Homework Assignment 4 - Extended hints

Due **Friday 20-02-04**

1. Let α be Ackermann's function. Prove Lemma 2(ii):

$$y < n \Rightarrow \alpha(m, y) < \alpha(m, n), \quad \text{for all } m, n \text{ and } y.$$

(*Hint:* Use main induction on n and secondary induction on m. You may use Lemma 2(i) and Lemma 3.)

Extended Hint: Ackermann's function is recursively defined as follows:

$$\begin{aligned} \alpha(m,0) &= s(m) && \text{(i)} \\ \alpha(0,s(n)) &= \alpha(1,n) && \text{(ii)} \\ \alpha(s(m),s(n)) &= \alpha(\alpha(m,s(n)),n). && \text{(iii)} \end{aligned}$$

In class the following facts have been proved. The Ackermann function is well defined:

Lemma 0. *For all* $y, x \in \mathbf{N}$, *there exists a* $z \in \mathbf{N}$ *such that* $\alpha(x, y) = z$.

The Ackermann function is *strictly increasing*:

Lemma 1. *For all* $m, n \in \mathbf{N}$, $\alpha(m, n) > m$.

The Ackermann function is *monotonic* in the first argument:

Lemma 2.(i) *For all* $y, z, x \in \mathbf{N}$, *if* $x < z$ *then* $\alpha(x, y) < \alpha(z, y)$.

The following useful fact has also been proved:

Lemma 3. *For all* $m, n \in \mathbf{N}$, $\alpha(m, s(n)) \geq \alpha(s(m), n)$.

Using the above facts, we are asked to prove that the Ackermann function is monotonic in the *second* argument:

Lemma 2.(ii) *For all* $y, z, x \in \mathbf{N}$, *if* $y < z$ *then* $\alpha(x, y) < \alpha(x, z)$.

We proceed by a main induction on z and a secondary induction on x. We must prove

Main base case: *For all* $y, x \in \mathbf{N}$, *if* $y < 0$ *then* $\alpha(x, y) < \alpha(x, 0)$.

Proof: . . . . . . (Think logically!)

Main inductive step: Assume the truth of the *inductive hypothesis*

For all $y, x \in \mathbf{N}$, *if* $y < n$ *then* $\alpha(x, y) < \alpha(x, n)$.

We need to prove that

For all $y, x \in \mathbf{N}$, *if* $y < s(n)$ *then* $\alpha(x, y) < \alpha(x, s(n))$.

We do this by a secondary induction on x:

Secondary base case: *For all* $y \in \mathbf{N}$, *if* $y < s(n)$ *then* $\alpha(0, y) < \alpha(0, s(n))$.

Proof: . . . . (Since $y < s(n)$, we have $y \leq n$. This fact can easily be proved by induction [try it!] and you don't need to write it down. Use Lemma 3, Lemma 2(i) and the main inductive hypothesis.)

Secondary inductive step: Assume the *secondary inductive hypothesis*

For all $y \in \mathbf{N}$, *if* $y < s(n)$ *then* $\alpha(m, y) < \alpha(m, s(n))$

We need to prove that

For all $y \in \mathbf{N}$, *if* $y < s(n)$ *then* $\alpha(s(m), y) < \alpha(s(m), s(n))$.

Proof: .... (Apply the 3rd clause in the definition on α to $\alpha(s(m), s(n))$, then the fact that α is strictly increasing, Lemma 3 and the fact that $y \leq n$.

This concludes the proof of the secondary inductive step, thus of the secondary induction and thus of the main inductive step. The proof is finished.

We say that a number a is *congruent to b modulo m* (written $a \equiv b \ (mod\ m)$) if and only if $a - b = md$ for some $d \in \mathbf{Z}$. (Thus, if $a = md_0 + r_0$ and $b = md_1 + r_1$ with $0 \leq r_0, r_1 < m$, then $r_0 = r_1$.)

2. Prove the *Chinese Remainder Theorem: Let* m_1, ..., m_r *be any pairwise coprime integers, then the congruences*

$$x \equiv a_i \pmod{m_i} \qquad (i = 1, \ldots, r)$$

have a common solution, which is unique mod m, where $m = m_1 \cdot \ldots \cdot m_r$.

Moreover, writing $M_i = m/m_i$, *we can obtain a solution in the form* $x = \Sigma_{i \leq r} M_i x_i$, *where* x_i *satisfies* $M_i x_i \equiv a_i \pmod{m_i}$.

Hint: Read section 2.3 of Cohn's book and write exactly the part you need to prove theorem 5 (nothing less, nothing more).

Tasks: This is an essay-like exercise. The proof at page 34 of Cohn's book first shows that the solution is unique mod m, then that a solution exists and has the form $x = \Sigma M_i x_i$.

In the proof of uniqueness, Proposition 3(i) of paragraph 2.2 is quoted (page 28), which was not proved in class and you need to write the proof of it.

In the proof of existence, there is an implicit use of Theorem 4, page 33, so you need to write a proof of it. In the proof of Theorem 4, there is a reference to Theorem 1(iii), page 31, which you need to prove and to Proposition 2, page 32, which you also need to prove. The proof of Proposition 2 relies on *Bezout's Lemma*, which was done in class [but if you really want your essay to be self contained, you may as well write it...]

Comment: The Chinese Remainder Theorem has an algebraic meaning which is spelt out at page 34-35; for our purpose, it provides an alternative way to code *sequences of natural numbers*. Considering the example of congruences mod 2 and mod 3, we have

$\mathbf{Z}/6$	$\rightarrow$	$\mathbf{Z}/2 \times \mathbf{Z}/3$
0	$\mapsto$	(0, 0)
1	$\mapsto$	(1, 1)
2	$\mapsto$	(0, 2)
3	$\mapsto$	(1, 0)
4	$\mapsto$	(0, 1)
5	$\mapsto$	(1, 2)

In general, there is a map $\mathbf{Z}/rs \rightarrow \mathbf{Z}/rx\mathbf{Z}/s$ given by

$$f : rm(x, rs) \mapsto (rm(x, r), rm(x, s))$$

and the Chinese Remainder Theorem proves that this map is *bijective if r and s are coprime*. In our example, since 2 and 3 are coprime the formula in the Chinese Remainder Theorem gives us a coding of the pairs (y, z) with $y < 2$ and $z < 3$ into numbers $z < 6$, and the remainder functions $rm(z, 2)$ and $rm(z, 3)$ give us the decoding functions.