Test and Depentability
Slide set 2:
Probabilities

Prof. G. Kemnitz

Institute for Computer Science, TU Clausthal (TV_F2_engl.pdf)
May 5, 2023

Contents slide set 2: Probabilities

lecture	5	6	7
slide	2	25	65

Probability

Definition, estimation

Probability

If an experiment is repeated N times, the relative frequency $\#A/N$ of a certain random event A tends with increasing N under constant experimental conditions towards the probability:

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

Examples of parameters previously defined as probabilities:

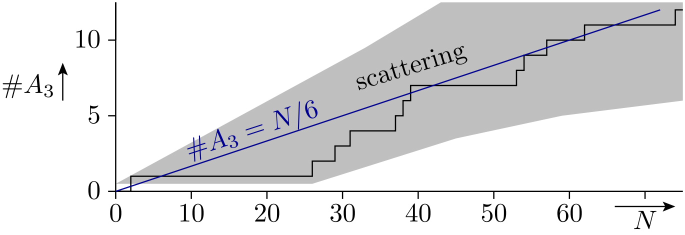
$$\zeta = \left.\frac{\#MF}{\#DS}\right|_{\mathrm{ACR}} \tag{1.4}$$

$$MC = \left.\frac{\#DM}{\#MF}\right|_{\mathrm{ACR}} \tag{1.17}$$

MC	**m**alfunction **c**overage, percentage of detected malfunctions.
ζ	malfunction rate during operation.
$\#MF$	number of **m**al**f**unctions.
$\#SR$	number of **s**ervice **r**equests.
$\#DM$	number of **d**etected **M**Fs.
ACR	**a**ppropriate **c**ounting **r**anges.

Example »rolling a 3 in a dice game«

- Possible results: 1, 2, ..., 6, favourable result: 3
- Number of trials: N



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

Probability is the best prediction for the expected relative frequency.

$\mathbb{P}(A)$ probability of event A.

Chained events

Chained events

Description of a random experiment by sub-experiments with linked results. In the following, dice are rolled twice for each experiment (events A and B, value range $\{1, 2, \dots, 6\}$ respectively). From this, the two-valued events C and D are formed with comparison operators and these are ANDed once and ORed once and counted.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	…	20	…	40
A	6	1	5	4	1	1	2	2	4	6	4	3	1		6		5
B	6	5	6	2	1	3	3	6	4	5	1	3	1		4		3
$C = (A > 3)$	1	0	1	1	0	0	0	0	1	1	1	0	0		1		1
$D = (B < 3)$	0	0	0	1	1	0	0	0	0	0	1	0	1		0		0
$E = (C \wedge D)$	0	0	0	1	0	0	0	0	0	0	1	0	0		0		0
$F = (C \vee D)$	1	0	1	1	1	0	0	0	1	1	1	0	1		1		1
$\#C$	1	1	2	3	3	3	3	3	4	5	6	6	6		11		21
$\#D$	0	0	0	1	2	2	2	2	2	2	3	3	4		6		9
$\#E$	0	0	0	1	1	1	1	1	1	1	2	2	2		5		6
$\#F$	1	1	2	3	4	4	4	4	5	6	7	7	8		13		24

event	relative frequency	probability
$C = (A > 3)$	$21/40 = 53\%$	$3/6 = 50\%$
$D = (B < 3)$	$9/40 = 23\%$	$2/6 = 33\%$
$E = (C \wedge D)$	$6/40 = 15\%$	$6/36 = 17\%$
$F = (C \vee D)$	$24/40 = 60\%$	$24/36 = 67\%$

The probability as limits for $N \to \infty$ results for each experiment from the ratio of the favourable to the number of possible outcomes. The throwing experiments have 6 possible outcomes. Of these, 3 and 2 are favourable for events C and D respectively. The chained events E and F have $6^2 = 36$ possible outcomes, of which 6 and 24 respectively are favourable.

A relative frequency with less than 100 repetitions of the random experiment still deviates considerably from the probability of occurrence on average.

We will deal later with the required number of counting trials in relation to the required estimation accuracy (see sec. 3.2.7 *Range estimation count values*).

Additional conditions

In a conditional probability, only the trials and events that fulfil the condition are counted*. Let's take the example of ORing mutually exclusive events:

$$E = C \vee D \text{ on condition } C \wedge D = 0.$$

																					$\sum$	$\sum$
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	16
C	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	0	1	1	11	7
D	0	0	0	1	1	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	6	2
$C \vee D$	1	0	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1	0	1	1	13	9

▨ events not counted or total without these events

Both the number of counted attempts and the favourable results are reduced by the four results with $C \wedge D = 1$ not to be counted.

Additional conditions can have a great influence on the possible outcomes of a random experiment and their probability of occurrence.

---

* Whether the events that are not to be counted can occur is unimportant for this purpose.

Conditional probability

Conditional probability that A occurs under condition B:

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(A \wedge B)}{\mathbb{P}(B)} \tag{2}$$

Conditional probability that B occurs under condition A:

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A \wedge B)}{\mathbb{P}(A)}$$

Bayes theorem:

$$\mathbb{P}(B|A) = \mathbb{P}(A|B) \cdot \frac{\mathbb{P}(B)}{\mathbb{P}(A)} \tag{3}$$

$A,\ B$ events.

Example 2.1: misclassification corona test

- Random variable A Person infected: $\mathbb{P}(A) = 10^{-4}$
- Random variable B Test positive: $\mathbb{P}(B) = 10^{-2}$
- Probability test positive if person infected: $\mathbb{P}(B|A) = 99\%$

What is the probability of a person being infected if test positive?

$\mathbb{P}(A) = 10^{-4}$, $\mathbb{P}(B) = 10^{-2}$, $\mathbb{P}(B|A) = 99\%$, $\mathbb{P}(B|A)$?

Bayes theorem:

$$\mathbb{P}(B|A) = \mathbb{P}(A|B) \cdot \tfrac{\mathbb{P}(B)}{\mathbb{P}(A)} \tag{2.3}$$

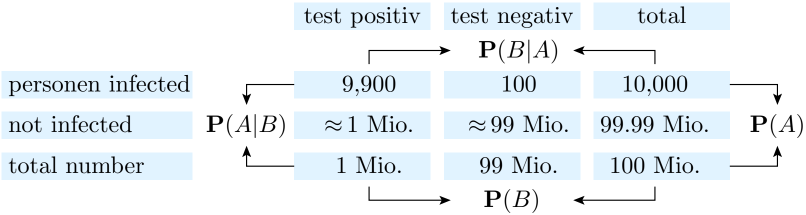
Probability $\mathbb{P}(A|B)$ that a person is infected if the test is positive::

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

If the test is triggered, it is a false alarm in 99% of cases.

$\mathbb{P}(A) = 10^{-4}$, $\mathbb{P}(B) = 10^{-2}$, $\mathbb{P}(B|A) = 99\%$, $\mathbb{P}(B|A)$?

Check with sample values:



	test positiv	test negativ	total
personen infected	9,900	100	10,000
not infected	≈ 1 Mio.	≈ 99 Mio.	99.99 Mio.
total number	1 Mio.	99 Mio.	100 Mio.

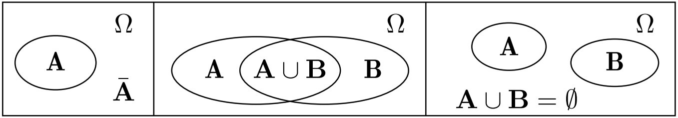
person infected: $\mathbb{P}(A) = \frac{10.000}{1\,\text{Mio.}} \approx 10^{-4}$

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

test positiv if person infected: $\mathbb{P}(B|A) = \frac{9.900}{10.000} = 99\%$

person infected, if test positiv: $\boxed{\mathbb{P}(A|B) = \frac{9.900}{1\,\text{Mio.}} \approx 1\% \surd}$

NOT / UND / ODER of events



NOT (non-occurrence probability):

$$\mathbb{P}\left(\bar{A}\right) = 1 - \mathbb{P}\left(A\right) \tag{4}$$

A – event, in the picture element of the set $\mathbf{A}$.

AND (simultaneous occurrence of events A and B):

- stochastic independence:

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

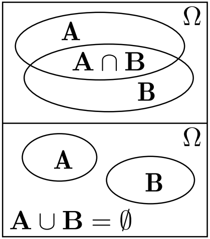
$$\mathbb{P}\left(A \wedge B\right) = \mathbb{P}\left(A\right) \cdot \mathbb{P}\left(B\right) \tag{5}$$

- mutually exclusive events:

$$\mathbb{P}\left(A \wedge B\right) = 0 \tag{6}$$

ODER (alternative occurrence of A and B):

$$\mathbb{P}\left(A \vee B\right) = \mathbb{P}\left(A\right) + \mathbb{P}\left(B\right) - \mathbb{P}\left(A \wedge B\right)$$



- stochastic independence:

$$\begin{aligned}\mathbb{P}\left(A \wedge B\right) &= \mathbb{P}\left(A\right) \cdot \mathbb{P}\left(B\right) \\ \mathbb{P}\left(A \vee B\right) &= \mathbb{P}\left(A\right) + \mathbb{P}\left(B\right) - \mathbb{P}\left(A\right) \cdot \mathbb{P}\left(B\right) \qquad (7)\end{aligned}$$

- mutually exclusive events:

$$\begin{aligned}\mathbb{P}\left(A \wedge B\right) &= 0 \\ \mathbb{P}\left(A \vee B\right) &= \mathbb{P}\left(A\right) + \mathbb{P}\left(B\right) \qquad (8)\end{aligned}$$

There is no simple solution for dependent, non-exclusive events. Workaround: Conversion into AND and OR terms of independent or mutually exclusive events, e.g.:

$$A \oplus B = \underbrace{\underbrace{\left(A \wedge \bar{B}\right)}_{\text{independent}} \vee \underbrace{\left(\bar{A} \wedge B\right)}_{\text{independent}}}_{\text{mutually exclusive}}$$

$$\mathbb{P}\left(A \oplus B\right) = \mathbb{P}\left(A\right) \cdot \left(1 - \mathbb{P}\left(B\right)\right) + \left(1 - \mathbb{P}\left(A\right)\right) \cdot \mathbb{P}\left(B\right)$$

Example 2.2: independently detectable faults

A system has three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

a) What is the probability of all faults being detected?
b) What is the probability of no fault being detected?
c) What is the probability of at least one fault detected?
d) What is the probability of proving exactly two faults?

Note:

- Definition of events F_i for fault i detectable.
- Definition of events A, B, C and D for the positive events per exercise part and describing them by logical equations.
- Transformation into AND of independent and OR of mutually exclusive events. Use eq. (2.4), (2.5) and (2.8).

A system has three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

a) What is the probability of all faults being detected?

All faults are proven if the first and second and third faults are proven. AND of independent events:

$$\begin{aligned} A &= F_1 \wedge F_2 \wedge F_3 \\ \mathbb{P}(A) &= \mathbb{P}(F_1) \cdot \mathbb{P}(F_2) \cdot \mathbb{P}(F_3) \\ &= p_1 \cdot p_2 \cdot p_3 = 10\% \cdot 5\% \cdot 20\% = 0.1\% \end{aligned}$$

F_i	Fehler i nachweisbar.
A	alle Fehler nachweisbar.

A system has three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

b) What is the probability of no fault being detected?

c) What is the probability of at least one fault detected?

b) No fault is proved if not the first or the second or the third fault is proved. Conversion according to de Morgan's rule into AND of independent events:

$$\begin{aligned} B &= \overline{F_1 \vee F_2 \vee F_3} = \bar{F}_1 \wedge \bar{F}_2 \wedge \bar{F}_3 \\ \mathbb{P}(B) &= (1 - \mathbb{P}(F_1)) \cdot (1 - \mathbb{P}(F_2)) \cdot (1 - \mathbb{P}(F_3)) \\ &= (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) = 90\% \cdot 95\% \cdot 80\% = 68.4\% \end{aligned}$$

c) At least one fault is proven if not no fault is provable:

$$\begin{aligned} C &= \bar{B} \\ \mathbb{P}(C) &= 1 - \mathbb{P}(B) = 1 - 68{,}4\% = 31.6\% \end{aligned}$$

A system has three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

d) What is the probability of proving exactly two faults?

Exactly 2 faults are proven if

- the first two, but not third,
- the second two, but not the first, or
- the first and the third, but not the second

are proved. All AND-linked events are independent and the OR-linked terms are mutually exclusive:

$$\begin{aligned} D &= \left(F_1 \wedge F_2 \wedge \bar{F}_3\right) \vee \left(\bar{F}_1 \wedge F_2 \wedge F_3\right) \vee \left(F_1 \wedge \bar{F}_2 \wedge F_3\right) \\ \mathbb{P}(D) &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\ &= 10\% \cdot 5\% \cdot 80\% + 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% = 3.2\% \end{aligned}$$

F_i	Fehler i nachweisbar.
D	genau zwei Fehler nachweisbar.

Example 2.3: dependent fault detection

The detection probability for fault 1 is $p_1 = 10\%$ regardless of the detection of fault 2. The detection probability for fault 2, if fault 1 is detected, is $p_2 = 20\%$ and 0 otherwise, i.e. the detection of fault 2 implies the detection of fault 1.

$p_1 = 10\%$, $p_2 = 20\%$, if fault 1 is detected and 0 otherwise.

What are the probabilities that 0, 1 or 2 faults are detectable?

Note: Define events F_i for fault i is detectable and events E_i for i fault are detectable.

$p_1 = 10\%$, $p_2 = 20\%$, if fault 1 is detected and 0 otherwise.

What are the probabilities that 0, 1 or 2 faults are detectable?

- No fault is detectable if fault 1 is not detectable. Detection of fault 2 and not fault 1 impossible:

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

- One fault is detectable if the first fault is detectable and the second is not:

$$\begin{aligned} E_1 &= F_1 \wedge \bar{F}_2 \\ \mathbb{P}(E_1) &= p_1 \cdot (1 - p_2) = 10\% \cdot 80\% = 8\% \end{aligned}$$

F_i	fault i is detectable.
E_i	i faults are detectable.
$\mathbb{P}(E_i)$	probability of event E_i.

$p_1 = 10\%$, $p_2 = 20\%$, if fault 1 is detected and 0 otherwise.

What are the probabilities that 0, 1 or 2 faults are detectable?

- Two faults are detectable if both faults are detectable:

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

- Check: The sum of the probabilities of the three possible outcomes must be 1:

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

F_i	fault i is detectable.
E_i	i faults are detectable.
$\mathbb{P}(E_i)$	probability of event E_i.

