigen Sie für Gl. 11 durch Einsetzen von $p_i = p + \delta_i$ mit $\sum_{i=1}^{N} \delta_i = 0$, dass eine Binomialverteilung von allen Zählverteilungen mit derselben Ereignisanzahl N und demselben Erwartungswert die größte Varianz hat. (Nach Vereinfachung muss herauskommen $\sum_{i=1}^{N} \delta_i^2 \geq 0$, was immer erfüllt ist).

Aufgabe 2.2: Berechnung einer Zählverteilung

Schreiben Sie ein Matlab-Programm zur Berechnung einer Zählverteilung nach dem Algorithmus auf Folie 71. Das Ergebnis soll in einem 2D Feld $P(i,k)$ stehen ($i = 1, 2, ..., N$ – Anzahl der berücksichtigten Summanden; k – Zählwert). Stellen Sie das Ergebnis mit

```
bar3(P);
xlabel('k');
ylabel('i');
zlabel('P(i,X=k)');
```

als 3D-Säulendiagramm graphisch dar. Testen Sie das Programm mit den Eintrittswahrscheinlichkeiten der zu zählenden Ereignisse $p_1 = 39\%$, $p_2 = 51\%$, $p_3 = 23\%$, $p_4 = 88\%$ und $p_5 = 36\%$.

Aufgabe 2.3: Multimodale Verteilung

Entsteht die auf den Folien 88 und 89 gezeigte Polarisierung in der zu erwartenden Fehleranzahl auch dann, wenn Profi und Anfänger die Software-Bausteine gemeinsam entwickeln? Stellen Sie in Analogie zu Gl. 12 die Berechnungsvorschrift $P(N, X = k)$ für diesen Fall auf.

Fehler und Fehlfunk.

Verteilung

Zählverteilung der Fehleranzahl

Von $i = 1$ bis Anz(PF) ist jeder potenzielle Fehler i mit einer Wahrscheinlichkeit p_i vorhanden. Beschreibung durch Bernoulli-Versuche mit den Zufallsgrößen:

$$\varphi_i = \begin{cases} 0 & \text{Fehler nicht vorhanden, } P(\varphi_i = 0) = 1 - p_i \\ 1 & \text{Fehler vorhanden, } P(\varphi_i = 1) = p_i \end{cases}$$

Anzahl aller vorhandenen Fehler:

$$\varphi = \sum_{i=1}^{\mathrm{Anz(PF)}} \varphi_i$$

Zählbare Fehler:

- entstandene Fehler,
- vom Test erkannte Fehler,
- beseitigte Fehler,
- im Einsatz noch vorhandene Fehler, ...

Kontrollfragen

Es sei unterstellt, dass zwischen dem Vorhandensein der zu zählenden Fehler keine Abhängigkeiten bestehen:

- Wie groß ist der Erwartungswert?
- Wie groß ist die Varianz?
- Durch welche bekannten Verteilungen lässt sich die Verteilung der Fehleranzahl annähern und was sind die Voraussetzung der jeweiligen Näherung?

Angenommen die zu zählenden Fehler sind nachweisbare Modellfehler und die Modellfehlermenge enthält immer paarweise zwei identische Fehler:

- Wie ändern sich Erwartungswert und Varianz[11]?

[11] Hinweis: Elementarverteilung je potentieller Fehler mit den möglichen Zählwerten null und zwei aufstellen. Erwartungswert und Varianz der Fehlerpaare und Summe. Erwartungswert wie bei unanhängig nachweisbaren Fehlern. Varianz verdoppelt sich.

Verteilung der Anzahl der Fehlfunktionen

Bei jedem der $i = 1$ bis N (N – Anzahl der Service-Aufrufe) kommt es mit einer Wahrscheinlichkeit p_i zu einer Fehlfunktion. Beschreibung durch Bernoulli-Versuche mit den Zufallsgrößen:

$$\zeta_i = \begin{cases} 0 & \text{FF nicht vorhanden}, P(\zeta_i = 0) = 1 - p_i \\ 1 & \text{FF vorhanden}, P(\zeta_i = 1) = p_i \end{cases}$$

(ζ – Zeta; FF – Fehlfunktion). Anzahl der auftretenden Fehlfunktionen:

$$\zeta = \sum_{i=1}^{N} \zeta_i$$

Berechnung Erwartungswert, Varianz, Annäherung durch bekannte Verteilungen, ... wie für die Fehleranzahl, nur mit anderen p_i.

FHNW-Funktion

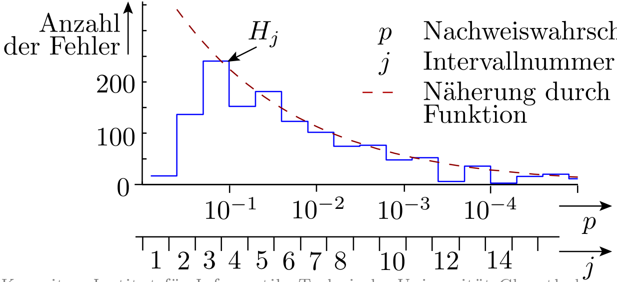
Fehlerauftrittshäufigkeit und Nachweiswahrsch.

Die FHNW-Funktion $H(p)$ beschreibt die Häufigkeit der Fehler in Abhängigkeit von ihrer Nachweiswahrscheinlichkeit. Abschätzbar durch zählen der Fehler pro Wahrscheinlichkeitsintervall:

$$H_j = \mathrm{Anz}\left(F_i|_{p_{j.\min}<p_{ji}\leq p_{j.\max}} \right)$$

Zweckmäßig Intervallgrenzen logarithmisch zum Kehrwert von p:

$$p_{j.\max} = v^{-j};\ p_{j.\min} = v^{-(j+1)}$$



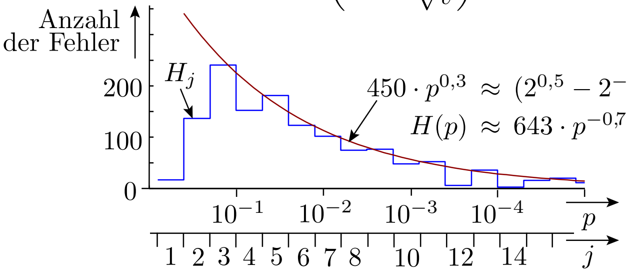
Von der Säulen- zur FHNW-Funktion

Die Säulenhöhe ist das Integral der FHNW-Funktion über die Intervallbreite:

$$H_j = \int_{v^{-(j+1)}}^{v^{-j}} H(p) \cdot dp$$

Wenn $H(p)$ innerhalb der Intervalle näherungsweise konstant ist:

$$\begin{aligned} H_j &\approx \left(v^{-j} - v^{-(j+1)}\right) \cdot H\left(v^{-(j+0{,}5)}\right) \\ &\approx p \cdot H(p) \cdot \left(\sqrt{v} - \frac{1}{\sqrt{v}}\right) \text{ für } p = v^{-(j+0{,}5)} \end{aligned}$$



Asymptotische Näherung

Aus der Erfahrung, dass die Fehleranzahl je Intervall mit der Intervallnummer abnimmt, folgt, das $p \cdot H(p)$ mit p abnimmt, d.h. $H(p)$ weniger als proportional mit p zu nimmt. Für weitere Modellrechungen sei $H(p)$ eine Potenzfunktion:

$$H(p) = \varphi_0 \cdot k \cdot p^{k-1} \text{ mit } 0 < k < 1 \tag{13}$$

(k – Parameter für die Ordnung der Abnahme der Fehlerhäufigkeit mit der Nachweiswahrscheinlichkeit). Der Parameter φ_0 ist eine Rechengröße für die Fehleranzahl ungetesteter Systeme.

Zu erwartende Fehleranzahl im ungetesten System

Die (zu erwartende[12]) Fehleranzahl ist die Summe der »Säulenwerte« bzw. das Integral über die FHNW-Funktion:

$$E(\varphi) = \int_0^1 H(p) \cdot dp$$

Für die Approximationsfunktion Gl. 13:

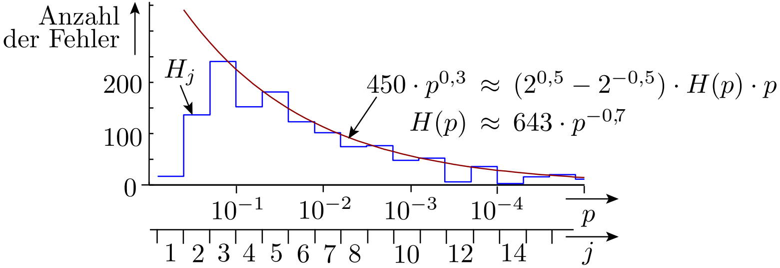
$$\begin{aligned} E(\varphi) &= \int_0^1 H(p) \cdot dp = \int_0^1 \varphi_0 \cdot k \cdot p^{k-1} \cdot dp \\ &= \varphi_0 \cdot \left(1^k - 0^k\right) = \varphi_0 \end{aligned}$$

ist sie der Parameter φ_0.

