CMPSCI 250: Introduction to Computation

Lecture 11: Proof Techniques
David Mix Barrington
5 March 2013

Proof Techniques

- Review: The General Setting for Proofs
- Types of Proof: Direct, Contraposition, Contradiction
- Types of Proof: By Cases, Exhaustive, Equivalences
- Existence Proofs
- Non-Constructive Existence Proofs
- Example: Tiling Problems

Review: The General Setting for Proofs

- Last time we described the general set-up for formal proofs. We have statements we are assuming to be true, called **premises**, and statements we want to prove true, called **conclusions**. There are also statements assumed true as part of the definitions of our terms, called **axioms**.

- Our goal is to produce more statements that will be true if the premises are true. We can use **logical equivalences**, rules of the form $p \leftrightarrow q$, to add new statements that are true if and only if existing statements are true. And we can use **logical implications**, rules of the form $p \rightarrow q$, to add to our store of true statements as well.

- Rosen points out that informal mathematical usage often leaves out the initial "let x be arbitrary" when we use the UG rule to prove a statement of the form $\forall x{:}P(x)$. But we should always be aware of the role of each variable.

Types of Proof: Direct Proof

- In a **direct proof** of a statement of the form $P \rightarrow C$, we assume that P is true and derive C from it. This is often done inside a UG proof.
- An **even number** is an integer that is 2 times an integer. Let's give a direct proof of "the square of any even number is even", or in symbols, "$\forall n: E(n) \rightarrow E(n^2)$". We let n be arbitrary, assume that n is even, and try to prove that n^2 is even.
- From the definition, "n is even" means that there exists a number k such that $n = 2k$. Given that, we calculate that $n^2 = 4k^2$. Can we show that $4k^2$ is even? Yes, it is equal to $2(2k^2)$. So we have established our conclusion.
- Note that formally, we use EI to introduce the variable k and EG to get rid of it, both times using the definition "$E(n) \leftrightarrow \exists k: n = 2k$".

iClicker Question #1: Direct Proof

- I would like to make a direct proof of the statement “Every odd integer is the difference of two perfect squares”. **How should I start**?
- (a) “Let $w = x^2$ and $y = z^2$ be two perfect squares.”
- (b) “Let $x = 2y + 1$ be an odd integer.”
- (c) “Let $x = 2y + 1$ be an odd integer that is not the difference of any two perfect squares.”
- (d) “Let $x = y^2 - z^2$ be an odd integer.”

The Forward-Backward Method and Indirect Proof

- Once we have established our premises and our conclusion, we need to construct a chain of equivalences and implications that lead from the premises to the conclusion. To search for this, we might try to find the *first* step in the chain, by finding something we can derive *from* a premise. Or we might find the *last* step in the chain, looking for something *from which* we can prove the conclusion. Either way, we have produced a different proof problem, and if our choice was correct we are looking for a shorter proof.

- We'll now see a group of methods that are collectively called **indirect proof**. These involve replacing our premise and our conclusion with a different premise and conclusion, or possibly a set of premise/conclusion pairs. By the rules of logic, carrying out the new proof or proofs will suffice to prove our original premise from our original conclusion.

- We choose these methods if they will make our proof easier, for example by giving us premises from which we can more easily derive more things.

Types of Proof: Contraposition

- Remember that the contrapositive of an implication "$p \rightarrow q$" is the statement "$\neg q \rightarrow \neg p$". An implication is true if and only if its contrapositive is true, so we may replace the implication by the contrapositive anywhere in a proof.

- Thus if we want to prove $P \rightarrow C$, we can do it by proving $\neg C \rightarrow \neg P$. A direct proof of $\neg C \rightarrow \neg P$ begins by assuming $\neg C$ and then uses this assumption to prove $\neg P$. Rosen calls this a **proof by contraposition**, and elsewhere it is often called an **indirect proof**.

- Let's try a proof by contraposition for "if $n = ab$ and both a and b are positive integers, then either $a \geq \sqrt{n}$ or $b \geq \sqrt{n}$". The contrapositive of this is "if $a < \sqrt{n}$ and $b < \sqrt{n}$, then $n \neq ab$". To prove this directly, we assume that $a < \sqrt{n}$ and $b < \sqrt{n}$, and just multiply the two inequalities together to get $ab < n$.

- Why would we do this? In this case $\neg C$ was easier to derive things from than was P.

Types of Proof: Contradiction

- The more and stronger premises we have, the easier it is to carry out a proof. In a **proof by contradiction**, we assume the negation of what we want to prove, and derive the statement "false". Because "0 → p" is a tautology, once we have one false statement we can derive any other one. So once we have derived something we know to be false, for example by deriving two statements that contradict each other, we have proven the original statement.

