期中之前

2019年4月22日 22:53

- A.1-Q.9 (b) If P is of any length, using any of the logical connectives $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$, prove that P is logically equivalent to a proposition of the form $A \square B$, where $\square$ is one of $\wedge, \vee, \leftrightarrow$, and A and B are chosen from $\{p, \neg p, q, \neg q\}$.

  Proof. If $A \in \{p, \neg p\}$, $B \in \{q, \neg q\}$, and $\square \in \{\wedge, \vee, \leftrightarrow\}$, then $A \square B$ has $2 \times 2 \times 3 = 12$ different possible forms. Together with $p \vee p \equiv p$, $p \vee \neg p \equiv T$, $q \vee q \equiv q$, $p \wedge \neg p \equiv F$, we will have the $2^4 = 16$ different forms by $A \square B$. This proves the statement.

- A.2-Q.15 Show that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}$, and a_n are real numbers and $a_n \neq 0$, then $f(x)$ is $\Theta(x^n)$.

  Proof. For the other direction, let k be chosen larger than 1 and larger than $2nm/|a_n|$, where m is the largest of the absolute values of the a_i's for $i < n$. Then each a_{n-i}/x^i will be smaller than $|a_n|/2n$ in absolute value for all $x > k$. Now we have for all $x > k$,

$$
\begin{aligned}
|f(x)| &= |a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0| \\
&= x^n \left| a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n} \right| \\
&\geq x^n |a_n/2|.
\end{aligned}
$$

- A.2-Q.16 Show that $n \log n$ is $O(\log n!)$.

  Proof. Note that $(n-i)(i+1) \geq n$ for $i = 0, 1, \ldots, n-1$. Hence, we have

  $$(n!)^2 = (n \cdot 1) \cdot ((n-1) \cdot 2) \cdot ((n-1) \cdot 3) \cdot \cdots \cdot (2 \cdot (n-1)) \cdot (1 \cdot n) \geq n^n.$$

  Therefore, $2 \log n! \geq n \log n$.

- A.3-Q.10 Prove that if m is a positive integer of the form $4k+3$ for some non-negative integer k, then m is not the sum of the squares of two integers.

  Proof. We first show the following lemma.
  Lemma: If n is an integer, then $n^2 \equiv 0 \text{ or } 1 \pmod 4$.
  Assume that $m = a^2 + b^2$ for two integers a and b. By the Lemma above, we know that $a^2, b^2 \equiv 0 \text{ or } 1 \pmod 4$. Thus, $m = a^2 + b^2 \equiv 0 \text{ or } 1 \text{ or } 2 \pmod 4$. But $4k + 3 \equiv 3 \pmod 4$, which leads to a contradiction.

- A.3-Q.14 Prove that there are infinitely many primes of the form $4k + 3$, where k is a nonnegative integer.

  Proof. Suppose that there are only finitely many primes of the form $4k + 3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.
  Let $Q = 4q_1q_2 \cdots q_n - 1$. Note that Q is of the form $4k + 3$ (where $k = q_1q_2 \cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed.
  If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k + 1$ or of the form $4k + 3$, and the product of primes of the form $4k + 1$ is also of this form (because $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$), there must be a factor of Q of the form $4k + 3$ different from the primes we listed.