

Lecture 17: Best Codes and The Hamming Bound

ENGR 76 lecture notes — May 26, 2026

David Tse, Stanford University

In last week's quiz, we compared several different codes of length $n = 7$. We saw that different codes achieve different tradeoffs between rate and error correction capability. So we cannot say that one code is better than another. This raises a natural question:

Which codes are the best?

Today we study this question by deriving *an upper bound* on the code rate that can be achieved by *any* code with a given error correction capability and seeing whether any of the three codes meet the upper bound. The upper bound is derived through a geometric viewpoint. The key idea is to think of codewords as points in the binary space $\{0, 1\}^n$, and to ask how many codewords can be packed into this space while still keeping them far apart from each other. This leads to the *Hamming bound*, also known as the *sphere-packing bound*.

1 The tradeoff picture

Recall the three codes from the quiz, all of length $n = 7$:

- Repetition code: $(7, 1)$
- Hamming code: $(7, 4)$
- Single parity-check code: $(7, 6)$

We can also include the uncoded scheme $(7, 7)$ as a reference point.

For a code of length n , let:

- M = number of codewords,
- $r = \frac{\log_2 M}{n}$ = code rate,
- $d_{\min}$ = minimum Hamming distance,
- $t = \lfloor \frac{d_{\min} - 1}{2} \rfloor$ = number of bit flips the code can correct.

We will plot the pair

$$\left(\frac{t}{n}, r \right),$$

i.e., (error tolerance rate, code rate).

The figure makes clear that there is no single code among these examples that is best in both parameters. Higher reliability usually comes at the expense of lower rate. The real question is: *what is the best rate one can achieve for a given error correction capability?* Do any of these codes achieve that, i.e., are any of them optimal?

The first easy observation is that the single parity-check code is definitely not optimal; the trivial uncoded scheme does better and is in fact trivially optimal for error tolerance rate 0. To see whether the other codes are optimal, we need to do a bit of work.

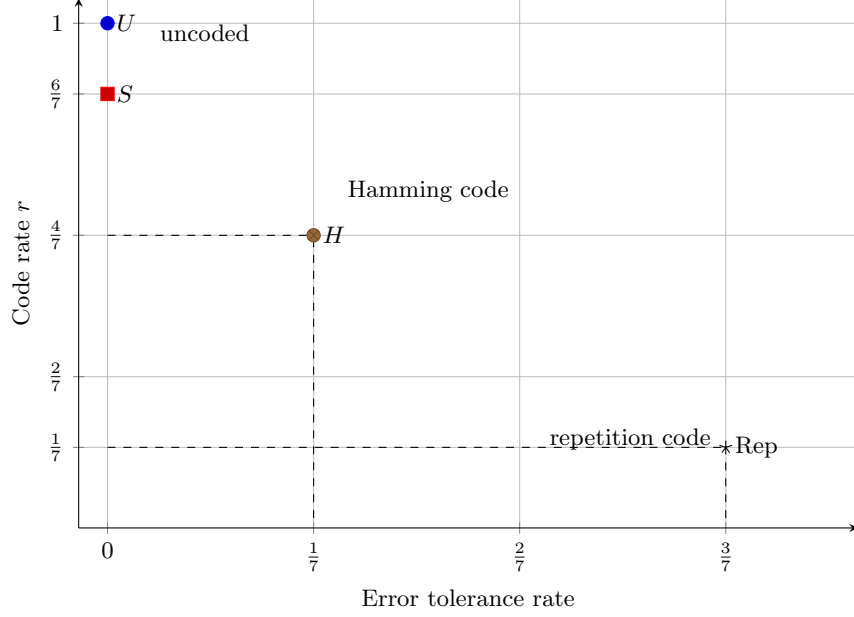


Figure 1: Tradeoff between error tolerance rate and code rate for the quiz examples. Here U denotes the uncoded scheme, S the single parity-check code, H the $(7, 4)$ Hamming code, and Rep the repetition code.

2 A geometric viewpoint

We now interpret codewords as points in the binary space $\{0, 1\}^n$. For example, when $n = 7$, there are

$$2^7 = 128$$

possible binary strings.

