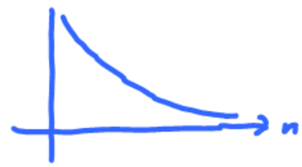
4.5 Shannon's Coding theorem

4.42. Shannon's (Noisy Channel) Coding theorem [Shannon, 1948]

(a) Reliable communication over a (discrete memoryless) channel is possible if the communication rate R satisfies $R < C$, where C is the channel capacity.

In particular, for any $R < C$, there exist codes (encoders and decoders) with sufficiently large n such that

$$P(\mathcal{E}) \leq 2^{-n \times E(R)},$$



where $E(R)$ is

- a positive function of R for $R < C$ and
- completely determined by the channel characteristics

$R>C$

(b) At rates higher than capacity, reliable communication is impossible.

4.43. Significance of Shannon's (noisy channel) coding theorem:

(a) Express the limit to reliable communication

(b) Provides a yardstick to measure the performance of communication systems.

- A system performing near capacity is a near optimal system and does not have much room for improvement.
- On the other hand a system operating far from this (C) fundamental bound can be improved (mainly through coding techniques).

4.44. Shannon's nonconstructive proof for his coding theorem

- Shannon introduces a method of proof called **random coding**.
- Instead of looking for the best possible coding scheme and analyzing its performance, which is a difficult task,
  - all possible coding schemes are considered
    - by generating the code randomly with appropriate distribution
  - and the performance of the system is averaged over them.

- Then it is proved that if $R < C$, the average error probability tends to zero.

- Again, Shannon proved that
  - as long as $R < C$,
  - at any arbitrarily small (but still positive) probability of error,
  - one can find (there exist) at least one code (with sufficiently long block length n) that performs better than the specified probability of error.

- If we used the scheme suggested and generate a code at random, the code constructed is likely to be good for long block lengths.

- No structure in the code. Very difficult to decode

4.45. Practical codes:

- In addition to achieving low probabilities of error, useful codes should be "simple", so that they can be encoded and decoded efficiently.

- Shannon's theorem does not provide a practical coding scheme.

- Since Shannon's paper, a variety of techniques have been used to construct good error correcting codes.
  - The entire field of coding theory has been developed during this search.

- Turbo codes have come close to achieving capacity for Gaussian channels.