

Linear Codes

Linear Codes

In general, finding the minimum distance of a code requires comparing every pair of distinct elements. For a linear code however this is not necessary.

Proposition 4: *In a linear code the minimum distance is equal to the minimal weight among all non-zero code words.*

Proof: Let x and y be code words in the code C , then $x - y$ is in C since C is linear. We then have $d(x,y) = d(x-y,0)$ which is the weight of $x-y$. □

(Notice that this proposition is actually valid in a larger class of codes ... one only requires that the alphabet permits algebraic manipulation and that the code is “closed” under subtraction.)

Generator Matrix

We shall now look at two ways of describing a linear code C .

The first is given by a *generator matrix* G which has as its rows a set of basis vectors of the linear subspace C . If C is an $[n,k]$ -code, then G will be a $k \times n$ matrix.

The code C is the set of all linear combinations of the rows of G , or as we usually call it, the **row space of G** .

Given the matrix G , the code C is obtained by multiplying G on the left by all possible $1 \times k$ row vectors (this gives all possible linear combinations):

$$C = \{xG \mid x \in V[k,q] \}.$$

Equivalence of Linear Codes

The general concept of equivalence of codes does not necessarily preserve the property of a code being linear. That is, linear codes may be equivalent to non-linear codes. In order to preserve the linear property we must limit the types of operations allowed when considering equivalence.

Two linear codes are *equivalent* if one can be obtained from the other by a series of operations of the following two types:

- 1) an arbitrary permutation of the coordinate positions, and
- 2) in any coordinate position, multiplication by any non-zero scalar.

(Note that this second operation preserves the 0 entries.)

Generator Matrix

Due to this definition of equivalence, elementary row and column operations on the generator matrix G of a linear code produce a matrix for an equivalent code.

Since G has rank k , by elementary row operations we can transform G to a matrix with a special form. Thus, we see that every linear code has an equivalent linear code with a generator matrix of the form $G = [I_k \ P]$, where I_k is the $k \times k$ identity matrix and P is a $k \times n-k$ matrix. We call this the *standard form of G* .

Example

Let C be the $[7,4]$ -code of $V[7,2]$ generated by the rows of G (in standard form):

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

We get the 16 code words by multiplying G on the left by the 16 different binary row vectors of length 4.

So for instance we get code words:

$$(1,1,0,0) G = (1,1,0,0,1,0,1)$$

$$(1,0,1,1) G = (1,0,1,1,1,0,0)$$

$$(0,0,0,0) G = (0,0,0,0,0,0,0).$$

Example

The list of all the codewords is:

0 0 0 0 0 0 0	1 1 0 1 0 0 0	0 1 1 0 1 0 0	0 0 1 1 0 1 0
0 0 0 1 1 0 1	1 0 0 0 1 1 0	0 1 0 0 0 1 1	1 0 1 0 0 0 1
1 1 1 1 1 1 1	0 0 1 0 1 1 1	1 0 0 1 0 1 1	1 1 0 0 1 0 1
1 1 1 0 0 1 0	0 1 1 1 0 0 1	1 0 1 1 1 0 0	0 1 0 1 1 1 0

Notice that there are 7 codewords of weight 3, 7 of weight 4, 1 of weight 7 and 1 of weight 0. Since this is a linear code, the minimum distance of this code is 3 and so it is a 1-error correcting code.

This $[7,4,3]$ code is called the $[7,4]$ – *Hamming Code*. It is one of a series of codes due to Hamming and Golay.

Parity Check Matrix

We now come to the second description of a linear code C .

The orthogonal complement of C , i.e. the set of all vectors which are orthogonal to every vector in C [**orthogonal = standard dot product is 0**], is a subspace and thus another linear code called the *dual code* of C , and denoted by C^\perp . If C is an $[n,k]$ -code then C^\perp is an $[n, n-k]$ code.

A generator matrix for C^\perp is called a *parity check* matrix for C . If C is an $[n,k]$ -code then a parity check matrix for C will be an $(n-k) \times n$ matrix. If H is a parity check matrix for C , we can recover the vectors of C from H because they must be orthogonal to every row of H (**basis vectors of C^\perp**).

Parity Check Matrix

Thus the code C is given by a parity check matrix H as follows:

$$C = \{ \mathbf{x} \in V[n,q] \mid H\mathbf{x}^T = \mathbf{0} \}$$

since the entries of this product are just the dot products of \mathbf{x} with the rows of H .

