

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering
ati.ttu.ee

IAF0530/IAF9530

Süsteemide usaldusväärsus ja veakindlus
Dependability and fault tolerance

Loeng 7
Liiasus (Informatsioon, aeg, keskkond)

Gert Jervan
gert.jervan@pld.ttu.ee

Tallinn University of Technology
Department of Computer Engineering
Estonia

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Lecture Outline

Some materials from:
Elena Dubrova
Paul Pop

- ✓ Introduction
- ✓ Hardware Redundancy
- ✓ Software Redundancy
- ✓ Information Redundancy
- ✓ Time Redundancy
- ✓ Environment Redundancy

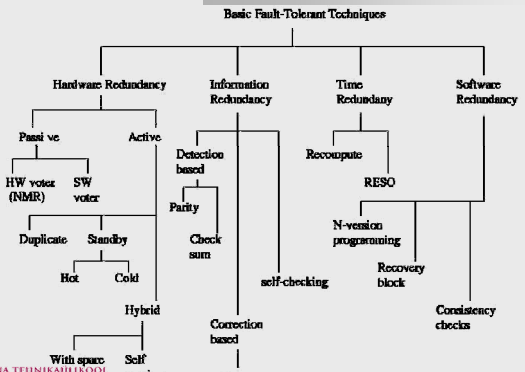


TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

2

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

A summary chart of all techniques



TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

3

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Information redundancy

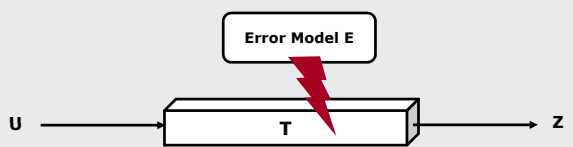
- ✓ Definition
 - Information redundancy is the addition of redundant information to data to allow fault detection, fault masking or possibly fault tolerance.
- ✓ Error detecting and correcting codes (EDC codes)
 - Encoding of information for transmission in noisy environments
 - Later for dependability: communications, memory, storage, etc.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

4

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Model



- ✓ Functional faults
- ✓ Technological faults
- ✓ Disruptions due to the environment

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

5

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Classes

- ✓ An error is **single** when it only affects a single bit of the output Z
- ✓ An error is **multiple of order p** when it affects at most p bits of Z
- ✓ Burst error – the erroneous bits of Z are within an l-distance neighbourhood

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

6

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Code

- ✓ **Code of length n** is a set of n -tuples satisfying some well-defined set of rules
- ✓ **Binary code** uses only 0 and 1 symbols
 - binary coded decimal (BCD) code
 - uses 4 bits for each decimal digit

0000	0
0001	1
0010	2
...	
1001	9

7

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Code Word

- ✓ A **code word** is a collection of symbols used to represent a particular piece of data based on specified code
- ✓ A **word** is an n -tuple not satisfying the rules of the code
- ✓ Codewords should be a subset of all possible $2n$ binary tuples to make error detection/correction possible
 - BCD: 0110 valid; 1110 invalid
 - any binary code: 2013 invalid
- ✓ The number of codewords in a code C is called the **size** of C

8

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Encoding vs. decoding

- ✓ The **encoding process** is the process of determining the corresponding code word for a particular data item.
 - Example: given the decimal 9, encoding determines the BCD representation of 1001.

```

graph LR
    data[data] --> encoding[encoding]
    encoding --> codeword[code word]
  
```

- ✓ The **decoding process** is the process of recovering the original data from the code word.
 - Example: decoding transforms the BCD code 0011 into the decimal 3

```

graph LR
    codeword[code word] --> decoding[decoding]
    decoding --> data[data]
  
```

9

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Encoding/decoding

- ✓ 2 scenario if errors affect codeword:
 - correct codeword → another codeword
 - correct codeword → word

10

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Detection

- ✓ We can define a code so that errors introduced in a codeword force it to lie outside the range of codewords
 - Basic principle of **error detection**

11

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Detection

- ✓ Error detection: code word is invalid

12

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Correction

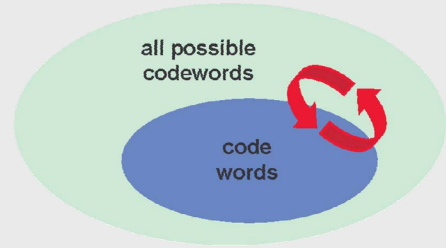
- ✓ We can define a code so that it is possible to determine the correct code word from the erroneous codeword
 - Basic principle of **error correction**

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Correction

- ✓ Error correction: correct word can be identified from the corrupted word

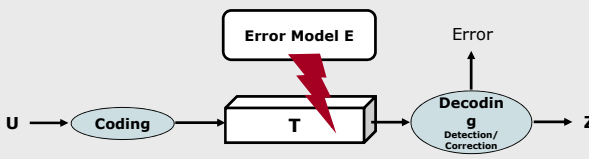


TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

EDC/ECC

- ✓ Error Detecting and Correcting Codes



- ✓ Separable/non-separable codes
 - Separable: original information is appended with new information

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

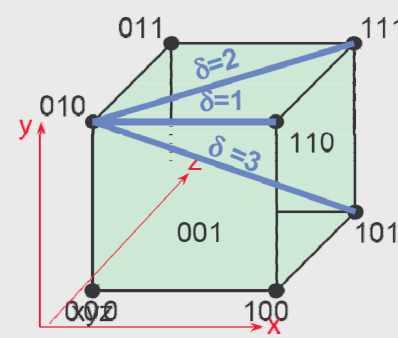
EDC/ECC

- ✓ Characterized by the number of bits that can be corrected
 - double-bit detecting code can detect two single-bit errors
 - single-bit correcting code can correct one single-bit error
- ✓ Hamming distance gives a measure of error detecting/correcting capabilities of a code
 - Number of bit positions in which the two words differ
 - Hamming distance of 1: 0000 to 0001; 2: 0000 to 0101
 - Code distance:
 - Minimum Hamming distance between any two valid code words

