Seminar H10: exercises week 2

Model solutions (Nils Donselaar)

October 11, 2013

Exercise 1

For natural numbers $k$, let $S_k$ be the sequence of digits $k(k-1)...10$. Give an exponential Diophantine equation $E_L(a, b) = E_R(a, b)$ such that we have $\forall k \exists x E_L(x, k) = E_R(x, k)$ and $\forall x \forall k (E_L(x, k) = E_R(x, k) \rightarrow \exists b(\tilde{x}(b) = S_k))$, where $\tilde{x}(b)$ denotes the digit representation of $x$ relative to base $b$. Does this yield an exponential Diophantine representation of the relation $R(x, k) :\iff \exists b(\tilde{x}(b) = S_k)$? (4 + 1 pts.)

An example of a number whose presentation is the sequence $S_k$ is the number $\sum_{i=0}^{k} i(k + 2)^i = k(k + 2)^k + ... + 0(k + 2)^0$. As we can see, this number has the representation $k(k-1)...10$ in base $k + 2$. We see that for every $k$ there is a number of this form $\sum_{i=0}^{k} i(k + 2)^i$. Therefore, we wish to take $x = \sum_{i=0}^{k} i(k + 2)^i$ as our exponential Diophantine equation. However, we first need to rewrite this sum as a simpler expression, since taking a sum of which the upper limit is one of the variables is not a standard operation when constructing exponential polynomials. We see $(k+1)\sum_{i=0}^{k} i(k + 2)^i = (k+2)\sum_{i=0}^{k} i(k + 2)^i - \sum_{i=0}^{k} i(k + 2)^i = k(k + 2)^{k+1} + 1 - \sum_{i=0}^{k} (k + 2)^i$. After multiplying both sides by $(k + 1)$ we get $(k+1)^2\sum_{i=0}^{k} i(k + 2)^i = k(k+1)(k + 2)^{k+1} + k + 1 - (k + 1)\sum_{i=0}^{k} (k + 2)^i$. Now $(k+1)^2\sum_{i=0}^{k} (k + 2)^i = (k+2)^2\sum_{i=0}^{k} (k + 2)^i - \sum_{i=0}^{k} (k + 2)^i = (k+2)^{k+1} - 1$, so we find $(k+1)^2\sum_{i=0}^{k} i(k + 2)^i = k(k+1)(k + 2)^{k+1} + k + 2 - (k+2)^{k+1}$. This means $(k+1)^2 x + (k + 2)^{k+1} = k(k+1)(k + 2)^{k+1} + k + 2$ is an exponential Diophantine equation which meets our requirements.

We can check for this equation that it does not yield an exponential Diophantine representation of the relation $R(x, k)$, as we can give a counterexample to the opposite direction. Working in base 4, the number 4 has digit representation 10, so $\exists b(\tilde{4}(b) = S_1)$. However, $2^2 \cdot 4 + 3^2 = 25$, yet $1 \cdot 2 \cdot 3^2 + 1 + 2 = 21$, so $k^2 x + (k + 1)^{k+1} = k^2(k + 1)^{k+1} + k + 1$ does not hold (amongst others) for the pair $(x, k) = (4, 1)$.
Exercise 2

Let \(m(x) = k\) express that \(x\) masks exactly \(k\) numbers.

a) Give an exponential Diophantine representation of the property \(m(x) = 2\).

b) Let \(b\) and \(c\) be natural numbers such that \(b \leq c\). Give a formula which expresses \(m(c - b)\) in terms of \(m(c)\), \(m(b)\) and \(m(b \land c)\).

c) Can you give a similar formula for arbitrary \(b\) and \(c\) (i.e., \(b\) and \(c\) for which the condition \(b \leq c\) does not necessarily hold)? (1.5 + 1.5 + 2 pts.)

---

a) One can verify that the only numbers which mask exactly 2 numbers are those numbers with exactly one 1 appearing in their binary representation. For instance, one can derive the general formula \(m(x) = 2^n\) where \(n_x\) is the number of 1’s appearing in the binary representation of \(x\); this formula can then be re-used in the next exercise. To derive this formula, simply notice that 0 only masks itself and that every added 1 doubles the amount of numbers masked, since it will then also mask those numbers which differ from a previously masked number only in that point of the representation (where they have a 1 instead of a 0). Numbers which mask exactly two numbers are thus of the form \(2^n\) with \(n\) a natural number, as these are the numbers with the \(n\)-th coefficient as the only non-zero coefficient. An exponential Diophantine representation of the property \(m(x) = 2\) is therefore \(m(x) = 2 \iff \exists n(x = 2^n)\).

b) Let \(b\) and \(c\) be natural numbers for which \(b \leq c\) is given, so \(\forall k(b_k \leq c_k)\). The number of 1’s appearing in the binary representation of \(c - b\) is then exactly the number of 1’s in the representation of \(c\) minus the number of 1’s in the representation \(b\). From this we obtain \(m(c - b) = 2^{n_{c-b}} = 2^{n_c - n_b} = 2^{n_c - 2^{n_b}} = m(c) m(b)\).

c) [I forgot to note for completeness' sake that we still need to have \(b \leq c\) for \(c - b\) to have a binary representation, but I take this assumption as implicit.] To see that \(m(c)\), \(m(b)\) and \(m(b \land c)\) are not enough for the arbitrary case, observe that \(m(1) = m(2) = 2\) and \(m(1 \land 4) = m(2 \land 4) = 1\), yet \(m(4 - 1) = 4\) whereas \(m(4 - 2) = 2\). This shows that we are unable to distinguish between 1 and 2 using just \(m(b)\) and \(m(b \land 4)\), even though \(m(4 - b)\) is different for the two, which means that we cannot give a formula for \(m(c - b)\) in terms of \(m(c)\), \(m(b)\) and \(m(b \land c)\). [The similar formula I had in mind was \(m(c - b) = 2^{n_{2^c-b,b}} m(c) m(b)\). This ought to work since \(n_{2^c-b,b}\) counts how many 1’s are undone in the representation of \(c - b\) when we add \(b\) to it, which is exactly the number of 1’s which are created when \(b\) is subtracted from \(c\). Lacking a proper proof of the correctness of this formula, I didn’t explicitly request a formula which does work, so I will also accept solutions which only establish the impossibility of giving a formula like the one in b).]