Course 50.050/50.550
Advanced Algorithms

Week 2 – Lecture L02.02

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Outline of Lecture

- Basic proof methods, proof by contradiction, induction

- Well-ordering principle, Fermat's method of infinite descent

Proofs: Overview of what to expect

Throughout this course, we would encounter numerous proofs.

- We know that theorems are true, that algorithms work as intended, because of proofs.

To understand proofs, we first have to understand proof methods, and how to think about writing proofs.

- Some proof methods are specific to some topic.
  - Graph-theoretic proofs, e.g. for graph algorithms.
    - (more in Weeks 3–6)
  - Number-theoretic proofs, e.g. for cryptography algorithms.
    - (more in Week 9)
  - Geometric proofs, e.g. for coding theory, data processing, etc.
    - (more in Weeks 10–13)
- Some proof methods are more general, and are applicable to all topics, and general problem-solving.
  - Double counting (covered in L02.01)
  - Proof by contradiction (to be covered today).
  - Extremal principle (to be covered in this week's cohort class).
  - Invariance (to be covered in this week's cohort class).
  - Pigeonhole principle (to be covered in Week 3).
  - and more...

Basic proof method: Proof by exhaustion

Idea: Split the statement we want to prove into a **finite** number of easier cases, then check that every case is true.

- **Example from textbook:** The pair $(8, 9)$ is the only pair of consecutive positive integers ≤ 100 that are perfect powers.
  - This statement is true and can be proven by checking all pairs.

More interesting example: (**Four-color theorem**)

Any flat map consisting of regions can be colored using (at most) **four colors**, such that regions sharing a common boundary (except for a single point) do not share the same color.

- First proven in 1977. First ever major theorem with a computer-assisted proof, using proof by exhaustion.
  - A total of 1936 cases were verified by a machine, as part of the first correct proof by exhaustion.
  - We will look into the statement (not proof) of the four-color theorem again in Week 3.

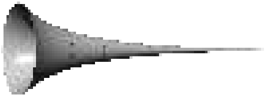
Basic proof method: Proof by counter-example

Idea: For a proposition declaring that all elements in the domain of discourse satisfy a certain property, we can show that the proposition is false by finding **one single counter-example**.

- **Example from textbook:** Is every positive integer always the sum of three perfect squares?
  - Answer: No. The integer 7 is a counter-example. It is not the sum of three perfect squares.

More interesting example: Must a 3-dimensional object with finite volume necessarily have a finite surface area?

- Answer: No. **Gabriel's horn** is a counter-example. It has finite volume, but infinite surface area.



Depiction of Gabriel's horn.

- Take the graph $y = \frac{1}{x}$ for the domain $x \geq 1$, and rotate this graph in 3-dimensional space about the x-axis. The resulting solid of revolution is called Gabriel's horn.

Proof by contradiction

Idea: To show that a proposition is true, start by supposing that the negation of the proposition is true, then get a contradiction.

- This implies that the negation of the proposition is false, so the original proposition must be true.

Example from textbook: $\sqrt{2}$ is an irrational number.

Proof: Suppose on the contrary that $\sqrt{2}$ is rational.

- This means we can write $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}^+$.
  - Assume without loss of generality that the fraction $\frac{a}{b}$ is already written in lowest terms, i.e. a, b have no common divisors other than ± 1.
- Squaring both sides and clearing denominators, we get $2b^2 = a^2$.
  - LHS $2b^2$ is even, so RHS a^2 must be even, which forces a to be even, i.e. $a = 2a_0$ for some $a_0 \in \mathbb{Z}^+$.
  - Then we get $2b^2 = 4a_0^2$, which implies $b^2 = 2a_0^2$.
  - Now $2a_0^2$ is even, so b^2 must be even, which forces b to be even, i.e. $b = 2b_0$ for some $b_0 \in \mathbb{Z}^+$.
- This means $\frac{a}{b} = \frac{2a_0}{2b_0}$ is not written in lowest terms, which is a contradiction.

What is "without loss of generality"?

This is used to indicate that an assumption is made to simplify the argument by considering a specific case, rather than a general case, such that there is **no loss of the validity** of the proof whether we consider this specific case, or we consider the general case.