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

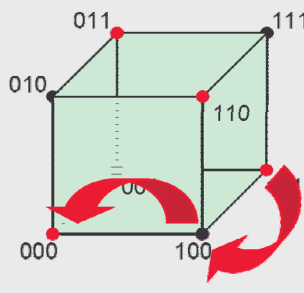
3-dimensional space (3-bit words)



TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Detection



- ✓ If codewords are on distance ≥ 2 , we can detect single-bit errors

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Correction

✓ If codewords are on distance ≥ 3 , we can correct single-bit errors

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

19

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Code Distance

✓ Code distance is the minimum Hamming distance between any two distinct codewords

$C_d = 2$ code detects all single-bit errors
code: 00, 11
invalid code words: 01 or 10

$C_d = 3$ code corrects all single-bit errors
code: 000, 111
invalid code words: 001, 010, 100, 101, 011, 110

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

20

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Code Capabilities

✓ To correct ε -bit errors a code should have the code distance $C_d \geq 2\varepsilon + 1$

✓ To be able to detect ε -bit errors a code should have the code distance $C_d \geq \varepsilon + 1$

✓ A code can correct up to c bit errors and detect up to d additional bit errors if and only if:

$$2c + d + 1 \leq C_d$$

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

21

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Separable/non-separable code

✓ Separable code

- codeword = data + check bits
- e.g. parity: 11011 = 1101 + 1

✓ Non-separable code

- codeword = data mixed with check bits
- e.g. cyclic: 1010001 $\rightarrow$ 1101

✓ Decoding process is much easier for separable codes (remove check bits)

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

22

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Information Rate

✓ The ratio k/n , where

- k is the number of data bits
- n is the number of data + check bits

is called the information rate of the code

✓ Example: a code obtained by repeating data three times has the information rate $1/3$

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

23

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Code Characterization

✓ Cost: number of bits n that it needs

✓ Power of expression (cardinality): number of codewords N that it is able to represent

✓ Error model: defining the errors detected and/or corrected

- Redundancy rate: $rr=r/k$ (r : added bits)
- Density of a code: $d=N/2^n$
- Coverage rate

TALLINNA TEHNIKALÜKÜÜL
TALLINN UNIVERSITY OF TECHNOLOGY

24

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Parity codes

✓ Addition of an extra bit to a binary word such that the resulted code word has either an even number or an odd number of 1s.

✓ Separable code

✓ Hamming distance of 2

✓ Can detect any single bit error

- Even parity
 - One bit flip: odd number of bits
- Odd parity
 - One bit flip: even number of bits

✓ Application: bus, memory, transmission

Decimal digit	BCD	BCD odd parity	BCD even parity
0	0000	0000:1	0000:0
1	0001	0001:0	0001:1
2	0010	0010:0	0010:1
3	0011	0011:1	0011:0
4	0100	0100:0	0100:1
5	0101	0101:1	0101:0
6	0110	0110:1	0110:0
7	0111	0111:0	0111:1
8	1000	1000:0	1000:1
9	1001	1001:1	1001:0

↑ Parity bit

↑ Parity bit

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

25

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Generation and checking circuit for parity codes: XOR

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

26

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Memory with parity coding

✓ 32-bit word + 4 parity bits = 36 bits stored

✓ 64-bit word + 8 parity bits = 72 bits stored

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

27

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Application

- ✓ Memories are built of individual chips
 - 4-bit chips
 - 98% of all memory errors are single-bit errors
 - 1GByte DRAM with parity code: 0,7 failures per year
- ✓ If one chip fails: multiple-bit errors
 - Parity codes cannot detect multiple bit errors
- ✓ Modifications of the basic parity scheme
 - Bit-per-word parity
 - Bit-per byte parity
 - Bit-per chip parity
 - Bit-per multiple chips parity
 - Interlaced parity

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

28

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Forms of parity code

Problems

- ← All bits are changed to 1 or 0
- ← Better, but still not able to detect a 4-bit chip failure
- ← Each bit from a chip forms a parity word with other bits
 - Cannot locate the problem
- ← Can detect and locate the error
 - Problem with chip-failure
- ← Used when errors in adjacent bits are of concern

Fig. 3.29 The five basic forms of the parity code include: bit-per-word, bit-per-byte, bit-per multiple-chips, bit-per chip, and interlaced parity.

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

29

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Forms of parity code

Code	Advantages	Disadvantages
Even parity	Detects single-bit errors	Certain errors go undetected, e.g., if a word, including the parity bit, becomes all is
Bit-per-word		
Bit-per-byte parity	Detects the all is and the all 0s conditions	Ineffective in detection of multiple errors
Bit-per-multiple-chips parity	Detects failure of entire chip	Failure of a complete chip is detected, but it is not located
Bit-per-chip parity	Detects single error and identifies the chip that contains the erroneous bit	Susceptible to the whole-chip failure
Interlaced parity	Detects errors in adjacent bits; does not take into account the physical memory organization	Parity groups not based on the physical memory organization

PTSE TALLINNA TEHNIKAKOOL TALLINN UNIVERSITY OF TECHNOLOGY

30

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Overlapping parity code

Fig. 3.30 Overlapping parity assigns each bit to multiple parity groups.

