CSE 311: Foundations of Computing I Spring 2025

Problem Set 4

Due: Wednesday, April 30th by 11:00pm

Instructions

The (a) parts of Tasks 1–6 should be submitted **first** on Cozy. You must **also** include your formal proofs in the PDF you submit on Gradescope so that the grader can confirm that your English proof properly translates your formal proof. If you are using LaTeX, you can copy Cozy's "Show LaTeX" output. If you are not using LaTeX, a screenshot is fine!

If you are unable to submit in Cozy due to technical problems or if you are unable to complete the problem, you can submit your work on Gradescope (for partial credit in the second case).

Your Gradescope submission should follow these rules:

- Each numbered task should be solved on its own page (or pages). Do not write your name on the individual pages. (Gradescope will handle that.)
- When you upload your pages, make sure each one is **properly rotated**. If not, you can use the Gradescope controls to turn them to the proper orientation.
- Follow the Gradescope prompt to **link tasks to pages**. You do not need to link tasks that you did not include, e.g., Task 7 (extra credit) or Tasks 6 (if you submitted on Cozy).
- You are not required to typeset your solution, but your submission must be **legible**. It is your responsibility to make sure solutions are readable — we will *not* grade unreadable write-ups.

Task 1 – Even So Soon? [16 pts]

For any predicate for which we have a definition, we have rules that allow us to replace the predicate with its definition or vice versa. As an example, consider "Even", defined by $\text{Even}(x) := \exists y\,(x = 2 \cdot y)$. We can use this definition via these two rules:

Def of Even

$$\frac{\text{Even}(x)}{\therefore\ \exists y\,(x = 2 \cdot y)}$$

Undef Even

$$\frac{\exists y\,(x = 2 \cdot y)}{\therefore\ \text{Even}(x)}$$

For example, if we know $\text{Even}(6)$ holds, then "Def of Even" allows us to infer $\exists y\,(6 = 2 \cdot y)$. On the other hand, if we know that $\exists y\,(10 = 2 \cdot y)$, then "Undef Even" allows us to infer $\text{Even}(10)$.

In English proofs, we do not distinguish between replacing $\text{Even}(x)$ by its definition and vice versa (both are "by the definition of Even"), but in Cozy, you need to say which direction you are doing by using `defof Even` or `undef Even`.

We will also need to use Cozy's `algebra` rule, which lets you infer equations implied by others:

Algebra

$$\frac{x_1 = y_1 \quad \ldots \quad x_n = y_n}{\therefore\ x = y \text{ (if implied)}}$$

For example, if you know that $2x = 3y + 1$ and $y = 2$, then you can infer $2x = 7$ by `algebra`. Cozy will not infer, from that, that $x = 7/2$ because the latter is not an integer. More generally, Cozy will only add equations and multiply both sides by constants. It will not do division.

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall x\,\forall y\,((\text{Even}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(3x + 2y))$$

In English, this says that, for any even integer x and odd integer y, the integer $3x + 2y$ is even.

a) Write a **formal proof** that the claim holds.

Remember that Cozy (like Java) expects a "`*`" for multiplication. It will misunderstand if you write `2a + 2 = 2(a+1)`. You have to write that as `2*a + 2 = 2*(a+1)`.

> Submit and check your formal proof here:
>
> http://cozy.cs.washington.edu
>
> You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 2 – Dividing the Difference [16 pts]

In this problem, we will use the predicate "Divides", defined by $\text{Divides}(x, y) := \exists k\,(y = k \cdot x)$. We can use this definition via these two rules:

Def of Divides

$$\frac{\text{Divides}(x, y)}{\therefore\ \exists k\,(y = k \cdot x)}$$

Undef Divides

$$\frac{\exists k\,(y = k \cdot x)}{\therefore\ \text{Divides}(x, y)}$$

Note that, in math, we write $\text{Divides}(x, y)$ with the nicer notation "$x \mid y$".

Let domain of discourse be the integers. Consider the following claim:

$$\forall a \forall b \forall c\,(((a \mid b) \wedge (a \mid (b + c)) \rightarrow (a \mid c))$$

In English, this claim says that *differences between divisible integers are divisible*: if a divides both two integers b and $b + c$ (for any a, b, c), a also divides the difference between them, c. As an example, if you know that 37 divides both 71706 and 88578, you know that 37 also divides $88578 - 71706$.

a) Write a **formal proof** that the claim holds.

