Arithmetic: A Programmatic Approach

Murisi Tarusenga

Monday 19$^{\text{th}}$ August, 2019 16:57

Introduction

What follows is a reformulation of the elementary parts of number theory, hard analysis, and linear algebra in terms of a system of procedures for achieving particular objectives, objectives like showing that modular exponentiation of a specific integer with specific properties yields a stated result. So, while formal mathematics usually takes the format of definition-theorem-proof, this project has the format of declaration-procedure objective-procedure implementation. So where there usually would have been a statement and proof of Euler's totient theorem, procedure I:76 is provided, and where there would have been a definition of Euler's totient function, declaration I:27 is provided.

At this point the natural question is that of how we are to know that the following procedure implementations achieve the corresponding procedure objectives for all inputs. Well, strictly speaking, the only way to know that the following procedures always achieve their respective objectives is to actually execute them on all possible inputs and actually verify that the objective is met. However, when the input can be any integer, this proposal is in-principle not possible. So the actual question is that of how we can see the *potential* of the following procedure implementations to achieve their respective objectives on different inputs, that is, of how we can get that feeling that if the input is changed to this or that, the objective should still be achieved. And the answer to this question is that we can see the potential of the following procedure implementations by simply looking at their (purposefully chosen) syntax in the same way that we can simply see from the syntax of the code fragment, "if $a = b$ and $b = c$, then verify that $a = c$", the potential of the instructions to be carried out successfully on different integer inputs.

For the purposes of storage and transmission of knowledge pertaining to the elementary parts of number theory, hard analysis, and linear algebra, the following procedures are interchangeable with their analogous proofs in the sense that, assuming equal competence in programming and proving, if you have the procedure objective and implementation, you can trivially generate the analogous theorem and proof, and if you are in possession of the theorem and proof, then you can trivially generate the analogous procedure objective and implementation.

Contents

Declarations

Part I

Integer Arithmetic

Declaration I:0

The phrase "integer" will be used as a shorthand for an ordered pair of natural numbers.

Declaration I:1

The phrase "the positive part of a" and the notation $\mathrm{po}(a)$, where a is an integer, will be used as a shorthand for the first entry of a.

Declaration I:2

The phrase "the negative part of a" and the notation $\mathrm{ne}(a)$, where a is an integer, will be used as a shorthand for the second entry of a.

Declaration I:3

The phrase "$a = b$", where a, b are integers, will be used as a shorthand for "$\mathrm{po}(a) + \mathrm{ne}(b) = \mathrm{ne}(a) + \mathrm{po}(b)$".

Procedure I:0

Objective

Choose an integer a. The objective of the following instructions is to show that $a = a$.

Implementation

1. Verify that $\mathrm{po}(a) + \mathrm{ne}(a) = \mathrm{ne}(a) + \mathrm{po}(a)$.
2. **Hence verify that $a = a$.**

Procedure I:1

Objective

Choose two integers a, b such that $a = b$. The objective of the following instructions is to show that $b = a$.

Implementation

1. Verify that $\mathrm{po}(a) + \mathrm{ne}(b) = \mathrm{ne}(a) + \mathrm{po}(b)$.
2. Hence verify that $\mathrm{po}(b)+\mathrm{ne}(a) = \mathrm{ne}(b)+\mathrm{po}(a)$.
3. **Hence verify that $b = a$.**

Procedure I:2

Objective

Choose three integers a, b, c such that $a = b$ and $b = c$. The objective of the following instructions is to show that $a = c$.

Implementation

1. Using declaration I:3, verify that $\mathrm{po}(a) + \mathrm{ne}(b) = \mathrm{ne}(a) + \mathrm{po}(b)$.
2. Using declaration I:3, verify that $\mathrm{po}(b) + \mathrm{ne}(c) = \mathrm{ne}(b) + \mathrm{po}(c)$.
3. Hence verify that $\mathrm{po}(a) + \mathrm{ne}(b) + \mathrm{po}(b) + \mathrm{ne}(c) = \mathrm{ne}(a) + \mathrm{po}(b) + \mathrm{ne}(b) + \mathrm{po}(c)$.
4. Hence verify that $\mathrm{po}(a)+\mathrm{ne}(c) = \mathrm{ne}(a)+\mathrm{po}(c)$.
5. **Hence verify that $a = c$.**

Declaration I:4

The notation $a + b$, where a, b are integers, will be used as a shorthand for the pair $\langle \mathrm{po}(a) + \mathrm{po}(b), \mathrm{ne}(a) + \mathrm{ne}(b)\rangle$.

Procedure I:3

Objective

Choose four integers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $a + b = c + d$.

Implementation

1. Using declaration I:3, verify that $\text{po}(a) + \text{ne}(c) = \text{ne}(a) + \text{po}(c)$.
2. Using declaration I:3, verify that $\text{po}(b) + \text{ne}(d) = \text{ne}(b) + \text{po}(d)$.
3. Hence verify that $a + b$

   (a) $= \langle \text{po}(a), \text{ne}(a)\rangle + \langle \text{po}(b), \text{ne}(b)\rangle$

   (b) $= \langle \text{po}(a) + \text{po}(b), \text{ne}(a) + \text{ne}(b)\rangle$

   (c) $= \langle \text{po}(a) + \text{po}(b) + \text{ne}(c) + \text{ne}(d), \text{ne}(a) + \text{ne}(b) + \text{ne}(c) + \text{ne}(d)\rangle$

   (d) $= \langle (\text{po}(a) + \text{ne}(c)) + (\text{po}(b) + \text{ne}(d)), \text{ne}(a) + \text{ne}(b) + \text{ne}(c) + \text{ne}(d)\rangle$

   (e) $= \langle (\text{ne}(a) + \text{po}(c)) + (\text{ne}(b) + \text{po}(d)), \text{ne}(a) + \text{ne}(b) + \text{ne}(c) + \text{ne}(d)\rangle$

   (f) $= \langle \text{ne}(a) + \text{ne}(b) + \text{po}(c) + \text{po}(d), \text{ne}(a) + \text{ne}(b) + \text{ne}(c) + \text{ne}(d)\rangle$

   (g) $= \langle \text{po}(c) + \text{po}(d), \text{ne}(c) + \text{ne}(d)\rangle$

   (h) $= \langle \text{po}(c), \text{ne}(c)\rangle + \langle \text{po}(d), \text{ne}(d)\rangle$

   (i) $= c + d$.

Procedure I:4

Objective

Choose three integers a, b, c. The objective of the following instructions is to show that $(a + b) + c = a + (b + c)$.

Implementation

1. Verify that $(a + b) + c$

   (a) $= \langle \text{po}(a) + \text{po}(b), \text{ne}(a) + \text{ne}(b)\rangle + \langle \text{po}(c), \text{ne}(c)\rangle$

   (b) $= \langle (\text{po}(a) + \text{po}(b)) + \text{po}(c), (\text{ne}(a) + \text{ne}(b)) + \text{ne}(c)\rangle$

   (c) $= \langle \text{po}(a) + (\text{po}(b) + \text{po}(c)), \text{ne}(a) + (\text{ne}(b) + \text{ne}(c))\rangle$

   (d) $= \langle \text{po}(a), \text{ne}(a)\rangle + \langle \text{po}(b) + \text{po}(c), \text{ne}(b) + \text{ne}(c)\rangle$

   (e) $= a + (b + c)$.

Procedure I:5

Objective

Choose two integers a, b. The objective of the following instructions is to show that $a + b = b + a$.

Implementation

1. $a + b$

   (a) $= \langle \text{po}(a) + \text{po}(b), \text{ne}(a) + \text{ne}(b)\rangle$

   (b) $= \langle \text{po}(b) + \text{po}(a), \text{ne}(b) + \text{ne}(a)\rangle$

   (c) $= b + a$.

Declaration I:5

The notation a, where a is a natural number, will contextually be used as a shorthand for the pair $\langle a, 0\rangle$.

Procedure I:6

Objective

Choose an integer a. The objective of the following instructions is to show that $0 + a = a$.

Implementation

1. Verify that $0 + a$

   (a) $= \langle 0, 0\rangle + \langle \text{po}(a), \text{ne}(a)\rangle$

   (b) $= \langle 0 + \text{po}(a), 0 + \text{ne}(a)\rangle$

   (c) $= \langle \text{po}(a), \text{ne}(a)\rangle$

   (d) $= a$.

Declaration I:6

The notation $-a$, where a is an integer, will be used as a shorthand for the pair $\langle \text{ne}(a), \text{po}(a)\rangle$.

Procedure I:7

Objective

Choose two integers a, b such that $a = b$. The objective of the following instructions is to show that $-a = -b$.

Implementation

1. Using declaration I:3, verify that $\mathrm{po}(a) + \mathrm{ne}(b) = \mathrm{ne}(a) + \mathrm{po}(b)$.
2. Hence verify that $-a$

(a) $= \langle \mathrm{ne}(a), \mathrm{po}(a) \rangle$

(b) $= \langle \mathrm{ne}(a) + \mathrm{po}(b), \mathrm{po}(a) + \mathrm{po}(b) \rangle$

(c) $= \langle \mathrm{po}(a) + \mathrm{ne}(b), \mathrm{po}(a) + \mathrm{po}(b) \rangle$

(d) $= \langle \mathrm{ne}(b), \mathrm{po}(b) \rangle$

(e) $= -b$.

Procedure I:8

Objective

Choose an integer a. The objective of the following instructions is to show that $-a + a = 0$.

Implementation

1. Verify that $-a + a$

(a) $= (-a) + a$

(b) $= \langle \mathrm{ne}(a), \mathrm{po}(a) \rangle + \langle \mathrm{po}(a), \mathrm{ne}(a) \rangle$

(c) $= \langle \mathrm{ne}(a) + \mathrm{po}(a), \mathrm{po}(a) + \mathrm{ne}(a) \rangle$

(d) $= \langle 0, 0 \rangle$

(e) $= 0$.

Declaration I:7

The notation ab, where a, b are integers, will be used as a shorthand for the pair $\langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b) \rangle$.

Procedure I:9

Objective

Choose four integers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $ab = cd$.

Implementation

1. Using declaration I:3, verify that $\mathrm{po}(a) + \mathrm{ne}(c) = \mathrm{ne}(a) + \mathrm{po}(c)$.
2. Using declaration I:3, verify that $\mathrm{po}(b) + \mathrm{ne}(d) = \mathrm{ne}(b) + \mathrm{po}(d)$.
3. Hence verify that ab

(a) $= \langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b) \rangle$

(b) $= \langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(c) $= \langle \mathrm{po}(a)(\mathrm{po}(b) + \mathrm{ne}(d)) + \mathrm{ne}(a)\,\mathrm{ne}(b) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(d) $= \langle \mathrm{po}(a)(\mathrm{ne}(b) + \mathrm{po}(d)) + \mathrm{ne}(a)\,\mathrm{ne}(b) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(e) $= \langle (\mathrm{po}(a) + \mathrm{ne}(c))\,\mathrm{po}(d) + \mathrm{ne}(a)\,\mathrm{ne}(b) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(f) $= \langle (\mathrm{ne}(a) + \mathrm{po}(c))\,\mathrm{po}(d) + \mathrm{ne}(a)\,\mathrm{ne}(b) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(g) $= \langle \mathrm{ne}(a)(\mathrm{po}(d) + \mathrm{ne}(b)) + \mathrm{po}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(h) $= \langle \mathrm{ne}(a)(\mathrm{po}(b) + \mathrm{ne}(d)) + \mathrm{po}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d), \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(i) $= \langle (\mathrm{ne}(a) + \mathrm{po}(c))\,\mathrm{ne}(d) + \mathrm{po}(c)\,\mathrm{po}(d), \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(j) $= \langle (\mathrm{po}(a) + \mathrm{ne}(c))\,\mathrm{ne}(d) + \mathrm{po}(c)\,\mathrm{po}(d), \mathrm{po}(a)\,\mathrm{ne}(d) + \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d) \rangle$

(k) $= \langle \mathrm{ne}(c)\,\mathrm{ne}(d) + \mathrm{po}(c)\,\mathrm{po}(d), \mathrm{ne}(c)\,\mathrm{po}(d) + \mathrm{po}(c)\,\mathrm{ne}(d)\rangle$

(l) $= cd$.

Procedure I:10

Objective

Choose three integers a, b, c. The objective of the following instructions is to show that $(ab)c = a(bc)$.

Implementation

1. Verify that $(ab)c$

(a) $= \langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b)\rangle\langle \mathrm{po}(c), \mathrm{ne}(c)\rangle$

(b) $= \langle(\mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b))\,\mathrm{po}(c) + (\mathrm{po}(a)\,\mathrm{ne}(b)+\mathrm{ne}(a)\,\mathrm{po}(b))\,\mathrm{ne}(c), (\mathrm{po}(a)\,\mathrm{po}(b)+\mathrm{ne}(a)\,\mathrm{ne}(b))\,\mathrm{ne}(c) + (\mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b))\,\mathrm{po}(c)\rangle$

(c) $= \langle \mathrm{po}(a)(\mathrm{po}(b)\,\mathrm{po}(c) + \mathrm{ne}(b)\,\mathrm{ne}(c)) + \mathrm{ne}(a)(\mathrm{po}(b)\,\mathrm{ne}(c)+\mathrm{ne}(b)\,\mathrm{po}(c)), \mathrm{po}(a)(\mathrm{po}(b)\,\mathrm{ne}(c)+\mathrm{ne}(b)\,\mathrm{po}(c)) + \mathrm{ne}(a)(\mathrm{po}(b)\,\mathrm{po}(c) + \mathrm{ne}(b)\,\mathrm{ne}(c))\rangle$

(d) $= \langle \mathrm{po}(a), \mathrm{ne}(a)\rangle\langle \mathrm{po}(b)\,\mathrm{po}(c) + \mathrm{ne}(b)\,\mathrm{ne}(c), \mathrm{po}(b)\,\mathrm{ne}(c) + \mathrm{ne}(b)\,\mathrm{po}(c)\rangle$

(e) $= a(bc)$.

Procedure I:11

Objective

Choose two integers a, b. The objective of the following instructions is to show that $ab = ba$.

Implementation

1. ab

(a) $= \langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b)\rangle$

(b) $= \langle \mathrm{po}(b)\,\mathrm{po}(a) + \mathrm{ne}(b)\,\mathrm{ne}(a), \mathrm{po}(b)\,\mathrm{ne}(a) + \mathrm{ne}(b)\,\mathrm{po}(a)\rangle$

(c) $= ba$.

Procedure I:12

Objective

Choose an integer a. The objective of the following instructions is to show that $1a = a$.

Implementation

1. Verify that $1a$

(a) $= \langle 1, 0\rangle\langle \mathrm{po}(a), \mathrm{ne}(a)\rangle$

(b) $= \langle 1\,\mathrm{po}(a) + 0\,\mathrm{ne}(a), 1\,\mathrm{ne}(a) + 0\,\mathrm{po}(a)\rangle$

(c) $= \langle \mathrm{po}(a), \mathrm{ne}(a)\rangle$

(d) $= a$.

Procedure I:13

Objective

Choose three integers a, b, c. The objective of the following instructions is to show that $a(b + c) = ab + ac$.

Implementation

1. $a(b + c)$

(a) $= \langle \mathrm{po}(a), \mathrm{ne}(a)\rangle\langle \mathrm{po}(b)+\mathrm{po}(c), \mathrm{ne}(b)+\mathrm{ne}(c)\rangle$

(b) $= \langle \mathrm{po}(a)(\mathrm{po}(b) + \mathrm{po}(c)) + \mathrm{ne}(a)(\mathrm{ne}(b) + \mathrm{ne}(c)), \mathrm{po}(a)(\mathrm{ne}(b) + \mathrm{ne}(c)) + \mathrm{ne}(a)(\mathrm{po}(b) + \mathrm{po}(c))\rangle$

(c) $= \langle(\mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b)) + (\mathrm{po}(a)\,\mathrm{po}(c) + \mathrm{ne}(a)\,\mathrm{ne}(c)), (\mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b)) + (\mathrm{po}(a)\,\mathrm{ne}(c) + \mathrm{ne}(a)\,\mathrm{po}(c))\rangle$

(d) $= \langle \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b), \mathrm{po}(a)\,\mathrm{ne}(b) + \mathrm{ne}(a)\,\mathrm{po}(b)\rangle + \langle \mathrm{po}(a)\,\mathrm{po}(c) + \mathrm{ne}(a)\,\mathrm{ne}(c), \mathrm{po}(a)\,\mathrm{ne}(c) + \mathrm{ne}(a)\,\mathrm{po}(c)\rangle$

(e) $= ab + ac$.

Procedure I:14

Objective

Choose an integer a. The objective of the following instructions is to show that $(-1)^{2a} = 1$ and

$(-1)^{2a+1} = -1$.

Implementation

1. Verify that $(-1)^2 = (-1)(-1) + 1 + (-1) = (-1)((-1) + 1) + 1 = (-1)0 + 1 = 1$.
2. **Hence verify that $(-1)^{2a} = ((-1)^2)^a = 1^a = 1$.**
3. **Hence verify that $(-1)^{2a+1} = (-1)^{2a}(-1) = 1(-1) = -1$.**

Declaration I:8

The phrase "$a < b$", where a, b are rational numbers, will be used as a shorthand for "$\mathrm{po}(a) + \mathrm{ne}(b) < \mathrm{ne}(a) + \mathrm{po}(b)$".

Procedure I:15

Objective

Choose four integers a, b, c, d such that $a < b$, $a = c$ and $b = d$. The objective of the following instructions is to show that $c < d$.

Implementation

1. Using declaration I:3, verify that $\mathrm{po}(a) + \mathrm{ne}(c) = \mathrm{ne}(a) + \mathrm{po}(c)$.
2. Using declaration I:3, verify that $\mathrm{po}(b) + \mathrm{ne}(d) = \mathrm{ne}(b) + \mathrm{po}(d)$.
3. Using declaration I:8, verify that $\mathrm{po}(a) + \mathrm{ne}(b) < \mathrm{ne}(a) + \mathrm{po}(b)$.
4. Hence verify that $\mathrm{po}(c) + \mathrm{ne}(d)$
   (a) $= (\mathrm{ne}(a) + \mathrm{po}(c)) + (\mathrm{po}(b) + \mathrm{ne}(d)) - \mathrm{ne}(a) - \mathrm{po}(b)$
   (b) $= (\mathrm{po}(a) + \mathrm{ne}(c)) + (\mathrm{ne}(b) + \mathrm{po}(d)) - \mathrm{ne}(a) - \mathrm{po}(b)$
   (c) $= (\mathrm{po}(a) + \mathrm{ne}(b)) + \mathrm{ne}(c) + \mathrm{po}(d) - \mathrm{ne}(a) - \mathrm{po}(b)$
   (d) $< (\mathrm{ne}(a) + \mathrm{po}(b)) + \mathrm{ne}(c) + \mathrm{po}(d) - \mathrm{ne}(a) - \mathrm{po}(b)$
   (e) $= \mathrm{ne}(c) + \mathrm{po}(d)$.
5. **Hence verify that $c < d$.**

Procedure I:16

Objective

Choose three integers a, b, c such that $a < b$. The objective of the following instructions is to show that $a + c < b + c$.

Implementation

1. Using declaration I:8, verify that $\mathrm{po}(a) + \mathrm{ne}(b) < \mathrm{ne}(a) + \mathrm{po}(b)$.
2. Hence verify that $\mathrm{po}(a + c) + \mathrm{ne}(b + c)$
   (a) $= \mathrm{po}(a) + \mathrm{po}(c) + \mathrm{ne}(b) + \mathrm{ne}(c)$
   (b) $= (\mathrm{po}(a) + \mathrm{ne}(b)) + \mathrm{po}(c) + \mathrm{ne}(c)$
   (c) $= (\mathrm{ne}(a) + \mathrm{po}(b)) + \mathrm{po}(c) + \mathrm{ne}(c)$
   (d) $= \mathrm{ne}(a) + \mathrm{ne}(c) + \mathrm{po}(b) + \mathrm{po}(c)$
   (e) $= \mathrm{ne}(a + c) + \mathrm{po}(b + c)$.
3. **Hence verify that $a + c < b + c$.**

Procedure I:17

Objective

Choose two integers a, b such that $a < b$. The objective of the following instructions is to show that $a \neq b$ and $b \not< a$.

Implementation

1. Verify that $\mathrm{po}(a) + \mathrm{ne}(b) < \mathrm{ne}(a) + \mathrm{po}(b)$.
2. Hence verify that $\mathrm{po}(a) + \mathrm{ne}(b) \neq \mathrm{ne}(a) + \mathrm{po}(b)$.
3. **Hence verify that $a \neq b$.**
4. Also verify that $\mathrm{ne}(a) + \mathrm{po}(b) \not< \mathrm{po}(a) + \mathrm{ne}(b)$.
5. **Hence verify that $b \not< a$.**

Procedure I:18

Objective

Choose two integers a, b such that $a = b$. The objective of the following instructions is to show that $a \not< b$ and $b \not< a$.

Implementation

Implementation is analogous to that of procedure I:17.

Procedure I:19

Objective

Choose two integers a, b such that $a \neq b$. The objective of the following instructions is to show that $a < b$ or $b < a$.

Implementation

1. Verify that $\mathrm{po}(a) + \mathrm{ne}(b) \neq \mathrm{ne}(a) + \mathrm{po}(b)$.
2. If $\mathrm{po}(a) + \mathrm{ne}(b) < \mathrm{ne}(a) + \mathrm{po}(b)$, then do the following:
   (a) **Verify that $a < b$.**
3. Otherwise do the following:
   (a) Verify that $\mathrm{ne}(a) + \mathrm{po}(b) < \mathrm{po}(a) + \mathrm{ne}(b)$.
   (b) **Hence verify that $b < a$.**

Procedure I:20

Objective

Choose two integers a, b such that $a \not< b$. The objective of the following instructions is to show that $a = b$ or $b < a$.

Implementation

Implementation is analogous to that of procedure I:19.

Procedure I:21

Objective

Choose two integers a, b such that $0 < a$ and $0 < b$. The objective of the following instructions is to show that $0 < a + b$.

Implementation

1. Using declaration I:8, verify that $\mathrm{ne}(a) = \mathrm{po}(0) + \mathrm{ne}(a) < \mathrm{ne}(0) + \mathrm{po}(a) = \mathrm{po}(a)$.
2. Using declaration I:8, verify that $\mathrm{ne}(b) = \mathrm{po}(0) + \mathrm{ne}(b) < \mathrm{ne}(0) + \mathrm{po}(b) = \mathrm{po}(b)$.
3. Hence verify that $\mathrm{po}(0) + \mathrm{ne}(a + b) = \mathrm{ne}(a + b) = \mathrm{ne}(a) + \mathrm{ne}(b) < \mathrm{po}(a) + \mathrm{po}(b) = \mathrm{po}(a + b) = \mathrm{ne}(0) + \mathrm{po}(a + b)$.
4. **Hence verify that $0 < a + b$.**

Procedure I:22

Objective

Choose two integers a, b such that $0 < a$ and $0 < b$. The objective of the following instructions is to show that $0 < ab$.

Implementation

1. Using declaration I:8, verify that $\mathrm{ne}(a) = \mathrm{po}(0) + \mathrm{ne}(a) < \mathrm{ne}(0) + \mathrm{po}(a) = \mathrm{po}(a)$.
2. Hence verify that $0 < \mathrm{po}(a) - \mathrm{ne}(a)$.
3. Using declaration I:8, verify that $\mathrm{ne}(b) = \mathrm{po}(0) + \mathrm{ne}(b) < \mathrm{ne}(0) + \mathrm{po}(b) = \mathrm{po}(b)$.
4. Hence verify that $0 < \mathrm{po}(b) - \mathrm{ne}(b)$.
5. Hence verify that $0 < (\mathrm{po}(a) - \mathrm{ne}(a))(\mathrm{po}(b) - \mathrm{ne}(b))$.
6. Hence verify that $\mathrm{ne}(a)(\mathrm{po}(b) - \mathrm{ne}(b)) < \mathrm{po}(a)(\mathrm{po}(b) - \mathrm{ne}(b))$.
7. Hence verify that $\mathrm{po}(0) + \mathrm{ne}(ab) = \mathrm{ne}(a)\,\mathrm{po}(b) + \mathrm{po}(a)\,\mathrm{ne}(b) < \mathrm{po}(a)\,\mathrm{po}(b) + \mathrm{ne}(a)\,\mathrm{ne}(b) = \mathrm{ne}(0) + \mathrm{po}(ab)$.
8. **Hence verify that $0 < ab$.**

Declaration I:9

The notation $\|a\|$ will be used as a shorthand for the following expression:

1. $-a$ if $a < 0$
2. a if $a \geq 0$

Procedure I:23

Objective

Choose two integers a, b. The objective of the following instructions is to show that $\|ab\| = \|a\|\|b\|$.

Implementation

1. If $a \geq 0$ and $b \geq 0$, then do the following:
   (a) Verify that $ab \geq 0$.
   (b) **Hence verify that** $\|ab\| = ab = \|a\|\|b\|$**.**
2. Otherwise if $a < 0$ and $b \geq 0$, then do the following:
   (a) Verify that $ab < 0$.
   (b) **Hence verify that** $\|ab\| = -(ab) = (-a)b = \|a\|\|b\|$**.**
3. Otherwise if $a \geq 0$ and $b < 0$, then do the following:
   (a) Verify that $ab < 0$.
   (b) **Hence verify that** $\|ab\| = -(ab) = a(-b) = \|a\|\|b\|$**.**
4. Otherwise do the following:
   (a) Verify that $a < 0$ and $b < 0$.
   (b) Hence verify that $ab > 0$.
   (c) **Hence verify that** $\|ab\| = ab = (-a)(-b) = \|a\|\|b\|$**.**

Procedure I:24

Objective

Choose two integers a, b. The objective of the following instructions is to show that $\|a+b\| \leq \|a\| + \|b\|$.

Implementation

1. If $a + b \geq 0$, then do the following:
   (a) Verify that $a \leq \|a\|$.
   (b) Verify that $b \leq \|b\|$.
   (c) **Hence verify that** $\|a + b\| = a + b \leq \|a\| + \|b\|$**.**
2. Otherwise do the following:
   (a) Verify that $-a \leq \|a\|$.
   (b) Verify that $-b \leq \|b\|$.
   (c) Verify that $a + b < 0$.
   (d) **Hence verify that** $\|a + b\| = -(a + b) = (-a) + (-b) \leq \|a\| + \|b\|$**.**

Procedure I:25

Objective

Choose two integers a, b. The objective of the following instructions is to show that $\|a\| - \|b\| \leq \|a - b\|$.

Implementation

1. Execute procedure I:24 on $\langle b, a - b\rangle$.
2. Hence verify that $\|a\| = \|b + (a - b)\| \leq \|b\| + \|a - b\|$.
3. **Hence verify that** $\|a\| - \|b\| \leq \|a - b\|$**.**

Declaration I:10

The notation $\text{sgn}(a)$ will be used as a shorthand for the following expression:

1. -1 if $a < 0$
2. 0 if $a = 0$
3. 1 if $a > 0$

Procedure I:26

Objective

Choose an integer a. The objective of the following instructions is to show that $a = \text{sgn}(a)\|a\|$.

Implementation

1. If $a > 0$, then do the following:
   (a) Verify that $\|a\| = a$.
   (b) Verify that $\operatorname{sgn}(a) = 1$.
   (c) **Hence verify that** $a = 1a = \operatorname{sgn}(a)\|a\|$**.**
2. If $a = 0$, then do the following:
   (a) Verify that $\|a\| = a = 0$.
   (b) **Hence verify that** $a = 0 = \operatorname{sgn}(a)0 = \operatorname{sgn}(a)\|a\|$**.**
3. Otherwise if $a < 0$, then do the following:
   (a) Verify that $\|a\| = -a$.
   (b) Verify that $\operatorname{sgn}(a) = -1$.
   (c) **Hence verify that** $a = (-1)(-a) = \operatorname{sgn}(a)\|a\|$**.**

Procedure I:27

Objective

Choose an integer a and a positive integer b. The objective of the following instructions is to construct integers n and m such that $a = nb + m$ and $0 \leq m < b$.

Implementation

1. Let $n = 0$.
2. While $(n+1)b \leq a$, do the following:
   (a) Let n receive $n + 1$.
   (b) Verify that $nb \leq a$.
3. While $nb > a$, do the following:
   (a) Let n receive $n - 1$.
   (b) Verify that $(n + 1)b > a$.
4. Therefore verify that $nb \leq a$.
5. Also verify that $(n + 1)b > a$.
6. Let $m = a - nb$.
7. **Now verify that** $b > a - nb = m \geq 0$**.**
8. **Also verify that** $a = bn + a - nb = nb + m$**.**
9. **Yield** $\langle n, m\rangle$**.**

Declaration I:11

The notation $a \operatorname{div} b$ will be used to refer to the first part of the pair yielded by executing procedure I:27 on $\langle a, b\rangle$.

Declaration I:12

The notation $a \bmod b$ will be used to refer to the second part of the pair yielded by executing procedure I:27 on $\langle a, b\rangle$.

Declaration I:13

The notation $a \equiv b \pmod c$ will be used as a shorthand for "$a \bmod c = b \bmod c$".

Procedure I:28

Objective

Choose four integers a, b, c, d and a positive integer e in such a way that $a \equiv c \pmod e$ and $b \equiv d \pmod e$. The objective of the following instructions is to show that $a + b \equiv c + d \pmod e$.

Implementation

1. Verify that $a + b$
   (a) $\equiv (a \operatorname{div} e)e + (a \bmod e) + (b \operatorname{div} e)e + (b \bmod e)$
   (b) $\equiv (a \bmod e) + (b \bmod e)$
   (c) $\equiv (c \bmod e) + (d \bmod e)$
   (d) $\equiv (c \operatorname{div} e)e + (c \bmod e) + (d \operatorname{div} e)e + (d \bmod e)$
   (e) $\equiv c + d \pmod e$**.**

Procedure I:29

Objective

Choose four integers a, b, c, d and a positive integer e in such a way that $a \equiv c \pmod e$ and $b \equiv d$

(mod e). The objective of the following instructions is to show that $ab \equiv cd \pmod{e}$.

Implementation

1. Verify that ab
   (a) $\equiv ((a \operatorname{div} e)e + (a \bmod e))((b \operatorname{div} e)e + (b \bmod e))$
   (b) $\equiv (a \operatorname{div} e)(b \operatorname{div} e)e^2 + (a \operatorname{div} e)(b \bmod e)e + (a \bmod e)(b \operatorname{div} e)e + (a \bmod e)(b \bmod e)$
   (c) $\equiv (a \bmod e)(b \bmod e)$
   (d) $\equiv (c \bmod e)(d \bmod e)$
   (e) $\equiv (c \operatorname{div} e)(d \operatorname{div} e)e^2 + (c \operatorname{div} e)(d \bmod e)e + (c \bmod e)(d \operatorname{div} e)e + (c \bmod e)(d \bmod e)$
   (f) $\equiv cd \pmod{e}$**.**

Procedure I:30

Objective

Choose an integer a and two positive integers b, c. The objective of the following instructions is to show that $(a \bmod bc) \bmod b = a \bmod b$.

Implementation

1. **Verify that** $(a \bmod bc) \bmod b = (a - (a \operatorname{div} bc)bc) \bmod b = a \bmod b$**.**

Procedure I:31

Objective

Choose a positive integer a and four integers b_1, b_0, c_1, c_0 such that $0 \le b_0 < a$, $0 \le c_0 < a$, and $b_1 a + b_0 = c_1 a + c_0$. The objective of the following instructions is to show that $b_1 = c_1$ and $b_0 = c_0$.

Implementation

1. **Verify that** $b_0 = b_0 \bmod a = (b_1 a + b_0) \bmod a = (c_1 a + c_0) \bmod a = c_0 \bmod a = c_0$**.**
2. Therefore verify that $b_1 a = c_1 a$.
3. **Therefore verify that** $b_1 = c_1$**.**

Procedure I:32

Objective

Choose an integer a and two positive integers b, c. The objective of the following instructions is to show that $ca \bmod cb = c(a \bmod b)$ and that $ca \operatorname{div} cb = a \operatorname{div} b$.

Implementation

1. Verify that $bc(a \operatorname{div} b) + c(a \bmod b) = c(b(a \operatorname{div} b) + a \bmod b) = ca = cb(ca \operatorname{div} cb) + ca \bmod cb$.
2. Now verify that $0 \le a \bmod b < b$.
3. Therefore verify that $0 \le c(a \bmod b) < cb$.
4. Now verify that $0 \le ca \bmod cb < cb$.
5. Execute procedure I:31 on $\langle bc, a \operatorname{div} b, c(a \bmod b), ca \operatorname{div} cb, ca \bmod cb \rangle$.
6. **Therefore verify that** $c(a \bmod b) = ca \bmod cb$**.**
7. **Also verify that** $a \operatorname{div} b = ca \operatorname{div} cb$**.**

Procedure I:33

Objective

Choose two integers a, b and a positive integer c such that $a \bmod c + b \bmod c < c$. The objective of the following instructions is to show that $a \operatorname{div} c + b \operatorname{div} c = (a+b) \operatorname{div} c$ and $a \bmod c + b \bmod c = (a+b) \bmod c$.

Implementation

1. Verify that $a = c(a \operatorname{div} c) + a \bmod c$.
2. Verify that $b = c(b \operatorname{div} c) + b \bmod c$.
3. Therefore verify that $a + b = c(a \operatorname{div} c + b \operatorname{div} c) + (a \bmod c + b \bmod c)$.
4. Verify that $0 \le a \bmod c + b \bmod c < c$.
5. Also verify that $a + b = ((a+b) \operatorname{div} c)c + (a+b) \bmod c$.
6. Verify that $0 \le (a+b) \bmod c < c$.

7. Execute procedure I:31 on $\langle c, a \operatorname{div} c + b \operatorname{div} c, a \bmod c + b \bmod c, (a+b) \operatorname{div} c, (a+b) \bmod c\rangle$.
8. **Therefore verify that** $a \operatorname{div} c + b \operatorname{div} c = (a+b) \operatorname{div} c$**.**
9. **Also verify that** $a \bmod c + b \bmod c = (a+b) \bmod c$**.**

Procedure I:34

Objective

Choose two integers a, b and a positive integer c such that $a \bmod c + b \bmod c \geq c$. The objective of the following instructions is to show that $1 + a \operatorname{div} c + b \operatorname{div} c = (a+b) \operatorname{div} c$ and $a \bmod c + b \bmod c - c = (a+b) \bmod c$.

Implementation

1. Verify that $a = c(a \operatorname{div} c) + a \bmod c$.
2. Verify that $b = c(b \operatorname{div} c) + b \bmod c$.
3. Therefore verify that $a + b = c(a \operatorname{div} c + b \operatorname{div} c) + a \bmod c + b \bmod c = c(1 + a \operatorname{div} c + b \operatorname{div} c) + (a \bmod c + b \bmod c - c)$.
4. Verify that $c \leq a \bmod c + b \bmod c < 2c$.
5. Therefore verify that $0 \leq a \bmod c + b \bmod c - c < c$.
6. Also verify that $a + b = c((a+b) \operatorname{div} c) + (a+b) \bmod c$.
7. Verify that $0 \leq (a+b) \bmod c < c$.
8. Execute procedure I:31 on $\langle c, 1 + a \operatorname{div} c + b \operatorname{div} c, a \bmod c + b \bmod c - c, (a+b) \operatorname{div} c, (a+b) \bmod c\rangle$.
9. **Therefore verify that** $1 + a \operatorname{div} c + b \operatorname{div} c = (a+b) \operatorname{div} c$**.**
10. **Therefore verify that** $a \bmod c + b \bmod c - c = (a+b) \bmod c$**.**

Procedure I:35

Objective

Choose an integer a and two positive integers b, c. The objective of the following instructions is to show that $a \operatorname{div} bc = (a \operatorname{div} b) \operatorname{div} c$ and $a \bmod bc = ((a \operatorname{div} b) \bmod c)b + a \bmod b$.

Implementation

1. Verify that $a = (a \operatorname{div} b)b + a \bmod b$.
2. Verify that $a \operatorname{div} b = ((a \operatorname{div} b) \operatorname{div} c)c + (a \operatorname{div} b) \bmod c$.
3. Therefore verify that $a = (((a \operatorname{div} b) \operatorname{div} c)c + (a \operatorname{div} b) \bmod c)b + a \bmod b = ((a \operatorname{div} b) \operatorname{div} c)bc + ((a \operatorname{div} b) \bmod c)b + a \bmod b$.
4. Verify that $0 \leq (a \operatorname{div} b) \bmod c \leq c - 1$.
5. Therefore verify that $0 \leq ((a \operatorname{div} b) \bmod c)b \leq cb - b$.
6. Verify that $0 \leq a \bmod b < b$.
7. Therefore verify that $0 \leq ((a \operatorname{div} b) \bmod c)b + a \bmod b < cb$.
8. Now verify that $a = (a \operatorname{div} bc)bc + a \bmod bc$.
9. Verify that $0 \leq a \bmod bc < bc$.
10. Execute procedure I:31 on $\langle bc, (a \operatorname{div} b) \operatorname{div} c, ((a \operatorname{div} b) \bmod c)b + a \bmod b, a \operatorname{div} bc, a \bmod bc\rangle$.
11. **Therefore verify that** $(a \operatorname{div} b) \operatorname{div} c = a \operatorname{div} bc$**.**
12. **Also verify that** $((a \operatorname{div} b) \bmod c)b + a \bmod b = a \bmod bc$**.**

Procedure I:36

Objective

Choose an integer a and a non-negative integer b. The objective of the following instructions is to consruct integers c, d, e, f, g such that $a = cd$, $b = ce$, $fa + gb = c$, and if $b = 0$, then $c = |a|$, otherwise $0 < c \leq b$.

Implementation

1. If $b = 0$, then do the following:
   (a) **Verify that** $a = \operatorname{sgn}(a)|a|$**.**
   (b) **Verify that** $b = 0|a|$**.**
   (c) **Verify that** $|a| = \operatorname{sgn}(a)a + 0b$**.**
   (d) **Yield** $\langle |a|, \operatorname{sgn}(a), 0, \operatorname{sgn}(a), 0\rangle$**.**
2. Otherwise do the following:
   (a) Verify that $0 \leq a \bmod b < b$.
   (b) Execute procedure I:36 on $\langle b, a \bmod b\rangle$ and let $\langle c, d, e, f, g\rangle$ receive.
   (c) **Now verify that** $b = cd$**.**
   (d) Also verify that $a \bmod b = ce$.
   (e) **Therefore verify that** $a = (a \operatorname{div} b)b + (a \bmod b) = c(d(a \operatorname{div} b) + e)$**.**
   (f) **Also verify that** $(f - g(a \operatorname{div} b))b + ga = fb + g(a - (a \operatorname{div} b)b) = fb + g(a \bmod b) = c$**.**
   (g) If $a \bmod b = 0$, then do the following:
      i. **Using (2) and (b), verify that** $0 < b = c \leq b$**.**
   (h) Otherwise do the following:
      i. **Using (b), verify that** $0 < c \leq a \bmod b < b$**.**
   (i) **Therefore yield** $\langle c, d(a \operatorname{div} b) + e, d, g, f - g(a \operatorname{div} b)\rangle$**.**

Declaration I:14

The notation (a, b) will be used to refer to the first part of the quintuple yielded by executing procedure I:36 on the pair $\langle a, b\rangle$.

Procedure I:37

Objective

Choose an integer a and a positive integer b. Let $1 \leq c \leq b$ be the largest integer such that $a \bmod c = 0$ and $b \bmod c = 0$. The objective of the following instructions is to either show that $0 \neq 0$ or $(a, b) = c$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. Verify that $0 < d \leq b$.
3. If $d > c$, then do the following:
   (a) Using the precondition, verify that $a \bmod d \neq 0$ or $b \bmod d \neq 0$.
   (b) If $a \bmod d \neq 0$, then do the following:
      i. Using (1), verify that $a = ed$.
      ii. Therefore verify that $a \bmod d = 0$.
      iii. **Therefore using (3b) and (3bii), verify that** $0 \neq 0$**.**
      iv. **Abort procedure.**
   (c) Otherwise if $b \bmod d \neq 0$, then do the following:
      i. Using (1), verify that $b = fd$.
      ii. Therefore verify that $b \bmod d = 0$.
      iii. **Therefore using (3c) and (3cii), verify that** $0 \neq 0$**.**
      iv. **Abort procedure.**
4. Otherwise if $d < c$, then do the following:
   (a) Verify that $ga + hb = d$.
   (b) Therefore verify that $0 \equiv gc(a \operatorname{div} c) + hc(b \operatorname{div} c) = g(c(a \operatorname{div} c) + a \bmod c) + h(c(b \operatorname{div} c) + b \bmod c) = ga + hb = d \not\equiv 0 \pmod{c}$.
   (c) **Therefore verify that** $0 \neq 0$**.**
   (d) **Abort procedure.**
5. **Otherwise verify that** $(a, b) = d = c$**.**

Procedure I:38

Objective

Choose integers a, c, d, j and a non-negative integer b. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle e, f, g, h, i\rangle$ receive. The objective of the following instructions is to show that $ca + db = (c + gj)a + (d - fj)b$.