- ✓ The impact of an erroneous bit is unique
 - Example: flip of data bit 2 affects parity bits P_1 and P_2
 - Bit can be detected and corrected
- ✓ The required redundancy decreases as the numbers of bits increase

Number of information bits	Number of parity bits	Redundancy percentage
2	3	150.0%
4	3	75.0
6	4	66.7
8	4	50.0
10	4	40.0
12	5	41.7
16	5	31.25
24	5	20.8
32	6	18.75
64	7	10.9

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

31

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error correction using overlapping parity

Fig. 3.31 Error correction using overlapped parity.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

32

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Syndrome and Costs

- ✓ Output of 3-8 decoder called syndrome bits
 - Indicates which of several possible bit flips occurred
- ✓ High Cost – 75% redundancy (3 parity bits for a 4-bit word). Cost goes down as information content increases.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

33

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

m-of-n codes

TABLE 3.5 3 of-6 code for representing three bits of information

Original information	3-of-6 code
000	000 111
001	001 110
010	010 101
011	011 100
100	100 011
101	101 010
110	110 001
111	111 000

Original information Appended information

- ✓ m-of-n codes define code words that are n bits in length and contain exactly m 1s
 - ✓ Example: 3-of-6
- ✓ Single Bit Errors – Erroneous word has m+1 or m-1 ones -- conceptually simple
- ✓ Disadvantage – Encoding, decoding, detection of fault difficult and complex
- ✓ Easiest Implementation:
 - i-of-2i code:
 - Take the original i-bits of information and append i bits such that the resulted code word has exactly i 1s

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

34

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Duplication codes

- ✓ Duplication codes are based on the concept of completely duplicating the original information to form the code word.
 - Simply append the original i bits of information to itself: code of length 2i
 - If an error occurs, the two halves disagree
- ✓ Advantage: simple to encode/decode and detect errors
- ✓ Disadvantage: 100% redundancy
- ✓ Application
 - Memory systems
 - Communication systems

Word 4
Word 3
Word 2
Word 1

Word 7 = complement of 4th word of original data

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

35

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Complemented duplication in a communication system

Fig. 3.33 Example of complemented duplication for error detection in a communication system.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

36

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Swap and compare duplication codes

- ✓ Maintain two copies of the original information, but swap the upper and lower halves of the second copy
- ✓ A single bit slice that is faulty affects the upper half of one copy of the information and the lower half of the other copy
 - By comparing the appropriate halves, the error can be detected

U1 = Upper Half of Word 1
L1 = Lower Half of Word 1

Single Faulty Bit Slice

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

37

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Checksum codes

- ✓ **Checksum:** sum of the original data, appended to the block of data
- ✓ Separable code applicable when blocks of data are transferred from one point to another
- ✓ Checksums cannot correct errors
- ✓ Four types of checksums
 1. Single-precision
 2. Double-precision
 3. Honeywell
 4. Residue checksums

Fig. 3.35 In checksum coding, the sum of the original data words is appended to the block of data.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

38

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Single-precision checksum

Fig. 3.36 A single-precision checksum is formed by adding the data words and ignoring any overflow.

Fig. 3.37 The single-precision checksum is unable to detect certain types of errors. The received checksum and the checksum of the received data are equal, so no error is detected.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

39

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Double-precision checksums

Fig. 3.38 A double-precision checksum is formed by adding the data using double-precision arithmetic. The received checksum and the checksum of the received data are not equal, so the error is detected.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

40

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Honeywell checksum

- ✓ Concatenate consecutive words to form a collection of double-length words.
 - The checksum is formed over the new double-length words
- ✓ If a complete column of the original data is erroneous, the modified data structure has two erroneous columns

Fig. 3.39 In the Honeywell checksum, adjacent data words are concatenated prior to forming the checksum.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

41

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error detection using Honeywell checksums

Fig. 3.40 Illustration of the error detection capability of the Honeywell checksum. The received checksum and the checksum of the received data are not equal, so the error is detected.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

42

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Residue checksums

✓ Residue checksums are similar with single-precision checksums, except that the most significant bit position is not ignored but is added back to the checksum in an end-around carry fashion.

Fig. 3.41 The residue checksum is formed using end-around carry addition so that information in the carry bit is not lost.

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

43

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error detection using residue checksums

Fig. 3.42 Illustration of the error detection capability of the residue checksum. The checksum of the received data and the received checksum are not equal, so the error is detected.

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

44

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Cyclic Codes

- ✓ Cyclic codes are special class of linear codes
- ✓ Used in applications where burst errors can occur
 - a group of adjacent bits is affected
 - digital communication, storage devices (disks, CDs)
- ✓ Important classes of cyclic codes:
 - Cyclic redundancy check (CRC)
 - Used in modems and network protocols
 - North-America T-carrier standard uses Extended-SuperFrame (ESF) cyclic code. Coding frame of 4632 bits. Detects 98,4% single or multiple errors
 - Reed-Solomon code
 - Used in CD and DVD players
 - CDs: up to 4000 consecutive errors can be corrected (2,5 mm of track)

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

45

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Cyclic codes

TABLE 3.7 Cyclic code words for 4-bit information words.