- In the case of an implication P → C, the negation is P ∧ ¬C. So we start with two premises, and we try to work toward a contradiction.

- Here's a proof by contradiction of "if $n^3 + 5$ is odd, then n is even". We assume that $n^3 + 5 = 2x + 1$ and that $n = 2y + 1$. We compute that $(2y + 1)^3 + 5 = 8y^3 + 4y^2 + 2y + 1 + 5 = 2(4y^3 + 2y^2 + y + 3)$, an even number. This is a contradiction because an integer cannot be both even and odd.

iClicker Question #2: Proof by Contradiction

- Here are three valid proofs of the statement “Duncan is asleep” from the premises (1) “If Duncan is not asleep, then he is barking”, and (2) “Duncan is not barking”. Which one is a proof by contradiction?

- (a) Duncan is not barking. By Modus Tollens on the first premise, he must be asleep.

- (b) The contrapositive of the first premise is “if Duncan is not barking, then he is asleep”. He is not barking by the second premise, so he is asleep.

- (c) Assume that Duncan is not asleep. Then by Modus Ponens, he would be barking. But he is not barking. So he is asleep.

Types of Proof: Cases and Syllogism

- As in programming, we can use the **divide-and-conquer method** to break our proof problem into two or more simpler ones. We have two basic ways to do this.

- In **proof by cases**, we prove $P \rightarrow C$ by choosing some other proposition X and then proving *both* $(P \wedge X) \rightarrow C$ and $(P \wedge \neg X) \rightarrow C$. In each case we have more premises to work with, but the point of this is usually that C is true for *different reasons* in the two cases.

- The **hypothetical syllogism** rule of the propositional calculus says that we may derive $P \rightarrow C$ from the two implications $P \rightarrow X$ and $X \rightarrow C$, where X is any proposition at all. So by a good choice of X, we can divide our proof problem into two separate problems that might be easier. Of course we must choose an X such that the two new implications are both true!

Types of Proof: Exhaustive

- An extension of proof by cases is **exhaustive proof**, named because we "exhaust" all the possible values for some variable. (Though these proofs can sometimes be exhausting for the prover as well.)

- The **method of truth tables** is an exhaustive proof method for propositional calculus problems. With k boolean variables, there are 2^k possible settings for those variables, and each one is a separate case. Each case is usually not difficult to evaluate, but the sheer number of cases can be prohibitive. Sometimes we can use the same proof for more than one case, by exploiting similarities between them and saying "**without loss of generality (WLOG)**".

- If the number of cases is infinite, no exhaustive proof that treats one case at a time can be valid. (Usually we use mathematical induction for such problems.)

Proving Multiple Statements Equivalent

- If we want to prove two statements p and q to be logically equivalent, that is, if we want to prove $p \leftrightarrow q$, we can do it by proving both $p \rightarrow q$ and $q \rightarrow p$.

  This is another divide-and-conquer step and is very common practice in mathematics. We often speak of the "two halves" of an "if and only if" statement.

- Sometimes we have more than two statements and we want to prove that each one is equivalent to the others. (For example, we might want to show $p \leftrightarrow q \leftrightarrow r \leftrightarrow s$.) Often the most efficient way to do this is to prove a chain of implications that allows us to get any of the propositions from any of the others by hypothetical syllogism. In our example, we might prove the four implications $p \rightarrow q$, $q \rightarrow r$, $r \rightarrow s$, and $s \rightarrow t$.

An Equivalence Example

- Here we prove three statements about an integer n to be equivalent. Let P(n) be “n is even”, Q(n) be “n - 1 is odd”, and R(n) be “n^2 is even”. We’ll do this by proving the three implications P(n) → Q(n), Q(n) → R(n), and R(n) → P(n).

- P(n) → Q(n): Assume that n is even. Then n = 2k for some integer k. Then we compute that n - 1 = 2k - 1 = 2(k - 1) + 1, and by definition n - 1 is odd.

- Q(n) → R(n): Assume that n - 1 is odd. Then n - 1 = 2k + 1 for some integer k. So n = 2k + 2 and $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$ which is even by the definition of even numbers.

- R(n) → P(n): Instead we choose to prove ¬P(n) → ¬R(n). Assume that P(n) is false, so that n is odd. Then n = 2k + 1 for some integer k and $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is odd. So R(n) is false and we are done.

Existence Proofs

- When we are proving a statement of the form ∃x:P(x), the EG rule tells us that it is enough to find a particular value a such that P(a) is true. This is called a **constructive existence proof**.

- For example, to prove "∃x:∃y: $x^2 = y^3 + 1$", where the type of x and y is "integer", I could try various small values of x and y until I find x = 3 and y = 2.

