Homework 2

Metamathematics II

Math 503, Spring 2006
Solutions.

1. By computation one first shows that
   (a) $\mathrm{Cantor}(a, b+1) = \mathrm{Cantor}(a, b) + a + b + 1$,
   (b) $\mathrm{Cantor}(a+1, b) = \mathrm{Cantor}(a, b) + a + b + 2$
   for all $a, b \in \mathbb{N}$. Now fix a number $n \in \mathbb{N}$, and consider the diagonal $D_n := \{(a, b) \in \mathbb{N}^2 : a + b = n\}$. The set D_n has $n + 1$ elements. We now show by induction on n that
   $$\mathrm{Cantor}(D_n) = \left\{\frac{n(n+1)}{2}, \dots, \frac{(n+1)(n+2)}{2} - 1\right\}.$$
   This will establish that Cantor is a bijection. By (a) and (b) we have $\mathrm{Cantor}(a+1, b) = \mathrm{Cantor}(a, b+1) + 1$
2. Show that if $m, n \in \mathbb{N}$ satisfy $n \geqslant (m+1)^{m+2}$, then $m! = n^m \operatorname{div} \binom{n}{m}$.
3. Let $(a_1, \dots, a_n) \in \mathbb{N}^n$, $n > 0$, and $b \in \mathbb{N}$, $b \geqslant 3$, with $a_i < b$ for $i = 1, \dots, n$, and let a be the cipher of the tuple $(a_1, \dots, a_n)$ to the base b. Define the b tuples
   $$(d_{01}, \dots, d_{0n}), \dots, (d_{b-1,1}, \dots, d_{b-1,n}) \in \mathbb{N}^n$$
   as follows: for $k = 0, \dots, b-1$ and $j = 1, \dots n$ let $d_{kj} = 0$ if $k \neq a_j$ and $d_{kj} = 1$ otherwise. Show that if $d_0, \dots, d_{b-1} \in \mathbb{N}$ satisfy
   $$\begin{cases} a = 0 \cdot d_0 + 1 \cdot d_1 + \cdots + (b-1) \cdot d_{b-1} \\ d_0 + \cdots + d_{b-1} = \mathrm{Repeat}(1, b, c) \\ \mathrm{Orthnorm}(d_k, d_l, b, c) \text{ for } 1 \leqslant k < l < b \end{cases}$$
   then $d_0, \dots, d_{b-1}$ are the ciphers of the tuples $(d_{01}, \dots, d_{0n}), \dots, (d_{b-1,1}, \dots, d_{b-1,n})$ to the base b, respectively.

In the next two exercises we discuss some algorithmically *solvable* diophantine problems. We let $n \in \mathbb{N}$, and by convention $\mathbb{N}^0 := \{0\}$.

4. Let us call a subset S of $\mathbb{N}^n$ **polynomial** if there is a polynomial $P \in \mathbb{Z}[u_1, \dots, u_n]$ such that
   $$S = \big\{(a_1, \dots, a_n) \in \mathbb{N}^n : P(a_1, \dots, a_n) = 0\big\}.$$
   (a) Show that the class of polynomial subsets of $\mathbb{N}^n$ is closed under universal quantification, i.e., if $S \subseteq \mathbb{N}^{n+1}$ is polynomial then so is
   $$S' := \big\{(a_1, \dots, a_n) \in \mathbb{N}^n : \forall b \in \mathbb{N}\big((a_1, \dots, a_n, b) \in S\big)\big\}.$$
   (b) Use (a) to show that there is an algorithm which decides, for given $P, Q \in \mathbb{Z}[u_1, \dots, u_n]$, whether $P(a_1, \dots, a_n) = Q(a_1, \dots, a_n)$ for all $(a_1, \dots, a_n) \in \mathbb{N}^n$.
5. Let $P(u_1, \dots, u_n, x) \in \mathbb{Z}[u_1, \dots, u_n, x]$, and consider the diophantine set
   $$S = \big\{(a_1, \dots, a_n) \in \mathbb{N}^n : \exists x(P(a_1, \dots, a_n, x) = 0)\big\}.$$

(a) Show that S is decidable by giving an informal algorithm which, for a given n-tuple $(a_1, \ldots, a_n) \in \mathbb{N}^n$ decides whether it belongs to S or not. (It is unknown whether the same result holds if P is replaced by a polynomial in $\mathbb{Z}[u_1, \ldots, u_n, x_1, x_2]$ and S by the analogously defined diophantine subset of $\mathbb{N}^n$.)

(b) Conclude that $\mathbb{N}^n \setminus S$ is diophantine.