Fault tree analysis

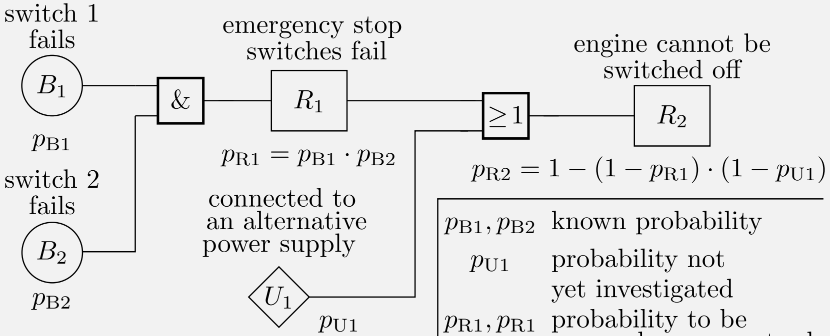
Fault tree analysis (FTA)

Graphical representation for event dependencies to estimate the probability of occurrence of hazardous situations, failures, malfunctions, ... Symbols for event types

○ B_i	basic event with known or otherwise estimable probability of occurrence
◇ U_i	undeveloped event about which insufficient information is available (unknown probability)
⌂ H_i	house event in normal operation that can cause problems in combination with others
□ R_i	resulting event whose probability of occurrence follows from that of ○, ◇ and ⌂

Contrary to the classical fault tree representation, we use the circuit symbols from digital technology for the representation of the logical AND, OR and NOT linkages of events.

Example 2.4: engine cannot be switched off

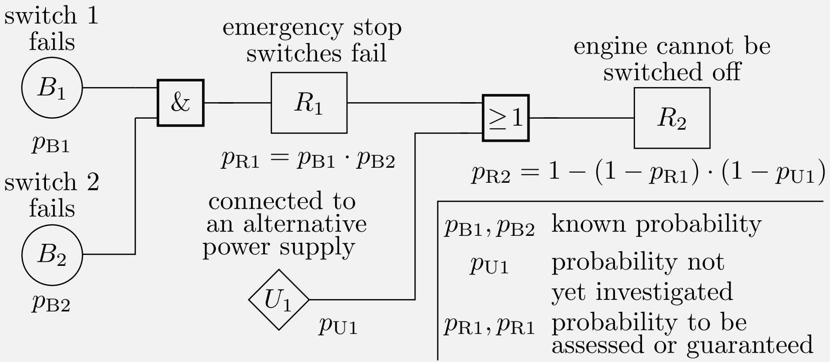


$p_{\mathrm{R1}} = p_{\mathrm{B1}} \cdot p_{\mathrm{B2}}$

$p_{\mathrm{R2}} = 1 - (1 - p_{\mathrm{R1}}) \cdot (1 - p_{\mathrm{U1}})$

$p_{\mathrm{B1}}, p_{\mathrm{B2}}$	known probability
p_{U1}	probability not yet investigated
$p_{\mathrm{R1}}, p_{\mathrm{R1}}$	probability to be assessed or guaranteed

Is $p_{\mathrm{R2}} \leq 10^{-6}$ achievable with $p_{\mathrm{B1}} = p_{\mathrm{B2}} = 10^{-3}$?



$p_{\mathrm{B1}}, p_{\mathrm{B2}}$	known probability
p_{U1}	probability not yet investigated
$p_{\mathrm{R1}}, p_{\mathrm{R1}}$	probability to be assessed or guaranteed

Is $p_{\mathrm{R2}} \leq 10^{-6}$ achievable with $p_{\mathrm{B1}} = p_{\mathrm{B2}} = 10^{-3}$?

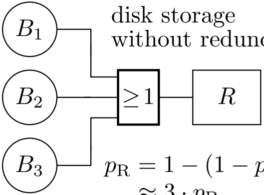
$$p_{\mathrm{R1}} = p_{\mathrm{B1}} \cdot p_{\mathrm{B2}} = 10^{-6}$$

$$p_{\mathrm{R2}} = 1 - (1 - p_{\mathrm{R1}}) \cdot (1 - p_{\mathrm{U1}}) \geq 10^{-6}$$

There is only the solution with $p_{\mathrm{U1}} = 0$. Can the risk of an alternative power supply be excluded or does the overall solution have to be improved?

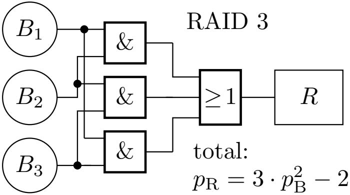
Data safety improvement through a RAID

A redundancy-free storage system consisting of three hard disks loses data if one of the three hard disks fails, a RAID 3 only if two disks fail at the same time.



disk storage without redundancy

$$p_R = 1 - (1 - p_B)^3 \approx 3 \cdot p_B$$



RAID 3

total:

$$p_R = 3 \cdot p_B^2 - 2 \cdot p_B^3$$

B_i	failure disc i
R	data loss
p_B	probability of failure per time step for a single disc
p_R	probability of data loss per time step entire system

B_3	B_2	B_1	R	
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$p_B^2 \cdot (1 - p_B)$
1	0	0	0	
1	0	1	1	$p_B^2 \cdot (1 - p_B)$
1	1	0	1	$p_B^2 \cdot (1 - p_B)$
1	1	1	1	p_B^3

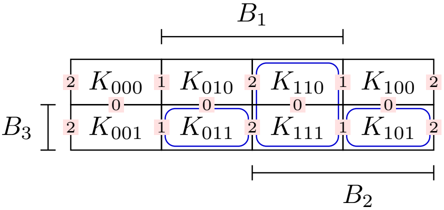
Reconvergent fan-outs

When the condition flow branches and meets again, partly dependent events are linked. In the example

$$R = B_1B_2 \vee B_2B_3 \vee B_1B_3$$

the OR-linked AND terms each have a common event variable. Unsuitable for probability estimation.

Transformation into terms of mutually exclusive events:



$$\begin{aligned} R &= B_1B_2 \vee \bar{B}_1B_2B_3 \vee B_1\bar{B}_2B_3 \\ p_{\mathrm{R}} &= p_{\mathrm{B}}^2 + p_{\mathrm{B}}^2 \cdot (1-p_{\mathrm{B}}) + p_{\mathrm{B}}^2 \cdot (1-p_{\mathrm{B}}) = 3 \cdot p_{\mathrm{B}}^2 - 2 \cdot p_{\mathrm{B}}^3 \end{aligned}$$

Generalisation to n hard disks

The probability that at least one of n discs fails is about

$$p_{\mathrm{F1oo}n} = n \cdot p_{\mathrm{B}}$$

The probability that at least two hard disks out of n fail is one minus the probabilities that zero or one disk fail:

$$p_{\mathrm{F2oo}n} = \underbrace{1 - \underbrace{\left(\underbrace{(1-p_{\mathrm{B}})^{n}}_{\text{no disc fails}} + \underbrace{n \cdot p_{\mathrm{B}} \cdot (1-p_{\mathrm{B}})^{n-1}}_{\text{one disc fails}} \right)}_{\text{no or one discs fails}}}_{\text{at least two discs fails at the same time}}$$

---

p_{B} probability that at least one disc fails.

$p_{i\mathrm{oo}n}$ probability that i out of n discs fail simultaniously.

History of fault tree analysis

- Introduction 1960: Final safety assessment of LGM-30 Minuteman intercontinental ballistic missiles.
- Subsequent years: Also for safety assessment of commercial aircraft.
- From the 70s: Safety assessment of nuclear power plants.
- Later also automotive industry and its suppliers.

When used for safety assessment

- the safety-relevant events
- the basic events and
- their probabilities

must be estimated in advance by other means: Pre-experiments, expert interviews, cause-effect (Ishikawa) diagrams, ...

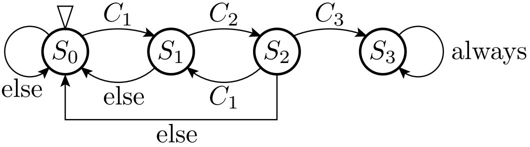
Estimation uncertainties, unconsidered hazard, dependencies, ...
Not very confidence-inspiring for nuclear missiles.

Markov chains

Markov chains (MC)

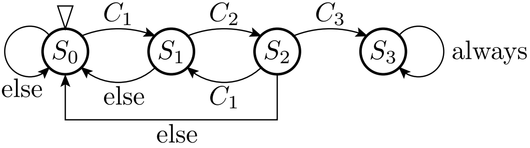
A Markov* chain (MC) is a stochastic model for sequences of possible events in which the probability of each event depends only on the state attained in the previous event.

State machine for fault detection with input sequence $C_1C_2C_3$:

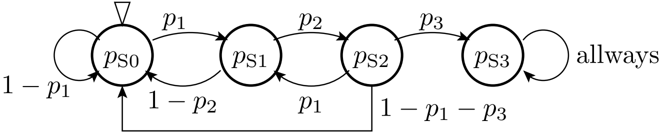


Start in state S_0 »no correct input« and remain in state S_3 »fault detected«.

S_i	state i correct inputs.
C_i	transition condition, here i-th correct input.
*	Andrej Andreevič Markov, Russian mathematician, 1856-1922.



In a Markov chain the transition conditions are replaced by the transition probabilities p_1 to p_3 and the states by state probabilities $p_{\mathrm{S.i}}$.

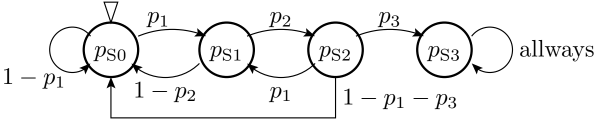


At the beginning, the initial state S_0 has probability $p_{\mathrm{S0}}=1$ and the other states have probability $p_{\mathrm{S.i}}\big|_{i\neq 0}=0$.

---

p_{Si}	probability that the FSM is in state i.
p_i	transition probability from state $i-1$ to state i.

Simulation of Markov chains



A Markov chain describes a linear system of equations for calculating the state probabilities for the next step:

$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & 0 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_{n-1}$$

with $\begin{pmatrix} p_{S0} & p_{S1} & p_{S2} & p_{S3} \end{pmatrix}_0^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$.

Control criteria for equation system and simulation result:

- Sum of probabilities per matrix column must be one.
- Sum of all $p_{S.i}$ in each step must be one.

$(\ldots)^T$ transposed matrix (exchange of rows and columns).

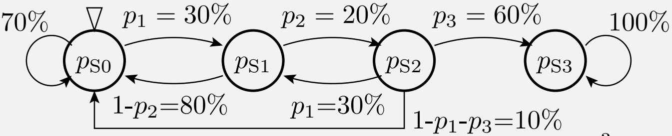
$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & 0 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_{n-1}$$

Simulation with Octave or Matlab:

```
p1 = ...;  p2 = ...;  p3 = ...;
M=[1-p1  1-p2  1-p1-p3  0;
    p1    0       0     0;
     0    p2      p1    0;
     0    0       p3    1];
Z=[1;  0;  0;  0];
for idx=1:100
 Z = M * Z;
  printf('%3i␣%6.2f%%␣%6.2f%%␣%6.2f%%␣%6.2f%%\n',idx,100*Z);
end;
```

Example 2.5: Simulation of the Markov chain

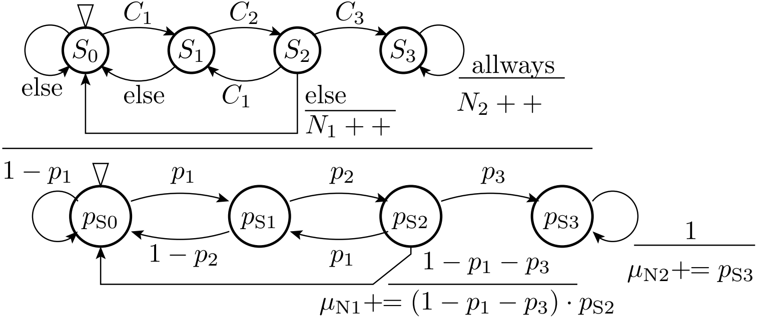
Transition probabilities: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$



step	p_{S0}	p_{S1}	p_{S2}	p_{S3}	$\sum_{i=0}^{3} p_{Si}$
0	100.00%	0	0	0	100%
1	70.00%	30.00%	0	0	100%
2	73.00%	21.00%	6.00%	0	100%
3	68.50%	21.90%	6.00%	3.60%	100%
4	66.07%	20.55%	6.18%	7.20%	100%
…	…	…	…	…	…
10	51.52%	16.11%	4.88%	27.49%	100%
…	…	…	…	…	…
50	9.89%	3.09%	0.94%	86.08%	100%
…	…	…	…	…	…
100	1.26%	0.39%	0.12%	98.23%	100%

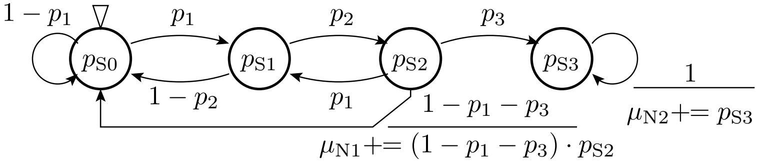
Edge counters

With counters on the edges, the number or the expected number of edge transitions can be determined:



n	number of steps.
N_1	Counter, how often two correct entries are followed by a wrong one.
N_2	Counter for the number of steps after fault detection.
$\mu_{\mathrm{N}i}$	expected value of N_i.
$n-\mu_{\mathrm{N}2}$	expected number of steps until fault detection.

The summation variables for the transition probabilities at the edges calculate the expected edge counts.



