CS 205: Logic, Inference, and Proof

16:198:205

One of the most fundamental questions that can be asked is the following:

Is the statement P true?

Obviously, in the most general sense, nothing can be said one way or the other without knowing the *content* of the statement P. Knowing the content may be helpful but not always enlightening - the statement "It is raining outside," is easily verified as true or false, but "Julius Caesar had three moles" is less so. But frequently, independent of the content of P, something may be determined from the **structure** of P.

Analysis of Compound Statements

For example, P may be composed of other statements that we know something about. If P is the statement that 'Statement Q is false,' if we know the truth value of Q, we can determine the truth value of P. Similarly, if P is of the form 'Statement A and Statement B', then knowing the truth value of A and B allows us to determine whether P is true.

We have a couple of standard ways of composing statements to produce new statements. The simplest is negation, $P = \neg Q$, to indicate that P is true if Q is false, and vice versa. The other two standard operations are **and** ($\wedge$) and **or**. The statement $P = A \wedge B$ is taken to be true only in the case that A and B are both truth, and false otherwise; the statement $P = A \vee B$ is taken to be true of at least one of A or B is true, and false only in the case that both are false. We can build more complex statements out of combinations and compositions of these tools, e.g.,

$$P = \neg A \vee (B \wedge C) \vee (A \wedge \neg C), \tag{1}$$

and we can determine the truth value of these compound statements by analyzing the truth value of the sub-statements. A frequently useful tool in this case is the **truth table** - essentially assessing, based on all the possible truth values of the component statements, what the truth value of the compound statement must be.

Boolean Functions and Operations

As mentioned, the three main ways of building compound statements are **negation**, **conjunction** (and), and **disjunction** (or). In many ways, these are all we need as **any composition of sub-statements can be built from these operations**. However, a number of other operations are frequently useful.

- **xor**: The statement $P = A$ xor B is taken to be true only in the case that A and B have different truth values, regardless of which one is true and which one is false. Otherwise P is false. This can equivalently be expressed as $P = (A \wedge \neg B) \vee (\neg A \wedge B)$.
- **iff / if and only if**: The statement $P = A \Leftrightarrow B$ is taken to be true only in the case that A and B have the *same* truth value, and false otherwise. This can equivalently be expressed as $P = (A \wedge B) \vee (\neg A \wedge \neg B)$.
- **implies**: The statement $P = (A \implies B)$ is taken to be *false* only in the case that A is true and B is false. This is discussed in more detail in the section on conditionals below. This can be equivalently expressed as $P = (\neg A \vee B)$.

Some Important Classes of Statements

We single out some types of statement as of particular interest - in particular, **tautologies** are statements that are true *for any* truth value of their sub-statements. The classic example of this is $A \vee \neg A$, which is true whether A is true or false. Similarly, statements are **unsatisfiable** if there is no possible truth value for their sub-statements that would render them true; the classic example of this is $A \wedge \neg A$, which is false regardless of whether A is true or false.

Conditionals

One of the most important operations when it comes to expressing ideas and the relationships between them is the conditional or implication operator. $A \implies B$ should be read as "If Hypothesis A is true, then it follows that Conclusion B must be true."

There are many subtleties to be addressed here. For one, it is entirely possible for an implication to be true even if neither of the components are true! For example, consider

$$P = (\text{it is raining} \implies \text{the grass is wet}).$$

The implication may be true, but just because P is true we do not know that it is currently raining, and we do not know whether the grass is currently wet.

This example is worth considering in some detail, as analysis of conditionals forms much of the basis of methods of inference to follow:

- If P is true and it is *not* raining, we cannot determine whether the grass is wet from the available information. It may be dry, or it may be wet due to other causes.
- If P is true and it *is* raining, it *must* be true that the grass is wet. This inference is one of the main uses of implication.
- If P is true, and the grass *is* wet, we cannot determine whether it is or is not raining from the available information. It may be raining, but the grass might be wet due to other causes.
- If P is true and the grass is *not* wet, it *must* be true that it is *not* raining. If it were raining, since P is true we could conclude that the grass were wet, which contradicts the available information. This is an early example of proof by contradiction.