---

[12]Wenn $H(p)$ eine geschätzte Funktion ist, was in der Regel der Fall sein wird, ist das Integral ein Schätzer für den Erwartungswert.

$$E(\varphi) = \int_0^1 H(p) \cdot dp = \varphi_0$$



Für die Schätzung der nicht beseitigten Fehler im Einsatz[13] genügt eine brauchbare Näherung für kleine p. Nur ist dann φ_0 kein brauchbarer Schätzwert für die Fehleranzahl des ungetesteten Systems.

[13] Bei Systemen im Einsatz sind die gut nachweisbaren Fehler beseitigt.

Anzahl der fehlerbezogenen Fehlfunktion

Die Auftrittswahrscheinlichkeit einer Fehlfunktion durch einen Fehler i ist seine Nachweiswahrscheinlichkeit p_i. Die zu erwartende Anzahl aller Fehlfunktionen ist die Summe für alle Fehler und alle N Service-Anforderungen. Unter Kenntnis der FHNW-Funktion $H(p)$:

$$E(\zeta) = N \cdot \underbrace{\int_0^1 \underbrace{p \cdot H(p)}_{*} \cdot dp}_{**}$$

($*$ – Wahrsch., dass Fehler mit einer Nachweiswahrsch. p bei einer Service-Anforderung eine Fehlfunktion verursachen; $**$ – basiert auf Summennäherung für ODER-verknüpfte Ereignisse; gilt nur, wenn das Integral als die geschätzte Fehlerauftrittshäufigkeit je Service-Anforderung viel kleiner eins ist. Für die Approximation Gl. 13 nur nach Beseitigung der gut nachweisbaren Fehler).

Zufälliger Nachweis

Zufälliger Fehlernachweis

Ein Zufallstest mit n Testschritten hat nach Gl. 1 die Nachweiswahrscheinlichkeit

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

(n – Anzahl der Tests). Die zu erwartende Anzahl der nachweisbaren Fehler ist die Summe der Produkte aus den Wahrscheinlichkeiten »Fehler vorhanden« und »Fehler nachweisbar«:

$$E(\varphi_{\text{Erk}}, n) = \sum_{i=1}^{\text{Anz(PF)}} p_{i.\text{vorh}} \cdot \left(1 - e^{-n \cdot p_{i.\text{nachw}}}\right)$$

Mit der FHNW-Funktion:

$$E(\varphi_{\text{Erk}}, n) = \int_0^1 H(p) \cdot \left(1 - e^{-n \cdot p}\right) \cdot dp$$

Anzahl der nicht nachweisbaren Fehler:

$$E(\varphi_{\text{NErk}}, n) = \int_0^1 H(p) \cdot e^{-n \cdot p} \cdot dp$$

Mit der Approximation $H(p) = \varphi_0 \cdot k \cdot p^{k-1}$

$$\begin{aligned} E(\varphi_{\mathrm{NErk}}, n) &= \int_0^1 \varphi_0 \cdot k \cdot p^{k-1} \cdot e^{-n \cdot p} \cdot dp \\ &= \varphi_0 \cdot k \cdot \int_0^1 p^{k-1} \cdot e^{-n \cdot p} \cdot dp \end{aligned}$$

Die Substitution $p = \frac{x}{n}$; $dp = \frac{dx}{n}$ holt die Testdauer n und die Nachweiswahrscheinlichkeit p aus dem Integral:

$$E(\varphi_{\mathrm{NErk}}, n) = \varphi_0 \cdot k \cdot n^{-k} \underbrace{\int_0^n x^{k-1} \cdot e^{-x} \cdot dx}_{\approx \Gamma(k) \approx k^{-1}}$$

Das Restintegral stebt für große n gegen die Gamma-Funktion $\Gamma(k)$ und diese für $0 < k \leq 1$ gegen $1/k$. Abnahme der Anzahl der nicht erkannten Fehler:

$$E(\varphi_{\mathrm{NErk}}, n) = \varphi_0 \cdot n^{-k}$$

Ersatz der Rechnegröße φ_0 durch den Erwartungswert für eine frei wählbare Testdauer n_0:

$$E\left(\varphi_{\mathrm{NErk}}, n\right) = E\left(\varphi_{\mathrm{NErk}}, n_0\right) \cdot \left(\frac{n}{n_0}\right)^{-k} \tag{14}$$

Bei einem Zufallstest nimmt die Anzahl der nicht nachweisbaren Fehler überschlagsweise mit dem Exponenten k ab $(0 < k < 1)$.

Beispielrechnung:
Ein System wurde mit angenommen 1.000 Zufallswerten getestet. welche Testanzahl ist erforderlich, um die Anzahl der nicht gefundenen Fehler zu halbieren, wenn der Exponent (die asymptodische Ordnung) der FHNW-Funktion $k = 0{,}3$, $0{,}5$ bzw. $0{,}8$ beträgt?

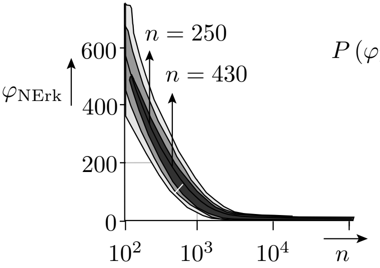
$$n = n_0 \cdot \left(\frac{E(\varphi_{\mathrm{NErk}}, n_0)}{E(\varphi_{\mathrm{NErk}}, n)}\right)^{\frac{1}{k}}$$

	$k = 0{,}3$	$k = 0{,}5$	$k = 0{,}8$
n	10.079	4.000	2.378

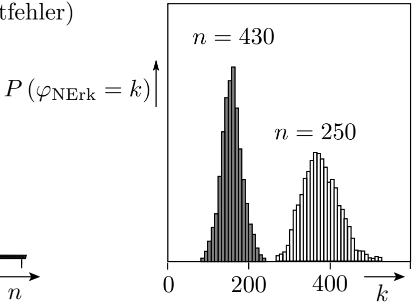
Experimente zur Haftfehlerüberdeckung

Kombinatorische Beispielschaltung (Benchmark c3540). Betrachtete Fehler sind 3606 simulierte, unterschiedlich nachweisbare Haftfehler. Bestimmung der Verteilung mit 1000 verschiedenen Zufallstestsätzen.

Verteilung der Anzahl der nicht erkannten Modellfehler als Funktion von n (Benchmark c3540, 3606 Haftfehler)



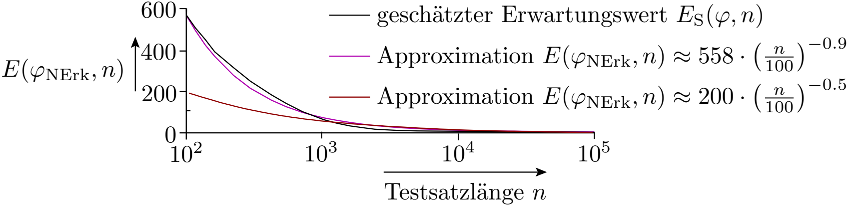
Verteilung für zwei Testsatzlängen



Annäherung von $E\left(\varphi_{\mathrm{NErk}}, n\right)$ durch eine Potenzfunktion

Annäherung der zu erwartenden Anzahl der nachweisbaren Fehler durch eine Potenzfunktion nach Gl. 14:

$$E\left(\varphi_{\mathrm{NErk}}, n\right) = E\left(\varphi_{\mathrm{NErk}}, n_0\right) \cdot \varphi_0 \cdot \left(\frac{n}{n_0}\right)^{-k}$$



Die Approximation mit $k = 0{,}9$ nähert den Bereich $n < 1000$ und die mit $k = 0{,}5$ den Bereich $n > 1000$ Testschritte besser an.

