4 Assessed Exercise II: The Binary Euclidean Algorithm

The greatest common divisor of two natural numbers can be computed efficiently using a binary version of Euclid's algorithm. It eliminates common factors of two (which in hardware can be done efficiently by shifting), and given two odd numbers it subtracts them, producing another even number.

- The GCD of x and 0 is x.
- If the GCD of x and y is z, then the GCD of $2x$ and $2y$ is $2z$.
- The GCD of $2x$ and y is the same as that of x and y if y is odd.
- The GCD of x and y is the same as that of $x - y$ and y if $y \leq x$.
- The GCD of x and y is the same as the GCD of y and x.

This algorithm is actually nondeterministic, in that the steps can be applied in any order. However the result is unique because a pair of positive integers has exactly one greatest common divisor.

Task 5 *Inductively define the set BinaryGCD such that* $(x, y, g) \in$ *BinaryGCD means* g *is computed from* x *and* y *as specified by the description above.* *[5 marks]*

consts *BinaryGCD* :: $(nat \times nat \times nat)$ *set*

Task 6 *Show that the BinaryGCD of* x *and* y *is really the greatest common divisor of both numbers, with respect to the divides relation. Hint: it may help to consider whether* d *is even or odd. Be careful to choose the right form of induction, and justify your choice in your write-up.* *[15 marks]*

lemma *GCD-greatest-divisor*:
$(x,y,g) \in BinaryGCD \Longrightarrow d\ dvd\ x \Longrightarrow d\ dvd\ y \Longrightarrow d\ dvd\ g$

Task 7 *Prove the following statement. In the form given (assuming* n *to be odd), it can be proved directly by induction.* *[10 marks]*

lemma *GCD-mult*:
$(x,y,g) \in BinaryGCD \Longrightarrow odd\ n \Longrightarrow (n*x,n*y,n*g) \in BinaryGCD$

Remark: the theorem above actually holds for all n, but the simplest way of proving it is probably to prove that *BinaryGCD* corresponds exactly to the true *gcd* function and then to use properties of the latter.

Task 8 *How do we know that BinaryGCD can compute a result for all values of a and b? To prove it requires a carefully formulated induction, as shown in the theorem statement below. We need course-of-values induction (expressed by the theorem less-induct), which allows us to assume the induction formula for everything smaller than n. (Why doesn't standard induction work here?) Hint: the algorithm is complete even if the steps GCDEven and GCDOdd are deleted. They merely improve performance, so your proof can ignore them. You will still need to consider various cases corresponding to the remaining steps of the algorithm.* *[20 marks]*

lemma *GCD-defined-aux*: $a+b \leq n \Longrightarrow \exists\, g.\ (a,\ b,\ g) \in \mathit{BinaryGCD}$

Armed with this lemma, the completeness statement is trivial.

theorem *GCD-defined*: $\exists\, g.\ (a,\ b,\ g) \in \mathit{BinaryGCD}$