The last example above also captures the idea of the **contrapositive**: in short, if $A \implies B$ is true, then $\neg B \implies \neg A$ is also true. This can be expressed in the following tautology:

$$(A \implies B) \Leftrightarrow (\neg B \implies \neg A). \tag{2}$$

The one major sticking point that people tend to have about implication has to do with the fact that the truth value of an implication statement may be independent of the content of the hypothesis and conclusion. For instance, if A is the statement 'Abe Lincoln was three feet tall' and B is the statement 'the moon is not made of cheese', the implication $A \implies B$ would still be taken as true since the hypothesis is false. The *only* way an implication statement is taken as false is if the hypothesis is true and the conclusion is false.

Bi-conditionals

Another way to interpret the statement A **iff** B is to unpack it it as quite literally

$$A \text{ if and only if } B.$$

In this case, if B, then A is true, and if $\neg B$, then A is not true. This gives the natural expansion in the following tautology,

$$(A \Leftrightarrow B) \Leftrightarrow (B \implies A) \wedge (\neg B \implies \neg A), \tag{3}$$

or, by use of the contrapositive above,

$$(A \Leftrightarrow B) \Leftrightarrow (B \implies A) \wedge (A \implies B). \tag{4}$$

Inference

Inference is the art and methods of taking a base of knowledge or set of initial premises that are taken to be true, and concluding from them other statements that must be true. In this case, we are addressing the question of 'Is Statement P true?' by first looking at what else we already know, and determining from that whether the truth value of P can be determined. This frequently has the structure of solving mysteries, taking clues to infer the identity of the culprit, but can easily be abstracted to the point of obscuring this.

The main inferential tool is a rule known as **modus ponens**: if the statement $(P \implies Q)$ is true, and additionally the statement P is true, it may be inferred that Q is true. If it is true that it being raining implies the grass is wet, and it is raining, then we may infer that the grass is wet. This highlights the point made earlier that an implication statement may be true by itself, without saying anything about the truth of its hypothesis or conclusion. But if we additionally know that the hypothesis is true, the conclusion *must* be true. This can be summarized in the following tautology,

$$[(P \implies Q) \wedge P] \implies Q. \tag{5}$$

What makes this, and the other rules of inference, so powerful is that it may be applied independent of the content of the statements. No matter what P and Q are actually saying, if it is known that P is true, and that $(P \implies Q)$ is true, i.e., whenever your knowledge may be expressed in this form, we may logically conclude that Q is true.

Based on the previous discussion of conditionals, we may construct an additional rule of inference based on the **contrapositive**; that is, if we know that $P \implies Q$ and that $\neg Q$, we may infer that $\neg P$:

$$[(P \implies Q) \wedge \neg Q] \implies \neg P. \tag{6}$$

In each of these cases, by starting with an initial knowledge base of statements known to be true ($[(P \implies Q, P]$ or $[P \implies Q, \neg Q]$ respectively), we can construct and augment our knowledge base with additional statements we know to be true (i.e., Q or $\neg P$).

One important aspect of inference is the following: it should not be viewed as discovery of knowledge or truth, so much as *unpacking* knowledge that was already contained in the premises. In the first example above, under the condition that $P \implies Q$ and also P, it was already true that Q, but using modus ponens as rule of inference we were able to unpack this, and state Q explicitly in our knowledge base as true. Rules of inference, given the context-free nature of logical propositions, can have a very mechanical flavor at times, and in fact serve as the basis of many automated logic or AI systems for taking data or models and making decisions based on that information.

There are a variety of rules of inference available - each generally of the form, given a collection of **Premises**, **Conclusion** must be true. Some frequently useful examples are the following:

- **If $P \wedge Q$, then P**: In order for the statement $P \wedge Q$ to be true, both sub-statements must be true, therefore we can conclude that P (and, separately, Q) must be true.

$$(P \wedge Q) \implies P \tag{7}$$

- **If $P \vee Q$ and $\neg Q$, then P**: If at least one of P and Q are true, but Q is false, we must conclude that P is true.

