Homework 02

HOMEWORK 02, DUE BY 2022-01-20

Question 1: Let the domain $\mathbb{Z}^+$ be the set of positive integers. Define these two predicates on this domain:

- $D(a, b)$ which is true iff a divides b (namely, b is divisible by a with remainder 0). For example $D(1, 6) = D(2, 6) = D(3, 6) = D(6, 6) =$ `True`, but $D(2, 1) = D(2, 5) =$ `False`.
- $O(a)$ which is true iff $a = 1$.

(A) Write these predicate sentences in English.

i. $\exists a \in \mathbb{Z}^+ \ \big(\forall b \in \mathbb{Z}^+ \ (D(a, b)) \wedge O(a)\big)$.

ii. $\forall a \in \mathbb{Z}^+ \ \forall b \in \mathbb{Z}^+ \ \forall c \in \mathbb{Z}^+ \ (D(a, b) \wedge D(b, c) \rightarrow D(a, c))$.

iii. $\forall a \in \mathbb{Z}^+ \ \exists b \in \mathbb{Z}^+ \ (D(a, b) \wedge D(b, a))$.

(B) Write these English sentences with predicates and quantifiers (use only the two given predicates, Boolean operations, parentheses and quantifiers). Use only the domain $\mathbb{Z}^+$ in all your expressions.

i. There exist two numbers a and b such that neither divides another one.

ii. There exists a number a in the domain that is a prime number (only two numbers divide it: 1 and a itself).

iii. For any positive integer a there exist a mutual prime b (namely, some number that has no common divisors with a except 1).

Answer:

(A)

i. There exists a positive integer a that divides every positive integer b, and $a = 1$. (Equivalently: There exists a number 1 that divides every positive integer.)

ii. For all positive integers a, b, c, if a divides b and b divides c, then also a divides c.

iii. For any positive integer a there exists a positive integer b such that both a divides b and b divides a.

(B)

i. $\exists a \in \mathbb{Z}^+ \ \exists b \in \mathbb{Z}^+ \ (\neg D(a, b) \wedge \neg D(b, a))$.

ii. $\exists a \in \mathbb{Z}^+ \ (\neg O(a) \wedge \exists b \in \mathbb{Z}^+ \ (D(b, a) \rightarrow D(a, b) \vee O(b)))$ (There exists a positive integer a that does not equal 1 and for every positive integer divisor b – either a also divides b (i.e. $a = b$) or b equals 1.)

iii. $\forall a \in \mathbb{Z}^+ \ \exists b \in \mathbb{Z}^+ \ \forall c \in \mathbb{Z}^+ \ (D(c, a) \wedge D(c, b) \rightarrow O(c))$ (For any positive integer a there exists a positive integer b such that for any common divisor of a and b we must have $c = 1$.)

Question 2: Consider the following predicate expression which uses the same divides predicate as the previous problem:

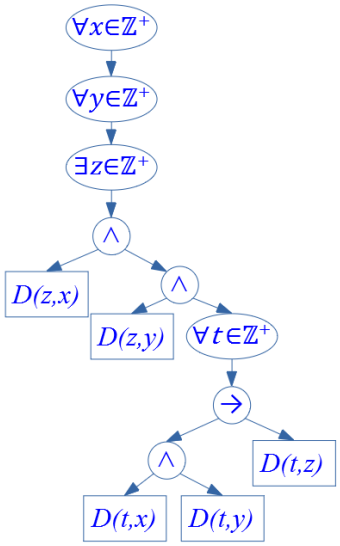
$$\forall x \in \mathbb{Z}^+ \ \forall y \in \mathbb{Z}^+ \ \exists z \in \mathbb{Z}^+ \ \Big(D(z, x) \wedge D(z, y) \wedge \forall t \in \mathbb{Z}^+ (D(t, x) \wedge D(t, y) \rightarrow D(t, z))\Big).$$

(A) Draw the abstract syntax tree for this predicate expression. (Assume that all quantifiers (such as $(\forall x \in \mathbb{Z}^+)$ and also $(\exists z \in \mathbb{Z}^+)$) are unary operators with the same precedence as negation.

(B) Let $x = 54$ and $y = 24$. Find a value $z \in \mathbb{Z}^+$ such that the statement in the big parentheses is true.

Answer:

(A) The syntax tree is shown in the picture below:



(B) Let $z = 6$. In this case $D(6, 54)$ and $D(6, 24)$ are both true. Also for every other positive integer t which divides both 54 and 24 we should have $D(t, 6)$. Indeed, the only numbers that divide **both** 24 and 54 are 1 ,:math:2, 3, and 6. And all of them are also divisors of 6.

