

CS888: Introduction to Profession and Communication Skills -- Theoretical CS

NITIN SAXENA (NITIN@CSE)

[*WITH HELP FROM INTERNET SOURCES]

2024; AUG 21, 23, 28, 30; SEP 4, 6



Proof Techniques

❖ Deduction

❖ If $(\alpha \rightarrow \beta)$ and α , then β .

❖ Induction

❖ If $(\alpha(k) \rightarrow \alpha(k + 1))$ and $\alpha(0)$, then $\forall \ell, \alpha(\ell)$.

❖ Contraposition

❖ If $(\alpha \rightarrow \beta)$, then $(\sim \beta) \rightarrow (\sim \alpha)$.

❖ Contradiction

❖ If $(\alpha \rightarrow \text{False})$, then $(\sim \alpha)$.

❖ Diagonalization

❖ Draw a matrix; *contradict* the diagonal!

```

s1 = 0 0 0 0 0 0 0 0 0 0 0 ...
s2 = 1 1 1 1 1 1 1 1 1 1 1 ...
s3 = 0 1 0 1 0 1 0 1 0 1 0 ...
s4 = 1 0 1 0 1 0 1 0 1 0 1 ...
s5 = 1 1 0 1 0 1 1 0 1 0 1 ...
s6 = 0 0 1 1 0 1 1 0 1 1 0 ...
s7 = 1 0 0 0 1 0 0 0 1 0 0 ...
s8 = 0 0 1 1 0 0 1 1 0 0 1 ...
s9 = 1 1 0 0 1 1 0 0 1 1 0 ...
s10 = 1 1 0 1 1 1 0 0 1 0 1 ...
s11 = 1 1 0 1 0 1 0 0 1 0 0 ...
⋮   ⋮   ⋮   ⋮   ⋮   ⋮   ⋮   ⋮   ⋮   ⋮   ⋮

```

```

s = 1 0 1 1 1 0 1 0 0 1 1 ...

```

Common proof techniques

Proof by intimidation Trivial!

Proof by cumbersome notation The theorem follows immediately from the fact that $|\bigoplus_{k \in S} (\mathbb{R}^{\mathbb{F}^\alpha(i)})_{i \in \mathcal{U}_k}| \leq \aleph_1$ when $[\mathfrak{H}]_{\mathcal{W}} \cap \mathbb{F}^\alpha(\mathbb{N}) \neq \emptyset$.

Proof by inaccessible literature The theorem is an easy corollary of a result proven in a hand-written note handed out during a lecture by the Yugoslavian Mathematical Society in 1973.

Proof by ghost reference The proof may be found on page 478 in a textbook which turns out to have 396 pages.

Circular argument Proposition 5.18 in [BL] is an easy corollary of Theorem 7.18 in [C], which is again based on Corollary 2.14 in [K]. This, on the other hand, is derived with reference to Proposition 5.18 in [BL].

Proof by authority My good colleague Andrew said he thought he might have come up with a proof of this a few years ago...

Internet reference For those interested, the result is shown on the web page of this book. Which unfortunately doesn't exist any more.

Proof by avoidance *Chapter 3:* The proof of this is delayed until Chapter 7 when we have developed the theory even further. *Chapter 7:* To make things easy, we only prove it for the case $z = 0$, but the general case is handled in Appendix C. *Appendix C:* The formal proof is beyond the scope of this book, but of course, our intuition knows this to be true.

facebook.com/Mathematicx

Types of statements

- ❖ **Conjecture**: an unproved belief.
 - ❖ $P \neq NP$.
- ❖ **Axiom**: an unprovable, defining, belief.
 - ❖ Peano's axioms [$s(\cdot)$ is called *successor*].
- ❖ **Hypothesis**: a testable prediction.
 - ❖ Riemann's hypothesis. Church-Turing thesis.
- ❖ **Theorem**: a formal statement with proof.
 - ❖ Prime number theorem.
- ❖ Corollary, Lemma, Claim, Proposition, Fact
 - ❖ diverse assertions from/towards a theorem.
- ❖ **Algorithm** (proved) vs **Heuristic** (unproved).