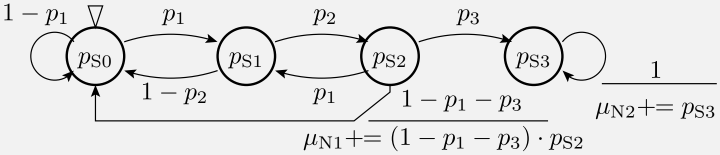
Extension of the simulation programme:

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

for idx=1:100
 Z = M * Z;
 N1 = N1+Z(3)*(1-p1-p3);
 N2 = N2+Z(4);
  printf('%3i␣%6.2f%%␣%6.2f%%␣%6.2f%%␣%6.2f%%',idx,100*Z);
  printf('%6.2f␣%6.2f\n', N1, N2);
end;
```

Example 2.6: MC simulation with edge counters

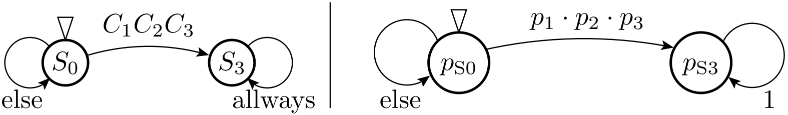
Transition probabilities: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



step	p_{S0}	p_{S1}	p_{S2}	p_{S3}	μ_{N1}	μ_{N2}
1	70.00%	30.00%	0	0	0	0
2	73.00%	21.00%	6.00%	0	0.01	0
3	68.50%	21.90%	6.00%	3.60%	0.01	0.04
4	66.07%	20.55%	6.18%	7.20%	0.02	0.11
…	…	…	…	…	…	…
10	51.52%	16.11%	4.88%	27.49%	0.05	1.27
…	…	…	…	…	…	…
50	9.89%	3.09%	0.94%	86.08%	0.14	27.36
…	…	…	…	…	…	…
100	1.26%	0.39%	0.12%	98.23%	0.16	74.48

Expected number of steps until detection: $n - \mu_{N2} \approx 25$

»Three correct input values« as a single event



Equation system of the modified Markov chain:

$$\begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_1\cdot p_2\cdot p_3 & 0 \\ p_1\cdot p_2\cdot p_3 & 1 \end{pmatrix}\cdot\begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_{n} \text{ mit } \begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

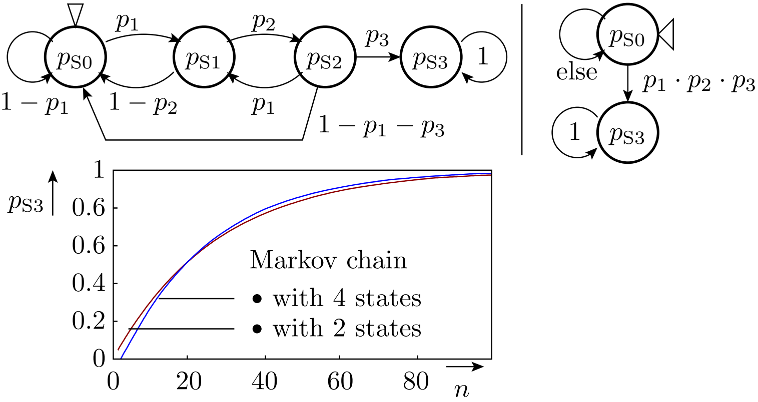
$$\begin{aligned} p_{S0}(n) &= (1-p_1\cdot p_2\cdot p_3)\cdot p_{Z0}(n-1) = (1-p_1\cdot p_2\cdot p_3)^n \\ &= \mathrm{e}^{\ln(1-p_1\cdot p_2\cdot p_3)\cdot n} \approx \mathrm{e}^{-p_1\cdot p_2\cdot p_3\cdot n} \quad \text{für } p_1\cdot p_2\cdot p_3 \ll 1^* \\ p_{S3}(n) &= 1-p_{Z0}(n) = 1-(1-p_1\cdot p_2\cdot p_3)^n \\ &\approx 1-\mathrm{e}^{-p_1\cdot p_2\cdot p_3\cdot n} \quad \text{für } p_1\cdot p_2\cdot p_3 \ll 1^* \end{aligned}$$

---

* Approximation by the first of the Taylor series elements:

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

Difference between both Markov chains

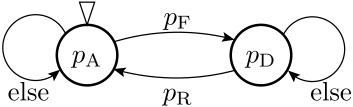


Apparently not identical behaviour:

- In the left MK missing edge $S_1 \overset{C_1}{\to} S_1$.
- MK right ignores dependencies $C_iC_jC_k,\ C_jC_kC_l, \ldots$, ...

Estimation of an availability

Let a system be functional at the beginning (state G), fail at each time step when it is intact with probability p_A (transition to state F) and be repaired when it is broken with probability p_R (transition to state G):



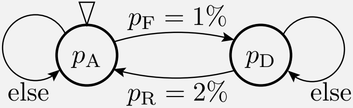
Modelling as a simulatable system of equations:

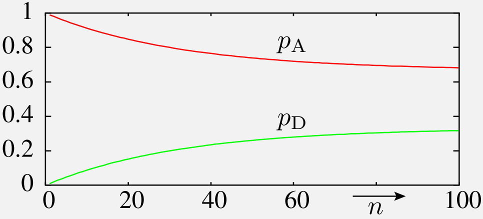
$$\begin{pmatrix} p_\mathrm{A} \\ p_\mathrm{D} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_\mathrm{F} & p_\mathrm{R} \\ p_\mathrm{F} & 1-p_\mathrm{R} \end{pmatrix} \cdot \begin{pmatrix} p_\mathrm{A} \\ p_\mathrm{D} \end{pmatrix}_{n} \text{ with } \begin{pmatrix} p_\mathrm{A} \\ p_\mathrm{D} \end{pmatrix}_{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

---

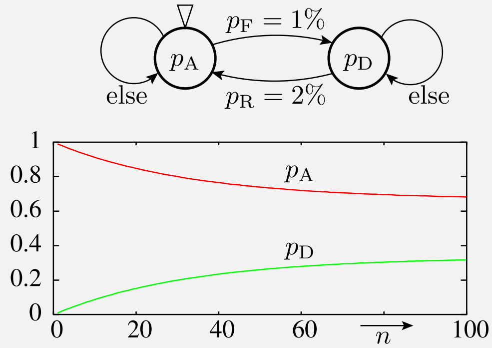
n	number of time steps.
p_A	probability that the system is **a**vailable.
p_D	probability that the system is **d**efect.
p_F	Probability that the system will **f**ail in the time step.
p_R	probability that the system will be **r**epaired in the time step.

Example 2.7: Availability in a repair process





p_A	probability that the system is **a**vailable.
p_D	probability that the system is **d**efect.
p_F	Probability that the system will **f**ail in the time step.
p_R	probability that the system will be **r**epaired in the time step.

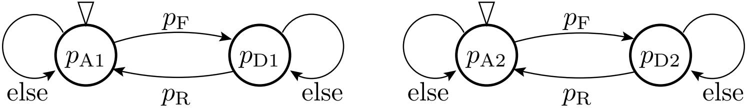


For large numbers of n, the repair process tends towards the steady state:

$$p_{\mathrm{A}} = \frac{p_{\mathrm{R}}}{p_{\mathrm{R}} + p_{\mathrm{F}}};\ p_{\mathrm{D}} = \frac{p_{\mathrm{F}}}{p_{\mathrm{R}} + p_{\mathrm{F}}}$$

Repair process for a 1oo2 system

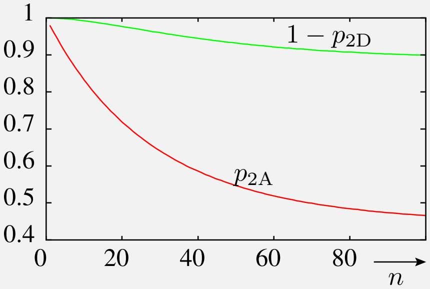
A 1oo2 (1 out of 2) System consisting of two identical subsystems functions as long as one subsystem functions:



