

**Problem 7.34.** Recall, in our discussion of the Church–Turing thesis, that we introduced the language  $D = \{\langle p \rangle \mid p \text{ is a polynomial in several variables having an integral root}\}$ . We stated, but didn't prove, that  $D$  is undecidable. In this problem, you are to prove a different property of  $D$ —namely, that  $D$  is NP-hard. A problem is **NP-hard** if all problems in NP are polynomial time reducible to it, even though it may not be in NP itself. So you must show that all problems in NP are polynomial time reducible to  $D$ .

*Proof.* To prove that  $D$  is NP-hard, we show that 3SAT is polynomial time reducible to  $D$ . The reduction converts a Boolean formula  $\phi$  in 3CNF into a polynomial  $p$  in several variables, so that  $\phi$  is satisfiable, iff  $p$  has an integral root.

Let  $\phi$  be any Boolean formula in 3CNF containing  $m$  clauses:

$$\phi = (a_1 \vee b_1 \vee c_1) \wedge (a_2 \vee b_2 \vee c_2) \wedge \cdots \wedge (a_m \vee b_m \vee c_m).$$

where each  $a$ ,  $b$  and  $c$  is a literal  $x_i$  or  $\overline{x_i}$ , and  $x_1, x_2 \dots x_n$  are the  $n$  variables of  $\phi$ . Now we show how to convert  $\phi$  to  $p$ .

We represent each variable  $x_i$  in  $\phi$  with a variable  $y_i$  in  $p$ . We represent each clause of  $\phi$  with a term in  $p$  as follows. Let  $C_i$  be any clause having literals  $a_i$ ,  $b_i$  and  $c_i$ . The term for the clause  $C_i$  is a product of three factors, one for each literal. If a literal is  $x_i$ , then the factor is  $y_i$ . Otherwise,  $(1 - y_i)$ . Finally, the sum of all terms in  $p$  is 0.

For example, if

$$\phi = (x_1 \vee x_1 \vee x_1) \wedge (\overline{x_1} \vee \overline{x_1} \vee \overline{x_1}),$$

then  $p$  is

$$[y_1 \cdot y_1 \cdot y_1] + [(1 - y_1) \cdot (1 - y_1) \cdot (1 - y_1)] = 0.$$

Suppose  $\phi$  has a satisfiable assignment. Then, at least one literal in every clause must be true. If variable  $x_i$  is assigned true (false) value, then set  $y_i = 0$  (1). Therefore, at least one factor in every term must be 0.

Suppose  $p$  has an integral root. Then, the values assigned to each variable give a satisfying assignment for  $\phi$ . If some variable  $y_i$  is assigned 0, then assign true value to  $x_i$ . Otherwise, false.

□