Math 422: Coding Theory

Winter, 2006 List of Theorems

Theorem 1.1 (Error Detection and Correction): *In a symmetric channel with error-probability $p > 0$,*

(i) a code C can detect up to t errors in every codeword $\iff$ $d(C) \geq t+1$;

(ii) a code C can correct up to t errors in any codeword $\iff$ $d(C) \geq 2t+1$.

Corollary 1.1.1: If a code C has minimum distance d, then C can be used either (i) to detect up to $d-1$ errors or (ii) to correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors in any codeword. Here $\lfloor x \rfloor$ represents the greatest integer less than or equal to x.

Theorem 1.2 (Special Cases): *For any values of q and n,*

(i) $A_q(n,1) = q^n$;

(ii) $A_q(n,n) = q$.

Lemma 1.1 (Reduction Lemma): *If a q-ary (n,M,d) code exists, with $d \geq 2$, there also exists an $(n-1,M,d-1)$ code.*

Theorem 1.3 (Even Values of d): *Suppose d is even. Then a binary (n,M,d) code exists $\iff$ a binary $(n-1,M,d-1)$ code exists.*

Corollary 1.3.1 (Maximum Code Size for Even d): If d is even, then $A_2(n,d) = A_2(n-1,d-1)$.

Lemma 1.2 (Zero Vector): *Any code over an alphabet containing the symbol 0 is equivalent to a code containing the zero vector* $\mathbf{0}$.

Lemma 1.3 (Counting): *A sphere of radius t in F_q^n, with $0 \leq t \leq n$, contains exactly*

$$\sum_{k=0}^{t} \binom{n}{k} (q-1)^k$$

vectors.

Theorem 1.4 (Sphere-Packing Bound): *A q-ary $(n,M,2t+1)$ code satisfies*

$$M \sum_{k=0}^{t} \binom{n}{k} (q-1)^k \leq q^n. \tag{1.1}$$

Lemma 2.1 (Distance of a Linear Code): *If C is a linear code in F_q^n, then $d(C) = w(C)$.*

Lemma 2.2 (Equivalent Cosets): *Let C be a linear code in F_q^n and $a \in F_q^n$. If b is an element of the coset $a + C$, then*

$$b + C = a + C.$$

Theorem 2.1 (Lagrange's Theorem): *Suppose C is an $[n, k]$ code in F_q^n. Then*

(i) every vector of F_q^n is in some coset of C;

(ii) every coset contains exactly q^k vectors;

(iii) any two cosets are either equivalent or disjoint.

Theorem 2.2 (Minimum Distance): *A linear code has minimum distance $d \iff d$ is the maximum number such that any $d-1$ columns of its parity-check matrix are linearly independent.*

Lemma 2.3: *Two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are in the same coset of a linear code $C \iff$ they have the same syndrome.*

Lemma 2.4: *An $(n-k) \times n$ parity-check matrix H for an $[n, k]$ code generated by the matrix $G = [1_k \,|\, A]$, where A is a $k \times (n-k)$ matrix, is given by*

$$[\,-A^t \,|\, 1_{n-k}\,]\,.$$

Theorem 2.3: *The syndrome of a vector that has a single error of m in the ith position is m times the ith column of H.*

Theorem 3.1 (Hamming Codes are Perfect): *Every* $\mathrm{Ham}(r, q)$ *code is perfect and has distance* 3.

Corollary 3.1.1 (Hamming Size): For any integer $r \geq 2$, we have $A_2(2^r - 1, 3) = 2^{2^r-1-r}$.

Theorem 4.1 (Extended Golay $[24, 12]$ code): *The* $[24, 12]$ *code generated by* G_{24} *has minimum distance* 8.

Theorem 4.2 (Nonexistence of binary $(90, 2^{78}, 5)$ codes): *There exist no binary* $(90, 2^{78}, 5)$ *codes.*

Theorem 5.1 (Cyclic Codes are Ideals): *A linear code C in R_q^n is cyclic* $\iff$

$$f(x) \in C, r(x) \in R_q^n \Rightarrow r(x)f(x) \in C.$$

Theorem 5.2 (Generator Polynomial): *Let C be a nonzero q-ary cyclic code in R_q^n. Then*

(i) there exists a unique monic polynomial $g(x)$ of smallest degree in C;

(ii) $C = \langle g(x) \rangle$;

(iii) $g(x)$ *is a factor of* $x^n - 1$ *in* $F_q[x]$.

Theorem 5.3 (Lowest Generator Polynomial Coefficient): *Let* $g(x) = g_0 + g_1 x + \ldots + g_r x^r$ *be the generator polynomial of a cyclic code. Then* g_0 *is non-zero.*

Theorem 5.4 (Cyclic Generator Matrix): *A cyclic code with generator polynomial*

$$g(x) = g_0 + g_1 x + \ldots + g_r x^r$$

has dimension $n - r$ *and generator matrix*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \ldots & g_r & \ldots & 0 \\ \vdots & \vdots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_r \end{bmatrix}.$$

Lemma 5.1 (Linear Factors): *A polynomial* $c(x)$ *has a linear factor* $x - a \iff c(a) = 0$.