Zuverlässigkeitswachstum

Zuverlässigkeit und versteckte Fehler

Ein Maß der Zuverlässigkeit ist die zu erwartende mittlere Anzahl von richtig ausgeführten Service-Leistungen zwischen zwei Fehlfunktionen als Kehrwert der Auftrittswahrscheinlichkeit einer Fehlfunktion je Service. Bei seltenem Versagen $p_{\mathrm{SF}} \ll 1$ summieren sich die Wahrscheinlichkeiten des Versagens bezogen auf Einzelursachen:

$$Z_{\mathrm{n}} = \frac{1}{p_{\mathrm{SF}} = p_{\mathrm{S}} + p_{\mathrm{B}} + \ldots + \underbrace{\sum_{i=1}^{\mathrm{Anz(PF)}} \left(p_{i.\mathrm{vorh}}\left(n\right) \cdot p_{i.\mathrm{nachw}}\right)}_{\text{Fehlfunkt. durch versteckte Fehler}}}$$

(p_{S} – Fehlfunktionen durch Störungen; p_{B} – Fehlfunktionen durch Bedienfehler). Im weiteren wird nur die Teilzuverlässigkeit $Z_{\mathrm{n.Fehler}} = \frac{1}{\sum \ldots}$ durch versteckte Fehler betrachtet.

Testaufwand und Fehlerhäufigkeit

Es sei angenommen, dass Betrieb und Test mit gleichem Operationsprofil erfolgen und ein Fehler a-mal beim Test beobachtbar sein muss, bevor er erfolgreich beseitigt wird[14]. Beseitigungswahrscheinlichkeit:

$$p_{i.\mathrm{Beseit}}(n) = 1 - e^{-\frac{n \cdot p_{i.\mathrm{nachw}}}{a}}$$

Abnahme seine Vorhandenseins:

$$p_{i.\mathrm{vorh}}(n) = p_{i.\mathrm{vorh}} \cdot (1 - p_{i.\mathrm{Beseit}}(n)) = p_{i.\mathrm{vorh}} \cdot e^{-\frac{n \cdot p_{i.\mathrm{nachw}}}{a}}$$

Wahrscheinlichkeit einer Fehlfunktion durch alle versteckten Fehler, wenn das Systeme mit n Schritten getestet und erkennbare Fehler im Mittel nach dem a-ten Auftreten beseitigt werden:

$$p_{\mathrm{SF.Fehler}} = \sum_{i=1}^{\mathrm{Anz(PF)}} \left(p_{i.\mathrm{vorh}} \cdot e^{-\frac{n \cdot p_{i.\mathrm{nachw}}}{a}} \cdot p_{i.\mathrm{nachw}} \right)$$

[14] Tests beim Hersteller $a \approx 1$, Nutzerbetrieb als Test $a \gg 1$, abhängig wie häufig/gut der Feedback zum Hersteller ist.

Mit der FHNW-Funktion

$$p_{\text{SF.Fehler}}(n) = \int_0^1 p \cdot H(p) \cdot e^{-\frac{n \cdot p}{a}} \cdot dp$$

Mit der Approximation $H(p) = \varphi_0 \cdot k \cdot p^{k-1}$:

$$\begin{aligned} p_{\text{SF.Fehler}}(n) &= \int_0^1 p \cdot \varphi_0 \cdot k \cdot p^{k-1} \cdot e^{-\frac{n \cdot p}{a}} \cdot dp \\ &= \varphi_0 \cdot k \cdot \int_0^1 p^k \cdot e^{-\frac{n \cdot p}{a}} \cdot dp \end{aligned}$$

Die Substitution $p = \frac{a \cdot x}{n}$; $dp = \frac{a \cdot dx}{n}$ holt wieder die Testdauer n und die Nachweiswahrscheinlichkeit p aus dem Integral:

$$p_{\text{SF.Fehler}}(n) = \varphi_0 \cdot k \cdot \left(\frac{n}{a}\right)^{-(k+1)} \underbrace{\int_0^n x^k \cdot e^{-x} \cdot dx}_{\approx \Gamma(k+1) \approx 1 \text{ für } 0<k<1}$$

Das Restintegral $\int_0^n x^k \cdot e^{-x} \cdot dx$ stebt für große n gegen die Gamma-Funktion $\Gamma(k+1)$ und diese ist für $0 < k \leq 1$ näherungsweis eins.

Abnahme der Wahrscheinlichkeit für Fehlfunktionen

$$p_{\text{SF.Fehler}}(n) = \varphi_0 \cdot k \cdot \left(\frac{n}{a}\right)^{-(k+1)}$$

Zu erwartende Fehleranzahl nach einem Test mit n Schritten und einer mittleren Anzahl von a Beseitigungsversuchen:

$$E(\varphi, n) = E\left(\varphi_{\text{NErk}}, \frac{n}{a}\right) = \varphi_0 \cdot \left(\frac{n}{a}\right)^{-k}$$

Das Verhältnis aus der Auftrittswahrscheinlichkeit fehlerbedingter Fehlfunktionen und der zu erwartender Fehleranzahl:

$$\frac{p_{\text{SF.Fehler}}(n)}{E(\varphi, n)} = \frac{\varphi_0 \cdot k \cdot \left(\frac{n}{a}\right)^{-(k+1)}}{\varphi_0 \cdot \left(\frac{n}{a}\right)^{-k}} = \frac{k \cdot a}{n}$$

Das Verhältnis der Auftrittswahrscheinlichkeit fehlerbedingter Fehlfunktionen für zwei Testdauern n und n_0 ist:

$$p_{\text{SF.Fehler}}(n) = p_{\text{SF.Fehler}}(n_0) \cdot \left(\frac{n_0}{n}\right)^{k+1}$$

Zuverlässigkeitswachstum

Mittlere Anzahl von Service-Leistungen zwischen zwei fehlerbedingten Fehlfunktionen nimmt mit der Testdauer mit der $k+1$-ten Potenz zu:

$$Z_{\text{n.Fehler}}(n) = Z_{\text{n.Fehler}}(n_0) \cdot \left(\frac{n}{n_0}\right)^{k+1}$$

Beispielrechnung:

Ein System wurde mit angenommen 1.000 Zufallswerten getestet. welche Testanzahl ist erforderlich, um die mittlere Anzahl der Service-Leistungen zwischen zwei fehlerbedingten Fehlfunktionen zu verdoppeln, wenn der Exponent (die asymptodische Ordnung) der FHNW-Funktion $k = 0{,}3$, $0{,}5$ bzw. $0{,}8$ beträgt?

$$n = n_0 \cdot \left(\frac{Z_{\text{n.Fehler}}(n)}{Z_{\text{n.Fehler}}(n_0)}\right)^{\frac{1}{k+1}}$$

	$k = 0{,}3$	$k = 0{,}5$	$k = 0{,}8$
n	1.704	1.587	1.470

Nachweisabhängigkeiten

Abhängigkeiten im Fehlernachweis

Die bisherigen Beispielrechungen unterstellen immer, dass alle betrachteten Fehler bzw. Fehlfunktionen unanhängig voneinander auftreten und nachweisbar sind.

Fehler im selben Teilsystem teilen sich Steuer- und Beobachtungsbedingungen und sind mit fast denselben Eingaben nachweisbar. Für andere Fehler schließt sich der Nachweis gegenseitig aus.

- Wir wirkt sich das auf die Verteilung aus?
- Wie wirkt sich das auf die Varianz aus?

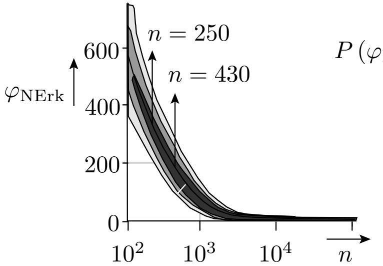
Nach Gl. 7 und 8 kommt bei Nachweisabhängigkeiten zur Varianz ein Covarianz-Summand hinzu:

$$\begin{aligned} D^2(X+Y) &= D^2(X) + D^2(Y) + 2 \cdot \mathrm{Cov}(X,Y) \\ \mathrm{Cov}(X,Y) &= E\left((X - E(X)) \cdot (Y - E(Y))\right) \end{aligned}$$

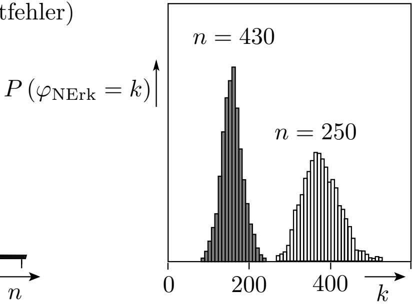
Nochmal das Experiment von Folie 110

Kombinatorische Beispielschaltung (Benchmark c3540). Betrachtete Fehler sind 3606 simulierte, unterschiedlich nachweisbare Haftfehler. Bestimmung der Verteilung mit 1000 verschiedenen Zufallstestsätzen.

