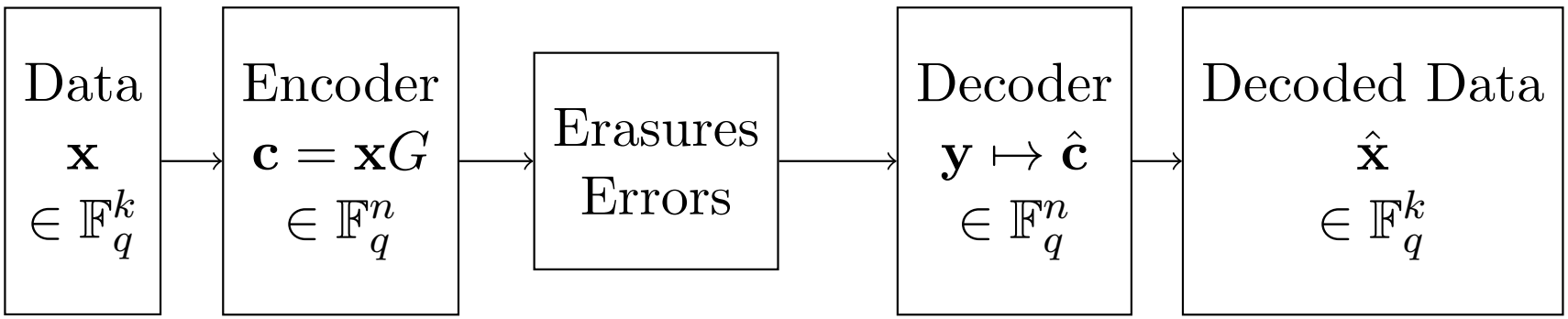
Coding Theory: Rate and Sphere Packing Bound

A Generic Communication Channel

Transmitter | Channel | Receiver



$d_H(\mathcal{C}) = d$ means $\mathcal{C}$ can recover from $d-1$ erasures and $t = \lfloor \frac{d-1}{2} \rfloor$ errors. Syndrome decoding achieves it.

Rate

For a linear (n, k) code, the fraction k/n.
It measures how much information is being transmitted.

$(n, k, d_H)_q$	k/n	name
$(n, 1, n)_q$	$\frac{1}{n}$	repetition
$(n, n-1, 2)_q$	$\frac{n-1}{n}$	parity check
$(7, 4, 3)_2$	$\frac{4}{7}$	Hamming
$(4, 2, 3)_3$	$\frac{1}{2}$	tetracode

Since

$$0 \leq \frac{k}{n} \leq 1,$$

the closest to 1 the best.

Fundamental problem

Given n and k, find a code $\mathcal{C}$ with $d_H(\mathcal{C})$ as high as possible.

Given n and d, determine the maximum number of codewords in a code $\mathcal{C}$ of length n and minimum distance d.

If the code is not linear, replace k with "number of codewords".

$A_q(n,d),\ B_q(n,d)$

$A_q(n,d)$ = number of codewords in a code over $\mathbb{F}_q$ of length n and minimum distance at least d.

$B_q(n,d)$ = number of codewords in a linear code over $\mathbb{F}_q$ of length n and minimum distance at least d.

Since linear brings a restriction

$$B_q(n,d) \leq A_q(n,d).$$

Sphere Packing Bound

$$B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i},$$

$t = \lfloor \frac{d-1}{2} \rfloor$.

Suppose $\mathcal{C}$ contains M codewords. Spheres of radius t about distinct codewords are disjoint and there are $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ vectors in any of these spheres.

Then $M \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ cannot be more than the number q^n of vectors in $\mathbb{F}_q^n$.

Perfect code

A code whose parameters match the Sphere Packing Bound with equality.

Equality in the Sphere Packing Bound means the space $\mathbb{F}_q^n$ is filled with disjoint spheres of radius t.

Every vector in $\mathbb{F}_q^n$ is contained in precisely one sphere of radius t.