Information (d_3, d_2, d_1, d_0)	Code ($v_7, v_6, v_5, v_4, v_3, v_2, v_1, v_0$)
0000	0000000
0001	0001101
0010	0011010
0011	0010111
0100	0110100
0101	0111001
0110	0101110
0111	0100011
1000	1101000
1001	1100101
1010	1110010
1011	1111111
1100	1011100
1101	1010001
1110	1000110
1111	1001011

Data polynomial = $d_3 + d_2x + d_1x^2 + d_0x^3$
 Generator polynomial = $1 + x + x^3$
 Code polynomial = $v_7 + v_6x + v_5x^2 + v_4x^3 + v_3x^4 + v_2x^5 + v_1x^6 + v_0x^7$

- ✓ Cyclic code: the end-around shift of a code word will produce another code word
 - n bits in the original, k in the code
 - Called (n, k) cyclic code
- ✓ Simple encoding
 - Shift registers with feedback connections
- ✓ Can detect n-k adjacent errors
 - Burst errors

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

46

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Cyclic code polynomial

TABLE 3.7 Cyclic code words for 4-bit information words.

Information (d_3, d_2, d_1, d_0)	Code ($v_7, v_6, v_5, v_4, v_3, v_2, v_1, v_0$)
0000	0000000
0001	0001101
0010	0011010
0011	0010111
0100	0110100
0101	0111001
0110	0101110
0111	0100011
1000	1101000
1001	1100101
1010	1110010
1011	1111111
1100	1011100
1101	1010001
1110	1000110
1111	1001011

Data polynomial = $d_3 + d_2x + d_1x^2 + d_0x^3$
 Generator polynomial = $1 + x + x^3$
 Code polynomial = $v_7 + v_6x + v_5x^2 + v_4x^3 + v_3x^4 + v_2x^5 + v_1x^6 + v_0x^7$

- ✓ Data polynomial
 - $D(X) = d_0 + d_1x + d_2x^2 + d_3x^3$
- ✓ Generator polynomial
 - $G(X) = 1 + x + x^3$
- ✓ Cyclic code generation:
 - $V(X) = D(X) * G(X)$
 - Modulo-2 addition!
- ✓ $V(X)$ is the code polynomial
 - $V(X) = v_0 + v_1x + v_2x^2 + v_3x^3 + v_4x^4 + v_5x^5 + v_6x^6 + v_7x^7$

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

47

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Encoding

Fig. 3.43 Example circuit for generating a cyclic code word by multiplying an incoming data polynomial $D(X)$ by the generator polynomial.

Legend:
 $\otimes$ = Multiplication by X
 $\oplus$ = Modulo-2 Addition

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

48

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Encoding, cont.

TABLE 3.8 The encoding process for the circuit of Fig. 3.44

Clock period	Register values 1 2 3	$D(x)$	$V(x)$
0	0 0 0	0	1
1	1 0 1	1	0
2	1 1 1	1	0
3	0 1 1	0	1
4	1 0 0	0	0
5	0 1 0	0	0
6	0 0 1	0	0
7	0 0 0	0	1

Fig. 3.44 Circuit for generating cyclic code words for the generator polynomial $G(X) = 1 + X + X^3$.

49

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Decoding and error detection

Fig. 3.45 A division circuit for use in decoding cyclic code words.

- ✓ Decoding is done through division
 - Data is obtained by dividing $V(X) / G(X)$
 - The circuit in the figure implements the division
- ✓ Syndrome polynomial $S(X)$ is zero in case of no error
 - $R(X) = D(X)G(X) + S(X)$

50

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Decoding and error detection, cont.

Fig. 3.46 Decoding circuit for the cyclic code with generator polynomial, $G(X) = 1 + X + X^3$.

51

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Decoding and error detection, cont.

TABLE 3.9 The decoding process for the circuit of Fig. 3.46

Clock period	Register values 1 2 3	$V(x)$	$R(x)$	$D(x)$
0	0 0 0	1	0	1
1	0 0 1	0	1	1
2	0 1 1	1	1	0
3	1 1 1	0	1	1
4	1 0 1	0	0	0
5	0 1 0	0	0	0
6	1 0 0	1	1	0
7	0 0 0	1	0	1

TABLE 3.10 The decoding process with erroneous information

Clock period	Register values 1 2 3	$V(x)$	$R(x)$	$D(x)$
0	0 0 0	1	0	1
1	1 0 0	1	0	1
2	0 1 1	1	1	0
3	1 1 1	0	1	1
4	1 0 1	0	0	0
5	0 1 0	0	0	0
6	0 0 1	1	1	0
7	1 1 0	1	1	0

52

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Reed-Solomon Code

- ✓ Reed-Solomon (RS) codes are a class of separable cyclic codes used to correct errors in a wide range of applications including
 - storage devices (tapes, compact disks, DVDs, bar-codes)
 - wireless communication (cellular telephones, microwave links)
 - satellite communication, digital television, high-speed modems (ADSL, xDSL)

53

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Reed-Solomon Code

- ✓ The encoding for Reed-Solomon code is done the using the usual procedure
 - codeword is computed by shifting the data right $n-k$ positions, dividing it by the generator polynomial and then adding the obtained remainder to the shifted data
- ✓ A key difference is that groups of m bits rather than individual bits are used as symbols of the code.
 - usually $m = 8$, i.e. a byte

54

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Encoding

- ✓ An encoder for an RS code takes k data symbols of s bits each and computes a codeword containing n symbols of m bits each
- ✓ A Reed-Solomon code can correct up to $n-k/2$ symbols that contain errors

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

55

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Example: RS(255,223) code

- ✓ A popular Reed-Solomon code is RS(255,223)
 - symbols are a byte (8-bit) long
 - each codeword contains 255 bytes, of which 223 bytes are data and 32 bytes are check symbols
 - $n = 255$, $k = 223$, this code can correct up to 16 bytes containing errors
 - each of these 16 bytes can have multiple bit errors.