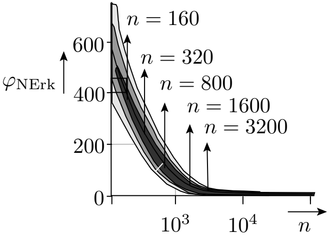
Verteilung der Anzahl der nicht erkannten Modellfehler als Funktion von n (Benchmark c3540, 3606 Haftfehler)



Verteilung für zwei Testsatzlängen



Varianz der Fehleranzahl im Experiment



Kontrolle, dass die tatsächliche Standardabweichung die Obergrenze

$$D^2_{\max}\left(\varphi_{\mathrm{NErk}}, n\right) = E\left(\varphi_{\mathrm{NErk}}, n\right) \cdot \left(1 - \frac{E(\varphi_{\mathrm{NErk}}, n)}{\mathrm{Anz(PF)}}\right)$$

nicht überschreitet.

n	160	320	800	1600	3200
$E\left(\varphi_{\mathrm{NErk}}, n\right)$	415	234	90	29	11
$\sqrt{D^2\left(\varphi_{\mathrm{NErk}}, n\right)}$	43,3	30,7	17,3	7,2	2,9
$\sqrt{D^2_{\max}\left(\varphi_{\mathrm{NErk}}, n\right)}$	19,2	14,8	9,37	5,36	3,31

Die Obergrenze unter der Annahme »unabhängiger Nachweis« wird deutlich überschritten. Für eine vollständige Haftfehlermenge offenbar nicht erfüllt.

Eine Deutung der Varianzerhöhung

Die tatsächlich deutlich größere Varianz ist so deutbar, das im Mittel

$$K = \frac{D^2\left(\varphi_{\text{NErk}}, n\right)}{D^2_{\max}\left(\varphi_{\text{NErk}}, n\right)}$$

($D^2_{\max}$ – theoretische Obergrenze, D^2 – experimentell bestimmte Varianz) identisch nachgewiesen werden. Die Bernoulli-Versuche haben dann die möglichen Ergebnisse 0 oder K:

$$\begin{aligned} P\left(\varphi_{i.\text{NErk}} = 0\right) &= 1 - p_i \\ P\left(\varphi_{i.\text{NErk}} = K\right) &= p_i \end{aligned}$$

Dafür gibt es weniger zu zählende Zufallsgrößen:

$$\varphi_{\text{NErk}} = \sum_{i=1}^{\text{Anz(PF)}/K} \varphi_{i.\text{NErk}}$$

(p_i – Nachweiswahrscheinlichkeit; Anz(PF) – Fehleranzahl).

Der Erwartungswert der Summanden:

$$E\left(\varphi_{i.\mathrm{NErk}}\right) = 0 \cdot (1 - p_i) + K \cdot p_i = K \cdot p_i$$

Varianz der Summanden:

$$\begin{aligned} D^2\left(\varphi_{i.\mathrm{NErk}}\right) &= (1 - p_i) \cdot (0 - K \cdot p_i)^2 + p_i \cdot (K - K \cdot p_i)^2 \\ &= p_i \cdot K^2 \cdot (1 - p_i) \end{aligned}$$

Auf den Erwartungswert der Summe hat es keinen Einfluss, ob K Fehler identisch nachgewiesen werden:

$$E\left(\varphi_{\mathrm{NErk}}\right) = \sum_{i=1}^{\mathrm{Anz(PF)}/K} K \cdot p_i = \sum_{i=1}^{\mathrm{Anz(PF)}} p_i$$

Die Varianz erhöht sich um den Faktor K:

$$D^2\left(\varphi_{\mathrm{NErk}}\right) = \sum_{i=1}^{\mathrm{Anz(PF)}/K} p_i \cdot K^2 \cdot (1 - p_i) = K \cdot \sum_{i=1}^{\mathrm{Anz(PF)}} \cdot p_i \cdot (1 - p_i)$$

Rückführbar auf eine Zählverteilung für weniger, dafür aber unabhängig nachweisbarer Fehler.

Effektive Fehleranzahl

Die effektive Fehleranzahl φ_{eff} sei die zu simulierte Fehleranzahl, bei der bei unabhängigem Fehlernachweis die Varianz gleich ihrer Obergrenze ist, aber nicht größer als die tatsächliche Anzahl der simulierten Fehler Anz(PF). Dazu wird die Anzahl der simulierten Fehler bei einer Varianzvergrößerung von $K > 1$ durch K geteilt:

$$\varphi_{\mathrm{eff}} = \begin{cases} \mathrm{Anz(PF)} & K \le 1 \\ \frac{\mathrm{Anz(PF)}}{K} & K > 1 \end{cases}$$

mit

$$K = \frac{D^2\left(\varphi_{\mathrm{NErk}}, n\right)}{D^2_{\mathrm{max}}\left(\varphi_{\mathrm{NErk}}, n\right)}$$

und

$$D^2_{\mathrm{max}}\left(\varphi_{\mathrm{NErk}}, n\right) = E\left(\varphi_{\mathrm{NErk}}, n\right) \cdot \left(1 - \frac{E\left(\varphi_{\mathrm{NErk}}, n\right)}{\mathrm{Anz(PF)}}\right)$$

Effektive Fehleranzahl für das Experiment

Die effektive Fehleranzahl ist ein Richtwert, wie viele Fehler für eine genauso genaue Schätzung zu simulieren sind, wenn die unterstellten Fehler unabhängig voneinander nachweisbar wären.

Für den Versuch auf Folie 110 ist die effektive Fehleranzahl zum Teil weniger als ein Viertel der simulierten Fehleranzahl:

n	160	320	800	1600	3200
φ_{eff} für $\mathrm{Anz(PF)} = 3606$	706	839	1037	2001	3606

Für $n = 320$ Testschritte würde man z.B. mit ca. 900 unabhängig nachweisbaren Fehlern keine größere Varianz als mit den 3600 angenommen Modellfehlern erhalten. Ist es da nicht zweckmäßiger, nur eine Fehlerstichprobe zu simulieren?

Simulation mit Fehlerstichproben

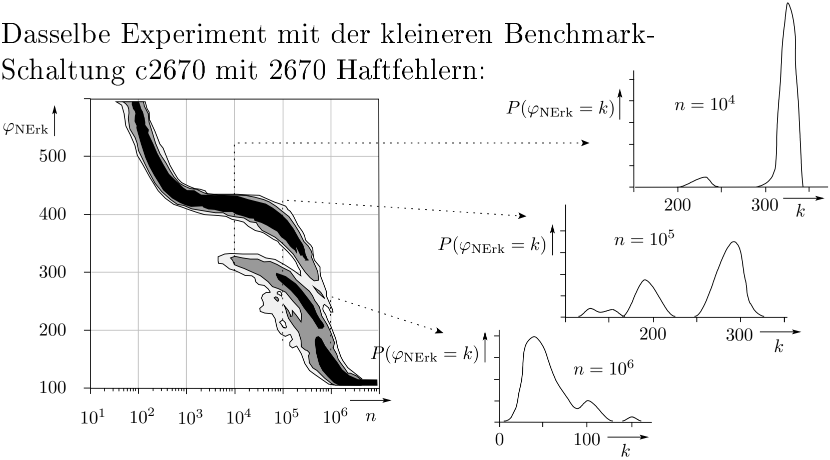
Im nachfolgenden Versuch wird eine zufällige Fehlestichprobe von 1000 bzw 300 der 3606 Haftfehler simuliert. Das naheliegende Ergebnis ist eine Verringerung der Abhängigkeiten im Fehlernachweis, erkennbar an einer effektiven Fehleanzahl, die näher an der tatsächlich simulierten Fehleranzahl liegt.

n	160	320	800	1600	3200
φ_{eff} für Anz(PF) = 1000	594	629	630	1000	1000
φ_{eff} für Anz(PF) = 300	297	268	277	231	300

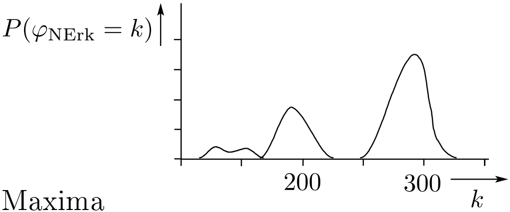
Bei der Stichprobe von 1000 Fehlern ist die effektive Fehleranzahl im ungünstigste Fall fast halb so groß und bei 300 Modellfehler 77% der Anzahl der simulierten Fehler.

