University of Cambridge
Computer Laboratory
Dr Tjark Weber

Easter Term 2010/11
Exercises 3
May 13, 2011

Interactive Formal Verification (L21)

1 Sums of Powers, Polynomials

This assignment *will be assessed* to determine 50% of your final mark. Please complete the indicated tasks and write a brief document explaining your work. You may prepare this document using Isabelle's theory presentation facility, but this is not required. (A very simple way to print a theory file legibly is to use the Proof General command Isabelle > Commands > Display draft. You can combine the resulting output with a document produced using your favourite word processing package.) A clear write-up describing elegant, clearly structured proofs of all tasks will receive maximum credit.

You must work on this assignment as an individual. Collaboration is not permitted.

1.1 Sums of Powers

We consider sums of consecutive powers: $S_p(n) = \sum_{k=1}^{n} k^p$.

▷ Define a corresponding function `S p n`.

```
S :: "nat ⇒ nat ⇒ nat"
```

Hint: exponentiation and summation functions are already available in Isabelle/HOL.

Clearly, $S_0(n) = n$. It is also well-known that $S_1(n) = \frac{n^2+n}{2}$.

▷ Prove these identities.

lemma `"S 0 n = n"`
lemma `"2 * S 1 n = n^2 + n"`

At this point, we might suspect that $S_p(n)$ is a polynomial in n with rational coefficients.

▷ Verify this conjecture for $p = 2$, i.e., find $k > 0$ and a polynomial *poly* in n so that $k \cdot S_2(n) = poly$. Prove the resulting identity.

lemma `"k * S 2 n = poly"` — replace `k` and `poly`

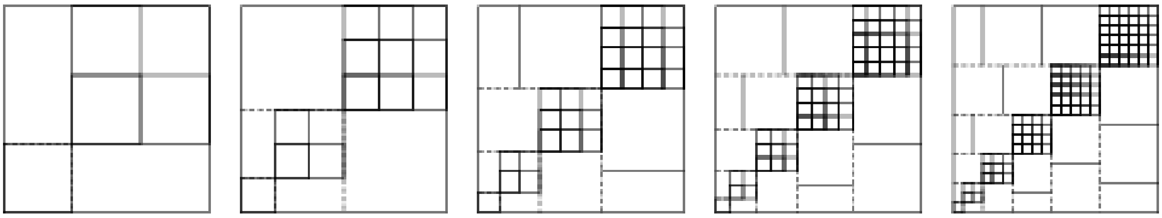

Figure 1: Visualization of Nicomachus's theorem

Hint: useful simplification rules for addition and multiplication are available as `algebra_simps`. The *Find theorems* command can be used to discover further lemmas.

For $p = 3$, our conjecture follows from the astonishing identity $\sum_{k=1}^{n} k^3 = (\sum_{k=1}^{n} k)^2$, which is known as *Nicomachus's theorem.*

▷ Prove Nicomachus's theorem.

theorem *"S 3 n = (S 1 n)^2"*

Before we could prove our conjecture for arbitrary p (which we will not do as part of this assignment, but search for *Faulhaber's formula* if you want to know more), we need to define polynomials.

1.2 Polynomials

A polynomial in one variable can be given by the list of its coefficients: e.g., $[0, \frac{1}{6}, \frac{1}{3}, \frac{1}{2}]$ represents the polynomial $\frac{1}{2}x^3 + \frac{1}{3}x^2 + \frac{1}{6}x + 0$. (We list coefficients in reverse order, i.e., from lower to higher degree.)

Coefficients may be integers, rationals, reals, etc. In general, we require coefficients to be elements of a commutative ring (cf. `Rings.thy`).

To every polynomial in one variable we can associate a *polynomial function* on the ring of coefficients. This function's value is obtained by substituting its argument for the polynomial's variable, i.e., by evaluating the polynomial.

▷ Define a function `poly cs x` so that $poly\ [c_0, c_1, \ldots, c_n]\ x = c_n \underbrace{x \cdot \ldots \cdot x}_{n \text{ factors}} + \ldots + c_1 x + c_0$.

poly :: "'a::comm_ring list ⇒ 'a::comm_ring ⇒ 'a::comm_ring"

▷ Define a function `poly_plus p q` that computes the sum of two polynomials.

poly_plus :: "'a::comm_ring list ⇒ 'a::comm_ring list ⇒ 'a::comm_ring list"

▷ Prove correctness of `poly_plus`.

lemma *"poly (poly_plus p q) x = poly p x + poly q x"*

Hint: Isabelle provides customized induction rules for recursive functions, e.g., `poly_plus.induct`. See the *Tutorial on Function Definitions* for details.

▷ Define a function `poly_times p q` that computes the product of two polynomials.

```
poly_times :: "'a::comm_ring list ⇒ 'a::comm_ring list ⇒ 'a::comm_ring list"
```

▷ Prove correctness of `poly_times`.

lemma `"poly (poly_times p q) x = poly p x * poly q x"`

▷ **Solutions are due on Friday, May 27, 2011, at 12 noon.** Please deliver a printed copy of the completed assignment to student administration by that deadline, and also send the corresponding Isabelle theory file to tw333@cam.ac.uk.