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

56

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Decoding

- ✓ Decoding of Reed-Solomon codes is performed using an algorithm designed by Berlekamp
 - popularity of RS codes is due to efficiency this algorithm to a large extent.
 - This algorithm was used by Voyager II for transmitting pictures of the outer space back to Earth
 - Basis for decoding CD in players

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

57

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Summary of Cyclic Codes

- ✓ Any end-around shift of a codeword produce another codeword
- ✓ Code is characterized by its generator polynomial $g(x)$, with a degree $(n-k)$, n = bits in codeword, k = bits in data word
- ✓ Detect all single errors and all multiple adjacent error affecting $(n-k)$ bits or less

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

58

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Arithmetic codes

- ✓ Arithmetic codes are invariants to (a set of) arithmetic operations
 - $A(b <op> c) = A(b) <op> A(c)$
- ✓ Application
 - Checking arithmetic operations
- ✓ Examples of arithmetic codes
 - AN codes
 - Residue codes
 - Inverse-residue codes
 - Residue number system

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

59

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

AN codes

TABLE 3.11 Resulting $3N$ code words for 4-bit information words

Original information	$3N$ code word
0000	000000
0001	000011
0010	000110
0011	001001
0100	001100
0101	001111
0110	010010
0111	010101
1000	011000
1001	011011
1010	011110
1011	100001
1100	100100
1101	100111
1110	101010
1111	101101

- ✓ AN code is formed by multiplying each data word N by some constant A
 - The magnitude of A determines the number of extra bits required to represent the code words and the error detection capability
- ✓ AN codes are invariant to addition and subtraction but not multiplication and division
- ✓ Example code: $3N$
 - The constant must not be a power of 2
 - Power of 2 is a shift, difficult to detect the error
 - $3N$ requires $n+2$ bit words

TALLINNA TEHNIKAILIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

60

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

AN codes encoding: $3N = 2N + N$

Fig. 3.48 Illustration of the use of an $(n + 1)$ -bit adder to create $3N$ code words.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error detection using AN codes

Normal Operation

If S_i is always "1"

Fig. 3.47 Illustration of the error detection capabilities of the $3N$ arithmetic code. The presence of the fault results in the sum being an invalid $3N$ code.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error detection circuit for AN codes

Karnaugh Map for Decoder

Fig. 3.49 A simple error detection circuit for the $3N$ code can be constructed using combinational logic.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Residue codes

✓ A residue code is a separable arithmetic code created by appending the residue (remainder) of a number to that number

TABLE 3.12 Residue code words for 4-bit information words using a modulus of three

Information	Residue	Code word
0000	0	0000 00
0001	1	0001 01
0010	2	0010 10
0011	0	0011 00
0100	1	0100 01
0101	2	0101 10
0110	0	0110 00
0111	1	0111 01
1000	2	1000 10
1001	0	1001 00
1010	1	1010 01
1011	2	1011 10
1100	0	1100 00
1101	1	1101 01
1110	2	1110 10
1111	0	1111 00

Code = $D \mid R$, where R is the remainder of the division with an integer m

The number of bits in R depend on m

Residue codes are invariant to addition

Low-cost residues:
 $m = 2b - 1$, b at least 2
 R requires b bits
 Easy to encode: division is Modulo-3 addition
 Decoding simply removes R

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Adder using residue codes

Fig. 3.50 The structure of an adder designed using the separable residue code.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Residue calculation for low-cost residues

Information to be Encoded = (10100111)
 Modulus = 3
 $b = 2$

10100111 (167₁₀)

Modulo-3 Addition

(Residue = 2)

Fig. 3.51 The residue calculation for a low-cost residue code can be performed using successive additions.

TALLINNA TEHNIKAKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Inverse residue codes

✓ An **inverse residue code** is similar to a residue code, but instead of appending the residue, the inverse residue **Q** is calculated and appended

- $Q = m - R$

✓ Better fault detection for repeated faults

- A repeated fault is encountered multiple times before the code is checked
- Difficult to detect because subsequent effects can cancel the previous effects of the fault

TABLE 3.13 Inverse-residue code words for 4-bit information words using a modulus of three

Information	Residue	Inverse residue	Code
0000	0	3	0000 11
0001	1	2	0001 10
0010	2	1	0010 01
0011	0	3	0011 11
0100	1	2	0100 10
0101	2	1	0101 01
0110	0	3	0110 11
0111	1	2	0111 10
1000	2	1	1000 01
1001	0	3	1001 11
1010	1	2	1010 10
1011	2	1	1011 01
1100	0	3	1100 11
1101	1	2	1101 10
1110	2	1	1110 01
1111	0	3	1111 11

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

67

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Berger codes

✓ **Berger codes** are formed by appending a special set of bits, called check bits, to each word of information

Berger code of length n

- I information bits
- k check bits
- $k = \lceil \log_2(I + 1) \rceil$
- $n = I + k$
- A code word is formed by first creating a binary number that corresponds to the number of 1s in the original I bits of information.
- The resulting binary number is complemented and appended to the I information bits to form the $(I+k)$ -bit code word.

TABLE 3.16 Berger code words for 4-bit information words

Original information	Berger code
0000	0000 111
0001	0001 110
0010	0010 110
0011	0011 101
0100	0100 110
0101	0101 101
0110	0110 101
0111	0111 100
1000	1000 110
1001	1001 101
1010	1010 101
1011	1011 100
1100	1100 101
1101	1101 100
1110	1110 100
1111	1111 011

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

68

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Berger codes, cont.

✓ If the number of information bits is small, the redundancy is high,

✓ As the number of information bits increases, the efficiency improves substantially.