Ein zweites Experiment zur Haftfehlerüberdeckung

Dasselbe Experiment mit der kleineren Benchmark-Schaltung c2670 mit 2670 Haftfehlern:



Im Bereich von $n = 10^4$ bis 10^6 multimodale Verteilung.



Verteilung mit mehreren Maxima

- Wie kann ein Zählprozess eine solche Verteilungen haben?

Gedankenexperiment:

- zehn Modellfehler, davon acht identisch nachweisbar.
- Wertebereich für die Anzahl der nachgewiesenen Fehler:

$$k \in \{0, 1, 2, 8, 9, 10\}$$

  Die Verteilung zerfällt in zwei Teilkämme.

- Die Haftfehlermenge des c2670 enthält offenbar ca. 80 sehr ähnlich nachweisbare Fehler.

Aufgaben

Aufgabe 3.1: Fehlernachweisdichte

Gegeben ist das nachfolge Säulendiagramm für die Fehlernachweisdichte. Das System soll mit $n = 1000$ zufällgen Service-Aufrufen getestet und die dabei erkannten Fehler alle beseitigt werden.

1. Wie groß ist der zu erwartende Anteil der beseitigten Fehler?
2. Bestimmen Sie die neuen Werte h_j des Fehlernachweisdichte nach Test und Fehlerbeseitigung.

Hinweis: Da für die Häufigkeitswerte jeder Säule ein Bereich der Nachweiswahrscheinlichkeit zugeordnet ist, kann nach einer von der Nachweiswahrscheinlichkeit Fehlerbeseitigung für die neuen Werte von h_j nur ein Bereich angegeben werden. Die beiden Bereichsgrenzen ergeben sich je durch Einsätzen der maximalen und der minimalen Nachweiswahrscheinlichkeit.

Aufgabe 3.2: Erforderliche Testsatzlänge

Bei einer Fehlersimulation mit 3000 Fehlern und 1000 verschieden Zufallsfolgen wurde die zu erwartende Anzahl der nicht nachweisbaren Fehler als Funktion der Testsatzlänge n bestimmt:

n	100	1.000	10.000	100.000	1.000.000
$E(\varphi)$	1532	751	370	95	48

1. Nähern Sie den Verlauf der Erwartungswerte für die drei längsten Testzeiten durch eine Potenzfunktion

$$E(\varphi, n) \approx E(\varphi, n_0) \cdot \left(\frac{n}{n_0}\right)^{-k}$$

an.

2. Wie lange sind Test und Fehlerbeseitigung bei dieser Approximation noch fortzusetzen, bis die zu erwartende Fehleranzahl nicht mehr größer als 20 ist?

Aufgabe 3.3: Effektive Fehleranzahl

Bei demselben Experiment wie in der Aufgabe zuvor wurde auch die Standardabweichung der nicht nachweisbaren Fehler in Abhängigkeiten von der Testsatzlänge n bestimmt:

n	100	1.000	10.000	100.000	1.000.000
$E(\varphi)$	751	532	370	95	48
$\sqrt{D^2(\varphi)}$	53.7	41,8	23,5	12,1	5,3

Wie groß ist die effektive Fehleranzahl φ_{eff} für die in der Tabelle angegebenen Testsatzlängen?

Aufgabe 3.4: Fehlerbedingte Fehlfunktionen 1

Bestimmen Sie für die Fehlernachweisdichte auf Aufgabe 3.1 und eine zu erwartende Fehleranzahl vor dem Test von $E(\varphi_{\mathrm{E}}) = 100$ die zu erwartende Anzahl der Fehlerfunktionen bei 10^6 Service-Anforderungen

1. vor den Test
2. nach dem Test mit 1000 zufälligen Service-Anforderungen und der Beseitigung der dabei nachgewiesen Fehler.

Hinweis: Da für die Häufigkeitswerte jeder Säule ein Bereich der Nachweiswahrscheinlichkeit zugeordnet ist, ist auch für die Anzahl der fehlerbedingten Fehlfunktionen nur eine Worst- und eine Best-Case-Rechnung möglich.

Aufgabe 3.5: Fehlerbedingte Fehlfunktionen 2

Für ein System wurden bei einer Fehlersimulation mit 3000 Fehlern und 1000 verschieden Zufallsfolgen die zu erwartende Anzahl der nicht nachweisbaren Fehler in Abhängigkeiten von der Testsatzlänge n bestimmt:

n	100	1.000	10.000	100.000	1.000.000
$E(\varphi)$	532	751	370	95	48

Beim Test des realen Systems mit 100 zufälligen Testbeispielen wurden insgesamt 53 Fehler erkannt und beseitigt. Schätzen Sie unter Verwendung von Gl. ?? die Wahrscheinlichkeiten für ein durch Fehler verursachtes Service-Versagen des Systems nach der Beseitigung der mit 100, 1.000, ... und 1.000.000 zufälligen Service-Aufrufen nachweisbaren Fehler.

Beurteilende Statistik

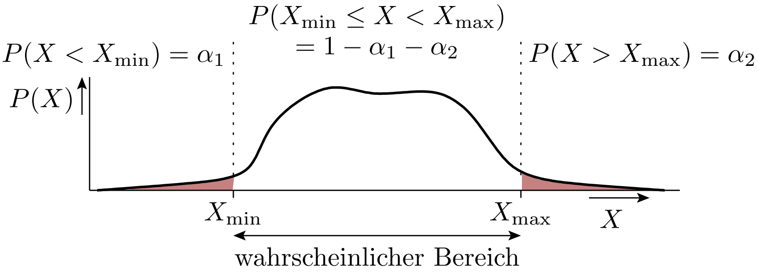
Beurteilende Statistik

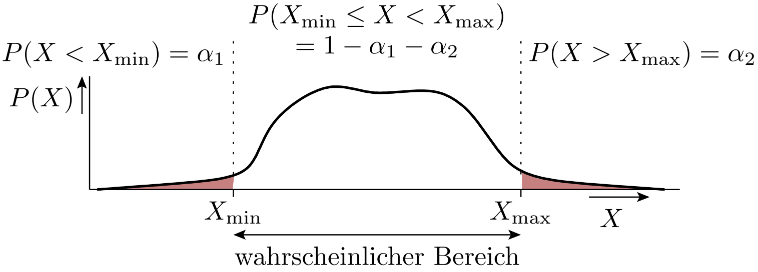
In den bisherigen Betrachtungen wurden ausgehend von den Versuchsbeschreibungen Verteilungen und ihre Eigenschaften hergeleitet, die beschreiben, was von einer Stichprobe von experimentellen Ergebnissen erwartet werden sollte. Die beurteilende Statisktik geht den umgekehrten Weg. Aus einer Stichprobe von experimentellen Ergebnissen soll auf die Verteilung geschlossen werden.

- nicht-parametrische Statistik: Es existiert kein Wissen über die Verteilung der Daten. Beispiel: Untersuchung, ob es wie auf den Folien 89 und 127 Polarisierungen gibt.
- parametrische Statistik: Es wird davon ausgegangen, dass schon Erfahrungen über die Art und Eigenschaften der Verteilung vorliegen und nur einzelne Parameter zu bestimmen sind, bzw. Prüfung, ob eine Annahme (Hypothese) stimmt.

Kontrolle von Hypothesen

Unter der Anahme einer bekannten Verteilung einer Zufallsgröße lässt sich ein Bereich $[X_{\mathrm{min}}, X_{\mathrm{max}}]$ der wahrscheinlichen Werte definieren, z.B. durch Vorgabe, dass der Wert nur mit einer Irrtumswahrscheinlich α_1 kleiner X_{min} und mit einer Irrtumswahrscheinlichkeit α_2 größer X_{max} sein darf.





Die Hypothese, dass ein Versuchsergebnis X diese Verteilung hat, wird angenommen, wenn der Ergebniswert im wahrscheinlichen Bereich liegt und sonst zurückgewiesen. Nur sinnvoll für Zufallsgrößen mit großem Wertebereich und geringer Streuung. Für einzelne Zählwerte, die nur null oder eins sein können, z.B. ob ein Service versagt oder ein potentieller Fehler existiert, ungeeignet. Für den Mittelwert oder die Summe vieler Bernoulli-Versuche geeignet.