$$[(P \vee Q) \wedge \neg Q] \implies P \tag{8}$$

- **If $P \Leftrightarrow Q$ and Q, then P**: If P and Q have the same truth value, and Q is true, we may conclude that P is true. This (and the immediate case when instead $\neg Q$) can be seen as a consequence of modus ponens.

$$[(P \leftrightarrow Q) \wedge Q] \implies P \tag{9}$$

- **If $P \vee Q$ and $\neg P \vee R$, then $Q \vee R$**: This is known as the **resolution inference rule** and can be seen as a generalization of the previous rule involving disjunction above. It is perhaps best seen by cases: in the case that P, we may conclude that R is true, in the case that $\neg P$, we may conclude that Q is true; in any case, we may conclude that the statement $Q \vee R$ is true.

$$[(P \vee Q) \wedge (\neg P \vee R)] \implies (Q \vee R). \tag{10}$$

There are many such rules, and more complex rules could be constructed by composing these: for instance, **if $P \implies Q$ and $Q \implies R$ and P, then R**. This could be treated as a rule of inference in its own right (since any time premises of this structure are known, we may draw the indicated conclusion), but it is really just two applications of modus ponens chained together.

In general, rules of inference may be derived by addressing the question: given that a set of premises is true, what **must** be true either to cause them, or as a result of them?

First-Order Logic

First-Order logic can be viewed as an extension of the propositional logic established thus far, which allows us to not only analyzing statements, but statements *about* things. This represents another class of statements that we might be considering in the initial question 'Is Statement P true?', and the additional structure first-order logic provides will give us more tools with which to approach the question.

In particular, in first-order logic we can make logical statements about members of a class, for instance

All men must die.

or

Not all rectangles are squares.

The main two features that first-order logic grants us are **universal** quantification, and **existential** quantification. For any object x in the *domain of interest*, let $P(x)$ be a statement about x. We may write 'P(x) is true for all x in the domain of interest' as

$$\forall x : P(x) \tag{11}$$

and similarly 'there exists some x in the domain of interest such that $P(x)$ is true' as

$$\exists x : P(x). \tag{12}$$

Both of these can be viewed as logical statements in their own right. Analyzing the two examples above, if the domain of interest is **men** and the predicate $D(x)$ states that x must die, 'all men must die' may be written as

$$\forall x : D(x). \tag{13}$$

Notice though, much depends on the domain of interest. If instead of men, we were interested in the set of people, we might consider an additional predicate $M(x)$ stating that x is a man. In that case, the statement might be written as

$$\forall x : (M(x) \implies D(x)). \tag{14}$$

Similarly, if the domain of interest where rectangles, and $S(x)$ is the predicate that 'x is a square', we might express the sentence 'not all rectangles are squares' as

$$\neg [\forall x : S(x)]. \tag{15}$$

An equivalent way of expressing this following: if not all rectangles are squares, there must exist rectangles that are not square. Hence we could express the same thought as

$$\exists x : \neg S(x). \tag{16}$$

This expresses a general relationship between universal and existential quantifiers - they are essentially duals under negation. If something is not true for everything, there exist things for which it is not true; if it is not true that there exists something with a given property, then that property does not hold for all things:

$$\begin{aligned} \neg [\forall x : P(x)] &\Leftrightarrow \exists x : \neg P(x) \\ \neg [\exists x : P(x)] &\Leftrightarrow \forall x : \neg P(x). \end{aligned} \tag{17}$$

With this convention, we can embed this first-order framework in our previous discussion of logical operations and inference, and additionally utilize the same results here.

Some other conventions worth noting: a given logical statement may involve multiple variables quantified in several ways. The classic example of this takes as the domain of interest people, and considers the predicate $S(x, y)$ to be the statement 'x is a child of y'. In this case, we might say that everyone has a parent (/is the child of someone),

$$\forall x : \exists y : S(x, y). \tag{18}$$

An important thing to note about the above - because x is quantified first, y potentially depends on x. Reversing the ordering yields a very different notion - that there exists someone who is a parent of everyone

$$\exists y : \forall x : S(x, y). \tag{19}$$

This is patently false as if there were such a person y, that person would not be their own parent, i.e., $\neg S(y, y)$. Considering the *negation* of this, we have that

$$\forall y : \exists x : \neg S(x, y), \tag{20}$$

i.e., for every person, there exists someone who is not their child. This is clearly *true*, taking $x = y$ as an example to prove existence.