If a code can correct t bit flips, then whenever a codeword c is transmitted, any received word within Hamming distance t of c must decode back to c . This means that the Hamming balls of radius t around distinct codewords must be disjoint.

Definition. For a codeword $c \in \{0, 1\}^n$, the *Hamming ball of radius t* around c is

$$B(c, t) = \{x \in \{0, 1\}^n : d(x, c) \leq t\}.$$

The size of a Hamming ball depends only on n and t , not on the center:

$$|B(c, t)| = \sum_{i=0}^t \binom{n}{i}.$$

Indeed, to obtain a word at distance i from c , we choose which i coordinates to flip.

This disjointness immediately yields the Hamming bound.

3 The Hamming bound

Theorem (Hamming bound / sphere-packing bound). *Let C be a binary code of length n with M codewords and minimum distance $d_{\min}$, which can correct*

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

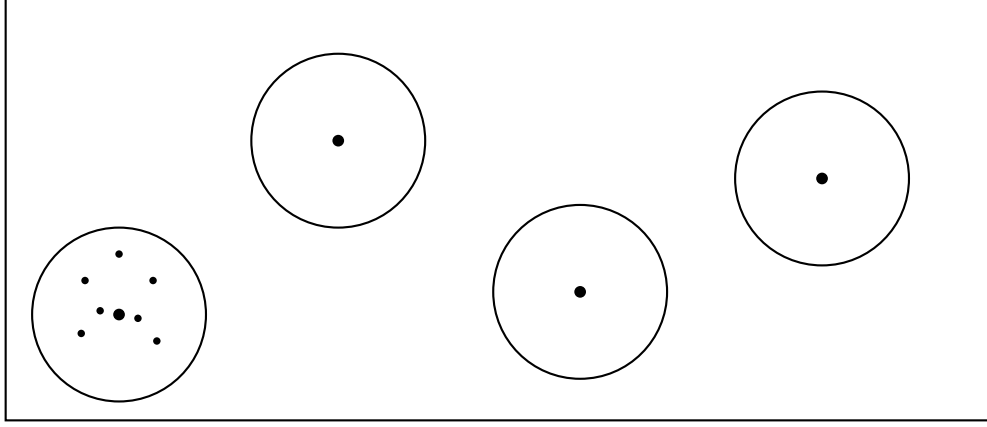


Figure 2: Sphere packing in the Hamming cube. To correct t errors, the Hamming balls of radius t around the codewords must be disjoint.

bit flips. Then

$$M \sum_{i=0}^t \binom{n}{i} \leq 2^n.$$

Equivalently,

$$M \leq \frac{2^n}{\sum_{i=0}^t \binom{n}{i}}.$$

Proof. Each codeword c has a Hamming ball $B(c, t)$ around it, and each such ball contains

$$\sum_{i=0}^t \binom{n}{i}$$

words. Because the code corrects t errors, these balls must be disjoint. Since all of them lie inside the ambient space $\{0, 1\}^n$, which has size 2^n , we obtain

$$M \sum_{i=0}^t \binom{n}{i} \leq 2^n.$$

□

4 Applying the bound to the quiz examples

We now return to the quiz with $n = 7$.

1. The Hamming code

The $(7, 4)$ Hamming code has minimum distance $d_{\min} = 3$, so it corrects

$$t = 1$$

error. The Hamming bound gives

$$M \leq \frac{2^7}{1 + \binom{7}{1}} = \frac{128}{1 + 7} = \frac{128}{8} = 16.$$

Hence

$$r \leq \frac{\log_2 16}{7} = \frac{4}{7}.$$

The Hamming code has exactly $M = 16$ codewords, so it *meets the bound with equality*. Such a code is called a *perfect code*. Clearly, this code is also *optimal*, i.e., it achieves the highest code rate for a given error correction capability of correcting 1 error.