The $(4, 2, 3)_3$ tetracode

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

The $(4, 2, 3)_3$ tetracode

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

The code contains $3^2 = 9$ codewords and

$$SPB = \frac{3^4}{\sum_{i=0}^{1} \binom{4}{i} 2^i} = \frac{3^4}{1+8} = 3^2$$

so this code is perfect.

The $(7, 4, 3)_2$ Hamming code

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

The $(7, 4, 3)_2$ Hamming code

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

The code contains $2^4 = 16$ codewords and

$$SPB = \frac{2^7}{\sum_{i=0}^{1} \binom{7}{i}} = \frac{2^7}{1+7} = 2^4$$

so this code is perfect.

Binary Hamming codes

For $n = 2^r - 1$, $r \geq 2$, and $q = 2$, codes whose parity check matrix is having as columns, in order, the binary representation of $1, \ldots, 2^r - 1$.

For $r = 2$:

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

For $r = 3$:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Hamming codes

Binary Hamming codes have parameters: $(n = 2^r - 1, k = n - r, 3)$, $r \geq 2$,

- $n = 2^r - 1$ by construction.
- H is an $(n - k) \times n$ of rank $n - k$, since there are r rows, we have $r = n - k$ so $k = n - r$.
- We can find $d = 3$ columns of H linearly dependent (e.g. those which are the binary representation of 1,2 and 3), but no $d - 1 = 2$ colums are linearly dependent, so the Hamming distance is 3.

q-ary Hamming codes

For $n = 2^r - 1$, $r \geq 2$, and q a prime power, codes whose parity check matrix is having as columns a nonzero vector from each 1-dimensional subspace of $\mathbb{F}_q^r$.

For $r = 2$ and $q = 3$,

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

For $r = 3$ and $q = 3$:

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

q-ary Hamming codes

q-ary Hamming codes have length $n = \frac{q^r-1}{q-1}$, $r \geq 2$.

We need to count 1-dimensional subspaces of $\mathbb{F}_q^r$.

A subspace is defined by a single vector which is not zero, there are $q^r - 1$ such vectors.

Each vector has $q - 1$ non-zero multiples included within the subspace it generates, giving

$$\frac{q^r - 1}{q - 1}.$$

q-ary Hamming codes

q-ary Hamming codes have parameters $(n = \frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3)$, $r \geq 2$.

- We already computed n.
- H is an $(n-k) \times n$ of rank $n-k$, since there are r rows, we have $r = n - k$ so $k = n - r$.
- We can find $d = 3$ columns of H linearly dependent (e.g. those which are the binary representation of 1,2 and 3 (or a multiple)), but no $d - 1 = 2$ colums are linearly dependent (we removed the multiples), so the Hamming distance is 3.

q-ary Hamming codes

q-ary Hamming codes are perfect.

q-ary Hamming codes

q-ary Hamming codes are perfect.

- For $r \geq 2$, q-ary Hamming codes have parameters $(n = \frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3)$, and

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

- The bound becomes $SPB = \frac{q^n}{\sum_{i=0}^{1} \binom{n}{i}(q-1)^i} = \frac{q^n}{1+n(q-1)}$.
- Since $n(q-1) = q^r - 1$, $SPB = \frac{q^n}{q^r} = q^k$.

Sphere Packing Bound
Questions

- More perfect codes? Yes, they are in fact classified (any non-trivial perfect code over a prime-power alphabet has the parameters of a Hamming code or a Golay code).

Sphere Packing Bound
Questions

- More perfect codes? Yes, they are in fact classified (any non-trivial perfect code over a prime-power alphabet has the parameters of a Hamming code or a Golay code).
- Checking that Hamming codes satisfy the Sphere Packing bound only involved their parameters, could there be other codes with the same parameters? (the answer is no, and will be discussed in the next lecture together with code equivalence).

Rate

Sphere Packing Bound

Perfect codes

Hamming codes