Model Solution Homework

Saskia van den Hoeven

Exercise 1

Prove that the class of Diophantine relations is closed under unbounded existential quantification, logical 'and', logical 'or', and bounded existential quantification.

Answer of exercise 1

Let R be an $(n+1)$-ary Diophantine relation. Then by definition $R(a_1,\ldots,a_n,y) \Leftrightarrow \exists x_1,\ldots,x_m(D(x_1,\ldots,x_m,a_1,\ldots,a_n,y)=0)$. Consider the relation $S(a_1,\ldots,a_n)$ defined by $S(a_1,\ldots,a_n) \Leftrightarrow \exists y R(a_1,\ldots,a_n,y)$. Then

$$\begin{aligned} S(a_1,\ldots,a_n) &\Leftrightarrow \exists y \exists x_1,\ldots,x_m(D(x_1,\ldots,x_m,a_1,\ldots,a_n,y)=0) \\ &\Leftrightarrow \exists x_1,\ldots,x_m,y(D(x_1,\ldots,x_m,a_1,\ldots,a_n,y)=0) \end{aligned}$$

hence S is a Diophantine relation.

Suppose R_1 and R_2 are both Diophantine relations. Then by definition

$$\begin{aligned} R_1(a_1,\ldots,a_n) &\Leftrightarrow \exists x_1,\ldots,x_k D_1(a_1,\ldots,a_n,x_1,\ldots,x_k)=0 \\ R_2(a_1,\ldots,a_n) &\Leftrightarrow \exists x_1,\ldots,x_l D_2(a_1,\ldots,a_n,x_1,\ldots,x_l)=0. \end{aligned}$$

Define $S_1 = R_1 \wedge R_2$ and $S_2 = R_1 \vee R_2$.

Consider the polynomial $P_1(a_1,\ldots,a_n,x_1,\ldots,x_{k+l}) = D_1^2(a_1,\ldots,a_n,x_1,\ldots,x_k) + D_2^2(a_1,\ldots,a_n,x_{k+1},\ldots,x_{k+l})$. Then

$$\begin{gathered} S_1(a_1,\ldots,a_n) \Leftrightarrow R_1(a_1,\ldots,a_n) \wedge R_2(a_1,\ldots,a_n) \\ \Leftrightarrow \exists x_1,\ldots,x_k D_1(a_1,\ldots,a_n,x_1,\ldots,x_k)=0 \text{ and } \exists x_1,\ldots,x_l D_2(a_1,\ldots,a_n,x_1,\ldots,x_l)=0 \\ \Leftrightarrow \exists x_1,\ldots,x_{k+l} P_1(a_1,\ldots,a_n,x_1,\ldots,x_{k+l})=0. \end{gathered}$$

Thus S_1 is a Diophantine relation.

Consider the polynomial $P_2(a_1,\ldots,a_n,x_1,\ldots,x_{k+l}) = D_1(a_1,\ldots,a_n,x_1,\ldots,x_k)\cdot D_2(a_1,\ldots,a_n,x_{k+1},\ldots,x_{k+l})$. Then

$$\begin{gathered} S_2(a_1,\ldots,a_n) \Leftrightarrow R_1(a_1,\ldots,a_n) \vee R_2(a_1,\ldots,a_n) \\ \Leftrightarrow \exists x_1,\ldots,x_k D_1(a_1,\ldots,a_n,x_1,\ldots,x_k)=0 \text{ or } \exists x_1,\ldots,x_l D_2(a_1,\ldots,a_n,x_1,\ldots,x_l)=0 \\ \Leftrightarrow \exists x_1,\ldots,x_{k+l} P_2(a_1,\ldots,a_n,x_1,\ldots,x_{k+l})=0. \end{gathered}$$

Thus S_2 is a Diophantine relation.

The relation $<$ is Diophantine, since $x < y \Leftrightarrow \exists z(x + z + 1 = y)$. Let R be an $(n+1)$-ary Diophantine relation. Consider the relation $S(a_1, \ldots, a_n)$ defined by $S(a_1, \ldots, a_n) \Leftrightarrow \exists y < t(R(a_1, \ldots, a_n, y))$ for any $t \in \mathbb{N}$. Then

$$\begin{aligned} S(a_1, \ldots, a_n) &\Leftrightarrow \exists y < t(R(a_1, \ldots, a_n, y)) \\ &\Leftrightarrow \exists y(y < t \wedge R(a_1, \ldots, a_n, y)). \end{aligned}$$

Since the set of Diophantine relations is closed under conjunction, S is a Diophantine set.

For each of these problems: recognizing what needs to be done yields one point, carrying it out yields one point.

Exercise 2

Show that a set of natural numbers is Diophantine if and only if it is the set of all natural number values assumed by some polynomial with integer coefficients for natural number values of its variables. In light of this, using Davis's conjecture, what can you say about the set of prime numbers?

Answer of exercise 2

Let M be a Diophantine set of natural numbers. Then

$$a \in M \Leftrightarrow \exists x_1, \ldots, x_k D(a, x_1, \ldots, x_k) = 0.$$

The equation

$$D(a, x_1, \ldots, x_k) = 0$$

has a solution in unknowns $x_1, \ldots, x_k$ if and only if the equation

$$(x_0 + 1)(1 - D^2(x_0, \ldots, x_k)) - 1 = a$$

has a solution in unknowns $x_0, \ldots, x_k$. (2,5 points)

In fact, if we have a solution of the first equation it can be expanded to a solution of the second equation by putting $x_0 = a$. Also, if we have a solution of the second equation, the factor $1 - D^2(x_0, \ldots, x_m)$ must be positive, which is possible only if $D(x_0, \ldots, x_m) = 0$ holds. But that implies that $x_0 = a$ and hence that the first equation also holds. (2,5 points)

Now let M be the set of all natural number values assumed by some polynomial $D(x_1, \ldots, x_k)$. Then $n \in M \Leftrightarrow \exists x_1, \ldots, x_k(D(x_1, \ldots, x_k) = n) \Leftrightarrow \exists x_1, \ldots, x_k(D(x_1, \ldots, x_k) - n = 0)$. Hence M is Diophantine. (1,5 points)

The set of all primes is easily seen to be listable. By Davis' Conjecture, it is then Diophantine. This implies the existence of a polynomial such that the set of all its non-negative values is exactly the set of all prime numbers. (1,5 points)