

Obsah

Úvod	7
I. Kódování bez šumu	9
1. Kódování a dekodování	9
2. Konstrukce prefixových kódů	12
3. Nejkratší kód	17
II. Bezpečnostní kódy	26
4. Objevování chyb	27
5. Opravování chyb	29
6. Dekódování	32
7. Informační znaky	33
III. Lineární kódy	36
8. Binární lineární kódy	36
9. Tělesa	39
10. Generující matice	45
11. Kontrolní matice	51
12. Objevování chyb	57
13. Opravování chyb	59
14. Hammingovy kódy — perfektní kódy pro jednoduché opravy	65
15. Golayův kód — perfektní kód pro trojnásobné opravy	70
16. Konstrukce kódů	76
17. Reedovy-Mullerovy kódy — kódy se snadným dekódováním	81
18. Boolovské funkce	81
19. Vlastnosti Reedových-Mullerových kódů	86
19. Dekódování Reedových-Mullerových kódů	91
V. Cyklické kódy	98
20. Okruhy polynomů	99
21. Cyklické kódy a generující polynomy	104
22. Kontrolní polynomy	111
VI. Konečná tělesa a polynomy	114
23. Kořeny polynomů a ireducibilita	114
24. Řád a primitivní prvky	119
25. Charakteristika tělesa	122
26. Minimální polynomy	127
27. Konečná tělesa	132
28. Generující kořeny cyklického kódu	135
VII. BCH kódy — obecné kódy s dobrými parametry	141
29. BCH kód délky 15	141
30. BCH kódy pro dvojnásobné opravy	143

31. Binární BCH kódy	146
32. Dekódování BCH kódů I: maticová metoda	151
33. BCH Kódy a Reedovy-Solomonovy kódy.....	159
34. Dekódování BCH kódů II: Euklidův algoritmus	165
VII. Kódování tajných zpráv	174
35. Nekvalitní odposlech.....	174
36. Kvalitní odposlech.....	175
37. Šifrování s veřejně přístupným klíčem	178
Dodatky	185
A1. Galoisova tělesa	185
A2. Přehled BCH kódů a Reedových-Mullerových kódů	187
Doporučená literatura a odkazy.....	189
Rejstřík	190