Implementation

1. **Verify that** $(c+gj)a+(d-fj)b = ca+db+gja-fjb = ca+db+gjef-fjeg = ca+db$**.**

Procedure I:39

Objective

Choose integers a, c, d and a non-negative integer b such that $ca+db=(a,b)$. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle e, f, g, h, i\rangle$ receive. The objective of the following instructions is to construct a j such that $c = h+gj$ and $d = i-fj$.

Implementation

1. Verify that $cef+deg = ca+db = (a,b) = e$.
2. Therefore verify that $cf+dg = 1$.
3. Now verify that $hef+ieg = ha+ib = e$.
4. Therefore verify that $hf+ig = 1$.
5. Let $j = ci-hd$.
6. Now verify that $cf = 1-dg$.
7. Therefore verify that $c-cig = c(1-ig) = chf = h(1-dg) = h-hdg$.
8. **Therefore verify that** $c = h+cig-hdg = h+g(ci-hd) = h+gj$**.**
9. Now verify that $dg = 1-cf$.
10. Therefore verify that $d-dhf = d(1-hf) = dig = i(1-cf) = i-icf$.
11. **Therefore verify that** $d = i-icf+dhf = i-f(ic-dh) = i-fj$**.**
12. **Yield** $\langle j\rangle$**.**

Procedure I:40

Objective

Choose an integer a and a positive integer b such that $0 < (a,b) < b$. The objective of the following instructions is to show that $0 \neq 0$ or $a \bmod b \neq 0$.

Implementation

1. If $a \bmod b = 0$, then do the following:
   (a) Using (1), verify that $af \equiv 0f \equiv 0 \pmod{b}$.
   (b) Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle c, d, e, f, g\rangle$ receive.
   (c) Verify that $0 < (a,b) = c = fa+gb < b$.
   (d) Therefore verify $fa \equiv (a,b) \not\equiv 0 \pmod{b}$.
   (e) Therefore using (1a) and (1d), verify that $0 \neq 0$.
   (f) **Abort ptocedure.**
2. **Otherwise verify that** $a \bmod b \neq 0$**.**

Procedure I:41

Objective

Choose five integers a, d, e, f, g and two non-negative integers b, c such that $a = cd$, $b = ce$, and $fa+gb = c$. The objective of the following instructions is to show that $0 < 0$ or $(a,b) = c$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle u, v, x, y, z\rangle$ receive.
2. Verify that $u \geq 0$.
3. Verify that $a = uv$.
4. Verify that $b = xu$.
5. Therefore verify that $c = fa+gb = (fv+gx)u$.
6. If $u = 0$, then do the following:
   (a) **Verify that** $c = (fv+gx)u = 0 = u = (a,b)$**.**
   (b) **Yield.**
7. Also using (1) and the precondition, verify that $u = ya+zb = (yd+ze)c$.
8. If $c = 0$, then do the following:
   (a) **Verify that** $(a,b) = u = (yd+ze)c = 0 = c$**.**
   (b) **Yield.**
9. Verify that $c > 0$.

10. Now verify that $c = (fv + gx)u = (fv + gx)(yd + ze)c$.
11. Therefore verify that $(fv + gx)(yd + ze) = 1$.
12. Therefore verify that $fv + gx = yd + ze = \pm 1$.
13. If $fv + gx = yd + ze = -1$, then do the following:
    (a) Using (7) and (9), verify that $u = (yd + ze)c = -c < 0$.
    (b) **Therefore using (2) and (13a), verify that** $0 \le u < 0$**.**
    (c) **Abort procedure.**
14. Otherwise, do the following:
    (a) Verify that $fv + gx = yd + ze = 1$.
    (b) **Therefore verify that** $c = (fv + gx)u = u = (a, b)$**.**

Procedure I:42

Objective

Choose an integer a and a non-negative integer b. The objective of the following instructions is to show that $0 < 0$ or $(a, b) = (-a, b)$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle c, d, e, f, g\rangle$ receive.
2. Verify that $a = dc$.
3. Therefore verify that $-a = (-d)c$.
4. Verify that $b = ec$.
5. Verify that $fa + gb = c$.
6. Therefore verify that $(-f)(-a) + gb = c$.
7. Execute procedure I:41 on $\langle -a, b, c, -d, e, -f, g\rangle$.
8. **Therefore verify that** $(-a, b) = c = (a, b)$**.**

Procedure I:43

Objective

Choose two non-negative integers a, b. The objective of the following instructions is to show that $0 < 0$ or $(a, b) = (b, a)$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle c, d, e, f, g\rangle$ receive.
2. Verify that $b = ec$.
3. Verify that $a = dc$.
4. Verify that $gb + fa = c$.
5. Execute procedure I:41 on $\langle b, a, c, e, d, g, f\rangle$.
6. **Therefore verify that** $(b, a) = c = (a, b)$**.**

Procedure I:44

Objective

Choose two integers a, b and a positive integer c such that $a \equiv b \pmod{c}$. The objective of the following instructions is to show that $0 < 0$ or $(a, c) = (b, c)$.

Implementation

1. Execute procedure I:36 on $\langle a, c\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. Verify that $a = ed$.
3. Verify that $c = fd$.
4. Let $j = b \operatorname{div} c - a \operatorname{div} c$.
5. Therefore verify that $b = a + jc = ed + jfd = (e + jf)d$.
6. Verify that $gb + (h - gj)c = g(a + jc) + (h - gj)c = ga + hc = d$.
7. Now execute procedure I:41 on $\langle b, c, d, e + jf, f, g, h - gj\rangle$.
8. **Therefore verify that** $(b, c) = d = (a, c)$**.**

Procedure I:45

Objective

Choose an integer a and two non-negative integers b, c. The objective of the following instructions is to show that either $0 < 0$ or $(ca, cb) = c(a, b)$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. Verify that $a = ed$.
3. Therefore verify that $ca = e(cd)$.
4. Verify that $b = df$.
5. Therefore verify that $cb = f(cd)$.
6. Verify that $ga + hb = d$.
7. Therefore verify that $g(ca) + h(cb) = cd$.
8. Now execute procedure I:41 on $\langle ca, cb, cd, e, f, g, h\rangle$.
9. Therefore verify that $(ca, cb) = cd = c(a, b)$.

Procedure I:46

Objective

Choose an integer a and two non-negative integers b, c. The objective of the following instructions is to show that either $0 < 0$ or $(a, (b, c)) = ((a, b), c)$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle d_0, e_0, f_0, g_0, h_0\rangle$ receive.
2. Execute procedure I:36 on $\langle b, c\rangle$ and let $\langle d_1, e_1, f_1, g_1, h_1\rangle$ receive.
3. Execute procedure I:36 on $\langle (a, b), c\rangle$ and let $\langle d_2, e_2, f_2, g_2, h_2\rangle$ receive.
4. Verify that $a = d_0e_0 = e_0(a, b) = e_0d_2e_2 = e_0e_2((a, b), c)$.
5. Verify that (b, c)

(a) $= g_1b + h_1c$

(b) $= g_1d_0f_0 + h_1d_2f_2$

(c) $= g_1f_0(a, b) + h_1f_2((a, b), c)$

(d) $= g_1f_0d_2e_2 + h_1f_2((a, b), c)$

(e) $= g_1f_0e_2((a, b), c) + h_1f_2((a, b), c)$

(f) $= (g_1f_0e_2 + h_1f_2)((a, b), c)$.

6. Verify that $((a, b), c)$

(a) $= d_2$

(b) $= g_2(a, b) + h_2c$

(c) $= g_2d_0 + h_2d_1f_1$

(d) $= g_2(g_0a + h_0b) + h_2f_1(b, c)$

(e) $= g_2g_0a + g_2h_0d_1e_1 + h_2f_1(b, c)$

(f) $= g_2g_0a + g_2h_0e_1(b, c) + h_2f_1(b, c)$

(g) $= g_2g_0a + (g_2h_0e_1 + h_2f_1)(b, c)$.

7. Execute procedure I:41 on $\langle a, (b, c), ((a, b), c), e_0e_2, g_1f_0e_2 + h_1f_2, g_2g_0, g_2h_0e_1 + h_2f_1\rangle$.
8. **Therefore verify that** $((a, b), c) = (a, (b, c))$**.**

Declaration I:15

The notation $(a_0, a_1, \cdots, a_{n-1})$ will be used to contextually refer to one of the following integers:

1. $((a_0), (a_1, a_2, \cdots, a_{n-1}))$
2. $((a_0, a_1), (a_2, a_3, \cdots, a_{n-1}))$
3. $\vdots$
4. $((a_0, a_1, \cdots, a_{n-2}), (a_{n-1}))$

Procedure I:47

Objective

Choose two integers a, b and a non-negative integer c such that $(a, c) = 1$ and $(b, c) = 1$. The objective of the following instructions is to show that either $0 < 0$ or $(ab, c) = 1$.

Implementation

1. Execute procedure I:36 on $\langle a, c\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. Verify that $ga + hc = d = (a, c) = 1$.
3. Execute procedure I:36 on $\langle b, c\rangle$ and let $\langle t, u, v, w, x\rangle$ receive.
4. Verify that $wb + xc = t = (b, c) = 1$.
5. Therefore verify that $(gw)(ab) + (gax + wbh + hxc)c = (ga + hc)(wb + xc) = 1$.
6. Now execute procedure I:41 on $\langle ab, c, 1, ab, c, gw, gax + wbh + hxc\rangle$.
7. **Therefore verify that** $(ab, c) = 1$**.**

Procedure I:48

Objective

Choose an integer a and two non-negative integers b, c such that $(a, bc) = 1$. The objective of the following instructions is to show that either $0 < 0$ or $(a, b) = 1$.

Implementation

1. Execute procedure I:36 on $\langle a, bc\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. Verify that $d = (a, bc) = 1$.
3. Verify that $ga + (hc)b = ga + h(bc) = d = 1$.
4. Now execute procedure I:41 on $\langle a, b, 1, a, b, g, hc\rangle$.
5. **Therefore verify that** $(a, b) = 1$**.**

Declaration I:16

The phrase "prime number" will be used to refer to integers a such that $a > 1$ and $a \bmod k \neq 0$ for $1 < k < a$.

Procedure I:49

Objective

Choose an integer a and a prime b such that $a \bmod b \neq 0$. The objective of the following instructions is to show that either $0 \neq 0$ or $(a, b) = 1$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle c, d, e, f, g\rangle$ receive.
2. Verify that $0 < c \leq b$.
3. If $c = b$, then do the following:
   (a) Verify that $a = cd = bd$.
   (b) Therefore verify that $a \bmod b = 0$.
   (c) **Therefore using the precondition and (3b), verify that** $0 \neq 0$**.**
   (d) **Abort procedure.**
4. Otherwise if $1 < c < b$, then do the following:
   (a) Verify that $b = ce$.
   (b) Therefore verify that $b \bmod c = 0$.
   (c) **Therefore using the precondition and (4b), verify that** $0 \neq 0$**.**
   (d) **Abort procedure.**
5. Otherwise, do the following:
   (a) **Verify that** $(a, b) = c = 1$**.**

Procedure I:50

Objective

Choose two integers a, b and a prime c such that $a \bmod c \neq 0$ and $b \bmod c \neq 0$. The objective of the following instructions is to show that either $0 \neq 0$ or $ab \bmod c \neq 0$.

Implementation

1. Execute procedure I:49 on $\langle a, c\rangle$.
2. Verify that $(a, c) = 1$.
3. Execute procedure I:49 on $\langle b, c\rangle$.

4. Verify that $(b, c) = 1$.
5. Execute procedure I:47 on $\langle a, b, c\rangle$.
6. Now verify that $0 < (ab, c) = 1 < c$.
7. Execute procedure I:40 on $\langle ab, c\rangle$.
8. **Now verify that $ab \bmod c \neq 0$.**

Declaration I:17

The notation $|a|$ will be used to refer to the number of items in the list a.

Declaration I:18

The notation $a \frown b$ will be used to refer to the list formed by concatenating a and b.

Declaration I:19

The notation $f(R)$, where R is a list and $f[r]$ is a function of r, will contextually be used as a shorthand for the list $\langle f(R_0), f(R_1), \cdots, f(R_{|R|-1})\rangle$.

Declaration I:20

The notation a_*, where a is a list, will be used as a shorthand for 1 if a is empty, otherwise it will be a shorthand for the product of the entries of a.

Declaration I:21

The notation $\prod_r^R f(r)$, where R is a list and $f[r]$ is a function of r, will be used as a shorthand for $f(R)_*$.

Procedure I:51

Objective

Choose a positive integer a. The objective of the following instructions is to construct a list of prime numbers b such that $a = b_*$.

Implementation

1. If $a = 1$, then do the following:
   (a) Verify that $a = 1 = \langle\rangle_*$.
   (b) Therefore yield $\langle\rangle$.
2. Otherwsie, do the following:
   (a) Verify that $a > 1$.
   (b) For $c = 2$ up to $c = a - 1$, do the following:
      i. If $a \bmod c = 0$, then do the following:
         A. Verify that $a = (a \operatorname{div} c)c$.
         B. Therefore verify that $1 < a \operatorname{div} c < a$.
         C. Execute procedure I:51 on $\langle a \operatorname{div} c\rangle$ and let $\langle d\rangle$ receive.
         D. Using (B) and (C), verify that $|d| > 0$.
         E. Verify that every element of d is prime.
         F. Verify that $a \operatorname{div} c = d_*$.
         G. Execute procedure I:51 on $\langle c\rangle$ and let $\langle e\rangle$ receive.
         H. Using (b) and (G), verify that $|e| > 0$.
         I. Verify that every element of e is prime.
         J. Verify that $c = e_*$.
         K. **Therefore verify that $|d \frown e| > 0$.**
         L. **Also verify that every element of $d \frown e$ is prime.**
         M. **Also verify that $a = (a \operatorname{div} c)c = d_* e_* = (d \frown e)_*$.**
         N. **Yield $\langle d \frown e\rangle$.**
   (c) Otherwise do the following:
      i. **Verify that a is prime.**
      ii. **Yield $\langle a\rangle$.**

Procedure I:52

Objective

Choose a prime a and a list of primes b such that $b_* \equiv 0 \pmod a$. The objective of the following instructions is to either show that $0 = 1$ or to construct a k such that $a = b_k$.

Implementation

1. Using declaration I:16, verify that $a > 1$.
2. If $|b| = 0$, then do the following:
   (a) Verify that $1 = b_* \equiv 0 \pmod{a}$.
   (b) **Therefore using (1) and (a), verify that $0 = 1$.**
   (c) **Abort procedure.**
3. Otherwise if $0 \notin b \bmod a$, then do the following:
   (a) Using procedure I:50, verify that $b_* \not\equiv 0 \pmod{a}$.
   (b) **Therefore using the precondition and (a), verify that $0 \neq 0$.**
   (c) **Abort procedure.**
4. Otherwise do the following:
   (a) Let k be such that $b_k \bmod a = 0$.
   (b) Verify that $b_k = (b_k \operatorname{div} a)a$.
   (c) Verify that $b_k \operatorname{div} a \geq 1$.
   (d) If $b_k \operatorname{div} a > 1$, then do the following:
      i. Using (1),(b), and (d), verify that $1 < a < b_k$.
      ii. Now, using declaration I:16 verify that $b_k \bmod a \neq 0$.
      iii. **Hence using (a) and (ii), verify that $0 \neq b_k \bmod a = 0$.**
      iv. **Abort procedure.**
   (e) Otherwise do the following:
      i. Verify that $b_k \operatorname{div} a = 1$.
      ii. **Therefore verify that $b_k = a$.**
      iii. **Yield $\langle k \rangle$.**

Declaration I:22

The notation $[a : b]$ will be used as a shorthand for the list:

1. $\langle a, a+1, \cdots, b-1 \rangle$, if $b > a$
2. $\langle \rangle$, if $b = a$
3. $\langle a-1, a-2, \cdots, b \rangle$, if $b < a$

Procedure I:53

Objective

Choose two lists of primes a, b such that $a_* = b_*$. The objective of the following instructions is to show that either $1 > 1$ or a is included in b.

Implementation

1. If $|a| = 0$, then do the following:
   (a) **Verify that a is included in b.**
2. Otherwise, do the following:
   (a) Verify that $|a| > 0$.
   (b) Verify that $b_* \equiv a_* \equiv 0 \pmod{a_0}$.
   (c) Execute procedure I:52 on $\langle a_0, b \rangle$ and let $\langle k \rangle$ receive.
   (d) Therefore verify that $b_k = a_0$.
   (e) Now verify $(a_{[1:|a|]})_* = (b_{[0:k]\frown[k+1:|b|]})_*$.
   (f) Now execute procedure I:53 on $\langle a_{[1:|a|]}, b_{[0:k]\frown[k+1:|b|]} \rangle$.
   (g) Now verify that $a_{[1:|a|]}$ is included in $b_{[0:k]\frown[k+1:|b|]} \rangle$.
   (h) **Therefore verify that a is included in b.**

Procedure I:54

Objective

Choose two lists of primes a, b such that $a_* = b_*$. The objective of the following instructions is to show that either $1 > 1$ or a is a rearrangement of b.

Implementation

1. Execute procedure I:53 on $\langle a, b \rangle$.
2. Verify that a is included in b.
3. Execute procedure I:53 on $\langle b, a \rangle$.
4. Verify that b is included in a.
5. **Therefore verify that a is a rearrangement of b.**

Procedure I:55

Objective

Choose a positive integer a. The objective of the following instructions is to either show that $0 = 1$ or to construct a prime b such that $b > a$ and $[a+1 : b]$ does not contain a prime.

Implementation

1. Verify that $a! + 1 > 1$.
2. Execute procedure I:51 on $\langle a! + 1\rangle$ and let $\langle d\rangle$ receive.
3. Therefore using (1) and (2), verify that $|d| > 0$.
4. Now verify that $(a! + 1) \bmod d_0 = 0$.
5. For $e = 2$ up to $e = a$, do the following:
   (a) Verify that $a! + 1 \equiv 1 \pmod e$.
   (b) If $e = d_0$, then do the following:
      i. Using (4) and (a), verify that $0 \equiv a! + 1 \equiv 1 \pmod{e = d_0}$.
      ii. **Therefore verify that $0 = 1$.**
      iii. **Abort procedure.**
6. Otherwise do the following:
   (a) **Using (2), verify that d_0 is prime.**
   (b) Using (a), verify that $d_0 > 1$.
   (c) **Using (a) and (5), verify that $d_0 > a$.**
   (d) **Let b be the least prime between $a + 1$ and d_0.**
   (e) **Yield $\langle b\rangle$.**

Procedure I:56

Objective

Choose a positive integer a. The objective of the following instructions is to construct a positive integer b such that $[b + 1 : b + a]$ does not contain a prime.

Implementation

1. Let $b = a! + 1$.
2. For $i = 1$ up to $i = a - 1$, do the following:
   (a) Verify that $b + i = a! + 1 + i = i!(i + 1)(i + 2)\cdots(a) + 1 + i = (1 + i)(i!(i + 2)(i + 3)\cdots(a) + 1)$.
   (b) Therefore verify that $b + i \equiv 0 \pmod{i + 1}$.
   (c) Also verify that $b + i = a! + 1 + i > a! \geq a \geq i + 1 > 1$.
   (d) **Therefore verify that $b+i$ is not prime.**
3. **Yield $\langle b\rangle$.**

Procedure I:57

Objective

Choose two lists of primes a, b in such a way that their intersection is empty. The objective of the following instructions is to show that $0 = 1$ or $(a_*, b_*) = 1$.

Implementation

1. Execute procedure I:36 on $\langle a_*, b_*\rangle$ and let $\langle c, d, e, f, g\rangle$.
2. Verify that $0 < c \leq b\rangle$.
3. If $c > 1$, then do the following:
   (a) Execute procedure I:51 on $\langle c\rangle$ and let $\langle h\rangle$ receive.
   (b) Using (3) and (a), verify that $|h| > 0$.
   (c) Now verify that $a_* = dc = dh_* = dh_0(h_{[1:|h|]})_* \equiv 0 \pmod{h_0}$.
   (d) Execute procedure I:52 on $\langle h_0, a\rangle$ and let $\langle k\rangle$ receive.
   (e) Now verify that $b_* = ec = eh_* = eh_0(h_{[1:|h|]})_* \equiv 0 \pmod{h_0}$.
   (f) Execute procedure I:52 on $\langle h_0, b\rangle$ and let $\langle m\rangle$ receive.
   (g) **Therefore verify that $a_k = h_0 = b_m$.**
   (h) **Abort procedure.**

4. Otherwise do the following:
   (a) **Verify that** $(a_*, b_*) = c = 1$**.**

Procedure I:58

Objective

Choose two lists of primes a, b. Let c be the common sublist with multiplicity of a and b. The objective of the following instructions is to show that either $0 < 0$ or $(a_*, b_*) = c_*$.

Implementation

1. Let d be the result of removing with multiplicity elements of c from a.
2. Verify that $a_* = c_* d_*$.
3. Let e be the result of removing with multiplicity elements of c from b.
4. Verify that $b_* = c_* e_*$.
5. Verify that d and e share no common elements.
6. **Therefore using procedure I:45 and procedure I:57, verify that** $(a_*, b_*) = (c_* d_*, c_* e_*) = c_*(d_*, e_*) = c_*$**.**

Procedure I:59

Objective

Choose an integer a and a positive integer b. The objective of the following instructions is to construct integers c, f, e such that $c = af$, $c = be$, $c(a, b) = ab$, and $|a| \leq c\,\mathrm{sgn}(a) \leq |a|b$.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle d, e, f, g, h\rangle$ receive.
2. **Let** $c = af$**.**
3. **Verify that** $c(a, b) = cd = afd = ab$**.**
4. Verify that $d > 0$.
5. Verify that $b = fd$.
6. Therefore verify that $1 \leq f \leq b$.
7. Therefore verify that $|a| \leq |a|f \leq |a|b$.
8. **Therefore verify that** $|a| \leq c\,\mathrm{sgn}(a) \leq |a|b$**.**
9. **Verify that** $c = af = def = be$**.**
10. **Yield the tuple** $\langle c, f, e\rangle$**.**

Declaration I:23

The notation $[a, b]$ will be used to refer to the first part of the triple yielded by executing procedure I:59 on $\langle a, b\rangle$.

Procedure I:60

Objective

Choose two positive integers a, b. The objective of the following instructions is to show that either $0 < 0$ or $[a, b] = [b, a]$.

Implementation

1. Verify that $(a, b) > 0$.
2. Using procedure I:43, verify that $[a, b](a, b) = ab = ba = [b, a](b, a) = [b, a](a, b)$.
3. **Therefore verify that** $[a, b] = [b, a]$**.**

Procedure I:61

Objective

Choose an integer a and two positive integers b, c. The objective of the following instructions is to show that either $0 < 0$ or $[ca, cb] = c[a, b]$.

Implementation

1. Verify that $(ca, cb) > 0$.
2. Using procedure I:45, verify that $[ca, cb](ca, cb) = cacb = c^2ab = c^2[a, b](a, b) = c[a, b](ca, cb)$.
3. **Therefore verify that** $[ca, cb] = c[a, b]$**.**

Procedure I:62

Objective

Choose an integer a and two positive integers b, c. The objective of the following instructions is to show that either $0 < 0$ or $[[a, b], c] = [a, [b, c]]$.

Implementation

1. Using procedure I:46, verify that $(a, b)(ab, (ac, bc))(b, c)[[a, b], c]$
   (a) $= (ab, (ac, bc))(b, c)[(a, b)[a, b], (a, b)c]$
   (b) $= (ab, (ac, bc))(b, c)[ab, (ac, bc)]$
   (c) $= ab(ac, bc)(b, c)$
   (d) $= abc(a, b)(b, c)$
   (e) $= bc(a, b)(ab, ac)$
   (f) $= (a, b)((ab, ac), bc)[(ab, ac), bc]$
   (g) $= (a, b)(ab, (ac, bc))[(ab, ac), bc]$
   (h) $= (a, b)(ab, (ac, bc))[a(b, c), [b, c](b, c)]$
   (i) $= (a, b)(ab, (ac, bc))(b, c)[a, [b, c]]$.
2. Verify that $(a, b)(ab, (ac, bc))(b, c) > 0$.
3. **Therefore verify that** $[[a, b], c] = [a, [b, c]]$**.**

Declaration I:24

The notation $[a_0, a_1, \cdots, a_{n-1}]$ will be used to contextually refer to one of the following integers:

1. $[[a_0], [a_1, a_2, \cdots, a_{n-1}]]$
2. $[[a_0, a_1], [a_2, a_3, \cdots, a_{n-1}]]$
3. $\vdots$
4. $[[a_0, a_1, \cdots, a_{n-2}], [a_{n-1}]]$

Procedure I:63

Objective

Choose three positive integers a, b, c. The objective of the following instructions is to show that either $0 < 0$ or $([a, b], c) = [(a, c), (b, c)]$.

Implementation

1. Using procedure I:59, procedure I:45, procedure I:46, procedure I:43, and procedure I:37, verify that $(a, b)((a, c), (b, c))([a, b], c)$
   (a) $= ((a, c), (b, c))((a, b)[a, b], (a, b)c)$
   (b) $= ((a, c), (b, c))(ab, (ac, bc))$
   (c) $= (a^2b, a^2c, c^2a, c^2b, b^2a, bac, b^2c)$
   (d) $= (a, b)(ab, ac, bc, c^2)$
   (e) $= (a, b)(a, c)(b, c)$
   (f) $= (a, b)((a, c), (b, c))[(a, c), (b, c)]$.
2. Verify that $(a, b)((a, c), (b, c)) > 0$.
3. **Therefore verify that** $([a, b], c) = [(a, c), (b, c)]$**.**

Procedure I:64

Objective

Choose three positive integers a, b, c. The objective of the following instructions is to show that either $0 < 0$ or $[(a, b), c] = ([a, c], [b, c])$.

Implementation

1. Using procedure I:59, procedure I:45, procedure I:46, procedure I:43, and procedure I:37, verify that $((a, b), c)(a, c)(b, c)[(a, b), c]$
   (a) $= (a, c)(b, c)(a, b)c$
   (b) $= (ab, ac, cb, c^2)(a, b)c$
   (c) $= (a^2b, a^2c, ac^2, ab^2, abc, cb^2, bc^2)c$
   (d) $= (a, b, c)(ab, ac, bc)c$
   (e) $= ((a, b), c)(ac(b, c), bc(a, c))$
   (f) $= ((a, b), c)(a, c)(b, c)([a, c], [b, c])$.
2. Verify that $((a, b), c)(a, c)(b, c) > 0$.
3. **Therefore verify that** $[(a, b), c] = ([a, c], [b, c])$**.**

Declaration I:25

The notation $\chi_{b,d}(a,c)$, where a, c are two integers and b, d are two positive integers such that $a \equiv c \pmod{(b,d)}$, will be used to refer to the result yielded by executing the following instructions:

1. Execute procedure I:36 on $\langle b, d\rangle$ and let $\langle f, g, h, i, j\rangle$ receive.
2. **Yield the tuple** $\langle (a + ((c - a)\operatorname{div}(b, d))ib) \bmod [b, d]\rangle$**.**

Procedure I:65

Objective

Choose three integers x, a, c and two positive integers b, d such that $x \equiv a \pmod{b}$ and $x \equiv c \pmod{d}$. The objective of the following instructions is to show that $0 \neq 0$ if $a \not\equiv d \pmod{(b,d)}$, otherwise $x \equiv \chi_{b,d}(a,c) \pmod{[b,d]}$.

Implementation

1. Execute procedure I:36 on $\langle b, d\rangle$ and let $\langle e, f, g, h, i\rangle$ receive.
2. Let $j = x \operatorname{div} b - a \operatorname{div} b$.
3. Verify that $x = a + jb$.
4. Let $k = x \operatorname{div} d - c \operatorname{div} d$.
5. Verify that $x = c + kd$.
6. Therefore verify that $c - a = jb - kd$.
7. If $a \not\equiv c \pmod{(b,d)}$, then do the following:
   (a) Verify that $0 \not\equiv d - a = jb - kd = jef - keg \equiv 0 \pmod{e}$.
   (b) **Therefore verify that** $0 \neq 0$**.**
   (c) **Abort procedure.**
8. Otherwise do the following:
   (a) Verify that $c - a \equiv 0 \pmod{(b,d)}$.
   (b) Let $l = (c - a)\operatorname{div}(b, d)$.
   (c) Verify that $l(b, d) = le = c - a = jb - kd = jef - keg$.
   (d) Therefore verify that $l = jf - kg$.
   (e) Therefore verify that $l \equiv jf \pmod{g}$.
   (f) Also, using (1) verify that $efh + egi = bh + di = e$.
   (g) Therefore verify that $fh + gi = 1$.
   (h) Therefore verify that $fh \equiv 1 \pmod{g}$.
   (i) Therefore verify that $lh \equiv jfh \equiv j \pmod{g}$.
   (j) Therefore using procedure I:32, verify that $lhb \equiv jb \pmod{bg = [b,d]}$.
   (k) **Therefore verify that** $x \equiv a + jb \equiv a + lhb \equiv \chi_{b,d}(a,c) \pmod{[b,d]}$**.**

Procedure I:66

Objective

Choose two integers a, c and two positive integers b, d in such a way that $a \equiv c \pmod{(b,d)}$. The objective of the following instructions is to show that either $0 < 0$ or $\chi_{b,d}(a,c) = \chi_{d,b}(c,a)$.

Implementation

1. Execute procedure I:36 on $\langle b, d\rangle$ and let $\langle f, g, h, i, j\rangle$ receive.
2. Verify that $ib + jd = f = (b, d)$.
3. Execute procedure I:36 on $\langle d, b\rangle$ and let $\langle k, l, m, n, p\rangle$ receive.
4. Verify that $pb + nd = k = (d, b) = (b, d)$.
5. Execute procedure I:39 on $\langle b, p, n, d\rangle$ and let $\langle q\rangle$ receive.
6. Therefore verify that $n = j - qg$.
7. Now using procedure I:60, verify that $\chi_{b,d}(a, c)$
   (a) $= (a + ((c - a)\operatorname{div}(b, d))ib) \bmod [b, d]$
   (b) $= (a + ((c - a)\operatorname{div}(b, d))(f - jd)) \bmod [b, d]$
   (c) $= (a + ((c - a)\operatorname{div}(b, d))f + ((a - c)\operatorname{div}(b, d))jd) \bmod [b, d]$
   (d) $= (a+(c-a)+((a-c)\operatorname{div}(b, d))jd) \bmod [b, d]$
   (e) $= (c + ((a - c)\operatorname{div}(d, b))(n + qg)d) \bmod [b, d]$
   (f) $= (c + ((a - c)\operatorname{div}(d, b))dn + ((a - c)\operatorname{div}(d, b))q[b, d]) \bmod [b, d]$

(g) $= (c + ((a - c)\operatorname{div}(d, b))dn) \bmod [b, d]$

(h) $= (c + ((a - c)\operatorname{div}(d, b))dn) \bmod [d, b]$

(i) $= \chi_{d,b}(c, a)$.

Procedure I:67

Objective

Choose three integers x, a, c and two positive integers b, d such that $a \equiv c \pmod{(b, d)}$ and $x \equiv \chi_{b,d}(a, c) \pmod{[b, d]}$. The objective of the following instructions is to show that $x \equiv a \pmod{b}$.

Implementation

1. Execute procedure I:36 on $\langle b, d\rangle$ and let $\langle e, f, g, h, i\rangle$.
2. Verify that $x \bmod [b, d] = \chi_{b,d}(a, c) \bmod [b, d]$.
3. Therefore verify that $x \bmod (bg) = \chi_{b,d}(a, c) \bmod (bg)$.
4. Therefore verify that $(x \bmod (bg)) \bmod b = (\chi_{b,d}(a, c) \bmod (bg)) \bmod b$.
5. **Therefore using procedure I:30, verify that $x \bmod b = \chi_{b,d}(a, c) \bmod b = (a + ((c - a)\operatorname{div}(b, d))hb) \bmod b = a \bmod b$.**

Procedure I:68

Objective

Choose three integers x, a, c and two positive integers b, d such that $a \equiv c \pmod{(b, d)}$ and $x \equiv \chi_{b,d}(a, c) \pmod{[b, d]}$. The objective of the following instructions is to either show that $0 < 0$ or to show that $x \equiv a \pmod{b}$ and $x \equiv c \pmod{d}$.

Implementation

1. Execute procedure I:67 on $\langle x, a, c, b, d\rangle$.
2. **Therefore verify that $x \equiv a \pmod{b}$.**
3. Now using procedure I:66, verify that $x \equiv \chi_{b,d}(a, c) \equiv \chi_{d,b}(c, a) \pmod{[d, b]}$
4. Execute procedure I:67 on $\langle x, c, a, d, b\rangle$.
5. **Therefore verify that $x \equiv c \pmod{d}$.**

Procedure I:69

Objective

Choose two integers a, c and three positive integers b, d, e such that $a \equiv c \pmod{(b, d)}$. The objective of the following instructions is to show that $\chi_{b,d}(ea, ec) = e\chi_{b,d}(a, c)$.

Implementation

1. Verify that $\chi_{b,d}(a, c) \equiv a \pmod{b}$.
2. Therefore using procedure I:32, verify that $e\chi_{b,d}(a, c) \equiv ea \pmod{b}$.
3. Verify that $\chi_{b,d}(a, c) \equiv c \pmod{d}$.
4. Therefore using procedure I:32, verify that $e\chi_{b,d}(a, c) \equiv ec \pmod{d}$.
5. Also using procedure I:29 and the precondition, verify that $ea \equiv ec \pmod{(b, d)}$.
6. Therefore using procedure I:65, verify that $e\chi_{b,d}(a, c) \equiv \chi_{b,d}(ea, ec) \pmod{[b, d]}$.
7. **Therefore verify that $e\chi_{b,d}(a, c) = \chi_{b,d}(ea, ec)$.**

Procedure I:70

Objective

Choose two integers a, c and three positive integers b, d, e such that $a \equiv c \pmod{(eb, ed)}$. The objective of the following instructions is to show that $\chi_{eb,ed}(a, c) \bmod [b, d] = \chi_{b,d}(a, c)$.

Implementation

1. Verify that $\chi_{eb,ed}(a, c) \equiv a \pmod{eb}$.
2. Therefore using procedure I:30, verify that $\chi_{eb,ed}(a, c) \equiv a \pmod{b}$.
3. Verify that $\chi_{eb,ed}(a, c) \equiv c \pmod{ed}$.
4. Therefore using procedure I:30, verify that $\chi_{eb,ed}(a, c) \equiv c \pmod{d}$.

5. Now verify that $a \equiv c \pmod{e(b, d)}$.

6. Therefore using procedure I:30, verify that $a \equiv c \pmod{(b, d)}$.

7. Therefore using procedure I:65, verify that $\chi_{eb,ed}(a, c) \equiv \chi_{b,d}(a, c) \pmod{[b, d]}$.

8. **Therefore verify that** $\chi_{eb,ed}(a, c) \bmod [b, d] = \chi_{b,d}(a, c)$**.**

Procedure I:71

Objective

Choose three integers a, c, e and three positive integers b, d, f such that $a \equiv e \pmod{(b, f)}$, and $c \equiv e \pmod{(d, f)}$. The objective of the following instructions is to show that either $0 < 0$ or $\chi_{b,d}(a, c) \equiv e \pmod{([b, d], f)}$.

Implementation

1. Execute procedure I:36 on $\langle b, f \rangle$ and let $\langle g_0, h_0, i_0, j_0, k_0 \rangle$ receive.

2. Execute procedure I:36 on $\langle d, f \rangle$ and let $\langle g_1, h_1, i_1, j_1, k_1 \rangle$ receive.

3. Verify that $e \equiv a \pmod{(b, f)}$.

4. Verify that $e \equiv c \pmod{(d, f)}$.

5. Therefore using procedure I:65 and procedure I:70, verify that e

   (a) $\equiv \chi_{(b,f),(d,f)}(a, c)$

   (b) $\equiv \chi_{(b,f)h_1,(d,f)h_2}(a, c)$

   (c) $= \chi_{b,d}(a, c) \pmod{[(b, f), (d, f)]}$.

6. **Therefore using procedure I:63, verify that** $e \equiv \chi_{b,d}(a, c) \pmod{([b, d], f)}$**.**

Procedure I:72

Objective

Choose three integers a, c, e and three positive integers b, d, f such that $a \equiv c \pmod{(b, d)}$, $a \equiv e \pmod{(b, f)}$, and $c \equiv e \pmod{(d, f)}$. Execute procedure I:71 on $\langle a, c, e, b, d, f \rangle$. Execute procedure I:71 on $\langle c, e, a, d, f, b \rangle$. The objective of the following instructions is to show that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) = \chi_{b,[d,f]}(a, \chi_{d,f}(c, e))$.

Implementation

1. Verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv e \pmod{f}$.

2. Verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv \chi_{b,d}(a, c) \pmod{[b, d] = gb = hd}$.

3. Therefore using procedure I:30, verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv \chi_{b,d}(a, c) \equiv a \pmod{b}$.

4. Also using procedure I:30, verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv \chi_{b,d}(a, c) \equiv c \pmod{d}$.

5. Therefore using (1), (4), and procedure I:65, verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv \chi_{d,f}(c, e) \pmod{[d, f]}$.

6. Therefore using (3), (5), and procedure I:65, verify that $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) \equiv \chi_{b,[d,f]}(a, \chi_{d,f}(c, e)) \pmod{[b, [d, f]] = [[b, d], f]}$.

7. **Therefore verify that** $\chi_{[b,d],f}(\chi_{b,d}(a, c), e) = \chi_{b,[d,f]}(a, \chi_{d,f}(c, e))$**.**

Declaration I:26

The notation $\chi_{b_0,b_1,\cdots,b_{n-1}}(a_0, a_1, \cdots, a_{n-1})$ will be used to contextually refer to one of the following integers:

1. $\chi_{b_0,[b_1,b_2,\cdots,b_{n-1}]}(a_0, \chi_{b_1,b_2,\cdots,b_{n-1}}(a_1, a_2, \cdots, a_{n-1}))$

2. $\chi_{[b_0,b_1],[b_2,b_3,\cdots,b_{n-1}]}(\chi_{b_0,b_1}(a_0, a_1), \chi_{b_2,b_3,\cdots,b_{n-1}}(a_2, a_3, \cdots, a_{n-1})$

3. $\vdots$

4. $\chi_{[b_0,b_1,\cdots,b_{n-2}],b_{n-1}}(\chi_{b_0,b_1,\cdots,b_{n-2}}(a_0, a_1, \cdots, a_{n-2}), a_{n-1})$

Declaration I:27

The notation $\phi(n)$ will be used as a shorthand for the sublist of $[0 : n]$ where each entry x is such that $(x, n) = 1$.

Procedure I:73

Objective

Choose an integer a and a positive integer b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that each element of $a\phi(b) \bmod b$ is in $\phi(b)$.

Implementation

1. Verify that $(a, b) = 1$.
2. For i in $[0 : |\phi(b)|]$, do the following:
   (a) Using declaration I:27, verify that $(\phi(b)_i, b) = 1$.
   (b) Execute procedure I:47 on $\langle a, \phi(b)_i, b\rangle$.
   (c) Therefore verify that $(a\phi(b)_i, b) = 1$.
   (d) Execute procedure I:44 on $\langle a\phi(b)_i \bmod b, a\phi(b)_i, b\rangle$.
   (e) Therefore verify that $(a\phi(b)_i \bmod b, b) = (a\phi(b)_i, b) = 1$.
   (f) Also verify that $0 \leq a\phi(b)_i \bmod b < b$.
   (g) Therefore verify that $a\phi(b)_i \bmod b$ is contained in the list $\phi(b)$.
3. **Therefore verify that each element of** $a\phi(b) \bmod b$ **is in** $\phi(b)$**.**

Procedure I:74

Objective

Choose an integer a and a positive integer b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 \neq 0$ or to show that each element of $a\phi(b) \bmod b$ is distinct.