Note, this is a good example of something to be discussed in the next section - proof by example.

First-Order Inference

First-order logic grants us a few more tools of inference to handle our expanded abilities. Namely, the following:

- If it is true that $\forall x : A(x)$, then for anything in the domain of interest, we may take A as true. If it is true that all cats are soft, then taking any cat, we may infer that cat to be soft.
- If it is true that $\exists x : A(x)$, then we can instantiate an instance of x where A is true. If there exist cats who drink coffee, then we can suppose coffeeCat to be a cat who drinks coffee - and we can be sure that this variable refers to an object that exists.
- If a is an object in the domain of interest where A is true, then $\exists x : A(x)$.
- If $\forall x : A(x)$, then $\exists x : A(x)$.

The benefit of these concepts is that they allow is to move from talking generally over the domain of interest to talking specifically about single objects. If we take as true that all lions are fierce creatures, and that some lions drink coffee - we may infer the existence of at least one creature, and name it for convenience coffeeLion, who drinks coffee. Since coffeeLion is a lion, we have that coffeeLion is a fierce creature. Hence, we know (by example!) that there exist fierce creatures which drink coffee.

Proof Techniques

At this point, we return to the question of

Is Statement P true?

We have established a couple of techniques we might use to try to verify whether P is true.

Logical Equivalence: If P is a compound proposition, composed of various sub-statements combined with logical operators, we might try to simplify or expand P, and find a simpler logical statement it is equivalent to. For instance, if we have

$$P = (A \vee \neg B) \wedge (\neg A \vee B) \wedge A, \tag{21}$$

it can be argued that $(\neg A \vee B) \wedge A$ is equivalent to $(\neg A \wedge A) \vee (B \wedge A)$ which is logically equivalent to $(\textbf{False}) \vee (B \wedge A)$ which is logically equivalent to $(B \wedge A)$ (*why?*). Hence we have that

$$P = (A \vee \neg B) \wedge B \wedge A. \tag{22}$$

Similarly, though, it can be argued that $(A \vee \neg B) \wedge B$ is equivalent to $(A \wedge B) \vee (\neg B \wedge B)$, which is equivalent to $(A \wedge B) \vee (\textbf{False})$, which is equivalent to $(A \wedge B)$. Hence, we have that

$$P = A \wedge B \wedge A, \tag{23}$$

or ultimately

$$P = A \wedge B. \tag{24}$$

Hence, we can analyze this much simpler logical statement instead of the original.

This can be very useful when attempting to prove statements true of the form $P = (A \implies B)$, which frequently arises in proofs and inference rules. We may equivalently express P as $\neg A \vee B$, and attempt to show or analyze this disjunction to verify it as true or false.

Direct Proof: If we want to verify P as true or false, we might consider what else we know that is connected to P. If P is a statement about lions or cats, for instance, we might consider what prior knowledge we have about animals. If P is a statement about numbers, we might consider what prior knowledge we have about mathematics and arithmetic. If we can establish that we have some prior knowledge base Q, and we can show that the statement $Q \implies P$ is true, we may conclude (via modus ponens) that P is true.

Consider the claim: if a natural number is even, then its square is even. If a number is even, we know that it is equal to $2 * k$ for some natural number k - this is our prior knowledge and definitions at work. We know further then that the square must be equal to $(2 * k)^2$ for the same k, or $2 * (2k^2)$. Since $2k^2$ is an integer, this implies that the square is even. Hence, starting from our knowledge base (that the number is even, and prior knowledge about arithmetic), we have shown by a direct sequence of implications that the conclusion must be true.

Proof by Contrapositive: This is a specific instance of the previous notions, that frequently arises in practice. In particular, when attempting to prove that $P \implies Q$, it can frequently be useful (or at least more semantically natural) to prove that $\neg Q \implies \neg P$. Since the two are equivalent, logically, verifying one as true verifies the other.

Consider by way of example, proving that 'if n^2 is odd, then n is odd' is much less straightforward than proving 'if n is not odd (even), then n^2 is not odd (even)' - this is the result laid out in the previous section above on direct proof.

