<https://www.youtube.com/watch?v=L3LMbpZIKhQ&list=PLB7540DEDD482705B>

Tom Leighton

**marten van dijk**

1. Proof: Proof is a method for ascertaining the truth
   1. How to ascertain truth
      1. Experimentation and observing
      2. Sampling and counter examples
2. Mathematical proof:
   1. **Mathematical proof is a verification of a proposition by a chain of logical deductions from a set of axioms**
3. **Proposition:** A proposition is a statement that is either true or false
   1. **Eg:** 2+3=5 is true proposition
   2. **Eg: ∀n ∈ N, n2+n+41** is a prime number
      1. **∀n is the quantifier**
      2. **N = {0,1,2,3,…..} -> Universe of discourse**
      3. **N is natural numbers (non negative)**
      4. **Here n2+n+41** is a prime number is a predicate. Predicate is a proposition whose truth depends on the value of variable n
      5. **To make the proposition true, we need to make this predicate to be true for all values of n**

A black board with white writing

Description automatically generated

* + 1. **Above proposition is false, until n is 40, it breaks for values n 40 and 41 . Hence the proposition is false**
  1. **Ex: a4 + b4  + c4  = d4  has no positive integer solutions** 
     1. **This proposition is conjectured to be true by euler in 1769**
     2. **After 218 years later, it was disprooved by noam elies**
     3. **Correct proposition is :**

**∃ a,b,c,d ∈ N+  then, a4 + b4  + c4  = d4**

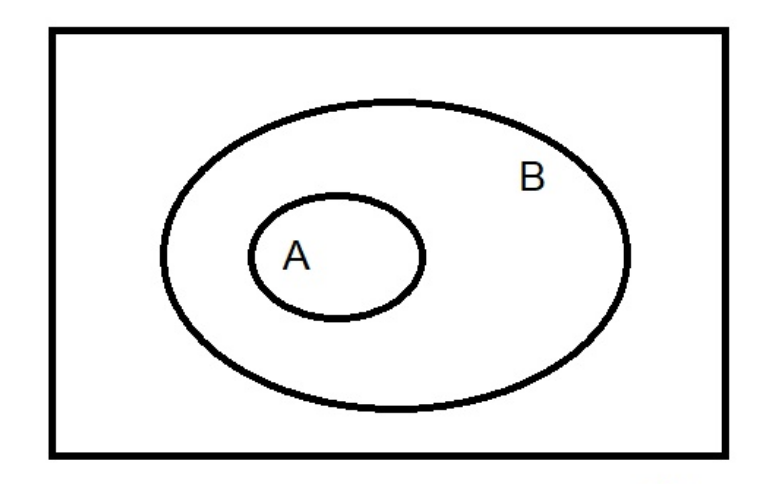
* 1. **313(x3 +y3) = Z3  has no positive integer solution**

A blackboard with white text

Description automatically generated

* 1. **Other Points;**
     1. **Who care about factoring :**
        1. **way to break cryptosystems like rsa**
  2. **Regions in any map can be colored in 4 colors so that adjacent regions have different colors – 4 color theorem . doen by Guthrie in 1853** 
     1. **False proof by kempe in 1879 26 years later than 1853** 
        1. **kempe gave proofs in form of picture which can be very convincing and very wrong**
     2. **heawood found a fatal flaw in the argument**
  3. **Every even integer but 2 is the sum of two primes** 
     1. **eg: 24= 11+13**
     2. **Goldbach’s conjecture by christian goldbach in 1742**
  4. **Rieman hypotheseis in 1859 by bernard riemann**
  5. **poincare conjecture**
  6. **Fields medal – highest prize in mathematics**
  7. **∀n  ∈ z, n >= z ⇒ n2 >=** 4
     1. **where z is {0,1,-1,2,-2,…..}**
  8. **What does implies mean : An implication , A => B is true, if A is false for B is true** 
     1. **truth table**

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **A=>B** |
| **t** | **t** | **t** |
| **t** | **f** | **f** |
| **f** | **t** | **t** |
| **f** | **f** | **t** |



* **Basically we arrive at whether scenario of A and B is possible in truth table, according to venn diagram**
* **In this truth table, if A is true and B is True is possible , Hence A => B for scenario 1**
* **In this truth table, if A is true and B is false, it is not at all possible, because B includes A. Hence this statement is not at all possible. Hence A=>B is false for scenario 2**
* **In this truth table, if A is false, and B is true, then this scenario is possible , Hence A=>B is true for scenario3**
* **in this truth table, if a is false and b is false, then this scenario is possible, hence A=>B is possible for scenario 4**

**if pigs file => i am king**

* 1. **equivalent**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **p** | **q** | **p=>q** | **q<== >p** | **p<== >q** |
| **t** | **t** | **t** | **T** | **t** |
| **t** | **f** | **f** | **t** | **f** |
| **f** | **t** | **t** | **f** | **f** |
| **f** | **f** | **t** | **t** | **t** |

