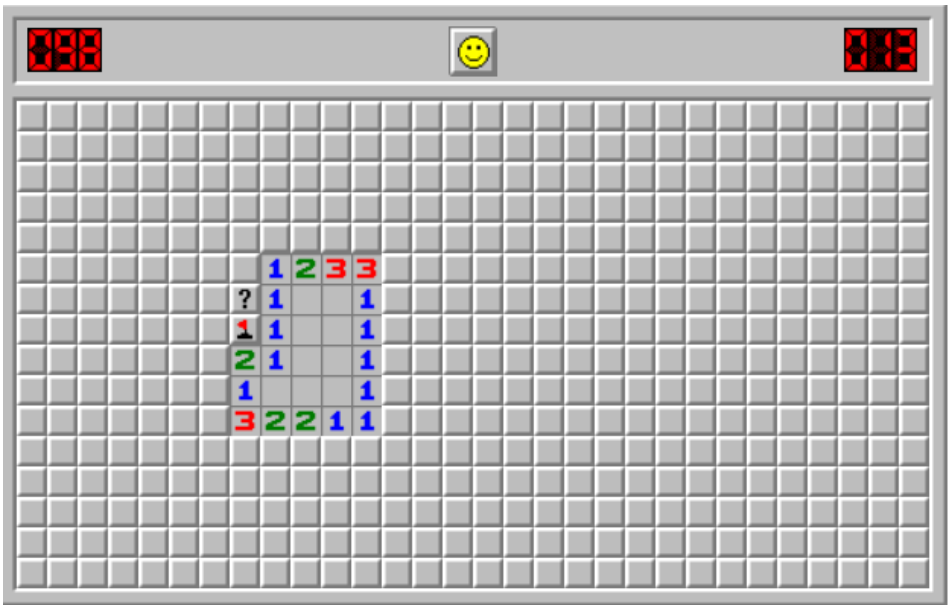
Proofs with Propositional Logic

CS236 - Discrete Structures
Instructor: Brett Decker
Fall 2021

Proof Intuition

The word *proof* is often intimidating, but logic proofs are actually quite common in daily living. To help you build some intuition on how logic proofs work. Let's consider the game Minesweeper. It's actually a logic game. In Minesweeper, you try to flag all of the bombs. To determine where the bombs are you use the numbers on discovered square that give the number of bombs that square is adjacent to. See the example below:



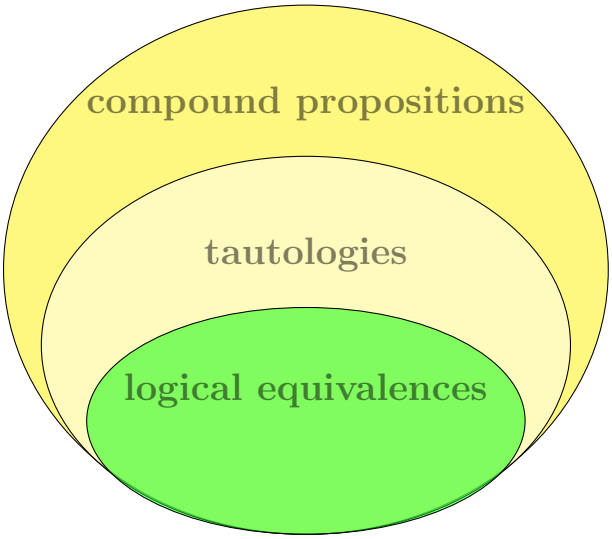
There are two ways to determine which hidden-square to flag:

1. Proof by deduction: by looking at the discovered squares we can deduce, or conclude certain squares must be a bomb, and thus flag them. In the example above, that is how we flagged the square next to the '1' – all other squares around the '1' have been discovered, so the remaining one must be a bomb, by deduction.

2. Proof by contradiction: we can assume a square is a bomb and mark it with the question mark. We use all other discovered squares to see if this marked square will cause a contradiction – a situation that is impossible based on the square already discovered. In the example above the marked square creates a contradiction for the two '1's that are adjacent to the already flagged bomb. Thus the marked square cannot be a bomb and we can safely press on the square to discover its value. For more information on Minesweeper, see here: `http://www.minesweeper.info/wiki/Windows_Minesweeper`.

Proposition Hierarchy

Recall that tautologies are special compound propositions and logical equivalences are a special type of tautology.



