Tips on how to approach a mathematical proof

This note summarises Section 0.3 of the textbook [2], with the addition of some technical insights about the induction proof principle. The content of this note is not part of the ALG course. It meant to be an additional aid to refresh some mathematical concepts and provide a more precise idea about typical proofs techniques typically used in computer science theory.

Theorems and Proofs

A **proof** is a convincing logical argument that a statement is true. In mathematics, an argument must be airtight; that is, convincing in an absolute sense. A **theorem** is a mathematical statement proved true. Generally we reserve the use of that word for statements of special interest. Occasionally we prove statements that are interesting only because they assist in the proof of another, more significant statement. Such statements are called **lemmas**. Occasionally a theorem or its proof may allow us to conclude easily that other, related statements are true. These statements are called **corollaries** of the theorem.
The only way to determine the truth or falsity of a mathematical statement is with a mathematical proof. Unfortunately, finding proofs isn?t always easy. It can't be reduced to a simple set of rules or processes. During this course, you will be asked to present proofs of various statements. Don?t despair at the prospect! Even though no one has a recipe for producing proofs, some helpful general strategies are available.
First, carefully read the statement you want to prove. Do you understand all the notation? Rewrite the statement in your own words. Break it down and consider each part separately.
Sometimes the parts of a multipart statement are not immediately evident. One frequently occurring type of multipart statement has the form "P if and only if Q", often written "P iff Q", where both P and Q are mathematical statements. This notation is shorthand for a two-part statement. The first part is "P only if Q", which means: If P is true, then Q is true, written $P \implies Q$. The second is "P if Q", which means: If Q is true, then P is true, written $Q \implies P$. The first of these parts is the **forward direction** of the original statement and the second is the **reverse direction**. We write "P if and only if Q" as $P \iff Q$. To prove a statement of this form, you must prove each of the two directions. Often, one of these directions is easier to prove than the other. Another type of multipart statement states that two sets A and B are equal. The first part states that A is a subset of B (i.e., $A \subseteq B$), and the second part states that B is a subset of A (i.e., $B \subseteq A$). Thus one common way to prove that $A = B$ is to prove that every member of A also is a member of B, and that every member of B also is a member of A.
Next, when you want to prove a statement or part thereof, try to get an intuitive, "gut" feeling of why it should be true. Experimenting with examples is especially helpful. Thus if the statement says that all objects of a certain type have a particular property, pick a few objects of that type and observe that they actually do have that property. After doing so, try to find an object that fails to have the property, called a **counterexample**. If the statement actually is true, you will not be able to find a counterexample. Seeing where you run into difficulty when you attempt to find a counterexample can help you understand why the statement is true.
The following are a few tips for producing a proof.

Be patient. Finding proofs takes time. If you don?t see how to do it right away, don?t worry. Researchers sometimes work for weeks or even years to find a single proof.

Come back to it. Look over the statement you want to prove, think about it a bit, leave it, and then return a few minutes or hours later. Let the unconscious, intuitive part of your mind have a chance to work.

Be neat. When you are building your intuition for the statement you are trying to prove, use simple, clear pictures and/or text. You are trying to develop your insight into the statement, and sloppiness gets in the way of insight. Furthermore, when you are writing a solution for another person to read, neatness will help that person understand it.

Be concise. Brevity helps you express high-level ideas without getting lost in details. Good mathematical notation is useful for expressing ideas concisely. But be sure to include enough of your reasoning when writing up a proof so that the reader can easily understand what you are trying to say.

Types of proofs

Several types of arguments arise frequently in mathematical proofs. Here, we describe a few that often occur in computer science. Note that a proof may contain more than one type of argument because the proof may contain within it several different subproofs.

Proof by Construction

Many theorems state that a particular type of object exists. One way to prove such a theorem is by demonstrating how to construct the object. This technique is a **proof by construction**.
Let see an example of a proof by construction. We say that an undirected graph $G = (V, E)$ is **k-regular** if every vertex in the graph has degree k, where the degree of a vertex is the number of nodes adjacent to it.