Verteilung unbekannt

Das schwache Gesetz der großen Zahlen

nach der tschebytschewschen Ungleichung:

$$P\left(|X - E(X)| \geq \varepsilon\right) \leq \frac{D^{\mathbf{2}}(X)}{\varepsilon^2}$$

ist die Wahrscheinlichkeit, das der Wert einer Zufallsgröße mehr als ein Intervallradius ε von seinem Erwartungswert abweicht, nicht größer als das Verhältnis der Varianz zum Quadrat des Intervallradius ε. Bei Zulassen einer Irrtumswahrscheinlichkeit α beträgt der Intervallradius mindestens:

$$\varepsilon \geq \sqrt{\frac{D^{\mathbf{2}}(X)}{\alpha}}$$

Ausgehend von einem bekannten Schätzwert X beschränkt das den Bereich des Erwartungswerts auf $X \pm \varepsilon$. Bei bekanntem oder vermutetem Erwartungswert $E(X)$ ist der zulässige Bereich für Schätzwerte, bei denen der Erwartungswert noch nicht anzuzweifeln ist, $E(X) \pm \varepsilon$.

Erwartungswert und Varianz einer Datenstichprobe

Für eine Datenstichprobe

$$X = (X_1, X_2, \ldots, X_{N_S})$$

ist der Schätzer für den Erwartungswert der Mittelwert:

$$E_S(X) = \frac{1}{N_S} \cdot \sum_{i=1}^{N_S} X_i$$

und für die Varianz:

$$D_S^2(X) = \frac{1}{N_S - 1} \cdot \sum_{i=1}^{N_S} (X_i - E(X))^2$$

Ohne Vorwissen über die Verteilung der Datenstichprobe ist der wahrscheinliche Bereich für künftige Datenwerte:

$$E_S(X) \pm \varepsilon \qquad \text{mit} \quad \varepsilon \leq \sqrt{\frac{D_S^2(X)}{\alpha}}$$

Zum Schätzen der Varianz

$$D_{\mathrm{S}}^{2}(X)=\frac{1}{N_{\mathrm{S}}-1}\cdot\sum_{i=1}^{N_{\mathrm{S}}}\left(X_{i}-E(X)\right)^{2}$$

sollte die Datensichprobe $N_{\mathrm{S}}\gg 1$ sein.

Beispiel: Erwartungswert einer Widerstandsmessung

Gegeben sei eine Stichprobe gemessener Widerstandswerte in kΩ:

$$X:\ 10{,}3,\ 10{,}5,\ 9{,}7,\ 8{,}9,\ 10{,}1,\ 11{,}0,\ 10{,}2,\ 9{,}5$$

Aus dieser Stichprobe soll ohne weitere Vorkenntnisse über die Verteilung auf den möglichen Bereich des Erwartungswertes geschlussfolgert werden. Zugelassene Irrtumswahrscheinlichkeit $\alpha = 2\%$.

Zur Lösung der Aufgabe sind Erwartungswert und Varianz der Datenstichprobe zu schätzen:

$$E_{\mathrm{S}}(R) = \frac{1}{8}(10{,}3 + \ldots)\ \mathrm{k\Omega} = 10{,}025\,\mathrm{k\Omega}$$

$$D^2_{\mathrm{S}}(R) = \frac{1}{7}\left((10{,}3 - 10{,}025)^2 + \ldots\right)\ \mathrm{k\Omega}^2 = 0{,}419\,\mathrm{k\Omega}^2$$

Der Intervallradius:

$$\varepsilon \geq \sqrt{\frac{D_{\mathrm{S}}^2\,(R)}{\alpha}} = \sqrt{\frac{0{,}419\,\mathrm{k}\Omega^2}{0{,}02}} = 4{,}58\,\mathrm{k}\Omega$$

Das Datenmaterial erlaubt die Zusicherung, dass der tatsächliche Erwartungswert nicht mehr als $\pm 4{,}58\,\mathrm{k}\Omega$ vom geschätzten Erwartungswert abweicht:

$$E(R) = 10{,}03\,\mathrm{k}\Omega \pm 4{,}58\,\mathrm{k}\Omega$$

Die tschebytschewsche Ungleichung erlaubt nur die sehr grobe Bereichsabschätzungen

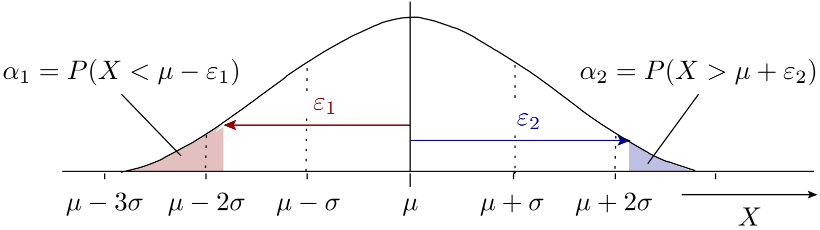
$$5,44\,\mathrm{k}\Omega < E\,(R) < 14,60\,\mathrm{k}\Omega$$

verlangt aber keinerlei Vorkenntnisse oder Annahmen über die Verteilung. Die Widerstandswerte dürfen z.B. auch eine multimodale Verteilung haben. Weiteres Zusatzwissen über die Verteilung erlaubt engere Bereichseingrenzungen.

Normalverteilung

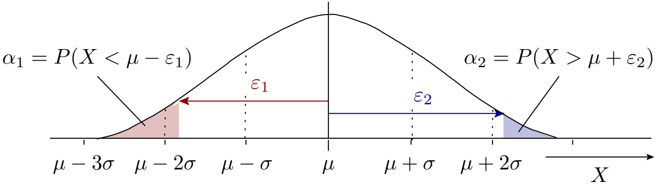
Bereichschätzungen für normalverteilte Größen

Die Werte von Widerständen aus demselben Fertigungsprozess und viele andere Zufallsgrößen sind in guter Näherung normalverteilt.



Die Irrtumswahrscheinlichkeiten beider Möglichkeiten einer einseitigen Bereichsschätzung betragen

$$\begin{aligned} \alpha_1 &= P\left(X < \mu - \varepsilon_1\right) \\ \alpha_2 &= P\left(X > \mu + \varepsilon_2\right) \end{aligned}$$



Sie ergeben sich aus der Tabelle der Standardnormalverteilung und der Standardabweichung σ.

$\varepsilon_\sigma = \frac{\varepsilon_{1/2}}{\sigma}$	1	2	3	4	2,05	2,33	2,57	2,88	3,10
$\alpha_{1/2}$	15,9%	2,27%	0,13%	0	2%	1%	0,5%	0,2%	0,1%

Die Irrtumswahrscheinlichkeiten der beiderseitigen Bereichsschätzung ist die Summe der Irrtumswahrscheinlichkeiten der beiden einseitigen Bereichsschätzungen:

$$\alpha = \alpha_1 + \alpha_2 = P(X < \mu - \varepsilon_1) + P(X > \mu + \varepsilon_2)$$

Beispiel: Erwartungswert einer Widerstandsmessung

Gegeben sei dieselbe Stichprobe gemessener Widerstandswerte wie auf Folie 143 mit dem Erwartunggswert $E_{\mathrm{S}}(R) = 10{,}025\,\mathrm{k}\Omega$ und der Varianz $D_{\mathrm{S}}^2(R) = 0{,}419\,\mathrm{k}\Omega^2$. Diesmal sei unterstellt, dass die Widerstände alle aus demselben Fertigungsprozess kommen, so dass die Messwerte normalverteilt sind. Zugelassene Irrtumswahrscheinlichkeit $\alpha = 2\%$.

Die Irrtumswahrscheinlichkeit $\alpha = 2\%$ soll gleich auf oberhalb und unterhalb des zulässigen Bereichs aufgeteilt werden: $\alpha_1 = \alpha_2 = 1\%$. Dafür beträgt der relative Intervallradius $\frac{\varepsilon}{\sigma} = \frac{\varepsilon_1}{\sigma} = \frac{\varepsilon_1}{\sigma} = 2,33$ und der absolute Intervallradius $\varepsilon = 2,33 \cdot \sqrt{0{,}419\,\mathrm{k}\Omega^2} = 1,51\,\mathrm{k}\Omega$. Der wahrscheinliche Bereich des Erwartungswertes

$$8,51\,\mathrm{k}\Omega < E(R) < 11,53\,\mathrm{k}\Omega$$

ist weniger als halb so breit, wie ohne Annahme »normalverteilt«.