Implementation

1. Execute procedure I:36 on $\langle a, b\rangle$ and let $\langle r, t, u, v, w\rangle$ receive.
2. Verify that $va + wb = r = (a, b) = 1$.
3. Therefore verify that $va \equiv 1 \pmod b$.
4. Now for i in $[0 : |\phi(b)|]$, do the following:
   (a) For j in $[i + 1 : |\phi(b)|]$, do the following:
      i. If $a\phi(b)_i \equiv a\phi(b)_j \pmod b$, then do the following:
         A. Verify that $\phi(b)_i \equiv va\phi(b)_i \equiv va\phi(b)_j \equiv \phi(b)_j \pmod b$.
         B. Therefore verify that $\phi(b)_i = \phi(b)_j$.
         C. Also verify that $i \neq j$.
         D. Therefore using declaration I:27, verify that $\phi(b)_i \neq \phi(b)_j$.
         E. **Therefore using (B) and (D), verify that** $\phi(b)_i \neq \phi(b)_i$**.**
         F. **Abort procedure.**
      ii. Otherwise, do the following:
         A. Verify that $a\phi(b)_i \not\equiv a\phi(b)_j \pmod b$.
5. **Therefore verify that** $a\phi(b) \bmod b$ **is composed of distinct elements.**

Procedure I:75

Objective

Choose an integer a and a positive integer b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that $a\phi(b) \bmod b$ is a rearrangement of $\phi(b)$.

Implementation

1. Execute procedure I:73 on $\langle a, b\rangle$.
2. Therefore verify that each element of $a\phi(b) \bmod b$ is in $\phi(b)$.
3. Verify that $|a\phi(b) \bmod b| = |\phi(b)|$.
4. Execute procedure I:74 on $\langle a, b\rangle$.
5. Therefore verify that $a\phi(b) \bmod b$ is composed of distinct elements.
6. **Therefore verify that** $a\phi(b) \bmod b$ **is a rearrangement of** $\phi(b)$**.**

Procedure I:76

Objective

Choose an integer a and a positive integer b such that $(a, b) = 1$. The objective of the following instructions is to show that either $0 < 0$ or $a^{|\phi(b)|} \equiv 1 \pmod{b}$.

Implementation

1. For i in $[0 : |\phi(b)|]$, do the following:
   (a) Execute procedure I:36 on $\langle \phi(b)_i, b\rangle$ and let $\langle r_i, t_i, u_i, v_i, w_i\rangle$.
   (b) Using declaration I:27, verify that $v_i\phi(b)_i + w_ib = r_i = (\phi(b)_i, b) = 1$.
   (c) Therefore verify that $v_i\phi(b)_i \equiv 1 \pmod{b}$.
2. Therefore using procedure I:75, verify that $\prod_i^{[0:|\phi(b)|]} \phi(b)_i \equiv \prod_i^{[0:|\phi(b)|]} a\phi(b)_i \equiv a^{|\phi(b)|} \prod_i^{[0:|\phi(b)|]} \phi(b)_i \pmod{b}$.
3. **Therefore verify that** $1 \equiv \prod_i^{[0:|\phi(b)|]}(v_i\phi(b)_i) = \prod_i^{[0:|\phi(b)|]} v_i \prod_i^{[0:|\phi(b)|]} \phi(b)_i \equiv a^{|\phi(b)|} \prod_i^{[0:|\phi(b)|]} \phi(b)_i \prod_i^{[0:|\phi(b)|]} v_i \equiv a^{|\phi(b)|} \pmod{b}$**.**

Declaration I:28

The notation $a \times b$ as a shorthand for the $|a| \times |b|$ matrix such that for i in $[0 : |a|]$, for j in $[0 : |b|]$, $(a \times b)_{i,j} = \langle a_i, b_j\rangle$.

Procedure I:77

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to show that each entry of $\chi_{a,b}([0 : a] \times [0 : b])$ is in $[0 : ab]$.

Implementation

1. Let $h = \chi_{a,b}([0 : a] \times [0 : b])$.
2. Therefore verify that $0 \leq h_{i,j} < [a, b] = [a, b](a, b) = ab$ for i in $[0 : a]$, for j in $[0 : b]$.
3. **Therefore verify that each entry of h is in $[0 : ab]$.**

Procedure I:78

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that each entry of $\chi_{a,b}([0 : a] \times [0 : b])$ is distinct.

Implementation

1. Let $h = \chi_{a,b}([0 : a] \times [0 : b])$.
2. For each distinct unordered pair of index pairs $\langle i, j\rangle$ and $\langle k, l\rangle$ of h, do the following:
   (a) If $h_{i,j} = h_{k,l}$, then do the following:
      i. Verify that $\chi_{a,b}([0 : a]_i, [0 : b]_j) = h_{i,j} = h_{k,l} = \chi_{a,b}([0 : a]_k, [0 : b]_l)$.
      ii. Verify that $\chi_{a,b}(i, j) = \chi_{a,b}(k, l)$.
      iii. Therefore using procedure I:68, verify that $i \equiv \chi_{a,b}(i, j) = \chi_{a,b}(k, l) \equiv k \pmod{a}$.
      iv. Therefore verify that $i = k$.
      v. Also using procedure I:68, verify that $j \equiv \chi_{a,b}(i, j) = \chi_{a,b}(k, l) \equiv l \pmod{b}$.
      vi. Therefore verify that $j = l$.
      vii. Therefore verify that $\langle i, j\rangle = \langle k, l\rangle$.
      viii. Using (2), verify that $\langle i, j\rangle \neq \langle k, l\rangle$.
      ix. **Therefore verify that $\langle i, j\rangle \neq \langle i, j\rangle$.**
      x. **Abort procedure.**
   (b) Otherwise do the following:
      i. Verify that $h_{i,j} \neq h_{k,l}$.
3. **Therefore verify that each entry of h is distinct.**

Procedure I:79

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to show that either $0 < 0$ or $\chi_{a,b}([0 : a] \times [0 : b])$ is a rearrangement $[0 : ab]$.

Implementation

1. Let $h = \chi_{a,b}([0 : a] \times [0 : b])$.
2. Execute procedure I:77 on $\langle a, b\rangle$.
3. Therefore verify that each element of h is in $[0 : ab]$.
4. Also verify that h has the same number of entries as $[0 : ab]$.
5. Execute procedure I:78 on $\langle a, b\rangle$.
6. Therefore verify that h is composed of distinct elements.
7. **Therefore verify that h is a rearrangement of $[0 : ab]$.**

Procedure I:80

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that each entry of $\chi_{a,b}(\phi(a) \times \phi(b))$ is in $\phi(ab)$.

Implementation

1. Let $h = \chi_{a,b}(\phi(a) \times \phi(b))$.
2. Now, for each index pair $\langle i, j\rangle$ of h, do the following:

(a) Verify that $0 \le h_{i,j} < [a, b] = [a, b](a, b) = ab$.

(b) Verify that $h_{i,j} = \chi_{a,b}(\phi(a)_i, \phi(b)_j) \equiv \phi(a)_i \pmod a$.

(c) Execute procedure I:44 on $\langle h_{i,j}, \phi(a)_i, a\rangle$.

(d) Therefore verify that $(a, h_{i,j}) = (h_{i,j}, a) = (\phi(a)_i, a) = 1$.

(e) Verify that $h_{i,j} = \chi_{a,b}(\phi(a)_i, \phi(b)_j) \equiv \phi(b)_j \pmod b$.

(f) Execute procedure I:44 on $\langle h_{i,j}, \phi(b)_j, b\rangle$.

(g) Therefore verify that $(b, h_{i,j}) = (h_{i,j}, b) = (\phi(b)_j, b) = 1$.

(h) Therefore verify that $(h_{i,j}, ab) = (ab, h_{i,j}) = 1$.

(i) Therefore verify that $h_{i,j}$ is in $\phi(ab)$.

3. **Therefore verify that each entry of $\chi_{a,b}(\phi(a) \times \phi(b))$ is in $\phi(ab)$.**

Procedure I:81

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that each entry of $\phi(ab)$ is in $\chi_{a,b}(\phi(a) \times \phi(b))$.

Implementation

1. For i in $[0 : |\phi(ab)|]$, do the following:

(a) Verify that $(\phi(ab)_i, ab) = 1$.

(b) Verify that $\phi(ab)_i \equiv \phi(ab)_i \bmod a \pmod a$.

(c) Therefore using procedure I:44, verify that $(\phi(ab)_i \bmod a, a) = (\phi(ab)_i, a) = 1$.

(d) Also verify that $0 \le \phi(ab)_i \bmod a < a$.

(e) Therefore verify that $\phi(ab)_i \bmod a$ is amongst $\phi(a)$.

(f) Verify that $\phi(ab)_i \equiv \phi(ab)_i \bmod b \pmod b$.

(g) Also using procedure I:44, verify that $(\phi(ab)_i \bmod b, b) = (\phi(ab)_i, b) = 1$.

(h) Also verify that $0 \le \phi(ab)_i \bmod b < b$.

(i) Therefore verify that $\phi(ab)_i \bmod b$ is amongst $\phi(b)$.

(j) Therefore verify that $\langle \phi(ab)_i \bmod a, \phi(ab)_i \bmod b\rangle$ is amongst $\phi(a) \times \phi(b)$.

(k) Also using (b) and (f) and procedure I:65, verify that $\phi(ab)_i \equiv \chi_{a,b}(\phi(ab)_i \bmod a, \phi(ab)_i \bmod b) \pmod{[a, b] = [a, b](a, b) = ab}$.

(l) Therefore verify that $\phi(ab)_i = \chi_{a,b}(\phi(ab)_i \bmod a, \phi(ab)_i \bmod b)$.

(m) Therefore using (j) and (l), verify that $\phi(ab)_i$ is amongst $\chi_{a,b}(\phi(a) \times \phi(b))$.

2. **Therefore verify that each entry of $\phi(ab)$ is in $\chi_{a,b}(\phi(a) \times \phi(b))$.**

Procedure I:82

Objective

Choose two positive integers a, b such that $(a, b) = 1$. The objective of the following instructions is to either show that $0 < 0$ or to show that $\phi(ab)$ is a rearrangement of $\chi_{a,b}(\phi(a) \times \phi(b))$ and that $|\phi(ab)| = |\phi(a)||\phi(b)|$.

Implementation

1. Execute procedure I:79 on $\langle a, b\rangle$.
2. Therefore verify that $\chi_{a,b}([0 : a] \times [0 : b])$ are a rearrangement of $[0 : ab]$.
3. Verify that $\chi_{a,b}(\phi(a) \times \phi(b))$ is a submatrix of $\chi_{a,b}([0 : a] \times [0 : b])$.
4. Therefore verify that the entries of $\chi_{a,b}(\phi(a) \times \phi(b))$ are distinct.
5. Execute procedure I:80 on $\langle a, b\rangle$.
6. Therefore verify that the entries of $\chi_{a,b}(\phi(a) \times \phi(b))$ are in $\phi(ab)$.
7. Verify that that the entries of $\phi(ab)$ are distinct.
8. Execute procedure I:81 on $\langle a, b\rangle$.
9. Therefore verify that the entries of $\phi(ab)$ are in $\chi_{a,b}(\phi(a) \times \phi(b))$.
10. **Therefore verify that $\phi(ab)$ is a rearrangement of $\chi_{a,b}(\phi(a) \times \phi(b))$.**
11. **Therefore verify that $|\phi(ab)| = |\chi_{a,b}(\phi(a) \times \phi(b))| = |\phi(a) \times \phi(b)| = |\phi(a)||\phi(b)|$.**

Declaration I:29

The notation $[P]$, where P is a condition, will be used as a shorthand for 1 if P, otherwise it will stand for 0.

Declaration I:30

The notation a_+, where a is a list, will be used as a shorthand for 0 if a is empty, otherwise it will be a shorthand for the sum of the entries of a.

Declaration I:31

The notation $\sum_r^R f(r)$, where R is a list and $f[r]$ is a function of r, will be used as a shorthand for $f(R)_+$.

Procedure I:83

Objective

Choose a positive integer a and a prime b. The objective of the following instructions is to show that either $0 < 0$ or $|\phi(b^a)| = b^a - b^{a-1}$.

Implementation

1. Using procedure I:48, verify that $\sum_r^{[0:b^a]}[(r, b^a) = 1] \leq \sum_r^{[0:b^a]}[(r, b) = 1]$.
2. Using procedure I:47, verify that $\sum_r^{[0:b^a]}[(r, b) = 1] \leq \sum_r^{[0:b^a]}[(r, b^a) = 1]$.
3. Therefore verify that $\sum_r^{[0:b^a]}[(r, b^a) = 1] = \sum_r^{[0:b^a]}[(r, b) = 1]$.
4. Using procedure I:40, verify that $\sum_r^{[0:b^a]}[(r, b) = 1] \leq \sum_r^{[0:b^a]}[r \bmod b \neq 0]$.
5. Using procedure I:49, verify that $\sum_r^{[0:b^a]}[r \bmod b \neq 0] \leq \sum_r^{[0:b^a]}[(r, b) = 1]$.
6. Therefore verify that $\sum_r^{[0:b^a]}[(r, b) = 1] = \sum_r^{[0:b^a]}[r \bmod b \neq 0]$.
7. **Therefore using (3) and (6), verify that $|\phi(b^a)| = \sum_r^{[0:b^a]}[(r, b^a) = 1] = \sum_r^{[0:b^a]}[(r, b) = 1] = \sum_r^{[0:b^a]}[r \bmod b \neq 0] = \sum_r^{[0:b^a]}(1 - [r \bmod b = 0]) = b^a - b^{a-1}$.**

Procedure I:84

Objective

Choose a list of primes a. Let b be the list of distinct primes in a. Let c be a list such that c_i is the multiplicity of b_i in a for $i = 1$ to $i = |b|$. The objective of the following instructions is to show that either $0 < 0$ or $|\phi(a_*)| = \prod_i^{[0:|b|]}({b_i}^{c_i} - {b_i}^{c_i-1})$.

Implementation

1. If $a = \langle\rangle$, then do the following:
   (a) Verify that $|b| = |a| = 0$.
   (b) **Therefore verify that** $\phi(a_*) = \phi(1) = 1 = \prod_i^{[0:|b|]}({b_i}^{c_i} - {b_i}^{c_i-1})$**.**
2. Otherwise, do the following:
   (a) Verify that $a_* = \prod_i^{[0:|b|]} {b_i}^{c_i}$.
   (b) Verify that $|a| > 0$.
   (c) Therefore verify that $|c| = |b| > 0$.
   (d) Therefore using procedure I:57, verify that $({b_0}^{c_0}, \prod_i^{[1:|b|]} {b_i}^{c_i}) = 1$.
   (e) Let d be the list a with all instances of a_0 removed.
   (f) Verify that $|d| < |a|$.
   (g) Now execute procedure I:84 on $\langle d\rangle$.
   (h) Hence verify that $\phi(d_*) = \phi(\prod_i^{[1:|b|]} {b_i}^{c_i}) = \prod_i^{[1:|b|]}({b_i}^{c_i} - {b_i}^{c_i-1})$.
   (i) **Therefore using (d), (h), procedure I:82 and procedure I:83, verify that** $|\phi(a_*)| = |\phi(\prod_i^{[0:|b|]} {b_i}^{c_i})| = |\phi({b_0}^{c_0} \prod_i^{[1:|b|]} {b_i}^{c_i})| = |\phi({b_0}^{c_0})||\phi(\prod_i^{[1:|b|]} {b_i}^{c_i})| = ({b_0}^{c_0} - {b_0}^{c_0-1})|\phi(\prod_i^{[1:|b|]} {b_i}^{c_i})| = ({b_0}^{c_0} - {b_0}^{c_0-1}) \prod_i^{[1:|b|]}({b_i}^{c_i} - {b_i}^{c_i-1}) = \prod_i^{[0:|b|]}({b_i}^{c_i} - {b_i}^{c_i-1})$**.**

Declaration I:32

The notation $a^{\underline{b}}$ will be used as a shorthand for $\prod_i^{[0:b]}(a - i)$.

Declaration I:33

The notation $a^{\overline{b}}$ will be used as a shorthand for $\prod_i^{[0:b]}(a + i)$.

Procedure I:85

Objective

Choose a list of distinct elements a and a non-negative integer b such that $b \leq |a|$. Let c be a list of length-b permutations of a. The objective of the following instructions is to show that $|c| = |a|^{\underline{b}}$.

Implementation

1. If $|b| > 0$, then do the following:
   (a) For each entry d in a, do the following:
      i. Let e be the list formed by removing d from a.
      ii. Verify that the entries of e are distinct.
      iii. Verify that $|e| = |a| - 1$.
      iv. Now execute procedure I:85 on $\langle e, b - 1\rangle$.
      v. Therefore verify that the number of length-$b-1$ permutations of e is $|e|^{\underline{b-1}}$.
      vi. Therefore verify that the number of length-b permutations of a beginning with d is $|e|^{\underline{b-1}} = (|a| - 1)^{\underline{b-1}}$.
   (b) Therefore verify that the number of length-b permutations of a beginning with any entry of a is $|a|(|a| - 1)^{\underline{b-1}} = |a|^{\underline{b}}$.
   (c) Therefore verify that the number of length-b permutations of a are $|a|^{\underline{b}}$.
   (d) **Therefore verify that** $|c| = |a|^{\underline{b}}$**.**
2. Otherwise do the following:
   (a) Verify that $b = 0$.
   (b) Verify that the number of length-0 permutations of a is 1.
   (c) **Therefore verify that** $|c| = 1 = |a|^{\underline{0}} = |a|^{\underline{b}}$**.**

Declaration I:34

The notation $\binom{n}{r}$ will be used as a shorthand for $n^{\underline{r}} \operatorname{div}(r!)$.

Procedure I:86

Objective

Choose a list of distinct elements n and a non-negative integer r such that $r \leq |n|$. Let b be the largest list of length-r sublists of n such that no two of them are permutations of each other. The objective of the following instructions is to either show that b contains at least two permutations of the same list, construct a list larger than b that is also a list of length-r sublists of n such that no two of them are permutations of each other, or to show that $|b| = \binom{|n|}{r}$ and that $|n|^{\underline{r}} \bmod r! = 0$.

Implementation

1. Let a and f be a list of all the permutations of n.
2. Using procedure I:85, verify that $|a| = |n|^{\underline{|n|}}$.
3. For each list c in b, do the following:
   (a) Using procedure I:85, verify that the number of permutations of c is $r!$.
   (b) Let d be the list obtained by removing the elements of c from n.
   (c) Using procedure I:85, verify that the number of permutations of d is $(n - r)!$.
   (d) Let e be the list of permutations of n beginning with a permutations of c.
   (e) Verify that $|e| = |c||d| = r!(|n| - r)!$.
   (f) If e is not a sublist of a, then do the following:
      i. Let g be a list in e that is not in a.
      ii. Verify that e is a sublist of f.
      iii. Therefore verify that g was in a but then was removed.
      iv. Therefore verify that the variable c was formerly equal to a permutation of the current c.
      v. **Therefore verify that b contains at least two permutations of c.**
      vi. **Abort procedure.**
   (g) Otherwise, do the following:
      i. Verify that e is a sublist of a.
      ii. Remove the lists in e from a.
4. If $a \neq \langle\rangle$, then do the following:
   (a) Let g be a list in a.
   (b) Let h be the sublist of g corresponding to its first r elements.
   (c) Therefore verify that the permutations of n beginning with a permutation of h were never removed from a.
   (d) Therefore verify that the variable c was never equal to a permutation of h.
   (e) Therefore verify that no permutation of h is in b.
   (f) **Therefore verify that $b \frown \langle h\rangle$ is larger than b and is also a list of length-r sublists of n such that no two of them are permutations of each other.**
   (g) **Abort procedure.**
5. Otherwise do the following:
   (a) Verify that $|n|! \bmod (r!(|n| - r)!) = 0$.
   (b) Therefore verify that $|n|! = (|n|! \operatorname{div}(r!(|n| - r)!))r!(|n| - r)!$.
   (c) Therefore verify that $|n|! \operatorname{div}(|n| - r)! = (|n|! \operatorname{div}(r!(|n| - r)!))r!$.
   (d) **Therefore verify that $n^{\underline{r}} \bmod r! = (|n|! \operatorname{div}(|n| - r)!) \bmod r! = 0$.**
   (e) Also verify that (3) iterated $|n|! \operatorname{div}(r!(|n| - r)!)$ times.
   (f) **Therefore using procedure I:35, verify that $|b| = |n|! \operatorname{div}(r!(|n| - r)!) = (|n|! \operatorname{div}(|n| - r)!) \operatorname{div}(r!) = n^{\underline{r}} \operatorname{div}(r!) = \binom{n}{r}$.**

Procedure I:87

Objective

Choose two positive integers a, b. The objective of the following instructions is to show that $\binom{a}{b} = \binom{a-1}{b-1} + \binom{a-1}{b}$.

Implementation

1. Using procedure I:32 and procedure I:33, verify that $\binom{a-1}{b-1} + \binom{a-1}{b}$
   (a) $= (a-1)^{\underline{b-1}} \operatorname{div} (b-1)! + (a-1)^{\underline{b}} \operatorname{div} b!$
   (b) $= ((a-1)^{\underline{b-1}} b) \operatorname{div} b! + (a-1)^{\underline{b}} \operatorname{div} b!$
   (c) $= ((a-1)^{\underline{b-1}} b + (a-1)^{\underline{b}}) \operatorname{div} b!$
   (d) $= ((a-1)^{\underline{b-1}} b + (a-1)^{\underline{b-1}}(a-b)) \operatorname{div} b!$
   (e) $= ((a-1)^{\underline{b-1}} a) \operatorname{div} b!$
   (f) $= a^{\underline{b}} \operatorname{div} b!$
   (g) $= \binom{a}{b}$.

Procedure I:88

Objective

Choose an integer x and a non-negative integer a. The objective of the following instructions is to show that the $(1+x)^a = \sum_r^{[0:a+1]} \binom{a}{r} x^r$.

Implementation

1. If $a = 0$, then do the following:
   (a) **Verify that $(1+x)^a = (1+x)^0 = 1 = \sum_r^{[0:1]} \binom{0}{r} x^r = \sum_r^{[0:a+1]} \binom{a}{r} x^r$.**
2. Otherwise, do the following:
   (a) Verify that $a > 0$.
   (b) Therefore verify that $a - 1 \geq 0$.
   (c) Execute procedure I:88 on $\langle x, a-1 \rangle$.
   (d) Therefore verify that $(1+x)^{a-1} = \sum_r^{[0:a]} \binom{a-1}{r} x^r$.
   (e) Therefore using procedure I:87, verify that $(1+x)^a$
      i. $= (1+x)(1+x)^{a-1}$
      ii. $= (1+x) \sum_r^{[0:a]} \binom{a-1}{r} x^r$
      iii. $= \sum_r^{[0:a]} \binom{a-1}{r} x^r + \sum_r^{[0:a]} \binom{a-1}{r} x^{r+1}$
      iv. $= \sum_r^{[0:a+1]} \binom{a-1}{r} x^r + \sum_r^{[1:a+1]} \binom{a-1}{r-1} x^r$
      v. $= 1 + \sum_r^{[1:a+1]} (\binom{a-1}{r} + \binom{a-1}{r-1}) x^r$
      vi. $= 1 + \sum_r^{[1:a+1]} \binom{a}{r} x^r$
      vii. $= \sum_r^{[0:a+1]} \binom{a}{r} x^r$.

Procedure I:89

Objective

Choose an integer r and a prime n such that $0 < r < n$. The objective of the following instructions is to show that either $0 \neq 0$ or $\binom{n}{r} \bmod n = 0$.

Implementation

1. Using procedure I:86, verify that $\binom{n}{r} r! = n^{\underline{r}} \equiv 0 \pmod{n}$.
2. If $\binom{n}{r} \bmod n \neq 0$, then do the following:
   (a) Verify that $i \bmod n \neq 0$ for $i = 1$ to $i = r$.
   (b) Therefore using procedure I:50, verify that $r! \bmod n \neq 0$.
   (c) Therefore using (2) and (b), verify that $\binom{n}{r} r! \bmod n \neq 0$.
   (d) **Therefore using (1) and (c), verify that $0 \neq 0$.**
   (e) **Abort procedure.**
3. Otherwise, do the following:
   (a) **Verify that $\binom{n}{r} \bmod n = 0$.**

Part II

Rational Arithmetic

Declaration II:0

The phrase "rational number" will be used as a shorthand for an ordered pair comprising an integer followed by a non-zero natural number.

Declaration II:1

The phrase "the numerator of a" and the notation $\mathrm{nu}(a)$, where a is a rational number, will be used as a shorthand for the first entry of a.

Declaration II:2

The phrase "the denominator of a" and the notation $\mathrm{de}(a)$, where a is a rational number, will be used as a shorthand for the second entry of a.

Declaration II:3

The phrase "$a = b$", where a, b are rational numbers, will be used as a shorthand for "$\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b)$".

Procedure II:0

Objective

Choose a rational number a. The objective of the following instructions is to show that $a = a$.

Implementation

1. Verify that $\mathrm{nu}(a)\,\mathrm{de}(a) = \mathrm{de}(a)\,\mathrm{nu}(a)$.
2. **Hence verify that** $a = a$**.**

Procedure II:1

Objective

Choose two rational numbers a, b such that $a = b$. The objective of the following instructions is to show that $b = a$.

Implementation

1. Verify that $\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. Hence verify that $\mathrm{nu}(b)\,\mathrm{de}(a) = \mathrm{de}(b)\,\mathrm{nu}(a)$.
3. **Hence verify that** $b = a$**.**

Procedure II:2

Objective

Choose three rational numbers a, b, c such that $a = b$ and $b = c$. The objective of the following instructions is to show that $a = c$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. Using declaration II:3, verify that $\mathrm{nu}(b)\,\mathrm{de}(c) = \mathrm{de}(b)\,\mathrm{nu}(c)$.
3. If $\mathrm{nu}(b) \neq 0$, then do the following:
   (a) Hence verify that $\mathrm{nu}(a)\,\mathrm{de}(b)\,\mathrm{nu}(b)\,\mathrm{de}(c) = \mathrm{de}(a)\,\mathrm{nu}(b)\,\mathrm{de}(b)\,\mathrm{nu}(c)$.
   (b) Hence verify that $\mathrm{nu}(a)\,\mathrm{de}(c) = \mathrm{de}(a)\,\mathrm{nu}(c)$.
4. Otherwise do the following:
   (a) Using declaration II:0, verify that $\mathrm{de}(b) \neq 0$.
   (b) Verify that $\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b) = 0$.
   (c) Hence verify that $\mathrm{nu}(a) = 0$.
   (d) Verify that $0 = \mathrm{nu}(b)\,\mathrm{de}(c) = \mathrm{de}(b)\,\mathrm{nu}(c)$.
   (e) Hence verify that $\mathrm{nu}(c) = 0$.
   (f) Hence verify that $\mathrm{nu}(a)\,\mathrm{de}(c) = 0 = \mathrm{de}(a)\,\mathrm{nu}(c)$.
5. **Hence verify that** $a = c$**.**

Declaration II:4

The notation $a + b$, where a, b are rational numbers, will be used as a shorthand for the pair $\langle \mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$.

Procedure II:3

Objective

Choose two rational numbers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $a + b = c + d$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(c) = \mathrm{de}(a)\,\mathrm{nu}(c)$.
2. Using declaration II:3, verify that $\mathrm{nu}(b)\,\mathrm{de}(d) = \mathrm{de}(b)\,\mathrm{nu}(d)$.
3. Hence verify that $a + b$

(a) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle + \langle \mathrm{nu}(b), \mathrm{de}(b)\rangle$

(b) $= \langle \mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(c) $= \langle \mathrm{de}(c)\,\mathrm{de}(d)(\mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b)), \mathrm{de}(c)\,\mathrm{de}(d)(\mathrm{de}(a)\,\mathrm{de}(b))\rangle$

(d) $= \langle \mathrm{nu}(a)\,\mathrm{de}(c)\,\mathrm{de}(b)\,\mathrm{de}(d) + \mathrm{de}(a)\,\mathrm{de}(c)\,\mathrm{nu}(b)\,\mathrm{de}(d), \mathrm{de}(c)\,\mathrm{de}(d)\,\mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(e) $= \langle \mathrm{de}(a)\,\mathrm{nu}(c)\,\mathrm{de}(b)\,\mathrm{de}(d) + \mathrm{de}(a)\,\mathrm{de}(c)\,\mathrm{de}(b)\,\mathrm{nu}(d), \mathrm{de}(c)\,\mathrm{de}(d)\,\mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(f) $= \langle \mathrm{de}(a)\,\mathrm{de}(b)(\mathrm{nu}(c)\,\mathrm{de}(d) + \mathrm{de}(c)\,\mathrm{nu}(d)), \mathrm{de}(a)\,\mathrm{de}(b)(\mathrm{de}(c)\,\mathrm{de}(d))\rangle$

(g) $= \langle \mathrm{nu}(c)\,\mathrm{de}(d) + \mathrm{de}(c)\,\mathrm{nu}(d), \mathrm{de}(c)\,\mathrm{de}(d)\rangle$

(h) $= \langle \mathrm{nu}(c), \mathrm{de}(c)\rangle + \langle \mathrm{nu}(d), \mathrm{de}(d)\rangle$

(i) $= c + d$.

Procedure II:4

Objective

Choose three rational numbers a, b, c. The objective of the following instructions is to show that $(a + b) + c = a + (b + c)$.

Implementation

1. Verify that $(a + b) + c$

(a) $= \langle \mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle + \langle \mathrm{nu}(c), \mathrm{de}(c)\rangle$

(b) $= \langle (\mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b))\,\mathrm{de}(c) + (\mathrm{de}(a)\,\mathrm{de}(b))\,\mathrm{nu}(c), (\mathrm{de}(a)\,\mathrm{de}(b))\,\mathrm{de}(c)\rangle$

(c) $= \langle \mathrm{nu}(a)(\mathrm{de}(b)\,\mathrm{de}(c)) + \mathrm{de}(a)(\mathrm{nu}(b)\,\mathrm{de}(c) + \mathrm{de}(b)\,\mathrm{nu}(c)), \mathrm{de}(a)(\mathrm{de}(b)\,\mathrm{de}(c))\rangle$

(d) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle + \langle \mathrm{nu}(b)\,\mathrm{de}(c) + \mathrm{de}(b)\,\mathrm{nu}(c), \mathrm{de}(b)\,\mathrm{de}(c)\rangle$

(e) $= a + (b + c)$.

Procedure II:5

Objective

Choose two rational numbers a, b. The objective of the following instructions is to show that $a + b = b + a$.

Implementation

1. $a + b$

(a) $= \langle \mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(b) $= \langle \mathrm{nu}(b)\,\mathrm{de}(a) + \mathrm{de}(b)\,\mathrm{nu}(a), \mathrm{de}(b)\,\mathrm{nu}(a)\rangle$

(c) $= b + a$.

Declaration II:5

The notation a, where a is an integer, will contextually be used as a shorthand for the pair $\langle a, 1\rangle$.

Procedure II:6

Objective

Choose a rational number a. The objective of the following instructions is to show that $0 + a = a$.

Implementation

1. Verify that $0 + a$

(a) $= \langle 0, 1\rangle + \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle$

(b) $= \langle 0\,\mathrm{de}(a) + 1\,\mathrm{nu}(a), 1\,\mathrm{de}(a)\rangle$

(c) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle$

(d) $= a$.

Declaration II:6

The notation $-a$, where a is a rational number, will be used as a shorthand for the pair $\langle -\mathrm{nu}(a), \mathrm{de}(a)\rangle$.

Procedure II:7

Objective

Choose two rational numbers a, b such that $a = b$. The objective of the following instructions is to show that $-a = -b$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b)$.

2. Hence verify that $-a$

(a) $= \langle -\mathrm{nu}(a), \mathrm{de}(a)\rangle$

(b) $= \langle -\mathrm{nu}(a)\,\mathrm{de}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(c) $= \langle -\mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(d) $= \langle -\mathrm{nu}(b), \mathrm{de}(b)\rangle$

(e) $= -b$.

Procedure II:8

Objective

Choose a rational number a. The objective of the following instructions is to show that $-a + a = 0$.

Implementation

1. Verify that $-a + a$

(a) $= (-a) + a$

(b) $= \langle -\mathrm{nu}(a), \mathrm{de}(a)\rangle + \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle$

(c) $= \langle -\mathrm{nu}(a)\,\mathrm{de}(a) + \mathrm{de}(a)\,\mathrm{nu}(a), \mathrm{de}(a)^2\rangle$

(d) $= \langle 0, \mathrm{de}(a)^2\rangle$

(e) $= \langle 0, 1\rangle$

(f) $= 0$.

Declaration II:7

The notation ab, where a, b are rational numbers, will be used as a shorthand for the pair $\langle \mathrm{nu}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$.

Procedure II:9

Objective

Choose two rational numbers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $ab = cd$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(c) = \mathrm{de}(a)\,\mathrm{nu}(c)$.

2. Using declaration II:3, verify that $\mathrm{nu}(b)\,\mathrm{de}(d) = \mathrm{de}(b)\,\mathrm{nu}(d)$.

3. Hence verify that ab

(a) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle\langle \mathrm{nu}(b), \mathrm{de}(b)\rangle$

(b) $= \langle \mathrm{nu}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(c) $= \langle (\mathrm{de}(c)\,\mathrm{de}(d))\,\mathrm{nu}(a)\,\mathrm{nu}(b), (\mathrm{de}(c)\,\mathrm{de}(d))\,\mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(d) $= \langle (\mathrm{nu}(a)\,\mathrm{de}(c))(\mathrm{nu}(b)\,\mathrm{de}(d)), \mathrm{de}(c)\,\mathrm{de}(d)\,\mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(e) $= \langle (\mathrm{de}(a)\,\mathrm{nu}(c))(\mathrm{de}(b)\,\mathrm{nu}(d)), \mathrm{de}(c)\,\mathrm{de}(d)\,\mathrm{de}(a)\,\mathrm{de}(b)\rangle$

(f) $= \langle (\mathrm{de}(a)\,\mathrm{de}(b))\,\mathrm{nu}(c)\,\mathrm{nu}(d), (\mathrm{de}(a)\,\mathrm{de}(b))\,\mathrm{de}(c)\,\mathrm{de}(d)\rangle$

(g) $= \langle \mathrm{nu}(c)\,\mathrm{nu}(d), \mathrm{de}(c)\,\mathrm{de}(d)\rangle$

(h) $= \langle \mathrm{nu}(c), \mathrm{de}(c)\rangle\langle \mathrm{nu}(d), \mathrm{de}(d)\rangle$

(i) $= cd$.

Procedure II:10

Objective

Choose three rational numbers a, b, c. The objective of the following instructions is to show that $(ab)c = a(bc)$.

Implementation

1. Verify that $(ab)c$
   (a) $= \langle \mathrm{nu}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle\langle \mathrm{nu}(c), \mathrm{de}(c)\rangle$
   (b) $= \langle \mathrm{nu}(a)\,\mathrm{nu}(b)\,\mathrm{nu}(c), \mathrm{de}(a)\,\mathrm{de}(b)\,\mathrm{de}(c)\rangle$
   (c) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle\langle \mathrm{nu}(b)\,\mathrm{nu}(c), \mathrm{de}(b)\,\mathrm{de}(c)\rangle$
   (d) $= a(bc)$.

Procedure II:11

Objective

Choose two rational numbers a, b. The objective of the following instructions is to show that $ab = ba$.

Implementation

1. ab
   (a) $= \langle \mathrm{nu}(a)\,\mathrm{nu}(b), \mathrm{de}(a)\,\mathrm{de}(b)\rangle$
   (b) $= \langle \mathrm{nu}(b)\,\mathrm{nu}(a), \mathrm{de}(b)\,\mathrm{de}(a)\rangle$
   (c) $= ba$.

Procedure II:12

Objective

Choose a rational number a. The objective of the following instructions is to show that $1a = a$.

Implementation

1. Verify that $1a$
   (a) $= \langle 1, 1\rangle\langle \mathrm{nu}(a), \mathrm{de}(a)\rangle$
   (b) $= \langle 1\,\mathrm{nu}(a), 1\,\mathrm{de}(a)\rangle$
   (c) $= \langle \mathrm{nu}(a), \mathrm{de}(a)\rangle$
   (d) $= a$.

Declaration II:8

The notation $\frac{1}{a}$, where a is a rational number such that $\mathrm{nu}(a) > 0$, will be used as a shorthand for the pair $\langle \mathrm{de}(a), \mathrm{nu}(a)\rangle$.

Declaration II:9

The notation $\frac{1}{a}$, where a is a rational number such that $\mathrm{nu}(a) < 0$, will be used as a shorthand for the pair $\langle -\mathrm{de}(a), -\mathrm{nu}(a)\rangle$.

Procedure II:13

Objective

Choose two rational numbers a, b such that $a = b$ and $a \neq 0$. The objective of the following instructions is to show that $\frac{1}{a} = \frac{1}{b}$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(b) = \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. Using declaration II:3 and declaration II:5, verify that $\mathrm{nu}(a) = \mathrm{nu}(a)\,\mathrm{de}(0) \neq \mathrm{de}(a)\,\mathrm{nu}(0) = 0$.
3. Hence using declaration II:0, verify that $\mathrm{de}(a)\,\mathrm{nu}(b) = \mathrm{nu}(a)\,\mathrm{de}(b) \neq 0$.
4. Hence verify that $\mathrm{nu}(b) \neq 0$.
5. If $\mathrm{nu}(a)\,\mathrm{nu}(b) > 0$, then do the following:
   (a) Verify that $\frac{1}{a}$
      i. $= \langle \mathrm{de}(a)\,\mathrm{nu}(b), \mathrm{nu}(a)\,\mathrm{nu}(b)\rangle$
      ii. $= \langle \mathrm{nu}(a)\,\mathrm{de}(b), \mathrm{nu}(a)\,\mathrm{nu}(b)\rangle$
      iii. $= \frac{1}{b}$.
6. Otherwise do the following:
   (a) Verify that $\mathrm{nu}(a)\,\mathrm{nu}(b) < 0$.
   (b) Hence verify that $\frac{1}{a}$
      i. $= \langle -\mathrm{de}(a)\,\mathrm{nu}(b), -\mathrm{nu}(a)\,\mathrm{nu}(b)\rangle$

ii. $= \langle -\operatorname{nu}(a)\operatorname{de}(b), -\operatorname{nu}(a)\operatorname{nu}(b)\rangle$

iii. $= \frac{1}{b}$.

Procedure II:14

Objective

Choose a rational number a such that $a \neq 0$. The objective of the following instructions is to show that $\frac{1}{a}a = 1$.

Implementation

1. Using declaration II:3 and declaration II:5, verify that $\operatorname{nu}(a) = \operatorname{nu}(a)\operatorname{de}(0) \neq \operatorname{de}(a)\operatorname{nu}(0) = 0$.
2. If $\operatorname{nu}(a) > 0$, then do the following:
   (a) Verify that $\frac{1}{a}a$
      i. $= \langle \operatorname{de}(a), \operatorname{nu}(a)\rangle\langle \operatorname{nu}(a), \operatorname{de}(a)\rangle$
      ii. $= \langle \operatorname{de}(a)\operatorname{nu}(a), \operatorname{nu}(a)\operatorname{de}(a)\rangle$
      iii. $= \langle 1, 1\rangle$
      iv. $= 1$.
3. Otherwise do the following:
   (a) Verify that $\operatorname{nu}(a) < 0$.
   (b) Hence verify that $\frac{1}{a}a$
      i. $= \langle -\operatorname{de}(a), -\operatorname{nu}(a)\rangle\langle \operatorname{nu}(a), \operatorname{de}(a)\rangle$
      ii. $= \langle -\operatorname{de}(a)\operatorname{nu}(a), -\operatorname{nu}(a)\operatorname{de}(a)\rangle$
      iii. $= \langle 1, 1\rangle$
      iv. $= 1$.

Procedure II:15

Objective

Choose three rational numbers a, b, c. The objective of the following instructions is to show that $a(b + c) = ab + ac$.