✓ Advantages

- Best separable code (fewest number of bits) considering its error detection capabilities
- Detects multiple, unidirectional errors

TABLE 3.15 Number of required check bits in a Berger code

Number of information bits	Number of check bits	Percentage redundancy
4	3	75.00%
8	4	50.00
16	5	31.25
32	6	18.75
64	7	10.94

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

69

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Horizontal and vertical parity

Fig. 3.56 Vertical and horizontal parity uses a parity bit for each row and each column. If bit d_{11} , for example, becomes in error, both P_{01} and P_{11} will be erroneous. All other parity bits will be correct.

- ✓ Can detect multiple errors in groups of data words
- ✓ Can correct single-bit errors
- ✓ Cannot correct **multiple** errors

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

70

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Hamming codes

✓ The hamming codes are similar to overlapping parity codes.

✓ The Hamming code is formed by partitioning the information bits into parity groups and specifying a parity bit for each group.

- uses c parity check bits to protect k bits of information
- $2^c \geq c + k + 1$

✓ The ability to locate which bit is faulty is obtained by overlapping the groups of bits.

TABLE 3.17 Check bits affected by single data bit errors

Erroneous bit	Check bits affected
d_0	c_1, c_2
d_1	c_1, c_3
d_2	c_2, c_3
d_3	c_1, c_2, c_3
c_1	c_1
c_2	c_2
c_3	c_3

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

71

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Single-bit error correction unit

TABLE 3.18 Resulting syndromes for each possible single bit error

Erroneous bit	Syndromes
d_0	110
d_1	101
d_2	011
d_3	111
c_1	100
c_2	010
c_3	001

Syndrome $\begin{pmatrix} S_1 \\ S_2 \\ S_3 \end{pmatrix}$ Controlled Complementation Unit Syndrome Determines Which Bit (if any) is Complemented

Corrected Bits $d_0, d_1, d_2, d_3, c_1, c_2, c_3$

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

72

Hamming correction in memories

- ✓ Memory: 60 to 70% of the faults in a system
 - Transient faults are becoming much more prevalent as memory chips become denser
- ✓ Many memory designs use hamming error correction
 - Relatively inexpensive: 10-40% redundancy
 - Encoding and the decoding are fast
 - Error correction circuit is readily available on inexpensive chips

Hamming correction in memories, cont.

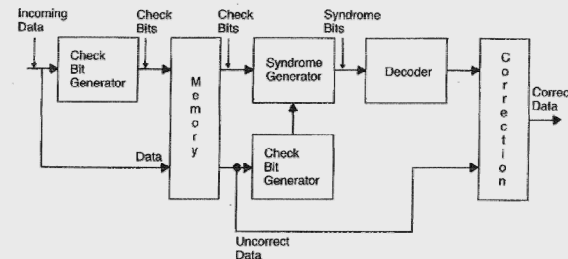
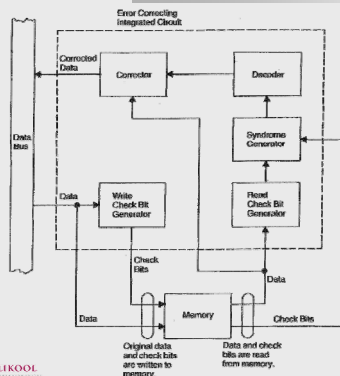


Fig. 3.59 Basic structure of a memory using Hamming single error correcting code.

Error correction in commercial circuits



Code selection issues

- ✓ Fulfills the desired error detection/correction while maintaining costs at an acceptable level
 - Cost of a code
 - Redundancy required; time redundancy is also considered
 - Effectiveness of a code
 - Number of bit errors detected/corrected
- ✓ Key design decisions
 - Separable or not
 - What is required? Detection, correction, both?
 - Number of bit errors to be detected/corrected

Information redundancy

- ✓ Self-Checking
 - This is a form of hardware redundancy but often it is closely related to ECC techniques, therefore I have chosen to include it here
 - Assumptions: inputs are coded and outputs are coded
 - Objective: in the presence of a fault the circuit should either continue to provide correct output(s) or indicate by providing an error indication that there is a fault.
 - Clearly error indication can not be 1-bit output (why?)
 - With 2-bits output, 00 and 11 may indicate no failure
 - other output combinations (10, 01) may indicate a failure

Self-Checking (contd.)

- ✓ Example application
 - two devices produce identical outputs and we compare these outputs to check their equality
 - checker has two outputs encoded as follows
 - 00 equal
 - 11 unequal
 - 01 or 10 possible fault in the circuit
 - (we will discuss input encoding when we discuss an example of a 2-rail 1-bit checker)

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Self-Checking (contd.)

- Definitions
 - a circuit is fault secure if in the presence of a fault, the output is either always correct, or not a code word for valid input code words
 - a circuit is self-testing if only valid inputs can be used to test it for the faults
 - a circuit is totally self-checking if it is fault secure and self-testing
- Example: a totally self-checking 2-rail 1-bit comparator
 - assumptions
 - 2 inputs and each input x is available as x and its complement
 - x and its complement are independently generated
 - note with these assumption the input space is encoded (4 valid inputs out of 16 possible inputs)
 - single stuck-at fault model

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 79

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Time redundancy

- ✓ Disadvantages of hardware and information redundancy
 - Require large amounts of extra hardware for their implementation.
- ✓ Time redundancy: reduce the extra hardware at the expense of using additional time.
 - Hardware is a physical entity that impacts weight, size, power consumption and cost.
 - Time may be readily available in some applications.