Example

A parity check matrix for the [7,4]-Hamming code is given by:

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

Recall from the earlier example that 0001101 is a codeword and notice that

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

Parity Check Matrices

Theorem 1 : *Let H be a parity-check matrix for an $[n,k]$ -code C in $V[n,F]$. Then every set of $s-1$ columns of H are linearly independent if and only if C has minimum distance at least s .*

Proof: First assume that every set of $s-1$ columns of H are linearly independent over F . Let $\mathbf{c} = (c_1 \ c_2 \ \dots \ c_n)$ be a non-zero codeword and let $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n$ be the columns of H . Then since H is the parity check matrix, $H\mathbf{c}^T = \mathbf{0}$. This matrix-vector product may be written in the form

$$H \mathbf{c}^T = \sum_{i=1}^n c_i \mathbf{h}_i = \mathbf{0}.$$

The weight of \mathbf{c} , $\text{wt}(\mathbf{c})$ is the number of non-zero components of \mathbf{c} .

Parity Check Matrices

If $\text{wt}(c) \leq s - 1$, then we have a nontrivial linear combination of less than s columns of H which sums to $\mathbf{0}$. This is not possible by the hypothesis that every set of $s - 1$ or fewer columns of H are linearly independent. Therefore, $\text{wt}(c) \geq s$, and since c is an arbitrary non-zero codeword of the linear code C it follows that the minimum non-zero weight of a codeword is $\geq s$. So, since C is linear (Prop. 4), the minimum distance of C is $\geq s$.

To prove the converse, assume that C has minimum distance at least s . Suppose that some set of $t < s$ columns of H are linearly dependent. Without loss of generality, we may assume that these columns are $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_t$.

Parity Check Matrices

Then there exist scalars λ_i in F , not all zero, such that

$$\sum_{i=1}^t \lambda_i h_i = 0.$$

Construct a vector c having λ_i in position i , $1 \leq i \leq t$, and 0's elsewhere. By construction, this c is a non-zero vector in C since $Hc^T = \mathbf{0}$. But $\text{wt}(c) = t < s$. This is a contradiction since by hypothesis, every non-zero codeword in C has weight at least s . We conclude that no $s-1$ columns of H are linearly dependent. ■

Parity Check Matrices

It follows from the theorem that a linear code C with parity-check matrix H has minimum distance (exactly) d if and only if *every* set of $d-1$ columns of H are linearly independent, and *some* set of d columns are linearly dependent. Hence this theorem could be used to determine the minimum distance of a linear code, given a parity-check matrix.

Parity Check Matrices

It is also possible to use this theorem to *construct* single-error correcting codes (i.e., those with a minimum distance of 3). To construct such a code, we need only construct a matrix H such that no 2 or fewer columns are linearly dependent. The only way a single column can be linearly dependent is if it is the zero column. Suppose two non-zero columns \mathbf{h}_i and \mathbf{h}_j are linearly dependent. Then there exist non-zero scalars $a, b \in F$ such that

$$a \mathbf{h}_i + b \mathbf{h}_j = \mathbf{0}.$$

This implies that

$$\mathbf{h}_i = -a^{-1}b \mathbf{h}_j,$$

meaning that \mathbf{h}_i and \mathbf{h}_j are scalar multiples of each other. Thus, if we construct H so that H contains no zero columns and no two columns of H are scalar multiples, then H will be the parity-check matrix for a linear code having distance at least 3.

Example

Over the field $F = \text{GF}(3) = \mathbb{Z}_3$ (integers mod 3), consider the matrix

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

The columns of H are non-zero and no column is a scalar multiple of any other column.

Hence, H is the parity-check matrix for a $[5,2]$ -code in $V[5,3]$ with minimum distance at least 3.

Hamming Codes

Hamming Codes

A *Hamming Code* of order r over $GF(q)$ is an $[n,k]$ -code where $n = (q^r - 1)/(q - 1)$ and $k = n - r$, with parity check matrix H_r an $r \times n$ matrix such that the columns of H_r are non-zero and no two columns are scalar multiples of each other.

Note that $q^r - 1$ is the number of non-zero r -vectors over $GF(q)$ and that $q - 1$ is the number of non-zero scalars, thus n is the maximum number of non-zero r -vectors no two of which are scalar multiples of each other. It follows immediately from Theorem 1 that the Hamming codes all have minimum distance exactly 3 and so are 1-error correcting codes.

