

OBSAH

<u>Předmluva</u>	3
<u>Obsah</u>	5
<u>1. kapitola: Informace a kódování</u>	9
1.1 Kódování a informační obsah zprávy	9
1.2 Komprimace zprávy	11
1.3 Ochrana zprávy proti šumu	12
1.4 Entropie zdroje zpráv	12
1.5 Řešené příklady	16
<u>2. kapitola: Nerovnoměrné kódy</u>	19
2.1 Bezztrátové kódování	19
2.2 Binární nerovnoměrné kódování	20
2.3 Prefixové kódy	21
2.4 Huffmanova konstrukce kódu	21
2.5 Redundance zprávy	23
2.6 Shannonova věta o kódování bez šumu	24
2.7 Ztrátová komprese	26
2.7.1 Definice pojmů diskrétního obrazu	26
2.7.2 Vytváření diskrétního obrazu	27
2.7.3 Aplikace kosinové transformace	29
2.7.4 Aplikace nerovnoměrného (Huffmanova) kódu	31
2.8 Příklady	32
<u>3. kapitola: Sdělovací kanál</u>	33
3.1 Sdělovací kanál bez paměti	33
3.2 Informační poměr kódu	34
3.3 Hammingova vzdálenost	35
3.4 Kapacita kanálu	36
3.5 Shannonova věta o kódování za přítomnosti šumu	37
3.6 Ochrana zprávy před působením šumu	38
3.7 Řešené příklady	40
<u>4. kapitola: Blokované kódy</u>	41
4.1 Lineární binární kódy	41
4.2 Maticový popis kódování, generující matice kódu	42
4.3 Kontrolní matice	43
4.4 VHDL model kodéru a dekodéru kódu celkové parity	43
4.4.1 Model propojení	45
4.4.2 Model chování	45
4.4.3 Aplikace kódu celkové parity - Disková pole	46
4.5 Hammingův kód	48
4.5.1 Algoritmické vytváření kódových slov	50
4.5.2 Opravování kódových slov	51
4.6 VHDL model kodéru a dekodéru Hammingova kódu	52
4.6.1 Kodér Hammingova kódu	52
4.6.2 Dekodér Hammingova kódu	53
4.7 Rozšířený Hammingův kód	53

4.8	Řešené příklady	54
4.9	Zobecnění lineárních kódů: Reedovy-Mullerovy kódy	56
4.9.1	Boolovské mnohočleny	56
4.9.2	Reedovy-Mullerovy kódy	57
4.9.3	Dekódování Reedových-Mullerových kódů	58
4.9.4	Aplikace Reedových-Mullerových kódů	59
5. kapitola: Cyklické kódy		61
5.1	Popis pomocí mnohočlenů	61
5.2	Generující mnohočlen	62
5.3	Nesystematické a systematické kódování	63
5.4	Kontrolní mnohočlen	66
5.5	Dekódování cyklických kódů	69
5.6	Meggittův dekodér	70
5.7	Řešené příklady	74
6. kapitola: BCH-kódy		75
6.1	Kódy pro opravy dvou a více chyb	75
6.2	Generující mnohočlen BCH-kódu	76
6.3	Kódování BCH-kódů	77
6.4	Dekódování BCH-kódů	77
6.5	Oprava chyb u BCH-kódů	78
6.6	Aplikace BCH-kódů	79
6.7	Meggittův dekodér BCH-kódu	80
7. kapitola: Reedovy-Solomonovy kódy		83
7.1	Definice RS-kódů	83
7.2	RS-kódy: kódy pro opravu shlukových chyb	84
7.3	Aplikace RS-kódů při zabezpečení polovodičových pamětí	84
7.4	Aplikace RS-kódů při zabezpečení optických diskových pamětí	86
7.5	Dekódování RS-kódů při čtení CD	88
8. kapitola: Konvoluční kódy		89
8.1	Vlastnosti konvolučního kódování	89
8.2	Rozdíl v popisu konvolučních kódů a kodérů	90
8.3	Definice konvolučního kódu	90
8.4	Definice kodéru konvolučního kódu	92
8.5	Minimální kódová vzdálenost konvolučního kódu	94
8.6	Dekódování konvolučního kódu	94
8.7	Některé jednoduché konvoluční kódy	95
8.8	Kódování konvolučního WA-kódu pro TV	96
8.9	Dekódování konvolučního WA-kódu	100
8.10	Srovnání účinnosti Hammingova kódu a WA-kódu pro TV	102
9. kapitola: Kryptografie		105
9.1	Moderní kryptosystémy	105
9.2	Kódování tajných zpráv pomocí bezpečnostních kódů	106
9.3	Šifrování s tajným klíčem	108
9.4	Šifrování algoritmem DES (Data Encryption Standard)	111
10. kapitola: Praktické použití algoritmu DES		117
10.1	Modifikace algoritmu DES	117

10.2	Použití a implementace algoritmu DES	118
10.3	Výpočetní jádro DES	119
10.4	Rozhraní obvodu pro DES	120
10.5	Modifikace algoritmu DES	120
10.6	Obvodové řešení DES	123
Příloha A: Doporučení MPEG 2		125
A.1	Kompresce pomocí soustavy MPEG 2	125
A.2	Transformační kódování	126
A.3	Kosinová transformace	127
A.4	Kvantování frekvenčních koeficientů	128
A.5	Entropické kódování	129
Příloha B: Návrh obvodů pomocí VHDL		131
B.1	Programovatelné logické obvody	131
B.1.1	Obvodový návrh	131
B.1.2	Systémový návrh	132
B.1.3	Technologický návrh	132
B.1.4	Vznik VHDL	132
B.2	Strukturované a nestrukturované logické obvody	133
B.3	Normální disjunktivní forma	133
B.4	Kategorizace struktur PLA	134
B.4.1	Vlastnosti PLA (i podle technologie výroby)	135
B.4.2	Obvody CPLD	136
B.5	Sekvenční funkce v CPLD	137
B.6	Optimalizace logických funkcí pro vícenásobné použití jádra PLA	137
B.7	Programovatelná hradlová pole FPGA	138
B.8	Přínos použití VHDL	140
B.9	Entity jako deklarační části modelů VHDL	141
B.10	Styl a hierarchie popisu modelů	142
B.11	Popis chování	143
B.12	Popis struktury	145
B.13	Model diskrétních událostí	147
B.14	Příklady modelů sekvenčních obvodů	148
B.15	Řešení komplexních modelů	150
B.16	Proces	153
B.17	Návrh konečného automatu	154
Příloha C: Galoisova tělesa		161
C.1	Tělesa	161
C.2	Galoisova tělesa	161
C.3	GF(4)	163
C.4	GF(8)	163
C.5	GF(9)	163
C.6	GF(16)	164
C.7	GF(25)	164
C.8	GF(32)	165
Příloha D: Meggitův dekodér		167
D.1	Systematický cyklický kód	167
D.2	Popis kodéru (15,11)-kódu	168

D.3	Vytvoření modelu kodéru	169
D.4	Dekodér (15,11)-kódu	172
D.5	Generování syndromu	173
D.6	Obvod dekodéru	173
D.7	Vytvoření modelu dekodéru	174
D.8	Simulace modelů kodéru a dekodéru	178
<u>Rejstřík</u>	179
<u>Literatura</u>	181