Contents

Preface i

Introduction 1

1 Block Error-correcting Codes 13
1.1 Basic concepts 14
1.2 Linear codes 34
1.3 Hadamard codes 63
1.4 Parameter bounds 78

2 Finite Fields 101
2.1 $\mathbb{Z}_n$ and $\mathbb{F}_p$ 103
2.2 Construction of finite fields 108
2.3 Structure of the multiplicative group of a finite field 124
2.4 Minimum polynomial 133

3 Cyclic Codes 141
3.1 Generalities 142
3.2 Effective factorization of $X^n - 1$ 154
3.3 Roots of a cyclic code 164
3.4 The Meggitt decoder 173

4 Alternant Codes 179
4.1 Definitions and examples 180
4.2 Error location, error evaluation and the key equation 195
4.3 The Berlekamp–Massey–Sugiyama algorithm 203
4.4 The Peterson–Gorenstein–Zierler algorithm 215

Appendix: The WIRIS/*cc* system 221
Index of Symbols 237
Alphabetic Index, Glossary and Notes 240