For the given x and y, the (unique) value z which is divided by every common divisor of x and y is named *the greatest common divisor*, it is denoted by $\gcd(x, y)$. In our case $\gcd(24, 54) = 6$.

Question 3: Introduce the following sets:

- Let P be the set of all points in a two-dimensional plane.
- Let L be the set of all lines in the same plane.

Points will be denoted by upper-case variables $A, B, C, \ldots \in P$, but lines will be denoted by the lower-case variables $a, b, c, \ldots \in L$. Define the following predicates:

- $S(A, a)$ is true iff the line a goes through the point A.
- $I(A, B)$ is true iff points A and B are identical (i.e. both variables represent the same point).
- $I(a, b)$ is true iff lines a and b are identical.

Using only sets P, L and predicates $S(A, a), I(A, B), I(a, b)$, and all predicates previously defined by you, express the following new predicates and Boolean propositions:

(A) Predicate $U(A, B, a)$ that is true iff the line a goes through both points A and B (we do not require for A, B to be different).

(B) Predicate $V(a, b, A)$ that is true iff two lines a and b have their only intersection point in A.

(C) Predicate $W(a, b)$ that is true iff two lines a and b are parallel (two lines are parallel, if they do not share any points; coinciding lines are not considered parallel).

(D) Predicate $X(A, B, C)$ that is true iff all three points are located on the same line (we do not require A, B, C to be mutually different points).

(E) Predicate $Y(A, B, C, D)$ that is true iff all four points A, B, C, D form a parallelogram (a parallelogram is a quadrangle where the opposite sides are parallel).

(F) Proposition K: For every two different points A, B there exist a third point C which is not on the same line as A and B.

(G) Proposition L: For every three different points A, B, C there exist three parallel lines a, b, c such that a goes through A, b goes through B, c goes through C.

(H) Proposition M: For any three points A, B, C that are not all on the same line there exists point D such that $ABCD$ is a parallelogram.

Note: You may use the predicates defined above and also the predicates already defined in earlier steps of your solution. You can also use Boolean connectors $\neg, \wedge, \vee, \oplus, \to, \leftrightarrow$ and quantifiers. Always specify the domain for each quantifier and also enclose quantifier scopes in parentheses.

When defining a predicate such as $Y(A, B, C, D)$ you can use additional variables for other points or lines, but they should be all bound by quantifiers. The only free variables in your formulas should be A, B, C, D. When defining a proposition, it should not contain any free variables. Similar predicate expressions for 3d-geometry concepts see https://bit.ly/3fEZJjo, page 3.

Answer:

We express every new predicate and proposition using the previously defined ones.

(A) $U(A, B, a) := S(A, a) \wedge S(B, a)$.

(B) $V(a, b, A) := S(A, a) \wedge S(A, b) \wedge \forall B \in P\ (S(B, a) \wedge S(B, b) \to I(A, B))$. (The point A belongs to both lines, and any other point that also belongs to both lines must be the same as A.)

Or, equivalently, $V(a, b, A) := S(A, a) \wedge S(A, b) \wedge \neg I(a, b)$. (The point A belongs to both lines, and these lines are not identical – so it must be their only intersection.)

(C) $W(a, b) := \forall A \in P(\neg S(A, a) \vee \neg S(A, b))$. (Two lines are parallel iff an arbitrary point does not belong to at least one of them – i.e. they do not intersect.)

Or equivalently, $W(a, b) = \neg\exists A \in P(S(A, a) \wedge S(A, b))$. (Two lines are parallel iff there does not exist a point belonging to both of them. Same as previous one – but rewritten using De Morgans law.)

(D) $X(A, B, C) := \exists a \in L\ (S(A, a) \wedge S(B, a) \wedge S(C, a))$.

(E) $Y(A, B, C, D) := \exists a \in L\ \exists b \in L\ \exists c \in L\ \exists d \in L\ (U(A, B, a) \wedge U(B, C, b) \wedge U(C, D, c) \wedge U(D, A, d) \wedge W(a, c) \wedge W(b, c))$. (Four points are the vertices of some parallelogram iff there exist four lines that form the sides of this parallelogram and opposite sides are parallel.)

(F) $K := \forall A \in P\ \forall B \in P\ \exists C \in P\ (\neg I(A, B) \to \neg X(A, B, C))$. (For any two different A and B there exist C such that the predicate $X(A, B, C)$ is false – i.e. all three are not on the same line.)

(G) $L := \forall A \in P\ \forall B \in P\ \forall C \in P\ \exists a \in L\ \exists b \in L\ \exists c \in L\ (\neg I(A, B) \wedge \neg I(B, C) \wedge \neg I(C, A) \to S(A, a) \wedge S(B, b) \wedge S(C, a) \wedge W(a, b) \wedge W(b, c) \wedge W(c, a))$.