Proof by Contradiction: In some instances, it may not be clear how to prove a claim in one direction or the other (directly or by contraposition). It is frequently useful to assume the *opposite* of what you want to prove, and try to figure out *why* it can't be true. Consider a universe counter to what you believe to be true - what breaks?

By way of example, consider a situation in which n is odd, and n^2 is even (i.e., the negation of n odd implies n^2 even). In this case, $n = 2a + 1$ for some integer a, and $n^2 = 2b$ for some integer b. But then $n^2 = 4a^2 + 4a + 1$, or

$$2b = 2(2a^2 + 2a) + 1, \tag{25}$$

in which case we have a value that must be even (on the left) and odd (on the right) at the same time. This is a contradiction, and cannot be true. Hence, something about the initial premise must be false: i.e., it cannot be true that n is odd and n^2 is even. This is logically equivalent to n odd implies n^2 odd being true.

Proof by Example: Suppose want to prove that a statement of the following form is true:

$$\exists x : P(x) \tag{26}$$

In this case, it suffices to demonstrate an example of some object in the domain of interest where P is true. This can frequently be combined with proof by contradiction as above. As an example, consider the statement 'for all positive integers n, $n^2 - n + 41$ is prime'. This seems to be true for the first couple of examples. Taking $n = 1, 2, 3$, we have $41, 43, 47$, etc. But is this true for all such n?

Consider the negation:

$$\exists n > 0 : n^2 - n + 41 \text{ is not prime.} \tag{27}$$

In this case, note that for $n = 41$ we have that $n^2 - n + 41 = 41^2 - 41 + 41 = 41^2$. The value 41^2 is very clearly not prime, hence the above claim is in fact true. We have therefore verified, by example, that the following claim is true:

$$\neg \left[\forall n \geq 1 : n^2 - n + 41 \text{ is prime.}\right] \tag{28}$$

Inductive Proofs

In this section, we are particularly focused on proving statements of the form, over the domain of non-negative integers ($n = 0, 1, 2, ...$):

$$\forall n : P(n). \tag{29}$$

Sometimes, the methods above suffice, for instance proving things like

$$\forall n : n \text{ even } \implies n^2 \text{ even}. \tag{30}$$

In cases where the claim can be considered effectively in isolation, these proof methods may suffice. However, in a number of circumstances, the *claim* for a given value of n may depend on the claim being true for other values as well.

A classic example of this is the following: the Fibonacci numbers are defined to be a sequence of numbers $1, 1, 2, 3, 5, 8, \ldots$, where every number is the sum of the two previous numbers (starting with 1 and 1). We may define this **recursively**, taking $f(0) = 1$, $f(1) = 1$, and $f(n + 2) = f(n) + f(n + 1)$ for all $n \geq 0$.

It is fairly immediate that the Fibonacci numbers are positive, and grow quickly. But how quickly? Consider the following claim:

$$\forall n \geq 0 : \frac{1}{2}1.5^n \leq f(n) \leq 2^n, \tag{31}$$

where the claim for any n is defined by the statement $P(n) = \frac{1}{2}1.5^n \leq f(n) \leq 2^n$.

How could this be verified? A direct proof would be difficult - showing that $P(n)$ for a given n would require knowing a lot about $f(n)$ itself. But in fact, we know a lot about $f(n)$ in terms of the previous two values, $f(n-1)$ and $f(n-2)$.

Assume that $P(n-1)$ and $P(n-2)$ are true. How can this information be utilized? Combining these two claims, for $n \geq 2$, we have

$$\frac{1}{2}(1.5)^{n-1} + \frac{1}{2}(1.5)^{n-2} \leq f(n-1) + f(n-2) \leq 2^{n-1} + 2^{n-2}, \tag{32}$$

or

$$\frac{1}{2}(1.5)^{n-2}(1.5 + 1) \leq f(n-1) + f(n-2) \leq 2^{n-2}(2 + 1). \tag{33}$$

Hence, noting that $f(n) = f(n-1) + f(n-2)$ (a given! by definition!), we have that

$$P(n-1) \wedge P(n-2) \implies \left[\frac{1}{2}(1.5)^{n-2}2.5 \leq f(n) \leq 2^{n-2}3\right]. \tag{34}$$