- Commonly abbreviated as WLOG. Common use of terminology:
  - "Assume without loss of generality that ..."
  - "Without loss of generality, assume that ..."
- Usually used when there is an "obvious" symmetry.
  - **Example:** Suppose we want to prove that for $m, n \in \mathbb{N}$, if either m or n is even, then mn is even.
    - If m is even, then we can write $m = 2m_0$ for some $m_0 \in \mathbb{N}$, thus $mn = 2m_0 n$ is even.
    - If n is even, then we can write $n = 2n_0$ for some $n_0 \in \mathbb{N}$, thus $mn = 2n_0 m$ is even.
    - Both cases have the same general argument, so we can write: "Assume WLOG that m is even. Then we can write $m = 2m_0$ for some $m_0 \in \mathbb{N}$, thus $mn = 2m_0 n$ is even."
- **Warning:** You can use "WLOG" only when it is obvious there is no loss of validity of your proof with your assumption.

Example: Halting problem

Recall from 50.004: The halting problem is described as follows:

- Given a computer program P and some input I, determine whether P will terminate when executed with input I.
  - Return `True` if P will terminate, and return `False` otherwise.
- **Theorem:** The halting problem is unsolvable.

Proof: Suppose on the contrary that the halting problem is solvable.

- i.e. there exists an algorithm $\texttt{halt}(P, I)$ that solves the problem.
- Consider the algorithm `func` whose pseudocode is shown on the right.
- What happens when we run $\texttt{func}(\texttt{func})$?

```
function FUNC(P)
    Require: P is a program.
    if halt(P, P) then
        Run infinite loop
```

Case: $\texttt{halt}(\texttt{func}, \texttt{func}) = \texttt{True}$.

- When we run $\texttt{func}(\texttt{func})$, we enter the if-loop and loop forever.
- This means `func` does not terminate when run with input `func`.
- Thus, by definition, we must have $\texttt{halt}(\texttt{func}, \texttt{func}) = \texttt{False}$.

Case: $\texttt{halt}(\texttt{func}, \texttt{func}) = \texttt{False}$.

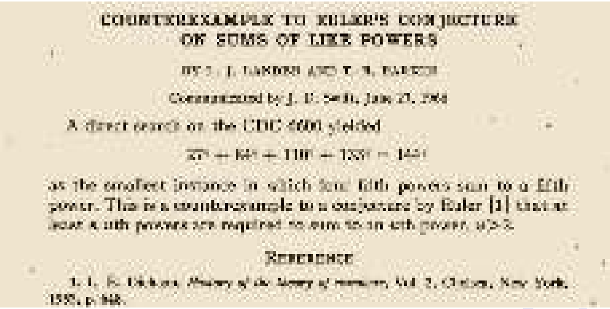
- When we run $\texttt{func}(\texttt{func})$, we do not enter the if-loop.
- This means `func` terminates when run with input `func`.
- Thus, by definition, we must have $\texttt{halt}(\texttt{func}, \texttt{func}) = \texttt{True}$.

Type of proof: Constructive proof

Idea: To show that there exists an object satisfying a certain property, we can **explicitly construct** an example.

- **Example from textbook:** There exists a positive integer that can be written as the sum of perfect cubes in two different ways.
  - Construction: $1729 = 10^3 + 9^3 = 12^3 + 1^3$.
- **Note:** You could have a constructive proof by counter-example.

More interesting example: One of the shortest math research papers (shown below) involves a constructive proof by counter-example.



COUNTEREXAMPLE TO EULER'S CONJECTURE
ON SUMS OF LIKE POWERS

BY L. J. LANDER AND T. R. PARKIN

Communicated by J. D. Swift, June 27, 1966

A direct search on the CDC 6600 yielded

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

as the smallest instance in which four fifth powers sum to a fifth power. This is a counterexample to a conjecture by Euler [1] that at least n nth powers are required to sum to an nth power, $n > 2$.

REFERENCE

1. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, p. 648.

Type of proof: Non-constructive proofs

Proposition: There exist irrational numbers a, b such that a^b is rational.

Proof Idea: $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.

Proof: We saw on Slide 5 that $\sqrt{2}$ is irrational.

- If $\sqrt{2}^{\sqrt{2}}$ is rational, then we can let $a = \sqrt{2}$, $b = \sqrt{2}$.
- If instead $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$.
  - Recall the exponentiation rule: $(x^\alpha)^\beta = x^{\alpha\beta}$.
  - Thus, $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$, which is rational.

Note: This is an example of a non-constructive existence proof.

- An existence proof is a proof that there exists an object satisfying a certain property that we are interested in.

