Constructive Logic (15-317), Fall 2025
Assignment 1: Say Hi to Logic!

Constructive Logic Staff
(Instructor: Karl Crary)

Due: Wednesday, September 3, 2025, 11:59 pm

Welcome to Constructive Logic!

This assignment will have a written portion and a coding portion. You will submit both portions through Gradescope, to the assignments labelled "Homework 1 (written)" and "Homework 1 (code)." Please submit a file named "`hw.pdf`" to the former, and a file named "`hw.deriv`" to the latter.

We recommend that you typeset your written solutions. Most students use LaTeX, but other software is acceptable. (Please put each task on its own page to speed up grading.) If you choose not to typeset your solutions, be aware that you are answerable for your handwriting. Any that the grader has difficulty reading (in the sole judgement of the grader), will be marked wrong.

For the coding portion you will use Dcheck. You can find documentation on Dcheck at `cs.cmu.edu/~crary/dcheck/dcheck.pdf` and a sample file at `cs.cmu.edu/~crary/dcheck/example.deriv`. (Be aware that the sample file uses several logics that we have not seen yet in class.)

1 Natural deduction

Recall the proof of $(A \wedge B) \supset (B \wedge A)\ \mathsf{true}$ from lecture:

$$\dfrac{\dfrac{\dfrac{[A \wedge B\ \mathsf{true}]_u}{B\ \mathsf{true}}\wedge E2 \quad \dfrac{[A \wedge B\ \mathsf{true}]_u}{A\ \mathsf{true}}\wedge E1}{B \wedge A\ \mathsf{true}}\wedge I}{(A \wedge B) \supset (B \wedge A)\ \mathsf{true}}\supset I^u$$

In Dcheck this proof is written:

```
system ND

deriv and_swap =
   (A /\ B) => (B /\ A) true
   by ImpI(u)
   >>
   B /\ A true
   by AndI
   >>
      {
      B true
```

```
by AndE2
>>
A /\ B true
by u
}

{
A true
by AndE1
>>
A /\ B true
by u
}
```

Using Dcheck, give derivations of each of the following judgements (naming them `task1`, `task2` and `task3`):

Task 1 (2 points).

$$(A \wedge (A \supset B)) \supset B \ \mathsf{true}$$

Task 2 (3 points).

$$(A \wedge ((A \wedge A) \supset B)) \supset B \ \mathsf{true}$$

Task 3 (3 points).

$$(A \wedge (A \supset B)) \supset (B \wedge B) \ \mathsf{true}$$

2 Constructive mathematics

In this class we will mostly be exploring constructive logic in a formal way, over an abstract problem domain. In this problem we will explore constructivity in informal proofs of practical mathematics.

When we ask for a constructive proof, we mean a proof that does not use any principle of reasoning that is forbidden in constructive logic. Specifically, you should not use the law of the excluded middle, double-negation elimination, or proof by contradiction.

Definition. A natural number a is said to *divide* a natural number b, written $a \mid b$, if there exists a natural number k such that $b = ak$. We write $a \nmid b$ for $\neg(a \mid b)$.

Definition. A natural number a is *composite* if there exist natural numbers $n, k > 1$ such that $a = nk$. A natural number is *prime* if it is not composite.

Task 4 (2 points). Give an (informal) constructive proof of the following proposition: for all natural numbers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Fermat's Little Theorem states that if p is prime, then for any integer a, $(a^p - a)\ mod\ p = 0$. Also note that $(2^{422687} - 2)\ mod\ 422687 = 376010$.

Task 5 (3 points). Using Fermat's Little Theorem, give a *non-constructive* proof that 422687 is composite.

Task 6 (3 points). Give a *constructive* proof that 422687 is composite. (Hint: you might find the number 331 useful.)

Task 7 (3 points). Give a constructive proof that 5 is prime. Simply stating the definition of primality is not a full proof. (Our proof is a few sentences.)

Definition. The *Fundamental Theorem of Arithmetic* states that every integer greater than 1 either is prime or factors as the product of prime numbers, and moreover, that this factorisation is unique up to reordering of factors.

Task 8 (2 points). Is the following proof that $3 \nmid 10$ constructive? Justify your answer.

> *Proof.* Assume to the contrary that $3 \mid 10$. Then there exists a k such that $10 = 3k$. By the fundamental theorem of arithmetic, k has some unique prime factorisation $k = \prod_{i=1}^{n} p_i$. So 10 factors into primes as $10 = 3 \prod_{i=1}^{n} p_i$. But we also know that 10 factors into primes as $10 = 2 \times 5$. The existence of two distinct prime factorisations for 10 contradicts the uniqueness guaranteed by the fundamental theorem of arithmetic. We thus conclude that $3 \nmid 10$.