Implementation

1. $a(b + c)$
   (a) $= \langle \operatorname{nu}(a), \operatorname{de}(a)\rangle\langle \operatorname{nu}(b)\operatorname{de}(c) + \operatorname{de}(b)\operatorname{nu}(c), \operatorname{de}(b)\operatorname{de}(c)\rangle$
   (b) $= \langle \operatorname{nu}(a)(\operatorname{nu}(b)\operatorname{de}(c) + \operatorname{de}(b)\operatorname{nu}(c)), \operatorname{de}(a)(\operatorname{de}(b)\operatorname{de}(c))\rangle$
   (c) $= \langle \operatorname{nu}(a)\operatorname{nu}(b)\operatorname{de}(c) + \operatorname{nu}(a)\operatorname{de}(b)\operatorname{nu}(c), \operatorname{de}(a)\operatorname{de}(b)\operatorname{de}(c)\rangle$
   (d) $= \langle \operatorname{de}(a)(\operatorname{nu}(a)\operatorname{nu}(b)\operatorname{de}(c)+\operatorname{nu}(a)\operatorname{de}(b)\operatorname{nu}(c)), \operatorname{de}(a)(\operatorname{de}(a)\operatorname{de}(b)\operatorname{de}(c))\rangle$
   (e) $= \langle (\operatorname{nu}(a)\operatorname{nu}(b))(\operatorname{de}(a)\operatorname{de}(c))+(\operatorname{de}(a)\operatorname{de}(b))(\operatorname{nu}(a)\operatorname{nu}(c)), (\operatorname{de}(a)\operatorname{de}(b))(\operatorname{de}(a)\operatorname{de}(c))\rangle$
   (f) $= \langle \operatorname{nu}(a)\operatorname{nu}(b), \operatorname{de}(a)\operatorname{de}(b)\rangle + \langle \operatorname{nu}(a)\operatorname{nu}(c), \operatorname{de}(a)\operatorname{de}(c)\rangle$
   (g) $= ab + ac$.

Procedure II:16

Objective

Choose an integer a. The objective of the following instructions is to show that $(-1)^{2a} = 1$ and $(-1)^{2a+1} = -1$.

Implementation

Implementation is analogous to that of procedure I:14.

Declaration II:10

The phrase "$a < b$", where a, b are rational numbers, will be used as a shorthand for "$\operatorname{nu}(a)\operatorname{de}(b) < \operatorname{de}(a)\operatorname{nu}(b)$".

Procedure II:17

Objective

Choose four rational numbers a, b, c, d such that $a < b$, $a = c$ and $b = d$. The objective of the following instructions is to show that $c < d$.

Implementation

1. Using declaration II:3, verify that $\mathrm{nu}(a)\,\mathrm{de}(c) = \mathrm{de}(a)\,\mathrm{nu}(c)$.
2. Using declaration II:3, verify that $\mathrm{nu}(b)\,\mathrm{de}(d) = \mathrm{de}(b)\,\mathrm{nu}(d)$.
3. Using declaration II:10, verify that $\mathrm{nu}(a)\,\mathrm{de}(b) < \mathrm{de}(a)\,\mathrm{nu}(b)$.
4. Hence verify that $\mathrm{nu}(c)\,\mathrm{de}(d)\,\mathrm{de}(a)\,\mathrm{de}(b)$
   (a) $= \mathrm{nu}(a)\,\mathrm{de}(c)\,\mathrm{de}(d)\,\mathrm{de}(b)$
   (b) $< \mathrm{de}(a)\,\mathrm{nu}(b)\,\mathrm{de}(c)\,\mathrm{de}(d)$
   (c) $= \mathrm{de}(b)\,\mathrm{nu}(d)\,\mathrm{de}(a)\,\mathrm{de}(c)$.
5. Hence verify that $\mathrm{nu}(c)\,\mathrm{de}(d) < \mathrm{de}(c)\,\mathrm{nu}(d)$.
6. **Hence verify that $c < d$.**

Procedure II:18

Objective

Choose three rational numbers a, b, c such that $a < b$. The objective of the following instructions is to show that $a + c < b + c$.

Implementation

1. Using declaration II:10, verify that $\mathrm{nu}(a)\,\mathrm{de}(b) < \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. Using declaration II:0, verify that $0 < \mathrm{de}(c)$.
3. Hence verify that $\mathrm{nu}(a + c)\,\mathrm{de}(b + c)$
   (a) $= (\mathrm{nu}(a)\,\mathrm{de}(c) + \mathrm{de}(a)\,\mathrm{nu}(c))\,\mathrm{de}(b)\,\mathrm{de}(c)$
   (b) $= \mathrm{nu}(a)\,\mathrm{de}(c)\,\mathrm{de}(b)\,\mathrm{de}(c)+\mathrm{de}(a)\,\mathrm{nu}(c)\,\mathrm{de}(b)\,\mathrm{de}(c)$
   (c) $< \mathrm{de}(a)\,\mathrm{de}(c)\,\mathrm{nu}(b)\,\mathrm{de}(c)+\mathrm{de}(a)\,\mathrm{nu}(c)\,\mathrm{de}(b)\,\mathrm{de}(c)$
   (d) $= (\mathrm{nu}(b)\,\mathrm{de}(c) + \mathrm{nu}(c)\,\mathrm{de}(b))\,\mathrm{de}(a)\,\mathrm{de}(c)$
   (e) $= \mathrm{nu}(b + c)\,\mathrm{de}(a + c)$.
4. **Hence verify that $a + c < b + c$.**

Procedure II:19

Objective

Choose two rational numbers a, b such that $a < b$. The objective of the following instructions is to show that $a \neq b$ and $b \not< a$.

Implementation

1. Verify that $\mathrm{nu}(a)\,\mathrm{de}(b) < \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. Hence verify that $\mathrm{nu}(a)\,\mathrm{de}(b) \neq \mathrm{de}(a)\,\mathrm{nu}(b)$.
3. **Hence verify that $a \neq b$.**
4. Also verify that $\mathrm{nu}(b)\,\mathrm{de}(a) \not< \mathrm{de}(b)\,\mathrm{nu}(a)$.
5. **Hence verify that $b \not< a$.**

Procedure II:20

Objective

Choose two rational numbers a, b such that $a = b$. The objective of the following instructions is to show that $a \not< b$ and $b \not< a$.

Implementation

Implementation is analogous to that of procedure II:19.

Procedure II:21

Objective

Choose two rational numbers a, b such that $a \neq b$. The objective of the following instructions is to show that $a < b$ or $b < a$.

Implementation

1. Verify that $\mathrm{nu}(a)\,\mathrm{de}(b) \neq \mathrm{de}(a)\,\mathrm{nu}(b)$.
2. If $\mathrm{nu}(a)\,\mathrm{de}(b) < \mathrm{de}(a)\,\mathrm{nu}(b)$, then do the following:
   (a) **Verify that $a < b$.**
3. Otherwise do the following:

(a) Verify that $\mathrm{nu}(b)\,\mathrm{de}(a) < \mathrm{de}(b)\,\mathrm{nu}(a)$.

(b) **Hence verify that $b < a$.**

Procedure II:22

Objective

Choose two rational numbers a, b such that $a \not< b$. The objective of the following instructions is to show that $a = b$ or $b < a$.

Implementation

Implementation is analogous to that of procedure II:21.

Procedure II:23

Objective

Choose two rational numbers a, b such that $0 < a$ and $0 < b$. The objective of the following instructions is to show that $0 < a + b$.

Implementation

1. Using declaration II:10, verify that $0 = \mathrm{nu}(0)\,\mathrm{de}(a) < \mathrm{de}(0)\,\mathrm{nu}(a) = \mathrm{nu}(a)$.
2. Using declaration II:0, verify that $0 < \mathrm{de}(a)$.
3. Using declaration II:10, verify that $0 = \mathrm{nu}(0)\,\mathrm{de}(b) < \mathrm{de}(0)\,\mathrm{nu}(b) = \mathrm{nu}(b)$.
4. Using declaration II:0, verify that $0 < \mathrm{de}(b)$.
5. Hence verify that $\mathrm{nu}(0)\,\mathrm{de}(a + b) = 0 < \mathrm{nu}(a)\,\mathrm{de}(b) + \mathrm{de}(a)\,\mathrm{nu}(b) = \mathrm{de}(0)\,\mathrm{nu}(a + b)$.
6. **Hence verify that $0 < a + b$.**

Procedure II:24

Objective

Choose two rational numbers a, b such that $0 < a$ and $0 < b$. The objective of the following instructions is to show that $0 < ab$.

Implementation

1. Using declaration II:10, verify that $0 = \mathrm{nu}(0)\,\mathrm{de}(a) < \mathrm{de}(0)\,\mathrm{nu}(a) = \mathrm{nu}(a)$.
2. Using declaration II:10, verify that $0 = \mathrm{nu}(0)\,\mathrm{de}(b) < \mathrm{de}(0)\,\mathrm{nu}(b) = \mathrm{nu}(b)$.
3. Hence verify that $\mathrm{nu}(0)\,\mathrm{de}(ab) = 0 < \mathrm{nu}(a)\,\mathrm{nu}(b) = \mathrm{de}(0)\,\mathrm{nu}(ab)$.
4. **Hence verify that $0 < ab$.**

Procedure II:25

Objective

Choose two rational numbers a, b. The objective of the following instructions is to show that $\|ab\| = \|a\|\|b\|$.

Implementation

Implementation is analogous to that of procedure I:23.

Procedure II:26

Objective

Choose two rational numbers a, b. The objective of the following instructions is to show that $\|a + b\| \leq \|a\| + \|b\|$.

Implementation

Implementation is analogous to that of procedure I:24.

Procedure II:27

Objective

Choose two rational numbers a, b. The objective of the following instructions is to show that $\|a\| - \|b\| \leq \|a - b\|$.

Implementation

Implementation is analogous to that of procedure I:25.

Procedure II:28

Objective

Choose a rational number a. The objective of the following instructions is to show that $a = \operatorname{sgn}(a)\|a\|$.

Implementation

Implementation is analogous to that of procedure I:26.

Declaration II:11

The notation $\lfloor a \rfloor$, where a is a rational number, will be used as a shorthand for $\operatorname{nu}(a) \operatorname{div} \operatorname{de}(a)$.

Declaration II:12

The notation $\lceil a \rceil$, where a is a rational number, will be used as a shorthand for $(\operatorname{nu}(a) \operatorname{div} \operatorname{de}(a)) + 1$.

Procedure II:29

Objective

Choose a rational number $r \neq 1$ and an integer $n \geq 0$. The objective of the following instructions is to show that $\sum_t^{[0:n]} r^t = \frac{1-r^n}{1-r}$.

Implementation

1. Verify that $r \sum_t^{[0:n]} r^t = \sum_t^{[0:n]} r^{t+1} = \sum_t^{[1:n+1]} r^t$.
2. Therefore verify that $(1-r)\sum_t^{[0:n]} r^t = \sum_t^{[0:n]} r^t - \sum_t^{[1:n+1]} r^t = 1 - r^n$.
3. **Therefore verify that $\sum_t^{[0:n]} r^t = \frac{1-r^n}{1-r}$.**

Procedure II:30

Objective

Choose a rational $0 < r < 1$ and an integer $n \geq 0$. The objective of the following instructions is to show that $\sum_t^{[0:n]} r^t < \frac{1}{1-r}$.

Implementation

1. **Using procedure II:29, verify that $\sum_t^{[0:n]} r^t = \frac{1-r^n}{1-r} < \frac{1}{1-r}$.**

Procedure II:31

Objective

Choose a non-negative integer a and a rational number x. The objective of the following instructions is to show that $(1+x)^a = \sum_r^{[0:a+1]} \binom{a}{r} x^r$.

Implementation

Instructions are analogous to those of procedure I:88.

Procedure II:32

Objective

Choose an integer $r \geq 0$ and a rational number $x \geq -1$. The objective of the following instructions is to show that $(1+x)^r \geq 1 + rx$.

Implementation

1. If $-1 \leq x < 0$, then do the following:
   (a) Using procedure II:29, verify that $(1+x)^r$
      i. $= 1 + (1+x)^r - 1$
      ii. $= 1 + x\frac{(1+x)^r - 1}{(1+x)-1}$
      iii. $= 1 + x\sum_k^{[0:r]}(1+x)^k$
      iv. $\geq 1 + x\sum_k^{[0:r]} 1$
      v. $= 1 + rx$.

2. Otherwise, do the following:

   (a) Verify that $x \geq 0$.

   (b) Using procedure II:31, verify that $(1+x)^r$

      i. $= \sum_k^{[0:r+1]} \binom{r}{k} x^k$

      ii. $\geq \binom{r}{0} x^0 + \binom{r}{1} x^1$

      iii. $= 1 + rx$

Procedure II:33

Objective

Choose a non-negative integer r and a rational number $x > -1$ such that $(r-1)x < 1$. The objective of the following instructions is to show that $(1+x)^r \leq \frac{1+x}{1-(r-1)x}$.

Implementation

1. Verify that $1 - \frac{x}{1+x} = \frac{1}{1+x} > 0$.
2. Hence using procedure II:32, verify that $(1 - \frac{x}{1+x})^r \geq 1 - \frac{rx}{1+x}$.
3. Verify that $0 < 1 + x - rx$.
4. Hence verify that $0 < 1 - \frac{rx}{1+x}$.
5. Hence verify that $(1 - \frac{x}{1+x})^r \geq 1 - \frac{rx}{1+x} > 0$.
6. Hence verify that $(1+x)^r$

   (a) $= (\frac{1}{1+x})^{-r}$

   (b) $= (1 - \frac{x}{1+x})^{-r}$

   (c) $\leq (1 - \frac{rx}{1+x})^{-1}$

   (d) $= \frac{1+x}{1-(r-1)x}$.

Declaration II:13

The notation $\min(c)$, where c is a list, will be used as a shorthand for ∞ if c is empty, otherwise it will stand for the minimum entry of c.

Declaration II:14

The notation $\min_r^R c(r)$, where R is a list and $c[r]$ is a function of r, will be used as a shorthand for $\min(c(R))$.

Declaration II:15

The notation $\max(c)$, where c is a list, will be used as a shorthand for $-\infty$ if c is empty, otherwise it will stand for the maximum entry of c.

Declaration II:16

The notation $\max_r^R c(r)$, where R is a list and $c[r]$ is a function of r, will be used as a shorthand for $\max(c(R))$.

Declaration II:17

The phrase "polynomial" will be used as a shorthand for a list of rational numbers.

Declaration II:18

The notation a_i, where a is a polynomial and i is a natural number such that $i \geq |a|$, will be used as a shorthand for 0.

Declaration II:19

The phrase "$a = b$", where a, b are polynomials, will be used as a shorthand for "$a_i = b_i$ for each $i \in [0 : \max(|a|, |b|)]$".

Declaration II:20

The notation $\Lambda(a, b)$ will be used as a shorthand for $\sum_r^{[0:|a|]} a_r b^r$.

Procedure II:34

Objective

Choose two polynomials a, b and a rational number c such that $a = b$. The objective of the following instructions is to show that $\Lambda(a, c) = \Lambda(b, c)$.

Implementation

1. Verify that $\Lambda(a, c)$

(a) $= \sum_r^{[0:|a|]} a_r c^r$

(b) $= \sum_r^{[0:\max(|a|,|b|)]} a_r c^r$

(c) $= \sum_r^{[0:\max(|a|,|b|)]} b_r c^r$

(d) $= \sum_r^{[0:|b|]} b_r c^r$

(e) $= \Lambda(b, c)$.

Procedure II:35

Objective

Choose a natural number c and two polynomials a, b such that $a = b$. The objective of the following instructions is to show that $a_c = b_c$.

Implementation

1. If $c < \max(|a|, |b|)$, then do the following:

(a) **Verify that** $a_c = b_c$**.**

2. Otherwise do the following:

(a) Verify that $c \geq \max(|a|, |b|)$.

(b) **Hence verify that** $a_c = 0 = b_c$**.**

Procedure II:36

Objective

Choose a polynomial a. The objective of the following instructions is to show that $a = a$.

Implementation

1. Verify that $a_i = a_i$ for each $i \in [0 : \max(|a|, |a|)]$.
2. **Hence verify that** $a = a$**.**

Procedure II:37

Objective

Choose two polynomials a, b such that $a = b$. The objective of the following instructions is to show that $b = a$.

Implementation

1. Verify that $a_i = b_i$ for each $i \in [0 : \max(|a|, |b|)]$.
2. Hence verify that $b_i = a_i$ for each $i \in [0 : \max(|b|, |a|)]$.
3. **Hence verify that** $b = a$**.**

Procedure II:38

Objective

Choose three polynomials a, b, c such that $a = b$ and $b = c$. The objective of the following instructions is to show that $a = c$.

Implementation

1. Using declaration II:19, verify that $a_i = b_i$ for each $i \in [0 : \max(|a|, |b|, |c|)]$.
2. Using declaration II:19, verify that $b_i = c_i$ for each $i \in [0 : \max(|a|, |b|, |c|)]$.
3. Hence verify that $a_i = c_i$ for each $i \in [0 : \max(|a|, |b|, |c|)]$.
4. **Hence verify that** $a = c$**.**

Declaration II:21

The notation $\langle f(j) \text{ for } j \in R\rangle$, where $f[j]$ is a function of j and R is a list, will be used as a shorthand for $\langle f(R)\rangle$.

Declaration II:22

The notation $a + b$, where a, b are polynomials, will be used as a shorthand for the list $\langle a_i + b_i \text{ for } i \in [0 : \max(|a|, |b|)]\rangle$.

Procedure II:39

Objective

Choose two polynomials a, b and a rational number c. The objective of the following instructions is to show that $\Lambda(a + b, c) = \Lambda(a, c) + \Lambda(b, c)$.

Implementation

1. Verify that $\Lambda(a + b, c)$

(a) $= \Lambda(\langle a_r + b_r \text{ for } r \in [0 : \max(|a|, |b|)]\rangle, c)$

(b) $= \sum_r^{[0:\max(|a|,|b|)]} (a_r + b_r)c^r$

(c) $= \sum_r^{[0:\max(|a|,|b|)]} a_r c^r + \sum_r^{[0:\max(|a|,|b|)]} b_r c^r$

(d) $= \sum_r^{[0:|a|]} a_r c^r + \sum_r^{[0:|b|]} b_r c^r$

(e) $= \Lambda(a, c) + \Lambda(b, c)$.

Procedure II:40

Objective

Choose a natural number c and two polynomials a, b. The objective of the following instructions is to show that $(a + b)_c = a_c + b_c$.

Implementation

1. If $c < \max(|a|, |b|)$, then do the following:

(a) **Verify that** $(a + b)_c = a_c + b_c$**.**

2. Otherwise do the following:

(a) Verify that $c \geq \max(|a|, |b|)$.

(b) Hence verify that $a_c = 0$.

(c) Also verify that $b_c = 0$.

(d) Also verify that $(a + b)_c = 0$.

(e) **Hence verify that** $(a + b)_c = a_c + b_c$**.**

Procedure II:41

Objective

Choose four polynomials a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $a + b = c + d$.

Implementation

1. Verify that $a_i = c_i$ for each $i \in [0 : \max(|a|, |b|, |c|, |d|)]$.
2. Verify that $b_i = d_i$ for each $i \in [0 : \max(|a|, |b|, |c|, |d|)]$.
3. Hence verify that $a + b$

(a) $= \langle a_i + b_i \text{ for } i \in [0 : \max(|a|, |b|, |c|, |d|)]\rangle$

(b) $= \langle c_i + d_i \text{ for } i \in [0 : \max(|a|, |b|, |c|, |d|)]\rangle$

(c) $= c + d$.

Procedure II:42

Objective

Choose three polynomials a, b, c. The objective of the following instructions is to show that $(a+b)+c = a + (b + c)$.

Implementation

1. Verify that $(a + b) + c$

(a) $\langle (a + b)_i + c_i \text{ for } i \in [0 : \max(|a + b|, |c|)]\rangle$

(b) $\langle (a_i + b_i) + c_i \text{ for } i \in [0 : \max(|a|, |b|, |c|)]\rangle$

(c) $\langle a_i + (b_i + c_i) \text{ for } i \in [0 : \max(|a|, |b + c|)]\rangle$

(d) $\langle a_i + (b + c)_i \text{ for } i \in [0 : \max(|a|, |b + c|)]\rangle$

(e) $= a + (b + c)$.

Procedure II:43

Objective

Choose two polynomials a, b. The objective of the following instructions is to show that $a + b = b + a$.

Implementation

1. Verify that $a+b$

(a) $= \langle a_i + b_i \text{ for } i \in [0 : \max(|a|, |b|)] \rangle$

(b) $= \langle b_i + a_i \text{ for } i \in [0 : \max(|b|, |a|)] \rangle$

(c) $= b + a$.

Declaration II:23

The notation a, where a is a rational number, will contextually be used as a shorthand for the list $\langle a \rangle$.

Procedure II:44

Objective

Choose a polynomial a. The objective of the following instructions is to show that $0 + a = a$.

Implementation

1. Verify that $0 + a$

(a) $= \langle 0_i + a_i \text{ for } i \in [0 : |a|] \rangle$

(b) $= \langle 0 + a_i \text{ for } i \in [0 : |a|] \rangle$

(c) $= a$.

Declaration II:24

The notation $-a$, where a is a polynomial, will be used as a shorthand for the list $\langle -a_i \text{ for } i \in [0 : |a|] \rangle$.

Procedure II:45

Objective

Choose a polynomial a and a rational number b. The objective of the following instructions is to show that $\Lambda(-a, b) = -\Lambda(a, b)$.

Implementation

1. Verify that $\Lambda(-a, b)$

(a) $= \Lambda(\langle -a_i \text{ for } i \in [0 : |a|] \rangle, b)$

(b) $= \sum_j^{[0:|a|]} (-a_j) b^j$

(c) $= -\sum_j^{[0:|a|]} a_j b^j$

(d) $= -\Lambda(a, b)$.

Procedure II:46

Objective

Choose two polynomials a, b such that $a = b$. The objective of the following instructions is to show that $-a = -b$.

Implementation

1. Verify that $a_i = b_i$ for $i \in [0 : \max(|a|, |b|)]$.
2. Hence verify that $-a$

(a) $= \langle -a_i \text{ for } i \in [0 : \max(|a|, |b|)] \rangle$

(b) $= \langle -b_i \text{ for } i \in [0 : \max(|a|, |b|)] \rangle$

(c) $= -b$.

Procedure II:47

Objective

Choose a polynomial a. The objective of the following instructions is to show that $-a + a = 0$.

Implementation

1. Verify that $-a + a$

(a) $= (-a) + a$

(b) $= \langle -a_i \text{ for } i \in [0 : |a|] \rangle + \langle a_i \text{ for } i \in [0 : |a|] \rangle$

(c) $= \langle -a_i + a_i \text{ for } i \in [0 : |a|] \rangle$

(d) $= \langle 0 \text{ for } i \in [0 : |a|] \rangle$

(e) $= 0$.

Declaration II:25

The notation ab, where a, b are integers, will be used as a shorthand for the list $\langle \sum_r^{[0:i+1]} a_r b_{i-r}$ for $i \in [0 : |a| + |b| - 1]\rangle$.

Procedure II:48

Objective

Choose two polynomials a, b and a rational number c. The objective of the following instructions is to show that $\Lambda(ab, c) = \Lambda(a, c)\Lambda(b, c)$.

Implementation

1. Verify that $\Lambda(ab, c)$
   (a) $= \Lambda(\langle \sum_r^{[0:j+1]} a_r b_{j-r}$ for $j \in [0 : |a| + |b| - 1]\rangle, c)$
   (b) $= \sum_j^{[0:|a|+|b|-1]} (\sum_r^{[0:j+1]} a_r b_{j-r}) c^j$
   (c) $= \sum_j^{[0:|a|+|b|-1]} \sum_r^{[0:j+1]} a_r c^r b_{j-r} c^{j-r}$
   (d) $= \sum_r^{[0:|a|+|b|-1]} \sum_j^{[r:|a|+|b|-1]} a_r c^r b_{j-r} c^{j-r}$
   (e) $= \sum_r^{[0:|a|+|b|-1]} a_r c^r \sum_j^{[r:|a|+|b|-1]} b_{j-r} c^{j-r}$
   (f) $= \sum_r^{[0:|a|+|b|-1]} a_r c^r \sum_j^{[0:|a|+|b|-1-r]} b_j c^j$
   (g) $= \sum_r^{[0:|a|]} a_r c^r \sum_j^{[0:|a|+|b|-1-r]} b_j c^j$
   (h) $= \sum_r^{[0:|a|]} a_r c^r \sum_j^{[0:|b|]} b_j c^j$
   (i) $= (\sum_j^{[0:|a|]} a_j c^j)(\sum_j^{[0:|b|]} b_j c^j)$
   (j) $= \Lambda(a, c)\Lambda(b, c)$.

Procedure II:49

Objective

Choose a natural number c and two polynomials a, b. The objective of the following instructions is to show that $(ab)_c = \sum_r^{[0:c+1]} a_r b_{c-r}$.

Implementation

1. If $c < |a| + |b| - 1$, then do the following:
   (a) **Verify that** $(ab)_c = \sum_r^{[0:c+1]} a_r b_{c-r}$.
2. Otherwise do the following:
   (a) Verify that $c \geq |a| + |b| - 1$.
   (b) Verify that $(ab)_c$
      i. $= 0$
      ii. $= \sum_r^{[0:|a|]} 0a_r + \sum_r^{[|a|:c+1]} 0b_{c-r}$
      iii. $= \sum_r^{[0:|a|]} a_r b_{c-r} + \sum_r^{[|a|:c+1]} a_r b_{c-r}$
      iv. $= \sum_r^{[0:c+1]} a_r b_{c-r}$.

Procedure II:50

Objective

Choose four polynomials a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $ab = cd$.

Implementation

1. Using declaration II:19, verify that $a_i = c_i$ for $i \in [0 : \max(|a|, |c|) + \max(|b|, |d|) - 1]$.
2. Using declaration II:19, verify that $b_i = d_i$ for $i \in [0 : \max(|a|, |c|) + \max(|b|, |d|) - 1]$.
3. Hence verify that ab
   (a) $= \langle \sum_r^{[0:i+1]} a_r b_{i-r}$ for $i \in [0 : \max(|a|, |c|) + \max(|b|, |d|) - 1]\rangle$
   (b) $= \langle \sum_r^{[0:i+1]} c_r d_{i-r}$ for $i \in [0 : \max(|a|, |c|) + \max(|b|, |d|) - 1]\rangle$
   (c) $= cd$.

Procedure II:51

Objective

Choose three polynomials a, b, c. The objective of the following instructions is to show that $(ab)c = a(bc)$.

Implementation

1. Verify that $(ab)c$

   (a) $= \langle \sum_t^{[0:j+1]} (ab)_t c_{j-t}$ for $j \in [0 : |ab| + |c| - 1] \rangle$

   (b) $= \langle \sum_t^{[0:j+1]} \langle \sum_r^{[0:i+1]} a_r b_{i-r}$ for $i \in [0 : |a| + |b| - 1] \rangle_t c_{j-t}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (c) $= \langle \sum_t^{[0:j+1]} \sum_r^{[0:t+1]} a_r b_{t-r} c_{j-t}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (d) $= \langle \sum_r^{[0:j+1]} \sum_t^{[r:j+1]} a_r b_{t-r} c_{j-t}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (e) $= \langle \sum_r^{[0:j+1]} a_r \sum_t^{[r:j+1]} b_{t-r} c_{j-t}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (f) $= \langle \sum_r^{[0:j+1]} a_r \sum_t^{[0:j-r+1]} b_t c_{j-r-t}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (g) $= \langle \sum_r^{[0:j+1]} a_r \langle \sum_t^{[0:i+1]} b_t c_{i-t}$ for $i \in [0 : |b| + |c| - 1] \rangle_{j-r}$ for $j \in [0 : |a| + |b| + |c| - 2] \rangle$

   (h) $= \langle \sum_r^{[0:j+1]} a_r (bc)_{j-r}$ for $j \in [0 : |a| + |bc| - 1] \rangle$

   (i) $= a(bc)$.

Procedure II:52

Objective

Choose two polynomials a, b. The objective of the following instructions is to show that $ab = ba$.

Implementation

1. ab

   (a) $= \langle \sum_r^{[0:i+1]} a_r b_{i-r}$ for $i \in [0 : |a| + |b| - 1] \rangle$

   (b) $= \langle \sum_r^{[0:i+1]} b_r a_{i-r}$ for $i \in [0 : |a| + |b| - 1] \rangle$

   (c) $= ba$.

Procedure II:53

Objective

Choose a polynomial a. The objective of the following instructions is to show that $1a = a$.

Implementation

1. Verify that $1a$

   (a) $= \langle \sum_r^{[0:i+1]} 1_r a_{i-r}$ for $i \in [0 : |1| + |a| - 1] \rangle$

   (b) $= \langle 1_0 a_{i-0}$ for $i \in [0 : |a|] \rangle$

   (c) $= \langle a_i$ for $i \in [0 : |a|] \rangle$

   (d) $= a$.

Procedure II:54

Objective

Choose three polynomials a, b, c. The objective of the following instructions is to show that $a(b + c) = ab + ac$.

Implementation

1. $a(b + c)$

   (a) $= \langle \sum_r^{[0:i+1]} a_r (b + c)_{i-r}$ for $i \in [0 : |a| + |b + c| - 1] \rangle$

   (b) $= \langle \sum_r^{[0:i+1]} a_r (b_{i-r} + c_{i-r})$ for $i \in [0 : |a| + |b + c| - 1] \rangle$

   (c) $= \langle \sum_r^{[0:i+1]} (a_r b_{i-r} + a_r c_{i-r})$ for $i \in [0 : |a| + |b + c| - 1] \rangle$

   (d) $= \langle \sum_r^{[0:i+1]} a_r b_{i-r} + \sum_r^{[0:i+1]} a_r c_{i-r}$ for $i \in [0 : |a| + |b + c| - 1] \rangle$

   (e) $= \langle \sum_r^{[0:i+1]} a_r b_{i-r}$ for $i \in [0 : |a| + |b| - 1] \rangle + \langle \sum_r^{[0:i+1]} a_r c_{i-r}$ for $i \in [0 : |a| + |c| - 1] \rangle$

   (f) $= ab + ac$.

Declaration II:26

The notation λ will be used as a shorthand for the list $\langle 0, 1 \rangle$.

Procedure II:55

Objective

Choose a polynomial a. The objective of the following instructions is to show that $\lambda a = \langle 0 \rangle ^\frown a$.

Implementation

1. Verify that $|\lambda a| = |\lambda| + |a| - 1 = |a| + 1$.
2. For $j \in [1 : |a| + 1]$, do the following:
   (a) Verify that $(\lambda a)_j$
      i. $= \sum_r^{[0:j+1]} \lambda_r a_{j-r}$
      ii. $= \sum_r^{[0:j+1]} [r = 1] a_{j-r}$
      iii. $= a_{j-1}$
3. Verify that $(\lambda a)_0 = \sum_r^{[0:1]} \lambda_r a_{0-r} = \lambda_0 a_0 = 0$.
4. **Hence verify that** $\lambda a = \langle 0 \rangle ^\frown a$**.**

Procedure II:56

Objective

Choose a natural number n. The objective of the following instructions is to show that $\lambda^n = \langle [j = n] \text{ for } j \in [0 : n + 1] \rangle$.

Implementation

1. If $n = 0$, then do the following:
   (a) Verify that λ^n
      i. $= \lambda^0$
      ii. $= \langle 1 \rangle$
      iii. $= \langle [j = 0] \text{ for } j \in [0 : 1] \rangle$
      iv. $= \langle [j = n] \text{ for } j \in [0 : n + 1] \rangle$.
2. Otherwise do the following:
   (a) Execute procedure II:63 on $\langle n - 1 \rangle$.
   (b) Hence verify that $\lambda^{n-1} = \langle [j = n-1] \text{ for } j \in [0 : n] \rangle$.
   (c) Hence verify that λ^n
      i. $= \lambda \lambda^{n-1}$
      ii. $= \lambda \langle [j = n - 1] \text{ for } j \in [0 : n] \rangle$
      iii. $= \langle 0 \rangle ^\frown \langle [j = n - 1] \text{ for } j \in [0 : n] \rangle$
      iv. $= \langle [j = n] \text{ for } j \in [0 : n + 1] \rangle$.

Declaration II:27

The notation $\deg(a)$, where a is a polynomial such that $a \neq 0$, will be used as a shorthand for the largest natural number $j < |a|$ such that $a_j \neq 0$.

Procedure II:57

Objective

Choose two polynomials a, b such that $a = b$ and $a \neq 0$. The objective of the following instructions is to show that $\deg(a) = \deg(b)$.

Implementation

1. For $j \in [\max(|a|, |b|) : 0]$, do the following:
   (a) If $a_j = 0$, then do the following:
      i. Verify that $0 = a_j = b_j$.
   (b) Otherwise do the following:
      i. Verify that $0 \neq a_j = b_j$.
      ii. Hence verify that $j < \min(|a|, |b|)$.
      iii. **Hence verify that** $\deg(a) = j = \deg(b)$**.**

Procedure II:58

Objective

Let $\deg(0) = -1$. Choose two polynomials a, b such that $\deg(a) < \deg(b)$. The objective of the following instructions is to show that $\deg(a + b) = \deg(b)$.

Implementation

1. For $j \in [\max(|a|, |b|) : \deg(b) + 1]$, do the following:
   (a) Verify that $j > \deg(b) > \deg(a)$.
   (b) Hence verify that $a_j = b_j = 0$.
   (c) Hence verify that $(a + b)_j = a_j + b_j = 0$.
2. Verify that $\deg(b) > \deg(a)$.
3. Hence verify that $(a + b)_{\deg(b)} = a_{\deg(b)} + b_{\deg(b)} = 0 + b_{\deg(b)} = b_{\deg(b)} \neq 0$.

4. **Hence verify that** $\deg(a + b) = \deg(b)$**.**

Procedure II:59

Objective

Let $\deg(0) = -1$. Choose two polynomials a, b. The objective of the following instructions is to show that $\deg(a + b) \leq \max(\deg(a), \deg(b))$.

Implementation

1. For $j \in [\max(|a|, |b|) : \max(\deg(a), \deg(b)) + 1]$, do the following:
   (a) Verify that $j > \deg(a)$.
   (b) Verify that $j > \deg(b)$.
   (c) Hence verify that $a_j = b_j = 0$.
   (d) Hence verify that $(a + b)_j = a_j + b_j = 0$.
2. **Hence verify that** $\deg(a+b) \leq \max(\deg(a), \deg(b))$**.**

Procedure II:60

Objective

Let $\deg(0) = -1$. Choose a polynomial a. The objective of the following instructions is to show that $\deg(-a) = \deg(a)$.

Implementation

1. For $j \in [|a| : \deg(a) + 1]$, do the following:
   (a) Verify that $j > \deg(a)$.
   (b) Hence verify that $a_j = 0$.
   (c) Hence verify that $(-a)_j = -(a_j) = -0 = 0$.
2. Verify that $a_{\deg(a)} \neq 0$.
3. Hence verify that $(-a)_{\deg(a)} = -(a_{\deg(a)}) \neq 0$.
4. **Hence verify that** $\deg(-a) = \deg(a)$**.**

Procedure II:61

Objective

Choose two polynomials a, b such that $a \neq 0$ and $b \neq 0$. The objective of the following instructions is to show that $(ab)_{\deg(a)+\deg(b)} = a_{\deg(a)} b_{\deg(b)} \neq 0$.

Implementation

1. Verify that $a_{\deg(a)} \neq 0$.
2. Verify that $b_{\deg(b)} \neq 0$.
3. Hence verify that $(ab)_{\deg(a)+\deg(b)}$
   (a) $= \sum_r^{[0:\deg(a)+\deg(b)+1]} a_r b_{\deg(a)+\deg(b)-r}$
   (b) $= \sum_r^{[0:\deg(a)]} a_r b_{\deg(a)+\deg(b)-r} + a_{\deg(a)} b_{\deg(a)+\deg(b)-\deg(a)} + \sum_r^{[\deg(a)+1:\deg(a)+\deg(b)+1]} a_r b_{\deg(\cdots)}$
   (c) $= \sum_r^{[0:\deg(a)]} 0a_r + a_{\deg(a)} b_{\deg(b)} + \sum_r^{[\deg(a)+1:\deg(a)+\deg(b)+1]} 0b_{\deg(a)+\deg(b)-r}$
   (d) $= a_{\deg(a)} b_{\deg(b)}$
   (e) $\neq 0$.

Procedure II:62

Objective

Choose two polynomials a, b such that $a \neq 0$ and $b \neq 0$. The objective of the following instructions is to show that $\deg(ab) = \deg(a) + \deg(b)$.

Implementation

1. For $j \in [\deg(a) + \deg(b) + 1 : |a| + |b| - 1]$, do the following:
   (a) Verify that $(ab)_j$
      i. $= \sum_r^{[0:j+1]} a_r b_{j-r}$
      ii. $= \sum_r^{[0:\deg(a)+1]} a_r b_{j-r} + \sum_r^{[\deg(a)+1:j+1]} a_r b_{j-r}$
      iii. $= \sum_r^{[0:\deg(a)+1]} 0a_r + \sum_r^{[\deg(a)+1:j+1]} 0b_{j-r}$
      iv. $= 0$.
2. Now using procedure II:61, verify that $(ab)_{\deg(a)+\deg(b)} = a_{\deg(a)} b_{\deg(b)} \neq 0$.

3. **Hence verify that** $\deg(ab) = \deg(a) + \deg(b)$**.**

Declaration II:28

The phrase "monic polynomial" will be used to refer to polynomials p such that $p \neq 0$ and $p_{\deg(p)} = 1$.

Declaration II:29

The notation $\mathrm{mon}(p)$, where p is a polynomial such that $p \neq 0$, will be used as a shorthand for $\frac{p}{p_{\deg(p)}}$.

Procedure II:63

Objective

Choose two polynomials, a, b such that $b \neq 0$. The objective of the following instructions is to construct two polynomials u, w such that $a = ub + w$ and $\deg(w) < \deg(b)$.

Implementation

1. If $\deg(a) \geq \deg(b)$, then do the following:
   (a) Let $y = \frac{a_{\deg(a)}}{b_{\deg(b)}} \lambda^{\deg(a)-\deg(b)}$
   (b) Let $e = a - yb$.
   (c) Verify that $\deg(e) < \deg(a)$.
   (d) Execute procedure II:63 on the tuple $\langle e, b\rangle$ and let $\langle c, d\rangle$ receive.
   (e) Verify that $cb + d = e$.
   (f) **Verify that** $\deg(d) < \deg(b)$**.**
   (g) Therefore verify that $cb + d = a - yb$
   (h) **Therefore verify that** $(y + c)b + d = a$**.**
   (i) **Now yield the tuple** $\langle y + c, d\rangle$**.**
2. Otherwise do the following:
   (a) **Verify that** $0b + a = a$**.**
   (b) **Verify that** $\deg(a) < \deg(b)$**.**
   (c) **Yield the tuple** $\langle 0, a\rangle$**.**

Declaration II:30

The notation $a \operatorname{div} b$, where a, b are polynomials, will be used to refer to the first part of the pair yielded by executing procedure II:63 on $\langle a, b\rangle$.

Declaration II:31

The notation $a \bmod b$, where a, b are polynomials, will be used to refer to the second part of the pair yielded by executing procedure II:63 on $\langle a, b\rangle$.

Procedure II:64

Objective

Choose a polynomial a and a rational number b. The objective of the following instructions is to show that $a \bmod (\lambda - b) = \Lambda(a, b)$.

Implementation

1. Let $d = \lambda - b$.
2. Verify that $d \neq 0$.
3. Let $c = a \operatorname{div} d$.
4. Verify that $a = cd + (a \bmod d)$.
5. Also verify that $\deg(a \bmod d) < \deg(d) = 1$.
6. Hence verify that $\deg(a \bmod d) = 0$.
7. Now verify that $\Lambda(a, b)$
   (a) $= \Lambda(cd + (a \bmod d), b)$
   (b) $= \Lambda(cd, b) + \Lambda(a \bmod d, b)$
   (c) $= \Lambda(c, b)\Lambda(d, b) + \Lambda(a \bmod d, b)$
   (d) $= \Lambda(c, b)(-b + b) + \Lambda(a \bmod d, b)$
   (e) $= 0\Lambda(c, b) + \Lambda(a \bmod d, b)$
   (f) $= \Lambda(a \bmod d, b)$
   (g) $= a \bmod d$.

