Undecidability exercises
Problem set

Summer 2012

1. Look up what *Richard's paradox* is.

2. Recall the meaning of the quantifiers *for all* $\forall$ and *there exists* $\exists$ as well as the Boolean operators *and* $\wedge$ and *or* $\vee$. Let $a, b, c, x, y \in \mathbb{N}$. What is the meaning of the following statements?

   a) $\forall a \exists b \forall x, y \big(b > a \wedge (x, y > 1 \implies xy \neq b)\big)$

   b) $\forall a \exists b \forall x, y \big(b > a \wedge (x, y > 1 \implies (xy \neq b \wedge xy \neq b + 2))\big)$

   c) $\forall a \exists b, c, x, y (a = b^2 + c^2 + x^2 + y^2)$

   Formulate Fermat's last theorem and Goldbach's conjecture in a similar way.

3. Define a function $f : \mathbb{N} \to \{0, 1\}$ by $f(x) := 0$ if statement b) above is false and $f(x) := 1$ if it is true. Can you write an algorithm which computes the function? Can you prove or disprove that $f(1) = 1$?

4. What is the largest natural number for which you can give a precise mathematical definition and explain it in, say 20 seconds, to your fellow student? (Remember that ∞ is not a natural number and something like in Berry's paradox doesn't work)

5. Compute $BB(1)$, i.e., the value of the busy beaver function for n=1.

6. Show that the cardinality of the set of algebraic numbers does not contradict the continuum hypothesis.

7. Decide whether or not the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(x, y) = |x - y|$ is primitive recursive.

8. Prove that the predicates $x \geq y$ and $x \neq y$ are primitive recursive.

9. Identify the function $Cn[Pr[Cn[s, z], Cn[prod, id^3_3, Cn[s, id^3_2]]], id^1_1, id^1_1]$

10. Prove that for any rational number $x \in [0,1)$ with decimal expansion $x = 0.x_0x_1x_2\ldots$ there is a primitive recursive function $f : \mathbb{N} \to \mathbb{N}$ such that $f(n) = x_n$ for all $n \in \mathbb{N}$ (Hint: think about a characteristic property of rational numbers regarding their decimal expansion).

11. A primitive recursive function similar to that in the preceding exercise exists not only for rational numbers; explicit representations are known for various roots, $\pi/4$, $e/3$, etc. Can there be a real number $x \in [0,1)$ for which no such primitive recursive function exists? Why?

12. Primitive recursive functions are dominated by the Ackermann-Péter function, i.e. for any such function $f : \mathbb{N}^m \to \mathbb{N}$ there exists $x \in \mathbb{N}$ such that $\forall z = (z_1, \ldots, z_m) \in \mathbb{N}^m : f(z) < A(x, \max\{z_1, \ldots, z_m\})$. Find the smallest possible such x for the following primitive recursive functions:

    a) $add = Pr[id^1_1, Cn[s, id^3_3]] : \mathbb{N}^2 \to \mathbb{N}$; $add(z_1, z_2) = z_1 + z_2$

    b) $prod = Pr[z, Cn[add, id^3_1, id^3_3]] : \mathbb{N}^2 \to \mathbb{N}$; $prod(z_1, z_2) = z_1 \cdot z_2$

    c) $pow = Pr[Cn[s, z], Cn[prod, id^3_1, id^3_3]] : \mathbb{N}^2 \to \mathbb{N}$; $pow(z_1, z_2) = {z_1}^{z_2}$

13. Knuth's up-arrow operation is defined on triples of natural numbers by its following properties:

$$\begin{aligned} a \uparrow^0 b &= a \cdot b \\ a \uparrow^n b &= \underbrace{a \uparrow^{n-1} (a \uparrow^{n-1} (\cdots a \uparrow^{n-1} a \cdots))}_{b \text{ copies of } a} \end{aligned}$$

    Show that for $x \geq 2$ the Ackermann-Péter function can be expressed as

$$A(x, y) = 2 \uparrow^{x-2} (y + 3) - 3$$

14. We have seen that the Ackermann-Péter function is not primitive recursive. Prove that for any natural number x the function $A_x : \mathbb{N} \to \mathbb{N}$ defined by $A_x(n) = A(x, n)$ is primitive recursive.

15. Let $G : \mathbb{N} \to \{0, 1\}$ be the predicate which gives 1 if every even integer greater than 2 but smaller than N can be written as the sum of two primes. Show that there exists a finite number N^* such that $G(N^*) = 1 \implies (\forall N \in \mathbb{N} : G(N) = 1)$, i.e. the former equality implies Goldbach's conjecture. (Hint: argue that there is a Turing machine (with finitely many states) which computes G, conclude that there exists a Turing machine which halts iff Goldbach's conjecture is false and returns the smallest counterexample. Now use the busy beaver function. Remark: it might be easier to think in terms of computer programs written in any programming language. You may use the fact that any function computable in this sense is also computable with a Turing machine with finitely many states.)