Lemma 5.2 (Irreducible 2nd or 3rd Degree Polynomials): *A polynomial* $c(x)$ *in* $F_q[x]$ *of degree* 2 *or* 3 *is irreducible* $\iff c(a) \neq 0$ *for all* $a \in F_q$.

Theorem 5.5 (Cyclic Check Polynomial): *An element* $c(x)$ *of* R_q^n *is a codeword of the cyclic code with check polynomial* $h \iff c(x)h(x) = 0$ *in* R_q^n.

Theorem 5.6 (Cyclic Parity Check Matrix): *A cyclic code with check polynomial*

$$h(x) = h_0 + h_1 x + \ldots + h_k x^k$$

has dimension k *and parity check matrix*

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 \end{bmatrix}.$$

Theorem 5.7 (Cyclic Binary Hamming Codes): *The binary Hamming code* $\mathrm{Ham}(r, 2)$ *is equivalent to a cyclic code.*

Corollary 5.7.1 (Binary Hamming Generator Polynomials): Any primitive polynomial of F_{2^r} is a generator polynomial for a cyclic Hamming code $\mathrm{Ham}(r, 2)$.

Theorem 6.1 (Vandermonde Determinants): *For* $t \geq 2$ *the* $t \times t$ *Vandermonde matrix*

$$V = \begin{bmatrix} 1 & 1 & \dots & 1 \\ e_1 & e_2 & \dots & e_t \\ e_1^2 & e_2^2 & \dots & e_t^2 \\ \vdots & \vdots & & \vdots \\ e_1^{t-1} & e_2^{t-1} & \dots & e_t^{t-1} \end{bmatrix}$$

has determinant $\displaystyle\prod_{\substack{i,j=1 \\ i>j}}^{t} (e_i - e_j)$.

Theorem 6.2 (BCH Bound): *The minimum distance of a BCH code of odd design distance* d *is at least* d.

Theorem 7.1 (Modified Fermat's Little Theorem): *If* s *is prime and* a *and* m *are natural numbers, then*

$$m \left[m^{a(s-1)} - 1 \right] = 0 \ (\mathrm{mod}\, s).$$

Corollary 7.1.1 (RSA Inversion): The RSA decoding function $\mathcal{D}_e$ is the inverse of the RSA encoding function $\mathcal{E}_e$.

Theorem A.1 ($\mathbb{Z}_n$): *The ring* $\mathbb{Z}_n$ *is a field* $\iff$ n *is prime.*

Theorem A.2 (Subfield Isomorphic to $\mathbb{Z}_p$): *Every finite field has the order of a power of a prime* p *and contains a subfield isomorphic to* $\mathbb{Z}_p$.

Corollary A.2.1 (Isomorphism to $\mathbb{Z}_p$): Any field F with prime order p is isomorphic to $\mathbb{Z}_p$.

Theorem A.3 (Prime Power Fields): *There exists a field* F *of order* n $\iff$ n *is a power of a prime.*

Theorem A.4 (Primitive Element of a Field): *The nonzero elements of any finite field can be written as powers of a single element.*

Corollary A.4.1 (Cyclic Nature of Fields): Every element β of a finite field of order q is a root of the equation $\beta^q - \beta = 0$.

Theorem A.5 (Minimal Polynomial): *Let* $\beta \in F_{p^r}$. *If* $f(x) \in F_p[x]$ *has* β *as a root, then* $f(x)$ *is divisible by the minimal polynomial of* β.

Corollary A.5.1 (Minimal Polynomials Divide $x^q - x$): The minimal polynomial of an element of a field F_q divides $x^q - x$.

Corollary A.5.2 (Irreducibility of Minimal Polynomial): Let $m(x)$ be a monic polynomial in $F_p[x]$ that has β as a root. Then $m(x)$ is the minimal polynomial of β $\iff$ $m(x)$ is irreducible in $F_p[x]$.

Theorem A.6 (Functions of Powers): *If $f(x) \in F_p[x]$, then $f(x^p) = [f(x)]^p$.*

Corollary A.6.1 (Root Powers): If α is a root of a polynomial $f(x) \in F_p[x]$ then α^p is also a root of $f(x)$.

Theorem A.7 (Reciprocal Polynomials): *In a finite field F_{p^r} the following statements hold:*

(a) If $\alpha \in F_{p^r}$ is a root of $f(x) \in F_p[x]$, then α^{-1} is a root of the reciprocal polynomial of $f(x)$.

(b) a polynomial is irreducible $\iff$ its reciprocal polynomial is irreducible.

(c) a polynomial is a minimal polynomial of $\alpha \in F_{p^r} \Rightarrow$ a (constant) multiple of its reciprocal polynomial is a minimal polynomial of α^{-1}.

(d) a polynomial is primitive $\Rightarrow$ a (constant) multiple of its reciprocal polynomial is primitive.