Procedure II:65

Objective

Choose a polynomial $p \neq 0$ and rational numbers $a_0 < a_1 < \cdots < a_{\deg(p)-2} < a_{\deg(p)-1}$ in such a way that $\Lambda(p, a_i) = 0$ for $i \in [0 : \deg(p)]$. The objective of the following instructions is to either show that $p = q_0 \prod_j^{[0:n]} (\lambda - a_j)$ or $0 \neq 0$.

Implementation

1. Let $n = \deg(p)$.
2. Let $q = p$.
3. For i in $[0 : n]$, do the following:
   (a) Verify that $p = q \prod_k^{[0:i]} (\lambda - a_k)$.
   (b) If $\Lambda(q, a_i) \neq 0$, do the following:
      i. Verify that $\Lambda(p, a_i) = \Lambda(q \prod_k^{[0:i]} (\lambda - a_k), a_i) = \Lambda(q, a_i) \prod_k^{[0:i]} \Lambda(\lambda - a_k, a_i) = \Lambda(q, a_i) \prod_k^{[0:i]} (a_i - a_k) \neq 0$.
      ii. Therefore using the precondition and (i), verify that $0 \neq 0$.
      iii. **Abort procedure.**
   (c) Otherwise do the following:
      i. Let $b = q$.
      ii. Let $q = b \operatorname{div} (\lambda - a_i)$.
      iii. Verify that $\Lambda(b, a_i) = 0$.
      iv. Execute procedure II:64 on $\langle b, a_i \rangle$.
      v. Hence verify that $b = (\lambda - a_i) q + b \bmod (\lambda - a_i) = (\lambda - a_i) q$.
      vi. Hence verify that $p = q \prod_j^{[0:i+1]} (\lambda - a_j)$.
4. Now verify that $0 \neq p = q \prod_j^{[0:n]} (\lambda - a_j)$.
5. Hence verify that $q \neq 0$.
6. Hence verify that $n = \deg(p) = \deg(q) + \sum_j^{[0:n]} \deg(\lambda - a_j) = \deg(q) + n$.
7. Hence verify that $\deg(q) = 0$.
8. Hence verify that $q = q_0 \neq 0$.
9. **Hence verify that** $p = q_0 \prod_j^{[0:n]} (\lambda - a_j)$**.**

Procedure II:66

Objective

Choose a polynomial $p \neq 0$ and rational numbers $a_0 < a_1 < \cdots < a_{\deg(p)-1} < a_{\deg(p)}$ in such a way that $\Lambda(p, a_i) = 0$ for $i \in [0 : \deg(p) + 1]$. The objective of the following instructions is to show that $0 \neq 0$.

Implementation

1. Let $n = \deg(p)$.
2. Execute procedure II:65 on $\langle p, a \rangle$.
3. Hence verify that $p = q_0 \prod_j^{[0:n]} (\lambda - a_j)$.
4. Hence verify that $\Lambda(p, a_n) = \Lambda(q_0 \prod_j^{[0:n]} (\lambda - a_j), a_n) = \Lambda(q_0, a_n) \prod_j^{[0:n]} \Lambda(\lambda - a_j, a_n) = q_0 \prod_j^{[0:n]} (a_n - a_j) \neq 0$.
5. Therefore using the precondition and (4), verify that $0 = \Lambda(p, a_n) \neq 0$.
6. **Abort procedure.**

Procedure II:67

Objective

Choose a polynomial p and a rational number X. The objective of the following instructions is to construct a rational number a and a procedure $q(y, z)$ to show that $|\Lambda(p, z) - \Lambda(p, y)| \leq a|z - y|$ when two rational numbers y, z such that $|y| \leq X$ and $|z| \leq X$ are chosen.

Implementation

1. Let $a = \sum_r^{[1:|p|]} r|p_r|X^{r-1}$.
2. Let $q(y, z)$ be the following procedure:
   (a) Verify that $|\Lambda(p, z) - \Lambda(p, y)|$
      i. $= |(\sum_r^{[0:|p|]} p_r z^r) - (\sum_r^{[0:|p|]} p_r y^r)|$
      ii. $= |\sum_r^{[1:|p|]} p_r (z^r - y^r)|$
      iii. $= |\sum_r^{[1:|p|]} p_r (z - y) \sum_t^{[0:r]} z^t y^{r-1-t}|$
      iv. $= |(z - y) \sum_r^{[1:|p|]} p_r \sum_t^{[0:r]} z^t y^{r-1-t}|$

v. $= |z-y||\sum_r^{[1:|p|]} p_r \sum_t^{[0:r]} z^t y^{r-1-t}|$

vi. $\leq |z-y| \sum_r^{[1:|p|]} |p_r \sum_t^{[0:r]} z^t y^{r-1-t}|$

vii. $= |z-y| \sum_r^{[1:|p|]} |p_r||\sum_t^{[0:r]} z^t y^{r-1-t}|$

viii. $\leq |z-y| \sum_r^{[1:|p|]} |p_r| \sum_t^{[0:r]} |z^t y^{r-1-t}|$

ix. $= |z-y| \sum_r^{[1:|p|]} |p_r| \sum_t^{[0:r]} |z|^t |y|^{r-1-t}$

x. $\leq |z-y| \sum_r^{[1:|p|]} |p_r| \sum_t^{[0:r]} X^t X^{r-1-t}$

xi. $= |z-y| \sum_r^{[1:|p|]} |p_r| \sum_t^{[0:r]} X^{r-1}$

xii. $= |z-y| \sum_r^{[1:|p|]} r|p_r| X^{r-1}$

xiii. $= a|z-y|$

3. **Yield the tuple** $\langle a, q\rangle$**.**

Procedure II:68

Objective

Choose a polynomial f. Choose rational numbers $a < b$ such that $\mathrm{sgn}(\Lambda(f,a)) = -\mathrm{sgn}(\Lambda(f,b))$. Choose a rational number target $B > 0$. The objective of the following instructions is to construct a rational number d such that $a \leq d \leq b$ and $|f(d)| < B$.

Implementation

1. Execute procedure II:67 on $\langle f, \max(|a|,|b|)\rangle$ and let $\langle G, q\rangle$ receive the result.
2. Let $c = a$ and $d = b$.
3. Until $G|d-c| < B$
   (a) Let $e = \frac{c+d}{2}$.
   (b) **Verify that** $a \leq c < e < d \leq b$**.**
   (c) If $\mathrm{sgn}(\Lambda(f,c)) = -\mathrm{sgn}(\Lambda(f,e))$, then do the following:
      i. Let $d = e$.
   (d) Otherwise if $\mathrm{sgn}(\Lambda(f,e)) = -\mathrm{sgn}(\Lambda(f,d))$, then do the following:
      i. Let $c = e$.
   (e) Otherwise if $\Lambda(f,e) = 0$, then do the following:
      i. **Verify that** $|\Lambda(f,e)| = 0 < B$**.**
      ii. **Yield the tuple** $\langle e\rangle$**.**
4. Execute procedure q on $\langle c, d\rangle$.
5. **Hence verify that** $|\Lambda(f,c)| < |\Lambda(f,d) - \Lambda(f,c)| \leq G|d-c| < B$**.**
6. **Yield the tuple** $\langle c\rangle$**.**

Procedure II:69

Objective

Choose a polynomial $f \neq 0$ and pairs of rational numbers $(a_{\deg(f)}, b_{\deg(f)}), (a_{\deg(f)-1}, b_{\deg(f)-1}), \cdots, (a_0, b_0)$ in such a way that:

1. $a_{\deg(f)} < b_{\deg(f)} \leq a_{\deg(f)-1} < b_{\deg(f)-1} \leq \cdots \leq a_1 < b_1 \leq a_0 < b_0$.
2. $\mathrm{sgn}(\Lambda(f,a_i)) = -\mathrm{sgn}(\Lambda(f,b_i))$ for $i \in [0 : \deg(f)+1]$.

The objective of the following instructions is to show that $1 = -1$.

Implementation

1. If $\deg(f) > 0$:
   (a) Let $B = \min_k^{[0:\deg(f)-1]} \min(|\Lambda(f,a_k)|, |\Lambda(f,b_k)|)$.
   (b) For $k \in [0 : \deg(f)]$, verify that $|\Lambda(f,a_k)| \geq B$.
   (c) Execute procedure II:68 on the formal polynomial f, interval $(a_{\deg(f)}, b_{\deg(f)})$, and target of B. Let the tuple $\langle d\rangle$ receive the result.
   (d) Verify that $|\Lambda(f,d)| < B$.
   (e) Let $h = f \operatorname{div} (\lambda - d)$.
   (f) Execute procedure II:64 on $\langle f, d\rangle$.
   (g) Hence verify that $f = (\lambda-d)h + f \bmod (\lambda - d) = (\lambda-d)h + \Lambda(f,d)$.
   (h) Hence verify that $0 \neq f - \Lambda(f,d) = (\lambda-d)h$.
   (i) Hence verify that $h \neq 0$.
   (j) Hence verify that $\deg(f) = \deg(f - \Lambda(f,d)) = \deg((\lambda-d)h) = \deg(\lambda-d) + \deg(h) = 1 + \deg(h)$.
   (k) Hence verify that $\deg(h) = \deg(f) - 1$.

(l) For $k \in [0 : \deg(h) + 1]$, do the following:

i. If $\Lambda(f, a_k) \geq B$, in-order verify that:

A. $\Lambda(f, a_k) \geq B > |\Lambda(f, d)| \geq \Lambda(f, d)$.

B. $\Lambda(f, a_k) - \Lambda(f, d) > 0$.

C. $(a_k - d)\Lambda(h, a_k) > 0$.

D. $\Lambda(h, a_k) > 0$.

E. $\Lambda(f, b_k) \leq -B < -|\Lambda(f, d)| \leq \Lambda(f, d)$.

F. $\Lambda(f, b_k) - \Lambda(f, d) < 0$.

G. $(b_k - d)\Lambda(h, b_k) < 0$.

H. $\Lambda(h, b_k) < 0$.

ii. Otherwise, if $\Lambda(f, a_k) \leq -B$, do the following:

A. **Using steps analogous to (ji), verify that $\Lambda(h, a_k) < 0$.**

B. **Using steps analogous to (ji), verify that $\Lambda(h, b_k) > 0$.**

(m) Execute procedure II:69 on h and $a_{\deg(h)} < b_{\deg(h)} \leq a_{\deg(h)-1} < b_{\deg(h)-1} \leq \cdots \leq a_1 < b_1 \leq a_0 < b_0$.

2. Otherwise, do the following:

(a) Verify that $\deg(f) = 0$.

(b) Therefore verify that $f = f_0 \neq 0$.

(c) Therefore verify that $\operatorname{sgn}(f_0) = \operatorname{sgn}(\Lambda(f, a_0)) = -\operatorname{sgn}(\Lambda(f, b_0)) = -\operatorname{sgn}(f_0)$.

(d) **Therefore verify that $1 = -1$.**

(e) **Abort procedure.**

Procedure II:70

Objective

Choose two lists of polynomials s, q in such a way that:

1. $|s| > 1$.
2. For i in $[0 : |s|]$, $\deg(s_i) = i$.
3. For i in $[0 : |s|]$, $\operatorname{sgn}((s_i)_i) = \operatorname{sgn}((s_m)_m)$.
4. For i in $[1 : |s| - 1]$, $s_{i-1} + s_{i+1} = q_i s_i$.

The objective of the following instructions is to construct lists of polynomials g, h such that $g_i s_{i+1} + h_i s_i = 1$ for i in $[0 : |s| - 1]$.

Implementation

1. Let $m = |s| - 1$
2. Let $g = h = \langle\rangle$.
3. If $m > 1$, do the following:

(a) Verify that $q_{m-1}s_{m-1} - s_m = s_{m-2}$.

(b) Execute procedure II:70 on $s_{[0:m]}$ and $q_{[1:m-1]}$ and let the tuple $\langle, , g, h\rangle$ receive.

(c) Verify that $g_{m-2}s_{m-1} + h_{m-2}s_{m-2} = 1$.

(d) Let $g_{m-1} = -h_{m-2}$.

(e) Let $h_{m-1} = g_{m-2} + h_{m-2}q_{m-1}$.

(f) Therefore verify that $g_{m-1}s_m + h_{m-1}s_{m-1}$

i. $= g_{m-2}s_{m-1} + h_{m-2}(q_{m-1}s_{m-1} - s_m)$

ii. $= g_{m-2}s_{m-1} + h_{m-2}s_{m-2}$

iii. $= 1$.

4. Otherwise, if $m = 1$ do the following:

(a) Let $g_0 = 0$.

(b) Let $h_0 = \frac{1}{s_0}$.

(c) **Therefore verify that $g_0 s_1 + h_0 s_0 = 1$.**

5. **Yield the tuple $\langle s, q, g, h\rangle$.**

Declaration II:32

The notation $J_s(x)$, where s is a list of polynomials and x is a rational number, will be used as a shorthand for the number of changes observed when the list $\operatorname{sgn}(\Lambda(s, x))$ is iterated through linearly.

Procedure II:71

Objective

Execute procedure II:70 and let $\langle s, q, g, h\rangle$ receive. Choose a rational number X. The objective of the following instructions is to construct a rational number l and a procedure $u(c, d)$ to show that either $0 < 0$ or $|J_s(d) - J_s(c)| = [\operatorname{sgn}(\Lambda(s_{|s|-1}, c)) \neq \operatorname{sgn}(\Lambda(s_{|s|-1}, d))]$, when rational numbers c, d such that $|c| \leq X$, $|d| \leq X$, $|d-c| \leq l$, $0 \notin \Lambda(s, c)$, and $0 \notin \Lambda(s, d)$ are chosen.

Implementation

1. Execute procedure II:67 on $\langle s, X\rangle$ and let $\langle G, t\rangle$ receive the result.
2. Let $B = \max_i^{[0:|s|]} G_i$.
3. Let $C = \max_i^{[0:|s|-1]} \max(|\Lambda(\|g_i\|, X)|, |\Lambda(\|h_i\|, X)|)$.
4. Let $D = \max_i^{[1:|s|-1]} \max(|\Lambda(\|q_i\|, X)|, 2)$.
5. Let $l = \frac{1}{BCD}$.
6. Let $u(c, d)$ be the following procedure:

(a) Let $i = 0$.

(b) If $i + 1 < |s|$, do the following:

i. Verify that $\operatorname{sgn}(\Lambda(s_i, c)) = \operatorname{sgn}(\Lambda(s_i, d))$.

ii. Verify that $J_{s_{[0:i+1]}}(c) = J_{s_{[0:i+1]}}(d)$.

iii. If $\operatorname{sgn}(\Lambda(s_{i+1}, c)) = \operatorname{sgn}(\Lambda(s_{i+1}, d))$, do the following:

A. Verify that $J_{s_{[0:i+2]}}(c) = J_{s_{[0:i+2]}}(d)$.

B. Set i to $i + 1$ and go to (b).

iv. Otherwise if $\operatorname{sgn}(\Lambda(s_{i+1}, c)) = \operatorname{sgn}(\Lambda(s_{i+1}, d))$ or $i + 2 \geq |s|$, do the following:

A. Verify that $\operatorname{sgn}(\Lambda(s_{i+1}, c)) \neq \operatorname{sgn}(\Lambda(s_{i+1}, d))$.

B. Verify that $|J_{s_{[0:i+2]}}(c) - J_{s_{[0:i+2]}}(d)| = 1$.

C. Verify that $i + 2 = |s|$.

D. Go to (c).

v. Execute procedure 2.5 auxilliary procedure on i.

vi. If $\operatorname{sgn}(\Lambda(s_{i+2}, c)) \neq \operatorname{sgn}(\Lambda(s_{i+2}, d))$, do the following:

A. Execute procedure t_{i+2} on $\langle c, d\rangle$.

B. Hence verify that $|\Lambda(s_{i+2}, c)| < |\Lambda(s_{i+2}, d) - \Lambda(s_{i+2}, c)| = |(d-c)G_{i+2}| \leq \frac{1}{BCD} \cdot B = \frac{1}{CD} = \frac{1}{C} \cdot \frac{1}{D} \leq \frac{1}{C}(1 - \frac{1}{D})$.

C. Using (A) and (i), verify that $\frac{1}{C}(1 - \frac{1}{D}) < |s_{i+2}(c)| < \frac{1}{C}(1 - \frac{1}{D})$.

D. **Abort procedure.**

vii. Otherwise if $\operatorname{sgn}(\Lambda(s_i, c)) = \operatorname{sgn}(\Lambda(s_{i+2}, c))$, do the following:

A. Verify that $2\frac{1}{C}(1 - \frac{1}{D}) < |\Lambda(s_i, c)| + |\Lambda(s_{i+2}, c)| = |\Lambda(s_i, c) + \Lambda(s_{i+2}, c)| = |q_{i+1}(c)\Lambda(s_{i+1}, c)| < D\frac{1}{CD}$.

B. Verify that $2(1 - \frac{1}{D}) < 1$.

C. Using (B) and the construction of D, verify that $2 \leq D < 2$.

D. **Abort procedure.**

viii. Otherwise, do the following:

A. Verify that $\operatorname{sgn}(\Lambda(s_i, d)) = \operatorname{sgn}(\Lambda(s_i, c)) \neq \operatorname{sgn}(\Lambda(s_{i+2}, c)) = \operatorname{sgn}(\Lambda(s_{i+2}, d))$.

B. Therefore verify that $1 = J_{s_{[0:i+3]}}(c) - J_{s_{[0:i+1]}}(c) = J_{s_{[0:i+3]}}(d) - J_{s_{[0:i+1]}}(d)$.

C. Therefore verify that $J_{s_{[0:i+1]}}(c) + 1 = J_{s_{[0:i+3]}}(c) = J_{s_{[0:i+3]}}(d) = J_{s_{[0:i+1]}}(d) + 1$.

D. Set i to $i + 2$ and go to (b).

(c) If $\operatorname{sgn}(\Lambda(s_{|s|-1}, c)) = \operatorname{sgn}(\Lambda(s_{|s|-1}, d))$, then do the following:

i. **Verify that $J_s(c) = J_s(d)$.**

(d) Otherwise do the following:

i. **Verify that $|J_s(d) - J_s(c)| = 1$.**

7. **Yield the tuple $\langle l, u\rangle$.**

Auxilliary Procedure

Objective Choose a non-negative integer $i < m$ and natural numbers c, d such that $\operatorname{sgn}(\Lambda(s_{i+1}, c)) \neq \operatorname{sgn}(\Lambda(s_{i+1}, d))$ and $i + 2 \leq m$. The objective of the following instructions is to show that $|\Lambda(s_{i+1}, c)| < \frac{1}{CD}$, $|\Lambda(s_{i+1}, d)| < \frac{1}{CD}$, $\frac{1}{C}(1 - \frac{1}{D}) < |\Lambda(s_i, c)|$, $\frac{1}{C}(1 - \frac{1}{D}) < |\Lambda(s_i, d)|$, $\frac{1}{C}(1 - \frac{1}{D}) < |\Lambda(s_{i+2}, c)|$, and $\frac{1}{C}(1 - \frac{1}{D}) < |\Lambda(s_{i+2}, d)|$.

Implementation

1. Verify the following in order:

(a) Execute procedure t_{i+1} on $\langle c, d\rangle$.

(b) $|\Lambda(s_{i+1},c)| < |\Lambda(s_{i+1},c) - \Lambda(s_{i+1},d)| = |c-d||G_{i+1}| \le |c-d|B \le \frac{1}{BCD} \cdot B = \frac{1}{CD}$

(c) $|\Lambda(s_{i+1},d)| < |\Lambda(s_{i+1},c) - \Lambda(s_{i+1},d)| \le \frac{1}{CD}$

(d) $1 = \Lambda(g_i,c)\Lambda(s_{i+1},c) + \Lambda(h_i,c)\Lambda(s_i,c) = |\Lambda(g_i,c)\Lambda(s_{i+1},c) + \Lambda(h_i,c)\Lambda(s_i,c)| \le |\Lambda(g_i,c)||\Lambda(s_{i+1},c)| + |\Lambda(h_i,c)||\Lambda(s_i,c)| < C(\frac{1}{CD} + |\Lambda(s_i,c)|)$

(e) $\frac{1}{C}(1-\frac{1}{D}) < |\Lambda(s_i,c)|$

(f) $1 < C(\frac{1}{CD} + |\Lambda(s_i,d)|)$

(g) $\frac{1}{C}(1-\frac{1}{D}) < |\Lambda(s_i,d)|$

(h) $1 = \Lambda(g_{i+1},c)\Lambda(s_{i+2},c) + \Lambda(h_{i+1},c)\Lambda(s_{i+1},c) = |\Lambda(g_{i+1},c)\Lambda(s_{i+2},c) + \Lambda(h_{i+1},c)\Lambda(s_{i+1},c)| \le |\Lambda(g_{i+1},c)||\Lambda(s_{i+2},c)| + |\Lambda(h_{i+1},c)||\Lambda(s_{i+1},c)| < C(|\Lambda(s_{i+2},c)| + \frac{1}{CD})$

(i) $\frac{1}{C}(1-\frac{1}{D}) < |\Lambda(s_{i+2},c)|$

(j) $1 < C(|\Lambda(s_{i+2},d)| + \frac{1}{CD})$

(k) $\frac{1}{C}(1-\frac{1}{D}) < |\Lambda(s_{i+2},d)|$

Procedure II:72

Objective

Choose a polynomial $p \neq 0$. Choose a rational number $k > 1 + \max_i^{[0:\deg(p)]} |\frac{p_i}{p_{\deg(p)}}|$. The objective of the following instructions is to show that $\operatorname{sgn}(\Lambda(p,k)) = \operatorname{sgn}(p_{\deg(p)})$.

Implementation

1. Let $n = \deg(p)$.
2. In reverse order verify the following:

(a) $\operatorname{sgn}(\Lambda(p,k)) = \operatorname{sgn}(p_{\deg(p)})$

(b) $\operatorname{sgn}(p_n k^n + p_{n-1}k^{n-1} + \cdots + p_0 k^0) = \operatorname{sgn}(p_n)$

(c) $\operatorname{sgn}(k^n + \frac{p_{n-1}}{p_n}k^{n-1} + \cdots + \frac{p_0}{p_n}k^0) = 1$

(d) $k^n + \frac{p_{n-1}}{p_n}k^{n-1} + \cdots + \frac{p_0}{p_n}k^0 > 0$

(e) $k^n > -(\frac{p_{n-1}}{p_n}k^{n-1} + \cdots + \frac{p_0}{p_n}k^0)$

(f) $k^n > |\frac{p_{n-1}}{p_n}k^{n-1} + \cdots + \frac{p_0}{p_n}k^0|$

(g) $k^n > |\max_i^{[0:n]}|\frac{p_i}{p_n}|(k^{n-1} + \cdots + k^0)|$

(h) $k^n > \max_i^{[0:n]}|\frac{p_i}{p_n}|\frac{k^n-1}{k-1}$

(i) $k^{n+1} - k^n > \max_i^{[0:n]}|\frac{p_i}{p_n}|(k^n - 1)$

(j) $k^{n+1} - (1+\max_i^{[0:n]}|\frac{p_i}{p_n}|)k^n + \max_i^{[0:n]}|\frac{p_i}{p_n}| > 0$

(k) $k > 1 + \max_i^{[0:n]}|\frac{p_i}{p_n}|$

Procedure II:73

Objective

Choose a polynomial $p \neq 0$. Choose a rational number $k < -(1 + \max_i^{[0:\deg(p)]}|\frac{p_i}{p_{\deg(p)}}|)$. The objective of the following instructions is to show that $\operatorname{sgn}(\Lambda(p,k)) = (-1)^{\deg(p)} \operatorname{sgn}(p_{\deg(p)})$.

Implementation

1. Let $t = \deg(p)$.
2. Let $q = \langle (-1)^{t-i} p_i \text{ for } i \in [0:t+1] \rangle$.
3. Verify that $k < -(1 + \max_i^{[1:t+1]}|\frac{q_i}{q_{\deg(q)}}|)$.
4. Therefore verify that $-k > 1 + \max_i^{[0:t]}|\frac{q_i}{q_{\deg(q)}}|$.
5. Execute procedure II:72 on $\langle q, -k \rangle$.
6. Hence verify that $(-1)^t \operatorname{sgn}(\Lambda(p,k))$

(a) $= \operatorname{sgn}((-1)^t \Lambda(p,k))$

(b) $= \operatorname{sgn}((-1)^t \sum_i^{[0:t+1]} p_i k^i)$

(c) $= \operatorname{sgn}(\sum_i^{[0:t+1]} (-1)^i (-1)^{t-i} p_i k^i)$

(d) $= \operatorname{sgn}(\sum_i^{[0:t+1]} q_i (-k)^i)$

(e) $= \operatorname{sgn}(\Lambda(q,-k))$

(f) $= \operatorname{sgn}(q_t)$

(g) $= \operatorname{sgn}(p_t)$.

7. **Therefore verify that** $\operatorname{sgn}(\Lambda(p,k)) = (-1)^t(-1)^t \operatorname{sgn}(\Lambda(p,k)) = (-1)^t \operatorname{sgn}(p_t)$**.**

Procedure II:74

Objective

Choose a list of polynomials, s, and rational numbers a, l, c such that $a < c$ and $l > 0$. The objective of the following instructions is to either show that $0 < 0$ or to construct a list of rational numbers, b, such that $a = b_0 < b_1 < \cdots < b_{|b|-1} = c$, $b_i - b_{i-1} \leq l$ for i in $[1 : |b|]$, and $0 \notin \Lambda(s, b_i)$ for i in $[1 : |b| - 1]$.

Implementation

1. Let $e = \langle\langle\rangle, \langle\rangle, \cdots, \langle\rangle\rangle$.
2. Let $f = \sum_r^{[0:|s|]} \deg(s_r)$.
3. Let $b = \langle a\rangle$.
4. Let $d = b_1$.
5. While $d + l < c$, do the following:
   (a) Let $m = l$.
   (b) While $0 \in \Lambda(s, d + m)$ and $\sum|e| \leq f$, do the following:
      i. Let $0 \leq i < |s|$ be an integer such that $\Lambda(s_i, d + m) = 0$.
      ii. Append $d + m$ onto e_i.
      iii. Set $m = \frac{m}{2}$
   (c) If $\sum|e| > f$, then do the following:
      i. If $|e_i| \leq \deg(s_i)$ for $0 \leq i < |s|$, then do the following:
         A. Verify that $\sum|e| \leq f$.
         B. Therefore using (c), verify that $\sum|e| \leq f < \sum|e|$.
         C. **Abort procedure.**
      ii. Otherwise, do the following:
         A. Let $0 \leq i < |s|$ be an integer such that $|e_i| > \deg(s_i)$.
         B. Execute procedure II:66 on s_i and a sorted e_i.
         C. **Abort procedure.**
   (d) Otherwise, do the following:
      i. **Verify that** $0 \notin \Lambda(s, d + m)$**.**
      ii. Append $d + m$ onto b.
      iii. **Verify that** $0 < b_{|b|-1} - b_{|b|-2} = m \leq l$**.**
      iv. Set d to $d + m$.
      v. Using (5), verify that $d < c$.
6. Verify that $d < c$.
7. Verify that $d + l \geq c$.
8. **Therefore verify that** $0 < c - d \leq l$**.**
9. Append c onto b.
10. **Yield** $\langle b\rangle$**.**

Procedure II:75

Objective

Execute procedure II:70 and let $\langle s, q, g, h\rangle$ receive. Let $m = |s| - 1$. The objective of the following instructions is to either show that $0 < 0$ or to construct two lists of rational numbers c, d such that $c_0 < d_0 \leq c_1 < d_1 \leq \cdots \leq c_{m-1} < d_{m-1}$ and $0 \neq \operatorname{sgn}(\Lambda(s_m, c_i)) = -\operatorname{sgn}(\Lambda(s_m, d_i))$ for i in $[0 : m]$.

Implementation

1. Let $U = 1 + \max_i^{[0:|s|]} \left(1 + \max_j^{[1:i+1]} |\frac{(s_i)_{i-j}}{(s_i)_i}|\right)$
2. Using procedure II:72, verify that $J(U) = 0$.
3. Using procedure II:73, verify that $J(-U) = m$.
4. Execute procedure II:71 on the tuple $\langle s, q, U\rangle$ and let $\langle l, u\rangle$ receive.
5. Execute procedure II:74 on s with endpoints $-U, U$ and a step size of l and let $\langle e\rangle$ receive the result.
6. Let $c = d = \langle\rangle$.
7. For $i = 1$ to $i = |e| - 1$:
   (a) Execute procedure u on the tuple $\langle e_{i-1}, e_i\rangle$.
   (b) If $J_m(e_{i-1}) \neq J_m(e_i)$, then do the following:
      i. Append e_{i-1} to c.
      ii. Append e_i to d.

iii. Verify that $0 \neq |J_s(d_{|d|-1}) - J_s(c_{|c|-1})| = [\mathrm{sgn}(\Lambda(s_{|s|-1}, c_{|c|-1})) \neq \mathrm{sgn}(\Lambda(s_{|s|-1}, d_{|d|-1}))]$.

iv. Therefore verify that $\mathrm{sgn}(s_m(c_{|c|-1})) \neq \mathrm{sgn}(s_m(d_{|d|-1}))$.

v. Therefore verify that $|J_m(d_{|d|-1}) - J_m(c_{|c|-1})| = 1$.

vi. Also verify that $0 \notin \Lambda(s, c_{|c|-1})$.

vii. Hence verify that $\Lambda(s_m, c_{|c|-1}) \neq 0$.

viii. Also verify that $0 \notin \Lambda(s, d_{|d|-1})$.

ix. Hence verify that $\Lambda(s_m, d_{|d|-1}) \neq 0$.

x. **Therefore verify that** $0 \neq \mathrm{sgn}(s_m(c_{|c|-1})) = -\mathrm{sgn}(s_m(d_{|d|-1}))$**.**

xi. **Also verify that** $d_{|d|-2} \leq c_{|c|-1} < d_{|d|-1}$**.**

8. If $|c| = |d| < m$, then do the following:

(a) Verify that each change of $J_m(x)$ over the course of (7) was by 1.

(b) Verify that $J_m(x)$ changed less than m times over the course of (12).

(c) Therefore verify that $|J_m(U) - J_m(-U)| < m$.

(d) Therefore using (2) and (3), verify that $m = |J_m(U) - J_m(-U)| < m$.

(e) **Abort procedure.**

9. Otherwise, do the following:

(a) **Verify that** $m \leq |c| = |d|$**.**

(b) **Yield the tuple** $\langle c, d \rangle$**.**

Procedure II:76

Objective

Choose two lists of polynomials s, q and a non-negative integer k in such a way that, letting $m = |s| - 1$,

1. $k < m$.

2. For $k \leq i \leq m$, $\deg(s_i) = i$.

3. For $k < i < m$, $s_{i-1} + s_{i+1} = q_i s_i$.

Let $\deg(0) = -1$. The objective of the following instructions is to construct polynomials g, h such that $s_k = g s_{m-1} + h s_m$, $\deg(g) = m - 1 - k$, and $\deg(h) = m - 2 - k$.

Implementation

1. If $k < m - 2$, do the following:

(a) Verify that $s_k + s_{k+2} = q_{k+1} s_{k+1}$.

(b) Therefore verify that $s_k = q_{k+1} s_{k+1} - s_{k+2}$.

(c) Execute procedure II:76 on $s, q, k+1$ and let the tuple $\langle g_1, h_1 \rangle$ receive.

(d) Verify that $s_{k+1} = g_1 s_{m-1} + h_1 s_m$.

(e) Verify that $\deg(g_1) = m - 1 - (k + 1) = m - k - 2$.

(f) Verify that $\deg(h_1) = m - 2 - (k + 1) = m - k - 3$.

(g) Execute procedure II:76 on $s, q, k+2$ and let the tuple $\langle g_2, h_2 \rangle$ receive.

(h) Verify that $s_{k+2} = g_2 s_{m-1} + h_2 s_m$.

(i) Verify that $\deg(g_2) = m - 1 - (k + 2) = m - k - 3$.

(j) Verify that $\deg(h_2) = m - 2 - (k + 2) = m - k - 4$.

(k) Let $g = q_{k+1} g_1 - g_2$.

(l) **Verify that** $\deg(g) = \max(1 + (m - k - 2), m - k - 3) = m - 1 - k$**.**

(m) Let $h = q_{k+1} h_1 - h_2$.

(n) **Verify that** $\deg(h) = \max(1 + (m - k - 3), m - k - 4) = m - 2 - k$**.**

(o) **Verify that** $s_k = q_{k+1}(g_1 s_{m-1} + h_1 s_m) - (g_2 s_{m-1} + h_2 s_m) = (q_{k+1} g_1 - g_2) s_{m-1} + (q_{k+1} h_1 - h_2) s_m = g s_{m-1} + h s_m$**.**

2. Otherwise, if $k = m - 2$ do the following:

(a) Verify that $s_{m-2} + s_m = q_{m-1} s_{m-1}$.

(b) Let $g = q_{m-1}$.

(c) **Verify that** $\deg(g) = 1 = m - 1 - k$**.**

(d) Let $h = -1$.

(e) **Verify that** $\deg(h) = 0 = m - 2 - k$**.**

(f) **Therefore verify that** $s_k = s_{m-2} = q_{m-1}s_{m-1} - s_m = gs_{m-1} + hs_m$**.**

3. Otherwise, if $k = m - 1$ do the following:

(a) Let $g = 1$.

(b) **Verify that** $\deg(g) = 0 = m - 1 - k$**.**

(c) Let $h = 0$.

(d) **Verify that** $\deg(h) = -1 = m - 2 - k$**.**

(e) **Verify that** $s_k = s_{m-1} = gs_{m-1} + hs_m$**.**

4. **Yield the tuple** $\langle g, h \rangle$**.**

Part III

Complex Arithmetic

Declaration III:0

The phrase ”complex number” will be used as a shorthand for an ordered pair of rational numbers.

Declaration III:1

The phrase ”the real part of a” and the notation $\mathrm{re}(a)$, where a is a complex number, will be used as a shorthand for the first entry of a.

Declaration III:2

The phrase ”the imaginary part of a” and the notation $\mathrm{im}(a)$, where a is a complex number, will be used as a shorthand for the second entry of a.

Declaration III:3

The phrase ”$a = b$”, where a, b are complex numbers, will be used as a shorthand for ”$\mathrm{re}(a) = \mathrm{re}(b)$ and $\mathrm{im}(a) = \mathrm{im}(b)$”.

Procedure III:0

Objective

Choose a complex number a. The objective of the following instructions is to show that $a = a$.

Implementation

1. Verify that $\mathrm{re}(a) = \mathrm{re}(a)$.
2. Verify that $\mathrm{im}(a) = \mathrm{im}(a)$.
3. **Hence verify that $a = a$.**

Procedure III:1

Objective

Choose two complex numbers a, b such that $a = b$. The objective of the following instructions is to show that $b = a$.

Implementation

1. Verify that $\mathrm{re}(a) = \mathrm{re}(b)$.
2. Hence verify that $\mathrm{re}(b) = \mathrm{re}(a)$.
3. Verify that $\mathrm{im}(a) = \mathrm{im}(b)$.
4. Hence verify that $\mathrm{im}(b) = \mathrm{im}(a)$.
5. **Hence verify that $b = a$.**

Procedure III:2

Objective

Choose three complex numbers a, b, c such that $a = b$ and $b = c$. The objective of the following instructions is to show that $a = c$.

Implementation

1. Verify that $\mathrm{re}(a) = \mathrm{re}(b)$.
2. Verify that $\mathrm{re}(b) = \mathrm{re}(c)$.
3. Hence verify that $\mathrm{re}(a) = \mathrm{re}(c)$.
4. Verify that $\mathrm{im}(a) = \mathrm{im}(b)$.
5. Verify that $\mathrm{im}(b) = \mathrm{im}(c)$.
6. Hence verify that $\mathrm{im}(a) = \mathrm{im}(c)$.
7. **Hence verify that $a = c$.**

Declaration III:4

The notation $a+b$, where a, b are complex numbers, will be used as a shorthand for the pair $\langle \mathrm{re}(a)+\mathrm{re}(b), \mathrm{im}(a) + \mathrm{im}(b)\rangle$.

Procedure III:3

Objective

Choose two complex numbers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $a + b = c + d$.

Implementation

1. Using declaration III:3, verify that $\mathrm{re}(a) = \mathrm{re}(c)$.
2. Using declaration III:3, verify that $\mathrm{im}(a) = \mathrm{im}(c)$.
3. Using declaration III:3, verify that $\mathrm{re}(b) = \mathrm{re}(d)$.
4. Using declaration III:3, verify that $\mathrm{im}(b) = \mathrm{im}(d)$.
5. Hence verify that $a + b$

(a) $= \langle \mathrm{re}(a), \mathrm{im}(a)\rangle + \langle \mathrm{re}(b), \mathrm{im}(b)\rangle$

(b) $= \langle \mathrm{re}(a) + \mathrm{re}(b), \mathrm{im}(a) + \mathrm{im}(b)\rangle$

(c) $= \langle \mathrm{re}(c) + \mathrm{re}(d), \mathrm{im}(c) + \mathrm{im}(d)\rangle$

(d) $= \langle \mathrm{re}(c), \mathrm{im}(c)\rangle + \langle \mathrm{re}(d), \mathrm{im}(d)\rangle$

(e) $= c + d$.

Procedure III:4

Objective

Choose three complex numbers a, b, c. The objective of the following instructions is to show that $(a + b) + c = a + (b + c)$.

Implementation

1. Verify that $(a + b) + c$

(a) $= \langle \mathrm{re}(a)+\mathrm{re}(b), \mathrm{im}(a)+\mathrm{im}(b)\rangle+\langle \mathrm{re}(c), \mathrm{im}(c)\rangle$

(b) $= \langle (\mathrm{re}(a) + \mathrm{re}(b)) + \mathrm{re}(c), (\mathrm{im}(a) + \mathrm{im}(b)) + \mathrm{im}(c)\rangle$

(c) $= \langle \mathrm{re}(a) + (\mathrm{re}(b) + \mathrm{re}(c)), \mathrm{im}(a) + (\mathrm{im}(b) + \mathrm{im}(c))\rangle$

(d) $= \langle \mathrm{re}(a), \mathrm{im}(a)\rangle+\langle \mathrm{re}(b)+\mathrm{re}(c), \mathrm{im}(b)+\mathrm{im}(c)\rangle$

(e) $= a + (b + c)$.

Procedure III:5

Objective

Choose two complex numbers a, b. The objective of the following instructions is to show that $a + b = b + a$.

Implementation

1. $a + b$

(a) $= \langle \mathrm{re}(a) + \mathrm{re}(b), \mathrm{im}(a) + \mathrm{im}(b)\rangle$

(b) $= \langle \mathrm{re}(b) + \mathrm{re}(a), \mathrm{im}(b) + \mathrm{im}(a)\rangle$

(c) $= b + a$.

Declaration III:5

The notation a, where a is a rational number, will contextually be used as a shorthand for the pair $\langle a, 0\rangle$.

Procedure III:6

Objective

Choose a complex number a. The objective of the following instructions is to show that $0 + a = a$.

Implementation

1. Verify that $0 + a$

(a) $= \langle 0, 0\rangle + \langle \mathrm{re}(a), \mathrm{im}(a)\rangle$

(b) $= \langle 0 + \mathrm{re}(a), 0 + \mathrm{im}(a)\rangle$

(c) $= \langle \mathrm{re}(a), \mathrm{im}(a)\rangle$

(d) $= a$.

Declaration III:6

The notation $-a$, where a is a complex number, will be used as a shorthand for the pair $\langle -\mathrm{re}(a), -\mathrm{im}(a)\rangle$.

Procedure III:7

Objective

Choose a complex number a. The objective of the following instructions is to show that $-a + a = 0$.

Implementation

1. Verify that $-a + a$

(a) $= (-a) + a$

(b) $= \langle -\operatorname{re}(a), -\operatorname{im}(a)\rangle + \langle \operatorname{re}(a), \operatorname{im}(a)\rangle$

(c) $= \langle -\operatorname{re}(a) + \operatorname{re}(a), -\operatorname{im}(a) + \operatorname{im}(a)\rangle$

(d) $= \langle 0, 0\rangle$

(e) $= 0$.