```
pF=0.01; pR=0.02;
M=[1-pF  pR; pF  1-pR];
S=[1; 0];
for n=1:100
  S = M * S;
  p2A(n)=S(1)**2; % both systems available
  p2D(n)=S(2)**2; % both systems defect
end;
plot(1:100, p2A, 1:100, 1-p2D)
```

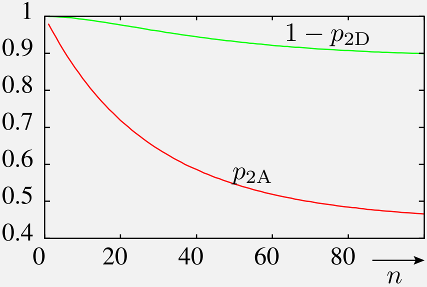
Example 2.8: Availabilty with 1oo2 redundancy

Transition probabilities: $p_\mathrm{F} = 1\%$ and $p_\mathrm{R} = 2\%$:



n	number of time steps.
p_F	Probability that the system will **f**ail in the time step.
p_R	probability that the system will be **r**epaired in the time step.
$1 - p_{2\mathrm{D}}$	probability that at least one system is available.
$p_{2\mathrm{A}}$	probability that both systems are available.

Transition probabilities: $p_{\mathrm{F}} = 1\%$ and $p_{\mathrm{R}} = 2\%$:



		stationär $(n \to \infty)$
beide Systeme verfügbar	$p_{2\mathrm{D}} = p_{\mathrm{D}}^2$	$\left(\frac{1}{3}\right)^2$
kein System verfügbar	$p_{2\mathrm{A}} = p_{\mathrm{A}}^2$	$\left(\frac{4}{3}\right)^2$
mindestens ein System verfügbar	$1 - p_{2\mathrm{D}}$	$1 - \frac{1}{9}$

Summary

Probability of chained events

Conditional probability:

$$\mathbb{P}\left(A|B\right)=\frac{\mathbb{P}(A\wedge B)}{\mathbb{P}(B)} \tag{2.2}$$

Bayes theorem:

$$\mathbb{P}\left(B|A\right)=\mathbb{P}\left(A|B\right)\cdot\frac{\mathbb{P}(B)}{\mathbb{P}(A)} \tag{2.3}$$

Counter probability:

$$\mathbb{P}\left(\bar{A}\right)=1-\mathbb{P}\left(A\right) \tag{2.4}$$

AND independent events:

$$\mathbb{P}\left(A\wedge B\right)=\mathbb{P}\left(A\right)\cdot\mathbb{P}\left(B\right) \tag{2.5}$$

AND mutually exclusive events:

$$\mathbb{P}\left(A\wedge B\right)=0 \tag{2.6}$$

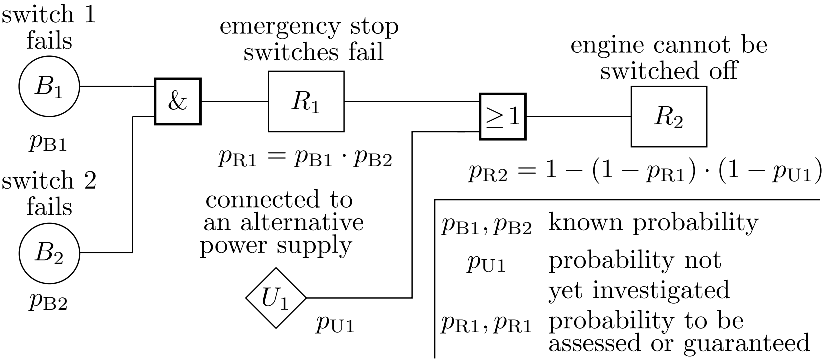
OR independent events:

$$\mathbb{P}\left(A\vee B\right)=\mathbb{P}\left(A\right)+\mathbb{P}\left(B\right)-\mathbb{P}\left(A\right)\cdot\mathbb{P}\left(B\right) \tag{2.7}$$

OR mutually exclusive events:

$$\mathbb{P}\left(A\vee B\right)=\mathbb{P}\left(A\right)+\mathbb{P}\left(B\right) \tag{2.8}$$

Fault tree analysis



switch 1 fails

B_1

p_{B1}

switch 2 fails

B_2

p_{B2}

&

emergency stop switches fail

R_1

$p_{\mathrm{R1}} = p_{\mathrm{B1}} \cdot p_{\mathrm{B2}}$

connected to an alternative power supply

U_1

p_{U1}

≥ 1

engine cannot be switched off

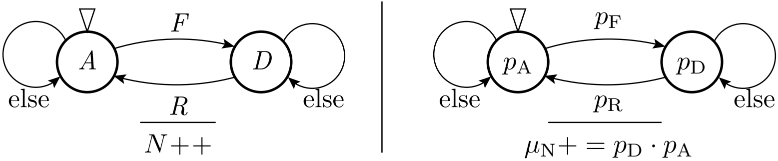
R_2

$p_{\mathrm{R2}} = 1 - (1 - p_{\mathrm{R1}}) \cdot (1 - p_{\mathrm{U1}})$

$p_{\mathrm{B1}}, p_{\mathrm{B2}}$	known probability
p_{U1}	probability not yet investigated
$p_{\mathrm{R1}}, p_{\mathrm{R1}}$	probability to be assessed or guaranteed

- Graphical representation of chained events.
- Allowed event linkages: NOT, AND and OR of independent or mutually exclusive events.

Markov chains



$$\begin{pmatrix} p_{\mathrm{A}} \\ p_{\mathrm{D}} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_{\mathrm{F}} & p_{\mathrm{R}} \\ p_{\mathrm{F}} & 1-p_{\mathrm{R}} \end{pmatrix} \cdot \begin{pmatrix} p_{\mathrm{A}} \\ p_{\mathrm{D}} \end{pmatrix}_{n} \text{ with } \begin{pmatrix} p_{\mathrm{A}} \\ p_{\mathrm{D}} \end{pmatrix}_{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mu_{\mathrm{N}} = \mu_{\mathrm{N}} + p_{\mathrm{D}} \cdot p_{\mathrm{A}}$$

Calculation of state probability for situations that can be described by finite state machines:

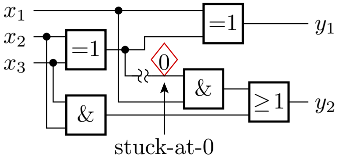
- Fault detection,
- fault creation,
- availability, ...

Edge counter for the expected number of transitions.

Fault detection

Without memory

Operation profile



▨ Input values that prove the fault

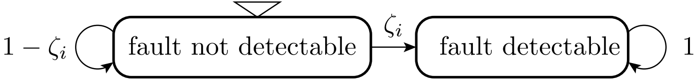
inputs x_3	 x_2	 x_1	output y_2	 y_1	Frequency of occurrence		
0	0	0	0	0	0.125	0.1	0.1
0	0	1	0	1	0.125	0.05	0.1
0	1	0	0	1	0.125	0.15	0.2
0	1	1	1	0	0.125	0.2	0.05
1	0	0	0	1	0.125	0.05	0.2
1	0	1	1	0	0.125	0.2	0.05
1	1	0	1	0	0.125	0.05	0.2
1	1	1	1	1	0.125	0.2	0.1
detection probabilityt:					0.25	0.4	0.1

The drawn sa0 fault (gate input constantly 0) is detectable with two of the eight possible input values. MF rate ζ_i is equal to the sum of the occurrence frequencies of both input values and obviously depends considerably on the frequencies of the single input values.

Operation profile

Description of the relative frequencies of occurrence of input values, function use, ... in operation or during the test.

The detection probability of a fault



A fault i is detectable if it causes at least one MF. The detection probability per service request is the fault-related MF rate ζ_i. Detection probability with n DS or tests:

$$p_i\left(\zeta_i, n\right)=1-\left(1-\zeta_i\right)^n=1-\mathrm{e}^{\ln\left(1-\zeta_i\right)\cdot n}$$

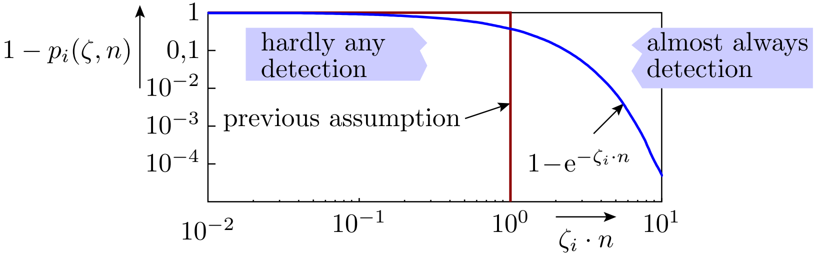
For $\zeta \ll 1$ by Tailor series $\ln\left(1-\zeta\right)=-\left(\zeta+\frac{\zeta^2}{2}+\frac{\zeta^3}{3}+\ldots\right)\approx-\zeta$:

$$p_i\left(n\right)=1-\mathrm{e}^{-\zeta_i\cdot n} \tag{9}$$

Prerequisites: $\zeta_i \leq 0.1$ and constant during the test.

$p_i\left(n\right)$	detection probability of fault i by n tests.
ζ_i	MF rate caused by fault i.
n	number of tests.
DS	delivered service.

Comparison with the assumption on slide set 1



Assumptions section 1 slide 1.128:

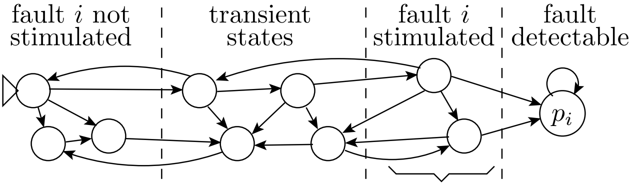
- Faults with $\zeta\cdot n\geq 1$ are detected (and removed) and
- Faults with $\zeta\cdot n<1$ are not detectable.

In fact, only

- almost always proof from $\zeta_i\cdot n>5$,
- hardly any proof until $\zeta_i\cdot n>\frac{1}{5}$ and
- $1/\zeta_i$ is the mean detection length.

With memory

Service with memory



after n_{I} initialisation steps:

- state probabilities: $\sim (1 - p_i)$
- transistion probabilities: $\approx \frac{\zeta_i}{1-p_i}$

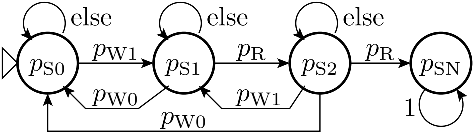
Many-state observer automaton in which typically a relative probability equilibrium is established between the states before detection after n_{I} initialisation steps. As with faults without memory, the probability inflow to the state »fault detected« is then inversely proportional to its state probability:

$$1 - \mathrm{e}^{-\zeta_i \cdot n} < p_i\left(n\right) < 1 - \mathrm{e}^{-\zeta_i \cdot (n - n_{\mathrm{I}})}$$

Example DR1 fault (destructive read of a one)

detection sequence write 1 → read read

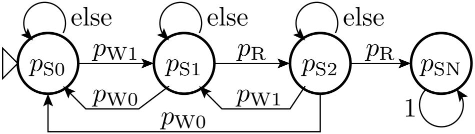
S0: value 0 or unknown
S1: value 1 written
S2: 1 destructive read
SN: fault detected



In a RAM, when the faulty memory cell with address a is read, a stored 1 is corrupted into a 0. The proof requires:

- write 1 to address a (transition to excited state S_1),
- read value from address a (transition to excited state S_2),
- read from address a without intermediate write access to a (transition to the detection state S_{N}).

$p_{\mathrm{W}\dots}$ probability that a 0 is written into the memory cell.
p_{W1} probability that a 1 is written into the memory cell.
p_{R} probability that the memory cell is read.



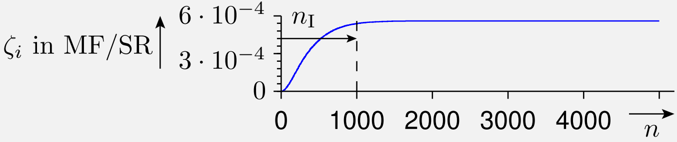
```
pS0=1; pS1=0; pS2=0; pSN(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW0 = pW1 = 1/(4*NA);
for n=1:N
  p0    = pS0 * (1-pW1) + pS1*pW0         + pS2*pW0;
  p1    = pS0 *    pW1  + pS1*(1-pW0-pR) + pS2*pW1;
  p2    = pS1 *    pR   + pS2*(1-pW1+pW0-pR);
  pSN     = pSN(n) + pS2 * pR;
  zeta   = pS2*pR / (pS0+pS1+pS2); % FF rate
  pS0 = p0; pS1 = p1; pS2 = p2;
end
plot(1:N, zeta);
```

Avoiding small differences of large numbers:

$$\zeta = \frac{p_{\mathrm{SN}}(n+1) - p_{\mathrm{SN}}(n)}{1 - p_{\mathrm{SN}}(n)} = \frac{p_{\mathrm{S2}} \cdot p_{\mathrm{R}}}{p_{\mathrm{S0}} + p_{\mathrm{S1}} + p_{\mathrm{S2}}}$$

$p_{\mathrm{W}\ldots}$	probability that a 0 or 1, respectively is written into the memory cell.
p_{R}	probability that the memory cell is read.
ζ	MF rate of the fault. Conditional probability that fault is detected if not detected previously.

Example 2.9: MF rate of the DR1 fault



The MF rate ζ caused by the fault initially increases with the number of tests n and than remains constant $\zeta \approx 5.7 \cdot 10^{-4}$ from $n_{\mathrm{I}} \gtrsim 1000$.

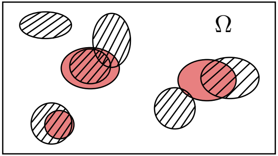
For long random tests $n \gg n_{\mathrm{I}}$, the MF rate of a fault in systems with memory can usually also be considered constant and the detection probability can be estimated as for systems without memory:

$$p_i(n) = 1 - \mathrm{e}^{-\zeta_i \cdot n} \tag{2.9}$$

$p_i(n)$	detection probability of fault i by n tests.
ζ_i	MF rate caused by fault i.
n_{I}	number of **i**nitialisation steps.
n	number of tests, for worst-case estimates without the n_{I} initialisation steps.

Actual and model faults

Actual faults and model faults

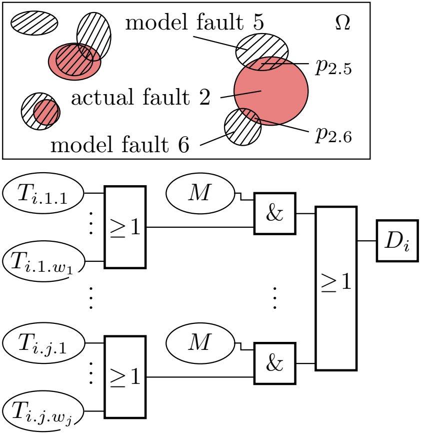


Ω	set of possible input values or sequences to proof a fault
▨	detection set of a model fault
🟥	detection set of an actual fault

- The faults to be found are unknown at the time of test selection. Therefore, fault models are used for test selection and estimation of fault coverage.
- A fault model is an algorithm that generates a large number of model faults from the test object description. Each model fault is a different small falsification.
- The detection set of a fault is the set of inputs with which the fault is detectable.

Most actual faults share detection constraints and detection sets with several model faults.

Targeted tests search



🟥 detection set of an actual fault

▨ detection set of a model fault

T_{ijk} test k for model fault j detects fault i:

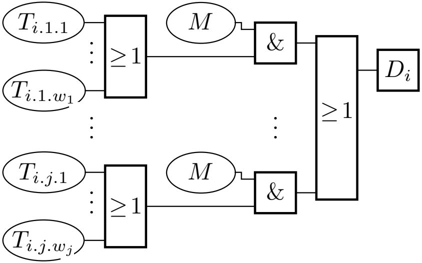
$$\mathbf{P}\left(T_{i.j.k}\right) = p_{ij} \neq f(k)$$

M for model fault j the w_j tests sought are found:

$$\mathbf{P}\left(M\right) = FC_{\mathrm{M}} \neq f(i,j)$$

D_i detection fault i

For each fault i, the model fault set contains $j = 1$ to v_i similarly detectable model faults, for each of which $k = 1$ to w_j tests are sought and found with probability $\mathbb{P}\left(M\right) = FC_{\mathrm{M}}$.



T_{ijk}	test k for model fault j detects fault i: $\mathbf{P}\left(T_{i.j.k}\right) = p_{ij} \neq f(k)$
M	for model fault j the w_j tests sought are found: $\mathbf{P}\left(M\right) = FC_{\mathrm{M}} \neq f(i,j)$
D_i	detection fault i

Tests search is difficult and only successful for FC_{M} model faults (see sec. 5.2). If one test can be found, with w_j times more effort, all w_j tests will be found:

$$D_i = \bigvee_{j=1}^{v_i}\left(\left(\bigvee_{k=1}^{w_j} T_{ijk}\right)\wedge M\right) = \overline{\bigwedge_{j=1}^{v_i}\overline{\left(\left(\overline{\bigwedge_{k=1}^{w_j}\bar{T}_{ijk}}\right)\wedge M\right)}}$$

$$p_i = \mathbb{P}\left(D_i\right) = 1 - \prod_{j=1}^{v_i}\left(1 - \left(FC_{\mathrm{M}}\cdot\left(1-\prod_{j=1}^{w_j}\left(1-p_{ij}\right)\right)\right)\right) \qquad (10)$$

$$p_i = 1 - \prod_{j=1}^{v_i}\left(1 - \left(FC_{\mathrm{M}} \cdot \left(1 - \prod_{j=1}^{w_j}(1 - p_{ij})\right)\right)\right)$$

Example 2.10: fault oriented test selection