- But this is not always so easy. Consider the polynomial $p(x) = x^2 + x + 41$, where x is a natural number. We can compute p(0) = 41, p(1) = 43, p(2) = 47, p(3) = 53, p(4) = 61, and notice that all the values are prime numbers. In fact the smallest counterexample to "p(x) is prime" is 41. There are other cases where long computer searches have found counterexamples to conjectures in number theory, and others where it is not known whether such counterexamples exist at all.

Non-Constructive Existence Proofs

- Sometimes you can prove that an object exists *without* naming it, by a **nonconstructive existence proof**. We give two examples.

- A rational number is a real number that can be written as p/q where p and q are both integers. We prove "there are irrational numbers x and y such that x^y is rational". It's proved elsewhere in Rosen that $\sqrt{2}$ is irrational. Let z be the number $\sqrt{2}^{\sqrt{2}}$. If z is rational, then we prove our theorem with $x = y = \sqrt{2}$. But if z is irrational, we note that $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ is rational. So we can prove our theorem with $x = z$ and $y = \sqrt{2}$. We don't know which case holds in the real world, so we don't know which x and y are the right ones, but we know that such an x and y exist.

The Game of Chomp

- **Chomp** is a two-player game played with a set of cookies laid out in an m by n rectangular array. The top left cookie is “poisoned”, and the player who takes it loses. A legal move is to take any cookie, along with all the cookies to the right of it and below it.

- We know that one player must have a winning strategy, but which? It turns out that we can prove that for any m and n, the first player has a winning strategy. But this proof is *nonconstructive* and doesn’t tell us the strategy!

- Here’s the argument. Consider the first player’s move that eats just the cookie at the bottom right. Either this leaves the second player in a losing position, or the second player has a move x that puts her in a winning position. Clearly the first player has a winning strategy in the first case. But in the second case, we can see that x was an option for the first player on her first move. Since x would then put the second player in a losing position, the first player has a winning strategy beginning with m.

iClicker Question 3: Chomp

- **Which statement is true** about games of Chomp when m = 1, so that there are n cookies in the first row and no others?

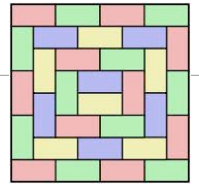
- (a) The first player can always win by eating one cookie on her first move.

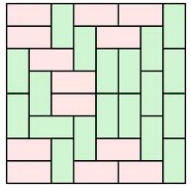
- (b) The first player has a winning strategy if n > 1, but not if n = 1.

- (c) The second player has a winning strategy for every positive n.

- (d) Trick question -- (a), (b), and (c) are all false.

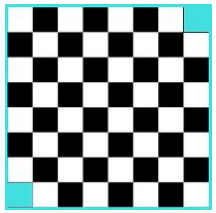
Tiling Problems





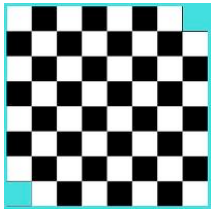
- Many puzzles involve finding a particular pattern out of a large number of possibilities. For example, **tiling problems** give us a geometrical figure to cover with some type of smaller figures. Here a valid covering has every piece of the large figure assigned to a small figure, and no overlap between small figures.

- For example, suppose we want to cover an 8 by 8 chessboard with 1 by 2 rectangles, called **dominoes**. This is not difficult at all. But what if we first remove two opposite corners from the chessboard?



Tiling Chessboards With Holes

- We can prove that no domino tiling of the 62-square figure at right is possible. The figure has 32 white squares and 30 black ones, but every domino covers one white and one black square.



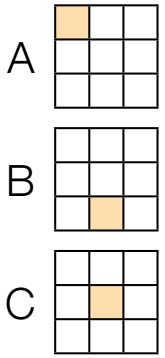
- The extra-credit question on HW#4 has you show that an 8 by 8 chessboard with two holes *can* be tiled with dominoes if the holes are on squares of opposite color.

- What about tiling the chessboard with 1 by 3 rectangles or **triominoes**? We need to delete one square, of course, but it turns out that this is not enough. The figure at right has letters to represent three colors, and any triomino covers one square of each color. But we have 21 A's, 22 B's, and 20 C's. Could we do it if we removed the northeast B instead?

```
ABCABCAB
BCABCABC
CABCABCA
ABCABCAB
BCABCABA
CABCABCA
ABCABCAB
BCABCAB
```

iClicker Question #4: An Easy Tiling Question

- To the left are three 3 by 3 rectangles, each with one square (the colored one) removed. **Which one cannot be tiled** with four 1 by 2 dominoes?



- (a) A cannot be tiled, B and C can
- (b) B cannot be tiled, A and C can
- (c) C cannot be tiled, A and B can
- (d) Trick question, any of the three can be tiled