Chapter 4

Hamming Codes

Lecture 14, March 3, 2011

4.1 Definition and Properties

A basis for a vector space V is a linearly independent set of vectors in V which spans the space V. The space V is finite-dimensional if it has a finite basis. The dimension of a finite-dimensional vector space V is the number of vectors in a basis for V. Let r be a positive integer. Then we know F_q^r is a finite-dimensional vector space over F_q. Any nonzero vector $\mathbf{v} \in F_q^r$ generates a subspace $\langle \mathbf{v} \rangle$ of dimension 1. Now we have a natural question:

Question. How many dimension 1 subspaces does F_q^r contain?

Solve. For $\mathbf{v}, \mathbf{u} \in F_q^r \setminus \{\mathbf{0}\}$, $\langle \mathbf{v} \rangle = \langle \mathbf{u} \rangle$ if and only if there is a nonzero scalar $\lambda \in F_q \setminus \{0\}$ such that $\mathbf{v} = \lambda \mathbf{u}$. Therefore, there are exactly $\frac{q^r-1}{q-1}$ distinct subspaces of dimension 1 in F_q^r. □

Remark. Let $\mathbf{v} = (v_1, v_2, \ldots, v_r)$ be a nonzero vector in F_q^r. Suppose $v_1 = v_2 = \cdots = v_{i-1} = 0$ and $v_i \neq 0$. Then we have $\langle \mathbf{v} \rangle = \langle v_i^{-1} \mathbf{v} \rangle$ and the first nonzero entry of $v_i^{-1}\mathbf{v}$ equals to 1. Let $\mathbf{u}$ and $\mathbf{v}$ be two nonzero vectors in F_q^r with the first nonzero entry equal to 1, then by the proof we know $\langle \mathbf{v} \rangle = \langle \mathbf{u} \rangle$ if and only if $\mathbf{v} = \mathbf{u}$.

Recall. For a q-ary $[n, k]$ linear code C, we can define the dual code $C^\perp$. Let H be a generator matrix for $C^\perp$, i.e., a parity-check matrix for C. Thus we can describe C as

follows:

$$C = \{\mathbf{v} \in F_q^n \mid H\mathbf{v}^t = 0\}.$$

So C is completely specified by the parity-check matrix H.

Now we can define the q-ary Hamming code:

Definition 4.1 (**q-ary Hamming Code).** Given an integer $r \geq 2$, let $n = \frac{q^r-1}{q-1}$. The **q-ary Hamming code** $\mathrm{Ham}(r, q)$ is a linear $[n, n-r]$ code in F_q^n, whose parity-check matrix H has the property that the columns of H are made up of precisely one nonzero vector from each vector subspace of dimension 1 of F_q^r.

Remark. 1). The order and the vectors of the columns of H have not been fixed in the Definition. Hence, for each $r \geq 2$, the q-ary Hamming code $\mathrm{Ham}(r, q)$ is only well defined up to equivalence of codes, i.e., all the q-ary Hamming codes of a given length are equivalent.

2). Note that the rows of H are linearly independent since H contains all the r columns of weight 1 words. Hence, H is indeed a parity-check matrix.

3). An easy way to write down a parity-check matrix for $\mathrm{Ham}(r, q)$ is to list as columns all the nonzero vectors in F_q^r whose first nonzero entry is 1.

4). Any two columns of H are linearly independent.

Remark (**Binary case).** 1). The columns of a parity-check matrix for the binary Hamming code $\mathrm{Ham}(r, 2)$ consist of all possible nonzero binary words of length r.

2). An equivalent way to construct the binary Hamming code $\mathrm{Ham}(r, 2)$ is given in Bowman's online notes P40.

Example 4.1. A parity-check matrix for the one-dimensional code $\mathrm{Ham}(2, 2)$ is ($r = 2$, hence $2^r - 1 = 3$)

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

which can row reduced to standard form:

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

The generator matrix is then seen to be $[1\ 1\ 1]$. That is, $\mathrm{Ham}(2, 2)$ is just the binary repetition code.

Example 4.2. A parity-check matrix for the Hamming code Ham$(3, 2)$ in standard form, is ($r = 3$, hence $2^r - 1 = 7$)

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

So the generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Then Hamming code Ham$(3, 2)$ is equivalent to the $(7, 16, 3)$ perfect code in Chapter 1.