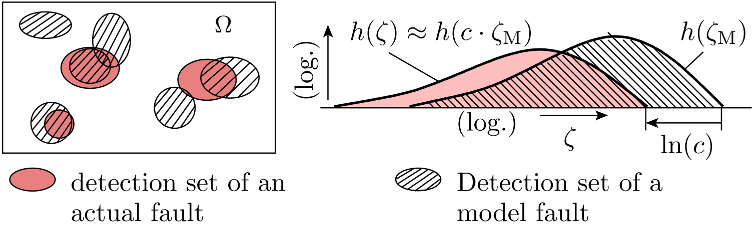
$p_{\mathrm{ij}} = 25\%$, $v_i = 5$ and all $w_j = w$

$p_i\,(w,\,FC_{\mathrm{M}})$	$w=1$	$w=2$	$w=3$	$w=4$	$w=5$
$FC_{\mathrm{M}} = 90\%$	72.0%	91.8%	97.5%	99.15%	99.70%
$FC_{\mathrm{M}} = 95\%$	74.2%	93.2%	98.1%	99.47%	99.84%

The detection probabilityp_i of actual faults depends less on the model fault coverage FC_{M}, but significantly on the number of tests w_j that are searched for each model fault j.

p_i	detection probability of fault i.
v_i	Number of similar detectable model faults for faults i.
FC_{M}	**f**ault **c**overage for model faults.
w_j	Number of tests for model faults j.
p_{ij}	**p**robability that a test to proof model fault j also proofs actual fault i.

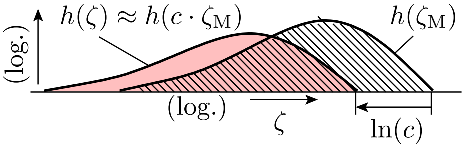
Random fault detection



- Real faults i and their similarly detectable model faults j share stimulation and observation conditions. This suggests a similar shape of the MF rate distribution with the same shape factor k.
- The ratio of the MF rates of the actual faults to their similarly detectable model faults tends towards a value

$$c \approx \frac{\zeta}{\zeta_{\mathrm{M}}}$$

which can also be smaller or larger than 1.



For the same effective reference test set length, for which all detectable faults are removed before random testing, the actual FC tends towards the model fault coverage of c times the test set length:

$$FC_{\mathrm{M}}(n) = FC(c \cdot n) \quad \text{with } c \approx \frac{\zeta}{\zeta_{\mathrm{M}}} \tag{11}$$

Random test selection places fewer demands on the fault model and allows more trustworthy estimates of FC from FC_{M}.

FC	**f**ault **c**overage, percentage of detectable faults.
FC_{M}	**f**ault **c**overage for model faults.
c	test number enlargement.
n_{T}	**n**umber of **t**ests.
ζ_{M}	Malfunction rate due to **m**odelled faults during test.
ζ	malfunction rate during operation.

Example 2.11: fault coverage random test

An increase from $n_0 = 100$ to $n = 10^4$ random tests detects $FC_{\mathrm{M}} = 90\%$ of the model faults undetectable with $n_0 = 100$ tests. The MF rate of undetectable model faults during testing is about twice that of undetectable actual faults in use.

$n_0 = 100$, $n_1 = 10^4$, $FC_{\mathrm{M}} = 90\%$, $c = \zeta/\zeta_{\mathrm{M}} = 0.5$

a) Form factor k under the assumption of a power function for the distribution of the MF rate?

b) Expected number of actual faults not detectable with the n_1 tests?

c) Expected MF rate after elimination of all detected faults?

d) How much simulation time is required to estimate the fault coverage for the effective test number n_1, if the fault simulation requires 1 s for a test step?

$n_0 = 100$, $n_1 = 10^4$, $FC_{\mathrm{M}} = 90\%$, $c = \zeta/\zeta_{\mathrm{M}} = 0.5$

a) Form factor k under the assumption of a power function for the distribution of the MF rate?

With a power function as the distribution of the MF rate, the expected number of faults decreases with the form factor as the exponent:

$$\mu_{\mathrm{FNE}}(n) = \mu_{\mathrm{FNE}}(n_0) \cdot \left(\frac{n}{n_0}\right)^{-k} \tag{1.42}$$

Model fault coverage:

$$FC_{\mathrm{M}}(n) = 1 - \frac{\mu_{\mathrm{FNE}}(n)}{\mu_{\mathrm{FNE}}(n_0)} = 1 - \left(\frac{[c\cdot]n}{[c\cdot]n_0}\right)^{-k}$$

Equation converted according to the form factor k:

$$k = \frac{\ln(1 - FC_{\mathrm{M}}(n))}{\ln\left(\frac{n}{n_0}\right)} = -\frac{\ln(0.1)}{\ln(100)} = 0.5$$

FC_{M}	**f**ault **c**overage for model faults.
μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.

$n_0 = 100$, $n_1 = 10^4$, $FC_{\mathrm{M}} = 90\%$, $c = \zeta/\zeta_{\mathrm{M}} = 0.5$

b) Expected number of actual faults not detectable with the n_1 tests?

Assuming that the distribution of MF rate for actual and model faults is a power function with the same form factor and the 100 detectable faults is the difference of the expected number of undetectable faults for test length n_0 and n_1:

$$\mu_{\mathrm{FNE}}\left(n_0\right) - \mu_{\mathrm{FNE}}\left(n_1\right) = \mu_{\mathrm{FNE}}\left(n_1\right) \cdot \left(\left(\frac{n_1}{n_0}\right)^k - 1\right) = 100$$

$$\mu_{\mathrm{FNE}}\left(n_1\right) = \frac{100}{\left(\frac{n}{n_0}\right)^k - 1} = 11.1$$

μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
n_0, n_1	number of tests with known malfunction rate or expected number of faults, respectively.
k	form factor of the distribution of the malfunction rate $(0 < k < 1)$.

$n_0 = 100$, $n_1 = 10^4$, $FC_\mathrm{M} = 90\%$, $c = \zeta/\zeta_\mathrm{M} = 0.5$

c) Expected MF rate after elimination of all detected faults?

MF rate due to the non-eliminated faults:

$$\zeta_\mathrm{F}\left(n\right) = \frac{k \cdot \mu_\mathrm{FNE}(n)}{n} \tag{1.43}$$

With the form factor from exercise part a, the expected number of faults from exercise part b and the test set length n_1:

$$\zeta_\mathrm{F} = \frac{0{,}5 \cdot 11{,}1}{10^4} = 5.56 \cdot 10^{-4} \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

FC	**f**ault **c**overage, percentage of detectable faults.
FC_M	**f**ault **c**overage for model faults.
c	test number enlargement.
n_T	**n**umber of **t**ests.

$n_0 = 100$, $n_1 = 10^4$, $FC_\mathrm{M} = 90\%$, $c = \zeta/\zeta_\mathrm{M} = 0.5$

d) How much simulation time is required to estimate the fault coverage for the effective test number n_1, if the fault simulation requires 1 s for a test step?

For the same effective reference test set length, the actual FC tends towards the model fault coverage of c times the test set length:

$$FC_\mathrm{M}(n) \approx FC(c \cdot n) \tag{2.11}$$

Number of tests to be simulated:

$$n_\mathrm{TS} = c \cdot n_1 == 5,000$$

$$t_\mathrm{Sim} = n_\mathrm{TS} \cdot 1\,\mathrm{s} = 5,000\,\mathrm{s} = 1.4\,\mathrm{h}$$

---

n_TS	number of tests to be simulated.
n_1	effective number of tests.
c	test number enlargement.
t_Sim	simulation time.

Summary

Fault detection probability random test

- Fault detection probability as a function of the number of tests n for systems without memory for $\zeta_i \leq 0{,}1$:

$$p_i\left(n\right) = 1 - \mathrm{e}^{-\zeta_i \cdot n} \tag{2.9}$$

- The MF rate ζ_i of the fault depends on the operation profile. Unless otherwise specified, let the operation profile for the test be constant and equal to the one in use.
- The relationship usually also applies to systems with memory if the number of tests is $n \gg n_{\mathrm{I}}$.

Actual fault and model fault coverages

Targeted tests search. If it is possible to find one test for a model fault, search will be mostly also successful for a total of $w_j \geq 1$ tests per fault:

$$p_i = 1 - \prod_{j=1}^{v_i} \left(1 - \left(FC_{\mathrm{M}} \cdot \left(1 - \left(1 - p_{ij}\right)^{w}\right)\right)\right) \qquad (2.10)$$

- Requires a fault model that generates $v_i \geq 1$ model faults for each fault, which detection implies detection of fault i with a high probability p_{ij}.
- FC depends more on the number of tests w_j sought per model fault than on FC_{M}.

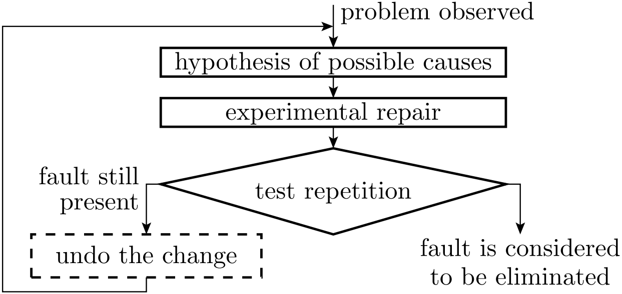
Random test: The model faults are only used to estimate the fault coverage, but not for the test selection:

$$FC_{\mathrm{M}}\left(n\right) \approx FC\left(c \cdot n\right) \qquad (2.11)$$

- Requires only a similar MF density shape for real and model fault.
- Allows much more trustworthy estimations compared to using the model faults for tests search.

Fault elimination

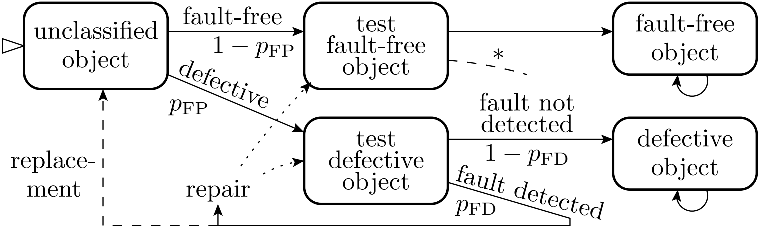
Experimental repair (see slide 1.96)



- Iteration of removal attempts for hypothetical faults and success control by test repetition.
- Removes all faults detectable by the test.
- To avoid the emergence of new faults during repair undo changes after unsuccessful repair attempts.

Presupposition: deterministic behaviour, so that the elimination result can be checked by test repetition (see sec. 1.5.2).

Fault elimination as a Markov chain



A fault i

- is present with probability p_{FP} and
- is detected with probability p_{FD}.

Two approaches are to be distinguished for fault elimination:

- replacement of the entire system and
- repair, e.g. by replacing a faulty subsystems.

---

p_{FD} **p**robability of **f**ault **d**etection.

p_{FP} **p**robability that **f**ault is **p**resent.

* additional edge for phantom defect from "test defect-free object" to repair or replacement.

Replacement or repair

When replacing detected defective systems with spare parts from the same manufacturing process

- original and spare parts have the same yield Y and
- the original part must be replaced on average μ_{R} times:

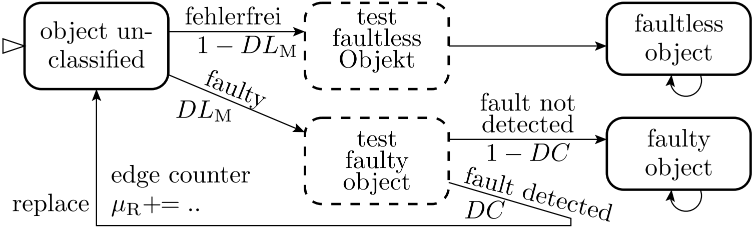
$$\mu_{\mathrm{R}} = \frac{1}{Y} - 1 \tag{12}$$

From this model-based extrapolation it can be derived that the production costs per system sold are $\approx \frac{1}{Y}$ times as high as the costs for the production of a single system. On the other hand, replacement saves the costs of design for testing and repair, localisation and stockpiling of repair capacities.

Replacement is the most cost-effective way of eliminating faults at high yields and priceless for yields $Y \ll 50\%$.

Replacement

Fault elimination by replacement



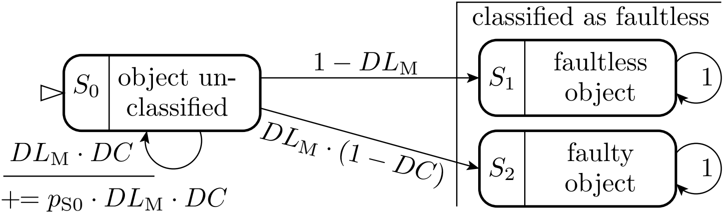
Original objects and replacements are defective with probability DL_M.

Each step turns an unclassified object with probability

- $1-DL_\mathrm{M}$ into a fault-free object or with probabilty
- $DL_\mathrm{M}\cdot(1-DC)$ ino an unrecognised defective object.
- Otherwise it remains unclassified.

DL_M	**d**efect **l**evel after **m**anufacturing.
DC	**d**efect **c**overage, percentage of detectable defective devices.
μ_R	Edge counter for the expected number of replacements.

Simplified Markov chain



classified as faultless

$1 - DL_{\mathrm{M}}$

S_0 object unclassified

S_1 faultless object

1

$DL_{\mathrm{M}} \cdot (1 - DC)$

S_2 faulty object

1

$DL_{\mathrm{M}} \cdot DC$

$\mu_{\mathbf{R}} \mathrel{+}= p_{\mathrm{S0}} \cdot DL_{\mathrm{M}} \cdot DC$

After replacing all recognisably defective objects*:

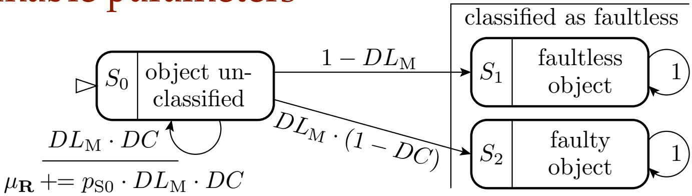
$$\begin{aligned}
\lim_{n\to\infty}(p_{\mathrm{S0}}) &= \lim_{n\to\infty}(DL_{\mathrm{M}} \cdot DC)^n = 0 \\
\lim_{n\to\infty}(p_{\mathrm{S1}}) &= (1 - DL_{\mathrm{M}}) \cdot \sum_{n=0}^{\infty}(DL_{\mathrm{M}} \cdot DC)^n = \frac{1 - DL_{\mathrm{M}}}{1 - DL_{\mathrm{M}} \cdot DC} \\
\lim_{n\to\infty}(p_{\mathrm{S2}}) &= 1 - \lim_{n\to\infty}(p_{\mathrm{S1}}) = 1 - \frac{1 - DL_{\mathrm{M}}}{1 - DL_{\mathrm{M}} \cdot DC} = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC}
\end{aligned}$$

---

summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

DC **defect coverage, per-**

Estimable parameters



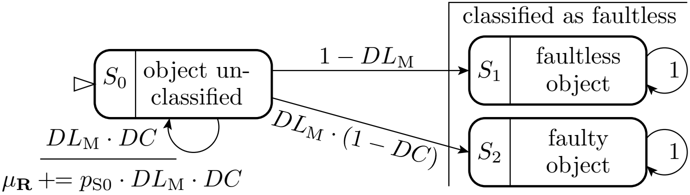