Theorem: (**Intermediate value theorem**) Let $[a, b]$ be a real interval such that $a \neq b$, and let $f : [a, b] \to \mathbb{R}$ be a continuous function such that $f(a) < f(b)$. If $\alpha \in \mathbb{R}$ such that $f(a) < \alpha < f(b)$, then there exists some $c \in \mathbb{R}$, $a < c < b$, such that $f(c) = \alpha$.

- Any proof of this theorem has to be non-constructive.
- We cannot construct and give an explicit c satisfying $f(c) = \alpha$, even though we can show that such a value c exists.

A closer look at induction

Let $P(n)$ be a statement in terms of $n \in \mathbb{N}$.

- **Induction:** If $P(0)$ is true, and if $P(n) \rightarrow P(n+1)$ is true for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.

Recall: (L01.02) In Peano's axioms for arithmetic, the 9th axiom says:

- If S is a set such that $0 \in S$, and if for every $n \in \mathbb{N}$, we have that $n \in S$ implies $n+1 \in S$, then S must contain $\mathbb{N}$.

Note: We can think of induction as a consequence of this 9th axiom.

Proof: (that induction is true) Let $S \subseteq \mathbb{N}$ be the set of all natural numbers n such that $P(n)$ is true. Then $P(0)$ is true means $0 \in S$, while $P(n) \Rightarrow P(n+1)$ implies $n \in S \Rightarrow n+1 \in S$. Thus by Peano's 9th axiom, we infer that $\mathbb{N} \subseteq S$, therefore $S = \mathbb{N}$. $\square$

Note: An induction argument does not have to start at $n = 0$.

- If $P(k)$ is true for some $k \in \mathbb{Z}$, and if $P(n) \rightarrow P(n+1)$ is true for all integers $n \geq k$, then $P(n)$ is true for all integers $n \geq k$.
  - This variant induction can be proven from Peano's 9th axiom by considering the set S of all $n \in \mathbb{N}$ such that $P(n+k)$ is true.

Other variants of induction

Strong induction: Let $P(n)$ be a statement in terms of $n \in \mathbb{N}$. If $P(0)$ is true, and if $(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \rightarrow P(n+1)$ is true for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.

- **Proof:** For all $n \in \mathbb{N}$, let $Q(n)$ be the statement "$P(k)$ is true for all $k \in \mathbb{N}$ satisfying $k \leq n$."
  - $P(0)$ is true implies $Q(0)$ is true.
  - $(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1)$ implies $Q(n) \Rightarrow Q(n+1)$.

  Thus by induction, $Q(n)$ (and hence $P(n)$) is true for all $n \in \mathbb{N}$. $\square$

Variant of strong induction: Let $k \in \mathbb{N}$, and let $P(n)$ be a statement in terms of $n \in \mathbb{N}$. If $P(0) \wedge P(1) \wedge \cdots \wedge P(k)$ is true, and if

$$(P(n) \wedge P(n+1) \wedge \cdots \wedge P(n+k)) \rightarrow P(n+k+1)$$

is true for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.

- Special case: If $P(0)$, $P(1)$ are both true, and if $P(n)$, $P(n+1)$ are true implies $P(n+2)$ is true, then $P(n)$ is true for all $n \in \mathbb{N}$.

Example: Fibonacci numbers

Recall: (from 50.004) The Fibonacci numbers $\{F_n\}_{n\in\mathbb{N}}$ are defined by $F_1 = F_2 = 1$, and the recurrence $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 3$.

Theorem: For all $n \in \mathbb{Z}^+$,

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Proof Sketch: (by variant of strong induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be the statement given by the formula of F_n above.

- **Base cases:** By substituting $n = 1$ and $n = 2$ into the above formula, we can check that $P(1)$ and $P(2)$ are both true.
- **Induction Step:** Suppose $n \geq 3$. By induction hypothesis,

$$\begin{aligned} F_n &= \left[\tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-1} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-1}\right] + \left[\tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2}\right] \\ &= \ \dots \\ &= \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n}. \end{aligned}$$

$\square$

Note: There are other "more intuitive" proofs of this formula for Fibonacci numbers; see, e.g., course textbook.

Well-ordering principle

Theorem: (**Well-ordering priniciple**) Every **non-empty** set of natural numbers contains a smallest element.

- This sounds obvious/self-evident, but it is actually a consequence of Peano's 9th axiom. *(i.e. it is not sufficiently self-evident to be an axiom)*

Proof: Suppose on the contrary there exists a non-empty subset $A \subseteq \mathbb{N}$ with no smallest element, and define $B := \mathbb{N} \backslash A$. For each $n \in \mathbb{N}$, let $P(n)$ be the statement "$n \in B$". We want to prove using strong induction that $P(n)$ is true for all $n \in \mathbb{N}$.

