

# Notes on Coding Theory

J.I.Hall  
Department of Mathematics  
Michigan State University  
East Lansing, MI 48824 USA

9 September 2010



# Preface

These notes were written over a period of years as part of an advanced undergraduate/beginning graduate course on Algebraic Coding Theory at Michigan State University. They were originally intended for publication as a book, but that seems less likely now. The material here remains interesting, important, and useful; but, given the dramatic developments in coding theory during the last ten years, significant extension would be needed.

\*\*\* concatenated codes, erasure correcting, *LDPC* codes, iterative decoding, codes on graphs, Viterbi, turbo-codes \*\*\*

The oldest sections are in the Appendix and are over ten years old, while the newest are in the last two chapters and have been written within the last year. The long time frame means that terminology and notation may vary somewhat from one place to another in the notes. (For instance,  $\mathbf{Z}_p$ ,  $\mathbb{Z}_p$ , and  $\mathbb{F}_p$  all denote a field with  $p$  elements, for  $p$  a prime.)

There is also some material that would need to be added to any published version. This includes the graphs toward the end of Chapter 2, an index, and in-line references. You will find on the next page a list of the reference books that I have found most useful and helpful as well as a list of introductory books (of varying emphasis, difficulty, and quality).

These notes are not intended for broad distribution. If you want to use them in any way, please contact me.

Please feel free to contact me with any remarks, suggestions, or corrections:

`jhall@math.msu.edu`

For the near future, I will try to keep an up-to-date version on my web page:

`www.math.msu.edu/~jhall`

Jonathan I. Hall  
3 August 2001

---

The notes were partially revised in 2002. A new chapter on weight enumeration

was added, and parts of the algebra appendix were changed. Some typos were fixed, and other small corrections were made in the rest of the text. I particularly thank Susan Loepp and her Williams College students who went through the notes carefully and made many helpful suggestions.

I have been pleased and surprised at the interest in the notes from people who have found them on the web. In view of this, I may at some point reconsider publication. For now I am keeping to the above remarks that the notes are not intended for broad distribution.

Please still contact me if you wish to use the notes. And again feel free to contact me with remarks, suggestions, and corrections.

Jonathan I. Hall  
3 January 2003

---

Further revision of the notes began in the spring of 2010. Over the years I have received a great deal of positive feedback from readers around the world. I thank everyone who has sent me corrections, remarks, and questions.

Initially this revision consists of small changes in the older notes. I plan to add some new chapters. Also a print version of the notes is now actively under discussion.

Please still contact me if you wish to use the notes. And again feel free to send me remarks, suggestions, and corrections.

Jonathan I. Hall  
9 September 2010

# Contents

Preface	iii
<b>1 Introduction</b>	<b>1</b>
1.1 Basics of communication . . . . .	1
1.2 General communication systems . . . . .	5
1.2.1 Message . . . . .	5
1.2.2 Encoder . . . . .	6
1.2.3 Channel . . . . .	7
1.2.4 Received word . . . . .	8
1.2.5 Decoder . . . . .	9
1.3 Some examples of codes . . . . .	11
1.3.1 Repetition codes . . . . .	11
1.3.2 Parity check and sum-0 codes . . . . .	11
1.3.3 The [7, 4] binary Hamming code . . . . .	12
1.3.4 An extended binary Hamming code . . . . .	13
1.3.5 The [4, 2] ternary Hamming code . . . . .	13
1.3.6 A generalized Reed-Solomon code . . . . .	14
<b>2 Sphere Packing and Shannon's Theorem</b>	<b>15</b>
2.1 Basics of block coding on the $mSC$ . . . . .	15
2.2 Sphere packing . . . . .	18
2.3 Shannon's theorem and the code region . . . . .	22
<b>3 Linear Codes</b>	<b>31</b>
3.1 Basics . . . . .	31
3.2 Encoding and information . . . . .	39
3.3 Decoding linear codes . . . . .	42
<b>4 Hamming Codes</b>	<b>49</b>
4.1 Basics . . . . .	49
4.2 Hamming codes and data compression . . . . .	55
4.3 First order Reed-Muller codes . . . . .	56

<b>5</b>	<b>Generalized Reed-Solomon Codes</b>	<b>63</b>
5.1	Basics . . . . .	63
5.2	Decoding GRS codes . . . . .	67
<b>6</b>	<b>Modifying Codes</b>	<b>77</b>
6.1	Six basic techniques . . . . .	77
6.1.1	Augmenting and expurgating . . . . .	77
6.1.2	Extending and puncturing . . . . .	78
6.1.3	Lengthening and shortening . . . . .	80
6.2	Puncturing and erasures . . . . .	82
6.3	Extended generalized Reed-Solomon codes . . . . .	84
<b>7</b>	<b>Codes over Subfields</b>	<b>89</b>
7.1	Basics . . . . .	89
7.2	Expanded codes . . . . .	90
7.3	Golay codes and perfect codes . . . . .	92
7.3.1	Ternary Golay codes . . . . .	92
7.3.2	Binary Golay codes . . . . .	94
7.3.3	Perfect codes . . . . .	95
7.4	Subfield subcodes . . . . .	97
7.5	Alternant codes . . . . .	98
<b>8</b>	<b>Cyclic Codes</b>	<b>101</b>
8.1	Basics . . . . .	101
8.2	Cyclic <i>GRS</i> codes and Reed-Solomon codes . . . . .	109
8.3	Cyclic alternant codes and <i>BCH</i> codes . . . . .	111
8.4	Cyclic Hamming codes and their relatives . . . . .	117
8.4.1	Even subcodes and error detection . . . . .	118
8.4.2	Simplex codes and pseudo-noise sequences . . . . .	120
<b>9</b>	<b>Weight and Distance Enumeration</b>	<b>125</b>
9.1	Basics . . . . .	125
9.2	MacWilliams' Theorem and performance . . . . .	126
9.3	Delsarte's Theorem and bounds . . . . .	131
9.4	Lloyd's theorem and perfect codes . . . . .	139
9.5	Generalizations of MacWilliams' Theorem . . . . .	149
<b>A</b>	<b>Some Algebra</b>	<b>A-155</b>
A.1	Basic Algebra . . . . .	A-156
A.1.1	Fields . . . . .	A-156
A.1.2	Vector spaces . . . . .	A-160
A.1.3	Matrices . . . . .	A-163
A.2	Polynomial Algebra over Fields . . . . .	A-168
A.2.1	Polynomial rings over fields . . . . .	A-168
A.2.2	The division algorithm and roots . . . . .	A-171
A.2.3	Modular polynomial arithmetic . . . . .	A-174

A.2.4	Greatest common divisors and unique factorization . . . .	A-177
A.3	Special Topics . . . . .	A-182
A.3.1	The Euclidean algorithm . . . . .	A-182
A.3.2	Finite Fields . . . . .	A-188
A.3.3	Minimal Polynomials . . . . .	A-194

