Recall that the Hamming ball of radius $r$ centered at a word $\overline{x}$ in $F_q^n$ is

$$B_r(\overline{x}) = \{ \overline{y} \in F_q^n : d(\overline{x}, \overline{y}) \leq r \}$$

Note that $B_r(\overline{x})$ depends on $r, \overline{x}, q, n$ but we suppress dependence on $q, n$ in the notation.

Example: $q = 2, n = 3 : B_1(000) = \{000, 100, 010, 001\}$

$B_2(100) = \{100, 000, 110, 101, 011, 001, 111\}$

For arbitrary $q, n$, $B_n(\overline{x}) = F_q^n$.

Let us now compute the “volume” of (i.e., the number of words in) the Hamming ball.

**Proposition:**

$$|B_r(\overline{x})| = \sum_{m=0}^{r} \binom{n}{m} (q - 1)^m$$

**Proof.**

$$|B_r(\overline{x})| = \sum_{m=0}^{r} |\{ \overline{y} \in F_q^n : d(\overline{x}, \overline{y}) = m \}|$$

and each word $\overline{y} \in F_q^n$ s.t. $d(\overline{x}, \overline{y}) = m$ is uniquely determined by the $m$ locations in which $\overline{x}$ and $\overline{y}$ differ and for each such location a choice of $q - 1$ symbols.

Note that the volume of $B_r(\overline{x})$ depends only on $n, q$ and $r$ but not on $\overline{x}$. We will sometimes abbreviate $B_r(\overline{x})$ by $B_r$.

**Special case:** $q = 2$:

$$|B_r(\overline{x})| = \sum_{m=0}^{r} \binom{n}{m}$$
Theorem (Hamming Bound or sphere-packing bound): Let $t \geq 1$.

$$A_q(n, 2t + 1) \leq \left\lfloor \frac{q^n}{\sum_{m=0}^{t} \binom{n}{m}(q - 1)^m} \right\rfloor$$

Proof: Let $C$ be an $(n, M, 2t + 1)$ code over $F_q$. Then $\{B_t(\bar{c}) : \bar{c} \in C\}$ are pairwise disjoint. Thus,

$$M \cdot |B_t| = |C| \cdot |B_t| = |\cup_{\bar{c} \in C} B_t(\bar{c})| \leq |F^n| = q^n$$

Thus,

$$M \leq \frac{q^n}{\sum_{m=0}^{t} \binom{n}{m}(q - 1)^m}$$

If $C$ is a code that achieves $A_q(n, 2t + 1)$, then we get the bound. \(\square\)

Remark: The Hamming bound applies only to odd $d = 2t + 1$, or equivalently, to $t$-error-correcting codes. However, for binary codes it also gives an upper bound for $A_2(n, d)$ for even $d$, using the identity $A_2(n, d) = A_2(n - 1, d - 1)$.

Let us now compare Hamming and Singleton in special cases. The winner is the smaller upper bound.

Example 1. $A_2(7, 3)$:

Hamming: $A_2(7, 3) \leq 2^7/(1 + 7) = 16$

Singleton: $A_2(7, 3) \leq 2^{7-3+1} = 32$

So, Hamming beats Singleton! We will later see that $A_2(7, 3) = 16$

Example 2. $A_8(5, 3)$:

Hamming: $A_8(5, 3) \leq \frac{8^5}{1 + 5 + 7} = \frac{8^5}{36}$

Singleton: $A_8(5, 3) \leq 8^{5-3+1} = 8^3$

So, Singleton beats Hamming: $8^3 < \frac{8^5}{36}$ iff $1 < \frac{8^2}{36}$, which is true.
Example 3. $A_2(n, 3)$:

Hamming:

$$A_2(n, 3) \leq \frac{2^n}{1 + n}$$

Singleton:

$$A_2(n, 3) \leq 2^{n-2} = \frac{2^n}{4}$$

In this case, Hamming wins for $n \geq 4$; for $n = 3$, there is a tie; and for $n = 1, 2$, $A_2(n, 3)$ doesn’t make sense (a code of length $n$ cannot have minimum distance $> n$).

Let us now return to Example 1.

**Proposition:** $A_2(7, 3) = 16$.

We already know that $A_2(7, 3) \leq 16$, so we only need to show that $A_2(7, 3) \geq 16$. To show this I constructed a $(7, 16, 3)$ using a finite projective plane of degree 2. This construction is carried out in detail on pp. 22-24 in the book.