Theorem 1 *For each even number n greater than 2, there exists a 3-regular graph with n veritices.*

Proof. Let n be an even number greater than 2. Construct the graph $G = (V, E)$ with set of vertices $V = \{0, 1, \ldots, n-1\}$, and the set of edges of G is the set

$$E = \{\{i, i+1\} \text{: for } 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \text{: } 0 \leq \text{for } i \leq n/2-1\}\,.$$

Picture the nodes of this graph written consecutively around the circumference of a circle. In that case, the edges described in red in the above equation go between adjacent pairs around the circle. The edges described in blue go between vertices on opposite sides of the circle. This mental picture clearly shows that every node in G has degree 3. □

Proof by Contradiction

In one common form of argument for proving a theorem, we assume that the theorem is false and then show that this assumption leads to an obviously false consequence, called a contradiction.
Next, let's prove by contradiction that the square root of 2 is an irrational number. A number is rational if it is a fraction $\frac{m}{n}$ where m and n are integers; in other words, a rational number is the ratio of integers m and n. For example, 2 obviously is a rational number. A number is irrational if it is not rational.

Theorem 2 *$\sqrt{2}$ is irrational.*

Proof. We assume for the purpose of later obtaining a contradiction that $\sqrt{2}$ is rational. Thus

$$\sqrt{2} = \frac{m}{n}$$

for some $m, n \in \mathbb{Z}$. Without loss of generality we can assume that m and n have greater common divisor equal to 1; otherwise we can divide both m and n by their greatest common divisor and repeat this operation until their greater common divisor is 1.
Now at least one of m and n must be an odd number. We multiply both sides of the equation by n and obtain

$$n\sqrt{2} = m\,,$$

then we square both sides and obtain

$$2n^2 = m^2\,.$$

Because m^2 is 2 times the integer n^2, we know that m^2 is even. Therefore, m must be even, as the square of an odd number is always odd. So we can write $m = 2k$ for some integer k. Then, substituting $2k$ for m in the above equation we get

$$2n^2 = 4k^2 \,.$$

Dividing both sides by 2, we obtain

$$n^2 = 2k^2 \,.$$

But, analogously as done before for m, the above equation tells us that n must be even. Thus we have established that both m and n are even, hence they can be both divided by 2. But we have earlier taken m and n such that their greatest common divisor was one 1 — a contradiction. □

Proof by Induction

Proof by induction is an advanced method used to show that all elements of an infinite set have a specified property. For example, we may use a proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, or that a program works correctly at all steps or for all inputs.

To illustrate how proof by induction works, let's take the infinite set to be the natural numbers, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, and say that the property is called P . Our goal is to prove that $P(n)$ is true for each natural number $n \in \mathbb{N}$. In other words, we want to prove that $P(0)$ is true, as well as $P(1)$, $P(2)$, $P(3)$, and so on.

Every proof by induction consists of two parts, the **basis** and the **induction step**. Each part is an individual proof on its own. The basis proves that $P(0)$ is true. The induction step proves that for each $i \geq 0$, if $P(i)$ is true, then so is $P(i + 1)$.

When we have proven both of these parts, the desired result follows —namely, that $P(n)$ is true for each $n \in \mathbb{N}$. Why? First, we know that $P(1)$ is true because the basis alone proves it. Second, we know that $P(2)$ is true because the induction step proves that if $P(1)$ is true then $P(2)$ is true, and we already know that $P(1)$ is true. Third, we know that $P(3)$ is true because the induction step proves that if $P(2)$ is true then $P(3)$ is true, and we already know that $P(2)$ is true. This process continues for all natural numbers, showing that $P(4)$ is true, $P(5)$ is true, and so on. This proof principe can be formulated as the following logical formula

$$(P(0) \wedge \forall i \geq 0.\, (P(i) \implies P(i+1))) \implies \forall n \in \mathbb{N}.\, P(n)\,.$$

The format for writing down a proof by induction is as follows.

Basis Prove that $P(0)$ is true.

Induction step For each $i \geq 0$, assume that $P(i)$ is true and use this assumption to show that $P(i + 1)$ is true.

In the induction step, the assumption that $P(i)$ is true is called the **induction hypothesis**.

Let's see an example of proof by induction.

