CSC236, Introduction to the theory of computation
Week 1

25th May 2005

Danny Heap
heap@cs.toronto.edu
Sandford Fleming 4306A
416-978-5899
http://ccnet.utoronto.ca/20055/csc236h1y/

Why does anybody want to be able to talk rigorously about computing?

More than just hacking Your experience in CSC108 and CSC148 should have convinced you that there's more to computer science than just trial-and-error. You need a good idea of whether (and how well) your design will work before you write many lines of code. You need to be able to analyze other people's code for correctness and performance.

Testing isn't everything At this point you probably have acquired the habit of systematically testing your code as you write it. That's good. However, you are also probably well aware that it is impossible to test every case (for example, there are infinitely many instances of String). Using mathematics allows you to reason about infinitely many starting conditions for your programs. You can even reason about programs that nobody has written yet.

You might get theoretical You could get to like this, and find that at least part of your life as a computer scientist involves theory.

How does somebody talk rigourously about computing?

It's grubby: Mathematics is not done at a keyboard (so if I produce any mathematics in this document, it's a fraud). Usually it involves scratching away with a pencil, chalk, rejecting ideas that don't work, and polishing ideas that nearly work.

Tools of the trade We begin with pencil, paper, erasers and lots of time. We need a body of commonly-acknowledged "facts" — things we already agree are true, either because we can easily find (or derive) a proof, or because they are so obvious they don't require proof (axioms).

Time You should get in the habit of thinking about course material over many days and weeks. Good problems fight back, and often the solution doesn't come to you the first time you attempt it. Try to solve simpler and/or related problems. If you start to wake up in the middle of the night thinking about CSC236, then you might have gotten the right spirit.

It's art: Rigorous mathematics is a way of talking to others in the same field. Sometimes it involves a lot of unfriendly notation ($\forall$, $\exists$, $\sum$), but mostly it involves saying things precisely. As well as convincing your audience, you should aim to write well, clearly, and perhaps have surprising or unexpected steps in your proofs.

Nobody (IMHO) gets it completely right.

How to succeed in CSC236

Course information sheet Look at the draft. If there's anything you strongly object to, let me know now. This is the document that we (try to) live by in this course.

Marking scheme

35% of the marks are for assignments, so you should be obsessed with them during your waking hours. Instructors have a rule-of-thumb that says you should spend 10 hours/week on our course (lectures and tutorials plus 7 more). You may have a different rule-of-thumb, but assignments are devised with that 7-hours-outside-class model. Since you have at least a couple of weeks to think about them, assignments in this course (as in other CS courses) will go well beyond examples covered in class. Let me know if assignments are too easy or too hard.

Another large (but not too large) portion (35%) of the marks are for the final exam. I require that you reach a threshold of 40% on the final exam to pass this course. The rationale for this is to make sure that you understand the material in the assignments, and don't simply coast on the work of others. Be sure you understand assignment and lecture material, since these are good sources for related exam, test, and quiz questions.

Two midterms worth 10% each. You should think of these as an early warning. You may be doing okay on the assignments, but you must also be able to demonstrate your mastery of the material in a test and exam setting. If the midterm doesn't go well for you, talk to me about how to change your study methods before the final exam.

Five quizzes worth 2% each. These are to re-inforce your review of the previous lecture.

Contact Ask questions during lectures. It makes both our jobs easier. Sometimes I'll ask questions back...

I've tried to schedule adequate office hours that work for daytime and evening students. You should make use of office hours, and tutorials, to ask questions about assignments and lecture material, since you pay very high tuition for them.

The course web page has a bulletin board where you can post questions about the course and assignments. I will try to answer questions, and post hints. Please don't post your solutions on the bulletin board (that could be an academic offense).

Plagiarism (not!) Don't gamble that you can plagiarize and get through this course. If a TA thinks you are passing off somebody else's work as your own, they are duty-bound to bring it to my attention. If I agree with them, I'm duty-bound to bring it to the attention of the Faculty of Arts and Science. The consequences are long (about a year for a decision), messy, and unpleasant for all concerned.

If you escape detection, you still have to pass the midterms and get at least 40% on the final exam. These thresholds are designed to be difficult if you haven't mastered the assignment material. I think the worst possible result is to attend 13 weeks of the course, and then bomb the exam.