Warsch. Zählereignisse

Eintrittswahrscheinlichkeit von Zählwerten

Zählwerte sind eine Summe von Einzelereignissen (z.B. Anzahl fehlerhaft ausgeführten Service-Leistungen, vorhandene Fehler, ...). Die Einzelereignisse können null oder eins sein und haben die Verteilung (vergl. Folie 69):

k	0	1
$P(X_i = k)$	$1 - p_i$	p_i

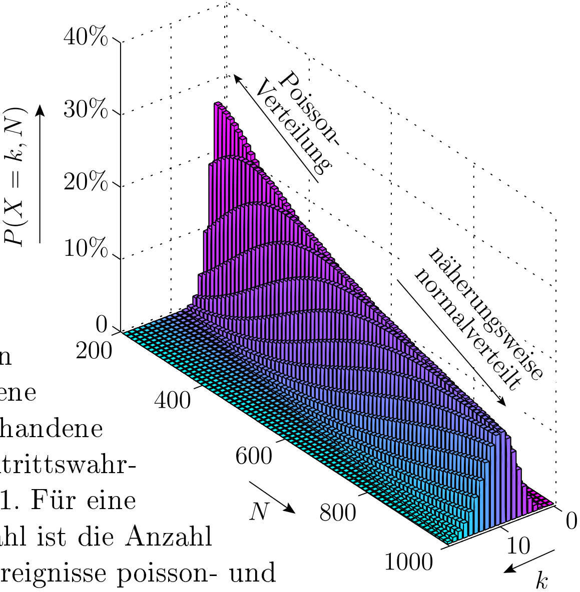
Die Verteilung der Summe

$$X = \sum_{i=1}^{N} X_i$$

für N nicht korrelierte Versuche leitet sich aus dem Erwartungswert (Gl. 9)

$$E(X) = \sum_{i=1}^{N} p_i = N \cdot \bar{p}$$

ab ($\bar{p}$ – mittlere Eintrittswahrscheinlichkeit).



Für die betrachteten Beispiele (eingetretene Fehlfunktionen, vorhandene Fehler) sind die Eintrittswahrscheinlichkeit $p_i \ll 1$. Für eine kleine Versuchsanzahl ist die Anzahl der eingetretenen Ereignisse poisson- und für eine größere näherungsweise normalverteilt.

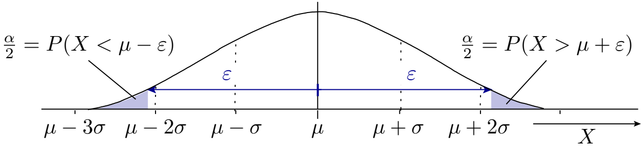
Die mittlere Eintrittswahrscheinlichkeit ist der Quotient aus Erwartungswert und Versuchsanzahl:

$$\bar{p} = \frac{E(X)}{N}$$

Eine Erwartungswertschätzung mit geringem Intervallradius (z.B. Schätzwert ±10%) verlangt eine Versuchsanzahl N, bei der der Zählwert normalverteilt ist. Bei Normalverteilung ist die Varianz einer Zählgröße nicht größer als die einer Binomialverteilung mit gleichem Erwartungswert (Gl. 77):

$$\sigma^2 = D^2(X) \leq E(X) \cdot \left(1 - \frac{E(X)}{N}\right) = N \cdot \bar{p} \cdot (1 - \bar{p}) \qquad (15)$$

und die beiden Irrtumswahrscheinlichkeiten sind gleich $\alpha_1 = \alpha_2 = \alpha/2$.



Schätzen der mittleren Eintrittswahrscheinlichkeit

Die geschätzte mittlere Eintrittswahrscheinlichkeit eines Zählereignisses ist die experimentell bestimmte Anzahl durch die Versuchsanzahl:

$$\bar{p}_{\mathrm{S}} = \frac{X}{N}$$

Der Schätzwert soll mit einer Irrtumswahrscheinlichkeit α maximal um einen Intervallradius $\varepsilon_{\bar{p}}$ von der zu schätzenden Wahrscheinlichkeit

$$\bar{p} = \frac{E(X)}{N}$$

abweichen.

Aus der Irrtumswahrscheinlichkeit ergibt sich tabellarisch der Intervallradius für eine standardisierte Normalverteilung ε_σ [15]:

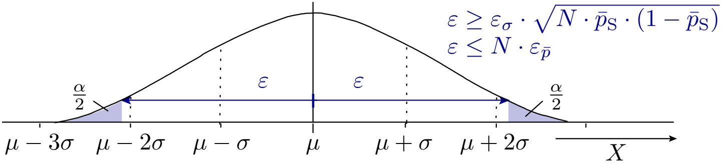
$\varepsilon_\sigma = \frac{\varepsilon}{\sigma}$	1	2	3	4	2,05	2,33	2,57	2,88	3,10
α	31,8%	4,54%	0,26%	0	4%	2%	1%	0,4%	0,2%

[15] Beiderseitige Bereichsschätzung mit $\alpha = \alpha_1 + \alpha_2$ (vergl. Tabelle Folie).

Der Intervallradius für eine standardisierte Normalverteilung multipliziert mit der Varianz ist der minimal zu fordernde Intervallradius der wahrscheinlichen Zählwerte. Für die Varianz soll die Obergrenze nach Gl. 15 mit $\bar{p} = \bar{p}_\mathrm{S}$ verwendet werden:

$$\varepsilon \geq \varepsilon_\sigma \cdot \sqrt{N \cdot \bar{p}_\mathrm{S} \cdot (1 - \bar{p}_\mathrm{S})}$$

Der minimal erforderliche Intervallradius ist der geforderte relative Intervallradius $\varepsilon_{\bar{p}}$ mal die Versuchsanzahl N:



Aus der Unter- und Obergrenze für den Intervallradius folgt:

$$\begin{aligned} N \cdot \varepsilon_{\bar{p}} &\geq \varepsilon_\sigma \cdot \sqrt{N \cdot \bar{p}_\mathrm{S} \cdot (1 - \bar{p}_\mathrm{S})} \\ N &\geq \left(\frac{\varepsilon_\sigma}{\varepsilon_{\bar{p}}}\right)^2 \cdot \bar{p}_\mathrm{S} \cdot (1 - \bar{p}_\mathrm{S}) \end{aligned}$$

Beispielabschätzung

Es soll die Wahrscheinlichkeit $p_{\mathrm{SF}} \ll 1$ für das Versagen einer Service-Leistung geschätzt werden. Intervallradius $\varepsilon_{\bar{p}}$ sei 10% des Schätzwertes und die Irrtumswahrscheinlichkeit, dass der Schätzwert außerhalb des Intervalls liegt, sei $\alpha = 2\%$.

Irrtumswahrscheinlichkeit 2% verlangt einen Intervallradius von $\varepsilon_\sigma \leq 2,33$. Der Intervallradius der zu schätzenden Wahrscheinlichkeit ist 10% des Schätzwerts $\varepsilon_{\bar{p}} = 0,1 \cdot \bar{p}_{\mathrm{S}}$. Die erforderliche Versuchsanzahl beträgt:

$$N \geq \left(\frac{2{,}33}{0{,}1 \cdot \bar{p}_{\mathrm{S}}}\right)^2 \cdot \bar{p}_{\mathrm{S}} \cdot (1 - \bar{p}_{\mathrm{S}}) \approx \left(\frac{2{,}33}{0{,}1}\right)^2 \cdot \frac{1}{\bar{p}_{\mathrm{S}}} = \frac{543}{\bar{p}_{\mathrm{S}}}$$

Die erforderliche Anzahl der Service-Anforderungen ist so groß zu wählen, dass mindesten 543 Fehlfunktionen zu beobachten sind, damit die geschätzte Wahrscheinlichkeit mit 98% Sicherheit nicht mehr als 10% vom tatsächlichen Wert abweicht.

Seltene Ereignisse

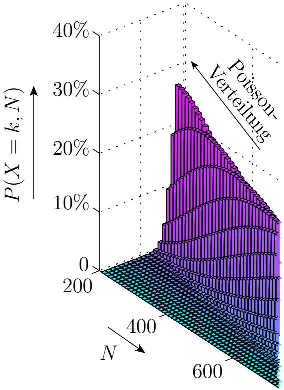
Ausschluss seltener Ereignisse

Ein IT-System in einer sicherheitskritischen Anwendung (Steuerung von Fahrzeugen, Anlagen, ...) kann bei einer Fehlfunktion erheblichen Schaden verursachen. Das gilt nur für einen kleinen Teil der möglichen Fehlfunktionen. Diese müssen mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden, ohne dass ein 100%-iger Ausschlussmöglich ist.

