COMPSCI 230: Discrete Mathematics for Computer Science

Recitation 3: Practice with Propositions, Predicates, Intro to Proofs

Spring 2020 *Created By: David Fischer*

1. Predicates and Quantifiers

   (a) Express the following as a predicate formula, and determine the truth value over the domain of discourse.

      i. Golbach's conjecture: "Every even integer greater than two is the sum of two primes."

$$R(a,b,c) \leftrightarrow a+b=c$$
$$E(d) \leftrightarrow \exists e \in \mathbb{Z} \; . \; d=2e \qquad \text{(d is even)}$$
$$G(f) \leftrightarrow (f>2)$$
$$P := \{g \in \mathbb{Z} \; . \; \text{g is prime}\} \qquad \text{(P is the set of all prime numbers)}$$
$$\forall x \in \mathbb{Z} \; . \; G(x) \wedge E(x) \rightarrow \exists y,z \in P \; . \; R(y,z,x)$$

      ii. "The sum of squares of any two integers is less than the square of their sum." Answer: The domain is the integers ($\mathbb{Z}$) and the predicate formula is

$$P(x,y) \leftrightarrow (x^2+y^2 < (x+y)^2)$$
$$\forall x,y \in \mathbb{Z} \; . \; P(x,y)$$

      To determine the truth value, expand $(x+y)^2$ into $x^2+2xy+y^2$, which yields the expression $P(x,y) \leftrightarrow (0 < 2xy)$, which is not the case if $x=1$ and $y=-1$. Note the expression does hold for the *positive* integers, or natural numbers (the proof is left as an exercise).

      iii. "The average of any two integers is an integer." The domain is the set of all integers $\mathbb{Z}$, and the formula is

$$P(a,b,c) \leftrightarrow (\frac{a+b}{2}=c)$$
$$\forall x,y \in \mathbb{Z}, \exists z \in \mathbb{Z} \; . \; P(x,y,z)$$

      This is clearly incorrect. (example x = 1, y = 2, average is a rational number).

      iv. "Every composite number greater than one has a factor other than one which is at most its square root." Answer: The domain is the set of all *positive* integers (implied since we can't take the square root of a negative number), and the formula is as follows

$$F(a,b,c) \leftrightarrow (ab=c); \; H(d) \leftrightarrow (d=1); \; L(e,f) \leftrightarrow e \leq \sqrt{f};$$
$$C(g) \leftrightarrow (\exists h,i \in \mathbb{Z} \; . \; \neg(H(h) \vee H(i)) \wedge F(h,i,g)) \qquad \text{("g is a composite number")}$$
$$\forall x \in \mathbb{Z}^+ \; . \; C(x) \rightarrow \exists y,z \in \mathbb{Z}^+ \; . \; (\neg(H(y) \vee H(z)) \wedge F(y,z,x) \wedge L(z,x))$$

(b) Express the negation of the following so that all negation symbols immediately precede predicates.

i. $\forall x, y \exists z \; . \; A(x, y, z)$

ii. Goldbach's conjecture

iii. $\forall g \; . \; [A(g) \lor \exists h \; . \; [B(g, h) \lor A(h)]]$

Answers:

i. $\exists x \exists y \forall z \; . \; \neg A(x, y, z)$

ii. Define P, $E(d)$ and $G(f)$ as in 1.a.i. Then the formula is $\exists x \in \mathbb{Z}, \forall y, z \in P \; . \; E(x) \land G(x) \rightarrow \neg R(y, z, x)$

iii. $\exists g \; . \; [\neg A(g) \land \forall h \; . \; [\neg B(g, h) \land \neg A(h)]]$

2. Proofs

Recall that all statements before $\rightarrow$ are called the *antecedent*, and all statements that follow are called the *consequent*.

(a) Prove the following theorems:

i.

Theorem 1. *If x is an even and prime integer, then $x = 2$.*
We will proceed with a direct proof, again by contradiction, and again by proving the contrapositive. The direct proof proceeds as follows:

Proof. Suppose a is an even and prime number. Since a is even, it is divisible by 2. Since a is prime, it is divisible by only itself and 1. Then, a is divisible by only 2 and 1, and so it must be 2 since 1 is odd. □

The proof by contradiction proceeds as follows:

Proof. Suppose there exists an integer b that is even and prime and which is not 2. Then, b is divisible by 2, and so it is not prime. This contradicts our definition of b, and so our original assertion (that b exists) must be false, and there is no even and prime integer that is not 2. □

For your edification, consider the predicate formula for the statement:

$$
\begin{aligned}
A(l) &\leftrightarrow (l = 2) && \text{(l equals 2)} \\
B(m) &\leftrightarrow (\exists n \in \mathbb{Z}^+ \; . \; m = 2n) && \text{(m is even)} \\
C(o, p) &\leftrightarrow (o = p) \\
D(q) &\leftrightarrow (q = 1) \\
E(r, s) &\leftrightarrow (\exists t \in \mathbb{Z} \; . \; r = st)/ && \text{(r is divisible by s)} \\
F(u) &\leftrightarrow (\forall v \in \mathbb{Z} \; . \; (\neg C(v, u) \land \neg D(v)) \rightarrow \neg E(u, v) && \text{(u is prime)} \\
\equiv F(u) &\leftrightarrow (\forall v \in \mathbb{Z} \; . \; E(u, v) \rightarrow C(v, u) \lor D(v)) \\
\forall x \in \mathbb{Z}^+ \; . \; (B(x) \land F(x)) &\rightarrow A(x) && \text{(if x is even and prime then x is 2)} \\
(\equiv \forall x \in \mathbb{Z}^+ \; . \; \neg B(x) &\lor \neg F(x) \lor A(x))
\end{aligned}
$$

The final proof technique follows:

Proof. The contrapositive of the statement is the following: if $x \neq 2$, then x is not even, or x is not prime. In predicate formulation this is

$$\forall x \in \mathbb{Z}^+ \, . \, \neg A(x) \to (\neg B(x) \vee \neg F(x))$$
$$(\equiv \forall x \in \mathbb{Z}^+ \, . \, A(x) \vee \neg B(x) \vee \neg F(x))$$

We proceed with a direct proof on this statement. Let c be a positive integer and assume $c \neq 2$. There are two cases for c (note that proof by cases is a general framework that can be used on situations when cases are exhaustive): either c is even, or c is odd. First, if c is even, then $c = 2d$ for some integer d, and so c must be strictly greater than 2. Since c is strictly greater than two, and is divisible by two, c must not be prime, and so the consequent is satisfied, and the contrapositive is TRUE in this case. If c is odd, then clearly c is not even or is not prime (since it is not even), and so the consequent is satisfied, and the contrapositive is TRUE in this case. Therefore, in all cases, the contrapositive is TRUE, and so the original statement must always be TRUE as well. □

ii.

Theorem 2. *For some integer x, if x^2 is divisible by 4, then x is even.*

Proof. We proceed with a proof on the contrapositive statement. The contrapositive is as follows: if x is odd, then x^2 is not divisible by 4. Now, let a be some odd integer. Since a is odd, then a^2 is odd. Then, a^2 is not divisible by 4, and so the contrapositive is TRUE, which proves our original claim as well. □