This is very close to the desire claim, but not quite there. However, noting that

$$2^{n-2}3 \leq 2^{n-2}4 = 2^{n-2+2} = 2^n, \tag{35}$$

and

$$\frac{1}{2}(1.5)^{n-2}2.5 \geq \frac{1}{2}(1.5)^{n-2}2.25 = \frac{1}{2}(1.5)^{n-2}1.5^2 = \frac{1}{2}(1.5)^n, \tag{36}$$

we have that

$$\left[\frac{1}{2}(1.5)^{n-2}2.5 \leq f(n) \leq 2^{n-2}3\right] \implies \left[\frac{1}{2}(1.5)^n \leq f(n) \leq 2^n\right], \tag{37}$$

which is in fact the claim for n.

Hence we've shown that for any $n \geq 2$,

$$P(n-1) \wedge P(n-2) \implies P(n). \tag{38}$$

We can build from this an infinite chain of reasoning, observing that $P(1) \wedge P(0) \implies P(2)$, and then $P(2) \wedge P(1) \implies P(3)$, and then $P(3) \wedge P(2) \implies P(4)$, etc. Hence if we can establish $P(1)$ and $P(0)$ as true, we can establish $P(2)$ as true, and following the chain, every $P(n)$ after that as true.

This infinite chain of implication is interesting, but it is not *useful* until we prove the initial premise, that $P(1)$ is true and $P(0)$ is true. These are the fuse that set off the entire chain of inference, allowing us to infer every $P(n)$ along the way. As noted previously, an implication may be true but until the hypothesis is verified nothing can be inferred.

However, $P(0)$ is simply the claim that $0.5 \leq f(0) \leq 1$ which is true, and $P(1)$ is simply the claim that $0.75 \leq f(1) \leq 2$, which is true. These initial or base cases are often verified fairly immediately, by direct evaluation.

This kicks off the infinite chain of implication. For any n, we may build a chain of implication to it starting from $P(0)$ and $P(1)$, and then chase modus ponens down the line until $P(n)$ is verified. Hence, we have verified that $P(n)$ is true for all $n \geq 0$.

We can summarize this particular case with the following rule of inference:

$$[[P(0) \wedge P(1)] \wedge [\forall n \geq 2 : P(n-1) \wedge P(n-2) \implies P(n)]] \implies [\forall n \geq 0 : P(n)] \tag{39}$$

This is the basic outline of proof by induction: by verifying some number of base cases, and that at every step, some degree of knowledge of prior cases implies that the next case must be true, this ignites the infinite inductive chain allowing us to conclude the claim for all n:

Proofs by Induction: First verify some number of base cases, $P(0), P(1), \ldots, P(k-1)$. Then prove the *inductive step*, that assuming the prior cases $P(n-k), P(n-k+1), P(n-k+2), \ldots, P(n-1)$, the case for $P(n)$ must be true. In this case, we may conclude

$$\forall n \geq 0 : P(n). \tag{40}$$

This is summarized with the following tautology: for some $k \geq 0$ (depending on the structure of the claim),

$$[[P(0) \wedge \ldots \wedge P(k-1)] \wedge [\forall n \geq k : P(n-k) \wedge \ldots \wedge P(n-1) \implies P(n)]] \implies [\forall n \geq 0 : P(n)] \tag{41}$$

This proof technique is frequently useful for verifying infinite classes of claims, particularly when a claim for n is structurally similar in some way to prior claims.