Theorem 3 *For all $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.*

Proof. We start by formalising the predicate $P(n)$ we want to prove:

$$P(n) = \left(\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \right)$$

We proceed by induction

Basis We prove that $P(0)$ is true. One can easily verify this by substituting $n = 0$ in the above equation. Indeed we have on on side that $\sum_{k=0}^{0} k = 0$ and on the other side $\frac{0(0+1)}{2} = \frac{0}{2} = 0$.

Induction step For an arbitrary $i \geq 0$, we assume that $P(i)$ is true and using this assumption we verity that $P(i+1)$ is true. Recall that predicate $P(i+1)$ we want to prove is

$$\left(\sum_{k=0}^{i+1} k = \frac{(i+1)(i+2)}{2}\right) \qquad (P(i+1))$$

The left hand side of $P(i+1)$ can be simplified as follows

$$\begin{aligned}
\sum_{k=0}^{i+1} k &= (\sum_{k=0}^{i} k) + (i+1) \\
&= \frac{i(i+1)}{2} + (i+1) && \text{(by inductive hypothesis)} \\
&= \frac{i(i+1)}{2} + \frac{2(i+1)}{2} \\
&= \frac{i^2 + i + 2i + 2}{2}\,.
\end{aligned}$$

The right hand side $P(i+1)$ can be expanded as follows

$$\frac{(i+1)(i+2)}{2} = \frac{i^2 + 2i + i + 2}{2}\,.$$

Therefore we can see that both sides of the equation $P(i+1)$ coincide.

By the induction proof principle, we can thus state that $P(n)$ is true for all $n \in \mathbb{N}$. □

Once you understand the preceding paragraph, you can easily understand variations and generalisations of the same idea.
For example having the stronger induction hypothesis that $P(j)$ is true for every $j \leq i$ is useful. The induction proof still works because when we want to prove that $P(i+1)$ is true, we have already proved that $P(j)$ is true for every $j \leq i$. This variant of the inductive proof principle is known as **complete induction** or **strong induction**. The complete induction proof principe is formalised as follows

$$(P(0) \wedge \forall i \geq 0.\, (\forall j \leq i.\, P(j) \implies P(i+1))) \implies \forall n \in \mathbb{N}.\, P(n)\,.$$

Note that the basis doesn't necessarily need to start with 0; it may start with any value $b \in \mathbb{N}$. In that case, the induction proof shows that $P(n)$ is true for every n that is less than or equal to b. Sometimes, when using the complete induction proof principle it may even be necessary to prove extra base cases such as $P(1)$ before the argument of the induction step can be applied.
An example of the use of the complete induction proof principle is given in the following theorem

Theorem 4 *Let F_n denote the n-th Fibonacci number and $\varphi = \frac{1+\sqrt{5}}{2}$ (the golden ratio) and $\psi = \frac{1-\sqrt{5}}{2}$. Then, $F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi}$ for all $n \in \mathbb{N}$.*

Proof. Let $P(n)$ be the statement "$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi}$". We want to prove that $P(n)$ is true for all $n \in \mathbb{N}$. Before we proceed, it's convenient to recall that the Fibonacci sequence is recursively defined as $F_0 = 0$, $F_1 = 1$ and, $F_n = F_{n-1} + F_{n-2}$ for $n > 1$.
We proceed by complete induction.

Basis We prove that $P(0)$ and $P(1)$ are true. As for $P(0)$ we have that $F_0 = 0$ and $\frac{\varphi^0 - \psi^0}{\varphi - \psi} = \frac{1-1}{\varphi - \psi} = 0$.

As for $P(1)$ we have that $F_1 = 1$ and $\frac{\varphi^1 - \psi^1}{\varphi - \psi} = \frac{\varphi - \psi}{\varphi - \psi} = 1$.

Induction step For each $i \geq 1$, we assume that $P(j)$ is true for all $j \leq i$ and use this assumption to show that $P(i+1)$ is true, i.e., we have to show that $F_{i+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi}$. We have the following

$$\begin{aligned} F_{i+1} &= F_i + F_{i-1} && \text{(def. } F_n\text{)} \\ &= \frac{\varphi^i - \psi^i}{\varphi - \psi} + \frac{\varphi^{i-1} - \psi^{i-1}}{\varphi - \psi} && (P(i) \text{ and } P(i-1) \text{ are true by ind. hypothesis}) \\ &= \frac{(\varphi^i + \varphi^{i-1}) - (\psi^i + \psi^{i-1})}{\varphi - \psi} \\ &= \frac{\varphi^{i+1} - \psi^{i+1}}{\varphi - \psi} \end{aligned}$$