Theorem 4.1. Given a positive integer $r \geq 2$ and $n = \frac{q^r - 1}{q - 1}$, then

1). The dimension of Ham(r, q) is $k = n - r$.

2). Ham(r, q) is an $[n, n - r, 3]$-code.

3). Ham(r, q) is a perfect exactly single-error-correcting code.

Proof. 1). Since H, a parity-check matrix for Ham(r, q), is an $r \times n$ matrix, the dimension of Ham(r, q) is $n - r$.

2). By the definition, we know any two columns of H are linearly independent. On the other hand, H contains the columns $(1, 0, 0, \ldots, 0)^t$, $(0, 1, 0, \ldots, 0)^t$ and $(1, 1, 0, \ldots, 0)^t$, which form a linearly dependent set. Hence, by the theorem in Chapter 3, the minimum distance of Ham(r, q) is equal to 3.

3). The minimum distance of Ham(r, q) is 3, so it is a exactly single-error-correcting code.

Recall (**Perfect code).** A **perfect code** is a q-ary $(n, M, 2t + 1)$ code such that $M \sum_{k=0}^{t} \binom{n}{k}(q - 1)^k = q^n$. Furthermore, we have $M = A_q(n, 2t + 1)$.

Let check the identity together,

$$\text{LHS} = q^{n-r} \sum_{k=0}^{1} \binom{n}{k}(q-1)^k = q^{n-r}(1 + n \cdot (q-1)) = q^{n-r}(1 + \frac{q^r - 1}{q-1} \cdot (q-1))$$
$$= q^{n-r} \cdot (1 + q^r - 1) = q^n = \text{RHS}.$$

So $\mathrm{Ham}(r,q)$ is a perfect exactly single-error-correcting code.

□

Corollary 4.2 (Hamming Size). For any integer $r \geq 2$, we have $A_q(\frac{q^r-1}{q-1}, 3) = q^{n-r} = q^{\frac{q^r-1}{q-1}-r}$.

Proof. By the Sphere-Packing Bound Theorem, we have

$$A_q(\frac{q^r-1}{q-1}, 3) \leq \frac{q^{\frac{q^r-1}{q-1}}}{\sum_{k=0}^{1} \binom{\frac{q^r-1}{q-1}}{k}(q-1)^k} = q^{\frac{q^r-1}{q-1}-r}.$$

And from above theorem, we know $\mathrm{Ham}(r,q)$ is an $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1}-r, 3]$-code. Hence $A_q(\frac{q^r-1}{q-1}, 3) = q^{n-r} = q^{\frac{q^r-1}{q-1}-r}$. □

Problem 4.1. Prove that for integer $r \geq 2$ a q-ary $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$ linear code C over the field F_q is a Hamming code.

Proof. Let H be a parity-check matrix for C and it is a $r \times \frac{q^r-1}{q-1}$ matrix. By $d(C) = 3$, we know any two columns of H are linearly independent. Hence the vectors, corresponding to any two columns, generate different 1 dimensional vector space in F_q^r. We already know F_q^r contains $\frac{q^r-1}{q-1}$ distinct subspaces of dimension 1 and $\frac{q^r-1}{q-1}$ is the number of columns of H. So by the definition of Hamming code, C is a Hamming code. □

Remark. Problem says that, among linear codes, the Hamming codes are characterized by their parameters length, dimension and distance. This is not the case if we drop the assumption of linearity. Of course any coset of a Hamming code $\mathrm{Ham}(r,q)$ has the same parameters as the code.

Lecture 15, March 8, 2011

4.2 Decoding with a q-ary Hamming code

Recall.

Remark. Let C be a linear code. Then all of the words of weight t could be a coset leader and they are the unique coset leaders in the corresponding cosets if and only if C can correct t errors.

Since Hamming code $\mathrm{Ham}(r, q)$ is a single-error-correcting linear code, hence every vector of weight 1 could be the coset leader and is the unique choice in the coset. Now we have coset leaders $\mathbf{0}$ and all vectors of weight 1. The number of these coset leaders is $1 + (q-1) \cdot n = 1 + (q-1) \cdot \frac{q^r-1}{q-1} = q^r$ and any coset contains $q^{\frac{q^r-1}{q-1}-r}$ vectors. So these cosets list all the words in F_q^n, i.e., they are all cosets of C. Now denote the vector whose j-th position is b and the others are 0 by $\mathbf{e}_{j,b}$ $(1 \leq j \leq n, b \in F_q\{0\})$. Note that the syndrome of $\mathbf{e}_{j,b}$ is

$$S(\mathbf{e}_{j,b}) = H\mathbf{e}_{j,b}^t = b\mathbf{c}_j,$$

where $\mathbf{c}_j$ denotes the j-th column of H.