Declaration III:7

The notation ab, where a, b are complex numbers, will be used as a shorthand for the pair $\langle \operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b), \operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b)\rangle$.

Procedure III:8

Objective

Choose four complex numbers a, b, c, d such that $a = c$ and $b = d$. The objective of the following instructions is to show that $ab = cd$.

Implementation

1. Using declaration III:3, verify that $\operatorname{re}(a) = \operatorname{re}(c)$.
2. Using declaration III:3, verify that $\operatorname{im}(a) = \operatorname{im}(c)$.
3. Using declaration III:3, verify that $\operatorname{re}(b) = \operatorname{re}(d)$.
4. Using declaration III:3, verify that $\operatorname{im}(b) = \operatorname{im}(d)$.
5. Hence verify that ab

(a) $= \langle \operatorname{re}(a), \operatorname{im}(a)\rangle\langle \operatorname{re}(b), \operatorname{im}(b)\rangle$

(b) $= \langle \operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b), \operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b)\rangle$

(c) $= \langle \operatorname{re}(c)\operatorname{re}(d) - \operatorname{im}(c)\operatorname{im}(d), \operatorname{re}(c)\operatorname{im}(d) + \operatorname{im}(c)\operatorname{re}(d)\rangle$

(d) $= \langle \operatorname{re}(c), \operatorname{im}(c)\rangle\langle \operatorname{re}(d), \operatorname{im}(d)\rangle$

(e) $= cd$.

Procedure III:9

Objective

Choose three complex numbers a, b, c. The objective of the following instructions is to show that $(ab)c = a(bc)$.

Implementation

1. Verify that $(ab)c$

(a) $= \langle \operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b), \operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b)\rangle\langle \operatorname{re}(c), \operatorname{im}(c)\rangle$

(b) $= \langle (\operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b))\operatorname{re}(c) - (\operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b))\operatorname{im}(c), (\operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b))\operatorname{im}(c) + (\operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b))\operatorname{re}(c)\rangle$

(c) $= \langle \operatorname{re}(a)(\operatorname{re}(b)\operatorname{re}(c) - \operatorname{im}(b)\operatorname{im}(c)) - \operatorname{im}(a)(\operatorname{re}(b)\operatorname{im}(c) + \operatorname{im}(b)\operatorname{re}(c)), \operatorname{re}(a)(\operatorname{re}(b)\operatorname{im}(c) + \operatorname{im}(b)\operatorname{re}(c)) + \operatorname{im}(a)(\operatorname{re}(b)\operatorname{re}(c) - \operatorname{im}(b)\operatorname{im}(c))\rangle$

(d) $= \langle \operatorname{re}(a), \operatorname{im}(a)\rangle\langle \operatorname{re}(b)\operatorname{re}(c) - \operatorname{im}(b)\operatorname{im}(c), \operatorname{re}(b)\operatorname{im}(c) + \operatorname{im}(b)\operatorname{re}(c)\rangle$

(e) $= a(bc)$.

Procedure III:10

Objective

Choose two complex numbers a, b. The objective of the following instructions is to show that $ab = ba$.

Implementation

1. ab

(a) $= \langle \operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b), \operatorname{re}(a)\operatorname{im}(b) + \operatorname{im}(a)\operatorname{re}(b)\rangle$

(b) $= \langle \operatorname{re}(b)\operatorname{re}(a) - \operatorname{im}(b)\operatorname{im}(a), \operatorname{re}(b)\operatorname{im}(a) + \operatorname{im}(b)\operatorname{re}(a)\rangle$

(c) $= ba$.

Procedure III:11

Objective

Choose a complex number a. The objective of the following instructions is to show that $1a = a$.

Implementation

1. Verify that $1a$

(a) $= \langle 1, 0\rangle\langle \operatorname{re}(a), \operatorname{im}(a)\rangle$

(b) $= \langle 1\operatorname{re}(a) - 0\operatorname{im}(a), 1\operatorname{im}(a) + 0\operatorname{re}(a)\rangle$

(c) $= \langle \operatorname{re}(a), \operatorname{im}(a)\rangle$

(d) $= a$.

Procedure III:12

Objective

Choose a non-negative integer a and a complex number x. The objective of the following instructions is to show that $(1+x)^a = \sum_r^{[0:a+1]} \binom{a}{r} x^r$.

Implementation

Instructions are analogous to those of procedure I:88.

Declaration III:8

The notation $\overline{a}$, where a is a complex number, will be used as a shorthand for $\langle \operatorname{re}(a), -\operatorname{im}(a)\rangle$.

Procedure III:13

Objective

Choose two complex numbers a, b. The objective of the following instructions is to show that $\overline{a+b} = \overline{a} + \overline{b}$.

Implementation

1. Verify that $\overline{a+b}$

(a) $= \langle \operatorname{re}(a+b), -\operatorname{im}(a+b)\rangle$

(b) $= \langle \operatorname{re}(a) + \operatorname{re}(b), -\operatorname{im}(a) - \operatorname{im}(b)\rangle$

(c) $= \overline{a} + \overline{b}$.

Procedure III:14

Objective

Choose two complex numbers a, b. The objective of the following instructions is to show that $\overline{ab} = \overline{a}\overline{b}$.

Implementation

1. Verify that $\overline{ab}$

(a) $= \langle \operatorname{re}(ab), -\operatorname{im}(ab)\rangle$

(b) $= \langle \operatorname{re}(a)\operatorname{re}(b) - \operatorname{im}(a)\operatorname{im}(b)), -\operatorname{re}(a)\operatorname{im}(b) - \operatorname{im}(a)\operatorname{re}(b)\rangle$

(c) $= \langle \operatorname{re}(a), -\operatorname{im}(a)\rangle\langle \operatorname{re}(b), -\operatorname{im}(b)\rangle$

(d) $= \overline{a}\overline{b}$.

Declaration III:9

The notation $\|a\|^2$, where a is a complex number, will be used as a shorthand for $\operatorname{re}(a)^2 + \operatorname{im}(a)^2$.

Procedure III:15

Objective

Choose a complex number a. The objective of the following instructions is to show that $a\overline{a} = \|a\|^2$.

Implementation

1. **Verify that $a\overline{a} = \|a\|^2$.**

Procedure III:16

Objective

Choose a list of complex numbers a. The objective of the following instructions is to show that $\|\sum_r^{[0:|a|]} a_r\|^2 \leq |a| \sum_r^{[0:|a|]} \|a_r\|^2$.

Implementation

1. Verify that $\|\sum_r^{[0:|a|]} a_r\|^2$
   (a) $= \sum_r^{[0:|a|]} \sum_k^{[0:|a|]} a_r \overline{a_k}$
   (b) $= \sum_r^{[0:|a|]} \|a_r\|^2 + 2 \sum_r^{[0:|a|]} \sum_k^{[r+1:|a|]} (\operatorname{re}(a_r) \operatorname{re}(a_k) + \operatorname{im}(a_r) \operatorname{im}(a_k))$
   (c) $= \sum_r^{[0:|a|]} \|a_r\|^2 + 2 \sum_r^{[0:|a|]} \sum_k^{[r+1:|a|]} (\operatorname{re}(a_r)^2 - (\operatorname{re}(a_r) - \operatorname{re}(a_k))^2 + \operatorname{re}(a_k)^2 + \operatorname{im}(a_r)^2 - (\operatorname{im}(a_r) - \operatorname{im}(a_k))^2 + \operatorname{im}(a_k)^2)$
   (d) $\leq \sum_r^{[0:|a|]} \|a_r\|^2 + \sum_r^{[0:|a|]} \sum_k^{[r+1:|a|]} (\operatorname{re}(a_r)^2 + \operatorname{re}(a_k)^2 + \operatorname{im}(a_r)^2 + \operatorname{im}(a_k)^2)$
   (e) $= \sum_r^{[0:|a|]} \|a_r\|^2 + \sum_r^{[0:|a|]} \sum_k^{[r+1:|a|]} (\|a_r\|^2 + \|a_k\|^2)$
   (f) $= \sum_r^{[0:|a|]} \|a_r\|^2 + \frac{1}{2} \sum_r^{[0:|a|]} \sum_k^{[0:r]^\frown[r+1:|a|]} (\|a_r\|^2 + \|a_k\|^2)$
   (g) $= \sum_r^{[0:|a|]} \|a_r\|^2 + \frac{1}{2} (\sum_r^{[0:|a|]} (|a|-1) \|a_r\|^2 + \sum_k^{[0:|a|]} (|a|-1) \|a_k\|^2)$
   (h) $= \sum_r^{[0:|a|]} \|a_r\|^2 + \sum_r^{[0:|a|]} (|a|-1) \|a_r\|^2$
   (i) $= |a| \sum_r^{[0:|a|]} \|a_r\|^2$

Procedure III:17

Objective

Choose a list of complex numbers a. The objective of the following instructions is to show that $\frac{\|a_0\|^2}{|a|} - \sum_r^{[1:|a|]} \|a_r\|^2 \leq \|a_0 - \sum_r^{[1:|a|]} a_r\|^2$.

Implementation

1. Using procedure III:16, verify that $\|a_0\|^2$
   (a) $= \|\sum_r^{[1:|a|]} a_r + (a_0 - \sum_r^{[1:|a|]} a_r)\|^2$
   (b) $\leq |a| \sum_r^{[1:|a|]} \|a_r\|^2 + |a| \|a_0 - \sum_r^{[1:|a|]} a_r\|^2$
2. **Therefore verify that $\frac{\|a_0\|^2}{|a|} - \sum_r^{[1:|a|]} \|a_r\|^2 \leq \|a_0 - \sum_r^{[1:|a|]} a_r\|^2$.**

Procedure III:18

Objective

Choose a list of complex numbers a and a list of rational numbers b such that $|a| = |b|$ and $\|a_i\|^2 \leq {b_i}^2$ for each $i \in [0:|a|]$. The objective of the following instructions is to show that $\|\sum_r^{[0:|a|]} a_r\|^2 \leq (\sum_r^{[0:|b|]} b_r)^2$.

Implementation

1. If $|a| = 0$, then do the following:
   (a) **Verify that $\|\sum_i^{[0:|a|]} a_i\|^2 = \|0\|^2 = (\sum_i^{[0:|b|]} b_i)^2$.**
2. Otherwise do the following:
   (a) Verify that $|a| > 0$.
   (b) Using procedure III:18 on $a_{[1:|a|]}$ and $b_{[1:|b|]}$, verify that $\|\sum_i^{[1:|a|]} a_i\|^2 \leq (\sum_i^{[1:|b|]} b_i)^2$.
   (c) Verify that $\operatorname{re}(\overline{a_0} \sum_i^{[1:|a|]} a_i)^2$
      i. $\leq \|\overline{a_0} \sum_i^{[1:|a|]} a_i\|^2$
      ii. $= \|\overline{a_0}\|^2 \|\sum_i^{[1:|a|]} a_i\|^2$
      iii. $\leq {b_0}^2 (\sum_i^{[1:|a|]} b_i)^2$.
   (d) Hence verify that $\|\sum_i^{[0:|a|]} a_i\|^2$
      i. $= (a_0 + \sum_i^{[1:|a|]} a_i)\overline{(a_0 + \sum_i^{[1:|a|]} a_i)}$
      ii. $= \|a_0\|^2 + a_0 \overline{\sum_i^{[1:|a|]} a_i} + \overline{a_0} \sum_i^{[1:|a|]} a_i + \|\sum_i^{[1:|a|]} a_i\|^2$
      iii. $\leq {b_0}^2 + \overline{\overline{a_0} \sum_i^{[1:|a|]} a_i} + \overline{a_0} \sum_i^{[1:|a|]} a_i + (\sum_i^{[1:|a|]} b_i)^2$
      iv. $= {b_0}^2 + 2 \operatorname{re}(\overline{a_0} \sum_i^{[1:|a|]} a_i) + (\sum_i^{[1:|a|]} b_i)^2$
      v. $\leq {b_0}^2 + 2 b_0 \sum_i^{[1:|a|]} b_i + (\sum_i^{[1:|a|]} b_i)^2$
      vi. $= (b_0 + \sum_i^{[1:|a|]} b_i)^2$
      vii. $= (\sum_i^{[0:|a|]} b_i)^2$.

Procedure III:19

Objective

Choose two complex numbers a, d and two rational numbers b, c such that $\|a\|^2 \leq b^2 < c^2 \leq \|d\|^2$. The objective of the following instructions is to show that $\|d-a\|^2 \geq (c-b)^2$.

Implementation

1. Verify that $\mathrm{re}(\frac{a}{d})^2$
   (a) $= \mathrm{re}(\frac{a\overline{d}}{\|d\|^2})^2$
   (b) $= \frac{\mathrm{re}(a\overline{d})^2}{\|d\|^4}$
   (c) $\leq \frac{\|a\overline{d}\|^2}{\|d\|^4}$
   (d) $= \frac{\|a\|^2\|d\|^2}{\|d\|^4}$
   (e) $= \frac{\|a\|^2}{\|d\|^2}$
   (f) $\leq \frac{b^2}{c^2}$
   (g) $= (\frac{b}{c})^2$.
2. Now verify that $\mathrm{re}(\frac{a}{d}) \leq \frac{b}{c} < 1$.
3. Hence verify that $\|d-a\|^2$
   (a) $= \|\frac{d-a}{d}\|^2\|d\|^2$
   (b) $= (\mathrm{re}(1-\frac{a}{d})^2 + \mathrm{im}(1-\frac{a}{d})^2)\|d\|^2$
   (c) $\geq \mathrm{re}(1-\frac{a}{d})^2\|d\|^2$
   (d) $= (1-\mathrm{re}(\frac{a}{d}))^2\|d\|^2$
   (e) $\geq (1-\frac{b}{c})^2c^2$
   (f) $= (c-b)^2$.

Declaration III:10

The notation $\frac{1}{a}$, where a is a complex number, will be used as a shorthand for the pair $\frac{1}{\|a\|^2}\overline{a}$.

Procedure III:20

Objective

Choose a complex number a such that $a \neq 0$. The objective of the following instructions is to show that $\frac{1}{a}a = 1$.

Implementation

1. Using declaration III:3, verify that $\mathrm{re}(a) \neq \mathrm{re}(0) = 0$ or $\mathrm{im}(a) \neq \mathrm{im}(0) = 0$.
2. Hence verify that $\|a\|^2 = \mathrm{re}(a)^2 + \mathrm{im}(a)^2 > 0$.
3. Hence verify that $\frac{1}{a}a$
   (a) $= (\frac{1}{\|a\|^2}\overline{a})a$
   (b) $= \frac{1}{\|a\|^2}(\overline{a}a)$
   (c) $= \frac{1}{\|a\|^2}\|a\|^2$
   (d) $= 1$.

Procedure III:21

Objective

Choose three complex numbers a, b, c. The objective of the following instructions is to show that $a(b+c) = ab + ac$.

Implementation

1. $a(b+c)$
   (a) $= \langle \mathrm{re}(a), \mathrm{im}(a)\rangle\langle \mathrm{re}(b)+\mathrm{re}(c), \mathrm{im}(b)+\mathrm{im}(c)\rangle$
   (b) $= \langle \mathrm{re}(a)(\mathrm{re}(b)+\mathrm{re}(c)) - \mathrm{im}(a)(\mathrm{im}(b)+\mathrm{im}(c)), \mathrm{re}(a)(\mathrm{im}(b)+\mathrm{im}(c)) + \mathrm{im}(a)(\mathrm{re}(b)+\mathrm{re}(c))\rangle$
   (c) $= \langle(\mathrm{re}(a)\,\mathrm{re}(b) - \mathrm{im}(a)\,\mathrm{im}(b)) + (\mathrm{re}(a)\,\mathrm{re}(c) - \mathrm{im}(a)\,\mathrm{im}(c)), (\mathrm{re}(a)\,\mathrm{im}(b) + \mathrm{im}(a)\,\mathrm{re}(b)) + (\mathrm{re}(a)\,\mathrm{im}(c) + \mathrm{im}(a)\,\mathrm{re}(c))\rangle$
   (d) $= \langle \mathrm{re}(a)\,\mathrm{re}(b) - \mathrm{im}(a)\,\mathrm{im}(b), \mathrm{re}(a)\,\mathrm{im}(b) + \mathrm{im}(a)\,\mathrm{re}(b)\rangle + \langle \mathrm{re}(a)\,\mathrm{re}(c) - \mathrm{im}(a)\,\mathrm{im}(c), \mathrm{re}(a)\,\mathrm{im}(c) + \mathrm{im}(a)\,\mathrm{re}(c)\rangle$
   (e) $= ab + ac$.

Declaration III:11

The notation i will be used as a shorthand for $\langle 0, 1\rangle$.

Procedure III:22

Objective

Choose an integer a. The objective of the following instructions is to show that $i^{4a} = 1$, $i^{4a+1} = i$, $i^{4a+2} = -1$, and $i^{4a+3} = -i$.

Implementation

1. Verify that $i^2 = -1$.
2. Hence verify that $i^4 = (-1)^2 = 1$.
3. **Hence verify that** $i^{4a} = (i^4)^a = 1^a = 1$**.**
4. **Hence verify that** $i^{4a+1} = i^{4a}i = 1i = i$**.**
5. **Hence verify that** $i^{4a+2} = i^{4a+1}i = i^2 = -1$**.**
6. **Hence verify that** $i^{4a+3} = i^{4a+2}i = (-1)i = -i$**.**

Declaration III:12

The notation $\exp_n(a)$, where a is a complex number, will be used as a shorthand for $(1 + \frac{a}{n})^n$.

Procedure III:23

Objective

Choose a rational number a and a positive integer n such that $-n < a$. The objective of the following instructions is to show that $\exp_n(a) \geq 1 + a$.

Implementation

1. Using procedure II:32, verify that $\exp_n(a)$
   (a) $= (1 + \frac{a}{n})^n$
   (b) $\geq 1 + n\frac{a}{n}$
   (c) $= 1 + a$.

Procedure III:24

Objective

Choose a rational number a and a positive integer n such that $-n < a < 1$. The objective of the following instructions is to show that $\exp_n(a) \leq \frac{1}{1-a}$.

Implementation

1. Using procedure II:32, verify that $\exp_n(a)$
   (a) $= (\frac{n+a}{n})^n$
   (b) $= (\frac{n}{n+a})^{-n}$
   (c) $= \frac{1}{(1+\frac{-a}{n+a})^n}$
   (d) $\leq \frac{1}{1+\frac{-an}{n+a}}$
   (e) $\leq \frac{1}{1-a}$.

Procedure III:25

Objective

Choose a rational number a and a positive integer n such that $a > -n$. The objective of the following instructions is to show that $\frac{\exp_{n+1}(a)}{\exp_n(a)} \geq 1$.

Implementation

1. Using procedure II:32, verify that $\frac{\exp_{n+1}(a)}{\exp_n(a)}$
   (a) $= \frac{(\frac{n+1+a}{n+1})^n}{(\frac{n+a}{n})^n}(1 + \frac{a}{n+1})$
   (b) $= (\frac{(n+1+a)n}{(n+1)(n+a)})^n(1 + \frac{a}{n+1})$
   (c) $= (\frac{n^2+n+na}{n^2+an+n+a})^n(1 + \frac{a}{n+1})$
   (d) $= (1 - \frac{a}{(n+1)(n+a)})^n(1 + \frac{a}{n+1})$
   (e) $\geq (1 - \frac{an}{(n+1)(n+a)})(1 + \frac{a}{n+1})$
   (f) $= 1 + \frac{a(n+a)}{(n+1)(n+a)} - \frac{an}{(n+1)(n+a)} - \frac{a^2n}{(n+1)^2(n+a)}$
   (g) $= 1 + \frac{a^2}{(n+1)(n+a)} - \frac{a^2n}{(n+1)^2(n+a)}$
   (h) $= 1 + \frac{a^2}{(n+1)^2(n+a)}$
   (i) ≥ 1

Procedure III:26

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct positive rational numbers a, b such that $a > 1$, and a procedure, p, to show that $\exp_n(x) \leq a^2$ when given a rational number x and a positive integer $n \geq b$ such that $x^2 \leq X^2$.

Implementation

1. Let $a = 2^{\lceil X \rceil}$.
2. Let $b = X$.
3. Let $p(x, n)$ be the following procedure:
   (a) Verify that $x^2 \leq X^2$.
   (b) Therefore verify that $-X \leq x \leq X$
   (c) Therefore verify that $-1 \leq \frac{x}{n} \leq 1$.
   (d) Therefore verify that $0 \leq 1 + \frac{x}{n} \leq 2$.
   (e) Hence using procedure III:24 and procedure III:25, verify that $\exp_n(x)$
      i. $\leq \exp_n(X)$
      ii. $\leq (1 + \frac{X}{2\lceil X \rceil n})^{2\lceil X \rceil n}$
      iii. $= ((1 + \frac{\frac{X}{2\lceil X \rceil}}{n})^n)^{2\lceil X \rceil}$
      iv. $= \exp_n(\frac{X}{2\lceil X \rceil})^{2\lceil X \rceil}$
      v. $\leq (\frac{1}{1 - \frac{X}{2\lceil X \rceil}})^{2\lceil X \rceil}$
      vi. $\leq 2^{2\lceil X \rceil}$
      vii. $= a^2$.
4. **Yield the tuple $\langle a, b, p \rangle$.**

Procedure III:27

Objective

Choose a rational number $X \leq 0$. The objective of the following instructions is to construct two rational numbers $a > 0, b$, and a procedure $p(x, n)$ to show that $\exp_n(x) \geq a^2$ when given a rational number x and a positive integer $n > b$ such that $X \leq x \leq 0$.

Implementation

1. Execute procedure III:26 on $\langle -2X \rangle$ and let $\langle c, d, q \rangle$ receive.
2. Let $a = c^{-1}$.
3. Let $b = \max(-2X, d)$.
4. Let $p(x, n)$ be the following procedure:
   (a) Verify that $X \leq x \leq 0$.
   (b) Therefore verify that $2X \leq 2x \leq 0$.
   (c) Therefore verify that $0 \leq -2x \leq -2X$.
   (d) Hence execute procedure q on $\langle -2x, n \rangle$.
   (e) Therefore verify that $\exp_n(-2x) \leq c^2$.
   (f) Also verify that $n > b \geq -2X \geq -2x \geq 0$.
   (g) Therefore verify that $-\frac{n}{2} \leq x \leq 0$.
   (h) Therefore verify that $\frac{n}{2} \leq n + x < n$.
   (i) Hence verify that $\exp_n(x)$
      i. $= (\frac{n+x}{n})^n$
      ii. $= (\frac{n}{n+x})^{-n}$
      iii. $= (1 - \frac{x}{n+x})^{-n}$
      iv. $\geq (1 - \frac{x}{\frac{1}{2}n})^{-n}$
      v. $= (1 - \frac{2x}{n})^{-n}$
      vi. $= (\exp_n(-2x))^{-1}$
      vii. $\geq (c^2)^{-1}$
      viii. $= a^2$.
5. **Yield the tuple $\langle a, b, p \rangle$.**

Procedure III:28

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers $a > 0, b$, and a procedure $p(x, n)$ to show that $\exp_n(x) \geq a^2$ when given a rational number x and a positive integer $n > b$ such that $x^2 \leq X^2$.

Implementation

1. Execute procedure III:27 on $\langle -X\rangle$ and let $\langle c, b, q\rangle$ receive.
2. Let $a = \min(1, c)$.
3. Let $p(x, n)$ be the following procedure:
   (a) If $x < 0$, then do the following:
      i. Verify that $x^2 \leq X^2$.
      ii. Therefore verify that $-X \leq x \leq 0$.
      iii. Hence execute procedure q on x.
      iv. **Hence verify that** $\exp_n(x) \geq c^2 \geq a^2$**.**
   (b) Otherwise do the following:
      i. Verify that $x \geq 0$.
      ii. **Using procedure III:23, verify that** $\exp_n(x) \geq 1 + x \geq 1 \geq a^2$**.**
4. **Yield the tuple** $\langle a, b, p\rangle$**.**

Procedure III:29

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct positive rational numbers a, b such that $a > 1$, and a procedure, $p(x, n)$, to show that $\|\exp_n(x)\|^2 \leq a^2$ when a complex number x and a positive integer $n > b$ such that $\|x\|^2 \leq X^2$ are chosen.

Implementation

1. Let $c = 2X + X^2$.
2. Execute procedure III:26 on $\langle c\rangle$ and let $\langle a, b, q\rangle$.
3. Let $p(x, n)$ be the following procedure:
   (a) Verify that $n > b$.
   (b) Let $y = 2|\mathrm{re}(x)| + \|x\|^2$.
   (c) Verify that $|\mathrm{re}(x)|^2 \leq \|x\|^2 \leq X^2$.
   (d) Therefore verify that $|\mathrm{re}(x)| \leq X$.
   (e) Therefore verify that $|y| = y \leq 2X+X^2 = c$.
   (f) Hence execute procedure q on $\langle y, n\rangle$.
   (g) Hence verify that $\exp_n(y) \leq a^2$.
   (h) Now using procedure III:15 verify that $\|\exp_n(x)\|^2$
      i. $= \exp_n(x)\overline{\exp_n(x)}$
      ii. $= (1 + \frac{x}{n})^n(1 + \frac{\overline{x}}{n})^n$
      iii. $= (1 + \frac{2\,\mathrm{re}(x)}{n} + \frac{\|x\|^2}{n^2})^n$
      iv. $\leq (1 + \frac{2|\mathrm{re}(x)|}{n} + \frac{\|x\|^2}{n^2})^n$
      v. $\leq (1 + \frac{2|\mathrm{re}(x)|+\|x\|^2}{n})^n$
      vi. $= \exp_n(y)$
      vii. $\leq a^2$.
4. **Yield the tuple** $\langle a, b, p\rangle$**.**

Procedure III:30

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, b and a procedure, $p(x, n)$, to show that $\|\exp_n(x)\|^2 \geq a^2$ when a rational number x and a positive integer $n > b$ such that $\|x\|^2 \leq X^2$ are chosen.

Implementation

1. Let $c = 2X + X^2$.
2. Execute procedure III:28 on $\langle c\rangle$ and let $\langle a, d, q\rangle$ receive.
3. Let $b = \max(c, d)$.
4. Let $p(x, n)$ be the following procedure:
   (a) Verify that $n > b \geq d$.
   (b) Let $y = 2|\mathrm{re}(x)| + \|x\|^2$.
   (c) Verify that $|-y| = y \leq 2X + X^2 = c$.
   (d) Hence execute procedure q on $\langle -y, n\rangle$.
   (e) Hence verify that $\exp_n(-y) \geq a^2$.
   (f) Also, verify that $n > b \geq c \geq y$.
   (g) Hence verify that $\|\exp_n(x)\|^2$
      i. $= \exp_n(x)\overline{\exp_n(x)}$

ii. $= (1+\frac{x}{n})^n(1+\frac{\overline{x}}{n})^n$

iii. $= (1+\frac{2\,\mathrm{re}(x)}{n}+\frac{\|x\|^2}{n^2})^n$

iv. $\geq (1-\frac{2|\mathrm{re}(x)|}{n}-\frac{\|x\|^2}{n^2})^n$

v. $\geq (1-\frac{2|\mathrm{re}(x)|+\|x\|^2}{n})^n$

vi. $= \exp_n(-y)$

vii. $\geq a^2$.

5. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:31

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct rational numbers a, b such that $a > 0$, and a procedure, p, to show that $\exp_n(x+y) \equiv \exp_n(x)\exp_n(y)$ (err $\frac{axy}{n}$) (err $\frac{aX^2}{n}$) when two complex numbers x, y and a positive integer $n > b$ such that $\|x\|^2 \leq X^2$, $\|y\|^2 \leq X^2$ are chosen.

Implementation

1. Execute procedure III:29 on $\langle 2X\rangle$ and let $\langle c, b, q\rangle$ receive.
2. Let $a = \max(1, c)^3$.
3. Let $p(x, y, n)$ be the following procedure:

(a) Verify that $\|x\|^2 \leq X^2$.

(b) Hence execute q on $\langle x, n\rangle$.

(c) Hence verify that $\|\exp_n(x)\|^2 \leq c^2$.

(d) Verify that $\|y\|^2 \leq X^2$.

(e) Hence execute q on $\langle y, n\rangle$.

(f) Hence verify that $\|\exp_n(y)\|^2 \leq c^2$.

(g) Verify that $\|x+y\|^2 \leq (2X)^2$.

(h) Hence execute q on $\langle x+y, n\rangle$.

(i) Hence verify that $\|\exp_n(x+y)\|^2 \leq c^2$.

(j) Hence using procedure III:16, verify that $\|\exp_n(x)\exp_n(y) - \exp_n(x+y)\|^2$

i. $= \|(1+\frac{x}{n})^n(1+\frac{y}{n})^n - (1+\frac{x+y}{n})^n\|^2$

ii. $= \|(1+\frac{x+y}{n}+\frac{xy}{n^2})^n - (1+\frac{x+y}{n})^n\|^2$

iii. $= \|\frac{xy}{n^2}\sum_r^{[0:n]}(1+\frac{x+y}{n}+\frac{xy}{n^2})^r(1+\frac{x+y}{n})^{n-1-r}\|^2$

iv. $= \frac{\|xy\|^2}{n^4}\|\sum_r^{[0:n]}(1+\frac{x}{n})^r(1+\frac{y}{n})^r(1+\frac{x+y}{n})^{n-1-r}\|^2$

v. $= \frac{\|xy\|^2}{n^3}\sum_r^{[0:n]}\|1+\frac{x}{n}\|^{2r}\|1+\frac{y}{n}\|^{2r}\|1+\frac{x+y}{n}\|^{2(n-1-r)}$

vi. $\leq \frac{\|xy\|^2}{n^3}\sum_r^{[0:n]}\max(1, \|\exp_n(x)\|^2)\max(1, \|\exp_n(y)\|^2)\max(1, \|\exp_n(x+y)\|^2)$

vii. $\leq \frac{\|xy\|^2}{n^3}\sum_r^{[0:n]}\max(1, c^2)^3$

viii. $= \frac{\|xy\|^2\max(1,c)^6}{n^2}$

ix. $= \frac{a^2\|xy\|^2}{n^2}$.

4. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:32

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct rational numbers a, b such that $a > 0$ and a procedure $p(x, y, n)$ to show that $\exp_n(x-y) \equiv \frac{\exp_n(x)}{\exp_n(y)}$ (err $\frac{a}{n}$) when two complex numbers x, y and a positive integer n such that $\|x\|^2 \leq X$, $\|y\|^2 \leq X$, and $n > b$ are chosen.

Implementation

1. Execute procedure III:31 on $\langle X\rangle$ and let $\langle c, d, q\rangle$ receive.
2. Execute procedure III:30 on $\langle X\rangle$ and let $\langle e, f, r\rangle$ receive.
3. Execute procedure III:29 on $\langle X\rangle$ and let $\langle g, h, t\rangle$ receive.
4. Let $b = \max(d, f, h)$.
5. Let $a = c(1+\frac{g}{e})X^2$.
6. Let $p(x, y, n)$ be the following procedure:

(a) Execute procedure r on $\langle y, n\rangle$.

(b) Hence verify that $\|\exp_n(y)\|^2 \geq e^2$.

(c) Execute procedure q on $\langle y, -y, n\rangle$.

(d) Hence verify that $\|\exp_n(y)\exp_n(-y)-1\|^2 = \|\exp_n(y)\exp_n(-y)-\exp_n(y-y)\|^2 \le \frac{c^2\|y\|^2}{n^2}$.

(e) Hence verify that $\|\exp_n(-y) - \frac{1}{\exp_n(y)}\|^2 = \frac{\|\exp_n(y)\exp_n(-y)-1\|^2}{\|\exp_n(y)\|^2} \le \frac{c^2\|y\|^4}{e^2n^2}$.

(f) Execute procedure t on $\langle x, n\rangle$.

(g) Hence verify that $\|\exp_n(x)\|^2 \le g^2$.

(h) Execute procedure q on $\langle x, -y, n\rangle$.

(i) Hence verify that $\|\exp_n(x)\exp_n(-y) - \exp_n(x-y)\|^2 \le \frac{c^2\|x\|^2\|y\|^2}{n^2}$.

(j) Hence verify that $\|\exp_n(x-y) - \frac{\exp_n(x)}{\exp_n(y)}\|^2$

i. $= \|\exp_n(x-y) - \exp_n(x)\exp_n(-y) + \exp_n(x)(\exp_n(-y) - \frac{1}{\exp_n(y)})\|^2$

ii. $\le (\frac{cX^2}{n} + \frac{gcX^2}{en})^2$

iii. $= (\frac{a}{n})^2$.

7. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:33

Objective

Choose a rational number $X \ge 0$. The objective of the following instructions is to construct positive rational numbers a, b and a procedure, $p(x, k, n)$, to show that $\exp_n(kx) \equiv \exp_n(x)^k$ (err $\frac{ak}{n}$) when a complex number x, and non-negative integers k, n such that $n > b$ and $\|kx\|^2 \le X^2$ are chosen.

Implementation

1. Execute procedure III:29 on $\langle X\rangle$ and let $\langle c, d, q\rangle$ receive.
2. Execute procedure III:31 on $\langle X\rangle$ and let $\langle e, f, t\rangle$ receive.
3. Let $a = ecX^2$
4. Let $b = \max(d, f)$.
5. Let $p(x, k, n)$ be the following procedure:

(a) If $k > 0$, then for $r \in [1 : k]$ do the following:

i. Verify that $\|xr\|^2 \le \|kx\|^2 \le X^2$.

ii. Execute procedure q on $\langle xr, nr\rangle$.

iii. Hence verify that $\|\exp_{nr}(xr)\|^2 \le c^2$.

iv. Hence verify that $\|\exp_n(x)^r\|^2 = \|(1 + \frac{x}{n})^{nr}\|^2 = \|(1 + \frac{xr}{nr})^{nr}\|^2 = \|\exp_{nr}(xr)\|^2 \le c^2$

(b) For r in $[0 : k]$, do the following:

i. Verify that $\|x\|^2 \le X^2$.

ii. Verify that $\|(k-r-1)x\|^2 \le \|kx\|^2 \le X^2$.

iii. Now execute procedure t on $\langle x, (k-r-1)x, n\rangle$.

iv. Hence verify that $\|\exp_n(x)\exp_n((k-r-1)x) - \exp_n((k-r)x)\|^2 \le \frac{e^2\|x\|^2\|(k-r-1)x\|^2}{n^2} \le \frac{e^2X^4}{n^2}$.

(c) Hence using (ciii), verify that $\|\exp_n(kx) - \exp_n(x)^k\|^2$

i. $= \|\sum_r^{[0:k]}(\exp_n(x)^r\exp_n((k-r)x) - \exp_n(x)^{r+1}\exp_n((k-r-1)x))\|^2$

ii. $= \|\sum_r^{[0:k]}\exp_n(x)^r(\exp_n((k-r)x) - \exp_n(x)\exp_n((k-r-1)x))\|^2$

iii. $\le (\sum_r^{[0:k]} c\frac{eX^2}{n})^2$

iv. $= (\frac{ak}{n})^2$.

6. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:34

Objective

Choose a rational number $X \ge 0$. The objective of the following instructions is to construct positive rational numbers a, b, and a procedure $p(x, y, n)$ to show that $\|\exp_n(y) - \exp_n(x)\|^2 \le \|x-y\|^2a^2$ when two complex numbers x, y and a positive integer $n > b$ such that $\|x\|^2 \le X$ and $\|y\|^2 \le X$ are chosen.

Implementation

1. Execute procedure III:29 on $\langle X\rangle$ and let $\langle c, b, q\rangle$ receive.
2. Let $a = \max(1, c)^2$.
3. Let $p(x, y, n)$ be the following procedure:

(a) Verify that $\|x\|^2 \le X$.

(b) Execute procedure q on $\langle x, n\rangle$.

(c) Hence verify that $\|\exp_n(x)\|^2 \leq c^2$.

(d) Verify that $\|y\|^2 \leq X$.

(e) Execute procedure q on $\langle y, n\rangle$.

(f) Hence verify that $\|\exp_n(y)\|^2 \leq c^2$.

(g) For each $r \in [0 : n]$, do the following:

i. Verify that $\|(1 + \frac{x}{n})^r\|^2$

A. $= (\|1 + \frac{x}{n}\|^2)^r$

B. $\leq \max((\|1 + \frac{x}{n}\|^2)^n, 1)$

C. $= \max(\|\exp_n(x)\|^2, 1)$

D. $\leq \max(c^2, 1)$

E. $= \max(c, 1)^2$.

ii. Using analogous steps, also verify that $\|(1 + \frac{y}{n})^r\|^2 \leq \max(c, 1)^2$.

(h) Hence verify that $\|\exp_n(y) - \exp_n(x)\|^2$

i. $= \|(1 + \frac{y}{n})^n - (1 + \frac{x}{n})^n\|^2$

ii. $= \|(\frac{y}{n} - \frac{x}{n}) \sum_r^{[0:n]} (1 + \frac{y}{n})^r (1 + \frac{x}{n})^{n-1-r}\|^2$

iii. $\leq \|y - x\|^2 (\frac{1}{n} \sum_r^{[0:n]} \max(c, 1)^2)^2$

iv. $= \|y - x\|^2 a^2$.

4. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:35

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, N, and a procedure, $p(x, n)$, to show that $\exp_n(x) \equiv \sum_r^{[0:n+1]} \frac{x^r}{r!}$ (err $\frac{a}{n}$) when a complex number x and an integer $n > N$ such that $\|x\|^2 \leq X^2$ are chosen.

Implementation

1. Let $N = \lfloor X \rfloor + 1$.

2. Let $a = X^2(\sum_r^{[0:N]} \frac{X^r}{r!} + \frac{X^N}{N!} \cdot \frac{1}{1-\frac{X}{N}})$.

3. Let $p(x, n)$ be the following procedure:

(a) Using procedure II:31, procedure III:16, procedure II:30, and procedure II:32, verify that $\|\sum_r^{[0:n+1]} \frac{x^r}{r!} - \exp_n(x)\|^2$

i. $= \|\sum_r^{[0:n+1]} \frac{x^r}{r!} - \sum_r^{[0:n+1]} \frac{n^{\underline{r}}}{r!} \cdot \frac{x^r}{n^r}\|^2$

ii. $= \|\sum_r^{[1:n+1]} (1 - \frac{n^{\underline{r}}}{n^r}) \frac{x^r}{r!}\|^2$

iii. $\leq (\sum_r^{[1:n+1]} (1 - \frac{n^{\underline{r}}}{n^r}) \frac{X^r}{r!})^2$

iv. $\leq (\sum_r^{[2:n+1]} (1 - \frac{(n-r+1)^r}{n^r}) \frac{X^r}{r!})^2$

v. $= (\sum_r^{[2:n+1]} (1 - (1 - \frac{r-1}{n})^r) \frac{X^r}{r!})^2$

vi. $\leq (\sum_r^{[2:n+1]} (1 - (1 - \frac{(r-1)r}{n})) \frac{X^r}{r!})^2$

vii. $= (\sum_r^{[2:n+1]} \frac{(r-1)r}{n} \frac{X^r}{r!})^2$

viii. $= (\frac{1}{n} \sum_r^{[2:n+1]} \frac{X^r}{(r-2)!})^2$

ix. $= (\frac{X^2}{n} \sum_r^{[0:n-1]} \frac{X^r}{r!})^2$

x. $= (\frac{X^2}{n}(\sum_r^{[0:N]} \frac{X^r}{r!} + \sum_r^{[N:n-1]} \frac{X^r}{r!}))^2$

xi. $\leq (\frac{X^2}{n}(\sum_r^{[0:N]} \frac{X^r}{r!} + \sum_r^{[N:n-1]} \frac{X^r}{N! N^{r-N}}))^2$

xii. $= (\frac{X^2}{n}(\sum_r^{[0:N]} \frac{X^r}{r!} + \frac{X^N}{N!} \sum_r^{[N:n-1]} \frac{X^{r-N}}{N^{r-N}}))^2$

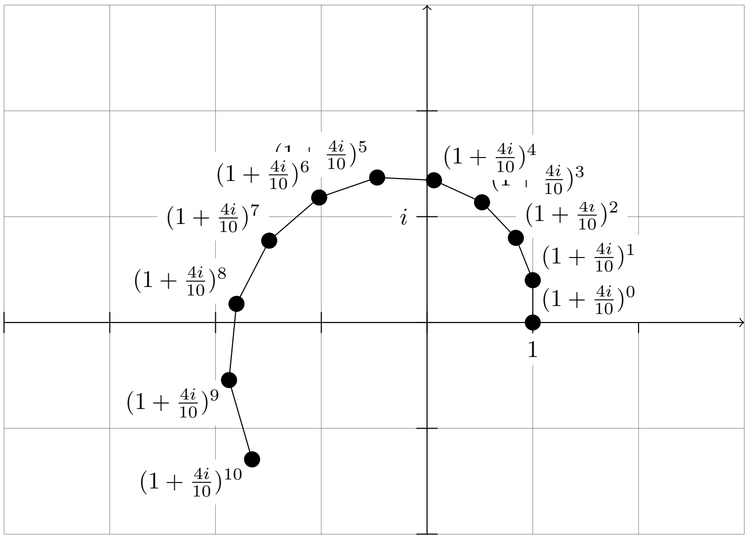
xiii. $= (\frac{X^2}{n}(\sum_r^{[0:N]} \frac{X^r}{r!} + \frac{X^N}{N!} \sum_r^{[0:n-N-1]} \frac{X^r}{N^r}))^2$

xiv. $= (\frac{X^2}{n}(\sum_r^{[0:N]} \frac{X^r}{r!} + \frac{X^N}{N!} \cdot \frac{1}{1-\frac{X}{N}}))^2$

xv. $= (\frac{a}{n})^2$.