Hamming Codes are Perfect

Since the number of codewords in a Hamming code is q^k , a direct computation shows that sphere packing bound is met, so:

Theorem 3 : *The Hamming codes of order r over $GF(q)$ are perfect codes.*

Proof: With $M = q^k$, and $d = 3 = 2e + 1$, ie. $e = 1$ we have:

$$M \sum_{i=0}^e \binom{n}{i} (q-1)^i = q^k (1 + n(q-1)) = q^k \left(1 + \frac{q^r - 1}{q-1} (q-1)\right) = q^{k+r} = q^n.$$

Example

The Hamming code of order $r = 3$ over $\text{GF}(2)$ is given by the parity-check matrix

$$H_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

This is the $[7,4]$ -code with distance 3. Re-ordering the columns of H_3 would define an equivalent Hamming code.

Example

The [13,10]-Hamming code of order 3 over GF(3) is given by the parity-check matrix

$$H_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 2 \end{pmatrix}.$$

Decoding Linear Codes

Decoding

The usefulness of an error-correcting code would be greatly diminished if the decoding procedure was very time consuming. While the concept of decoding, i.e., finding the nearest codeword to the received vector, is simple enough, the algorithms for carrying this out can vary tremendously in terms of time and memory requirements.

Usually, the best (i.e., **fastest**) decoding algorithms are those designed for specific types of codes. We shall examine some algorithms which deal with the general class of linear codes and so, will not necessarily be the best for any particular code in this class.

Syndromes

When a codeword \mathbf{c} is transmitted and vector \mathbf{r} is received, the difference between the two is called the *error vector* \mathbf{e} , i.e. $\mathbf{r} = \mathbf{c} + \mathbf{e}$.

If H is a parity-check matrix for the linear code C , then

$$\mathbf{H}\mathbf{r}^T = \mathbf{H}(\mathbf{c} + \mathbf{e})^T = \mathbf{H}\mathbf{c}^T + \mathbf{H}\mathbf{e}^T = \mathbf{H}\mathbf{e}^T$$

since $\mathbf{H}\mathbf{c}^T = \mathbf{0}$ for any codeword.

$\mathbf{H}\mathbf{r}^T$ is called the *syndrome* of \mathbf{r} .

Syndromes

If $\text{wt}(\mathbf{e}) \leq 1$ then the syndrome of $\mathbf{r} = \mathbf{H}\mathbf{e}^T$ is just a scalar multiple of a column of \mathbf{H} . This observation leads to a simple decoding algorithm for 1-error correcting linear codes.

First, calculate the syndrome of \mathbf{r} . If the syndrome is $\mathbf{0}$, no error has occurred and \mathbf{r} is a codeword.

Otherwise, find the column of \mathbf{H} which is a scalar multiple of the syndrome.

If no such column exists then more than one error has occurred and the code can not correct it.

If however, the syndrome is α times column j , say, then add the vector with $-\alpha$ in position j and 0's elsewhere to \mathbf{r} . This corrects the error.

Example

Let $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$ be the parity check matrix of a code C

in $V[5,3]$. Now $\mathbf{x} = (1 \ 0 \ 1 \ 2 \ 0)$ is a code word since,

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

If $\mathbf{r} = (1 \ 0 \ 1 \ 1 \ 0)$ is received when \mathbf{x} is transmitted, then the syndrome of \mathbf{r} is:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Correction: $\mathbf{r} + (0 \ 0 \ 0 \ -2 \ 0) = (1 \ 0 \ 1 \ -1 \ 0) = (1 \ 0 \ 1 \ 2 \ 0)$.

Hamming Decoding

This method can be improved for binary Hamming codes. The very simple decoding algorithm that results is called *Hamming Decoding*.

Rearranging the columns of the parity check matrix of a linear code gives the parity check matrix of an equivalent code. In the binary Hamming code of order r , the columns are all the non-zero binary vectors of length r . Each such column represents the binary form of an integer between 1 and $n = 2^r - 1$. We can arrange the columns of the parity check matrix so that the column in position i represents the integer i . Let H be the parity check matrix formed in this way.

Hamming Decoding

For example, the parity check matrix for the [7,4]-Hamming code would be written as:

$$H_3' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Here, the column $(x,y,z)^T$ represents the number $x(2^0) + y(2^1) + z(2^2)$.

If v is the received vector, calculate the syndrome Hv^T . If at most one error has been made, the result is a vector of length r , either the zero vector or a column of H . When one error has been made the number represented by this column is the position in v which is in error – and since this is a binary code, we can correct it.

Hamming Decoding

0101010 is a codeword in the [7,4]-Hamming code. Suppose that we received the vector $v = 0101\mathbf{1}10$. We calculate:

$$H_3' v^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

The result represents the number 5, which is the position of the error.