The Theory of Computation

Bernard M.E. Moret

Addison-Wesley-Longman, 1998

Solution Manual
Chapter 7, Additional Problem 10

Membership in NP is obvious, since multiplication can be done in time polynomial in the length of the numbers to be multiplied.

We prove the problem NP-complete by transforming *Positive NAE3SAT* to it. The idea is to use prime encoding for truth values, using one prime for each variable. Thus, if the variables of *Positive NAE3SAT* are $x_1, \ldots, x_n$, we use prime numbers $p_1, p_2, \ldots, p_n$, where p_i corresponds to $x_i =$ true. Since $p_n \in O(n^2)$ and since we can test a number k for primality in $O(\sqrt{k} \log k)$ time, we can obtain these n primes in polynomial time. Denote the product of all n primes by P; i.e., $P = \prod_{i=1}^{n} p_i$. Let the clauses of *Positive NAE3SAT* be $c_1, \ldots, c_m$; the $\{a_i\}$ sequence consists of $3m$ numbers and the $\{b_j\}$ sequence of $4m - 1$ numbers. For clause $c_k = \{x_{k_1}, x_{k_2}, x_{k_3}\}$, let product P_k be defined by $P_k = P/(p_{k_1} p_{k_2} p_{k_3})$. For each clause c_k, we place numbers $p_{k_1} P_k$, $p_{k_2} P_k$, and $p_{k_3} P_k$ in the $\{b_j\}$ sequence and numbers $p_{k_1} p_{k_2} P_k$, $p_{k_1} p_{k_3} P_k$, and $p_{k_2} p_{k_3} P_k$ in the $\{a_i\}$ sequence. Verify that, if c has none of the factors p_{k_1}, p_{k_2}, or p_{k_3}, or has all three of them, then it divides the same proportion on both sides (all 3 in absence, none in presence of the 3 primes), whereas it divides one more a_i value than b_j value in cases where it has one or two of the factors. Finally, we place $m - 1$ copies of P in the b_j sequence. Any certificate c always divides P. Hence, for a certificate to divide more numbers in the a_i series than in the b_j series, it must make up that difference of $m - 1$, plus one: hence it must gain m over the first $3m$ elements. But we have observed that it can gain at most one per clause, and that only when the clause is satisfied in *NAE3SAT* mode; hence all clauses must be satisfied. (There are as many ways of solving this as there are people to write proofs; one can start from any of the *SAT* variations and derive a simple proof.)