Finally, if you escape all those consequences, plagiarism devalues the U of T degree. We claim our graduates are bright, independent thinkers, and we don't want widespread plagiarism to make

this untrue.
Give generous credit to whomever (and whatever) you consult as sources. Work alone when possible. Consult your instructor and TAs.

What sort of proof techniques are there?

The mathematical community agrees on certain conventional rules that a proof is allowed to use (implication, contradiction, etcetera). As well, there are certain commonly-used categories of proof. Here are some:

Direct proof: (If integer n is even $\Rightarrow n^2$ is even)

In everyday language, an implication corresponds to the forms "P implies Q," "Q follows from P," "if P then Q," and "P is sufficient for Q" (among others). You can think of this as a Venn diagram where P is a subset of Q (think "all P are Q"). In a direct proof, the idea is to assume that n is even and derive the fact that n^2 is even. Try to use definitions and already well-known implications that follow from n being even.

Rough work: What do we know already about even integers? How can we represent a generic (arbitrary) even integer? $n = 2k$, so $n^2 = 4k^2$. so What properties of integers will we need to verify that the square is even?
Sample solution:[1]

In general, having proved that n even $\Rightarrow$ n^2 is even does not prove the converse, n^2 even $\Rightarrow$ n even. It turns out that (in this particular case), the converse is true. Try to prove it directly, to see what sort of difficulties you run into (I predict it doesn't follow as smoothly as the proof above).

Contrapositive (of converse): (n odd $\Rightarrow$ n^2 is odd)

The idea is that the implication $A \Rightarrow B$ is logically equivalent to $\neg B \Rightarrow \neg A$, so proving one proves the other. In the Venn diagram from the previous example, this corresponds to observing that if P is a subset of Q, then $\overline{Q}$ (the complement of Q) is a subset of $\overline{P}$. It appears as though proving the contrapositive of "For integer n, n^2 even $\Rightarrow$ n is even" is easier to prove than the direct implication.

Rough work: What do we know about odd integers, and how can we represent an arbitrary one? What properties of integers help us verify that the square is odd?

Sample solution:[2]

A natural number p is prime if (a) p is greater than 1, and (b) the only natural numbers that divide p are 1 and p itself. You can practice proving that if a natural number p is both prime and greater than 2, then p is odd. Notice that the converse is false: it is not the case that if a natural number is odd, then it is both prime and greater than 2.

Contradiction (infinitely many primes)

You may think of contradiction as a special case of the contrapositive. Suppose I want to prove fact F. I gather together the entire body of human knowledge, which I denote as the conjunction of facts $F_1 \wedge F_2 \wedge \cdots \wedge F_k$ (as a species, I'm assuming humans know exactly k facts). I want to show that $F_1 \wedge \cdots \wedge F_k \Rightarrow F$. This is equivalent to the contrapositive, $\neg F \Rightarrow \neg(F_1 \wedge \cdots \wedge F_k)$. So if I assume F is false and find that this contradicts even one of the huge number of facts, F_i already known to be true, then this implies that the conjunction $F_1 \wedge \cdots \wedge F_k$ is false, and I've just proved the contrapositive.
Claim: There are infinitely many primes (Euclid).

ROUGH WORK: What do we know about finite sets that might help us? What do we know about primes that could help? If somebody told you that the largest prime is p, how would you convince them otherwise?

Sample solution:[3]

CONSTRUCTIVE (long prime-free stretches)

Sometimes a cleverly-constructed (counter)-example is all that's needed to prove a given fact. If somebody were to claim that there are no coyotes in Toronto, you might be able to take them to High Park and show them one. Similarly, somebody might argue that since there are infinitely many primes, at least one prime occurs in any sufficiently-long stretch of natural numbers. You could counter with an example.

Claim: For any natural number k, there are k consecutive composite numbers.

ROUGH WORK: Engage in wishful thinking. If you had a long composite sequence of numbers, wouldn't it be nice if their prime factors were arranged in some orderly way? Try to make this so. $2(3)(4)(5)(6)\cdots(k+1)$ is our huge number. Tell me something about huge number plus 2?

