Solutions - Homework 1
CS611 Theory of Computation

Problem 1. [Category: Proof] Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1$, 2, and 3.)
We will use induction to prove the above statement:

1. Formulate the problem in terms of proposition $P(n)$;
2. Prove the base case, $P(4)$ is true;
3. Write the induction hypothesis;
4. Prove that $P(k+1)$ is true assuming the induction hypothesis is true.

Solution:

1. Let $P(n)$ be the proposition that $2^n < n!$.
2. **Base Case:** To prove the inequality for $n \geq 4$ requires that the base case be $P(4)$. Note that $P(4)$ is true, because $2^4 = 16 < 24 = 4!$.
3. **Induction Hypothesis:** We assume that $P(k)$ is true for an arbitrary integer k with $k \geq 4$. That is, we assume that $2^k < k!$ for the positive integer k with $k \geq 4$.
4. **Inductive Step:** For the inductive step, we must show that under the induction hypothesis, $P(k+1)$ is also true. That is, we must show that if $2^k < k!$ for an arbitrary positive integer k where $k \geq 4$, then $2^{k+1} < (k+1)!$. We have

$$\begin{aligned}
2^{k+1} &= 2 \cdot 2^k && \text{by definition of exponent} \\
&< 2 \cdot k! && \text{by the inductive hypothesis} \\
&< (k+1) \cdot k! && \text{because} 2 < k+1 \\
&= (k+1)! && \text{by definition of factorial function.}
\end{aligned}$$

This show that $P(k+1)$ is true when $P(k)$ is true. This complete this inductive step of the proof.

We have completed the proof with induction. Hence, by induction, $P(n)$ is true for all integers n with $n \geq 4$. That is, we have proved that $2^n < n!$ is true for all integers n with $n \geq 4$.

■

Problem 2. [Category: Proof] Show that if n is an integer greater than 1, then n can be written as the product of primes.
We will use strong induction to prove the above statement:

1. Formulate the problem in terms of proposition $P(n)$;

2. Prove the base case, $P(2)$ is true;
3. Write the strong induction hypothesis;
4. Prove that $P(k+1)$ is true assuming the induction hypothesis is true.

Solution:

1. Let $P(n)$ be the proposition that n can be written as the product of primes.
2. **Base Case:** $P(2)$ is true because 2 can be written as the product of one prime, itself. (Note that $P(2)$ is the first case we need to establish.)
3. **Induction Hypothesis:** The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k.
4. **Inductive Step:** To complete the inductive step, it must be shown that $P(k+1)$ is true under the induction hypothesis, that is, $k+1$ is the product of primes.

   There are two cases to consider, namely, when $k+1$ is prime and when $k+1$ is composite. If $k+1$ is prime, we immediately see that $P(k+1)$ is true. Otherwise, $k+1$ is composite and can be written as product of two positive integers a and b with $2 \leq a \leq b < k+1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k+1$ is composite, it can be written as the the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

We have complete the proof. Hence, by strong induction $P(n)$ is true for all integers n greater than 1. That is, n can be written as the product of primes if n is an integer greater than 1.

$\blacksquare$

Problem 3. [Category: Comprehensive] Let $A = \{1, 2, 3, 4, 5\}$, $R \subseteq A \times A$ be the relation $\{(a, b) | a - b$ is a multiple of $2\}$.

1. Show that R is an equivalence relation. Recall that R is an equivalence relation if it is reflexive ($\forall a \in A, (a, a) \in R$), symmetric ($\forall a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$), and transitive ($\forall a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$).
2. Given $a \in A$, let $[a]\_R$, called an equivalence class, be the set of all elements related to a through R, that is, $[a]\_R = \{b | (a, b) \in R\}$. What is $[1]\_R, [2]\_R, [3]\_R, [4]\_R, [5]\_R$?
3. How many distinct equivalence classes are there for R?
4. If A is the set of all natural numbers and R is defined as above, then how many distinct equivalence classes does it have?

Solution: To answer these questions, we first write down what $A \times A$ is (omit here). Then according to the definition, $R = \{(1, 1), (1, 3), (1, 5), (2, 2), (2, 4), (3, 1), (3, 3), (3, 5), (4, 2), (4, 4), (5, 1), (5, 3), (5, 5)\}$.

1. To show that R is an equivalence relation on A, we need to show that R satisfies three properties according to equivalence relation definition.

- Reflexive: For this property, it's trivial. Since $a - a = 0 = 2 \cdot 0$, is a multiple of 2, then $(a, a) \in R$ for all $a \in A$, hence, R satisfies this property.
- Symmetric: For this property, we need to show that for $\forall a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$. If $(a, b) \in R$ then $a - b = i = 2k$ is a multiple of 2 where k is an integer, then $b - a = -i = 2(-k)$, the negation of i is also a multiple of 2. Hence, $(b, a) \in R$.
- Transitive: For this property, we need to show that for $\forall a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. If $(a, b) \in R$ and $(b, c) \in R$, then $a-b = i = 2k$ and $b-c = j = 2k'$, i and j both are numbers of multiples of 2. Then it follows that $a-c = (a-b)+(b-c) = i+j = 2k+2k' = 2(k+k')$ is still a multiple of 2. Hence, $(a, c) \in R$.

We have proved that R satisfies these three properties, that is R is an equivalence relation according to definition.

2. $[1]\_R$ is the set of b related to 1, that is $\{b|(1, b) \in R\}$. Hence, $[1]\_R = \{1, 3, 5\}$. Similarly, $[2]\_R = \{2, 4\}$, $[3]\_R = \{1, 3, 5\}$, $[4]\_R = \{2, 4\}$, $[5]\_R = \{1, 3, 5\}$.
3. As we can see in the previous answer, there are two distinct equivalence classes for R, which are $\{1, 3, 5\}$, $\{2, 4\}$.
4. If A is the set of all natural numbers with same R defined, then there are still two distinct equivalence classed for R. We can write these two classes as $even = \{2k|k \in N\}$, and another one as $odd = \{2k + 1|k \in N\}$, where N is natural numbers set.

■