Submit and check your formal proof here:

http://cozy.cs.washington.edu

You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 3 – #modgoals [16 pts]

In this problem, we will use "Congruent", defined by $\text{Congruent}(a, b, m) := \text{Divides}(m, a - b)$ (i.e., $m \mid a - b$). We can use this definition via these two rules:

Def of Congruent

$$\frac{\text{Congruent}(a, b, m)}{\therefore \ \text{Divides}(m, a - b)}$$

Undef Congruent

$$\frac{\text{Divides}(m, a - b)}{\therefore \ \text{Congruent}(a, b, m)}$$

Note that, in math, we write $\text{Congruent}(a, b, m)$ with the nicer notation $a \equiv_m b$.

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall a \, \forall b \, (((a \equiv_6 2) \wedge (a + b \equiv_3 1)) \rightarrow (a - b \equiv_3 0))$$

In English, this says that, for any integers a and b, if a is congruent to 2 modulo 6 and $a + b$ is congruent to 1 modulo 3, then $a - b$ is congruent to 0 modulo 3.

a) Write a **formal proof** that the claim holds.

Submit and check your formal proof here:

http://cozy.cs.washington.edu

You can make as many attempts as needed to find a correct answer.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Task 4 – Div and Let Div [16 pts]

Now we're good at proving statements about parity (odd and even), divisibility, and congruence using their definitions and "algebra" in Cozy. Unfortunately, "algebra" doesn't always work — **it can't handle division** :(

Integers are not closed under division, which means we can't freely divide in the domain of integers because the result might not be an integer. So if we want to divide both sides of an equation by the same number, we need to make sure that both sides are actually divisible by it, and this rule is already built into Cozy as a **theorem**!

For any known theorem, we have rules that allow us to cite the fact that the theorem holds and, if the statement of the theorem is a domain-restricted $\forall$, to apply it in one step to specific values.

In this problem, we will use the theorem "DivideEqn". It says that, if you have the equation $ca = cb$ and you know that $c \neq 0$, then you can divide both sides of the equation by c to get $a = b$. We can use this theorem in a formal proof via these two rules:

Cite DivideEqn

$$\therefore \quad \forall a\, \forall b\, \forall c\, ((ca = cb \wedge \neg(c = 0)) \rightarrow a = b)$$

Apply DivideEqn

$$\frac{ca = cb \wedge \neg(c = 0)}{\therefore \quad a = b}$$

The first rule simply writes down the statement of DivideEqn. To use it, you apply Elim $\forall$ to get an implication and then Modus Ponens to get the conclusion. The second rule does these three things (Cite, Elim $\forall$, Modus Ponens) in a single step.

To gain some familiarity with these rules, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall a\, \forall b\, ((4 \mid 2a) \wedge (3b \equiv_6 9) \rightarrow \mathsf{Odd}(a - b))$$

In English, this says that, for any integers a and b, if 4 divides $2a$, and $3b$ is congruent to 9 modulo 6, then their difference, $a - b$, is odd.

a) Write a **formal proof** that the claim holds. You are given the facts $2 \neq 0$, $3 \neq 0$, and $4 \neq 0$, so that you may divide by any of those numbers.

We **strongly** recommend that you use the first rule above, via "`cite DivideEqn`" in Cozy. If you want try using the second rule, you will need to consult the Cozy documentation.

Note that this theorem only applies to an equation that looks like $c(\dots) = c(\dots)$ for some c. If your equation doesn't look exactly like this, then you would need to use Algebra to first put it in this form. For example, if your equation says $ca + cb = 5c$, then you would need to rewrite it as $c(a + b) = c(5)$ with Algebra before applying DivideEqn.

Submit and check your formal proof here:

http://cozy.cs.washington.edu

You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim ∃) can be skipped.

Task 5 – Divide and Conquer [16 pts]

As noted above, the Algebra rule mainly just knows how to multiply equations by constants and add them together. It does also know about the commutativity of multiplication, so it knows that $xy = yx$, and it can perform arithmetic on constants, so it knows that $3 \cdot 4 = 12$. However, it is easily stumped by algebra that involves multiplication and division (by non-constants).

To handle those situations, we need an even lower-level tool: the ability to substitute one side of an equation where the other appears. Since the two sides are equal to each other, whatever facts hold for one side, hold for the other. That reasoning is formalized in the following rule:

Substitute

$$\frac{P(x) \quad x = y}{\therefore \;\; P(y)}$$

For example, if we know Prime$(2x + 5)$ — i.e., that $2x + 5$ is a prime number — and we know that $x = 2y + 1$, then we can substitute $2y + 1$ for x in the first fact to get Prime$(2(2y + 1) + 5)$ — i.e., that $2(2y + 1) + 5$ is a prime number. The Algebra rule is able to see that $2(2y + 1) + 5 = 4y + 7$, so we could then conclude that Prime$(4y + 7)$ — i.e., that $4y + 7$ is prime — by Algebra.

To gain some familiarity with this new rule, let's do a proof...