Defect level after sorting out as probability $\lim_{n\to\infty}(p_{\mathrm{S2}})$ that an object identified as defect-free is defective

$$DL_{\mathrm{R}} = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{1.68}$$

was derived on slide set 1 by subtracting the number of detected defective products from the number of defective and all products in the numerator and denominator.

DC	**d**efect **c**overage, percentage of detectable defective devices.
DL_{M}	**d**efect **l**evel after **m**anufacturing.
DL_{R}	**d**efect **l**evel after **r**eplacement of detected defective parts.

Yield, replacement, defect level



Probability that a defective object will not be replaced:

$$p_{\mathrm{NR}}=\frac{DL_{\mathrm{R}}}{DL_{\mathrm{M}}}=\frac{\frac{DL_{\mathrm{M}}\cdot(1-DC)}{1-DL_{\mathrm{M}}\cdot DC}}{DL_{\mathrm{M}}}=\frac{(1-DC)}{1-DL_{\mathrm{M}}\cdot DC}$$

Expected number of replacements per object found to be good:

$$\mu_{\mathrm{R}} \quad = \quad \sum_{n=1}^{\infty}(DL\cdot DC)^n=\frac{DL_{\mathrm{M}}\cdot DC}{1-DL_{\mathrm{M}}\cdot DC} \qquad (13)$$

The expected number of objects to be produced per object found to be good is $\mu_{\mathrm{R}}+1$ and equal to the reciprocal of the yield (see eq. 2.12):

$$Y=\frac{1}{\mu_{\mathrm{R}}+1}=\frac{1}{\frac{DL_{\mathrm{M}}\cdot DC}{1-DL_{\mathrm{M}}\cdot DC}+1}=1-DL\cdot DC\surd$$

Example 2.12: Yield, replacement, defect level

Circuit yields Y: 10%, 30%, 50%, 80% and 90%, Defect coverage DC: 90%, 99% and 99.9%.

a) What is the expected number of substitutions μ_{R}, until a circuit passes the test?

b) What is the defect level DL_{M} of the circuits after manufacturing before sorting out?

c) What is the defect level DL_{R} after sorting out the detected defective circuits

Circuit yields Y: 10%, 30%, 50%, 80% and 90%, Defect coverage DC: 90%, 99% and 99.9%.

a) What is the expected number of substitutions μ_{R}, until a circuit passes the test?

Expected number of replacements per good circuit:

$$\mu_{\mathrm{R}} = \frac{1}{Y} - 1 \tag{2.12}$$

Y	10%	30%	50%	80%	90%
$\mu_{\mathrm{R}} = \frac{1}{Y} - 1$	9	2.33	1	0.25	0,11

Circuit yields Y: 10%, 30%, 50%, 80% and 90%, Defect coverage DC: 90%, 99% and 99.9%.

b) What is the defect level DL_{M} of the circuits after manufacturing before sorting out?

Convert equation

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{1.67}$$

according to the defect level DL_{M} before replacement of detected defective parts:

$DL_{\mathrm{M}} = \frac{1-Y}{DC}$	$Y = 10\%$	...=30%	...=50%	...=80%	...=90%
90%	100.0%	77.8%	55.6%	22.2%	11.1%
99%	90.9%	70.7%	50.50%	20.2%	10.1%
$99{,}9\%$	90.1%	70.1%	50.1%	20.0%	10.0%

For $Y = 1 - DC$ all manufactured circuits are defective and $Y < 1 - DC$ is not possible according to eq. 1.67.

Circuit yields Y: 10%, 30%, 50%, 80% and 90%, Defect coverage DC: 90%, 99% and 99.9%.

c) What is the defect level DL_{R} after sorting out the detected defective circuits for the defect level before sorting out $DL = 100\%$, 90%, 70%, 50%, 20% und 10% and with the values of defect coverage DC from above?

$$DL_{\mathrm{R}} = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{1.68}$$

	$DC = 90\%$	$DC = 99\%$	$DC = 99{,}9\%$
$DL_{\mathrm{M}} = 100\%$	100%	100%	100%
$DL_{\mathrm{M}} = 90\%$	47.4%	8.26%	8920 dpm
$DL_{\mathrm{M}} = 70\%$	18.9%	2.28%	2328 dpm
$DL_{\mathrm{M}} = 50\%$	9.09%	9901 dpm	999 dpm
$DL_{\mathrm{M}} = 20\%$	2.43%	2494 dpm	250 dpm
$DL_{\mathrm{M}} = 10\%$	1.10%	1110 dpm	111 dpm

Circuit yields Y: 10%, 30%, 50%, 80% and 90%, Defect coverage DC: 90%, 99% and 99.9%.

c) What is the defect level DL_{R} after sorting out the detected defective circuits ...

	$DC = 90\%$	$DC = 99\%$	$DC = 99{,}9\%$
$DL_{\mathrm{M}} = 100\%$	100%	100%	100%
$DL_{\mathrm{M}} = 90\%$	47.4%	8.26%	8920 dpm
$DL_{\mathrm{M}} = 70\%$	18.9%	2.28%	2328 dpm
$DL_{\mathrm{M}} = 50\%$	9.09%	9901 dpm	999 dpm
$DL_{\mathrm{M}} = 20\%$	2.43%	2494 dpm	250 dpm
$DL_{\mathrm{M}} = 10\%$	1.10%	1110 dpm	111 dpm

For the defect level of tested circuits DL_{R} one finds in the literature the order of magnitude 100 ... 1000 dpm. For $Y = 30\% \ldots 80\%$, this results in defect coverages of $DC \approx 99.9\%$.

- Are the defect coverages really that high or
- are the literature data on the defect percentage too low?

These questions will continue to be with us.

Repair

Fault elimination by repair

In the case of a repair, only the parts of the overall system diagnosed as defective are replaced or modified. Subsystems to be replaced:

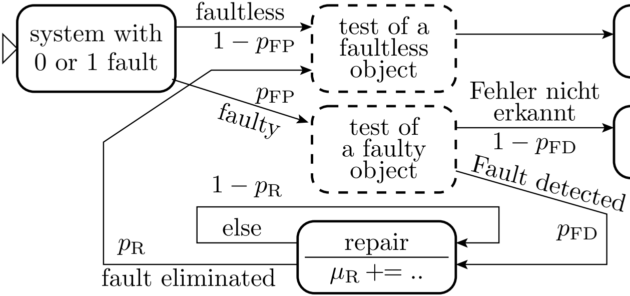
- are cheaper than complete systems that need to be replaced and
- have a smaller defect level (fewer multiple replacements).

In exchange, repair requires additional effort:

- Repair-friendly design (modular interchangeability),
- fault localisation and
- Organisational units + personnel capacity for repair (for software for maintenance).

Unprofitable for systems with yield $Y > 50$.

Elimination iteration for one fault



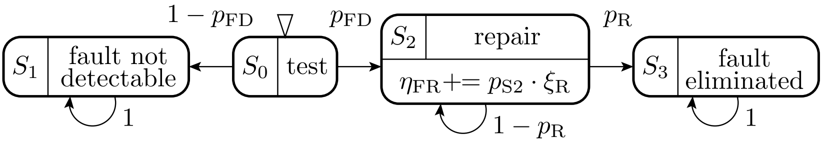
- For a detected fault, repairs are carried out until the visible faulty behaviour has been eliminated.
- With each repair attempt, with little probability, new faults are created.

---

p_{R} probability of **r**epair success.

μ_{R} expected number of **r**epair attempts per fault.

Improved Markov chain per fault



The probability of eliminating an existing fault is equal to the probability of detection*:

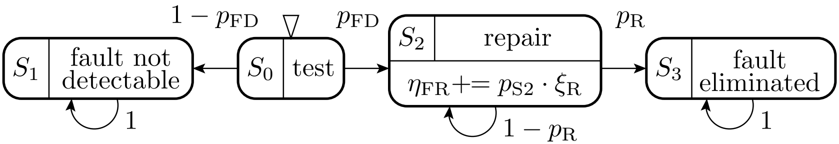
$$p_{\mathrm{FE}} = p_{\mathrm{Z3}} = p_{\mathrm{FD}} \cdot p_{\mathrm{R}} \cdot \sum_{n=0}^{\infty} (1-p_{\mathrm{R}})^n = p_{\mathrm{FD}}$$

All detectable faults are eliminated.

---

p_{FD}	**p**robability of **f**ault **d**etection.
p_{R}	probability of **r**epair success.
p_{Si}	Probability that the Markov chain is in state S_i.
p_{FE}	**p**robability of **f**ault **e**limination.
*	summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3. Fault elimination

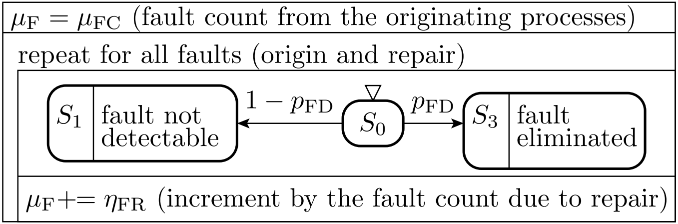


- Expected number of new emerging faults per fault present at the beginning*:

$$\eta_{\mathrm{FR}} = p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}} \cdot \sum_{n=0}^{\infty} (1-p_{\mathrm{R}})^n = \frac{p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}} \qquad (14)$$

η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
p_{FD}	**p**robability of **f**ault **d**etection.
p_{R}	**p**robability of **r**epair success.
ξ_{R}	fault emerging rate in faults per **r**epair attempt.
*	summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

Multiple faults from the creation processes



$\mu_{\mathrm{F}} = \mu_{\mathrm{FC}}$ (fault count from the originating processes)

repeat for all faults (origin and repair)

$\mu_{\mathrm{F}} \mathrel{+}= \eta_{\mathrm{FR}}$ (increment by the fault count due to repair)

- One Markov chain for each fault to be eliminated.
- Any detectable fault is eliminated: $p_{\mathrm{FE}} = p_{\mathrm{FD}}$

Total number of emerging faults for $\eta_{\mathrm{FR}} < 1$:

$$\mu_{\mathrm{FCR}} = \mu_{\mathrm{FCP}} \cdot (1 + \eta_{\mathrm{FR}} \cdot (1 + \eta_{\mathrm{FR}} \cdot (1 + \ldots))) = \mu_{\mathrm{FCP}} \cdot \sum_{i=0}^{\infty} (\eta_{\mathrm{FR}})^i$$

μ_{FCR}	expected number of **f**aults from **c**reation and repair processes.
μ_{FCP}	expected number of **f**aults from **c**reation **p**rocess.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .

3. Fault elimination

Continuation from previous slide ...

$$\mu_{\mathrm{FCR}} = \mu_{\mathrm{EF}} \cdot \sum_{i=0}^{\infty} \left(\eta_{\mathrm{FR}}\right)^{i} = \frac{\mu_{\mathrm{FCP}}}{1-\eta_{\mathrm{FR}}}$$

Expected number of faults not eliminated:

$$\mu_{\mathrm{FNE}} = \mu_{\mathrm{FCR}} \cdot \left(1 - p_{\mathrm{FD}}\right) = \frac{\left(1 - p_{\mathrm{FD}}\right) \cdot \mu_{\mathrm{FCP}}}{1-\eta_{\mathrm{FR}}} \tag{15}$$

$$= \frac{\left(1 - p_{\mathrm{FD}}\right) \cdot \mu_{\mathrm{EF}}}{1 - \frac{p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}}} = \frac{\left(1 - p_{\mathrm{FD}}\right) \cdot p_{\mathrm{R}} \cdot \mu_{\mathrm{FCP}}}{p_{\mathrm{R}} - p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}} \tag{16}$$

μ_{FCR}	expected number of **f**aults from **c**reation and repair processes.
μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
p_{FD}	**p**robability of **f**ault **d**etection.
μ_{FCP}	expected number of **f**aults from **c**reation **p**rocess.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
p_{R}	**p**robability of **r**epair success.
ξ_{R}	fault emerging rate in faults per **r**epair attempt.

$$\mu_{\mathrm{FNE}} = \frac{(1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}}{1-\eta_{\mathrm{FR}}} \tag{2.15}$$

An important measure of the quality of a repair process is the expected number of new faults per eliminated fault μ_{FR}:

1. $\mu_{\mathrm{FR}} < 0{,}1$: Desired case, μ_{FNE} increases proportionally by μ_{FR}:

$$\mu_{\mathrm{FNE}} = \frac{(1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}\cdot(1+\mu_{\mathrm{FR}})}{(1-\mu_{\mathrm{FR}})\cdot(1+\mu_{\mathrm{FR}})} = \frac{(1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}\cdot(1+\mu_{\mathrm{FR}})}{1-\mu_{\mathrm{FR}}^2}$$
$$\approx (1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}\cdot(1+\mu_{\mathrm{FR}})$$

2. $\mu_{\mathrm{FR}} = p_{\mathrm{FD}}$: Elimination of all detectable faults without reducing the expected total fault count:

$$\mu_{\mathrm{FNE}} = \frac{(1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}}{(1-\mu_{\mathrm{FR}})} = \mu_{\mathrm{FCP}}$$

3. $1 > \mu_{\mathrm{FR}} > p_{\mathrm{R}}$: Despite the elimination of all detectable faults, the repair process increases the expected fault count.
4. $\mu_{\mathrm{FR}} > 1$: The repair goal, the elimination of all detectable faults, is not achievable.

A reasonable repair process should aim for $\mu_{\mathrm{FR}} < 0.1$.

Example 2.13: Good student programming performance

- Low fault programming, lets say $\mu_{\mathrm{FCP}} = 5$ faults (without syntax faults).
- Thorough test, e.g. $p_{\mathrm{FD}} = 50\%$ with $n = 10$ tests.
- Successful fault elimination, e.g. 2 to 3 repair attempts per fault ($p_{\mathrm{R}} = 40\%$), one emerging fault per 10 repair attempts ($\xi_{\mathrm{R}} = 0.1$).
- Form factor of the MF rate distribution $k = 0.5$.

$$\begin{array}{llllll}
\text{Gl. 2.14} & \eta_{\mathrm{FR}} & = \frac{p_{\mathrm{FD}}\cdot\xi_{\mathrm{R}}}{p_{\mathrm{R}}} & = \frac{50\%\cdot 0.1}{40\%} & = 0.12 \\
\text{Gl. 2.15} & \mu_{\mathrm{FNE}} & = \frac{(1-p_{\mathrm{FD}})\cdot\mu_{\mathrm{FCP}}}{1-\mu_{\mathrm{FR}}} & = \frac{(1-50\%)\cdot 5}{1-0.12} & = 3.75 \\
\text{Gl. 1.43} & \zeta_{\mathrm{F}} & \approx \frac{k\cdot\mu_{\mathrm{FNE}}}{n} & = \frac{0.5\cdot 3.75}{10} & = 0.1875
\end{array}$$