Für seltene Ereignisse ist die Anzahl der eintretenden Ereignisse poisson-verteilt:

$$P(X = k) = e^{-\bar{p}\cdot N} \cdot \frac{(\bar{p}\cdot N)^k}{k!}$$

($\bar{p} \ll 1$ – mittlere Eintrittswahrscheinlichkeit; N – Versuchsanzahl, z.B. Anzahl der genutzten Service-Leistungen).



Die hier zu untersuchenden Fragestellungen sind:

- Wie hoch ist die Sicherheit, dass keines oder nur eine tolerierbar geringe Anzahl von kritischen Ereignissen eintritt?
- Wie groß darf die mittlere Eintrittswahrscheinlichkeit kritischer Ereignisse maximal sein?
- Wie oft dürfen Service-Leistungen, bei denen kritische Fehlfunktionen auftreten können, genutzt werden?

Wenn mit einer Irrtumswahrscheinlichkeit α kein kritisches Ereignis tolerierbar ist, muss die Wahrscheinlichkeit »kein kritisches Ereignis« größer $1-\alpha$ sein:

$$P(X=0) = e^{-\bar{p}\cdot N} \geq 1-\alpha$$

Das Produkt aus der Eintrittswahrscheinlichkeit kritischer Fehlfunktionen und der Anzahl der genutzten Service-Leistungen darf nicht größer sein als:

$$\bar{p}\cdot N \leq -\ln(1-\alpha)$$

Beispiel absturzfreie Nutzungsdauer

Eine sehr störende Fehlfunktion ist der Absturz eines Programms mit Datenverlust. Die Wahrscheinlichkeit dafür sei im Mittel je Programmbenutzung $\bar{p} = 10^{-3}$. Wie oft kann das Programm hintereinander genutzt werden, ohne dass der Schadesfall eintritt. Irrtumswahrscheinlichkeit, dass der Schaden doch innerhalb dieser Nutzungsdauer eintritt, sei $\alpha = 1\%$.

Maximale Nutzungsanzahl:

$$N = \frac{-\ln(1 - 1\%)}{10^3} \approx 10$$

Bei nicht mehr als 10-maliger Programmnutzung bleiben im Mittel 99% der Nutzer von dieser Fehlersituation verschont.

Wenige tolerierbare Schadensfälle

Für eine Anzahl von $k_{\max}$ tolerierbaren kritschen Ereignissen beträgt die Sicherheit $1-\alpha$, dass sie nicht überschritten wird:

$$P(X \leq k) = e^{-\bar{p}\cdot N} \cdot \frac{(\bar{p}\cdot N)^k}{k!} \leq 1-\alpha$$

Nachfolgende Tabelle zeigt die maximalen Erwartungswerte $\bar{p}\cdot N$, bis zu denen mit unterschiedlichen Irrtumswahrscheinlichkeiten garantiert werden kann, dass die kritischen Ereignisse nicht öfter als 0, 1, 2 oder 3 mal eintreten:

	$k_{\max}=0$	$k_{\max}=1$	$k_{\max}=2$	$k_{\max}=3$
$\alpha = 0{,}5\%$	$5{,}01\cdot 10^{-3}$	$1{,}03\cdot 10^{-1}$	$3{,}38\cdot 10^{-1}$	$6{,}72\cdot 10^{-1}$
$\alpha = 1\%$	$1{,}01\cdot 10^{-2}$	$1{,}49\cdot 10^{-1}$	$4{,}36\cdot 10^{-1}$	$8{,}23\cdot 10^{-1}$
$\alpha = 2\%$	$2{,}02\cdot 10^{-2}$	$2{,}15\cdot 10^{-1}$	$5{,}67\cdot 10^{-1}$	$1{,}02$

Erweiterung des vorherigen Beispiels

Die Wahrscheinlichkeit für ein Programmabsturz sei weiterhin im Mittel $\bar{p} = 10^{-3}$ je Programmbenutzung. Die Fragestellung sei dahingehend erweitert, wie oft kann das Programm hintereinander genutzt werden, ohne dass der Schadesfall mehr als 1, 2 oder 3 mal eintritt. Die Irrtumswahrscheinlichkeit sei weiterhin $\alpha = 1\%$.

Ergebnis sind die Tabellenwerte für $\alpha = 1\%$ multipliziert mit $N^{-1} = 1000$:

	$k_{\max} = 0$	$k_{\max} = 1$	$k_{\max} = 2$	$k_{\max} = 3$
$\alpha = 1\%$	$10,1$	149	436	823

Aufgaben

Aufgabe 4.1: Erwartungswert und Varianz

Schätzen Sie den Erwartungswert und die Varianz der nachfolgenden Datenstichprobe:

```
8,45, 11,90, 12,22,  9,74, 10,80,
7,62,  7,66, 10,54, 11,96, 16,25,
8,77, 10,73, 10,11,  5,85,  9,29,
6,17, 12,23,  8,26, 10,53,  9,05
```

Aufgabe 4.2: Bereichsschätzung Schichtdicke

Gegeben ist die Messreihe einer Halbleiterschichtdicke in nm:

```
232.37 235.62 238.14 236.65 237.96
231.42 233.29 234.65 232.75 232.89
229.59 238.69 229.39 233.68 242.76
233.15 239.26 235.40 234.25 230.72
```

Schätzen Sie Erwartungswert und Varianz der Messergebnisse

1. In welchem Bereich liegt der Erwartungswert ohne Zusatzwissen über die Verteilung.
2. In welchem Bereich liegt die zu erwartende Schichtdicke, wenn von einer Normalverteilung ausgegangen werden kann?

Zulässige Irrtumswahrscheinlichkeit $\alpha = 1\%$.

Lösungsvorschlag

```
x=[232.37 235.62 238.14 236.65 237.96 231.42 ...
233.29 234.65 232.75 232.89 229.59 238.69 229.39 ...
233.68 242.76 233.15 239.26 235.40 234.25 230.72];
EX=0;
for i=1:length(x)
 EX=EX+x(i);
end EX=EX/length(x);
DX2=0;
for i=1:length(x)
 DX2=DX2+(x(i)-EX)^2;
end
DX=sqrt(DX2/(length(x)-1));
fprintf('Bereich Tschb: %f <X< %f\n', EX-10*DX, EX+10*DX);
fprintf('Bereich Norma: %f <X< %f\n', ...
         EX-2.33*DX, EX+2.33*DX);
```

Aufgabe 4.3: Fehlerentstehungswahrscheinlichkeit

Beim Programmieren entstehen Fehler in der Größenordnung von $\bar{p} \approx 1...10\%$ je Codezeile. Der Wert schwankt aber von Programmierer zu Programmierer. Zur Motivierung zu qualitativ guter Arbeit soll ein leistungsabhängiges Gehalt in Abhängigkeit vom »Güteparameter« $\bar{p}$ des Programmierers gezahlt werden. Dazu sei der Güteparameter mit einer relativen Genauigkeit von $\varepsilon_{\bar{p}} = 5\% \cdot \bar{p}$ und einer Irrtumswahrscheinlichkeit $\alpha = 1\%$ für jeden Programmierer zu schätzen. Für wie viele Code-Zeilen an Programmen müssten dazu von jedem zu evaluierenden Programmierer die entstandenen Fehler gezählt werden?

Aufgabe 4.4: Garantierbarer fehlerfreier Betrieb

Für wie viele Service-Anforderungen hintereinander kann für maximal ein Versagen (kein oder ein falsches Ergebnis) garantiert werden, wenn die mittlere Auftrittswahrscheinlichkeit einer Fehlfunktion je Service-Leistung $\bar{p} = 10^{-6}$ beträgt. Irrtumswahrscheinlichkeit $\alpha = 1\%$.

Aufgabe 4.5: Bereichsschätzung Fehleranzahl

Eine Test hat $\varphi = 400$ Fehler erkannt. In welchem Bereich liegt die zu erwartende Anzahl der nachweisbaren Fehler bei einer Irrtumwahrscheinlichkeit von $\alpha = 2\%$

Aufgabe 4.6: Anzahl der nicht erkannten Fehlfunktionen

Eine Kontrolle habe einer Erkennungswahrscheinlichkeit $p_{\mathrm{E}} = 99\%$. Es werden

1. 1000
2. 10000
3. 100000

Service-Leistungen kontrolliert, von denen 10% fehlerhaft sind. Wie hoch ist die Wahrscheinlichkeit, das weniger als 95% der fehlerhaften Service-Leistungen erkannt werden?

Hinweise: Bei einem Erwartungswert kleiner zehn ist die Anzahl der nicht erkannten falschen Service-Leistungen näherungsweise Poisson- und bei einem Erwartungswert ab zehn normalverteilt.

Literatur