1. Which of the following are tautologies, which are conditional propositions, and which are contradictions? (No proof is necessary.)

(a) \((p \rightarrow q) \oplus r \rightarrow ((p \oplus r) \rightarrow (q \oplus r))\)
(b) \[((p \vee q) \land r) \leftrightarrow (p \lor (q \land r))\)
(c) \((p \oplus q) \oplus (p \leftrightarrow q)\)
(d) \(p \land q \land \neg r \land (\neg q \lor r)\)

2. Write each of the following as a statement in the Predicate Calculus. You may use only the domain and predicates specified, as well as any algebraic expression.

(a) “If \(n\) is odd, then \(n^2\) is odd.” Domain: \(Z\); Predicates: \(O(n)\), meaning “\(n\) is odd.”
(b) “For every \(n\), there is a solution to \(a^2 + b^2 = c^2\) with \(a, b,\) and \(c\) greater than \(n\) and having no factors in common other than 1.” Domain: \(N\); Predicates: \(D(x, y)\), meaning “\(x\) divides \(y\).”
(c) “For every two distinct rational numbers, there is an irrational number between them.” Domain: \(R\); Predicates: \(Q(x)\), meaning “\(x\) is rational.”
(d) “There exists a bijection between the rationals and the natural numbers.” Domain: \(f \in N \rightarrow Q\), \(q, r, n, m \in N\); Predicates: none.

3. Prove that the following proposition is a tautology using logical equivalences:

\((p \land (\neg q \rightarrow \neg p)) \rightarrow q\)

You may use without proof the fact that \((p \rightarrow q) \equiv (\neg p \lor q)\); refer to this as “Fact A.”

4. Show that \(\forall x \exists y P(x, y)\) and \(\exists y \forall x P(x, y)\) are not logically equivalent.

5. Prove that, for any sets \(S\) and \(T\), \(P(S) \cap P(T) = P(S \cap T)\). (Recall that \(P(A)\) denotes the power set of \(A\).)

6. Let \(\rho(n)\), for \(n \in Z^+\), denote the largest natural number \(k\) so that \(2^k\) divides \(n\). Show that

\[\forall a \forall b (\rho(ab) = \rho(a) + \rho(b))\]

where the domain of \(a\) and \(b\) is \(Z^+\).

7. Show that the following statements are equivalent for a set \(A\) and a natural number \(n\).

(a) \(|A| = n\).
(b) \(n\) is the smallest natural number so that, for all finite sets \(B\), \(|A \cap B| \leq n\).
(c) \(n\) is the largest natural number so that, if \(A \subset B\) and \(B\) is finite, then \(|B| > n\).
(d) For all finite sets \(B\), \(|A \cup B| + |A \cap B| = n + |B|\).

8. Prove that, for each positive integer \(n\),

\[
\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1}.
\]

9. Prove that the set of all polynomials with integer coefficients is countable. (You may use without proof the fact that every subset of a countable set is countable.)
Solutions

1. (a) Tautology
   (b) Conditional
   (c) Tautology
   (d) Contradiction

2. (a) \( \forall n(O(n) \rightarrow O(n^2)) \)
   (b) \( \forall n \exists a \exists b c \exists ((a > n) \land (b > n) \land (c > n) \land (a^2 + b^2 = c^2) \land \forall d(D(d, a) \land D(d, b) \land D(d, c) \rightarrow (d = 1))) \)
   (c) \( \forall q \forall r ((q \neq r) \land Q(q) \land Q(r) \rightarrow \exists s(\neg Q(s) \land (((q < s) \land (s < r)) \lor ((r < s) \land (s < q)))) \))
   (d) \( \exists f \forall q \forall r (((f(q) = f(r)) \rightarrow (q = r)) \land \forall n \exists (f(q) = n)) \)

3. Let \( A = (p \land (\neg q \rightarrow \neg p)) \rightarrow q \). Then
   \[
   A \equiv (p \land (\neg q \lor \neg p)) \rightarrow q \\
   \equiv (p \land (q \lor \neg p)) \rightarrow q \\
   \equiv ((p \land q) \lor (p \land \neg p)) \rightarrow q \\
   \equiv ((p \land q) \lor \top) \rightarrow q \\
   \equiv (p \land q) \rightarrow q \\
   \equiv \neg (p \land q) \lor q \\
   \equiv (p \lor \neg q) \lor q \\
   \equiv p \lor (\neg q \lor q) \\
   \equiv p \lor \top \\
   \equiv \top 
   \]
   by Fact A
   by Negation Law
   by Double Negation
   by Idempotence
   by Distributivity
   by De Morgan’s Law
   by Negation Law
   by Identity Law
   by Negation Law
   by Domination Law.

