Corollary
Hamming codes over GF(q) are single error correcting.

As a more general result than Proposition 6.1 we have the following proposition.

Proposition 6.2
The minimum distance of a code over GF(q) with parity check matrix $\mathbf{H}$ is at least $k+1$ iff every set of k columns of $\mathbf{H}$ is linearly independent.

Definition 6.3
Let F be a field of order q and for a positive integer n, let $F^{(n)} = V(n,q)$ denote, as before, the space of all n-tuples of length n over F. Let $\rho > 0$ and $\mathbf{x} \in V(n,q)$. Then the sphere in $V(n,q)$ of radius ρ with centre at the point $\mathbf{x}$ is defined by

$$S_\rho(\mathbf{x}) = \{\mathbf{y} \in V(n,q)/d(\mathbf{x},\mathbf{y}) \le \rho\}$$

Observe that the sphere $S_1(\mathbf{x})$:

(i) in $\mathbb{B}^n$ contains exactly $n+1$ elements;
(ii) in $V(n,3)$ contains exactly $2n+1$ elements; and
(iii) in $V(n,q)$ contains exactly $n(q-1)+1$ elements.

Definition 6.4
An e-error-correcting code $\mathscr{C}$ of length n over GF(q) is called **perfect** if

$$\bigcup_{\mathbf{x}\in\mathscr{C}} S_e(X) = V(n,q)$$

Proposition 6.3
Hamming codes are single error correcting perfect codes.

Proof
We know that Hamming codes are single error correcting. So, we only need to prove that these are perfect. Let $\mathscr{C}$ be a Hamming code of length $n = (q^r-1)/(q-1)$ over GF(q) so that a parity check matrix of $\mathscr{C}$ is an $r \times n$ matrix over GF(q). Therefore, the dimension of $\mathscr{C}$ over GF(q) is $n-r$ and order of $\mathscr{C}$ is q^{n-r}. The minimum distance of the code being at least 3, every sphere $S_1(\mathbf{x})$, $\mathbf{x}\in\mathscr{C}$, contains exactly one code word inside it, namely, the vector associated with the word x itself. Also, for $\mathbf{x},\mathbf{y}\in\mathscr{C}, \mathbf{x}\ne\mathbf{y}, S_1(\mathbf{x})$ and $S_1(\mathbf{y})$ are disjoint. Therefore,

$$\begin{aligned} \mathrm{O}\left(\bigcup_{\mathbf{x}\in\mathscr{C}} S_1(\mathbf{x})\right) &= (n(q-1)+1)\mathrm{O}(\mathscr{C}) = (n(q-1)+1)q^{n-r} = q^n \\ &= \mathrm{O}(V(n,q)) \end{aligned}$$

Hence

$$\bigcup_{\mathbf{x}\in\mathscr{C}} S_1(\mathbf{x}) = V(n, q)$$

Having defined spheres, we now obtain the **sphere-packing** or **Hamming bound**.

Theorem 6.4
A k-error-correcting binary code of length n containing M code words must satisfy:

$$M\left\{1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{k}\right\}\leq 2^n$$

Proof
Since the code is k error correcting, distance between any two code words is at least $2k+1$. Therefore, the spheres of radius k around the code words are disjoint. But every sphere around a code word contains the code word and vectors which are at a distance $1 \leq d \leq k$ from this code word. The number of vectors which are at distance d from the code word is $\binom{n}{d}$. Therefore, the number of all vectors of length n contained within the above spheres is

$$M\left\{1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{k}\right\}$$

Since the total number of vectors of length n is 2^n, the result follows. ■

As an application of Proposition 6.2 we obtain the following theorem.

Theorem 6.5 (The Gilbert–Varshamov bound)
There exists a binary linear code of length n, with at most r parity checks and minimum distance at least d, provided

$$1+\binom{n-1}{1}+\cdots+\binom{n-1}{d-2}<2^r$$

Proof
We know that if $\mathscr{C}$ is a code with parity check matrix $\mathbf{H}$ such that all $d-1$ columns of $\mathbf{H}$ are linearly independent, then the minimum distance of the code is at least d. Furthermore, if $\mathbf{H}$ is an $r \times n$ matrix, then the number of parity checks is r. Therefore, we need to construct an $r \times n$ matrix $\mathbf{H}$ in which all $d-1$ columns are linearly independent.

The first column can be chosen to be any non-zero r-tuple. Suppose that we have chosen i columns so that no $d-1$ columns out of these are linearly dependent. There are at most

$$\binom{i}{1}+\binom{i}{2}+\cdots+\binom{i}{d-2}$$

distinct linear combinations of these i columns taken at most $d-2$ at a time. If this number is less than 2^r-1, we can certainly find an r-tuple which does not equal any of these linear combinations and, thus, can add a column such that any $d-1$ columns of the new $r \times (i+1)$ array are linearly independent. We can go on doing this as long as

$$1+\binom{i}{1}+\cdots+\binom{i}{d-2}<2^r$$

Therefore, if

$$1+\binom{n}{1}+\cdots+\binom{n}{d-2}<2^r$$

we can certainly find an $r \times n$ matrix in which all $d-1$ columns are linearly independent.

Theorem 6.6 (The Gilbert–Varshamov bound – non-binary case)
There exists a linear code over a field of q elements, having length n, at most r parity checks, and minimum distance at least d, provided

$$\sum_{i=0}^{d-2}(q-1)^i\binom{n-1}{i}<q^r$$

Proof

As in the binary case, we have to construct an $r \times n$ matrix $\mathbf{H}$ in which all $d-1$ columns are linearly independent.

The first column may be chosen to be any non-zero r-tuple. Suppose that we have chosen i columns so that no $d-1$ columns out of these are linearly dependent. Out of the i columns, k columns can be chosen in $\binom{i}{k}$ ways. Also there are $(q-1)^k$ linear combinations of any k chosen columns. Therefore, there are at most

$$(q-1)\binom{i}{1}+(q-1)^2\binom{i}{2}+\cdots+(q-1)^{d-2}\binom{i}{d-2}$$

distinct linear combinations of these i columns taken at most $d-2$ at a time. The rest of the argument is the same as in the binary case.

Next, we give a bound on the minimum distance of any code whether linear or not. A code of length n over a set (or field) of q elements is called non-linear if the set of all code words is not a vector space. First, we have a simple number theoretic lemma.