1. **what is not a proposition**
   1. **hello**
2. **what are axioms** 
   1. **Axioms are same like propositions , only difference is that axioms are propositions that we just assume that are true**
   2. **def: axiom is a proposition that is assumed to be true**
   3. **eg: if a=b & b=c, then a=c**
3. **guiding principles to axioms**
   1. **axioms should be consistent**
   2. **and axioms should be complete**
   3. **Def: A set of axioms is consistent if no proposition can be proved to be both true and false**
   4. **def: a sets of axioms is said to be complete if it can be used to prove every proposition is either true or false** 
      1. **there cannot be any axiom that can be consistent and complete**
4. **proof by contradiction**
   1. **To prove proposition p is true, we assume that p is false** 
      1. **i.e.( ¬ P is T) & then use this hypothesis name P is false, to derive a falsehood or contradiction**

A blackboard with white text

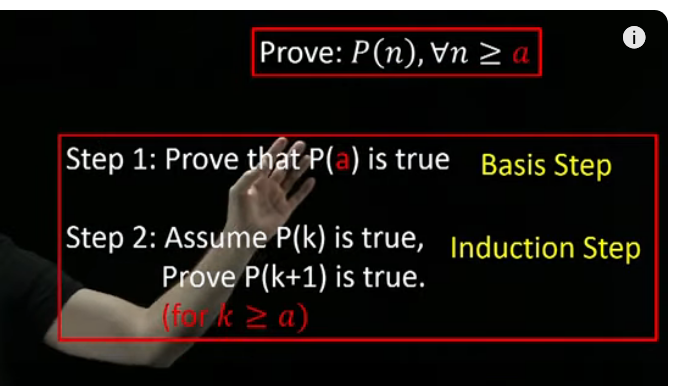
Description automatically generated

**Thus we can conclude P is true if ¬ P => F**

A black board with white text

Description automatically generated

1. **False proof** 
   1. **A false proof is a mathematical argument that contains a logical error and leads to an incorrect conclusion**
2. **Proof by induction** 
   1. **commonly used proof technique in computer science**
   2. **Steps according to DR: Trefor Bazett**



* 1. **Induction Axiom by tom leighton:**

**Let P(n) be predicate, if P(0) is true and ∀ n∈ N,**

**(p(N) => p(N+1)** is True, then **∀ N ,**  P(n) is true

1. 7 characteristics of good proof
   1. Correct
   2. Complete
   3. clear
   4. brief
   5. elegant
   6. well organized
   7. in order

A blackboard with white chalk writing on it

Description automatically generated

* Major crashes with wrong code
  + Therac-25 – cancer treatment
  + boeing 787 crash
  + us 2000 elections

1. top 10 proof techniques that should not be used:
   1. proof by throwing in the kitchen sink 10
   2. proof by example 9
   3. proof by vigorous hand waving 8
   4. proof by cumbersome notation 7
   5. proof by exhaustion 6
   6. proof by omission 5
   7. proof by picture 4
   8. proof by vehement assertion 3
   9. proof by appeal to intuition 2
   10. proof by reference to authority 1

A blackboard with white text

Description automatically generated

A blackboard with white text

Description automatically generated

1. Puzzles
   1. Find sequence of moves to go
2. invariant
   1. very powerful and commonly used concept in computer SCIENCE CLOSELY tied to induction
   2. in order to show your system can never reach a particular special state, it is sufficient to show – there is some property called the invariant that holds at the initial state and is preserved by every legal move.

A blackboard with white chalk on it

Description automatically generated

* 1. PRACTICAL USE OF INVARIANT:
     1. while building software for nuclear reactor, we can prove through invariant that meltdown state
     2. while building software for airplane, we can use invariant to prove that it will never reach the crash state
     3. If we build a radiation device, you never want to get in to the state, that fries the patient

1. Strong induction
   1. like regular induction strong induction can be expressed with an axiom
   2. **strong induction axiom:**
      1. let P(n) be any predicate, if p(0) is true & **∀n  ,** (P(0) ^P(1) ^……….^P(n) are all true , then => p(n+1) is true ,

then **∀n** P(n) is true

A blackboard with white text

Description automatically generated

* 1. difference between strong induction and ordinary induction:
     1. Difference is the highlighted part

A blackboard with white text and red square

Description automatically generated

* + 1. In ordinary induction, we assume P(N) is true,whereas in strong induction we assume, P(0) is true, P(1) is true and upto P(n) we assume it to be true.
    2. Since we assume a lot more in strong induction, it is a stronger proof technique
    3. any proof you can do with strong induction, we can do with ordinary induction

1. puzzle for strong induction: unstacking game
   1. in this game we have a stack of 8 blocks
      1. in the first move, divide the stack into two sub stacks . Here 8 divided into 5 and 3 stacks for which we get 15 (3x5)points

A blackboard with white text

Description automatically generated

A person standing in front of a desk

Description automatically generated

ii) in the next move, stack with 5 points is divided into 1 and 4 , for which we get 4 points