Decoding works as follows:

Step 1: Given a received word $\mathbf{y}$, calculate syndrome $S(\mathbf{y}) = H\mathbf{y}^t$.

Step 2: If $S(\mathbf{y}) = 0$, then assume no errors.

Step 3: If $S(\mathbf{y}) \neq 0$, i.e., it is nonzero vector in F_q^r, then find the unique $\mathbf{e}_{j,b}$ such that $S(\mathbf{y}) = S(\mathbf{e}_{j,b}) = b\mathbf{c}_j \neq \mathbf{0}$. Assume the error vector is $\mathbf{e}_{j,b}$ and decode the received word $\mathbf{y}$ as $\mathbf{y} - \mathbf{e}_{j,b}$.

Example 4.3. We can write a parity-check matrix for a $\mathrm{Ham}(3, 2)$ code in in the binary ascending form

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

If the vector 1110110 is received, the syndrome is $[0, 1, 1]^t$, which corresponds to the third column of H, so we know immediately that the a single error must have occurred in the third position. Thus, the transmitted codeword was 1100110.

Remark. For nonbinary Hamming codes, we need to compare the computed syndrome with all nonzero multiples of the columns of the parity-check matrix.

Example 4.4. A parity-check matrix for $\mathrm{Ham}(2, 3)$ is

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix}$$

If the vector 2020, which has syndrome $[2, 1]^t = 2[1, 2]^t$, is received and at most a single digit is in error, we see that an error of 2 has occurred in the last position and decode the vector as $\mathbf{x} = \mathbf{y} - \mathbf{e} = 2020 - 0002 = 2021$.

Example 4.5. A parity-check matrix for $\mathrm{Ham}(3, 3)$ is

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

If the vector 2000000000001 is received and at most a single error has occurred, then from the syndrome $[1, 2, 1]^t$ we see that an error of 1 has occurred in the second-last position, so the transmitted vector was 2000000000021.

4.3 Extended binary Hamming code

Definition 4.3 (Extended binary Hamming code). The *extended binary Hamming code*, denoted $\overline{\mathrm{Ham}(r, 2)}$, is the code obtained from $\mathrm{Ham}(r, 2)$ by adding a parity-check digit.

Proposition 4.4 (Properties of the extended binary Hamming codes). 1). $\mathrm{Ham}(r, 2)$ is a binary $[2^r, 2^r - 1 - r, 4]$-linear code.

2). A parity-check matrix $\bar{H}$ for $\overline{\mathrm{Ham}(r, 2)}$ is

$$\bar{H} = \left[\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right]$$

where H is a parity-check matrix for $\mathrm{Ham}(r, 2)$.

Proof. 1). By the proof of **Even Value of d Theorem**, we know if C is an $[n, M, 2t+1]$ binary code then after adding a parity-check digit we get an $[n, M, 2t+2]$ binary code $\bar{C}$. Moreover, if C is linear then $\bar{C}$ is also linear. 2). Let G be a generator matrix of $\mathrm{Ham}(r, 2)$, hence we have $GH^t = 0$ and adding a parity-check digit we get a generator matrix $\bar{G} = [G, \mathbf{c}]$ of $\overline{\mathrm{Ham}(r, 2)}$. We know $\bar{H}$ has the right size as a parity-check matrix for $\overline{\mathrm{Ham}(r, 2)}$ and its rows are linearly independent. Hence it is enough to show that $\bar{G}\bar{H}^t = \mathbf{0}$ i.e., every row of $\bar{H}$ is orthogonal to every row of $\bar{G}$. Indeed

$$\bar{G}\bar{H}^t = [G, \mathbf{c}] \begin{bmatrix} H^t & \mathbf{1}^t \\ \mathbf{0} & 1 \end{bmatrix} = [GH^t, \bar{G}\mathbf{1}^t] = [\mathbf{0}, 0] = \mathbf{0}$$

since all the rows of $\bar{G}$ have even weights. □