The last step comes from the fact that φ and ψ are the roots of the polynomial $x^2 - x - 1$, i.e., $\phi^2 - \phi - 1 = 0$ and $\psi^2 - \psi - 1 = 0$. Therefore we get that $\phi^2 = \phi + 1$. If we multiply both sides of the equation by ϕ^{i-1} we get $\phi^{i+1} = \phi^i + \phi^{i-1}$. The same argument can be used to show $\psi^{i+1} = \psi^i + \psi^{i-1}$.

Note that, in this case, we did not need to use all of prior statements $P(j)$ for $j \leq i$, but just the previous two. □

Remark 1 *Complete induction and ordinary induction are actually equivalent, in the sense that a proof by one method can be transformed into a proof by the other. Suppose there is a proof of $P(n)$ by complete induction. Let $Q(n)$ be the statement "$P(m)$ holds for all m such that $0 \leq m \leq n$". Then $Q(n)$ holds for all n if and only if $P(n)$ holds for all n, and our proof of $P(n)$ is easily transformed into a proof of $Q(n)$ by ordinary induction. If, on the other hand, $P(n)$ had been proven by ordinary induction, the proof would already effectively be one by complete induction: $P(0)$ is proved in the basis, using no assumptions, and $P(i+1)$ is proved in the inductive step, in which one may assume all earlier cases but need only use the case $P(i)$.*

Well-founded sets and Well-founded Induction

In this section we go deeper in generalising the induction proof principle. This generalisation is based on the concept of well-founded relation.
A binary relation $\sqsubset$ over a set X is called **well-founded** if every non-empty subset Y of X has a minimal element with respect to $\sqsubset$, that is, an element $m \in Y$ such that $y \not\sqsubset m$ for all $y \in Y$. In that case, the pair $(X, \sqsubset)$ is called a well-founded set.
More formally, $(X, \sqsubset)$ is well-founded set if

$$(\forall Y \subseteq X)\,[Y \neq \emptyset \implies (\exists m \in Y)\,(\forall y \in Y)\,\neg(y \sqsubset m)]\,.$$

Note that the above definition entails that the set X does not admit infinite decreasing chains of the form $x_0 \sqsupset x_1 \sqsupset x_2 \sqsupset \cdots$. Indeed, if such chain exists, then the subset $\{x_i\}_{i \in \mathbb{N}}$ would not have a minimal element, since for all $i \in \mathbb{N}$, $x_{i+1} \sqsubset x_i$. Furthermore, note that for a well-founded set $(X, \sqsubset)$, a subset $Y \subseteq X$ may have more than one minimal element.
Examples of well-founded sets are:

- the set $\mathbb{N}$ of natural numbers ordered by $<$, i.e., the "less then" relation;
- the set of tree structures ordered by the "sub-tree" relation;
- the set $\mathbb{N} \times \mathbb{N}$, ordered by $(n_1, n_2) \sqsubset (m_1, m_2)$ iff $n_1 < m_1$ and $n_2 < m_2$;
- the set $\mathbb{N} \times \mathbb{N}$ ordered by $(n_1, n_2) \prec (m_1, m_2)$ iff $n_1 < m_1$, or $(n_1 = m_1)$ and $n_2 < m_2$.

We are now ready to reformulate the induction proof principle for well-founded sets. Given a well-founded set $(X, \sqsubset)$, and $P(x)$ some property of elements of X, if we want to show that $P(x)$ holds for all elements $x \in X$, it suffices to prove that:

if $i \in X$ and $P(j)$ is true for all j such that $j \sqsubset i$, then $P(i)$ must also be true.

This generalisation of the induction proof principle is called **well-founded induction** or **Noetherian induction**. The well-founded induction principle is formalised as follows

$$[\forall i \in X. (\forall j \in X. j \sqsubset i \implies P(j)) \implies P(i)] \implies \forall x \in X. P(x) .$$

At first sight one may think that the above formulation miss to consider the basis. That is not the case. Note that for all minimal elements m of X, the implication $j \sqsubset m \implies P(j)$ is trivially true because, by construction, $j \not\sqsubset m$. Therefore, the above formulation requires one to consider as basis of the proof all the minimal elements of the set X.
One may now appreciate that well-founded induction encompasses all the induction proof principles seen before, including also the so-called **structural induction**.