- **Base case:** Note that $0 \notin A$, since otherwise 0 would be the smallest element in A. Since B is the complement of A, this means $0 \in B$, hence $P(0)$ is true.
- **Induction step:** Let $n \in \mathbb{N}$, and suppose $P(k)$ is true for all integers $0 \leq k \leq n$. This means that every natural number $\leq n$ is in B, and so every natural number $\leq n$ is NOT in A.
  - If $n + 1 \in A$, then $n + 1$ must be the smallest element in A, which contradicts the supposition that A has no smallest element.
  - Thus, $n + 1 \notin A$, so $n + 1 \in B$, i.e. $P(n + 1)$ is true. $\square$

Proof method: Fermat's method of infinite descent

Intuition: A variant of induction based on the well-ordering principle.

- Let $P(n)$ be a statement in terms of $n \in \mathbb{N}$.
- If we start by assuming that $P(n_0)$ is true for some $n_0 \in \mathbb{N}$, and then find an **infinite descending sequence** $n_1 > n_2 > n_3 > \cdots$ of natural numbers such that $P(n_1), P(n_2), P(n_3), \ldots$ are all true, then our original assumption cannot possibly be true.
  - The well-ordering principle yields: For any strictly descending sequence of natural numbers, there must be a smallest entry!
  - **Important Consequence of the well-ordering principle:** Any strictly descending sequence of natural numbers must terminate!

Theorem: (**Fermat's method of infinite descent**) Let $P(n)$ be a statement in terms of $n \in \mathbb{N}$. Suppose that whenever $P(n)$ is true for some $n \in \mathbb{N}$, there always exists some $m \in \mathbb{N}$ satisfying $m < n$, such that $P(m)$ is true. Then $P(n)$ is false for all $n \in \mathbb{N}$.

- In logic notation: If $\forall r \exists (s < r) (P(r) \rightarrow P(s))$ is true, then $P(n)$ is false for all $n \in \mathbb{N}$.

A hard example

Theorem: Let $a, b \in \mathbb{N}$ such that $k := \frac{a^2+b^2}{ab+1}$ is a natural number. Then k must be a perfect square.

Proof: Suppose on the contrary there exists $(a_1, b_1) \in \mathbb{N} \times \mathbb{N}$ such that $k_1 = \frac{a_1^2+b_1^2}{a_1 b_1+1}$ is a natural number but not a perfect square.

- **Note:** $a_1 \neq 0$ (otherwise $k = b_1^2$) and $b_1 \neq 0$ (otherwise $k = a_1^2$).
- $\frac{a_1^2+b_1^2}{a_1 b_1+1}$ is symmetric in a_1, b_1, so assume WLOG that $b_1 \leq a_1$.
- **Note:** $k_1 = \frac{a_1^2+b_1^2}{a_1 b_1+1} \Leftrightarrow a_1^2 - (k_1 b_1)a_1 + (b_1^2 - k_1) = 0$.

Idea 1: Consider the quadratic equation $x^2 - (k_1 b_1)x + (b_1^2 - k_1) = 0$.

- x is a variable. The coefficients $-k_1 b_1$ and $b_1^2 - k_1$ are constants.
- Note that $x = a_1$ is a root of this quadratic equation.

Idea 2: Let $x = a_2$ be the other root of this quadratic equation.

- This means $(x - a_1)(x - a_2) = x^2 - (k_1 b_1)x + (b_1^2 - k_1)$.
  - Expanding LHS, we get $a_1 + a_2 = k_1 b_1$ and $a_1 a_2 = (b_1^2 - k_1)$.
- Since $x = a_2$ is a root, we have $k_1(a_2 b_1 + 1) = a_2^2 + b_1^2$.

A hard example (continued)

So far we have: $b_1 \leq a_1$, $a_1 + a_2 = k_1 b_1$, $a_1 a_2 = (b_1^2 - k_1)$, $k_1(a_2 b_1 + 1) = a_2^2 + b_1^2$, $a_1 \neq 0$, $b_1 \neq 0$, $k_1 = \frac{a_1^2 + b_1^2}{a_1 b_1 + 1} \in \mathbb{N}$.

Idea 3: $a_2 b_1 + 1 \neq 0$, so $k_1(a_2 b_1 + 1) = a_2^2 + b_1^2$ implies $k_1 = \frac{a_2^2 + b_1^2}{a_2 b_1 + 1}$.

