Perfect codes, HAMMING codes

Let us first prove the so-called *Hamming bound (or: sphere packing bound)* for codes.

Proposition (Hamming bound)**.** *Assume that $C \subseteq Q^n$, $|Q| = q$, and C is a t-error correcting code. Then*

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

The proof is easy: in case of a t-error correcting code the balls of radius t around codewords are disjoint. The number of words in a ball of radius t does not depend on the centre, so we have to multiply $|C|$ with the number of words in one specific ball, hence $|C| \cdot |B(0,t)| \leq q^n$. The ball of radius t around 0 contains words of weight i with $i \leq t$. To get a word of weight i we have to choose the i non-zero coordinate (out of n), and then put a non-zero elemnt of Q in these coordinates. This can be done in $\binom{n}{i}(q-1)^i$ ways, so $|B(0,t)| = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$.

Definition. Codes attaining equality in the Hamming-bound are called *perfect* codes. So, for perfect codes we have

$$|C| = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Let us first focus on the binary case ($q = 2$) and $t = 1$.

Proposition. *The parameters of a binary, 1-error correcting perfect code are $n = 2^m - 1$, $|C| = 2^{n-m}$ (and $d = 3$.)*

As $|B(0,t)| = \sum_{i=0}^{1} \binom{n}{i} = 1 + n$ divides 2^n, we have $1 + n = 2^m$. The rest simply follows from the relation $|C|(1+n) = 2^n$, and the relation between the minimum distance and the error correcting capability.

We can construct a linear code, the so-called Hamming code, which is a 1-error correcting perfect code.

Definition. Let us write the non-zero binary vectors of length m in the columns of a matrix H. So, H is an $m \times (2^m - 1)$ matrix. The *binary Hamming code* $\mathrm{Ham}(m)$ is the code whose parity check matrix is H.

As an example let us write the parity check matrix of Ham(4).

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

The previous results immediately give the parameters of Ham(m). Note that any two columns of the parity check matrix H are independent and there are 3 columns that are dependent (e.g. the first three in the example), so $d = 3$ indeed.

Proposition. Ham(m) *is a* $[2^m - 1, 2^m - 1 - m, 3]$ *code.*

Note that the introductory example of a code of length 7 was the code Ham(3). The order in which we list the non-zero binary vectors in the columns of the parity check matrix H does not really matter in the sense that different orders give equivalent codes. One convenient order is to put in column i the binary expansion of the number i (if it contains less than n bits, then we extend it by zeroes in the front).

Proposition. *If C is a linear, 1-error-correcting binary perfect code, then C is equivalent to* Ham(m).

We saw above that n must be $2^m - 1$ for some m, and $|C| = 2^{n-m}$. Hence the parity check matrix of C has to be an $m \times (2^m - 1)$ matrix. As $d = 3$ every two columns have to be independent (so different because of $q = 2$). So, there is no other possibility than to put each non-zero vector in the columns of the parity check matrix (in some order; but they give equivalent codes).

The dual code of the Hamming codes are also interesting. Here the codewords are linear combinations of the rows of H. First, observe that every row of H contains $2^{m-1} - 1$ zeroes and 2^{m-1} ones, so the weight of any row of H is 2^{m-1}. The same applies for any linear combination of the rows. Indeed, let us denote the rows by $h_1, \dots h_m$ and consider a linear combination $h = c_1 h_1 + \dots + c_m h_m$. In order to determine $w(h)$, we need to find the number of those columns $(x_1, \dots, x_m)^T$ for which $c_1 x_1 + \dots + c_m x_m = 1$. It is easier to determine the number of solutions of $c_1 x_1 + \dots + c_m x_m = 0$. This is the equation of a hyperplane, so this has 2^{m-1} solutions. One of the solutions is the zero vector, which is not a column of H, so the number of solutions of $c_1 x_1 + \dots c_m x_m = 0$ is $2^{m-1} - 1$. So, the number of solutions of $c_1 x_1 + \dots + c_m x_m = 1$ is $(2^m - 1) - (2^{m-1} - 1) = 2^{m-1}$. Let us also remark that the solutions of $c_1 x_1 + \dots + c_m x_m = 1$ form an affine hyperplane (a translate of a vector hyperplane). We just proved that every non-zero vector in the dual code has weight 2^{m-1}, which also means that the distance of any two codewords is also 2^{m-1}, so the code is *equidistant*. The conclusion on the parameters of the dual code is the following.

Proposition. *The code* $\mathrm{Ham}(m)^\perp$ *is a* $[2^m-1, m, 2^{m-1}]$ *code. It is called the* symplex code *and it is equidistant.*

Let us see how one can generalize the Hamming codes over a q-ary alphabet. Let us start listing the non-zero vectors of length m over $\mathrm{GF}(q)$. We want to keep the property that every two columns are independent. In other words, two columns cannot be constant multiples of each other. So, if we keep a non-zero vector, then have to leave out its constant multiples. This can be done for example by taking the last non-zero coordinate in a column to be 1. Using this, we keep one out of the $q-1$ multiples of a column, so we keep $(q^m-1)/(q-1)$ vectors. Let us illustrate this for $q=3$ and $m=3$.

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

So, with this normalization we start with the vector $(1,0,0)^T$, then come three vectors of type $(*,1,0)$ (and we see the three elements 0,1,2 in place of $*$), then come the $3 \cdot 3$ vectors of type $(*,*,1)$. So in total we have $1+q+q^2+\ldots+q^{m-1} = n$ columns for a general m. Note that we indeed have $n=(q^m-1)/(q-1)$.

Definition. The *q-ary Hamming code* has parity check matrix H as described above. It is denoted as $\mathrm{Ham}_q(m)$ and has parameters $n=(q^m-1)/(q-1)$, $k=n-m$, and $d=3$. $\mathrm{Ham}_q(m)$ is perfect.

With the above normalization we achieve that every two columns of H are independ (but some three are dependent), so $d=3$. This means that $\mathrm{Ham}_q(m)$ is 1-error correcting. Since the ball of radius 1 has $1+n(q-1)=q^m$ words and $|\mathrm{Ham}_q(m)| = q^{n-m}$, we see that $\mathrm{Ham}_q(m)$ is perfect. Actually, also in the q-ary case one can show that for a perfect 1-error correcting code C, n has to be $(q^m-1)/(q-1)$, for some m and $|C| = q^{n-m}$. Moreover, if C is a linear 1-error correcting perfect code, then it has to be equivalent to $\mathrm{Ham}_q(m)$.

We may also notice that the colums of the parity check matrix are the points of $\mathrm{PG}(m-1,q)$. The parameters of the dual code can also be computed as above, taking into account that the columns correspond to projective points.

Proposition. *The dual code* $\mathrm{Ham}_q(m)^\perp$ *has parameters* $[n=(q^m-1)/(q-1), k=m, d=q^{m-1}]_q$.