Theorem
The average height $a$ of a $k$-ary tree having $n$ leaves satisfies
$$ a = \log_k(n) $$

Corollary
The average height $a$ of a binary tree having $n$ leaves satisfies
$$ a \geq \log(n) $$

See P. 416 of Brassard & Bratley for Proof of Corollary ($k=2$).

Theorem
Any comparison sort must, in average case, at least $\log(n!)$ comparisons on input arrays of length $n$.

Corollary
Any comparison based sorting algorithm runs in (average case) time $\Omega(n \log(n))$. 
(1) **Determine the maximum number of outcomes to each test of the input data**, call that number \( k \).

(2) **Determine the number of verdicts** \( f(n) \) (i.e., possible algorithm outputs) as a function of the **input size** \( n \).  
   - e.g., searching: \( f(n) = n \)  
   - sorting: \( f(n) = n! \)

(3) **Conclude** that any algorithm which solves the problem using only tests of the kinds analyzed in (1) **must do at least**

\[
\text{Worst case: } \lceil \log_k f(n) \rceil \\
\text{Average case: } \log_k f(n)
\]

**Tests on input of size** \( n \).

**Note:** These arguments do **not** assert the existence of algorithms which perform the number of tests listed above. Instead they assert the non-existence of algorithms which do fewer tests.
ADVERSARY ARGUMENTS

Consider again the game of 20 questions, except now your opponent cheats.

Call the players A and B.

A: Pretends to pick \( x \in \{1, \ldots, 10^6\} \)

B: Asks a sequence \( Q_1, Q_2, \ldots \) of yes/no questions (each question depends on preceding answers.)

A: Always gives an answer which is consistent with all previous answers, but which is designed to prolong the game as far as possible.

For A's answers to be consistent, there must always exist an \( x \in \{1, \ldots, 10^6\} \) such that if \( x \) had been picked (by an honest player), the true answers would have been those given by A.

How long can A keep this up? The answer to this question provides a lower bound on the worst case number of questions which must be asked by any algorithm playing the part of B.
we must specify a strategy for answering questions.

Let \( S_i \) denote the remaining set of candidates for the mystery number \( x \) after the \( i \)th question has been asked (and answered.)

\[ S_0 = \{1, \ldots, 10^6\} \]

Let \( Q_i \) = \( i \)th question, and let \( A_i(x) \) denote the (true) answer to \( Q_i \) if the mystery number is \( x \).

\[ Q_1 = \text{"is } x \leq 500,000\text{"} \]
\[ A_1(400,000) = \text{'yes'} \]
\[ A_1(600,000) = \text{'no'} \]

Let \( Y_i = \{ x \in S_{i-1} \mid A_i(x) = \text{'yes'} \} \)
\[ N_i = \{ x \in S_{i-1} \mid A_i(x) = \text{'no'} \} \]

\[ Q_1 = \text{"is } x \leq 500,000\text{"} \]
\[ Y_1 = \{1, \ldots, 500000\} \]
\[ N_1 = \{500001, \ldots, 1000000\} \]

Note \( Y_i \cap N_i = \emptyset \) and \( Y_i \cup N_i = S_{i-1} \). Thus
\[ |Y_i| + |N_i| = |S_{i-1}| \]
By the Pigeonhole Principle, at least one of $Y_i$ or $N_i$ must contain at least:

$$\left\lceil \frac{|S_{i-1}|}{2} \right\rceil$$

As strategy is to always answer $Q_i$ in a way which implies $x$ is in the larger of the two sets $Y_i$ or $N_i$.

Thus

$$S_i = \begin{cases} Y_i & |Y_i| \geq |N_i| \\ N_i & |Y_i| < |N_i| \end{cases}$$

Therefore

$$|S_i| \geq \left\lceil \frac{|S_{i-1}|}{2} \right\rceil$$

Let $b_i = |S_i|$ so that $b_i \geq \left\lceil b_{i-1}/2 \right\rceil$ for $i > 0$. Then

- $b_0 = 10^6$
- $b_1 \geq \left\lceil 10^6/2 \right\rceil$
- $b_2 \geq \left\lceil 10^6/2^2 \right\rceil$
- $\vdots$
- $b_{19} \geq \left\lceil 10^6/2^{19} \right\rceil = 2$
- $b_{20} \geq \left\lceil 10^6/2^{20} \right\rceil = 1$
Thus if $R$ claims to know $x$ after no more than 19 questions, then $A$ can claim at least one number other than $x$ (which is consistent with all his previous answers) as his true pick.

Therefore any algorithm which plays the part of $R$ must ask at least 20 questions, in worst case.

An adversary account for a lower bound process as follows.

- **Start the algorithm on an input which is unspecified, except as to size.**

- Whenever the algorithm processes the input data a malevolent adversary (also called a daemon) answers in a way which makes the algorithm work hard. He is consistent in that there must always exist an input (of the given size) which would elicit the daemon's sequence of answers.
• The daemon's strategy for prolonging the run time must be specified exactly.

• Prove that there is a number M (depending on input size) such that if the algorithm were to produce an output after fewer than M probes, then there exists at least one input which is consistent with all the daemon's answers, but whose correct solution is different from the algorithm output.

• Conclude that M is a lower bound on the worst case number of probes which must be performed by any algorithm which solves the problem.

Just as with any lower bound argument, the above program does not prove the existence of an algorithm which can solve the problem using at most M probes. Instead, it proves the non-existence of an algorithm which solves the problem using at most M - 1 probes.
ADVERSARY ARGUMENTS ARE MORE COMPLICATED
THAN DECISION TREE ARGUMENTS. WHY
DO WE USE THEM?

OFTEN THE LOWER BOUND OBTAINED BY A
DECISION TREE IS FAR FROM TIGHT.

PROBLEM

Given an array \( A[1 \ldots n] \) of numbers, find
its maximum entry and the index where
it is located.

WE CONSIDER ONLY ALGORITHMS WHICH ARE RESTRICTED
TO PERFORMING COMPARISONS OF ARRAY ELEMENTS,
(i.e. NO ARITHMETIC OPERATIONS ON ELEMENTS.)
THIS IS ANALOGOUS TO THE CLASS OF COMPARISON
SORTS.

DECISION TREE LOWER BOUND:

\[
\begin{align*}
\# \text{ Outcomes per Test} &= k = 2 \\
\# \text{ Verdicts} &= n \\
\therefore h &\geq \lceil \log n \rceil
\end{align*}
\]

Thus any algorithm does at least \( \lceil \log n \rceil \)
comparisons (in worst case) on input
of size \( n \).