Let domain of discourse be the integers. Consider the following claim:

$$\forall x \, \forall y \, \forall z \, ((4x \mid y) \wedge (6y \mid z)) \rightarrow (24x \mid z))$$

In English, this says that, for any integer x, y, and z, where $4x$ divides y and $6y$ divides z, it must be the case that $24x$ divides z.

a) Write a **formal proof** that the claim holds.

Note: If you're struggling with "Intro ∃" in Cozy, try putting (..) around the expression you want to replace. What you want to replace may not be a subexpression even if it looks like one when *pretty printed*. For example, even though xy looks like a subexpression in "$3xy$", it is not. The latter parses as $(3x)y$, so xy is nowhere in the expression! If you rewrite it as $3(xy)$, then it will be.

Submit and check your formal proof here:

http://cozy.cs.washington.edu

You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim ∃) can be skipped.

Task 6 – When All Is Said and One [16 pts]

Let the domain of discourse be the integers. Consider the following claim

$$\forall a \, \forall b \, ((a \neq 0 \wedge b \neq 0) \rightarrow ab \neq 0)$$

In English, this says that, for all integers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
We have used this fact lecture, now you will prove it.

a) Write a **formal proof** that the claim holds. Here are some **hints** on how to do this:

- Instead of proving this implication, you should prove the *contrapositive* and then turn that implication into this one via equivalence.
- You will likely need to work by cases, separately considering when a variable is zero or non-zero. To do so, note that $(x = 0) \vee \neg(x = 0)$ is a *tautology*.

Submit and check your formal proof here:

http://cozy.cs.washington.edu

You **must also** include your solution (as a screenshot, typeset LaTeX, or rewritten by hand) in the PDF you submit to **Gradescope**.

b) Translate your formal proof to an **English proof**.

Keep in mind that your proof will be read by a *human*, not a computer, so you should explain the algebra steps in more detail, whereas some of the predicate logic steps (e.g., Elim $\exists$) can be skipped.

Also remember that humans want to be told where you are going before you go there, not afterward as in formal proof. Keep this in mind when applying equivalences.

Task 7 – Extra Credit: In Mod Daylight [0 pts]

In this problem, we will need a few theorems. The first one is the Division Theorem from lecture. Here, we will call it "Division" and use it via the following two rules:

Cite Division

$$\therefore \quad \forall a\, \forall b\, ((0 < b) \to ((a = \mathsf{div}(a,b) \cdot b + \mathsf{mod}(a,b)) \wedge (0 \leqslant \mathsf{mod}(a,b)) \wedge (\mathsf{mod}(a,b) < b)))$$

Apply Division

$$\frac{0 < b}{\therefore \quad (a = \mathsf{div}(a,b) \cdot b + \mathsf{mod}(a,b)) \wedge (0 \leqslant \mathsf{mod}(a,b)) \wedge (\mathsf{mod}(a,b) < b)}$$

We will also, "MultEqns", which says that we can multiply the left- and right-hand sides of two separate equations to get a new equation. We can use this theorem in a formal proof via these two rules:

Cite MultEqns

$$\therefore \quad \forall a\, \forall b\, \forall c\, \forall d\, ((a = b \wedge c = d) \to (ac = bd))$$

Apply MultEqns

$$\frac{a = b \wedge c = d}{\therefore \quad ac = bd}$$

Finally, we will need the following theorem, "Cases3", which says that any number satisfying $0 \leqslant n$ and $n < 3$ must be 0, 1, or 2. We can use this theorem in a formal proof via these two rules:

Cite Cases3

$$\therefore \quad \forall n\, (((0 \leqslant n) \wedge (n < 3)) \to ((n = 0) \vee (n = 1) \vee (n = 2)))$$

Apply Cases3

$$\frac{(0 \leqslant n) \wedge (n < 3)}{\therefore \quad (n = 0) \vee (n = 1) \vee (n = 2)}$$

With those theorems available to us, we are now ready to state the claim we wish to prove...

Let domain of discourse be the integers. Consider the following claim:

$$\forall n\,((n^2 \equiv_3 0) \vee (n^2 \equiv_3 1))$$

In English, this says that, for any integer n, its square is congruent either to 0 or to 1 modulo 3 (i.e., it is not congruent to 2 modulo 3).

a) Write a **formal proof** that the claim holds.

You can take as given the fact that $0 < 3$, which is a hypothesis you need in order to divide by 3 via the Division Theorem.[1]

If you want, you can do this proof in Cozy via this link, but note that Cozy will not save your answer. You need to submit your formal proof in Gradescope.

b) Translate your formal proof to an **English proof**.

[1] Cozy should really be smart enough to figure out that $0 < 3$ is true — then, we could simply cite "Algebra" or something like that — but it doesn't understand inequalities at present, so we must provide this.