Solutions

1. Metalogic [10 pts] Consider the following proof tree:

\[ \begin{array}{c}
\ldots \vdash P \land Q \quad \text{assum} \\
\ldots \vdash Q \quad \land \text{elim} \\
\ldots \vdash P \rightarrow \neg Q \quad \text{assum} \\
\ldots \vdash \neg Q \quad \land \text{elim} \\
\ldots \vdash P \quad \text{assum} \\
\end{array} \]

(a) [2 pts] Identify the rule used in the step labeled (a) above:

Answer: \( \rightarrow \text{elimination} \).

(b) [2 pts] What should go in the portion of the tree labeled (b) above?

Answer: \[ \begin{array}{c}
\ldots \vdash P \land Q \vdash \neg (P \land Q) \quad \text{absurd} \\
\ldots \vdash (P \rightarrow \neg Q) \quad \land \text{elim} \\
\ldots \vdash (P \rightarrow \neg Q) \rightarrow \neg (P \land Q) \quad \rightarrow \text{intro} \\
\end{array} \]

(c) [6 pts] Convert the proof tree to an English proof

Answer:
Claim: if \( P \rightarrow \neg Q \) then “\( P \land Q \)” is false.
Proof: Assume \( P \rightarrow \neg Q \), and assume for the sake of contradiction that \( P \land Q \) is true.
Since \( P \land Q \) is true, we have \( P \) is true, so (since \( P \rightarrow \neg Q \)) we have \( Q \) is false. But we also have \( Q \) is true, since \( P \land Q \) was assumed. This is a contradiction, so our initial assumption of \( P \land Q \) must be false, as required.

2. Probability [15 pts] Event \( E \) is evidence in favor of event \( H \) if \( \Pr(H \mid E) > \Pr(H) \), and is evidence against \( H \) if \( \Pr(H \mid E) < \Pr(H) \). Prove that if \( E \) is evidence in favor of \( H \) then \( \neg E \) is evidence against \( H \). (You may assume that \( 0 < \Pr(E) < 1 \)).
Suppose that $E$ is evidence in favor of $H$. Then $Pr(H \mid E) > Pr(H)$.

We have

$$Pr(E \mid H) = \frac{Pr(H \mid E)Pr(E)}{Pr(H)} > \frac{Pr(H)Pr(E)}{Pr(H)} = Pr(E)$$

by Bayes’s rule.

Now, $Pr(E \mid H) = 1 - Pr(E \mid H) < 1 - Pr(E) = Pr(\overline{E})$.

We can apply Bayes’s rule again to get

$$Pr(H \mid \overline{E}) = Pr(\overline{E} \mid H)Pr(H)/Pr(\overline{E}) < Pr(\overline{E})Pr(H)/Pr(\overline{E}) = Pr(H)$$

Which shows that $\overline{E}$ is evidence against $H$, as required.

3. Probability [20 pts] In this question, we will randomly generate a bit string of length three (that is, a sequence of 0s and 1s of length 3). You may assume that each string is selected with probability 1/8.

(a) [4 pts] Give a reasonable sample space for this experiment.

Answer:

Let $S$ be the set of all length-three bit strings, i.e. $S = \{000, 001, 010, \ldots, 111\}$.

(b) [8 pts] Let $E$ be the event that the bit string contains an odd number of 1s, and let $F$ be the event that the bit string starts with a 1. Are $E$ and $F$ independent? If so, prove it; if not, explain why. (Make sure that you carefully define the events $E$ and $F$.)

Answer:

Let $E := \{001, 010, 100, 111\}$ and let $F := \{100, 101, 110, 111\}$.

We see that $Pr(E) = 4/8 = 1/2$, since all strings are equally likely. Similarly $Pr(F) = 1/2$.

We have $E \cap F = \{100, 111\}$, and $Pr(E \cap F) = 1/4 = Pr(E)Pr(F)$, so $E$ and $F$ are independent.