2. The repetition code

The length-7 repetition code has minimum distance

$$d_{\min} = 7,$$

so it corrects

$$t = 3$$

errors. The Hamming bound gives

$$M \leq \frac{2^7}{1 + \binom{7}{1} + \binom{7}{2} + \binom{7}{3}} = \frac{128}{1 + 7 + 21 + 35} = \frac{128}{64} = 2.$$

Hence

$$r \leq \frac{\log_2 2}{7} = \frac{1}{7}.$$

The repetition code has exactly 2 codewords, so it also meets the bound with equality. Thus the repetition code is another perfect code.

5 The “for fun” quiz question

The three codes achieve error tolerance rates of 0, $1/7$ and $3/7$. That leaves $2/7$, $4/7$, $5/7$, $6/7$ and 1.

First it is clear that no codes can achieve error tolerance rates greater than $3/7$, because $d_{\min}$ cannot be greater than 7. This leaves only the question of finding a code that can achieve error tolerance rate of $2/7$. This leads to the last question we asked on the quiz: does there exist a code of length 7 that can correct 2 bit flips and has rate strictly larger than the repetition code?

To correct 2 errors, we need

$$d_{\min} \geq 5, \quad t = 2.$$

The Hamming bound gives

$$M \leq \frac{2^7}{1 + \binom{7}{1} + \binom{7}{2}} = \frac{128}{1 + 7 + 21} = \frac{128}{29} \approx 4.41.$$

Therefore

$$M \leq 4, \quad r \leq \frac{\log_2 4}{7} = \frac{2}{7}.$$

So the Hamming bound alone does *not* rule out a code with rate bigger than $\frac{1}{7}$. It only says the rate cannot exceed $\frac{2}{7}$.

However, for this particular $n = 7$ problem, we can prove something stronger.

A stronger bound

Assume, without loss of generality, that 0000000 is a codeword. (This is without loss of generality because XORing every codeword with a fixed codeword preserves all pairwise Hamming distances, so one can translate any set of codewords to one with an all-zeros codeword without changing the minimum distance.) If $d_{\min} \geq 5$, then every other codeword must have Hamming weight at least 5.

Now take any two codewords x and y of weight at least 5. Since there are only 7 coordinates, the supports of x and y must overlap in at least

$$5 + 5 - 7 = 3$$

positions. Hence x and y can differ in at most

$$7 - 3 = 4$$

positions, so

$$d(x, y) \leq 4.$$

Therefore two distinct nonzero codewords cannot both coexist in a code with minimum distance at least 5.

So the code can contain at most

$$0000000$$

and one additional codeword. Thus

$$M \leq 2, \quad r \leq \frac{1}{7}.$$

This shows that the repetition code is in fact optimal even among all length-7 codes correcting 2 errors.

6 Perfect codes

A code is called *perfect* if the Hamming balls around its codewords exactly fill the ambient space, with no overlaps and no gaps.

Definition. A binary code C correcting t errors is called *perfect* if

$$M \sum_{i=0}^t \binom{n}{i} = 2^n.$$

For $n = 7$, we have seen two perfect codes:

- the $(7, 4)$ Hamming code, which is perfect for $t = 1$,
- the $(7, 1)$ repetition code, which is perfect for $t = 3$.

These two examples sit at different points in the tradeoff plot of Figure 1, but both are optimal for their respective error correction levels. Each code is also known as *Pareto-optimal*, which means that no one can find another code that is strictly better in code rate for the same error tolerance rate, or another code that is strictly better in error tolerance rate for the same code rate. (In the tradeoff figure above, that means the points achieved by these codes cannot be improved by going up or going to the right.)

7 Takeaways

- A codeword is a point in $\{0, 1\}^n$.
- To correct t errors, we need disjoint Hamming balls of radius t around the codewords.
- Counting the total number of points in these balls yields the Hamming bound:

$$M \sum_{i=0}^t \binom{n}{i} \leq 2^n.$$

- The $(7, 4)$ Hamming code and the length-7 repetition code meet this bound with equality, and are therefore perfect.
- The bound is not always tight: for the $t = 2, n = 7$ case, it gives $M \leq 4$, whereas the true maximum is only $M \leq 2$.
- For block length 7, we have identified all the Pareto-optimal points among binary codes: $(0, 1), (1/7, 4/7), (3/7, 1/7)$

In the next lecture, we will see whether we can accomplish this last task for *all* block lengths.