4. **Yield the tuple $\langle a, N, p\rangle$.**

Figure III:0



A plot of the list of complex numbers $(1+\frac{4i}{10})^{[0:11]}$. Notice that each multiplication of a complex number by $1+\frac{4i}{10}$ results in an anti-clockwise rotation about the origin and a small radial movement outwards. This can be seen to reflect the computation $(1+\frac{4i}{10})a = 1a + \frac{4}{10}(ai)$ after one notes that ai is perpendicular to a. Also note that each line segment has a length of roughly $\frac{4}{10}$ units. Hence the entire path has a length of approximately $10 * \frac{4}{10} = 4$ units.

Declaration III:13

The notation $\cos_n(z)$, where z is a complex number and n is a positive integer, will be used as a shorthand for $\frac{\exp_n(iz)+\exp_n(-iz)}{2}$.

Procedure III:36

Objective

Choose a rational number x and a positive integer n. The objective of the following instructions is to show that $\mathrm{re}(\exp_n(ix)) = \cos_n(x)$.

Implementation

1. Verify that $\mathrm{re}(\exp_n(ix))$
   (a) $= \frac{\exp_n(ix)+\overline{\exp_n(ix)}}{2}$
   (b) $= \frac{\exp_n(ix)+\exp_n(\overline{ix})}{2}$
   (c) $= \frac{\exp_n(ix)+\exp_n(-ix)}{2}$
   (d) $= \cos_n(x)$.

Declaration III:14

The notation $\sin_n(z)$, where z is a complex number and n is a positive integer, will be used as a shorthand for $\frac{\exp_n(iz)-\exp_n(-iz)}{2i}$.

Procedure III:37

Objective

Choose a rational number x and a positive integer n. The objective of the following instructions is to show that $\mathrm{im}(\exp_n(ix)) = \sin_n(x)$.

Implementation

1. Verify that $\mathrm{im}(\exp_n(ix))$
   (a) $= \frac{\exp_n(ix)-\overline{\exp_n(ix)}}{2i}$
   (b) $= \frac{\exp_n(ix)-\exp_n(\overline{ix})}{2i}$
   (c) $= \frac{\exp_n(ix)-\exp_n(-ix)}{2i}$
   (d) $= \sin_n(x)$.

Procedure III:38

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, b, and a procedure, $p(x, y, n)$, to show that $\cos_n(x+y) \equiv \cos_n(x)\cos_n(y) -$

$\sin_n(x)\sin_n(y)$ (err $\frac{axy}{n}$) (err $\frac{aX^2}{n}$) when two complex numbers x, y and a positive integer $n > b$ such that $\|x\|^2 \leq X^2$ and $\|y\|^2 \leq X^2$ are chosen.

Implementation

1. Execute procedure III:31 on $\langle X\rangle$ and let $\langle a, b, q\rangle$ receive.
2. Let $p(x, y, n)$ be the following procedure:
   (a) Verify that $\|ix\|^2 \leq X^2$.
   (b) Verify that $\|iy\|^2 \leq X^2$.
   (c) Execute procedure q on $\langle ix, iy, n\rangle$.
   (d) Hence verify that $\|\exp_n(ix)\exp_n(iy) - \exp_n(ix+iy)\|^2 \leq \frac{a^2\|i^2xy\|^2}{n^2} = \frac{a^2\|xy\|^2}{n^2}$.
   (e) Verify that $\|-ix\|^2 \leq X$.
   (f) Verify that $\|-iy\|^2 \leq X$.
   (g) Execute procedure q on $\langle -ix, -iy, n\rangle$.
   (h) Hence verify that $\|\exp_n(-ix)\exp_n(-iy) - \exp_n(-ix-iy)\|^2 \leq \frac{a^2\|(-i)^2xy\|^2}{n^2} = \frac{a^2\|xy\|^2}{n^2}$.
   (i) Using procedure III:16, verify that $\|\cos_n(x)\cos_n(y) - \sin_n(x)\sin_n(y) - \cos_n(x+y)\|^2$
      i. $= \|\frac{(\exp_n(ix)+\exp_n(-ix))(\exp_n(iy)+\exp_n(-iy))}{4} - \frac{\exp_n(ix)-\exp_n(-ix))(\exp_n(iy)-\exp_n(-iy))}{4i^2} - \cos_n(x+y)\|^2$
      ii. $= \|\frac{\exp_n(ix)\exp_n(iy)}{2} + \frac{\exp_n(-ix)\exp_n(-iy)}{2} - \frac{\exp_n(i(x+y))+\exp_n(-i(x+y))}{2}\|^2$
      iii. $\leq \frac{\|\exp_n(ix)\exp_n(iy)-\exp_n(i(x+y))\|^2}{2} + \frac{\|\exp_n(-ix)\exp_n(-iy)-\exp_n(-i(x+y))\|^2}{2}$
      iv. $\leq \frac{a^2\|xy\|^2}{n^2}$.
3. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:39

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, b, and a procedure, $p(x, y, n)$, to show that $\sin_n(x+y) \equiv \sin_n(x)\cos_n(y) - \cos_n(x)\sin_n(y)$ (err $\frac{axy}{n}$) (err $\frac{aX^2}{n}$) when two complex numbers x, y and a positive integer $n > b$ such that $\|x\|^2 \leq X^2$ and $\|y\|^2 \leq X^2$ are chosen.

Implementation

Implementation is analogous to that of procedure III:38.

Procedure III:40

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, b, and a procedure, $p(x, n)$, to show that $\cos_n(x)^2 + \sin_n(x)^2 \equiv 1$ (err $\frac{a\|x\|^2}{n}$) (err $\frac{aX^2}{n}$) when a complex number x and a positive integer n such that $\|x\|^2 \leq X^2$ and $n > b$ are chosen.

Implementation

1. Execute procedure III:31 on $\langle X\rangle$ and let $\langle a, b, q\rangle$ receive.
2. Let $p(x, n)$ be the following procedure:
   (a) Verify that $\|ix\|^2 \leq X^2$.
   (b) Verify that $\|-ix\|^2 \leq X^2$.
   (c) Execute procedure q on $\langle ix, -ix, n\rangle$.
   (d) Hence verify that $\|\exp_n(ix)\exp_n(-ix) - \exp_n(ix-ix)\|^2 \leq \frac{a^2\|-i^2x^2\|^2}{n^2} = \frac{a^2\|x\|^4}{n^2}$.
   (e) Hence verify that $\|\cos_n(x)^2 + \sin_n(x)^2 - 1\|^2$
      i. $= \|\frac{(\exp_n(ix)+\exp_n(-ix))^2}{4} + \frac{(\exp_n(ix)-\exp_n(-ix))^2}{4i^2} - 1\|^2$
      ii. $= \|\exp_n(ix)\exp_n(-ix) - 1\|^2$
      iii. $= \|\exp_n(ix)\exp_n(-ix) - \exp_n(ix-ix)\|^2$
      iv. $\leq \frac{a^2\|x\|^4}{n^2}$.
3. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:41

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, b, and a procedure, $p(x, y, n)$, to show that $\|x \exp_n(iy)\|^2 \equiv \|x\|^2$ (err $\frac{a\|x\|^2\|y\|^2}{n}$) (err $\frac{a\|x\|^2X^2}{n}$) when a complex number x, a rational number y, and a positive integer n such that $\|y\|^2 \leq X^2$ and $n > b$ are chosen.

Implementation

1. Execute procedure III:40 on $\langle X\rangle$ and let $\langle a, b, q\rangle$ receive.
2. Let $p(x, y, n)$ be the following procedure:
   (a) Execute procedure q on $\langle y, n\rangle$.
   (b) Hence verify that $\|\cos_n(y)^2 + \sin_n(y)^2 - 1\|^2 \leq \frac{a^2\|y\|^4}{n^2}$.
   (c) Hence using procedure III:36 and procedure III:37, verify that $\|\|x \exp_n(iy)\|^2 - \|x\|^2\|^2$
      i. $= \|\|x\|^2\|\exp_n(iy)\|^2 - \|x\|^2\|^2$
      ii. $= \|x\|^4\|\text{re}(\exp_n(iy))^2 + \text{im}(\exp_n(iy))^2 - 1\|^2$
      iii. $= \|x\|^4\|\cos_n(y)^2 + \sin_n(y)^2 - 1\|^2$
      iv. $\leq \frac{a^2\|y\|^4\|x\|^4}{n^2}$.

Procedure III:42

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, N, and a procedure, $p(x, n)$, to show that $\cos_n(x) \equiv \sum_r^{[0:\lceil\frac{n}{2}\rceil]} \frac{(-1)^r x^{2r}}{(2r)!}$ (err $\frac{a}{n}$) when a complex number x and an integer $n > N$ such that $\|x\|^2 \leq X^2$ is chosen.

Implementation

1. Execute procedure III:35 on $\langle X\rangle$ and let $\langle a, N, q\rangle$ receive.
2. Let $p(x, n)$ be the following procedure:
   (a) Verify that $\|ix\|^2 = \|x\|^2 \leq X$.
   (b) Execute procedure q on $\langle ix, n\rangle$.
   (c) Hence verify that $\|\sum_r^{[0:n+1]} \frac{(ix)^r}{r!} - \exp_n(ix)\|^2 \leq (\frac{a}{n})^2$.
   (d) Verify that $\|-ix\|^2 = \|x\|^2 \leq X$.
   (e) Execute procedure q on $\langle -ix, n\rangle$.
   (f) Hence verify that $\|\sum_r^{[0:n+1]} \frac{(-ix)^r}{r!} - \exp_n(-ix)\|^2 \leq (\frac{a}{n})^2$.
   (g) Hence using procedure III:16, verify that $\|\sum_r^{[0:\lceil\frac{n}{}\rceil 2]} \frac{(-1)^r x^{2r}}{(2r)!} - \cos_n(x)\|^2$
      i. $= \|\sum_r^{[0:n+1]} \frac{[r \bmod 2=0](-1)^{\frac{r}{2}} x^r}{r!} - \cos_n(x)\|^2$
      ii. $= \|\sum_r^{[0:n+1]} \frac{(i^r+(-i)^r)x^r}{2(r!)} - \frac{\exp_n(ix)+\exp_n(-ix)}{2}\|^2$
      iii. $= \frac{1}{4}\|\sum_r^{[0:n+1]} \frac{(ix)^r}{r!} - \exp_n(ix) + \sum_r^{[0:n+1]} \frac{(-ix)^r}{r!} - \exp_n(-ix)\|^2$
      iv. $\leq \frac{1}{2}(\|\sum_r^{[0:n+1]} \frac{(ix)^r}{r!} - \exp_n(ix)\|^2 + \|\sum_r^{[0:n+1]} \frac{(-ix)^r}{r!} - \exp_n(-ix)\|^2)$
      v. $\leq \frac{1}{2}((\frac{a}{n})^2 + (\frac{a}{n})^2)$
      vi. $\leq (\frac{a}{n})^2$.

Procedure III:43

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct two rational numbers a, N, and a procedure, $p(x, n)$, to show that $\sin_n(x) \equiv \sum_r^{[0:\lfloor\frac{n+1}{2}\rfloor]} \frac{(-1)^r x^{2r+1}}{(2r+1)!}$ (err $\frac{a}{n}$) when a complex number x and an integer $n > N$ such that $\|x\|^2 \leq X^2$ is chosen.

Implementation

Implementation is analogous to that of procedure III:42.

Declaration III:15

The notation $(1+x)_n^a$, where x, a are complex numbers and n is a positive integer, will be used as a shorthand for $\sum_r^{[0:n]} \binom{a}{r} x^r$.

Procedure III:44

Objective

Choose a complex number x and two non-negative integers a, n such that $n > a$. The objective of the following instructions is to show that $(1+x)^a_n = (1+x)^a$.

Implementation

1. Using procedure III:12, verify that $(1+x)^a_n =$
   (a) $= \sum_r^{[0:n]} \binom{a}{r} x^r$
   (b) $= \sum_r^{[0:n]} \frac{a^{\underline{r}}}{r!} x^r$
   (c) $= \sum_r^{[0:a+1]} \frac{a^{\underline{r}}}{r!} x^r + \sum_r^{[a+1:n]} \frac{a^{\underline{r}}}{r!} x^r$
   (d) $= \sum_r^{[0:a+1]} \frac{a^{\underline{r}}}{r!} x^r + \sum_r^{[a+1:n]} \frac{0}{r!} x^r$
   (e) $= \sum_r^{[0:a+1]} \binom{a}{r} x^r$
   (f) $= (1+x)^a$.

Procedure III:45

Objective

Choose two complex numbers x, y and a positive integer N. The objective of the following instructions is to show that $\binom{x+y}{N} = \sum_k^{N+1} \binom{x}{k}\binom{y}{N-k}$.

Implementation

1. If $N = 0$, then do the following:
   (a) Verify that $\binom{x+y}{N} = 1 = \sum_k^{[0:N+1]} \binom{x}{k}\binom{y}{N-k}$.
2. Otherwise do the following:
   (a) Verify that $N > 0$.
   (b) Execute procedure III:45 on $\langle x-1, y, N-1\rangle$.
   (c) Hence verify that $\binom{x+y-1}{N-1} = \sum_k^{[0:N]} \binom{x-1}{k}\binom{y}{N-1-k}$.
   (d) Execute procedure III:45 on $\langle x, y-1, N-1\rangle$.
   (e) Hence verify that $\binom{x+y-1}{N-1} = \sum_k^{[0:N]} \binom{x}{k}\binom{y-1}{N-1-k}$.
   (f) Hence verify that $\binom{x+y}{N}$
      i. $= \frac{x+y}{N}\binom{x+y-1}{N-1}$
      ii. $= \frac{x}{N}\binom{x+y-1}{N-1} + \frac{y}{N}\binom{x+y-1}{N-1}$
      iii. $= \frac{x}{N}\sum_k^{[0:N]} \binom{x-1}{k}\binom{y}{N-1-k} + \frac{y}{N}\sum_k^{[0:N]} \binom{x}{k}\binom{y-1}{N-1-k}$
      iv. $= \frac{x}{N}\sum_k^{[1:N+1]} \binom{x-1}{k-1}\binom{y}{N-k} + \frac{y}{N}\sum_k^{[0:N]} \binom{x}{k}\binom{y-1}{N-1-k}$
      v. $= \sum_k^{[0:N+1]} \frac{k}{N}\binom{x}{k}\binom{y}{N-k} + \sum_k^{[0:N+1]} \frac{N-k}{N}\binom{x}{k}\binom{y}{N-k}$
      vi. $= \sum_k^{[0:N+1]} \binom{x}{k}\binom{y}{N-k}$.

Procedure III:46

Objective

Choose complex numbers a, b, x and a natural number n. The objective of the following instructions is to show that $(1+x)^a_n(1+x)^b_n - (1+x)^{a+b}_n = \sum_k^{[1:n]}\sum_r^{[k:n]} \binom{a}{k+n-1-r}\binom{b}{r} x^{k+n-1}$.

Implementation

1. Verify that $(1+x)^a_n(1+x)^b_n - (1+x)^{a+b}_n$
   (a) $= (\sum_k^{[0:n]} \binom{a}{k} x^k)(\sum_r^{[0:n]} \binom{b}{r} x^r) - \sum_k^{[0:n]} \binom{a+b}{k} x^k$
   (b) $= \sum_k^{[0:n]}\sum_r^{[0:n]} \binom{a}{k}\binom{b}{r} x^{k+r} - \sum_k^{[0:n]} \binom{a+b}{k} x^k$
   (c) $= \sum_k^{[0:n]}\sum_r^{[0:k+1]} \binom{a}{k-r}\binom{b}{r} x^k + \sum_k^{[n:2n-1]}\sum_r^{[k-n+1:n]} \binom{a}{k-r}\binom{b}{r}$ $\sum_k^{[0:n]} \binom{a+b}{k} x^k$
   (d) $= \sum_k^{[0:n]} \binom{a+b}{k} x^k + \sum_k^{[1:n]}\sum_r^{[k:n]} \binom{a}{k+n-1-r}\binom{b}{r} x^{k+n-1} - \sum_k^{[0:n]} \binom{a+b}{k} x^k$
   (e) $= \sum_k^{[1:n]}\sum_r^{[k:n]} \binom{a}{k+n-1-r}\binom{b}{r} x^{k+n-1}$.

Procedure III:47

Objective

Choose two rational numbers $A > 0$ and $0 < X < 1$. The objective of the following instructions is to construct rational numbers $Y > 0$, $0 < Z < 1$ and a procedure $p(a, x, n)$ to show that $\|\binom{a}{n}x^n\|^2 \leq (YZ^n)^2$ when complex numbers a, x such that $\|a+1\|^2 < A^2$ and $\|x\|^2 < X^2$ are chosen.

Implementation

1. Let $e = \frac{AX}{1-X} - 1$.
2. Let $d = \lfloor \frac{AX}{1-X} \rfloor$.
3. Verify that $d > e > -1$.
4. Let $Z = (1 + \frac{A}{d+1})X$.
5. Verify that $0 < Z < (1 + \frac{A}{e+1})X = 1$.
6. Let $Y = Z^{-d} \prod_k^{[0:d]} \frac{(A+k+1)X}{k+1} = Z^{-d} \prod_k^{[0:d]} X(1 + \frac{A}{k+1})$.
7. Let $p(a, x, n)$ be the following procedure:
   (a) Verify that $\mathrm{re}(a+1)^2 \le \|a+1\|^2 \le A^2$.
   (b) Hence verify that $|\mathrm{re}(a+1)| \le A$.
   (c) Hence verify that $\|\binom{a}{n} x^n\|^2$
      i. $= \|\frac{a^{\underline{n}}}{n!} x^n\|^2$
      ii. $= \|\prod_k^{[0:n]} (\frac{a+1-(k+1)}{k+1} \cdot x)\|^2$
      iii. $= \prod_k^{[0:n]} \frac{\|(a+1)-(k+1)\|^2 \|x\|^2}{(k+1)^2}$
      iv. $= \prod_k^{[0:n]} \frac{(\|a+1\|^2 - 2\,\mathrm{re}(a+1)(k+1) + (k+1)^2)\|x\|^2}{(k+1)^2}$
      v. $\le \prod_k^{[0:n]} \frac{(A^2 + 2A(k+1) + (k+1)^2)X^2}{(k+1)^2}$
      vi. $= (\prod_k^{[0:n]} \frac{(A+k+1)X}{k+1})^2$
      vii. $= (\prod_k^{[0:n]} X(1 + \frac{A}{k+1}))^2$.
   (d) If $n \le d$, then do the following:
      i. Verify that $\|\binom{a}{n} x^n\|^2$
         A. $\le (\prod_k^{[0:n]} X(1 + \frac{A}{k+1}))^2$
         B. $= (\prod_k^{[0:d]} X(1 + \frac{A}{k+1}))^2 (\prod_k^{[n:d]} X(1 + \frac{A}{k+1}))^{-2}$
         C. $\le (\prod_k^{[0:d]} X(1 + \frac{A}{k+1}))^2 (X(1 + \frac{A}{d+1}))^{-2(d-n)}$
         D. $= Y^2 Z^{2n}$.
   (e) Otherwise do the following:
      i. Verify that $\|\binom{a}{n} x^n\|^2$
         A. $\le (\prod_k^{[0:n]} X(1 + \frac{A}{k+1}))^2$
         B. $= (\prod_k^{[0:d]} X(1 + \frac{A}{k+1}))^2 (\prod_k^{[d:n]} X(1 + \frac{A}{k+1}))^2$
         C. $\le (\prod_k^{[0:d]} X(1 + \frac{A}{k+1}))^2 (X(1 + \frac{A}{d+1}))^{2(n-d)}$
         D. $= Y^2 Z^{2n}$.
8. **Yield the tuple $\langle Y, Z, p \rangle$.**

Procedure III:48

Objective

Choose a rational number $0 < X < 1$ and a positive integer k. The objective of the following instructions is to construct rational numbers $Y > 0$, $0 < Z < 1$ and a procedure $p(x, n)$ to show that $\|n^k x^n\|^2 \le (YZ^n)^2$ when a complex number x such that $\|x\|^2 \le X^2$ is chosen.

Implementation

1. Let $e = \frac{k}{1-X} - 1$.
2. Let $d = \lfloor \frac{k}{1-X} \rfloor$.
3. Verify that $d > e > k - 1$.
4. Let $Z = (1 + \frac{1}{d})^k X$.
5. Verify that $Z < (1 + \frac{1}{e})^k X$.
6. Now using procedure II:33, verify that $0 < Z < (1 + \frac{1}{e})^k X \le \frac{1 + \frac{1}{e}}{1 - (k-1)\frac{1}{e}} \cdot X = 1$.
7. Let $Y = Z^{-d} X \prod_r^{[1:d]} X(1 + \frac{1}{r})^k$.
8. Let $p(x, n)$ be the following procedure:
   (a) Verify that $\|n^k x^n\|^2$
      i. $\le \|x \prod_r^{[1:n]} x \cdot \frac{(r+1)^k}{r^k}\|^2$
      ii. $= \|x\|^2 \prod_r^{[1:n]} \|x\|^2 (\frac{(r+1)^k}{r^k})^2$
      iii. $\le X^2 \prod_r^{[1:n]} ((1 + \frac{1}{r})^k X)^2$.
   (b) If $n \le d$, then do the following:
      i. Verify that $\|n^k x^n\|^2$
         A. $\le X^2 (\prod_r^{[1:n]} X(1 + \frac{1}{r})^k)^2$
         B. $= X^2 (\prod_r^{[1:d]} X(1 + \frac{1}{r})^k)^2 \cdot (\prod_r^{[n:d]} X(1 + \frac{1}{r})^k)^{-2}$
         C. $\le X^2 (\prod_r^{[1:d]} X(1 + \frac{1}{r})^k)^2 (X(1 + \frac{1}{d})^k)^{-2(d-n)}$

D. $= Y^2 Z^{2n}$.

(c) Otherwise do the following:

i. Verify that $\|n^k x^n\|^2$

A. $\leq X^2 (\prod_r^{[1:n]} X(1+\frac{1}{r})^k)^2$

B. $= X^2 (\prod_r^{[1:d]} X(1+\frac{1}{r})^k)^2 (\prod_r^{[d:n]} X(1+\frac{1}{r})^k)^2$

C. $\leq X^2 (\prod_r^{[1:d]} X(1+\frac{1}{r})^k)^2 (X(1+\frac{1}{d})^k)^{2(n-d)}$

D. $= Y^2 Z^{2n}$.

9. **Yield the tuple $\langle Y, Z, p \rangle$.**

Procedure III:49

Objective

Choose two rational numbers $A > 0$, $1 > X > 0$. The objective of the following instructions is to construct rational numbers $D > 0$, $0 < G < 1$, and a procedure $p(x, a, b, n)$ to show that $(1+x)_n^{a+b} \equiv (1+x)_n^a (1+x)_n^b$ (err DG^n) when $\|x\|^2 \leq X$, and $\|a\|^2, \|b\|^2 < A$.

Implementation

1. Execute procedure III:47 on $\langle A, X \rangle$ and let $\langle B, C, q \rangle$ receive.
2. Execute procedure III:48 on $\langle C, 1 \rangle$ and let $\langle F, G, t \rangle$ receive.
3. Let $D = \frac{B^2 F}{1-C}$.
4. Let $p(x, a, b, n)$ be the following procedure:

(a) For each $r \in [1:n]$, do the following:

i. Execute procedure q on $\langle a, x, r \rangle$.

ii. Hence verify that $\|\binom{a}{r} x^r\|^2 \leq (BC^r)^2$.

iii. Execute procedure q on $\langle b, x, r \rangle$.

iv. Hence verify that $\|\binom{b}{r} x^r\|^2 \leq (BC^r)^2$.

(b) Execute procedure t on $\langle C, n \rangle$.

(c) Hence verify that $\|nC^n\|^2 \leq (FG^n)^2$.

(d) Hence verify that $\|(1+x)_n^a (1+x)_n^b - (1+x)_n^{a+b}\|^2$

i. $= \|\sum_k^{[1:n]} \sum_r^{[k:n]} \binom{a}{k+n-1-r} \binom{b}{r} x^{k+n-1}\|^2$

ii. $= \|\sum_k^{[1:n]} \sum_r^{[k:n]} \binom{a}{k+n-1-r} x^{k+n-1-r} \binom{b}{r} x^r\|^2$

iii. $\leq (\sum_k^{[1:n]} \sum_r^{[k:n]} BC^{k+n-1-r} BC^r)^2$

iv. $= (B^2 C^n \sum_k^{[1:n]} \sum_r^{[k:n]} C^{k-1})^2$

v. $= (B^2 C^n \sum_r^{[1:n]} \sum_k^{[1:r+1]} C^{k-1})^2$

vi. $\leq (B^2 C^n \sum_r^{[1:n]} \frac{1}{1-C})^2$

vii. $< (\frac{B^2}{1-C} \cdot nC^n)^2$

viii. $\leq (\frac{B^2 F}{1-C} G^n)^2$

ix. $= (DG^n)^2$.

Procedure III:50

Objective

Choose two rational numbers $A > 0$, $1 > X > 0$. The objective of the following instructions is to construct a rational number D and a procedure $p(x, n, a, k)$ to show that $\|((1+x)_n^a)^k\|^2 < D^2$ when complex numbers x, a and positive integers n, k such that $\|x\|^2 < X^2$ and $\|ka\|^2 < A^2$.

Implementation

1. Execute procedure III:29 on $\langle \frac{ABX}{1-C} \rangle$ and let $\langle E, N, t \rangle$ receive.
2. Execute procedure III:47 on $\langle A+1, X \rangle$ and let $\langle B, C, q \rangle$ receive.
3. Let $D = \max(E, (1 + \frac{ABX}{1-C})^{\lfloor N \rfloor})$.
4. Let $p(x, n, a, k)$ be the following procedure:

(a) For each $r \in [1:n]$, do the following:

i. Verify that $\|a\|^2 \leq \|ka\|^2 \leq A^2$.

ii. Verify that $\|a-1\|^2 \leq (A+1)^2$.

iii. Execute procedure q on $\langle a-1, x, r-1 \rangle$.

iv. Hence verify that $\|\binom{a-1}{r-1} x^{r-1}\|^2 \leq (BC^r)^2$.

(b) Hence verify that $\|k \sum_r^{[1:n]} \binom{a}{r} x^r\|^2$

i. $= \|k \sum_r^{[1:n]} \frac{a}{r} \binom{a-1}{r-1} x^r\|^2$

ii. $= \|kax \sum_r^{[1:n]} \frac{1}{r} \binom{a-1}{r-1} x^{r-1}\|^2$

iii. $\leq (AX\sum_r^{[1:n]} BC^{r-1})^2$

iv. $\leq (\frac{ABX}{1-C})^2$.

(c) If $k > N$, then do the following:

i. Execute procedure t on $\langle k\sum_r^{[1:n]} \binom{a}{r}x^r\rangle$.

ii. Hence verify that $\|((1+x)_n^a)^k\|^2$

A. $= \|(\sum_r^{[0:n]} \binom{a}{r}x^r)^k\|^2$

B. $= \|(1+\sum_r^{[1:n]} \binom{a}{r}x^r)^k\|^2$

C. $= \|\exp_k(k\sum_r^{[1:n]} \binom{a}{r}x^r)\|^2$

D. $\leq E^2$

E. $\leq D^2$.

(d) Otherwise do the following:

i. Verify that $\|\sum_r^{[1:n]} \binom{a}{r}x^r)^k\|^2$

A. $\leq \|k\sum_r^{[1:n]} \binom{a}{r}x^r\|^2$

B. $\leq (\frac{ABX}{1-C})^2$.

ii. Hence verify that $\|((1+x)_n^a)^k\|^2$

A. $= (\|(1+x)_n^a\|^2)^k$

B. $= (\|1+\sum_r^{[1:n]} \binom{a}{r}x^r\|^2)^k$

C. $\leq (1+\frac{ABX}{1-C})^{2k}$

D. $\leq D^2$.

5. **Yield $\langle D, p\rangle$.**

Procedure III:51

Objective

Choose two rational numbers $A > 0$, $1 > X > 0$. The objective of the following instructions is to construct rational numbers $G > 0$, $0 < C < 1$, and a procedure $p(x, n, a, k)$ to show that $(1+x)_n^{ka} \equiv ((1+x)_n^a)^k$ (err GkC^n) when a non-negative integer k and complex numbers x, a such that $\|x\|^2 \leq X^2$ and $\|ka\|^2 < A^2$ are chosen.

Implementation

1. Execute procedure III:50 on $\langle A, X\rangle$ and let $\langle D, t\rangle$ receive.

2. Execute procedure III:49 on $\langle A, X\rangle$ and let $\langle B, C, q\rangle$ receive.

3. Let $G = DB$.

4. Let $p(x, n, a, k)$ be the following procedure:

(a) If $k > 0$, then for $r \in [1 : k]$ do the following:

i. Verify that $\|ar\|^2 \leq \|ak\|^2 < A^2$.

ii. Execute procedure t on $\langle x, n, a, r\rangle$.

iii. Hence verify that $\|((1+x)_n^a)^r\|^2 < D^2$.

(b) For r in $[0 : k]$, do the following:

i. Verify that $\|a\|^2 \leq \|ka\|^2 < A^2$.

ii. Verify that $\|(k-r-1)a\|^2 \leq \|ka\|^2 < A^2$.

iii. Execute procedure q on $\langle x, a, (k-r-1)a, n\rangle$.

iv. Hence verify that $\|(1+x)_n^a(1+x)_n^{(k-r-1)a} - (1+x)_n^{(k-r)a}\|^2 \leq (BC^n)^2$.

(c) Hence verify that $\|(1+x)_n^{ka} - ((1+x)_n^a)^k\|^2$

i. $= \|\sum_r^{[0:k]}(((1+x)_n^a)^r(1+x)_n^{(k-r)a} - ((1+x)_n^a)^{r+1}(1+x)_n^{(k-r-1)a})\|^2$

ii. $= \|\sum_r^{[0:k]}((1+x)_n^a)^r((1+x)_n^{(k-r)a} - (1+x)_n^a(1+x)_n^{(k-r-1)a})\|^2$

iii. $\leq (\sum_r^{[0:k]} DBC^n)^2$

iv. $= (kDBC^n)^2$

v. $= (GkC^n)^2$.

5. **Yield the tuple $\langle G, C, D, p\rangle$.**

Procedure III:52

Objective

Choose a rational number $A > 0$. The objective of the following instructions is to construct rational numbers $M > 1$, $N > 0$, and a procedure $p(a, n)$ to show that $\|\binom{a}{n}\|^2 \leq (\frac{M}{n})^{2(\lfloor a\rfloor+1)}$ and $\frac{M}{n} < 1$ when a rational number $-1 < a < A$ and an integer $n > N$ are chosen.

Implementation

1. Let $M = 2A$.
2. Let $N = 2A$.
3. Let $p(a, n)$ be the following procedure:
   (a) Verify that $-1 < a < A$.
   (b) Verify that $n > N = 2A > 2a$.
   (c) Hence verify that $\frac{2a}{n} < \frac{2A}{2A} = 1$.
   (d) Verify that $\frac{n}{2} > a$.
   (e) Therefore verify that $n - \lfloor a \rfloor > n - a > n - \frac{n}{2} = \frac{n}{2}$.
   (f) Hence verify that $\|\binom{a}{n}\|^2$
      i. $= \|\frac{a^n}{n!}\|^2$
      ii. $= \|\prod_k^{[0:n]} \frac{a-k}{k+1}\|^2$
      iii. $= \prod_k^{[0:n]} \frac{(a-k)^2}{(k+1)^2}$
      iv. $= \prod_k^{[0:\lfloor a \rfloor+1]} (k-a)^2 \cdot \prod_k^{[0:n]} \frac{(k+\lfloor a \rfloor+1-a)^2}{(k+1)^2} \cdot \prod_k^{[n-\lfloor a \rfloor-1:n]} \frac{1}{(k+1)^2}$
      v. $\leq (a^{\lfloor a \rfloor+1} \cdot 1^n \cdot (\frac{1}{n-\lfloor a \rfloor})^{\lfloor a \rfloor+1})^2$
      vi. $= (\frac{a}{n-\lfloor a \rfloor})^{2(\lfloor a \rfloor+1)}$
      vii. $\leq (\frac{2a}{n})^{2(\lfloor a \rfloor+1)}$
      viii. $\leq (\frac{M}{n})^{2(\lfloor a \rfloor+1)}$.
4. **Yield the tuple $\langle M, N, p \rangle$.**

Procedure III:53

Objective

Choose a rational number $X > 0$. The objective of the following instructions is to construct rational numbers $B > 0$, $N > 0$, and a procedure $p(x, a, b, n)$ to show that $(1 + x)^{a+b}_n \equiv (1 + x)^a_n (1 + x)^b_n$ (err $\frac{B}{n}$) when a complex number x, two rational numbers a, b, and a positive integer n such that $\|x\|^2 \leq 1$, $\mathrm{re}(x) + 1 \geq X$, $0 < a < 1$, $0 < b < 1$, and $n > N$ are chosen.

Implementation

1. Execute procedure III:52 on $\langle 1 \rangle$ and let $\langle M, N, q \rangle$ receive.
2. Let $B = \frac{6M^2}{X}$.
3. Let $p(x, a, b, n)$ be the following procedure:
   (a) For $r \in [1 : n]$, for $k \in [0 : r]$, verify that $\binom{a}{k+1+n-r}(-1)^{k+1} - \binom{a}{k+n-r}(-1)^k$
      i. $= (-1)^{k+1}(\binom{a}{k+1+n-r} + \binom{a}{k+n-r})$
      ii. $= (-1)^{k+1}\binom{a+1}{k+1+n-r}$
      iii. $= (-1)^{-(k+1)}|\binom{a+1}{k+1+n-r}|(-1)^{k+1+n-r}$
      iv. $= |\binom{a+1}{k+1+n-r}|(-1)^{n-r}$.
   (b) Now use procedure q to verify the following:
      i. $\|\binom{a+b}{n}\|^2 \leq (\frac{M}{n})^{2(\lfloor a+b \rfloor+1)} \leq (\frac{M^2}{n})^2$
      ii. $\|\binom{a}{n}\|^2 \leq (\frac{M}{n})^{2(\lfloor a \rfloor+1)} \leq (\frac{M^1}{n})^2 \leq (\frac{M^2}{n})^2$
      iii. $\|\binom{b}{n}\|^2 \leq (\frac{M}{n})^{2(\lfloor b \rfloor+1)} \leq (\frac{M^1}{n})^2 \leq (\frac{M^2}{n})^2$
   (c) Hence using procedure III:46, verify that $\|(1 + x)^a_n (1 + x)^b_n - (1 + x)^{a+b}_n\|^2$
      i. $= \|\sum_k^{[1:n]} \sum_r^{[k:n]} \binom{a}{k+n-1-r}\binom{b}{r} x^{k+n-1}\|^2$
      ii. $= \|x^n\|^2 \|\sum_r^{[1:n]} \binom{b}{r} \sum_k^{[0:r]} \binom{a}{k+n-r} x^k\|^2$
      iii. $= \|x^n\|^2 \|\sum_r^{[1:n]} \binom{b}{r} \sum_k^{[0:r]} (\binom{a}{k+1+n-r}(-1)^{k+1} \cdot \frac{(-x)^{k+1}}{-x-1} - \binom{a}{k+n-r}(-1)^k \cdot \frac{(-x)^k}{-x-1} - \frac{(-x)^{k+1}}{-x-1}(\binom{a}{k+1+n-r}(-1)^{k+1} - \binom{a}{k+n-r}(-1)^k))\|^2$
      iv. $= \frac{\|x^n\|^2}{\|x+1\|^2} \|\sum_r^{[1:n]} \binom{b}{r}(\binom{a}{n}x^r - \binom{a}{n-r} - \sum_k^{[0:r]} (-x)^{k+1}(\binom{a}{k+1+n-r}(-1)^{k+1} - \binom{a}{k+n-r}(-1)^k))\|^2$
      v. $\leq \frac{1}{\mathrm{re}(x+1)^2 + \mathrm{im}(x)^2}(\sum_r^{[1:n]} |\binom{b}{r}|(|\binom{a}{n}| + |\binom{a}{n-r}| + \sum_k^{[0:r]} |\binom{a}{k+1+n-r}(-1)^{k+1} - \binom{a}{k+n-r}(-1)^k|))^2$
      vi. $\leq \frac{1}{X^2}(\sum_r^{[1:n]} |\binom{b}{r}|(|\binom{a}{n}| + |\binom{a}{n-r}| + |\sum_k^{[0:r]} (\binom{a}{k+1+n-r}(-1)^{k+1} - \binom{a}{k+n-r}(-1)^k)|))^2$
      vii. $= \frac{1}{X^2}(\sum_r^{[1:n]} |\binom{b}{r}|(|\binom{a}{n}| + |\binom{a}{n-r}| + |\binom{a}{n}(-1)^r - \binom{a}{n-r}|))^2$
      viii. $= \frac{1}{X^2}(2\sum_r^{[1:n]} |\binom{b}{r}||\binom{a}{n-r}|)^2$
      ix. $= (\frac{2}{X})^2(|\binom{a+b}{n}| + |\binom{a}{n}| + |\binom{b}{n}|)^2$

x. $\le (\frac{B}{n})^2$.

Procedure III:54

Objective

Choose a rational number $0 < X < 2$. The objective of the following instructions is to construct a positive rational number D such that $D > 1$, and a procedure $p(x, n, a, k)$ to show that $\|((1+x)^a_n)^k\|^2 < D^2$ when a complex number x, a rational number a, and positive integers n, k such that $\|x\|^2 \le 1$, $\mathrm{re}(x)+1 \ge X$, and $(ka)^2 < 1$ are chosen.

