Algorithms, NP

July 22, 2014

Horse Paradox

Claim: In any group of n horses, all the horses are the same color.
Base Case: In any group of one horse, all the horses are the same color.
Inductive Step: Assume that k horses always are the same color.
Let us consider a group consisting of $k+1$ horses.
Horses $h_1, \ldots h_k$ are the same color since k horses always are the same color. Likewise, horses $h_2, \ldots, h_{k+1}$ are the same color.
Therefore, h_1 is of the same color as horses $h_2, \ldots, h_k$, who in turn are of the same color as h_{k+1}. Hence the first horse, middle horses, and last horse are all of the same color.

Sample responses

- The proof is false because you are proving something that's false.
- The writer didn't say he/she was using induction.
- $P(n)$ is not vivid enough.
- $P(n)$ is not well defined.
- You are assuming $P(k+1)$, which is what you are trying to prove.
- You can't assume that horses $h_2, \ldots, h_{k+1}$ are the same color. You can only assume that horses $h_1, \ldots, h_k$ are the same color.
- You need to include $n = 2$ in the base case.
- Horses $h_1, \ldots, h_k$ might be one color, and horses $h_2, \ldots, h_{k+1}$ might be another color, but they're not necessarily the same color.

Answer

Consider the statement "h_1 is of the same color as horses $h_2, \ldots, h_k$, who in turn are of the same color as h_{k+1}."
This statement makes no sense when $k = 1$, because horses $h_2, \ldots, h_k$ don't exist.

Multiplication

The standard procedure for multiplying two n-digit numbers is $O(n^2)$.
Suppose $x = x_1 10^m + x_0$ and $y = y_1 10^m + y_0$, where x_1, x_0, y_1, y_0 are $(n/2)$-digit numbers.
Calculating

$$x_1 yp_1 10^{2m} + (x_0 y_1 + x_1 y_0) 10^m + x_0 y_0$$

requires 4 multiplications of $(n/2)$-digit numbers.

Karatsuba's algorithm

Instead, calculate $x_1 y_1$, $x_0 y_0$, and

$$(x_1 + x_0)(y_1 + y_0) - x_1 y_1 - x_0 y_0.$$

Calculating

$$x_1 yp_1 10^{2m} + (x_0 y_1 + x_1 y_0) 10^m + x_0 y_0$$

requires 3 multiplications of $(n/2)$-digit numbers.

P is the set of all yes/no problems that can be solved in polynomial time.
Example: (s, t)-connectivity is in P
Cobham's thesis says that

NP

NP stands for "non-deterministic polynomial time."
Problems in NP are yes/no problems where, if the answer is "yes," then

- there is a proof that the answer is "yes," and
- this proof can be verified in polynomial time.

Example: Is a graph 3-colorable?

NPC

NP-complete problems are the hardest problems in NP.
No polynomial time algorithms have been found for NP-complete problems, and it is conjectured that none exist.

3-colorability

Input: graph G
Question: Can G be 3-colored?

Boolean Satisfiability Problem

Input: A logical formula
Question: Is there an assignment of true/false values to the variables in the formula such that the entire formula is true?

Independent set problem

definition

Given a graph G, an **independent set** is a set of vertices $S \subseteq V(G)$ such that no two vertices in S are connected by an edge in G.

Input: Graph G, positive integer k.
Question: Does there exist an independent size in G of size k?

Vertex cover problem

Definition

Given a graph G, a **vertex cover** is a set of nodes $S \subseteq V(G)$ such that every edge in G has at least one endpoint in S.

Input: Graph G, positive integer k.
Question: Does there exist an vertex cover in G of size k?

Clique problem

Definition

A **clique** is a complete graph.

Input: Graph G, positive integer k.
Question: Is K_k a subgraph of G?

Hamiltonian cycle problem

Definition

A Hamiltonian cycle in a graph is a cycle that visits all of the vertices exactly once.

Input: Graph G
Question: Does there exist a Hamiltonian cycle in G?

Traveling Salesman Problem

Input: Complete graph K_n where every edge is labeled with a distance
Question: What is the shortest Hamiltonian path in G, where the length of a path is the sum of the distances of the path's edges?

Proof by contradiction

- I want to prove that P is true.
- I assume that $\neg P$ is true.
- I prove that both Q and $\neg Q$ are true.
- This is impossible, so my initial assumption of $\neg P$ must be wrong.
- Thus, P is true.

$\sqrt{2}$

Proposition

$\sqrt{2}$ is irrational.

Infinitude of primes

Proposition

There are infinitely many prime numbers.

Compression

A compression algorithm is lossless if any input file can be reconstructed from its input file.

Proposition

There is no lossless compression algorithm that shrinks all files.

Sets of sets

Sets can contain sets as elements

Example: $\{\{1, 2\}, 3, \{3\}\}$

Power Sets

The power set of A is the set of all subsets of A and is denoted $\mathbb{P}(A)$.
For example, $\mathbb{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Russell's Paradox

Some sets can contain themselves.

For example, the set of all non-squares is not a square, so it should contain itself.

On the other hand, the set of all squares is not a square, so it does not contain itself.

Let S be the set of all sets that do not contain themselves. Does S contain itself?

Combinations

How many possible 5-card hands are there in a deck of 52 distinct cards?
We define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Combinations

- How many 10-character strings of 0s and 1s have exactly 5 0s?
- How many 10-character strings of uppercase letters contain no more than 3 A's?
- How many ways are there to walk from the origin to (n, k) while only following the grid lines?

Balls and urns

I have 10 balls and 5 urns. The balls are indistinguishable but the urns are distinguishable. How many ways can I put the balls into the urns?

Pascal's triangle and identities

- $$\binom{n}{k} = \binom{n}{n-k}$$
- (Pascal's identity)
$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{}{}$$
- (Hockey Stick identity)

Binomial theorem

What is $(x+y)^n$?