**Binomial coefficients**

\[ \binom{n}{i} \] is the number of unordered selections of \( i \) elements out of a set of \( n \) elements.

Examples: (1) \( \binom{n}{n} = 1 \), (2) \( \binom{n}{1} = n \), (3) \( \binom{n}{n-1} = n \).

Exercise: Prove these.

**Proposition:** \( \binom{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1) \ldots (n-i+1)}{i!} \).

*Proof.* First count the number of ordered selections of \( i \) elements from \( \{1, \ldots, n\} \). There are

\[ n \text{ ways to choose the first element, } n-1 \text{ ways to choose the second element, } \ldots, (n-i+1) \text{ ways to choose the } i \text{th element.} \]

All in all, we obtain \( n(n-1) \ldots (n-i+1) = \frac{n(n-1) \ldots (n-i+1)}{i!} \) ordered selections.

Now given a selection of \( i \) elements out of \( n \), there are \( i! \) ways to order these \( i \) elements. Thus each unordered selection corresponds to exactly \( i! \) ordered selections. In other words,

\[ \text{Number of unordered selections} = \frac{\text{Number of ordered selections}}{i!}, \]

and the proposition follows. \( \square \)

**Proposition:** Let \( \overline{x} = (x_1, \ldots, x_n) \) be a word in \( F_q^n \). Then the number of words \( \overline{y} = y_i = (y_1, \ldots, y_n) \) such that \( d(\overline{x}, \overline{y}) = r \) is

(a) \( \binom{n}{r} \), if \( q = 2 \), and more generally,
(b) \((q - 1)^r \binom{n}{r}\) for arbitrary \(q \geq 2\).

Proof. (a) \(\overline{y}\) is completely determined by the choice of \(r\) positions where it differs from \(\overline{x}\). If \(i\) is one of those positions, then \(y_i\) is uniquely determined by the requirement that \(y_i\) should be different from \(x_i\): if \(x_i = 1\), then \(y_i = 0\) and if \(x_i = 0\), then \(y_i = 1\). Thus the number of \(\overline{y}\) at distance \(r\) from \(\overline{x}\) is the number of ways to choose \(r\) positions out of \(n\). This number is, by definition, \(\binom{n}{r}\).

(b) \(\overline{y}\) is completely determined by the choice of \(r\) positions where it differs from \(\overline{x}\) and the \(r\) elements that are used to fill these \(r\) positions. If \(i\) is one of these positions, then \(y_i\) can be any element of \(F_q\), other than \(x_i\). there are \(q - 1\) such choices. Thus the number of \(\overline{y}\) at distance \(r\) from \(\overline{x}\) is \((q - 1)^r \binom{n}{r}\). \(\square\)

Binomial coefficients appear in just about every area of mathematics. There are many intricate identities involving them. Here is a small sample.

(1) \(\binom{n}{i} = \binom{n}{n-i}\).

(2) \(\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n\).

(3) \(\binom{n}{i} = \binom{n-1}{i} + \binom{n}{i}\).

Can you prove these?

The Hamming Bound
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 \( A_2(n, d) = A_2(n-1, d-1) \).

**Perfect codes**

A \( q \)-ary \((n, M, 2t + 1)\)-code \( C \) is called perfect if it meets the Hamming bound, i.e., if

\[
|C| = \frac{q^n}{\sum_{m=0}^{t} \binom{n}{m} (q - 1)^m}.
\]

In other words, \( |C||B_t| = |F^n| \). This means that the Hamming balls of radius \( t \) centered at the codewords of \( C \) form a partition of \( F_q^n \), i.e., they are pairwise disjoint and their union is all of \( F_q^n \).

Note that a necessary condition for a \( q \)-ary \((n, M, d)\)-code to be perfect is that \( d \) should be odd, \( d = 2t + 1 \), and expression \( \frac{q^n}{\sum_{m=0}^{t} \binom{n}{m} (q - 1)^m} \) should be an integer. (These necessary conditions may not be sufficient!)
A perfect code is very convenient for decoding, because every received codeword \( \overline{y} \) lies in exactly one of these balls \( B_t(\overline{x}) \), with \( \overline{x} \) is in \( C \): we decode \( \overline{y} \) as \( \overline{x} \). Unfortunately, perfect codes are rare.

Example: Let us take a closer look at perfect codes \( q = 2, t = 1 \). Then a code \( C \) is perfect iff:

\[
|C| = \frac{2^n}{1 + n}
\]

A necessary condition for this is that right hand side (RHS) must be an integer. This means that \( n = 2^\ell - 1 \) for some \( \ell \). So, the only possibilities are \( n = 3, 7, 15, 31, \ldots \) (\( n = 1 \) is too small). As we shall see later in the course, these are all achievable.

Question: Which bound is better, Hamming or Singleton?

I will address this question at the beginning of the next lecture.