Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 6: General Hamming Codes

September 10, 2007

Lecturer: Atri Rudra *Scribe: Nathan Russell*

In the last lecture, we saw the following ways of defining an $[n, k, d]_q$ linear code C:

- An $k \times n$ generator matrix $\mathbf{G}$, so that C is the result of multiplying all vectors $\mathbf{x}$ of length n with $\mathbf{G}$, giving codewords $C = \{\mathbf{x} \cdot \mathbf{G} | \mathbf{x} \in \mathbb{F}_q^k\}$.
- An $(n-k) \times n$ parity check matrix $\mathbf{H}$ such that $C = \{\mathbf{x} \in \mathbb{F}_q^n | \mathbf{H} \cdot \mathbf{x}^T = \mathbf{0}\}$. Note that since $\mathbf{x}$ is a row vector, we need to take the transpose so that multiplication is defined.

We forgot to explicitly define the following notion related to linear subspaces in the last lecture.

Definition 0.1 (Linear independence of vectors)**.** *We say that* $\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_k$ *are linearly independent if for every* $1 \leq i \leq k$

$$\mathbf{v}_i \neq a_1\mathbf{v}_1 + \ldots + a_{i-1}\mathbf{v}_{i-1} + a_{i+1}\mathbf{v}_{i+1} + \ldots + a_k\mathbf{v}_k,$$

for every $k-1$*-tuple* $(a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k) \in \mathbb{F}_q^{k-1}$.

Note that the basis of a linear subspace must be linearly independent.

In today's lecture, we will look at a couple more properties of linear codes and then define the general family of (binary) Hamming codes.

1 Some More Properties of Linear Codes

We start with the following property, which we have seen for the special case of binary linear codes.

Proposition 1.1. *For a* $[n, k, d]_q$ *code* C*,*

$$d = \min_{\substack{\mathbf{c} \in C, \\ \mathbf{c} \neq \mathbf{0}}} wt(\mathbf{c}).$$

Proof. First, we show that d is no more than the minimum weight. We can see this by considering $\Delta(\mathbf{0}, \mathbf{c}')$ where $\mathbf{c}'$ is the non-zero codeword in C with minimum weight; its distance from $\mathbf{0}$ is equal to its weight.

Now, to show that d is no less than the minimum weight, consider any $\mathbf{c_1} \neq \mathbf{c_2} \in C$, and note that $\mathbf{c}_1 - \mathbf{c_2} \in C$ (this is because $-\mathbf{c_2} = -1 \cdot \mathbf{c}_2 \in C$, where -1 is the additive inverse of 1 in $\mathbb{F}_q$ and $\mathbf{c}_1 - \mathbf{c}_2 = \mathbf{c}_1 + (-\mathbf{c}_2)$, which by the definition of linear codes is in C). Now note that the weight of $\mathbf{c_1} - \mathbf{c_2}$ is $\Delta(\mathbf{c_1}, \mathbf{c_2})$, since the non-zero symbols in $\mathbf{c}_1 - \mathbf{c}_2$ occur exactly in the positions where the two codewords differ. $\square$

Next, we look at another property implied by the parity check matrix of a linear code.

Proposition 1.2. *For any $[n, k, d]_q$ code C with parity check matrix $\mathbf{H}$, d is the minimum number of linearly dependent columns in H.*

Proof. By Proposition 1.1, we need to show that the minimum weight of a non-zero codeword in C is the minimum number of linearly dependent columns. Now note that, by the definition of the parity check matrix, $\mathbf{c} \in C \Rightarrow \mathbf{H} \cdot \mathbf{c}^T = \mathbf{0}$. Working through the matrix multiplication, this gives us that $\sum_{i=1}^{n} c_i \mathbf{H}^i$, where $\mathbf{H}^i$ is the ith column of $\mathbf{H}$. Note that we can skip multiplication for those columns for which the corresponding bit c_i is zero, so for this to be zero, those $\mathbf{H}^i$ with $c_i \neq 0$ are linearly dependent. This means that d is at least the minimum number of linearly dependent columns.

For the other direction, consider the minimum set of columns from $\mathbf{H}$, $\mathbf{H}^{i_1}, \mathbf{H}^{i_2}, \ldots, \mathbf{H}^{i_t}$ that are linearly dependent. Now let $c'_{i_i}\mathbf{H}^{i_1} + \ldots + c'_{i_t}\mathbf{H}^{i_t} = \mathbf{0}$ and consider the vector $\mathbf{c}'$ such that $c'_j = 0$ for $j \notin \{i_1, \ldots, i_t\}$. Note that $\mathbf{c}' \in C$ and thus, $d \leq w(\mathbf{c}') = t$ (where recall t is the minimum number of linearly independent columns in $\mathbf{H}$). $\square$

2 Hamming Codes

For any $r \geq 2$, there is a $[2^r - 1, 2^r - r - 1, 3]_2$ Hamming code. We have seen this code for $r = 3$.

Consider the $r \times (2^r - 1)$ matrix $\mathbf{H}_r$ over $\mathbb{F}_2$, where the ith column $\mathbf{H}_r^i$, $1 \leq i \leq 2^r$, is the binary representation of i (note that such a representation is a vector in $\{0, 1\}^r$). For example, for the case we have seen ($r = 3$),

$$\mathbf{H}_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Note that by its definition, the code that has $\mathbf{H}_r$ as its parity check matrix has block length $2^r - 1$ and dimension $2^r - r - 1$.

Definition 2.1. *The $[2^r - 1, 2^r - r - 1]_2$ Hamming code has parity check matrix $\mathbf{H}_r$.*

In other words, the general $[2^r - 1, 2^r - r - 1]_2$ Hamming code is the code $\{\mathbf{c} \in \{0, 1\}^{2^r - 1} | H_r \cdot \mathbf{c}^T = \mathbf{0}\}$.

Next we argue that the above Hamming code has distance 3 (we argued this earlier for $r = 3$).

Proposition 2.2. *The Hamming code $[2^r - 1, 2^r - r - 1, 3]_2$ has distance 3.*

Proof. No two columns in $\mathbf{H}_r$ are linearly dependent. If they were, we would have $\mathbf{H}_r^i + \mathbf{H}_r^j = \mathbf{0}$, but this is impossible since they differ in at least one bit (being binary representations of integers, $i \neq j$). Thus, by Proposition 1.2, the distance is at least 3. It is at most 3, since (e.g.) $\mathbf{H}_r^1 + \mathbf{H}_r^2 + \mathbf{H}_r^3 = \mathbf{0}$. $\square$

Now note that under the Hamming bound for $d = 3$, $k \leq n - \log_2(n + 1)$, so for $n = 2^r - 1$, $k \leq 2^r - r - 1$. Hence, the Hamming code is a perfect code.