Foreword

This chapter is based on lecture notes from the course CSE 545– Error-Correcting Codes: Combinatorics, Algorithms and Applications taught by Atri Rudra at University at Buffalo, SUNY.

This version is dated **February 29, 2012**. For the latest version, please go to

http://www.cse.buffalo.edu/ atri/courses/coding-theory/book/

The material in this chapter is supported in part by the National Science Foundation under CAREER grant CCF-0844796. Any opinions, findings and conclusions or recomendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

Appendix A

Notation Table

$\mathbb{R}$	The set of real numbers	
$\neg E$	Negation of the event E	
$\log x$	Logarithm to the base 2	
Σ^m	Vectors of length m with symbols from Σ	
$\mathbf{v}$	A vector	
$\mathbf{0}$	The all zero vector	
$\mathbf{e}_i$	The ith standard vector, i.e. 1 in position i and 0 everywhere else	
$\mathbf{v}_S$	Vector $\mathbf{v}$ projected down to indices in S	
$\langle \mathbf{u}, \mathbf{v} \rangle$	Inner-product of vectors $\mathbf{u}$ and $\mathbf{v}$	
$[a, b]$	$\{x \in \mathbb{R} \mid a \leq x \leq b\}$	
$[x]$	The set $\{1, \ldots, x\}$	Section 1.2
n	Block length of a code	Definition 1.2.1
Σ	Alphabet of a code	Definition 1.2.1
q	$q = \lvert\Sigma\rvert$	Definition 1.2.1
k	Dimension of a code	Definition 1.2.2
R	Rate of a code	Definition 1.2.3
$\Delta(\mathbf{u}, \mathbf{v})$	Hamming distance between $\mathbf{u}$ and $\mathbf{v}$	Definition 1.4.1
d	Minimum distance of a code	Definition 1.4.2
$wt(\mathbf{v})$	Hamming weight of $\mathbf{v}$	Definition 1.5.1
$B(\mathbf{x}, r)$	Hamming ball of radius r centered on $\mathbf{x}$	Definition 1.6.1
$(n, k, d)_\Sigma$	A code with block length n, dimension k, distance d and alphabet Σ	Definition 1.7.1
$(n, k, d)_q$	A code with block length n, dimension k, distance d and alphabet size q	Definition 1.7.1
$[n, k, d]_q$	A linear $(n, k, d)_q$ code	Definition 2.0.4
$\mathbb{F}_q$	The finite field with q elements (q is a prime power)	Section 2.1
$\mathbb{F}^*$	The set of non-zero elements in the field $\mathbb{F}$	
$\mathbb{F}_q^{m \times N}$	The set of all $m \times N$ matrices where each entry is from $\mathbb{F}_q$	
$R(C)$	Rate of a code family C	Definition 2.5.1
$\delta(C)$	Relative distance of a code family C	Definition 2.5.1
$\mathcal{U}$	The uniform distribution	Definition 3.1.1

$\mathbb{E}[V]$	Expectation of a random variable V	Definition 3.1.2
$\mathbb{1}_E$	Indicator variable for event E	Section 3.1
$H_q(x)$	$x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$	Definition 3.3.1
$H_q^{-1}(y)$	Unique $x \in [0, 1-1/q]$ such that $H_q(x) = y$	Section 3.3.2
$\deg(P)$	Degree of polynomial $P(X)$	Definition 5.1.2
$\mathbb{F}_q[X]$	The set of all univariate polynomials in X over $\mathbb{F}_q$	Section 5.1