4. To show that two statements in the Predicate Calculus are not logically equivalent, we need only provide a domain and interpretation of the predicates so that one statement is true and the other is false. So, let the domain be \( \mathbb{Z} \), and let \( P(x, y) \) mean “\( x + y = 0 \)” in \( \mathbb{Z} \). Then it is true that \( \forall x \exists y P(x, y) \), since \( y = -x \) is well defined for all integers, and \( x + (-x) = 0 \). On the other hand, it is not true that \( \exists y \forall x P(x, y) \). If there existed such a \( y \), then \( x + y = 0 \) for every \( x \). In particular, \( 0 + y = 0 \), so \( y = 0 \). We may also take \( x = 1 \), so \( 1 + y = 0 \); however, \( 1 + y = 1 + 0 = 1 \), a contradiction. \( \square \)

5. We show that \( P(S) \cap P(T) = P(S \cap T) \) by proving two facts: \( P(S) \cap P(T) \subseteq P(S \cap T) \) and \( P(S \cap T) \subseteq P(S) \cap P(T) \). For the first set inclusion, suppose \( A \in P(S) \cap P(T) \). Then \( A \in P(S) \) and \( A \in P(T) \), so \( A \subseteq S \) and \( A \subseteq T \). Since \( A \subseteq S \) and \( A \subseteq T \), if \( a \in A \), then \( a \in S \) and \( a \in T \). But then \( a \in S \cap T \). Therefore, for every \( a \in A \) we know that \( a \in S \cap T \), i.e., \( A \subseteq S \cap T \). Then, by the definition of the power set, \( A \in P(S \cap T) \). For the second inclusion, suppose \( A \in P(S \cap T) \). Then \( A \subseteq S \cap T \). For any \( a \in A \), \( a \in S \cap T \), so \( a \in S \) in particular. Therefore, \( A \subseteq S \), and we may conclude that \( A \in P(S) \). Similarly, \( A \in P(T) \). Combining these two facts, we may conclude that \( A \in P(S) \cap P(T) \). \( \square \)

6. Let \( m = \rho(a) \) and \( n = \rho(b) \). Then \( 2^m | a \), so \( a = 2^m k \) for some \( k \in \mathbb{Z} \). Similarly, \( b = 2^n l \) for some \( l \in \mathbb{Z} \). Then \( ab = 2^m 2^m k l = 2^{m+n} k l \), so \( 2^{m+n} | ab \). Now, suppose that \( 2^r | ab \), where \( r > m + n \). Then \( ab = 2^p \) for some \( p \in \mathbb{Z}^+ \). Writing \( ab = 2^{m+n} k l \) as before, we find
   \[
   2^{m+n} k l = 2^p 
   \]
   so that
   \[
   k l = 2^{-(m+n)} p. 
   \]
   Clearly, the right-hand side is even, since \( r > m + n \) implies that \( r - (m + n) \geq 1 \). We argue that \( k l \) is odd, which would be a contradiction. First of all, note that \( k \) is odd, because \( a = 2^m k \); if \( k \) were even,
then we could let \( k' = k/2 \) and write \( a = 2^{m+1}k' \), so that \( m \) would not be the largest natural number so that \( 2^m \) divides \( a \) (which is the definition of \( \rho(a) \)). Similarly, \( \ell \) is odd. Then we may write \( k = 2c+1 \) and \( \ell = 2d+1 \) for some \( c, d \in \mathbb{Z} \), and \( kl = (2c+1)(2d+1) = 2cd + 2c + 2d + 1 = 2(cd + c + d) + 1 = 2f + 1 \), where \( f = cd + c + d \). Therefore, \( kl \) is odd as well, and we have a contradiction.

Finally, we may conclude that \( 2^{m+n} \) is the largest power of 2 which divides \( ab \), so \( \rho(ab) = m + n = \rho(a) + \rho(b) \). □

7. Show that the following statements are equivalent for a set \( A \) and a natural number \( n \).

(a) \( |A| = n \).

(b) \( n \) is the smallest natural number so that, for all finite sets \( B \), \( |A \cap B| \leq n \).

(c) \( n \) is the largest natural number so that, if \( A \subset B \) and \( B \) is finite, then \( |B| > n \).

(d) For all finite sets \( B \), \( |A \cup B| + |A \cap B| = n + |B| \).

(a) \( \rightarrow \) (d): Here we use the statement of the inclusion-exclusion formula:

\[
|A \cup B| = |A| + |B| - |A \cap B|.
\]

Adding \( |A \cap B| \) to both sides and replacing \( |A| \) by \( n \) yields

\[
|A \cup B| + |A \cap B| = n + |B|.
\]

(d) \( \rightarrow \) (b): First, we show that \( |A \cap B| \leq n \) by applying (d). Subtracting \( |A \cup B| \) from both sides of the equation in (d) yields

\[
|A \cap B| = n + |B| - |A \cup B|.
\]

Since \( B \subseteq A \cup B \), we have \( |A \cup B| = |B| + |A - B| \geq |B| \), because \( B \) and \( A - B \) are disjoint and \( B \cup (A - B) = A \). Therefore, \( n + |B| - |A \cup B| \leq n \). Now, we need to show that the statement \( \forall \exists (|A \cap B| \leq m) \) does not hold for any \( m < n \). Suppose it did. Then we may take \( B = A \), so

\[
|A \cap A| = |A| = n \leq m,
\]

a contradiction.