(c) [8 pts] Let $N$ be the random variables giving the number of 1’s in the string, and let $I_1$ be the random variable giving the the first bit of the string. Are $N$ and $I_1$ independent? If so, prove it; if not, explain why.
4. Probability [10 pts] Suppose we roll 8 fair six-sided dice independently and count the number of pairs showing the same value. Each die can be part of multiple pairs: for example, if we roll the same number 4 times it would count as 6 pairs.

(a) [3 pts] If we roll the same number $k$ times, how many pairs would we count for that number?

Answer: \( \binom{k}{2} \)

(b) [5 pts] Find the expected number of pairs rolled.

Answer:
Let $I_{ij}(s)$ give 1 if $s_i = s_j$. Then $N = \sum I_{ij}$ so $E(N) = \sum E(I_{ij})$.
Two dice will have the same value with probability $1/6$, so $E(I_{ij}) = 1 \cdot 1/6$.
There are $\binom{8}{2}$ possible pairs $i, j$, so there are $\binom{8}{2}$ terms in the sum, giving $E(N) = \binom{8}{2}/6 = 28/6 = 4.5$.

(c) [2 pts] Apply Markov’s inequality to give a bound on the probability that there are at least 12 pairs.

Answer:
\[ Pr(N \geq 12) \leq \frac{E(N)}{12} = \frac{9}{24}. \]

5. Combinatorics [10 pts] Give a combinatoric proof that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Answer:
We will show that both sides give the number of two-element subsets of $A$ where $A = \{0, 1, \ldots, n\}$.

For the left hand side, we can produce such a subset by first choosing the larger of the two elements (calling it $i$, with $0 \leq i \leq n$), and then choosing a smaller element $j$ with $0 \leq j < i$. Once $i$ is chosen, there are $i$ options for $j$, so the total number of options is the sum over $i$ of $i$, or the left hand side.

For the right hand side, we first select any element $i$ of $A$, and then we select any other element $j$ of $A$. There are $n + 1$ options for $i$, and $n$ options for $j$, giving a total of $n(n + 1)$ options. However, each output $\{i, j\}$ is counted twice, because $\{i, j\} = \{j, i\}$. Therefore, we use the quotient rule and divide by two.

We see that the number of two-element subsets of $A$ is $LHS$ and is also $RHS$, so we conclude that $LHS = RHS$.

6. Regular expressions [10 pts] Give an $\varepsilon$-NFA that recognizes $L((01 + 10)^*)$. 

7. **Induction** [20 pts] The Catalan numbers $C_i$ are defined inductively by the equations

\[ C_0 := 1 \text{ and } C_{n+1} := \sum_{i=0}^{n} C_i C_{n-i}. \]

Prove by induction that for all $n > 0$, $C_n \leq n^n$. Be sure to indicate which kind of induction you are using, where you use your inductive hypothesis, and which inductive hypothesis you use.

**Answer:**

We will prove this by strong induction on $n$. Let $P(n)$ be the statement “$C_n \leq n^n$”.

In the base case, we need to show $P(1)$, i.e. that $C_1 \leq 1^1$. We see that $C_1 = C_0 \cdot C_0 = 1 \leq 1 = 1^1$.

Now, assume $P(i)$ for all $i \leq n$; we wish to show $P(n+1)$. We have

\[
C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i} \quad \text{by definition}
\]

\[
\leq \sum_{i=0}^{n} i (n-i)^{n-i} \quad \text{by } P(i) \text{ and } P(n-i)
\]

\[
\leq \sum_{i=0}^{n} n^i n^{n-i} \quad \text{since } i \leq n \text{ and } n-i \leq n
\]

\[
= \sum_{i=0}^{n} n^n = n \cdot n^n = n^{n+1} \leq (n+1)^{n+1} \quad \text{algebra}
\]

as required.
8. Well-defined function [15 pts]

(a) [5 pts] Write down Euclid’s GCD algorithm:

**Answer:**

\[
gcd(a, 0) := a \text{ and } gcd(a, b) := gcd(b, r) \text{ where } r = \text{rem}(a, b).
\]

(b) [10 pts] Let \( g : \mathbb{Z}_m \to \mathbb{N} \) be given by \( g([a]_m) := gcd(a, m) \). Prove that \( g \) is well-defined.