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 80

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Time redundancy

- ✓ Key Concept - do a job more than once over time
 - examples
 - re-execution
 - re-transmission of information
 - different faults and capabilities of different schemes
 - transient faults
 - re-execution and re-transmission can detect such faults provided we wait for transient to subside
 - permanent faults
 - simple re-execution or re-transmission will not work. Possible solutions
 - send or process shifted version of data
 - send or process complemented data during second transmission

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 81

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Time redundancy

- ✓ Different faults and capabilities of different schemes (contd.)
 - faults in ALU
 - re-execution with complement or shifted version can detect permanent and transient faults
 - (RESO concept - re-computation with shifted operands)
 - multiple re-computations
 - can detect and possibly correct transient and permanent faults if properly employed/designed

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 82

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Time redundancy: transient fault detection

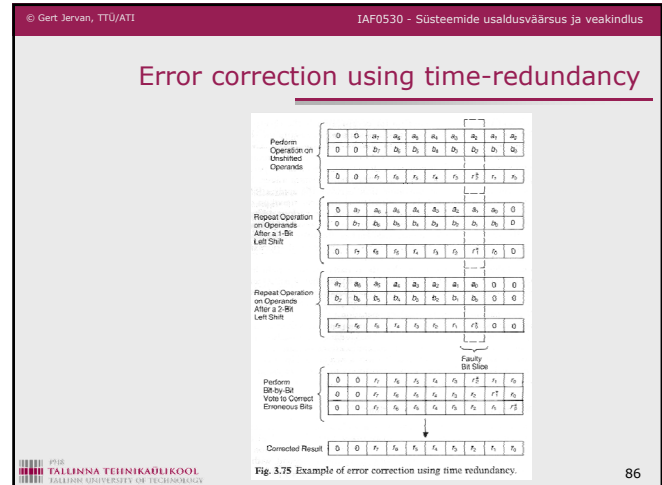
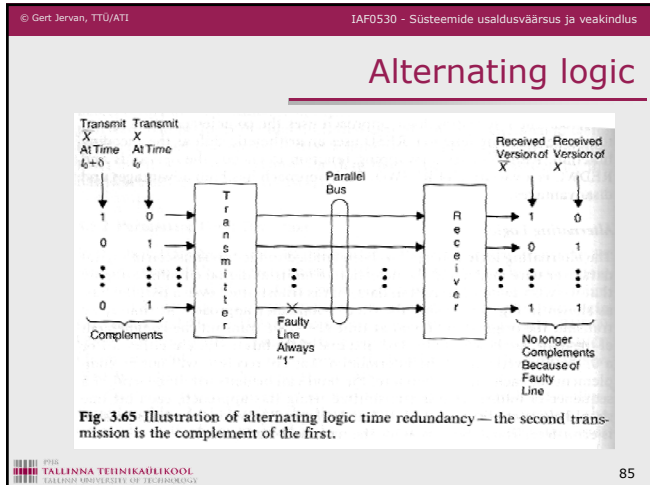
Fig. 3.62 In time redundancy, computations are repeated at different points in time and then compared.

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 83

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Time redundancy: permanent fault detection

PTIS TALLINNA TEHNIKALÜKOOUL TALLINN UNIVERSITY OF TECHNOLOGY 84



© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Environment Diversity

- ✓ To diversify the software operating circumstance temporarily.
- ✓ The typical examples of environment diversity technique are progressive retry, rollback, rollforward, recovery with checkpointing, restart, hardware reboot, etc.

TALLINNA TEHNIKALIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

87

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Adjudicators

- ✓ Voter
- ✓ AT
- ✓ Hybrid, other

TALLINNA TEHNIKALIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

88

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

What's new

- ✓ Modifications to Traditional Techniques
 - Adaptive N-version Systems
 - Fuzzy Voting
 - Abstraction
 - Parallel Graph Reduction
- ✓ New Concepts (Not Classifiable in Data or Design Diversity)
 - Rejuvenation

TALLINNA TEHNIKALIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

89

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Why Adaptive

- ✓ Defective components should be removed from the voting process
- ✓ The voting procedure can be adaptively modified and tailored to the fault state of the overall system

TALLINNA TEHNIKALIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

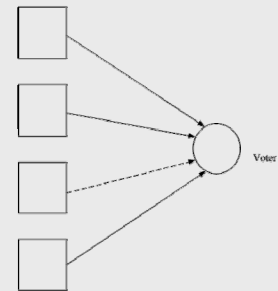
90

An Adaptive Approach for n-Version Systems

- ✓ Model and manage different quality levels of the versions by introducing an individual weight factor to each version of the n-version system.
- ✓ This weight factor is then included in the voting procedure, i.e. the voting is based on a weighted counting.

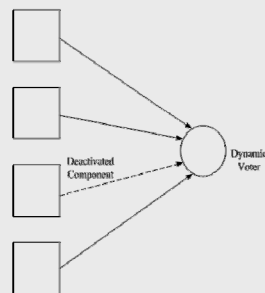
Voting schemes

- ✓ Static voting:
fixed number of versions



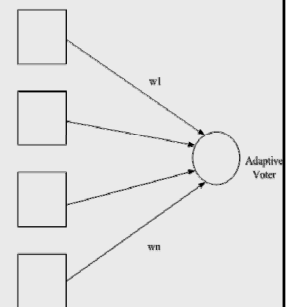
Voting schemes

- Dynamic voting:
defective components
are removed from
the voting
process



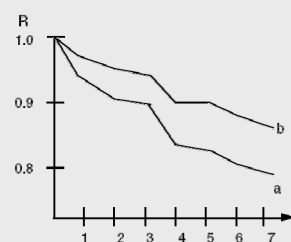
Voting schemes

- Adaptive voting:
versions have
dynamically
changeable
weight factors



Example

- ✓ Cumulated reliability of 7 components of a software system for a satellite control application
 - a) classical 3-version system
 - b) 3-version system with adaptive weight factors



