*(n,k)* Linear Code Over a Finite Field *F*

A *k*-dimensional subspace *V* of the vector space  (*n* copies) over a field *F*. The members of *V* are called *code words*. When *F* is , the code is called *binary*.

Hamming distance

The number of components in which two vectors of a vector space differ. Notation: *d(u,v)*.

Hamming weight

The number of non-zero components of a vector *u*. Notation: *wt(u)*.

Hamming weight of a linear code

The minimum weight of any nonzero vector in the code.

Properties of Hamming Distance and Hamming Weight

For any vectors *u, v*, and *w*,  and .

Correcting Capabilities of a Linear Code

If the Hamming weight of a linear code is at least , then the code can correct any *t* or fewer errors. Alternatively, the code can detect any  or fewer errors.

Standard generator matrix

(or standard encoding matrix)

A *k* by *n* matrix in which the first *k* columns are the identity matrix. When using this transformation matrix, the message constitutes the first *k* components of the transformed vectors.

Systematic code

An *(n,k)* linear code in which the *k* information digits occur at the beginning of each code word.

Parity-check matrix

Let  be the standard generator matrix.

The  matrix *H* whose first *k* rows are *–A* and whose next  rows are the identity matrix.

Decoding procedure using parity-check matrix

(steps 1-3 of 4)

Step 1: For any received word *w*, compute *wH*.

Step 2: If *wH* is the zero vector, assume no error was made.

Step 3: If there is exactly one instance of a nonzero element  and a row *i* of *H* such that *wH* is *s* times row *i*, assume the sent word was , where *s* occurs in the *i*-th component. If there is more than one such instance, do not decode.

Decoding procedure using parity-check matrix

(steps 3’ and 4 of 4)

Step 3’: When the code is binary, category 3 reduces to the following. If *wH* is the *i*-th row of *H* for exactly one *i*, assume that an error was made in the *i*-th component of *w*. If *wH* is more than one row of *H*, do not decode.

Step 4: If *wH* does not fit into either category 2 or category 3, we know that at least two errors occurred in transmission and we do not decode.

Orthogonality Relation

Let *C* be an *(n,k)* linear code over *F* with generator matrix *G* and parity-check matrix *H*. Then, for any vector *v* in , we have  (the zero vector) if any only if *v* belongs to *C*.

Parity-Check Matrix Decoding

Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no one row is a scalar multiple of any other.

Standard array

A table constructed as follows.

The first row is the set of *C* code words, beginning in column 1 with the identity .

To form additional rows, choose an element *v* of *V* not listed so far. Among all the elements of the coset , choose one of minimum weight, say *v’*. Complete the next row of the table by placing under the column headed by the code word *c* the vector .

Continue this process until all vectors in *V* have been listed.

Coset leader

The words in the first column of the standard array.

Coset Decoding Is Nearest-Neighbor Decoding

In coset decoding, a received word *w* is decoded as a code word *c* such that  is a minimum.

Syndrome of *u*

An *(n,k)* linear code over *F* has parity matrix *H*.

For any vector , the vector .

Same Coset---Same Syndrome

Let *C* be an *(n,k)* linear code over *F* with parity-check matrix *H*. Then, two vectors of  are in the same coset of *C* if and only if they have the same syndrome.

Procedure for decoding a word in coset decoding

1. Calculate *wH*, the syndrome of *w*.
2. Find the coset leader *v* such that .
3. Assume that the vector sent was .