- On average 2.5 original plus 1.25 undetectable defects arising during repair.
- A further random test will not fail with a probability of $1 - \zeta > 80\%$.

Good enough for a course credit.

Example 2.14: Poor student programming performance

- More design faults, e.g. $\mu_{\mathrm{FCP}} = 7$ (without syntax faults).
- Less tests, e.g. $p_{\mathrm{FD}} = 30\%$ with $n = 5$ tests.
- On average 3 to 4 repair attempts per fault ($p_{\mathrm{R}} = 30\%$) and due to the lack of rebuilding after unsuccessful repair attempts only $\xi_{\mathrm{R}} = 0.5$.
  Form factor of the MF rate distribution $k = 0.5$.

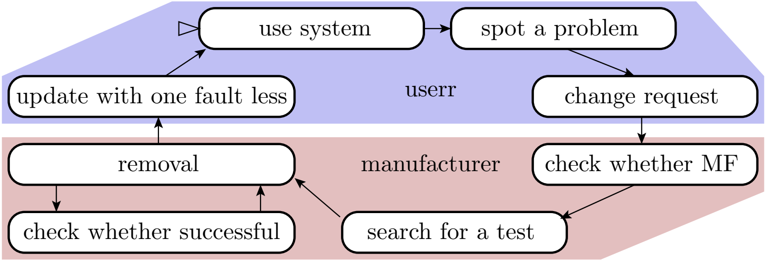
$$\begin{array}{lrlll}
\text{Gl. 2.14} & \eta_{\mathrm{FR}} & = \frac{p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}} & = \frac{0.3 \cdot 50\%}{40\%} & = 0.375 \\
\text{Gl. 2.15} & \mu_{\mathrm{FNE}} & = \frac{(1 - p_{\mathrm{FD}}) \cdot \mu_{\mathrm{FCP}}}{1 - \mu_{\mathrm{FR}}} & = \frac{(1 - 30\%) \cdot 7}{1 - 0.375} & = 7.9 \\
\text{Gl. 1.43} & \zeta & \approx \frac{k \cdot \mu_{\mathrm{FNE}}}{n} & = \frac{0.5 \cdot 7.9}{5} & = 0.8
\end{array}$$

- On average 4.9 original faults plus 2.9 undetectable faults resulting from the repair.
- A further random test will fail with a probability of $\zeta > 80\%$.

How to pass the exam? Doubling the number of tests to $n = 10$ tests. Deconstruction to halve ξ_{R}. ...

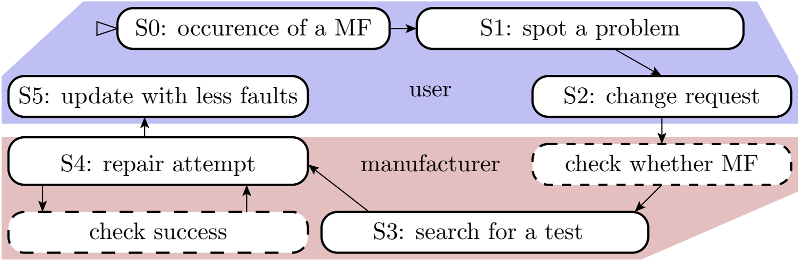
Maturation processes

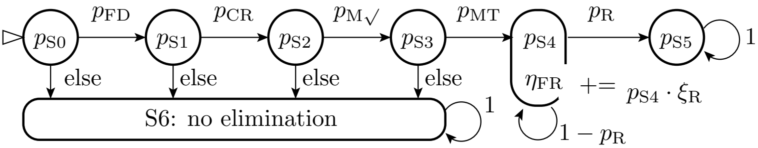
Elimination of faults in a maturing process



1. In case of a suspected malfunction, the user makes a change request. Alternatively, the system sends a MF report. MF reports are collected in drawers of suspected same cause.
2. The manufacturer favours for elimination drawers that suggest faults with frequent serious MF.
3. Search for tests that stimulate the MFs in a reproducible way.
4. Experimental repair. Installation of updates.

Modelling as Markov chain

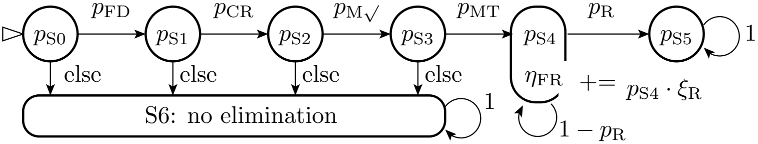




---

p_{Si} Probability that the Markov chain is in state S_i.

η_{FR} Expected number of **f**aults emerging during **r**epair per originally occurring fault .



Fault elimination probability in the case of an MF:

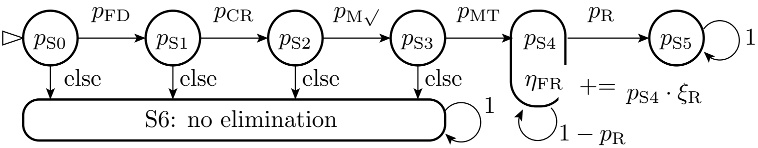
$$p_{\mathrm{FE}} = p_{\mathrm{FD}} \cdot p_{\mathrm{CR}} \cdot p_{\mathrm{M}\surd} \cdot p_{\mathrm{MT}} \tag{17}$$

The edge counter μ_{FR} is used to estimate the expected number of new faults that arise during the repair process. For faults created during repair, the maturing time counts from emergence.

---

p_{FE}	**p**robability of **f**ault **e**limination.
p_{FD}	**p**robability of **f**ault **d**etection.
p_{CR}	probability of a **c**hange **r**equest being made for an observed MF.
$p_{\mathrm{M}\surd}$	probability that **m**anufacturer can reconstruct the MF.
p_{MT}	probability that the **m**anufacturer will find a **t**est for fault detection.
p_{R}	probability of **r**epair success.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
ξ_{R}	fault emerging rate in faults per **r**epair attempt.

Newly created faults per existing fault



$$\eta_{\mathrm{FR}} = p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}} \cdot \sum_{n=0}^{\infty} (1 - p_{\mathrm{R}})^n = \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}} \tag{18}$$

With the elimination of each newly created fault, on average η_{FR} new faults are created with the elimination of which η_{FR} new faults are created:

$$\eta_{\mathrm{FRR}} = \eta_{\mathrm{FR}} + \eta_{\mathrm{FR}}^2 + \eta_{\mathrm{FR}}^3 + \ldots = \frac{\eta_{\mathrm{FR}}}{1 - \eta_{\mathrm{FR}}} \tag{19}$$

η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
p_{FE}	**p**robability of **f**ault **e**limination.
ξ_{R}	fault emerging rate in faults per **r**epair attempt.
p_{R}	**p**robability of **r**epair success.

Decrease in the number of errors and the MF rate

Decrease in the expected number of faults not eliminated without new fault occurrence (see sec. 1.4.6):

$$\mu_{\mathrm{FNE}}\left(n_{\mathrm{M}}\right)=\mu_{\mathrm{FNE}}\left(n_{\mathrm{M0}}\right)\cdot\left(\frac{n_{\mathrm{M}}}{n_{\mathrm{M0}}}\right)^{-k} \tag{1.57}$$

with

$$n_{\mathrm{M}}=n_{\mathrm{MV}}\cdot u+n_{\mathrm{MR}} \tag{1.56}$$

$$\mu_{\mathrm{FNE}}\left(u\right)=\mu_{\mathrm{FNE}}\left(n_{\mathrm{M0}}\right)\cdot\left(\frac{n_{\mathrm{MV}}\cdot u+n_{\mathrm{MR}}}{n_{\mathrm{MR}}}\right)^{-k} \tag{20}$$

μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
n_{M}	effective number of services, for which all detected faults are eliminated.
n_{MR}	Effective number of tests before the first and each subsequent version release.
k	form factor of the distribution of the malfunction rate $(0<k<1)$.
n_{MV}	additional effective number of tests per **v**ersion **r**elease interval.
u	version number of the maturing object.

3. Fault elimination

The first and each improved version is only released after passing all n_{M0} manufacturer tests without MF. Effective test set length in version u for faults from version v:

$$n_{\mathrm{M}}\left(u,v\right)=n_{\mathrm{MR}}+\left(u-v\right)\cdot n_{\mathrm{MV}} \tag{21}$$

The detection probability from the origin version v to the use version u results from the reduction of the expected number of faults in eq. 2.20 by increasing the effective test number from n_{M0} to $n_{\mathrm{M}}\left(u,v\right)$ in eq. 2.21:

$$p_{\mathrm{NE}}\left(u,v\right)=\left(\frac{n_{\mathrm{MR}}+\left(u-v\right)\cdot n_{\mathrm{MU}}}{n_{\mathrm{MR}}}\right)^{-k} \tag{22}$$

The faults$\mu_{\mathrm{FNE}}\left(0\right)$, which were already present in version 0, are eliminated in the subsequent versions with $p_{\mathrm{NE}}\left(u,0\right)$:

$$\mu_{\mathrm{F}}\left(u,0\right)=\mu_{\mathrm{FNE}}\left(0\right)\cdot p_{\mathrm{NE}}\left(u,0\right)$$

---

n_{M}	effective number of services, for which all detected faults are eliminated.
n_{MR}	Effective number of tests before the first and each subsequent version release.
u	version number of the maturing object.
v	Number of the version in which the fault emerged.
n_{MV}	additional effective number of tests per **v**ersion **r**elease interval.
$p_{\mathrm{NE}}\left(u,v\right)$	Probability that a fault from version v is not eliminated in version u.

3. Fault elimination

In subsequent versions $v > 0$, a number of faults proportional to the number of faults removed is added to the usage version $u = v$, which is reduced by$p_{\mathrm{NE}}\left(u, v\right)$ in subsequent versions $u > v$:

$$\mu_{\mathrm{F}}\left(u, v\right) = \begin{cases} \underbrace{\eta_{\mathrm{FR}} \cdot \sum_{i=0}^{u} \mu_{\mathrm{F}}\left(u, i\right) - \mu_{\mathrm{F}}\left(u-1, i\right)}_{\text{expected no. of faults eliminated}} & v = u \\ \mu_{\mathrm{F}}\left(u, u\right) \cdot p_{\mathrm{NE}}\left(v - u\right) & v > u \end{cases} \tag{23}$$

Expected total number of faults of each version u:

$$\mu_{\mathrm{FNE}}\left(u\right) = \sum_{i=0}^{u} \mu_{\mathrm{F}}\left(u, i\right) \tag{24}$$

$\mu_{\mathrm{F}}\left(u, v\right)$	expected number of faults that emerged in version v and are not fixed in version u.
u	version number of the maturing object.
v	Number of the version in which the fault emerged.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
$p_{\mathrm{NE}}\left(u, v\right)$	Probability that a fault from version v is not eliminated in version u.
μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.

Taking into account

$$\zeta_{\mathrm{F}}(n_{\mathrm{M}}) = \frac{k \cdot \mu_{\mathrm{FNE}}(n_{\mathrm{M}})}{n_{\mathrm{M}}} \tag{1.58}$$

the MF rate in version u due to faults from version v is:

$$\zeta_{\mathrm{F}}(u,v) = \frac{k \cdot \mu_{\mathrm{F}}(u,v)}{n_{\mathrm{M}}(u,v)} \tag{25}$$

MF rate version u through all faults:

$$\zeta_{\mathrm{F}}(u) = \sum_{i=0}^{u} \zeta_{\mathrm{F}}(u,v) \tag{26}$$

ζ_{F}	malfunction rate caused by **f**aults.
n_{M}	effective number of services, for which all detected faults are eliminated.
k	form factor of the distribution of the malfunction rate $(0 < k < 1)$.
μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
$\zeta_{\mathrm{F}}(u,v)$	MF rate in version u caused by faults emerged in version v.
$\mu_{\mathrm{F}}(u,v)$	expected number of faults that emerged in version v and are not fixed in version u.
$n_{\mathrm{M}}(u,v)$	effective number of tests version u for faults from version v.

Example 2.15: Maturation process with newly emerging faults

Parameter: $\mu_{\text{FNE}}(0) = 100$, $n_{\text{MR}} = 10^5$, $n_{\text{MU}} = 10^6$, $\eta_{\text{FR}} = 0{,}1$, $k = 0{,}4$.

a) Expected fault rates $\mu_{\text{F}}(u, v)$ for $u = 0$ to 5 matured versions per origin version v and in total

b) MF rates version u by faults from version v and sum

c) Relative increase in the expected number of faults due to the new faults emerging during elimination.

d) Relative increase in MF rate due to emerging faults.

μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
n_{MR}	Effective number of tests before the first and each subsequent version release.
n_{MU}	effective number of tests in a single update intervall of the **m**aturity process.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
k	form factor of the distribution of the malfunction rate $(0 < k < 1)$.

Parameter: $\mu_{\mathrm{FNE}}(0) = 100$, $n_{\mathrm{MR}} = 10^5$, $n_{\mathrm{MU}} = 10^6$, $\eta_{\mathrm{FR}} = 0{,}1$, $k = 0{,}4$.

a) Expected fault rates $\mu_{\mathrm{F}}(u, v)$ for $u = 0$ to 5 matured versions per origin version v and in total

Table $\mu_{\mathrm{F}}(u, v)$ and $\mu_{\mathrm{FNE}}(u)$ for version 1 to 5:

u	0	1	2	3	4	5
$v = 0$	100	38.32	29.59	25.32	22.64	20.75
$v = 1$	0	6.17	2.36	1.82	1.56	1.40
$v = 2$	0	0	1.25	$4.80 \cdot 10^{-1}$	$3.71 \cdot 10^{-1}$	$3.17 \cdot 10^{-1}$
$v = 3$	0	0	0	$5.58 \cdot 10^{-1}$	$2.14 \cdot 10^{-1}$	$1.65 \cdot 10^{-1}$
$v = 4$	0	0	0	0	$3.40 \cdot 10^{-1}$	$1.30 \cdot 10^{-1}$
$v = 5$	0	0	0	0	0	$2.37 \cdot 10^{-1}$
$\mu_{\mathrm{FNE}}(u)$	100	44.49	33.21	28.18	25.13	22.99

$\mu_{\mathrm{F}}(u, v)$ expected number of faults that emerged in version v and are not fixed in version u.

μ_{FNE} expected number of **n**ot **e**liminated **f**aults.

Parameter: $\mu_{\text{FNE}}(0) = 100$, $n_{\text{MR}} = 10^5$, $n_{\text{MU}} = 10^6$, $\eta_{\text{FR}} = 0{,}1$, $k = 0{,}4$.

b) MF rates version u by faults from version v and sum

$$\zeta_{\text{F}}(u, v) = k \cdot \frac{\mu_{\text{F}}(u,v)}{n_{\text{u}}(u,v)} \tag{2.25}$$

$$\zeta_{\text{F}}(u) = \sum_{i=0}^{u} \zeta_{\text{F}}(u, v) \tag{2.26}$$

u	0	1	2	3	4	5
$v = 0$	$4\cdot 10^{-4}$	$1.39\cdot 10^{-5}$	$5.64\cdot 10^{-6}$	$3.27\cdot 10^{-6}$	$2.21\cdot 10^{-6}$	$1.63\cdot 10^{-6}$
$v = 1$	0	$2.47\cdot 10^{-5}$	$8.59\cdot 10^{-7}$	$3.48\cdot 10^{-7}$	$2.02\cdot 10^{-7}$	$1.36\cdot 10^{-7}$