Logic Proofs: Rules of Inference

We'd like to use propositional logic to reason about other propositions, also called statements, and conclude their truth values. Specifically, we'd like to prove (reason mathematically) that given the truth of certain propositions, we can conclude without error that other propositions of interest are always true.

Rules of Inference: Definitions, Section 1.6*

We use logical proofs to prove that an argument is valid, or sound. An argument ends with some *conclusion* – the proposition we claim to always be true, when all preceding statements, called *premises*, are true. The argument is said to be valid if and only if the conclusion cannot be false when the premises are true. We use *rules of inference*, or simple argument forms, to help build larger proofs.

Rules of Inference: Modus Ponens

Rules of inference often take the following form: the starting premises (often called the *knowledge base*) are each on a separate line. There is an implicit $\wedge$ after each line, i.e. all the premises are joined together with conjunction. After the premises is a vertical line, after which the next line contains the therefore symbol, $\therefore$, and the concluding proposition(s) or conclusion(s).

Here is "modus ponens":

(premise 1)	p
(premise 2)	$p \to q$
(conclusion)	$\therefore q$

"Modus ponens" in essence states: if a proposition p is true, and the compound proposition $p \to q$ is true, then the proposition q *must* be true. Verify this with the truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

The only row with both p and $p \to q$ true also has q as true.

Rules of Inference: Modus Tollens

Here is "modus tollens":

(premise 1)	$\neg q$
(premise 2)	$p \to q$
(conclusion)	$\therefore \neg p$

"Modus Tollens" in essence states: if a proposition q is false, and the compound proposition $p \to q$ is true, then the proposition p *must* be false. Verify this with the truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

The only row with $\neg q$ true (thus q as false) and $p \to q$ true also has $\neg p$ as true (p is false).

Rules of Inference: Simplification

Here is simplification (to convince yourself, build the truth table):

(premise 1) $p \wedge q$

(conclusion 1) $\therefore p$
(conclusion 2) $\therefore q$

Rules of Inference: Resolution

Here is resolution (to convince yourself, build the truth table):

(premise 1) $p \vee q$
(premise 2) $\neg p \vee r$

(conclusion) $\therefore q \vee r$

Here is disjunctive syllogism:

(premise 1) $p \vee q$
(premise 2) $\neg p$

(conclusion) $\therefore q$

Consider the following:

(premise 1) $p \vee q$
(premise 2) $\neg p \vee F$

(conclusion) $\therefore q \vee F$

Thus, disjunctive syllogism is just a special case of resolution. Another form of resolution is:

(premise 1) $p \vee F$
(premise 2) $\neg p \vee F$

(conclusion) $\therefore F$

Thus, it follows that:

(premise 1) p
(premise 2) $\neg p$

(conclusion) $\therefore F$

The above is often the last step in Proofs by Contradiction with Resolution (see below).

Logic Proofs: Deduction

We can use rules of inference to help us *deduce*, or logically arrive at, conclusions. When we use deduction as the reasoning for a proof, we call this method *proof by deduction* (the book* also calls these *direct proofs*).

Proof by Deduction Example:

The following is an example of a proof by deduction. We start with labeling all premises in our knowledge base. Then we add the vertical line. For each new conclusion under the line, we give a rule of inference used to deduce the conclusion from the above premises (note that we can use prior conclusions to deduce new conclusions):

Proof. Given the premises, deduce t (i.e, prove that t is always true):

1. $\neg p \wedge q$
2. $r \rightarrow p$
3. $\neg r \rightarrow s$
4. $s \rightarrow t$

---

5. $\neg p$ simplification on 1
6. $\neg r$ modus tollens on 5 and 2
7. s modus ponens on 6 and 3
8. t modus ponens on 7 and 4

$\therefore t$ □

Logic Proofs: Contradiction

Section 1.7.7* gives an excellent description and definition of proof by contradiction. To execute a proof by contradiction, we simply negation the desired conclusion and then continue concluding new premises until we conclude the premise false. At this point we have our contradiction and have proved the desired conclusion (this is valid because of the logical equivalence: $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow F$).