A desk with a few objects on it

Description automatically generated

A chalkboard with a person and numbers

Description automatically generated

iii) We keep on going until i have 8 stacks of 8 stacks of height 1 and the last move will be splitting a two into two ones

iv) At last we add up all points and then we get the final score

v) Final goal is to get the most number of points, when we add the entire score

* 1. Class Vs TA: Class
     1. CLASS IST move: 4 and 4 = 16 points

A blurry image of a person's feet on a table

Description automatically generated A blackboard with white text and numbers

Description automatically generated

* + 1. ta first move:

A stack of wood blocks

Description automatically generated

A chalkboard with a person and numbers

Description automatically generated

* + 1. Class second move:



A blackboard with white chalk writing

Description automatically generated

iv. TA second move:



A chalkboard with a person and numbers

Description automatically generated

v. class third move:

A blurry image of a couple of boxes on a table

Description automatically generated

A chalkboard with a person drawing on it

Description automatically generated

vi. TA third move: 5points

A blurry image of a stack of boxes

Description automatically generated

A person standing next to a chalkboard

Description automatically generated

vii. class 4th move: 2 points: total:

A blurry image of a group of objects

Description automatically generated

A blackboard with white chalk writing on it

Description automatically generated

viii. TA 4th move: 4 points:22 points

A blurry image of a yellow box

Description automatically generated

A blackboard with white chalk writing on it

Description automatically generated

ix. class 5th move: 2points - 26 points total

A blurry image of a table

Description automatically generated

A blackboard with white chalk on it

Description automatically generated

x. TA 5th move: 3 points - 25 points

A yellow rectangular object on a table

Description automatically generated

A screenshot of a blackboard

Description automatically generated

xi. class 6th move: 1point 27 points

A blurry image of a keyboard

Description automatically generated

A person walking on the street

Description automatically generated  
xii. TA 6th move: 2 point : 27 points

A blurry picture of a yellow rectangular object

Description automatically generated

A person standing in front of a chalkboard

Description automatically generated

xiii. class 7th move: 1 point: 28 points

A blurry image of a person's face

Description automatically generated

A blackboard with chalk on it

Description automatically generated

xiv. TA last move 1 point: 28 points

It is a tie

* 1. Is there any strategy possible which could give more than 28 points:
     1. You cannot get more than 28 points
     2. you cannot get less than 28 points
  2. **Theorem:** all strategies for the n-block game produce the same score . S(n)
     1. **eg: S(8) =28**
     2. proof by strong induction
  3. **What should i do, when i am stuck with my induction proof**
     1. **Make the induction hypothesis stronger**

**by: marten van dijk**

1. **number theory:**
   1. **Introduction**
      1. **one of the oldest mathematical disciplines**
      2. **number theory is the study of integers; 0,1,2,3….**
      3. **has application in cryptography**
   2. **number theory definition:**

**m | a i.e. m divides a**

**∃ - There exists**

A blackboard with white text

AI-generated content may be incorrect.

**in words: m divides a, if and only if , there exists an integer K, such that “a” can be written as multiple of m, namely k times m**

A blackboard with white writing on it

AI-generated content may be incorrect.

* 1. **Theorem:**
     1. **We will define a state machine which has states , we can see what kind of possible transitions we can have**
     2. **Once we have modelled all these precisely, we can prove them**
     3. **Assumptions:** 
        1. **we have “a” gallon jug, so a=3 , “b” gallon jug, b=5 and we will assume a is utmost B**

**i.e A<=B**

* + 1. **theorem proof:**

**if m|a and also m|b, then m should divide any result with pouring, emptying and filling those jugs**

A white text on a black background

AI-generated content may be incorrect.

* + 1. **State machine: State machine we use will look like this**
       1. **states we have are: no of gallons, that are present in these two jugs**
       2. **We will denote them by pairs (x,y)**
       3. **Where x denotes number of gallons in “a” jug and y denotes no of gallons in “B” jug**

A blackboard with white text

AI-generated content may be incorrect.

* + - 1. **start state: (0,0)**
      2. **So we have expressed the whole situation/scenario by a pair of numbers**
      3. **Next we need to find, what we can do with it**
  1. **Transitions:** 
     1. **We can fill one of those jugs, empty those jugs**
     2. **pour from one jug into the other one**

A blackboard with white text

AI-generated content may be incorrect.

* + 1. **Filling: transitions**

A blackboard with white text

AI-generated content may be incorrect.

* + 1. **pouring of one jug into another:**
       1. **pouring everything from a to b**

**x+y utmost B, so that B has sufficient space**

A white x on a black background

AI-generated content may be incorrect.

* + - 1. **Pouring from A to B**

A blackboard with white text

AI-generated content may be incorrect. **here x+y should be at least b. i.e. x+y >=b**

* + - 1. **Pouring everything from B to A**

A black background with colorful writing

AI-generated content may be incorrect.

* + - 1. **pour a-x galons from y to jug a which causes a to be completely filled up**

A blackboard with white writing on it

AI-generated content may be incorrect.

* 1. **proof to the theorem using transition states;**

A blackboard with writing on it

AI-generated content may be incorrect.