$v = 2$	0	0	$5.02\cdot 10^{-6}$	$1.75\cdot 10^{-7}$	$7.07\cdot 10^{-8}$	$4.10\cdot 10^{-8}$
$v = 3$	0	0	0	$2.23\cdot 10^{-6}$	$7.78\cdot 10^{-8}$	$3.14\cdot 10^{-8}$
$v = 4$	0	0	0	0	$1.36\cdot 10^{-6}$	$4.73\cdot 10^{-8}$
$v = 5$	0	0	0	0	0	$9.48\cdot 10^{-7}$
$\zeta_{\text{F}}(u)$	$4\cdot 10^{-4}$	$3.86\cdot 10^{-5}$	$1.15\cdot 10^{-5}$	$6.02\cdot 10^{-6}$	$3.92 \cdot 10^{-6}$	$2.83\cdot 10^{-6}$

$\mu_{\text{F}}(u, v)$ expected number of faults that emerged in version v and are not fixed in version u.

$n_{\text{M}}(u, v)$ effective number of tests version u for faults from version v.

Parameter: $\mu_{\mathrm{FNE}}(0) = 100$, $n_{\mathrm{MR}} = 10^5$, $n_{\mathrm{MU}} = 10^6$, $\eta_{\mathrm{FR}} = 0{,}1$, $k = 0{,}4$.

c) Relative increase in the expected number of faults due to the new faults emerging during elimination.

u	1	2	3	4	5
$\frac{\mu_{\mathrm{FNE}}(u)}{\mu_{\mathrm{F}}(u,0)}$	1.161	1.122	1.113	1.110	1.108

In comparison, the rate of recursively newly arising faults per originally existing fault according to the Markov chain

$$\eta_{\mathrm{FRR}} = \frac{\eta_{\mathrm{FR}}}{1-\eta_{\mathrm{FR}}} \tag{2.19}$$

$$\eta_{\mathrm{FRR}} = \frac{\eta_{\mathrm{FR}}}{1-\eta_{\mathrm{FR}}} = \frac{0.1}{1-0.1} = 0{,}111$$

μ_{FNE}	expected number of **n**ot **e**liminated **f**aults.
$\mu_{\mathrm{F}}(u, v)$	expected number of faults that emerged in version v and are not fixed in version u.
η_{FR}	Expected number of **f**aults emerging during **r**epair per originally occurring fault .
η_{FRR}	new emerging faults per original fault recursive.

Parameter: $\mu_{\mathrm{FNE}}(0) = 100$, $n_{\mathrm{MR}} = 10^5$, $n_{\mathrm{MU}} = 10^6$, $\eta_{\mathrm{FR}} = 0{,}1$, $k = 0{,}4$.

d) Relative increase in MF rate due to emerging faults.

Relative increase in MF rate due to the emergence of new faults:

u	1	2	3	4	5
$\frac{\zeta_{\mathrm{F}}(u)}{\zeta_{\mathrm{F}}(u,0)}$	2.78	2.04	1.84	1.77	1.74

Significantly dependent on η_{FR} and n_{MR}. Also, if new faults emerge during elimination, the MF rate decreases with $u^{-(k+1)}$ for $u_0 > 1$:

$$\zeta_{\mathrm{F}}(u) = \zeta_{\mathrm{F}}(u_0) \cdot \left(\frac{u}{u_0}\right)^{-(k+1)} \tag{27}$$

Summary

F2.3.1 bis F2.3.3 Replacement, repair

A fault elimination iteration with success control, eliminates all detectable faults.

Fault elimination by replacement:

- expected number of replacements per object found to be good:

$$\mu_{\mathrm{R}} = \frac{1}{Y} - 1 \tag{2.12}$$

- Defect level after replacement of detected defective units as before:

$$DL_{\mathrm{R}} = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{1.68}$$

Fault elimination by repair:

- Expected number of new faults per originally existing fault:

$$\eta_{\mathrm{FR}} = \frac{p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}} \tag{2.14}$$

- Expected number of not eliminated faults:

$$\mu_{\mathrm{FNE}} = \frac{(1 - p_{\mathrm{FD}}) \cdot \mu_{\mathrm{FCP}}}{1 - \eta_{\mathrm{FR}}} \tag{2.15}$$

$$\mu_{\mathrm{FNE}} = \frac{(1 - p_{\mathrm{FD}}) \cdot p_{\mathrm{R}} \cdot \mu_{\mathrm{FCP}}}{p_{\mathrm{R}} - p_{\mathrm{FD}} \cdot \xi_{\mathrm{R}}} \tag{2.16}$$

2.3.4 Maturing process

Probability of fault elimination:

$$p_{\mathrm{FE}} = p_{\mathrm{FD}} \cdot p_{\mathrm{CR}} \cdot p_{\mathrm{M}\surd} \cdot p_{\mathrm{MT}} \tag{2.17}$$

Expected number of new faults per originally existing fault

$$\eta_{\mathrm{FR}} = \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}}} \tag{2.18}$$

and recursively when eliminating newly created faults

$$\eta_{\mathrm{FRR}} = \frac{\eta_{\mathrm{FR}}}{1-\eta_{\mathrm{FR}}} \tag{2.19}$$

Probability of non-elimination for faults in version u from version v $(0 < v \leq u)$:

$$p_{\mathrm{NE}}(u,v) = \left(\frac{n_{\mathrm{M0}} + (u-v) \cdot n_{\mathrm{MU}}}{n_{\mathrm{M0}}} \right)^{-k} \tag{2.22}$$

Expected number of faults originating from fault elimination in version $v > 0$ that are still present in version $u \geq v$:

$$\mu_{\mathrm{F}}(u,v) = \begin{cases} \eta_{\mathrm{FR}} \cdot \sum_{i=0}^{u} \mu_{\mathrm{F}}(u,i) - \mu_{\mathrm{F}}(u-1,i) & v = u \\ \mu_{\mathrm{F}}(u,u) \cdot p_{\mathrm{NE}}(v-u) & v > u \end{cases} \tag{2.23}$$

Total expected fault count in version u:

$$\mu_{\mathrm{FNE}}(u) = \sum_{i=0}^{u} \mu_{\mathrm{F}}(u,i) \tag{2.24}$$

MF-rate of version u due to faults from version v:

$$\zeta_{\mathrm{F}}(u,v) = k \cdot \frac{\mu_{\mathrm{F}}(u,v)}{n_{\mathrm{u}}(u,v)} \tag{2.25}$$

Total MF rate due to faults in version u:

$$\zeta_{\mathrm{F}}(u) = \sum_{i=0}^{u} \zeta_{\mathrm{F}}(u,v) \tag{2.26}$$

Decrease in the expected number of faults and MF rate caused by faults estimated from the example for with growing version number:

$$\zeta_{\mathrm{F}}(u) = \zeta_{\mathrm{F}}(u_0) \cdot \left(\frac{u}{u_0}\right)^{-(k+1)} \tag{2.28}$$

Resulting increase in reliability:

$$R_{\mathrm{MT}}(u) = R_{\mathrm{MT}}(u_0) \cdot \left(\frac{u}{u_0}\right)^{k+1} \tag{28}$$

R_{MT}	**r**eliability with **m**alfunction **t**reatment.
u	version number of the maturing object.
u_0	version number of the maturing object with knows MF rate or reliablity, respectively.

Fault emergence

Estimation of the expected fault count

- Simple estimation model via metrics:

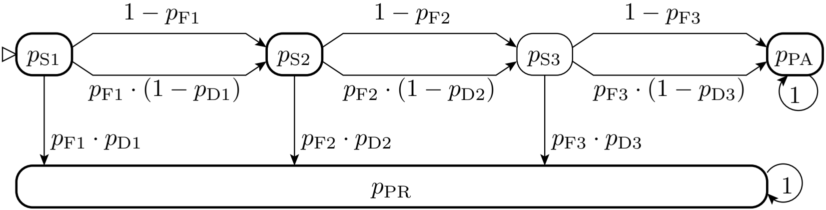
$$\mu_{\mathrm{FCP}} = \xi \cdot C \tag{1.73}$$

- Modelling the emergence of good and defective products using Markov chains.
- Modelling of product emergence by Markov chains with edge counters for effort estimation. Estimation of the expected number of faults arising from the effort and the proportion of faults not eliminated from it via (non-) detection probabilities of the tests.

μ_{FCP}	expected number of **f**aults from **c**reation **p**rocess.
ξ	fault generation rate **c**reation process.
C	metric for **c**reation effort or scale.

Creation processes with checks

Linear sequence of creation steps. If control i detects a fault, the object is sorted out, otherwise transition to the next step faultless or with undetected faults:



p_{Si}	Probability that the Markov chain is in state S_i.
$p_{\mathrm{F}i}$	probability that a **f**ault emerges in step i.
$p_{\mathrm{D}i}$	Fault **d**etection probability of the check after step i.
p_{PA}	Probability that the **p**roduct is **a**ccepted as fault-free.
p_{PR}	Probability that the **p**roduct is **r**ejected as faulty.

4. Fault emergence

Probability that the object will be accepted as defect-free:

$$p_{\mathrm{PA}} = \prod_{i=1}^{3} \left(1 - p_{\mathrm{D}i} \cdot p_{\mathrm{F}i}\right)$$

Probability of creating a defect-free object:

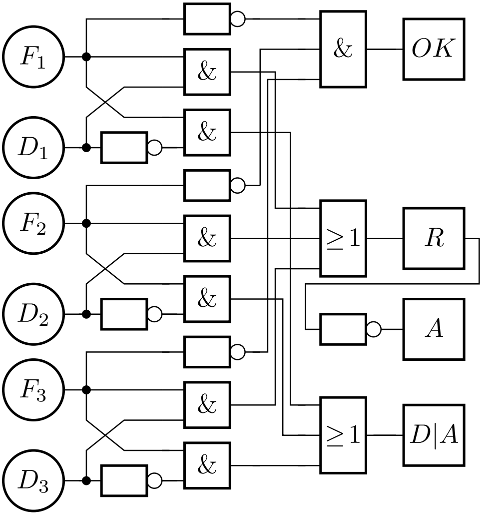
$$p_{\mathrm{OK}} = \prod_{i=1}^{3} \left(1 - p_{\mathrm{F}i}\right)$$

Defect level, counter probability of the conditional probability that a product is ok if it is not sorted out:

$$DL_{\mathrm{M}} = 1 - \mathbb{P}\left(OK|A\right) = 1 - \frac{p_{\mathrm{OK}}}{p_{\mathrm{OA}}} = 1 - \prod_{i=1}^{3} \left(\frac{1-p_{\mathrm{F}i}}{1-p_{\mathrm{D}i}\cdot p_{\mathrm{F}i}}\right)$$

DL_{M}	**d**efect **l**evel after **m**anufacturing.
A	event product **a**ccepted as fault-free.
OK	event product **ok** (faultless).
p_{PR}	Probability that the **p**roduct is ok (faultless).

Linear creation process as a fault tree



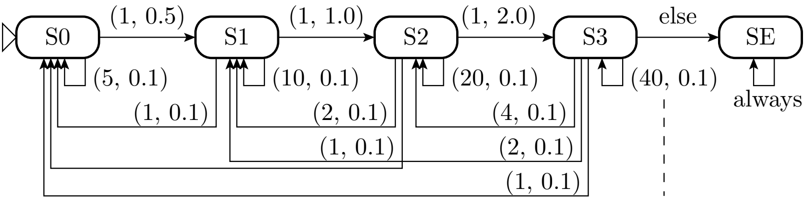
events during product creation

F_i	fault originated in step i
D_i	fault in step i detected
OK	product ok
R	rejection due to faults
A	accepted as faultless
$D\|A$	accepted but faulty

Creation processes with backtracks

Processing stages, e.g. S0 – requirements analysis,
S1 – specification, S2 – system design and S3 – coding

creation
completed



(μ_{ij}, ζ_{ij})

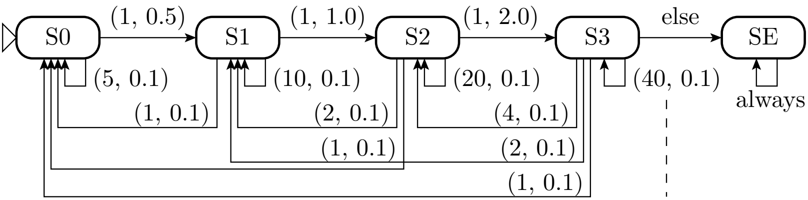
expected number of faults arising at edge transition(i, j)

expected number of transitions until the next level is reached

The transition probability per edge is the expected number of transitions divided by the sum of the transition counts of all edges starting from the same state:

$$p_{\mathrm{T}ij} = \frac{\mu_{iu}}{\sum_{u=0}^{4} \mu_{iu}}$$

4. Fault emergence



(μ_{ij}, ζ_{ij}) expected number of faults arising at edge transition(i, j)

expected number of transitions until the next level is reached

Transition matrix of the Markov chain:

$$\begin{pmatrix} p_{\mathrm{S0}} \\ p_{\mathrm{S1}} \\ p_{\mathrm{S2}} \\ p_{\mathrm{S4}} \\ p_{\mathrm{SE}} \end{pmatrix}_{n+1} = \begin{pmatrix} \frac{5}{6} & \frac{1}{12} & \frac{1}{24} & \frac{1}{48} & 0 \\ \frac{1}{6} & \frac{10}{12} & \frac{2}{24} & \frac{2}{48} & 0 \\ 0 & \frac{1}{12} & \frac{20}{24} & \frac{4}{48} & 0 \\ 0 & 0 & \frac{1}{24} & \frac{40}{48} & 0 \\ 0 & 0 & 0 & \frac{1}{48} & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{\mathrm{S0}} \\ p_{\mathrm{S1}} \\ p_{\mathrm{S2}} \\ p_{\mathrm{S4}} \\ p_{\mathrm{SE}} \end{pmatrix}_{n}$$

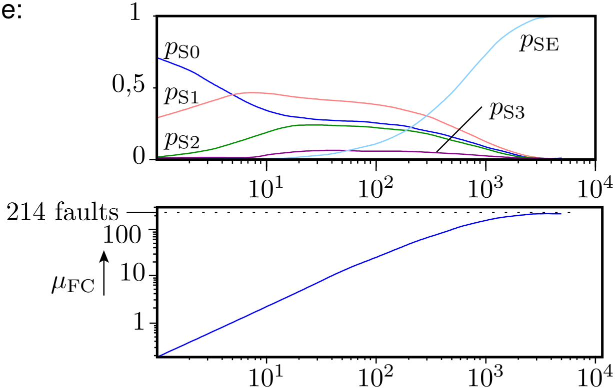
p_{Si}	Probability that the Markov chain is in state S_i.
$p_{\mathrm{T}ij}$	transition probability from state i to state j.
n	number of simulation steps.

4. Fault emergence

Increase of number of undetectable faults per simulation step:

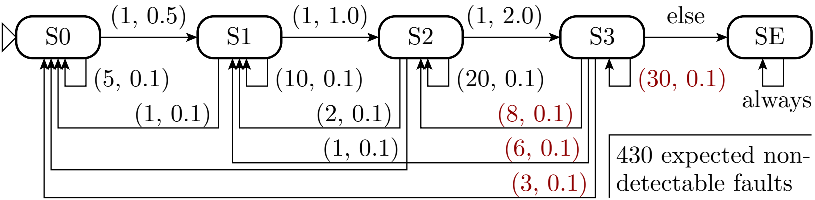
```
For all edges from state $S_i$ to state $S_j$
    $\mu_{\mathrm{FC}} += p_{\mathrm{S}i} \cdot p_{\mathrm{T}ij} \cdot \zeta_{ij}$
```

Simulation example:



μ_{FCP}	expected number of **f**aults from **c**reation **p**rocess.
$p_{\mathrm{T}ij}$	transition probability from state i to state j.
ζ_{ij}	expected number of faults emerging during edge transition from state i to state j.

Increase of the expected number of recourses



A change in the recourse probabilities in stage S3:

$$\begin{array}{llcl} p_{\mathrm{T3.3}}: & \frac{40}{48} & \to & \frac{30}{48} \\ p_{\mathrm{T3.2}}: & \frac{4}{48} & \to & \frac{8}{48} \\ p_{\mathrm{T3.1}}: & \frac{2}{48} & \to & \frac{6}{48} \\ p_{\mathrm{T3.0}}: & \frac{1}{48} & \to & \frac{3}{48} \\ \mu_{\mathrm{FNE}}: & 214 & \to & 450 \end{array}$$

roughly doubles the number of faults that arise and also roughly doubles the effort required to create them. Therefore, in step models, regressions over several steps should be avoided as far as possible.

Summary

- Simple estimation model via metrics:

$$\mu_{\mathrm{FCP}} = \xi \cdot C \tag{1.73}$$

- An example of a Markov chain for a creation process to estimate the probabilities of creating good products, sorted out product and products with undetectable faults..
- An example Markov chain for a step model with fallbacks and edge counters for estimating the number of arising faults.
- Using example simulations, it was shown that small increases in the depth of fallback cause significant increases in the amount of work and the number of faults that can be expected to arise.