Logic Proofs: Resolution

Resolution is a proof technique used to streamline proofs. We take all starting premises and convert them into Conjunctive Normal Form (CNF). CNF is defined by terms being *grouped* by disjunction and *separated* by conjunction. Also, negation must be atomic—bound to a propositional variable. The conditional and bi-conditional operators are not allowed. For example, $p \vee q \vee r$, $p \wedge \neg q$, and $(p \vee q) \wedge r$ are in CNF, but $p \rightarrow q$, $\neg(p \vee q)$, and $(p \wedge q) \vee r$ are NOT in CNF. Once the premises are in CNF, we simple apply resolution (and/or disjunctive syllogism—which is just a special type of resolution) until we conclude the conclusion. The benefit of this technique is that we avoid having to determine which law or rule of inference to use at each step of the proof; instead we always use resolution or disjunctive syllogism.

Automating Proofs

One problem with proof by deduction is that it isn't obvious what new premises should be deduced as steps to the conclusion (what we want to prove). Without an algorithmic process, we cannot automate proofs. Proof by contradiction, using resolution, is a proof technique that can be automated.

Proof by Contradiction using Resolution

Here's the intuition: we know that all the arguments (A) are true and we want to prove the conclusion (C). We'll negate C and then show that $A \wedge \neg C$ is false. Since we know that A is true, this means that $\neg C$ must be false, therefore C must be true – which is exactly what we want to prove.

Let's get more technical now. The goal of our proof is to show that the compound proposition 'arguments (A) $\rightarrow$ conclusion (C)' is a tautology. Remember that when the left hand side of the implication is true it doesn't inform us about the truth value of the right hand side. Thus, what we need to prove is that the right hand side (the conclusions) cannot be false, when the left hand side (the arguments) are true.

Proof by contradiction makes it easy to prove that the compound proposition $(A \rightarrow C)$ is a tautology. Consider the following:

1. $A \rightarrow C$
2. $\neg A \vee C$ using Conditional-disjunction equivalence

Thus, we want to prove 2 is a tautology. Now, if we negate 2, we get 3.

3. $\neg(\neg A \vee C)$
4. $A \wedge \neg C$ using De Morgan's Law

Side note: 4 matches our intuition (see the first paragraph in this section)

Therefore, since 4 is the negation of 2, it should be a contradiction if 1 is a tautology. Note that 4 is in a form where the arguments, A, are true. Thus, if we negate our conclusion and use simplification with A to show that we find a contradiction, then statement 2 is a tautology and thus we have proved our conclusion.

Here then are the steps in our algorithm for proof by contradiction using resolution:

- Convert all arguments to Conjunctive Normal Form (CNF) – (use Conditional-Disjunction Equivalence and De Morgan's laws and split out arguments joined by conjunction to separate lines)
- Negate the desired conclusion
- Use Resolution and Disjunction Syllogism (starting with the negated conclusion) until we conclude F
- This creates a contradiction, so the desired conclusion is true (see above for details)

Proof by Contradiction Example:

Proof. Given the premises, prove t (use proof by contradiction with resolution):

1. $\neg p \wedge q$
2. $r \rightarrow p$
3. $\neg r \rightarrow s$
4. $s \rightarrow t$

The above can be converted to CNF form using Conditional-Disjunction Equivalence and De Morgan's laws:

$\neg p \wedge q \wedge (\neg r \vee p) \wedge (r \vee s) \wedge (\neg s \vee t)$

1. $\neg p$
2. q
3. $\neg r \vee p$
4. $r \vee s$
5. $\neg s \vee t$

---

6. $\neg t$ negate the conclusion, t (because we want to solve for t)
7. $\neg s$ resolution on 6 and 5

8. r resolution on 7 and 4

9. p resolution on 8 and 3

10. F resolution on 1 and 9

This is a contradiction, therefore t must be true.
$\therefore$ t $\square$

An alternate proof, and just as sound, is as follows:

Proof. Given the premises, prove t (use proof by contradiction with resolution):

1. $\neg p$

2. q

3. $\neg r \vee p$

4. $r \vee s$

5. $\neg s \vee t$

---

6. $\neg t$ negate the conclusion, t (because we want to solve for t)

7. $p \vee s$ resolution on 3 and 4

8. $p \vee t$ resolution on 7 and 5

9. p resolution on 8 and 6

10. F resolution on 1 and 9

This is a contradiction, therefore t must be true.
$\therefore$ t $\square$

Conclusion

Logic proofs give a mathematical way to create sound arguments. They are fundamental to the field of Computer Science. See the book* for further examples and details.

*All definitions are from *Discrete Mathematics and Its Applications*, by Kenneth H. Rosen.