(For any three points A, B, C, if they are pairwise different, then there exist lines a, b, c such that a contains A, b contains B, and c contains C. And the lines are pairwise parallel.)

(H) $M := \forall A \in P\ \forall B \in P\ \forall C \in P\ \exists D \in P\ (\neg X(A, B, C) \to Y(A, B, C, D))$

Question 4:

In a game the initial position is a pile with N stones (N is a nonnegative integer). Two players A and B make moves alternately (player A moves first). In a single step a player can remove either 1 or 4 stones from the pile. Whoever takes the last stone wins. Prove that a position of N stones is *cold* iff either N is divisible by 5 or N gives remainder 2 when divided by 5.

Note: A game position is called *hot*, if the player making the first move can win. A game position is called *cold*, if the player making the first move from this position loses. (In both cases assume that both players make optimal moves). See https://bit.ly/3noX5lQ.

Answer:

We define the following two predicates on the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$:

- $C(n)$ is true iff the position of n stones is cold.
- $\textsc{Rem0or2}(n)$ is true iff number n is divisible by 5 (namely, gives remainder 0) or it gives remainder 2 when divided by 5.

We should prove that $\forall n \in \mathbb{N}\ (C(n) \leftrightarrow \textsc{Rem0or2}(n))$.

Assume by a contradiction that there exists a nonempty set S, where this is false:

$$S := \{n \in \mathbb{N} \mid \neg C(n) \wedge \textsc{Rem0or2}(n) \vee C(n) \wedge \neg\textsc{Rem0or2}(n)\}.$$

Namely, there must exist some number(s) for which $C(n)$ is true, but $\textsc{Rem0or2}(n)$ is false or vice versa.

By the principle of well-ordering, there should be the minimal element $n^* \in S$: for all the smaller $k < n^*$ the equivalence $(C(k) \leftrightarrow \textsc{Rem0or2}(k))$ is satisfied, but for n^* it is not. Let us analyze cases.

Case 1: $C(n^*)$ is true, so the position of n^* stones is cold. Then the other predicate $\textsc{Rem0or2}(n^*)$ must be false, so n^* gives some other remainder $(1, 3, 4)$.

If (as the first player) we get such a game position then we can always make the move to another cold position (and make our adversary lose).

- If the remainder is 1, remove one stone from the pile. The new game position is $n^* - 1$, which is divisible by 5 (and must be cold position - because we assumed that n^* is the *smallest* natural number for which the problem statement does not hold.
- If the remainder is 4, remove four stones from the pile. The new game position is $n^* - 4$, which is divisible by 5 (and must be cold position).
- If the remainder is 3, remove one stone from the pile. The new game position is $n^* - 1$, it gives remainder 2 when divided by 5, so it must be cold position again by our assumption that n^* is the smallest for which the problem statement does not hold.

In all these cases we get a contradiction: In fact, it should never be possible to move from a cold position to another cold position. Indeed, everybody who has to make a move in a cold position necessarily loses (if both players make optimal moves), so it must be impossible to move to another position and to make the other player lose.

Case 2: $C(n^*)$ is false, so the position of n^* stones is hot. The other predicate $\textsc{Rem0or2}(n^*)$ must be true, so n^* gives remainder 0 or 2 when divided by 5.

If $n^* = 0$, the position cannot be hot (since everybody who has to move from a position of zero stones cannot make a move and loses). If $n^* > 0$, then by removing either 1 or 4 stones the position would no longer give remainder 0 or 2 – so it must be hot again.

We get a contradiction – as there is no winning move for a player from a hot position (contradicts the definition of hot positions).

We summarize that playing this game means following a simple strategy – remove one or four stones to reach a cold position (shown with blue C in the pictuer below). On the other hand, if your opponent has already moved to such a cold position, then you will lose the game (unless bluffing helps and your opponent makes some mistake).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	...
C	H	C	H	H	C	H	C	H	H	C	H	C	H	H	C	H	C	H	H	...

Question 5: A larger-than-usual chessboard is subdivided into 10×10 smaller squares.

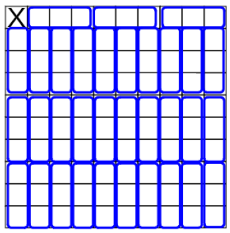
(A) Is it possible to remove one of the little squares so that the remaining chessboard can be cut into 33 rectangles of size 1×3? (The rectangles can be either horizontal or vertical).