(a) \( \rightarrow \) (c): Suppose it is true that \( |A| = n \). Let \( B \) be a finite set of which \( A \) is a proper subset. Then \( B = A \cup (B - A) \), and \( A \cap (B - A) = \emptyset \), so \( |B| = |A| + |B - A| \). Since \( B \not\subseteq A \), there is some \( b \in B \) so that \( b \not\in A \), i.e., \( b \in B - A \). Then \( |B - A| \geq 1 \), and we may conclude that \( |B| > |A| = n \). Now, suppose there were an \( m > n \) so that, for all finite \( B \) with \( A \subset B \), \( |B| > m \). Let \( x \) be any element not in \( A \). Then, if \( B = A \cup \{x\} \), \( m < |B| = |A| + 1 = n + 1 < m + 1 \). However, there is no integer strictly between \( m \) and \( m + 1 \), so we have a contradiction. Therefore, \( n \) is the largest integer so that, for all finite sets \( B \) with \( A \subset B \), \( |B| > n \).

(b) \( \rightarrow \) (a): Suppose it is true that, for all finite sets \( B \), \( |A \cap B| \leq n \), and \( n \) is the least natural number with this property. If we let \( B = A \), then \( |A \cap A| = |A| \leq n \). If \( n = 0 \), then \( |A| = 0 \). Therefore, we may assume that \( |A| \geq 1 \). Suppose \( |A| < n \). Then, for any set \( B \), \( |A \cap B| + |A - B| = |A| \leq n - 1 \), since \( (A \cap B) \cap (A - B) = \emptyset \) and \( (A \cap B) \cup (A - B) = A \). However, \( |A - B| \geq 0 \), so then \( |A \cap B| \leq n - 1 \), contradicting the fact that \( n \) is the least natural number so that \( |A \cap B| \leq n \) for all finite sets \( B \). We may conclude that \( |A| = n \).

(c) \( \rightarrow \) (a): Suppose it is true that, for all finite sets \( B \) with \( A \subset B \), \( |B| > n \), and \( n \) is the greatest integer with this property. If we let \( x \) be anything not an element of \( A \) and define \( B = A \cup \{x\} \), then \( A \subset B \), so \( |B| > n \). However, \( |B| = |A| + 1 \), so \( |A| + 1 > n \), or \( |A| \geq n \). On the other hand, suppose that \( |A| = m > n \). Then, for any finite \( B \) so that \( A \subset B \), \( |B| = |B - A| + |A| \geq |A| + 1 = m + 1 > n + 1 \). Therefore, \( n \) is not the largest integer so that, for any finite \( B \) with \( A \subset B \), \( |B| > n \) (since \( n + 1 \) has this property as well). This is a contradiction, and we may conclude that \( |A| = n \). □
8. We proceed by induction. First, the base case \( n = 1 \): \( \sum_{j=1}^{1} \frac{1}{j(j+1)} = 1/2 \), and \( 1 - 1/(1+1) = 1/2 \), so the base case holds. Now, the induction step. Suppose \( \sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1} \). Then

\[
\sum_{j=1}^{n+1} \frac{1}{j(j+1)} = \sum_{j=1}^{n} \frac{1}{j(j+1)} + \frac{1}{(n+1)(n+2)} = 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)}
\]

by the inductive hypothesis. Continuing the computation,

\[
\sum_{j=1}^{n+1} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1} \left( 1 - \frac{1}{n+2} \right) = 1 - \frac{1}{n+1} \cdot \frac{n+1}{n+2} = 1 - \frac{1}{n+2}.
\]

\(\Box\)

9. We define a map \( f \) from the set \( S \) of all polynomials with integer coefficients to \( \mathbb{N} \) which is one-to-one. Since \( f \) is onto its range \( f(S) \), and \( f(S) \subset \mathbb{N} \), \( f(S) \) is countable and \( S \) is in bijection with a countable set, making it countable itself (by the unproven assertion in the statement of the problem). Define \( f \) as follows. Suppose \( p = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \) for some integers \( a_0, \ldots, a_k \). Let \( w_j \) be the string representing \( |a_j| \) in binary. Let \( w^*_j \) be \( w_j \) with the symbol 2 prepended to it if \( a_j < 0 \), and the symbol 3 prepended to it if \( a_j \geq 0 \). Then the string

\[
w^*_k w^*_{k-1} \cdots w^*_0
\]

can be interpreted as an integer \( N \) in base 4. Since the entire sequence \( a_j, 0 \leq j \leq k \), can be recovered from \( N = f(p) \), \( f \) is one-to-one. Indeed, we may write \( N \) as a string \( z \) in base 4 and define \( z_j, 0 \leq j \leq m \), by choosing strings of 0’s and 1’s so that

\[
z = b_0 z_0 b_1 z_1 \cdots b_m z_m,
\]

where \( b_j \in \{2,3\} \) for \( 0 \leq j \leq m \). Then \( p \) is given by

\[
p = b_m + b_{m-1} x + b_{m-2} x^2 + \cdots + b_0 x^m.
\]

\(\Box\)