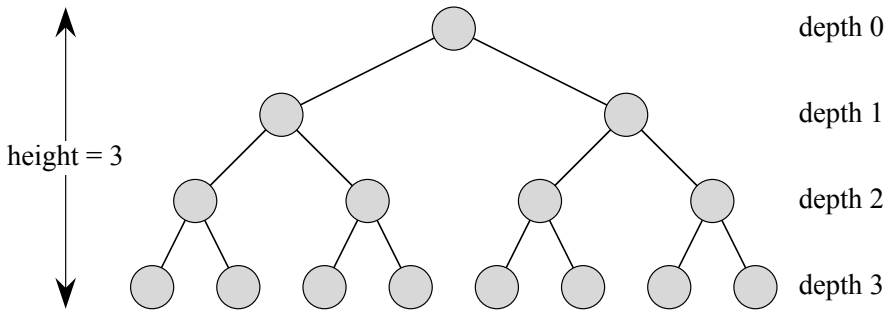

Figure 1: A complete binary tree of height 3 with 8 leaves and 7 internal nodes. Figure taken from [1]

1. Additional Examples

Binary trees. In line with [1, B.5.3], we define binary trees recursively. A binary tree T is a structure defined on a finite set of nodes that either

- contains no nodes (also called **empty tree**), or
- is composed of three *disjoint* sets of nodes: a **root** node, a binary tree called **left subtree**, a binary tree called **right subtree**.

The empty tree is sometimes denoted NIL. If the left (resp. right) subtree is nonempty, its root is called the left (resp. right) child of the root of the entire tree. If a subtree is the empty tree NIL, we say that the child is **absent** or **missing**. A **leaf** of the tree is a node with no children, all nodes with at least one child are called **internal nodes**. A binary tree is said **complete** when all internal nodes have both children (Figure 1 shows a complete binary tree).
Given a node x in the tree, the **depth** of x in T is the length of a simple path from the root node to x. A level of a tree consists of all the nodes at the same depth. The **height of a node** in a tree in the number of edges on the longest simple downward path from the node to a leaf. Likewise, the **height of a tree** is the eight of its root node.

Exercise 1 *Prove that the set of binary trees ordered by $T < T'$ iff T is a subtree of T' is well-founded.*

Theorem 5 *A complete binary tree of height h has $2^h - 1$ internal nodes.*

Proof. We proceed by induction on the height of the tree. Thus our predicate will be $P(h)$ = "A complete binary tree of height h has $2^h - 1$ internal nodes"

Basis We prove that $P(0)$ is true. If the height of the tree is 0, then the root of the tree is a leaf, meaning that there are no internal nodes. Since $P(0)$ reads as "A complete binary tree of height 0 has 0 internal nodes", we conclude that $P(0)$ is true.

Induction step For $h \geq 0$, we assume that $P(h)$ is true and using this assumption we verify that $P(h+1)$ is true. The predicate $P(h+1)$ reads as

"A complete binary tree of height $h+1$ has $2^{h+1} - 1$ internal nodes".

For a complete binary tree of height $h+1$ both left and right subtrees are binary complete trees of height h. The total number of internal nodes is given by the sum of internal nodes of the two subtrees plus 1 to count the root node. Since $P(h)$ is true, we have that the total number of internal nodes is $(2^h - 1) + (2^h - 1) + 1 = 2^{h+1} - 1$. Therefore $P(h+1)$ is true.

□

Exercise 2 *Use induction to show that a nonempty binary tree with n nodes has height at least $\lfloor \lg n \rfloor$.*

Exercise 3 ***(Kraft inequality)*** *Let us associate a "weight" $w(x) = 2^{-d}$ with each leaf x of depth d in a binary tree T, and let L be the set of leaves of T. Prove by induction that $\sum_{x \in L} w(x) \leq 1$.*

Bibliography

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 3rd Edition.* MIT Press, 2009.

[2] Michael Sipser. *Introduction to the Theory of Computation, 3rd Edition.* Cengage Learning, 2013.