Sample solution:[4]

CASES (floor/ceiling stuff)

You may need to prove an implication of the form $(A_1 \vee A_2 \vee \cdots \vee A_k) \Rightarrow P$. This is logically equivalent to showing $(A_1 \Rightarrow P) \wedge \cdots \wedge (A_k \Rightarrow P)$ (you can draw a Venn diagram, or wait until we cover this in Chapter 5 of the notes). If this seems a bit messy or tedious, that's because it is. However, occasionally it seems to be the natural way to proceed.

Definition: If x is a real number (it possibly has a fractional part), then the FLOOR of x, denote $\lfloor x \rfloor$, is the largest integer that is no larger than x. Symmetrically, the CEILING of x, denoted $\lceil x \rceil$, is the smallest integer that is no smaller than x. Operations on floors and ceilings can be a bit tricky, and it is occasionally helpful to consider cases.

Claim: If n is a natural number, then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

ROUGH WORK: What do the floor and ceiling of $n/2$ look like when n is odd/even? Is one case particularly easy (do it first if that's the case). How can you write the cases in a generic fashion?

Sample solution:[5]

Since the claim holds for both odd and even n, it holds for all natural numbers n . QED.

INDUCTION

In this course many of the properties we'd like to prove are connected to the natural numbers (for example, by iterations of a loop in a program). A useful proof technique is induction, which comes in several flavours: Simple Induction (aka PMI), Complete Induction (aka Strong Induction), Well-Ordering Principle, Structural Induction. We'll look at:

PRINCIPLE OF MATHEMATICAL INDUCTION: what is it, and why do we think it works?

COMPLETE INDUCTION: what is it, why do we think it works

WELL-ORDERING PRINCIPLE: what is it?

Next we'll look at the connection between the three principles.

Notes

[1]Proof: Assume n is even. This means that $n = 2k$ for some integer k. Squaring this gives you $n^2 = 4k^2$. Since 2 and k are integers, so are k^2 and $2k^2$. Thus $n^2 = 2(2k^2)$, which is an even integer. So, if n is even, so is n^2. QED.

[2]Proof: Assume that n is odd. This means that $n = 2k + 1$ for some integer k. Squaring this gives you $n^2 = 4k^2 + 4k + 1$. Since k is an integer, so are k^2, $2k$, and $2k^2$, so we can re-write $n^2 = 2(2k^2 + 2k) + 1$, where $2k^2 + 2k$ is an integer. This implies that n^2 is odd. So n odd implies n^2 is odd, which is the contrapositive of what we want to prove. QED.

[3]Proof: Suppose not. Then there is a finite collection of primes, which we could list as $p_1, p_2, \ldots, p_k$. Take the product of these k primes and add 1: $n = p_1 \times \cdots \times p_k + 1$. Notice that n is not divisible by any of the primes on our list (a remainder of 1 is left if you divide by any of the p_i). Since n is a natural number greater than 2, by Proposition 1.14 in the course notes, n can be written as the product of primes (this includes unary products, so that 3 can be represented as the product of prime 3). However, none of the prime factors of n appear in the list $p_1, \ldots, p_k$, contradicting our assumption that this is a complete list of primes. Thus there are infinitely many primes, QED.

[4]Claim: Let k be your favourite (at the moment) natural number. Then there exists k consecutive composite (that is, non-prime) natural numbers.
Proof: Let $n = (k + 1)! = (k + 1)(k)(k - 1) \cdots (2)(1)$. Then the k consecutive numbers from $n + 2$ up to $n + k + 1$ are composite, since for any $i \in \{2, \ldots\ k + 1\}$, you have $n + i = i[(k + 1) \cdots (i + 1)(i - 1) \cdots (2) + 1]$. This CONSTRUCTS the proof of the claim, by exhibiting k consecutive composite numbers.

[5]Case 1: n is even, that is $n = 2k$ for some natural number k. Then $\lfloor n/2 \rfloor = k = \lceil n/2 \rceil$, so the result holds.
Case 2: n is odd, that is $n = 2k + 1$ for some natural number k. Then $\lfloor n/2 \rfloor = \lfloor (2k + 1)/2 \rfloor = \lfloor k + \frac{1}{2} \rfloor = k$, and $\lceil n/2 \rceil = \lceil (2k + 1)/2 \rceil = \lceil k + \frac{1}{2} \rceil = k + 1$, and

$$\lfloor n/2 \rfloor + \lceil n/2 \rceil = k + k + 1 = n.$$

... and the claim holds.