Why Fuzzy Voting

- ✓ In traditional voting, equality relation regards two real numbers as equal if their difference is smaller than fixed tolerance ϵ . For different version outputs that are "closer" to each other than the fixed threshold there is no gradual comparison. As a result, certain interconnection of faults could incur incorrect selection.
- ✓ Fuzzy equivalence relation results in more reliable systems

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Fuzzy Equality Equation

- ✓ Traditional Equality Equation

$$r_{i,j} = \begin{cases} 1, & \text{if } |x_i - x_j| \leq \varepsilon \\ 0, & \text{otherwise} \end{cases}$$
- ✓ Fuzzy Equality Equation

$$\mu_{A_i}(x_i) = \begin{cases} 1 - \frac{|a_i - x_i|}{\varepsilon/2}, & \text{if } |x_i - a_i| \leq \varepsilon/2 \\ 0, & \text{otherwise} \end{cases}$$

TALLINNA TEHNIKAKÜLKOO
TALLINN UNIVERSITY OF TECHNOLOGY

97

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Output of Fuzzy Sets (Triangular Shape)

- ✓ The fuzzy logic maps the input vector into an output nonlinearly

TALLINNA TEHNIKAKÜLKOO
TALLINN UNIVERSITY OF TECHNOLOGY

98

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Why Abstraction Improve Fault Tolerance

- ✓ Reduce the cost of fault tolerance
- ✓ Improve its ability to mask software errors.

TALLINNA TEHNIKAKÜLKOO
TALLINN UNIVERSITY OF TECHNOLOGY

99

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

An Example of Abstraction: BASE

- ✓ Byzantine fault tolerance (BFT) with Abstract Specification Encapsulation (BASE)

TALLINNA TEHNIKAKÜLKOO
TALLINN UNIVERSITY OF TECHNOLOGY

100

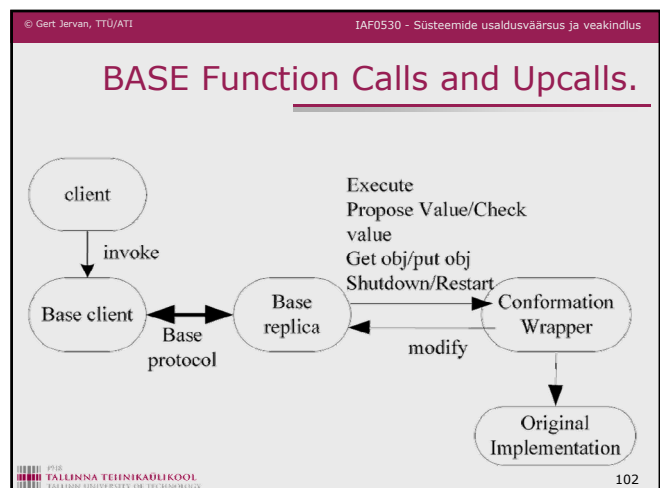
© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

How BASE Works

- ✓ BASE reduces cost because it enables reuse of off-the-shelf service implementations.
- ✓ It improves availability because each replica can be repaired periodically using an abstract view of the state stored by correct replicas, and because each replica can run distinct or nondeterministic service implementations, which reduces the probability of common mode failures.

TALLINNA TEHNIKAKÜLKOO
TALLINN UNIVERSITY OF TECHNOLOGY

101



© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Modifications to Traditional Techniques

- ✓ Adaptive N-version systems
- ✓ Fuzzy Voting
- ✓ Abstraction
- ✓ Parallel Graph Reduction

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

103

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Parallel Graph Reduction

- ✓ Fault-tolerance of functional programs in parallel computing

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

104

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Why Parallel Graph Reduction

- ✓ Reduce time overhead of fault tolerance by taking advantage of referential transparency.

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

105

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

An Example of Graph Reduction

- ✓ A program is a graph --- Graph " $f(x)*g(y)$ "
- ✓ Execution of program --- Graph Reduction

Assuming that $f(x)=3$, $g(y)=7$
@ application node

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

106

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

An Example of Parallel Graph Reduction

Task A Task B

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

107

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

System Architecture

- ✓ Each subgraph is assigned to each node and reduced in parallel
- ✓ A task is executed in a node and its backup is stored in another node

Parallel Functional Program

Task(Redundancy)
Message Passing Library
Stable Storage

Node

TALLINNA TEHNIKAKÜLKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

108

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Backup Procedure

- ✓ Transmission
- ✓ Backup
- ✓ Reduction

109

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Error Recovery

- ✓ Rollback
- ✓ Retransmission
- ✓ Checkpointing
- ✓ Reduction

110

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Software Aging

- ✓ When software application executes continuously for long periods of time, some of the faults cause software appear to age due to the error conditions that accrue with time and/or load. This phenomenon is called software aging which is reported in
 - Telecommunication billing application over time experiences a crash or a hang failure.
 - A telecommunication switching software
 - Netscape and xrm
 - Safety critical systems Patriot missile's software, where the accumulated errors led to a failure that resulted in loss of human lives.

111

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Discussion

- ✓ Each software fault tolerance technique need to be tailored to particular applications.
- ✓ This should also be based on the cost of the fault tolerance effort required by the customer. The differences between each technique provide some flexibility of application.

112

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

Summary

- ✓ Hardware redundancy
 - passive, active, and hybrid
- ✓ Information redundancy
 - coding method and self-checking
- ✓ Time redundancy
- ✓ Software redundancy
 - N-version programming, recovery block, N-self checking, ...

113

© Gert Jervan, TTÜ/ATI IAF0530 - Süsteemide usaldusväärsus ja veakindlus

A summary chart of all techniques

114