**Answer:**

Suppose \([a] = [a']\). Then \( a = a' + km\). We want to show that \([gcd(a, m)] = [gcd(a', m)]\). We have

\[
gcd(a, m) = gcd(m, rem(a, m)) \quad \text{by definition of gcd}
\]

Since \([a] = [a']\) we have \(rem(a, m) = rem(a', m)\); thus \(gcd(a, m) = gcd(m, rem(a', m)) = gcd(a', m)\).

9. Sets of functions [20 pts] Recall that the PMF of a \( T \)-valued random variable \( X \) is the function \( PMF_X : T \to \mathbb{R} \) given by \( PMF_X(x) := Pr(X = x) \).

Now, consider the function \( PMF \) which, on input \( X \), outputs \( PMF_X \).

(a) [4 pts] Use the \([X \to Y]\) notation to give the domain and codomain of \( PMF \).

\[ PMF : [S \to T] \longrightarrow [T \to \mathbb{R}] \]

(b) [8 pts] Prove or disprove: \( PMF \) is injective.

**Answer:**

\( PMF \) is not injective. For example, consider a sample space \( S = \{H, T\} \) with \( Pr(\{H\}) = Pr(\{T\}) = 1/2 \). Let \( X(H) := 1 \) and \( X(T) := 0 \) and let \( Y(H) := 0 \) and \( Y(T) := 1 \).

Then \( PMF(X) = PMF(Y) \), since both of these are the function that map both 0 and 1 to 1/2. But \( X \neq Y \), so \( PMF \) is not injective.

(c) [8 pts] Prove or disprove: \( PMF \) is surjective.

**Answer:**

\( PMF \) is not surjective. For example, it never outputs the function \( f : S \to \mathbb{R} \) given by \( f(x) := 500 \).

10. Quantified statements [20 pts]

We say that \( x_0 \) is an infimum of \( X \) if \( \forall x \in X, x_0 \leq x \). We say that \( X \) is closed below if there is some \( x_0 \in X \) such that \( x_0 \) is an infimum of \( X \).
(a) [4 pts] Which of the following statements is equivalent to “$X$ is not closed below”?

- $\neg \exists x_0 \in X, \forall x \in X, x_0 \not\leq x$
- $\forall x_0 \in X, \exists x \not\in X, x_0 \not\leq x$
- $\forall x_0 \in X, \exists x \in X, x_0 \not\leq x \leftarrow $ correct solution
- $\forall x_0 \not\in X, \exists x \not\in X, x_0 \not\leq x$
- $\exists x \in X, \forall x_0 \in X, x_0 \not\leq x$

(b) [8 pts] Prove that if $X$ and $Y$ are closed below that $X \cup Y$ is closed below.

**Answer:**
Suppose $X$ and $Y$ are closed below. Then there exists infima $x_0 \in X$ and $y_0 \in Y$. Let $z_0$ be the smaller of the two. Then $z_0$ is an infimum of $X \cup Y$, since for any $z \in X \cup Y$, we have $z \in X$ or $z \in Y$; if $z \in X$ then $z_0 \leq x_0 < z$, and similarly if $z \in Y$.

Moreover, $z_0$ is either equal to $x_0$ or $y_0$, and is thus either in $X$ or in $Y$. In either case, $z_0 \in X \cup Y$, so $X \cup Y$ contains an infimum and is thus closed below.

(c) [8 pts] Disprove the following claim: if $X$ and $Y$ are closed below then $X \cap Y$ is closed below.

**Answer:**
Let $X = \{0\}$ and $Y = \{1\}$. Clearly both $X$ and $Y$ are bounded below. But $X \cap Y = \emptyset$, and there does not exist any element of $\emptyset$ (although any number would be an infimum of $\emptyset$, $\emptyset$ does not contain any numbers). Thus $\emptyset$ is not bounded below.