16. Can you write a program (using your favourite programming language) which prints its own source code?

17. Prove that for any recursive function $f : \mathbb{N}^2 \to \mathbb{N}$ there exists an $m \in \mathbb{N}$ such that $F_m(y) = f(m, y)$ for all y. (Use the s-m-n theorem and the recursion theorem.)

18. Using the result of the previous problem, show that there in an $n \in \mathbb{N}$ so that $F_n(x) = n$ for all x.

19. Use the recursion theorem to show that the Ackermann functon is recursive. (Hint: define a three-argument function by cases which mimics the defining relations of the Ackermann function, e.g. set $g(n, x+1, y+1) := F(n, x, F(n, x+1, y))$, $g(n, x+1, 0) := F(n, x, 1)$, $g(n, 0, y) := y + 1$.)

20. Show that there is a $y \in \mathbb{N}$ such that the set $S := \{x | F_y(x) \text{ undefined}\}$ is not recursive.

21. Show that if two sets are recursive, then their intersection and union are recursive sets as well.

22. Let A and B be subsets of $\mathbb{N}$. Construct a set $C \subseteq \mathbb{N}$ which is recursive iff both A and B are.

23. Is the following set $S_7 \subset \mathbb{N}$ recursively enumerable? $S_7 := \{x | F_x(7) \text{ undefined}\}$

24. Regard the function f_1 defined in a previous lecture as the characteristic function of a set. Is this set recursively enumerable? ($f_1 : \mathbb{N} \to \{0, 1\}$ was defined as $f_1(x) = 1$ iff exactly x consecutive ones occur somewhere in the binary expansion of π and $f_1(x) = 0$ otherwise.)

25. In the lecture two types of "halting problems" for a universal TM appeared. They ask whether or not (depending on the input) (i) the TM halts or (ii) the TM halts in a standard configuration. Argue, possibly employing the Church-Turing thesis, that undecidability of (ii) implies undecidability of (i).

26. For words $w = a_1 \dots a_m$ over the alphabet $A = \{1, 2, 3\}$ define a map $W(w) = \sum_{k=1}^{m} a_k 4^{m-k}$ from A^* to $\mathbb{N}$. Denote by $|w|$ the length of a word and define a map from $A^* \times A^*$ into the set of 3×3 integer matrices by

$$M(u, w) := \begin{pmatrix} 4^{|u|} & 0 & 0 \\ 0 & 4^{|w|} & 0 \\ W(u) & W(w) & 1 \end{pmatrix}.$$

Prove that $(u, w) \mapsto M(u, w)$ is a monoid monomorphism if we use concatenation of words and matrix multiplication as binary operations in the domain and codomain respectively.

27. We will now approach Hilberts 10th problem. Let P be the set of all multivariate polynomials in $x_1, x_2, \ldots$ with integer coefficients (i.e., including objects like $x_1^3 - 13x_1x_2 - x_3^5$).

    a) assume there is an oracle capable of deciding whether or not any element $p \in P$ has an integral root, i.e., a solution of $p(x)$ for which $x \in \mathbb{Z}^n$ where n is the number of variables of p. Show that by using the oracle we can decide whether or not there is a non-negative integral root, i.e., $0 \in p(\mathbb{N}^n)$.

    b) show the same as in a) but the other way round: assuming the oracle can deal with non-negative integral roots, provide a method for deciding the existence of an integral root.

    c) assume were interested in the existence of an integral root for the subset of P which contains only polynomials for which the degree, the number of variables and the absolute value of the coefficients are all bounded by 42. Is this problem recursively decidable?

28. For any polynomial $p(x_1, \ldots, x_n)$ with integer coefficients let $N(p)$ be the cardinal number of the subset $\{x \in \mathbb{N}^n | p(x) = 0\}$. Call a set of cardinal numbers $\leq \aleph_0$ non-trivial if it is neither empty nor does it contain all such cardinal numbers. Prove that for any given non-trivial set C of cardinal numbers $\leq \aleph_0$ there cannot be any algorithm which decides whether or not $N(p) \in C$ for any polynomial with integer coefficients. (Hint: note that $C = \{0\}$ is Hilberts tenth problem. Consider the following three further cases and reduce them to this known one: (i) $0, \aleph_0 \in C$, (ii) $0 \in C, \aleph_0 \notin C$, (iii) $0 \notin C$.)

29. In the lecture we proved that the class of diophantine sets (in $\mathbb{N}^k$, say) is closed under unions and intersections. Can you show that it is closed under taking complements?

30. Specify a subset of $\mathbb{N}$ which is not diophantine.