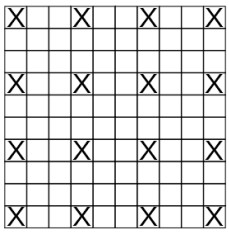
(B) Is it possible to remove one of the little squares so that the remaining chessboard cannot be cut into 33 rectangles of size 1×3?

Note: The theory of chessboard cutting is in (Rosen2019, p.108); see subchapter *1.8.8 Tilings*.

Answer:

(A) If we remove the little square in the upper-left corner, then the remaining square is easy to cut to pieces – see image. In fact, there are 16 out of 100 squares such that any one of them can be removed and the remaining square can be cut into 1×3 rectangles. All of them are marked in the image below with X.

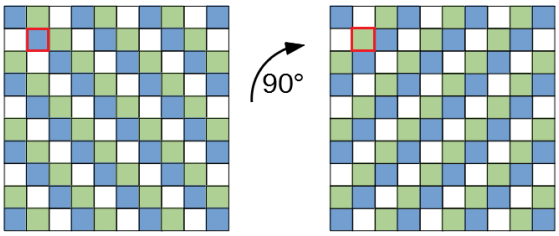




(B) If we remove any of the remaining $100 - 16 = 84$ squares (for example, the 2nd square on the 2nd row), then the remaining square cannot be cut into rectangles 1×3. A chessboard coloring into three colors is shown below. There are $1 + 4 + 7 + 10 + 7 + 4 + 1 = 34$ blue squares, there are also 33 green and 33 white ones.

The coloring has been made so that every rectangle 1×3 (horizontal or vertical) contains exactly one square of every color. Removing any green or white square will result in only 32 squares of some color, so it will not be sufficient for 33 rectangles 1×3.

If we rotate the colored chessboard by $90°$ angle, then the colors change. Consider removing the second square on the second row (highlighted). In one of the colorings this square was blue, but in another coloring it is evident that removing it is not OK. The only squares that stay blue (namely, belong to the "surplus" color) are the 16 squares found in (A).



Question 6 (Supplementary Task):

Introduction: Coq is a proof assistant that can verify the correctness of formal proofs. The simplest results to prove in Coq are Boolean tautologies – expressions built from propositional variables that are always true. You can run Coq in a browser (see https://coq.vercel.app/scratchpad.html) or install a standalone Coq IDE on your computer.

Problem: Use Coq proof assistant to prove the following tautologies (Rosen2019, p.38, Problem 12):

(A) $(\neg p \wedge (p \vee q)) \rightarrow q$

(B) $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

(C) $(p \wedge (p \rightarrow q)) \rightarrow q$

(D) $((p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)) \rightarrow r$

```
Lemma L12A: forall p q: Prop, (~p /\ (p \/ q)) -> q.
Proof.
  Admitted.

Lemma L12B: forall p q r: Prop, ((p -> q) /\ (q -> r)) -> (p -> r).
Proof.
  Admitted.

Lemma L12C: forall p q r: Prop, (p /\ (p -> q)) -> q.
Proof.
  Admitted.

Lemma L12D: forall p q r: Prop, ((p \/ q) /\ (p -> r) /\ (q -> r)) -> r.
Proof.
  Admitted.
```

Note: Your proofs with Coq should not contain commands like `tauto` or `Admitted`. Proofs of many tautologies can be found here: https://bit.ly/321Osqc. Another good source to learn about Coq is Buffalo CSE191 (an equivalent of the RBS course *Discrete Structures*) – https://bit.ly/3rfIACe.

Answer:

Here is a possible solution with all four Lemmas proven in Coq:

```
Lemma lemma12A: forall p q: Prop, (~p /\ (p \/ q)) -> q.
Proof.
  intros p q.
  intros H1.
  destruct H1 as [H2 H3].
  destruct H3 as [H4 | H5].
  contradiction.
  apply H5.
Qed.


Lemma lemma12B: forall p q r: Prop, ((p -> q) /\ (q -> r)) -> (p -> r).
Proof.
  intros p q r.
  intros H1.
  destruct H1 as [H2 H3].
  intros H4.
  apply H3.
  apply H2.
  apply H4.
Qed.


Lemma lemma12C: forall p q: Prop, (p /\ (p -> q)) -> q.
```

(continues on next page)

(continued from previous page)

```
Proof.
  intros p q.
  intros H1.
  destruct H1 as [H2 H3].
  apply H3.
  apply H2.
Qed.


Lemma lemma12D: forall p q r: Prop, ((p \/ q) /\ (p -> r) /\ (q -> r)) -> r.
Proof.
  intros p q r.
  intros H1.
  destruct H1 as [H2 H3].
  destruct H3 as [H4 H5].
  destruct H2 as [H6 | H7].
  apply H4.
  apply H6.
  apply H5.
  apply H7.
Qed.
```