Peano Axioms for natural numbers

$$\text{PA1 } \forall x (\neg(s(x) = 0))$$

$$\text{PA2 } \forall x \forall y (s(x) = s(y) \rightarrow x = y)$$

$$\text{PA3 } \forall x (x + 0 = x)$$

$$\text{PA4 } \forall x \forall y (x + s(y) = s(x + y))$$

$$\text{PA5 } \forall x (x \cdot 0 = 0)$$

$$\text{PA6 } \forall x \forall y (x \cdot s(y) = x \cdot y + x)$$

$$\text{PA7 } [A(0) \wedge \forall x (A(x) \rightarrow A(s(x)))] \rightarrow \forall x A(x)$$

- “Hypothesis is a tentative prediction or explanation of the relationship between two variables’ It implies that there is a systematic relationship between an independent and dependent variable”.



Fundamental Theorem of Arithmetic: Every positive integer has a prime factorisation, unique up to the order of the factors

Fundamental Theorem of Algebra: Every nonconstant polynomial over the field of complex numbers has at least one root

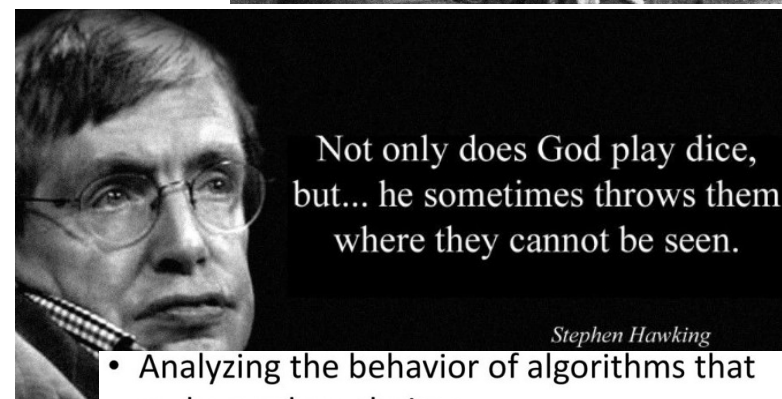
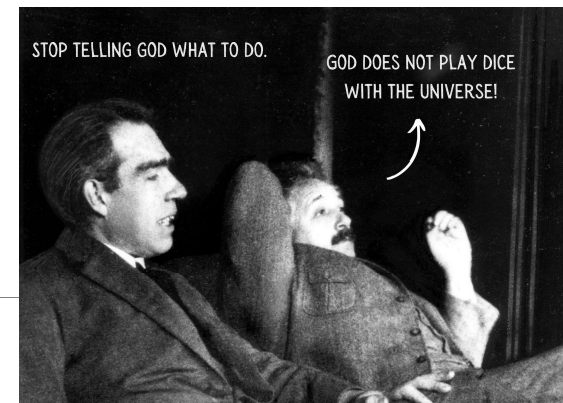
Fundamental Theorem of Calculus: For every continuous function f on an interval $[a, b]$ the function $g(x) = \int_a^x f(t) dt$ is an antiderivative of f on (a, b)

Fundamental Theorem of Linear Algebra: The row space of a matrix is orthogonal to the nullspace of the matrix, and the dimensions add up to the number of columns of the matrix

Does God play dice?

- ❖ CS relies on **probabilities**.
 - ❖ Are they necessary?
- ❖ **Random sampling** is a powerful tool:
 - ❖ algorithms, systems testing, networks
 - ❖ prover-verifier protocol, proof-checking, cryptosystems
 - ❖ ML model with biased input distribution
- ❖ **If I toss any coin the probability of Heads is ½.** 
- ❖ For an *unbiased* coin, probability of Heads is ½.
- ❖ **My ML model works very well on real data.** 
- ❖ My ML model decides x on dataset X with *mean-absolute-error* of 10%.

$$\text{MAE} = \frac{1}{n} \sum_{i=1}^n |x_i - x|$$



- Analyzing the behavior of algorithms that make random choices
 - Running time, performance
- Testing computer systems
 - Generating input/demand to test a system
- Modeling discrete structures
 - Understanding the structure of the internet or social networks

Assignment 8

<https://hello.iitk.ac.in/>

deadline <12pm (end of class)