As another example of this, consider the following claim: for any positive number α,

$$\forall n \geq 0 : \ 1 + \alpha + \alpha^2 + \ldots + \alpha^n = \frac{\alpha^{n+1} - 1}{\alpha - 1}. \tag{42}$$

In this case, because the claim for n is structurally similar to the claim for $n-1$, this is highly suggestive of a proof by induction:

$$\begin{aligned} P(n) &: \left[1 + \alpha + \ldots + \alpha^{n-1}\right] + \alpha^n = \frac{\alpha^{n+1} - 1}{\alpha - 1} \\ P(n-1) &: \left[1 + \alpha + \ldots + \alpha^{n-1}\right] = \frac{\alpha^n - 1}{\alpha - 1}. \end{aligned} \tag{43}$$

In this case, we have that

$$\begin{aligned} P(n-1) &\implies \left[1 + \alpha + \ldots + \alpha^{n-1}\right] + \alpha^n = \frac{\alpha^n - 1}{\alpha - 1} + \alpha^n \\ &\implies \left[1 + \alpha + \ldots + \alpha^{n-1}\right] + \alpha^n = \frac{\alpha^n - 1 + (\alpha - 1)\alpha^n}{\alpha - 1} \\ &\implies \left[1 + \alpha + \ldots + \alpha^{n-1}\right] + \alpha^n = \frac{\alpha^{n+1} - 1}{\alpha - 1} \\ &\implies P(n). \end{aligned} \tag{44}$$

Since we have established then that for any $n \geq 1$, $P(n-1) \implies P(n)$, establishing the base case of $P(0)$ would complete the proof by induction, and verify the claim for all n.

Strong Induction and Proof by Minimal Counter Example

In some instances, it may not be enough to establish the infinite chain of induction simply looking at one or two (or some small number) of prior cases. Verifying the claim $P(n)$ may depend on assuming a prior $P(m)$ for some $0 \leq m < n$, where m is unknown. In this case, we may make use of the **principle of strong induction**, in which, after a base case is verified, the inductive step depends on assuming P for *all prior* m. This may be summarized via the following tautology:

$$[P(0) \wedge [\forall n \geq 1 : P(0) \wedge P(1) \wedge \ldots \wedge P(n-1) \implies P(n)]] \implies [\forall n \geq 0 : P(n)]\,. \tag{45}$$

The classic use of this principle is to show that for any natural number $n(\geq 2)$, n can be factored as the product of primes. The proof proceeds by arguing that $P(n)$ is clearly true for n prime, and for n not prime, i.e., $n = a * b$, if we assume $P(m)$ for all $2 \leq m < n$ then $P(a)$ and $P(b)$ must be true. But if $n = a * b$, then we can use the prime factorization of a and the prime factorization of b to build a prime factorization of n.

The importance of strong induction here is that in general, for arbitrary n, we cannot be certain where prior factors of n must fall. Hence, to be certain that the appropriate prior cases are assumed for the inductive step, we simply assume *all* the prior cases are true for each n.

A related concept to this is the **proof by minimal counter example**: In short, assume that it is not true that ever $n \geq 2$ can be factored into primes. Let n' be *the smallest example of such an n that cannot be factored into primes.* If n' is prime, then we have an immediate contradiction. Hence, assume that n' is not prime, i.e., $n' = a * b$. Since $a, b < n'$, since n' is the *smallest* counter-example to P by assumption, $P(a)$ and $P(b)$ must be true. However, we see again that the prime factorization of a and b can then be used to build a prime factorization of n', contradicting n' as a counter example to P. As such, P has *no* minimal counter example. Hence, $P(n)$ must be true for all $n \geq 2$.

The assumption of minimality, for a counter example, is very powerful when the claim for a given n can be related to the claim for some prior values.

Limits of Logic

It is worth pointing out, as a closing note, some of the limitations of the models and frameworks built here. One thing that all the previous discussion fails to deal with is *time*: in particular, statements might be true at one time, and false at future times. Imagine, for instance, a ship captain making the statement 'We are currently in sight of land'. Treating all statements as having immutable truth values fails to capture this possibility.

Another thing that these models fail to capture is the fact that statements may not be true or false in any typical sense, or expecting them to be true or false may not be useful. Describing the sea as blue may prompt some people to declare the statement false, others true. Other statements may be true or false, but essentially unknown or unknowable - consider flipping a coin and hiding the result. You know the coin either came up heads or tails, but there is no way to assess which based on the available information.

Dealing with these kinds of situations requires more refined tools than those developed here, but the material here serves as the foundation of a lot of mathematics and computer science.

