Problem Set 4

Due: **Wednesday**, February 5th by 11:00pm

Instructions

Solutions submission. You must submit your solution via Gradescope. In particular:

– The (a) parts of Tasks 1–5 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!

– Cozy provides an English proof translation from a formal proof, but it sounds unnatural (intentionally). It can be used as a starting point for the (b) parts of Tasks 1–5, but **any submission significantly similar to Cozy's English proofs will receive little or no credit**.

– Taks 6 is a formal proof done on paper. It is to be submitted only in GradeScope.

– Submit a *single* PDF file containing your solutions to Tasks 1–6 (and optionally 7). Follow the prompt on Gradescope to link tasks to your pages. (There, we will only grade your English translations in Tasks 1–5, but your formal proof needs to be included in the PDF for reference.)

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

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

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:

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

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.

Note that Cozy will provide an English translation of your formal proof, but this translation is *purposefully bad*. It will give you something to start with, but as you will see, it is not well written.

Task 2 – You Only Div Once [16 pts]

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

Def of Divides	Undef Divides
$\dfrac{\mathsf{Divides}(x, y)}{\therefore\ \exists k\, (y = k \cdot x)}$	$\dfrac{\exists k\, (y = k \cdot x)}{\therefore\ \mathsf{Divides}(x, y)}$

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

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

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

$$\forall a\, \forall b\, (((3 \mid a) \wedge (4 \mid b)) \rightarrow (12 \mid 4a - 6b))$$

In English, this says that, for any integer a divisible by 3 and integer b divisible by 4, the integer $4a - 6b$ is divisible by 12.

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 ∃) can be skipped.

Task 3 – #modgoals [18 pts]

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

Def of Congruent	Undef Congruent
Congruent(a, b, m) $\therefore$ Divides$(m, a - b)$	Divides$(m, a - b)$ $\therefore$ Congruent(a, b, m)

Note that, in math, we write 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:

$$\forall a \, \forall b \, (((a \equiv_8 5) \land (a + b \equiv_4 3)) \to (a - b \equiv_4 3))$$

In English, this says that, for any integers a and b, if a is congruent to 5 modulo 8 and $a + b$ is congruent to 3 modulo 4, then $a - b$ is congruent to 3 modulo 4.

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 ∃) can be skipped.

Task 4 – Div and Let Div [16 pts]

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

$$\frac{}{\therefore\ \ \forall a\,\forall b\,\forall c\,((ca = cb \land \neg(c = 0)) \to a = b)}$$

Apply DivideEqn

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

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:

$$\forall a\,\forall b\,((3a \equiv_{12} 15 \land 2b \equiv_8 4) \to (a - b \equiv_4 3))$$

In English, this says that, for any integers a and b, if $3a$ is congruent to 15 modulo 12, and $2b$ is congruent to 4 modulo 8, then their difference, $a - b$, is congruent to 3 modulo 4.

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 $\exists$) can be skipped.

Task 5 – Trying To Hit a Proving Target [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:

$$\forall a\, \forall b\, \forall c\, (((2a \mid b) \land (3b \mid c)) \to (6a \mid c))$$

In English, this says that, for any integer a, b, and c, where $2a$ divides b and $3b$ divides c, it must be the case that $6a$ divides c.

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

In this problem, in addition to the theorem "DivideEqn" we saw in Task 4, we will also use the theorem "Units", which says that 1 and -1 are the only numbers that multiply together to give you 1. We can use this theorem in a formal proof via these two rules:

Cite Units
$\therefore\ \forall a\, \forall b\, (ab = 1 \rightarrow (a = 1 \vee a = -1))$

Apply Units
$ab = 1$
$\therefore\ a = 1 \vee a = -1$

The first rule simply writes down the statement of Units. 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:

$$\forall a\, \forall b\, (((a \mid b) \wedge (b \mid a) \wedge \neg(b = 0)) \rightarrow (a = b \vee a = -b))$$

In English, this says that, for any integers a and b, if a divides b and b divides a, then you must have either $a = b$ or $a = -b$.

Consider the following English proof of the claim:

> Let a and b be arbitrary integers.
>
> Suppose that $a \mid b$, $b \mid a$, and $b \neq 0$. By the definition of divides, we have $a = jb$ and $b = ka$ for some integers j, k. Combining these equations, we see that $b = ka = k(jb) = b(jk)$. Since $b \neq 0$, we can divide both sides by b to see that $jk = 1$.
>
> Since $jk = 1$, the theorem Units tells us that $j = 1$ or $j = -1$. If the first holds, then we have $a = jb = b$. If the second holds, then we have $a = jb = -b$. Hence, in either case, we have $a = b$ or $a = -b$.
>
> Since a and b were arbitrary, we have proven the claim.

Translate this English proof into a **formal proof** that claim holds.

Hint: You will likely need several tools introduced in earlier problems, e.g., the theorems DivideEqn and Units and Substitute rule.

Task 7 – Extra Credit: Walk Like an Encryption [0 pts]

We know that we can reduce the *base* of an exponent modulo $m : a^k \equiv_m (a \text{ mod } m)^k$. But the same is not true of the exponent! That is, we cannot write $a^k \equiv_m a^{k \text{ mod } m}$. This is easily seen to be false in general. Consider, for instance, that 2^{10} mod $3 = 1$ but $2^{10 \text{ mod } 3}$ mod $3 = 2^1$ mod $3 = 2$.

The correct law for the exponent is more subtle. We will prove it in steps....

(a) Let $R = \{n \in \mathbb{Z} : 1 \leqslant n \leqslant m - 1 \wedge \gcd(n, m) = 1\}$. Define the set $aR = \{ax \text{ mod } m : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a, m) = 1$.

(b) Consider the product of all the elements in R modulo m and the elements in aR modulo m. By comparing those two expressions, conclude that, for all $a \in R$, we have $a^{\phi(m)} \equiv_m 1$, where $\phi(m) = |R|$.

(c) Use the last result to show that, for any $b \geqslant 0$ and $a \in R$, we have $a^b \equiv_m a^{b \text{ mod } \phi(m)}$.

(d) Finally, prove the following two facts about the function ϕ above. First, if p is prime, then $\phi(p) = p - 1$. Second, for any primes a and b with $a \neq b$, we have $\phi(ab) = \phi(a)\phi(b)$. (Or slightly more challenging: show this second claim for *all positive integers* a and b with $\gcd(a, b) = 1$.)

The second fact of part (d) implies that, if p and q are primes, then $\phi(pq) = (p - 1)(q - 1)$. That along with part (c) prove the final claim from (forthcoming) lecture about RSA, completing the proof of correctness of the algorithm.