- a_2 is an integer, since $a_1 + a_2 = k_1 b_1$ implies $a_2 = k_1 b_1 - a_1$, and since k_1, b_1, a_1 are all integers.
- If $a_2 b_1 + 1 = 0$, then we are forced to have $a_2 = -1, b_1 = 1$, so $k_1 = \frac{a_1^2 + 1}{a_1 + 1} = (a_1 - 1) + \frac{2}{a_1 + 1}$, which forces $a_1 = 1$ and $k_1 = 1$.

Idea 4: $a_1 a_2 = (b_1^2 - k_1)$ implies $a_2 = \frac{b_1^2 - k_1}{a_1} \leq \frac{b_1^2 - k_1}{b_1} < \frac{b_1^2}{b_1} = b_1$.

- From $b_1 \leq a_1$ above, we thus have $\boxed{a_2 < b_1 \leq a_1}$.

Idea 5: We claim that $a_2 \in \mathbb{N}$.

- $a_2 b_1 + 1 > 0$, since $k_1 = \frac{a_2^2 + b_1^2}{a_2 b_1 + 1} \geq 0$ and $a_2^2 + b_1^2 \geq 0$.
    - $k_1 = \frac{a_2^2 + b_1^2}{a_2 b_1 + 1} \geq 0$, since $k \in \mathbb{N}$.
    - $a_2^2 + b_1^2 \geq 0$, since it is a sum of squares, and $x^2 \geq 0$ for all $x \in \mathbb{R}$.
- **Note:** a_2 is an integer and $a_2 b_1 + 1 > 0$ together imply that $a_2 b_1 + 1 \geq 1$, so $a_2 b_1 \geq 0$, and so $a_2 \geq 0$ (since $b_1 \neq 0$).
    - Thus, $a_2 \in \mathbb{N}$ as claimed.

A hard example (continued)

Define $b_2 := b_1$. We have two pairs $(a, b) = (a_1, b_1)$, $(a, b) = (a_2, b_2)$.

- Both pairs are in $\mathbb{N} \times \mathbb{N}$, and satisfy the two conditions that $\frac{a^2+b^2}{ab+1} \in \mathbb{N}$, and that $\frac{a^2+b^2}{ab+1}$ is not a perfect square.
  - We constructed (a_2, b_2) from (a_1, b_1), and showed $a_2 + b_2 < a_1 + b_1$.

Idea 6: Apply Fermat's method of infinite descent.

- We start from (a_2, b_2) and construct a new pair (a_3, b_3) in $\mathbb{N} \times \mathbb{N}$ satisfying our above two conditions, such that $a_3 + b_3 < a_2 + b_2$.
- By iterating this process, we thus get an infinite sequence

$$(a_1, b_1), (a_2, b_2), (a_3, b_3), \ldots$$

  of pairs in $\mathbb{N} \times \mathbb{N}$ satisfying our above two conditions, and a corresponding infinite descending sequence of terms in $\mathbb{N}$:

$$a_1 + b_1 > a_2 + b_2 > a_3 + b_3 > \ldots$$

- Thus, by Fermat's method of infinite descent, there is no possible $(a, b) \in \mathbb{N} \times \mathbb{N}$ that satisfies the above two conditions.

Therefore: If $a, b \in \mathbb{N}$ such that $k := \frac{a^2+b^2}{ab+1} \in \mathbb{N}$, then k must be a perfect square.

Remarks on our hard example

Technicality: When we applied Fermat's method of infinite descent to our hard perfect square example, we are technically applying this proof method to the statement $P(n)$, where for every $n \in \mathbb{N}$, $P(n)$ is the statement "There exists some pair $(a, b) \in \mathbb{N} \times \mathbb{N}$, such that $a + b = n$, $\frac{a^2+b^2}{ab+1} \in \mathbb{N}$, and $\frac{a^2+b^2}{ab+1}$ is not a perfect square." We proved that if $P(n)$ is true, corresponding to the existence of some pair (a_1, b_1) satisfying $a_1 + b_1 = n$, then we can find another pair (a_2, b_1) such that $m := a_2 + b_1$ is a **natural number strictly less than** n, and such that $P(m)$ is true.

In general, when applying Fermat's method of infinite descent, we should be clear about what our infinite descending sequence of natural numbers correspond to.

Summary

- Basic proof methods, proof by contradiction, induction
- Well-ordering principle, Fermat's method of infinite descent

Reminder:
Homework Set 1 is due this Friday (online submission, 1pm).