Questions

1) Verify the following identities (distribution laws) via truth table or by giving a short justification:

$$\begin{aligned} A \wedge (B \vee C) &\Leftrightarrow (A \wedge B) \vee (A \wedge C) \\ A \vee (B \wedge C) &\Leftrightarrow (A \vee B) \wedge (A \vee C). \end{aligned} \tag{46}$$

2) Verify the following identities (de Morgan's Laws) via truth table or by giving a short justification:

$$\begin{aligned} \neg(A \vee B) &\Leftrightarrow (\neg A) \wedge (\neg B) \\ \neg(A \wedge B) &\Leftrightarrow (\neg A) \vee (\neg B). \end{aligned} \tag{47}$$

3) Someone hands you a small stack of cards. Each card has a letter on one side, and a number on the other. They tell you, 'Each card with a vowel on one side has an even number on the other.' Dealing out the first four cards, you see an A, a 7, a 10, and a B.

   - What does the person's rule tell you about the hidden side of each card?
   - If you want to check or verify the person's rule by flipping over a card or cards, which cards should you flip, and what should you conclude from the reverse side?

4) Find a satisfying assignment for the following, or show that one does not exist.

$$(A \vee B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C). \tag{48}$$

5) Verify the following as true or provide a counter example:

$$(A \text{ xor } B) \Leftrightarrow \neg(A \Leftrightarrow B). \tag{49}$$

6) Answer the following, justifying your answer logically.

   - All men must die. I am not a man. Must I die?
   - All men must die. I must die. Am I a man?
   - All men must die. I must not die. Must I die?
   - All men must die. Must Socrates die?
   - All men must die. John Tucker must die. Is John Tucker Socrates?

10) Argue that modus ponens is actually just a special case of the resolution inference rule.

11) It can be argued that the resolution inference rule is in fact *complete*, in the sense that it is the only rule needed to infer everything that can be inferred. Why might other inference rules (not just modus ponens) be useful to know?

12) Suppose that the following premises are granted as an initial knowledge base:

$$B \vee C, \neg B \vee \neg C, A \vee B, A \vee C, \neg A \vee \neg B \vee \neg C \tag{50}$$

    We might attempt to infer that A is true, via contradiction, in the following way. Suppose an additional premise that $\neg A$ is true, and derive a contradiction using a general resolution inference rule:

$$\text{If } P_1 \vee P_2 \vee \ldots \vee P_n \text{ and } \neg P_i, \text{ then } P_1 \vee \ldots \vee P_{i-1} \vee P_{i+1} \vee \ldots P_n.$$

Show your steps, what you conclude along the way, and identify the final contradiction. Conclude, from this contradiction, that $\neg A$ must be false.

13) Consider the following statement, where the domain of interest is the integers:

$$\forall n : n \text{ not divisible by } 3 \implies n^2 \text{ gives a remainder of 1 when divided by 3..} \tag{51}$$

- What would the initial step / formulation of a direct proof look like?
- What would the initial step / formulation of a proof by contrapositive look like?
- What would the initial step / formulation of a proof by contradiction look like?
- What would the inductive step of a proof by induction look like?
- Which of these approaches seems most promising? Why?

An alternative approach might be to consider proof by cases. In particular, for any n, n gives a remainder of 0, 1, or 2 when divided by 3. By considering these three cases separately, prove the claim for a given n.

14) Prove that over the domain of non-negative integers,

$$\forall n : n^2 + n \text{ is even.} \tag{52}$$

Can you construct a proof by minimal counter example? What is the best approach to take here?

15) Consider again the Fibonacci numbers, defined by the sequence $f(0) = 1$, $f(1) = 1$, and $f(n+2) = f(n)+f(n+1)$ for $n \geq 0$. In the sections above, we proved that $f(n) \leq 2^n$ for all n. What is the smallest positive number α you can find such that the proof can be adapted to show

$$\forall n \geq 0 : f(n) \leq \alpha^n? \tag{53}$$

16) Show that for $n \geq 3$ over the set of positive integers, we have

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \leq 2\ln(n). \tag{54}$$

You may find the inequality $x \leq -2\ln(1-x)$ for $0 < x < 1$ useful here.

17) Suppose that cats are sold in sets of 3 or sets of 5. Show that for any $n \geq 8$, someone can buy exactly n cats.