Implementation

1. Execute procedure III:29 on $\langle \frac{2}{X} \rangle$ and let $\langle E, N, q\rangle$ receive.
2. Let $D = \max(E, (1+\frac{2}{X})^{\lfloor N \rfloor})$.
3. Let $p(x, n, a, k)$ be the following procedure:
   (a) For $t \in [1:n]$, verify that $\binom{a}{t+1}(-1)^{t+1} - \binom{a}{t}(-1)^t$
      i. $= (-1)^{t+1}(\binom{a}{t+1} + \binom{a}{t})$
      ii. $= (-1)^{t+1} \cdot \frac{(a+1)^{\underline{t+1}}}{(t+1)!}$
      iii. > 0.
   (b) Hence verify that $\|k \sum_t^{[1:n]} \binom{a}{t} x^t\|^2$
      i. $= \|k \sum_t^{[1:n]}((\binom{a}{t+1}(-1)^{t+1} \cdot \frac{(-x)^{t+1}}{-x-1} - \binom{a}{t}(-1)^t \cdot \frac{(-x)^t}{-x-1} - \frac{(-x)^{t+1}}{-x-1}((\binom{a}{t+1}(-1)^{t+1} - \binom{a}{t}(-1)^t))\|^2$
      ii. $= \frac{k^2}{\|x+1\|^2}\|\binom{a}{n}x^n - \binom{a}{1}x^1 - \sum_t^{[1:n]}(-x)^{t+1}((\binom{a}{t+1}(-1)^{t+1} - \binom{a}{t}(-1)^t)\|^2$
      iii. $\le \frac{k^2}{(\mathrm{re}(x)+1)^2+\mathrm{im}(x)^2}(|\binom{a}{n}| + a + \sum_t^{[1:n]}|\binom{a}{t+1}(-1)^{t+1} - \binom{a}{t}(-1)^t|)^2$
      iv. $\le \frac{k^2}{X^2}(|\binom{a}{n}| + a + \sum_t^{[1:n]}(\binom{a}{t+1}(-1)^{t+1} - \binom{a}{t}(-1)^t))^2$
      v. $= \frac{k^2}{X^2}(|\binom{a}{n}| + a + \binom{a}{n}(-1)^n - \binom{a}{1}(-1)^1)^2$
      vi. $= \frac{k^2}{X^2}(|\binom{a}{n}| + a - |\binom{a}{n}| + a)^2$
      vii. $= (\frac{2ak}{X})^2$
      viii. $\le (\frac{2}{X})^2$.
   (c) If $k > N$, then do the following:
      i. Execute procedure q on $\langle k \sum_t^{[1:n]} \binom{a}{t} x^t, k\rangle$.
      ii. Hence verify that $\|((1+x)^a_n)^k\|^2$
         A. $= \|(\sum_t^{[0:n]} \binom{a}{t} x^t)^k\|^2$
         B. $= \|(1 + \sum_t^{[1:n]} \binom{a}{t} x^t)^k\|^2$
         C. $= \|\exp_k(k \sum_t^{[1:n]} \binom{a}{t} x^t)\|^2$
         D. $\le E^2$.
         E. $\le D^2$.
   (d) Otherwise do the following:
      i. Verify that $\|\sum_t^{[1:n]} \binom{a}{t} x^t\|^2$
         A. $\le \|k \sum_t^{[1:n]} \binom{a}{t} x^t\|^2$
         B. $\le (\frac{2}{X})^2$.
      ii. Verify that $\|((1+x)^a_n)^k\|^2$
         A. $= (\|(1+x)^a_n\|^2)^k$
         B. $= (\|1 + \sum_t^{[1:n]} \binom{a}{t} x^t\|^2)^k$
         C. $\le (1+\frac{2}{X})^{2k}$
         D. $\le D^2$.
4. **Yield the tuple $\langle D, p\rangle$.**

Procedure III:55

Objective

Choose a rational number $0 < X < 2$. The objective of the following instructions is to construct positive rational numbers G, N and a procedure $p(x, n, a, k)$ to show that $(1+x)^{ka}_n \equiv ((1+x)^a_n)^k$ (err $\frac{Gk}{n}$) when positive integers n, k, a rational number a, and a complex number x such that $\|x\|^2 \le 1$, $\mathrm{re}(x+1) \ge X$, $k > 1$, $0 < ka \le 1$, and $n > N$ are chosen.

Implementation

1. Execute procedure III:54 on $\langle X\rangle$ and let $\langle D, t\rangle$ receive.
2. Execute procedure III:53 on $\langle X\rangle$ and let $\langle B, N, q\rangle$ receive.
3. Let $G = DB$.

4. Let $p(x,n,a,k)$ be the following procedure:
   (a) If $k>0$, then for $r\in[1:k]$ do the following:
      i. Verify that $\|ar\|^2 \le \|ak\|^2 \le 1$.
      ii. Execute procedure t on $\langle x,n,a,r\rangle$.
      iii. Hence verify that $\|((1+x)^a_n)^r\|^2 \le D^2$.
   (b) For $r\in[0:k]$, do the following:
      i. Verify that $a^2 \le (ka)^2 \le 1$.
      ii. Verify that $((k-r-1)a)^2 \le (ka)^2 \le 1$.
      iii. Execute procedure q on $\langle x,a,(k-r-1)a, n\rangle$.
      iv. Hence verify that $\|(1+x)^a_n(1+x)^b_n-(1+x)^{a+b}_n\|^2 \le (\frac{B}{n})^2$.
   (c) Hence verify that $\|(1+x)^{ka}_n-((1+x)^a_n)^k\|^2$
      i. $=\|\sum_r^{[0:k]}(((1+x)^a_n)^r(1+x)^{(k-r)a}_n-((1+x)^a_n)^{r+1}(1+x)^{(k-r-1)a}_n)\|^2$
      ii. $=\|\sum_r^{[0:k]}((1+x)^a_n)^r((1+x)^{(k-r)a}_n-(1+x)^a_n(1+x)^{(k-r-1)a}_n)\|^2$
      iii. $\le(\sum_r^{[0:k]}\frac{DB}{n})^2$
      iv. $=(\frac{Gk}{n})^2$.
5. **Yield the tuple $\langle G,D,N,p\rangle$.**

Procedure III:56

Objective

Choose a rational number $X>0$. The objective of the following instructions is to construct positive rational numbers a,c such that $b>1$, and a procedure $p(x,n,k)$ to show that $\exp_n(n((1+x)^{\frac{1}{n}}_k-1)) \equiv 1+x$ (err $\frac{an}{k}$) when a complex number x, and positive integers n,k such that $\|x\|^2\le 1$, $\mathrm{re}(x)+1\ge X$, $n>1$, and $k>c$ are chosen.

Implementation

1. Execute procedure III:55 on $\langle X\rangle$ and let $\langle a,c,p_1\rangle$ receive.
2. Let $p(x,n,k)$ be the following procedure:
   (a) Using procedure III:44, verify that $(1+x)^1_k=(1+x)^1=1+x$.
   (b) Execute procedure p_1 on $\langle x,k,\frac{1}{n},n\rangle$.
   (c) Hence verify that $\|(1+x)^1_k-((1+x)^{\frac{1}{n}}_k)^n\|^2 \le (\frac{an}{k})^2$.
   (d) Hence verify that $\|\exp_n(n((1+x)^{\frac{1}{n}}_k-1))-(1+x)\|^2$
      i. $=\|(1+\frac{1}{n}(n((1+x)^{\frac{1}{n}}_k-1)))^n-(1+x)\|^2$
      ii. $=\|((1+x)^{\frac{1}{n}}_k)^n-(1+x)^1_k\|^2$
      iii. $\le(\frac{an}{k})^2$.
3. **Yield the tuple $\langle a,c,p\rangle$.**

Procedure III:57

Objective

Choose a rational number $X>0$. The objective of the following instructions is to construct a rational number $a>0$ and a procedure $p(x,n,k)$ to show that $\|n((1+x)^{\frac{1}{n}}_k-1)\|^2\le a^2$ when positive integers n,k, and a complex number x such that $\|x\|^2\le 1$ and $\mathrm{re}(x)+1\ge X$ are chosen.

Implementation

1. Let $a=\frac{2}{X}$.
2. Let $p(x,n,k)$ be the following procedure:
   (a) Verify that $\|n((1+x)^{\frac{1}{n}}_k-1)\|^2$
      i. $=\|n(\sum_r^{[0:k]}\binom{\frac{1}{n}}{r}x^r-1)\|^2$
      ii. $=\|n\sum_r^{[1:k]}\binom{\frac{1}{n}}{r}(-1)^r(-x)^r\|^2$
      iii. $=n^2\|\sum_r^{[1:k]}(\binom{\frac{1}{n}}{r+1}(-1)^{r+1}\cdot\frac{(-x)^{r+1}}{-x-1}-\binom{\frac{1}{n}}{r}(-1)^r\cdot\frac{(-x)^r}{-x-1}-(\binom{\frac{1}{n}}{r+1}(-1)^{r+1}-\binom{\frac{1}{n}}{r}(-1)^r)\frac{(-x)^{r+1}}{-x-1})\|^2$
      iv. $=\frac{n^2}{\|x+1\|^2}\|\binom{\frac{1}{n}}{k}x^k-\binom{\frac{1}{n}}{1}x^1-\sum_r^{[1:k]}(\binom{\frac{1}{n}}{r+1}(-1)^{r+1}-\binom{\frac{1}{n}}{r}(-1)^r)(-x)^{r+1}\|^2$
      v. $\le\frac{n^2}{\|x+1\|^2}\|\binom{\frac{1}{n}}{k}(-1)^{k-1}+\frac{1}{n}+\sum_r^{[1:k]}(\binom{\frac{1}{n}}{r+1}(-1)^{r+1}-\binom{\frac{1}{n}}{r}(-1)^r)\|^2$
      vi. $=\frac{n^2}{(\mathrm{re}(x)+1)^2+\mathrm{im}(x)^2}(\binom{\frac{1}{n}}{k}(-1)^{k-1}+\frac{1}{n}+\binom{\frac{1}{n}}{k}(-1)^k-\binom{\frac{1}{n}}{1}(-1)^1)^2$

vii. $\leq \frac{n^2}{X^2}(\frac{2}{n})^2$

viii. $= a^2$.

3. **Yield the tuple $\langle a, p \rangle$.**

Declaration III:16

The notation $\omega(r)$ will be used as a shorthand notation for $\frac{1}{r}(1 - \prod_t^{[1:r]}(1 - \frac{1}{nt}))$.

Procedure III:58

Objective

Choose two positive integers r, n such that $r > 1$. The objective of the following instructions is to show that $\frac{\omega(r+1)}{\omega(r)} \leq 1$.

Implementation

1. Using procedure II:32, verify that $\frac{\omega(r+1)}{\omega(r)}$

   (a) $= \frac{\frac{1}{r+1}(1-\prod_t^{[1:r+1]}(1-\frac{1}{nt}))}{\frac{1}{r}(1-\prod_t^{[1:r]}(1-\frac{1}{nt}))}$

   (b) $= \frac{r}{r+1} \cdot \frac{1-(1-\frac{1}{nr})\prod_t^{[1:r]}(1-\frac{1}{nt})}{1-\prod_t^{[1:r]}(1-\frac{1}{nt})}$

   (c) $= \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}\prod_t^{[1:r]}(1-\frac{1}{nt})}{1-\prod_t^{[1:r]}(1-\frac{1}{nt})}\right)$

   (d) $= \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}}{(\prod_t^{[1:r]}(1-\frac{1}{nt}))^{-1}-1}\right)$

   (e) $\leq \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}}{(1-\frac{1}{n(r-1)})^{-(r-1)}-1}\right)$

   (f) $= \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}}{(1+\frac{1}{nr-n-1})^{r-1}-1}\right)$

   (g) $\leq \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}}{(1+\frac{1}{n(r-1)})^{r-1}-1}\right)$

   (h) $\leq \frac{r}{r+1}\left(1 + \frac{\frac{1}{nr}}{1+\frac{r-1}{n(r-1)}-1}\right)$

   (i) $= \frac{r}{r+1}(1 + \frac{1}{r})$

   (j) $= 1$.

Declaration III:17

The notation $\ln_k(1 + x)$ will be used as a shorthand for $\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r} x^r$.

Procedure III:59

Objective

Choose a rational number $X > 0$. The objective of the following instructions is to construct a positive rational number a and a procedure $p(x, n, k)$ to show that $\ln_k(1+x) \equiv n((1+x)_k^{\frac{1}{n}} - 1)$ (err $\frac{a}{n}$) when positive integers n, k and a complex number x such that $\|x\|^2 \leq 1$ and $\mathrm{re}(x) + 1 \geq X$ are chosen.

Implementation

1. Let $a = \frac{1}{X}$.
2. Let $p(x, n, k)$ be the following procedure:

   (a) For $r \in [2 : k]$, use procedure III:58 to verify that $\frac{\omega(r+1)}{\omega(r)} \leq 1$.

   (b) Hence verify that $\|\ln_k(1+x) - n((1+x)_k^{\frac{1}{n}} - 1)\|^2$

      i. $= \|\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r} x^r - n(\sum_r^{[0:k]} \binom{\frac{1}{n}}{r} x^r - 1)\|^2$

      ii. $= \|\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r} x^r - n\sum_r^{[1:k]} \binom{\frac{1}{n}}{r} x^r\|^2$

      iii. $= \|\sum_r^{[1:k]} \frac{(-1)^{\underline{r-1}}}{r!} x^r - \sum_r^{[1:k]} \frac{(\frac{1}{n}-1)^{\underline{r-1}}}{r!} x^r\|^2$

      iv. $= \|\sum_r^{[1:k]} \frac{1}{r!}((-1)^{\underline{r-1}} - (\frac{1}{n} - 1)^{\underline{r-1}}) x^r\|^2$

      v. $= \|\sum_r^{[1:k]} \frac{(-1)^{\underline{r-1}}}{r!}(1 - \frac{(\frac{1}{n}-1)^{\underline{r-1}}}{(-1)^{\underline{r-1}}}) x^r\|^2$

      vi. $= \|\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r}(1 - \prod_t^{[1:r]} \frac{\frac{1}{n}-t}{-t}) x^r\|^2$

      vii. $= \|\sum_r^{[1:k]} \omega(r)(-x)^r\|^2$

      viii. $= \|\sum_r^{[1:k]}(\omega(r+1) \cdot \frac{(-x)^{r+1}}{-x-1} - \omega(r) \cdot \frac{(-x)^r}{-x-1} - (\omega(r+1) - \omega(r)) \cdot \frac{(-x)^{r+1}}{-x-1})\|^2$

      ix. $= \frac{1}{\|x+1\|^2}\|\omega(k)(-x)^k - \omega(1)(-x)^1 - \sum_r^{[1:k]}(\omega(r+1) - \omega(r))(-x)^{r+1}\|^2$

      x. $\leq \frac{1}{\|x+1\|^2}(\omega(k) + \omega(1) + \sum_r^{[2:k]}(\omega(r) - \omega(r+1)) + \omega(2) - \omega(1))^2$

xi. $= \frac{1}{((\mathrm{re}(x)+1)^2+\mathrm{im}(x)^2)}(\omega(k) - \omega(k) + \omega(2) + \omega(2) + \omega(1) - \omega(1))^2$

xii. $\leq (\frac{a}{n})^2$.

3. **Yield the tuple $\langle a, p \rangle$.**

Procedure III:60

Objective

Choose a rational number $X > 0$. The objective of the following instructions is to construct a rational number $a > 0$ and a procedure $p(x, k)$ to show that $\|\ln_k(1+x)\|^2 \leq a^2$ when a positive integer k and a complex number x such that $\|x\|^2 \leq 1$ and $\mathrm{re}(x) + 1 \geq X$ are chosen.

Implementation

1. Let $a = \frac{2}{X}$.
2. Let $p(x, k)$ be the following procedure:

(a) Verify that $\|\ln_k(1+x)\|^2$

i. $= \|\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r} x^r\|^2$

ii. $= \|\sum_r^{[1:k]} \frac{1}{r}(-x)^r\|^2$

iii. $= \|\sum_r^{[1:k]}(\frac{1}{r+1} \cdot \frac{(-x)^{r+1}}{-x-1} - \frac{1}{r} \cdot \frac{(-x)^r}{-x-1} - (\frac{1}{r+1} - \frac{1}{r}) \cdot \frac{(-x)^{r+1}}{-x-1})\|^2$

iv. $= \frac{1}{\|x+1\|^2}\|\frac{1}{k}(-x)^k - \frac{1}{1}(-x)^1 - \sum_r^{[1:k]}(\frac{1}{r+1} - \frac{1}{r})(-x)^{r+1}\|^2$

v. $\leq \frac{1}{\|x+1\|^2}(\frac{1}{k} + 1 + \sum_r^{[1:k]}(\frac{1}{r} - \frac{1}{r+1}))^2$

vi. $= \frac{1}{\|x+1\|^2}(\frac{1}{k} + 1 - \frac{1}{k} + 1)^2$

vii. $= \frac{4}{(\mathrm{re}(x)+1)^2+\mathrm{im}(x)^2}$

viii. $\leq a^2$

3. **Yield the tuple $\langle a, p \rangle$.**

Procedure III:61

Objective

Choose a rational number $X > 0$. The objective of the following instructions is to construct positive rational numbers a, c, d, e such that $b > 1$, and a procedure $p(x, n, k)$ to show that $\exp_n(\ln_k(1+x)) \equiv (1+x)$ (err $\frac{an}{k} + \frac{c}{n}$) when positive integers n, k, and a complex number x such that $\|x\|^2 \leq 1$, $\mathrm{re}(x) + 1 \geq X$, $k > d$, and $n > e$ are chosen.

Implementation

1. Execute procedure III:57 on $\langle X \rangle$ and let $\langle a_1, p_1 \rangle$ receive.
2. Execute procedure III:60 on $\langle X \rangle$ and let $\langle a_2, p_2 \rangle$ receive.
3. Execute procedure III:34 on $\langle \max(a_1, a_2) \rangle$ and let $\langle a_3, e, p_3 \rangle$ receive.
4. Execute procedure III:59 on $\langle X \rangle$ and let $\langle a_4, p_4 \rangle$ receive.
5. Execute procedure III:56 on $\langle X \rangle$ and let $\langle a, d, p_5 \rangle$ receive.
6. Let $c = a_4 a_3$.
7. Let $p(x, n, k)$ be the following procedure:

(a) Execute procedure p_1 on $\langle x, n, k \rangle$.

(b) Hence verify that $\|n((1+x)_k^{\frac{1}{n}} - 1)\|^2 \leq {a_1}^2$.

(c) Execute procedure p_2 on $\langle x, k \rangle$.

(d) Hence verify that $\|\ln_k(1+x)\|^2 \leq {a_2}^2$.

(e) Execute procedure p_4 on $\langle x, n, k \rangle$.

(f) Hence verify that $\|\ln_k(1+x) - n((1+x)_k^{\frac{1}{n}} - 1)\|^2 \leq (\frac{a_4}{n})^2$.

(g) Execute procedure p_3 on $\langle \ln_k(1+x), n((1+x)_k^{\frac{1}{n}} - 1), n \rangle$.

(h) Hence verify that $\|\exp_n(\ln_k(1+x)) - \exp_n(n((1+x)_k^{\frac{1}{n}} - 1))\|^2 \leq (\frac{a_4}{n})^2 {a_3}^2 = (\frac{c}{n})^2$.

(i) Execute procedure p_5 on $\langle x, n, k \rangle$.

(j) Hence verify that $\|\exp_n(n((1+x)_k^{\frac{1}{n}} - 1)) - (1+x)\|^2 \leq (\frac{an}{k})^2$.

(k) Hence verify that $\|\exp_n(\ln_k(1+x)) - (1+x)\|^2$

i. $= \|\exp_n(\ln_k(1+x)) - \exp_n(n((1+x)_k^{\frac{1}{n}} - 1)) + \exp_n(n((1+x)_k^{\frac{1}{n}} - 1)) - (1+x)\|^2$

ii. $\leq (\frac{c}{n} + \frac{an}{k})^2$.

8. **Yield the tuple $\langle a, c, d, e, p \rangle$.**

Declaration III:18

The notation τ_n, where n is a positive integer, will be used as a shorthand for $8\,\mathrm{im}(\ln_n(1+i))$.

Procedure III:62

Objective

Choose a positive integer k. The objective of the following instructions is to show that $\tau_k = 8\sum_r^{[0:\lfloor\frac{k}{2}\rfloor]} \frac{(-1)^r}{2r+1}$.

Implementation

1. Using declaration III:18, verify that τ_k
   (a) $= 8\,\mathrm{im}(\sum_r^{[1:k]} \frac{(-1)^{r-1}}{r} i^r)$
   (b) $= 8\,\mathrm{im}(\sum_r^{[0:\lfloor\frac{k}{2}\rfloor]} \frac{(-1)^{2r}}{2r+1} i^{2r+1})$
   (c) $= 8\sum_r^{[0:\lfloor\frac{k}{2}\rfloor]} \frac{i^{2r}}{2r+1}$
   (d) $= 8\sum_r^{[0:\lfloor\frac{k}{2}\rfloor]} \frac{(-1)^r}{2r+1}$.

Procedure III:63

Objective

The objective of the following instructions is to construct positive rational numbers a, b such that $a \geq 4$, and a procedure, $p(n)$, to show that $\tau_n \geq a$ when a positive integer $n \geq b$ is chosen.

Implementation

1. Let $a = \frac{16}{3}$.
2. **Verify that $a \geq 4$.**
3. Let $b = 4$.
4. Let $p(n)$ be the following procedure:
   (a) Let $d = n \operatorname{div} 4$.
   (b) Let $g = n \bmod 4$.
   (c) Hence verify that $n = 4d + g$.
   (d) If $g = 0$ or $g = 1$, then do the following:
      i. Using procedure III:62, verify that τ_n
         A. $= 8\sum_r^{[0:\lfloor\frac{4d+g}{2}\rfloor]} \frac{(-1)^r}{2r+1}$
         B. $= 8\sum_r^{[0:2d]} \frac{(-1)^r}{2r+1}$
         C. $= 8(1 - \frac{1}{3} + \sum_r^{[2:2d]} \frac{(-1)^r}{2r+1})$
         D. $= \frac{16}{3} + 8\sum_r^{[1:d]}(\frac{1}{4r+1} - \frac{1}{4r+3})$
         E. $\geq \frac{16}{3}$.
   (e) Otherwise do the following:
      i. Verify that $g = 2$ or $g = 3$.
      ii. Hence verify that τ_n
         A. $= 8\sum_r^{[0:\lfloor\frac{4d+g}{2}\rfloor]} \frac{(-1)^r}{2r+1}$
         B. $= 8\sum_r^{[0:2d+1]} \frac{(-1)^r}{2r+1}$
         C. $= 8(1 - \frac{1}{3} + \sum_r^{[0:2d]} \frac{(-1)^r}{2r+1} + \frac{(-1)^{2d}}{4d+1})$
         D. $\frac{16}{3} + 8\sum_r^{[1:d]}(\frac{1}{4r+1} - \frac{1}{4r+3}) + \frac{8}{4d+1}$
         E. $\geq \frac{16}{3}$.
5. **Yield the tuple $\langle a, b, p\rangle$.**

Procedure III:64

Objective

The objective of the following instructions is to construct rational numbers a, b such that $a \geq 4$ and $a^2 < 48$, and a procedure, $p(n)$, to show that $\tau_n \leq a$ when a positive integer n such that $n \geq b$ is chosen.

Implementation

1. Let $a = \frac{2104}{315}$.
2. **Verify that $a \geq 4$.**
3. **Verify that $a^2 = \frac{4426816}{99225} < 48$.**
4. Let $b = 10$.
5. Let $p(n)$ be the following procedure:
   (a) Let $d = n \operatorname{div} 4$.
   (b) Let $g = n \bmod 4$.
   (c) Hence verify that $n = 4d + g$.
   (d) If $g = 0$ or $g = 1$, then do the following:
      i. Verify that τ_n

A. $= 8\sum_r^{[0:\lfloor \frac{n}{2} \rfloor]} \frac{(-1)^r}{2r+1}$

B. $= 8\sum_r^{[0:5]} \frac{(-1)^r}{2r+1} + 8\sum_r^{[5:\lfloor \frac{4d+g}{2} \rfloor]} \frac{(-1)^r}{2r+1}$

C. $= a + 8\sum_r^{[5:2d]} \frac{(-1)^r}{2r+1}$

D. $= a + 8\sum_r^{[5:2d-1]} \frac{(-1)^r}{2r+1} + \frac{8(-1)^{2d-1}}{4d-1}$

E. $= a - 8\sum_r^{[3:d]} (\frac{1}{4r-1} - \frac{1}{4r+1}) - \frac{8}{4d-1}$

F. $\leq a$.

(e) Otherwise do the following:

i. Verify that $g = 2$ or $g = 3$.

ii. Hence verify that τ_n

A. $= 8\sum_r^{[0:\lfloor \frac{n}{2} \rfloor]} \frac{(-1)^r}{2r+1}$

B. $= 8\sum_r^{[0:5]} \frac{(-1)^r}{2r+1} + 8\sum_r^{[5:\lfloor \frac{4d+g}{2} \rfloor]} \frac{(-1)^r}{2r+1}$

C. $= a + 8\sum_r^{[5:2d+1]} \frac{(-1)^r}{2r+1}$

D. $= a - 8\sum_r^{[2:d]} (\frac{1}{4r+3} - \frac{1}{4r+5})$

E. $\leq a$.

6. **Yield the tuple** $\langle a, b, p \rangle$**.**

Procedure III:65

Objective

The objective of the following instructions is to construct positive rational numbers a, c, d, e, and a procedure $p(n, k)$ to show that $\exp_n(\frac{1}{4}\tau_k i) \equiv i$ (err $\frac{an}{k} + \frac{c}{n}$) when integers k, n such that $n > e$ and $k > d$ are chosen.

Implementation

1. Execute procedure III:60 on $\langle 1 \rangle$ and let $\langle a_1, p_1 \rangle$ receive.

2. Execute procedure III:32 on $\langle a_1 \rangle$ and let $\langle a_2, b_2, p_2 \rangle$ receive.

3. Execute procedure III:30 on $\langle a_1 \rangle$ and let $\langle a_3, b_3, p_3 \rangle$ receive.

4. Execute procedure III:61 on $\langle 1 \rangle$ and let $\langle a_4, c_4, d, e_4, p_4 \rangle$ receive.

5. Let $a = \frac{2a_4}{a_3}$.

6. Let $c = \frac{2c_4}{a_3} + a_2$.

7. Let $e = \max(b_2, b_3, e_4)$.

8. Let $p(n, k)$ be the following procedure:

(a) Execute procedure p_1 on $\langle i, k \rangle$.

(b) Hence verify that $\|\ln_k(1+i)\|^2 \leq {a_1}^2$.

(c) Execute procedure p_2 on $\langle \ln_k(1+i), \overline{\ln_k(1+i)}, n \rangle$.

(d) Hence verify that $\|\exp_n(\ln_k(1+i) - \overline{\ln_k(1+i)}) - \frac{\exp_n(\ln_k(1+i))}{\exp_n(\overline{\ln_k(1+i)})}\|^2 \leq \frac{{a_2}^2}{n^2}$.

(e) Execute procedure p_4 on $\langle i, n, k \rangle$.

(f) Hence verify that $\|\exp_n(\ln_k(1+i)) - (1+i)\|^2 \leq (\frac{a_4 n}{k} + \frac{c_4}{n})^2$.

(g) Execute procedure p_3 on $\langle \ln_k(1+i), n \rangle$.

(h) Hence verify that $\|\exp_n(\ln_k(1+i))\|^2 \geq a_3$.

(i) Hence verify that $\|\frac{\overline{\exp_n(\ln_k(1+i))}}{\exp_n(\overline{\ln_k(1+i)})} - \frac{\overline{1+i}}{\exp_n(\overline{\ln_k(1+i)})}\|^2 \leq \frac{1}{{a_3}^2}(\frac{a_4 n}{k} + \frac{c_4}{n})^2$.

(j) Also verify that $\|\frac{\overline{1+i}}{\exp_n(\overline{\ln_k(1+i)})} - \frac{\overline{1+i}}{1+i}\|^2 = \|\frac{(\overline{1+i})(\overline{(1+i) - \exp_n(\ln_k(1+i))})}{\exp_n(\overline{\ln_k(1+i)})(1+i)}\|^2 \leq \frac{1}{{a_3}^2}(\frac{a_4 n}{k} + \frac{c_4}{n})^2$.

(k) Hence verify that $\|\exp_n(\frac{1}{4}\tau_k i) - i\|^2$

i. $= \|\exp_n(2\operatorname{im}(\ln_k(1+i))i) - i\|^2$

ii. $= \|\exp_n(\ln_k(1+i) - \overline{\ln_k(1+i)}) - i\|^2$

iii. $= \|\exp_n(\ln_k(1+i) - \overline{\ln_k(1+i)}) - \frac{\exp_n(\ln_k(1+i))}{\exp_n(\overline{\ln_k(1+i)})} + \frac{\exp_n(\ln_k(1+i))}{\exp_n(\overline{\ln_k(1+i)})} - \frac{\overline{1+i}}{\exp_n(\overline{\ln_k(1+i)})} + \frac{\overline{1+i}}{\exp_n(\overline{\ln_k(1+i)})} - \frac{\overline{1+i}}{1+i}\|^2$

iv. $\leq (\frac{a_2}{n} + \frac{2}{a_3}(\frac{a_4 n}{k} + \frac{c_4}{n}))^2$

v. $= (\frac{an}{k} + \frac{c}{n})^2$.

9. **Yield the tuple** $\langle a, c, d, e, p \rangle$**.**

Procedure III:66

Objective

The objective of the following instructions is to construct positive rational numbers a, c, d, e such that $b > 1$, and a procedure, $p(n, k)$, to show that $\exp_n(-\frac{1}{4}\tau_k i) \equiv -i$ (err $\frac{an}{k} + \frac{c}{n}$) when integers k, n such that $n > e$ and $k > d$ are chosen.

Implementation

Implementation is analogous to that of procedure III:65.

Procedure III:67

Objective

Choose an integer $K \geq 0$. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n, m, k)$, to show that $\exp_n(\frac{k}{4}\tau_m i) \equiv i^k$ (err $\frac{an}{m} + \frac{b}{n}$) when a non-negative integer k and two positive integers n, m such that $k \leq K$, $n > c$, and $m > d$ are chosen.

Implementation

1. Execute procedure III:64 and let $\langle a_1, d, p_1\rangle$ receive.
2. Execute procedure III:33 on $\langle(\frac{a_1}{4})^2\rangle$ and let $\langle a_2, b_2, p_2\rangle$ receive.
3. Execute procedure III:65 and let $\langle a_3, b_3, c_3, p_3\rangle$ receive.
4. Execute procedure III:29 on $\langle(\frac{a_1}{4})^2\rangle$ and let $\langle a_4, b_4, p_4\rangle$ receive.
5. Let $a = a_3 \cdot \frac{{a_4}^K - 1}{a_4 - 1}$.
6. Let $b = a_2 K + b_3 \cdot \frac{{a_4}^k - 1}{a_4 - 1}$.
7. Let $c = \max(b_2, b_4, c_3)$.
8. Let $p(n, k, m)$ be the following procedure:
   (a) Execute procedure p_1 on $\langle m\rangle$.
   (b) Hence verify that $\tau_m \leq a_1$.
   (c) Hence verify that $\|\frac{1}{4}\tau_m i\|^2 = \|\frac{1}{4}\tau_m\|^2 \leq (\frac{a_1}{4})^2$.
   (d) Execute procedure p_2 on $\langle\frac{1}{4}\tau_m i, k, n\rangle$.
   (e) Hence verify that $\|\exp_n(\frac{k}{4}\tau_m i) - \exp_n(\frac{1}{4}\tau_m i)^k\|^2 \leq (\frac{a_2 k}{n})^2 \leq (\frac{a_2 K}{n})^2$.
   (f) Execute procedure p_3 on $\langle n, m\rangle$.
   (g) Hence verify that $\|\exp_n(\frac{1}{4}\tau_m i) - i\|^2 \leq (\frac{a_3 n}{m} + \frac{b_3}{n})^2$.
   (h) Execute procedure p_4 on $\langle\frac{1}{4}\tau_m i, n\rangle$.
   (i) Hence verify that $\|\exp_n(\frac{1}{4}\tau_m i)\|^2 \leq a_4$.
   (j) Verify that $\|\exp_n(\frac{k}{4}\tau_m i) - i^k\|^2$
      i. $= \|\exp_n(\frac{k}{4}\tau_m i) - \exp_n(\frac{1}{4}\tau_m i)^k + \exp_n(\frac{1}{4}\tau_m i)^k - i^k\|^2$
      ii. $= \|\exp_n(\frac{k}{4}\tau_m i) - \exp_n(\frac{1}{4}\tau_m i)^k + (\exp_n(\frac{1}{4}\tau_m i) - i)\sum_t^{[0:k]} \exp_n(\frac{1}{4}\tau_m i)^t i^{k-1-t}\|^2$
      iii. $\leq (\frac{a_2 K}{n} + (\frac{a_3 n}{m} + \frac{b_3}{n})\sum_t^{[0:k]} {a_4}^t)^2$
      iv. $= ((a_2 K + b_3 \frac{{a_4}^k - 1}{a_4 - 1})\frac{1}{n} + (a_3 \frac{{a_4}^k - 1}{a_4 - 1})\frac{n}{m})^2$
      v. $\leq (\frac{an}{m} + \frac{b}{n})^2$.
9. **Yield the tuple $\langle a, b, c, d, p\rangle$.**

Procedure III:68

Objective

Choose an integer $K \geq 0$. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n, m, k)$, to show that $\exp_n(\frac{k}{4}\tau_m i) \equiv i^k$ (err $\frac{an}{m} + \frac{b}{n}$) when an integer k and two positive integers n, m such that $|k| \leq K$, $n > c$, and $m > d$ are chosen.

Implementation

Implementation is an extension of that of procedure III:67 using procedure III:66.

Procedure III:69

Objective

Choose an integer $K \geq 0$. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n, m, k)$, to show that $\cos_n(\frac{k}{4}\tau_m) \equiv \frac{i^k + (-i)^k}{2}$ (err $\frac{an}{m} + \frac{b}{n}$) when an integer k and two positive integers n, m such that $|k| \leq K$, $n > c$, and $m > d$ are chosen.

Implementation

1. Execute procedure III:68 on $\langle K\rangle$ and let $\langle a, b, c, d, q\rangle$ receive.
2. Let $p(n, m, k)$ be the following procedure:
   (a) Execute procedure q on $\langle n, m, k\rangle$.
   (b) Hence verify that $\|\exp_n(\frac{k}{4}\tau_m i) - i^k\|^2 \leq (\frac{an}{m} + \frac{b}{n})^2$.
   (c) Execute procedure q on $\langle n, m, -k\rangle$.
   (d) Hence verify that $\|\exp_n(-\frac{k}{4}\tau_m i) - i^{-k}\|^2 \leq (\frac{an}{m} + \frac{b}{n})^2$.
   (e) Hence verify that $\|\cos_n(\frac{k}{4}\tau_m) - \frac{i^k+(-i)^k}{2}\|^2$
      i. $= \|\frac{\exp_n(\frac{k}{4}\tau_m i)+\exp_n(-\frac{k}{4}\tau_m i)}{2} - \frac{i^k+(-i)^k}{2}\|^2$
      ii. $= \|\frac{\exp_n(\frac{k}{4}\tau_m i)-i^k}{2} + \frac{\exp_n(-\frac{k}{4}\tau_m i)-(-i)^k}{2}\|^2$
      iii. $\leq \frac{1}{2}\|\exp_n(\frac{k}{4}\tau_m i)-i^k\|^2+\frac{1}{2}\|\exp_n(-\frac{k}{4}\tau_m i)-(-i)^k\|^2$
      iv. $\leq (\frac{an}{m} + \frac{b}{n})^2$.
3. **Yield the tuple** $\langle a, b, c, d, p\rangle$**.**

Procedure III:70

Objective

Choose an integer $K \geq 0$. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n, m, k)$, to show that $\sin_n(\frac{k}{4}\tau_m) \equiv \frac{i^k-(-i)^k}{2i}$ (err $\frac{an}{m} + \frac{b}{n}$) when an integer k and two positive integers n, m such that $|k| \leq K$, $n > c$, and $m > d$ are chosen.

Implementation

Implementation is analogous to that of procedure III:69.

Procedure III:71

Objective

Choose two integers $X \geq 0, K \geq 0$. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(x, n, m, k)$, to show that $\exp_n(x + \frac{k}{4}\tau_m i) \equiv i^k \exp_n(x)$ (err $\frac{an}{m} + \frac{b}{n}$) when an integer k and two positive integers n, m such that $\|x\|^2 \leq X$, $|k| \leq K$, $n > c$, and $m > d$ are chosen.

Implementation

1. Execute procedure III:64 and let $\langle a_1, b_1, p_1\rangle$ receive.
2. Execute procedure III:31 on $\langle \max(X, \frac{K^2{a_1}^2}{16})\rangle$ and let $\langle a_2, b_2, p_2\rangle$ receive.
3. Execute procedure III:29 on $\langle X\rangle$ and let $\langle a_3, b_3, p_3\rangle$ receive.
4. Execute procedure III:68 on $\langle K\rangle$ and let $\langle a_4, b_4, c_4, d_4, p_4\rangle$ receive.
5. Let $a = a_3 a_4$.
6. Let $b = \frac{a_2 X K a_1}{4} + a_3 b_4$.
7. Let $c = \max(b_2, b_3, c_4)$.
8. Let $d = \max(b_1, d_4)$.
9. Let $p(x, n, k, m)$ be the following procedure:
   (a) Verify that $\|x\|^2 \leq X$.
   (b) Execute procedure p_1 on $\langle m\rangle$.
   (c) Hence verify that $\tau_m \leq a_1$.
   (d) Hence verify that $\|\frac{k}{4}\tau_m i\|^2 = \frac{k^2{\tau_m}^2}{16} \leq \frac{K^2{a_1}^2}{16}$.
   (e) Now execute procedure p_2 on $\langle x, \frac{k}{4}\tau_m i, n\rangle$.
   (f) Hence verify that $\|\exp_n(x)\exp_n(\frac{k}{4}\tau_m i) - \exp_n(x + \frac{k}{4}\tau_m i)\|^2 \leq \frac{{a_2}^2\|x\|^2\|\frac{k}{4}\tau_m i\|^2}{n^2} \leq \frac{{a_2}^2X^2K^2{a_1}^2}{16n^2}$.
   (g) Execute procedure p_3 on $\langle x, n\rangle$.
   (h) Hence verify that $\|\exp_n(x)\|^2 \leq {a_3}^2$.
   (i) Execute procedure p_4 on $\langle n, m, k\rangle$.
   (j) Hence verify that $\|\exp_n(\frac{k}{4}\tau_m i) - i^k\|^2 \leq (\frac{a_4 n}{m} + \frac{b_4}{n})^2$.
   (k) Verify that $\|\exp_n(x + \frac{k}{4}\tau_m i) - i^k\exp_n(x)\|^2$
      i. $= \|\exp_n(x+\frac{k}{4}\tau_m i)-\exp_n(x)\exp_n(\frac{k}{4}\tau_m i)+\exp_n(x)\exp_n(\frac{k}{4}\tau_m i) - i^k\exp_n(x)\|^2$

ii. $= \|\exp_n(x+\frac{k}{4}\tau_m i)-\exp_n(x)\exp_n(\frac{k}{4}\tau_m i)+\exp_n(x)(\exp_n(\frac{k}{4}\tau_m i)-i^k)\|^2$

iii. $\leq (\frac{a_2 X K a_1}{4n} + a_3(\frac{a_4 n}{m} + \frac{b_4}{n}))^2$

iv. $= (\frac{an}{m} + \frac{b}{n})^2$.

10. **Yield the tuple $\langle a,b,c,d,p\rangle$.**

Procedure III:72

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n,m,k)$, to show that $\exp_n(\frac{k}{K}\tau_m i)^K \equiv 1$ (err $\frac{an}{m} + \frac{b}{n}$) when an integer k and positive integers n, m such that $0 \leq k < K$, $n \geq c$, and $m > d$ are chosen.

Implementation

1. Execute procedure III:64 and let $\langle a_1, b_1, p_1\rangle$ receive.
2. Execute procedure III:33 on $\langle K a_1\rangle$ and let $\langle a_2, b_2, p_2\rangle$ receive.
3. Execute procedure III:68 on $\langle 4K\rangle$ and let $\langle a_3, b_3, c_3, d_3, p_3\rangle$ receive.
4. Let $a = a_3$.
5. Let $b = a_2 K + b_3$.
6. Let $c = \max(b_2, c_3)$.
7. Let $d = \max(b_1, d_3)$.
8. Let $p(n,m,k)$ be the following procedure:

(a) Execute procedure p_1 on $\langle m\rangle$.

(b) Hence verify that $\tau_m \leq a_1$.

(c) Hence verify that $\|K\frac{k}{K}\tau_m i\| = \|k\tau_m\|^2 \leq (K a_1)^2$.

(d) Execute procedure p_2 on $\langle \frac{k}{K}\tau_m i, K, n\rangle$.

(e) Hence verify that $\|\exp_n(K\frac{k}{K}\tau_m i) - \exp_n(\frac{k}{K}\tau_m i)^K\|^2 \leq (\frac{a_2 K}{n})^2$.

(f) Execute procedure p_3 on $\langle n, m, 4k\rangle$.

(g) Hence verify that $\|\exp_n(\frac{4k}{4}\tau_m i) - i^{4k}\|^2 \leq (\frac{a_3 n}{m} + \frac{b_3}{n})^2$.

(h) Verify that $\|\exp_n(\frac{k}{K}\tau_m i)^K - 1\|^2$

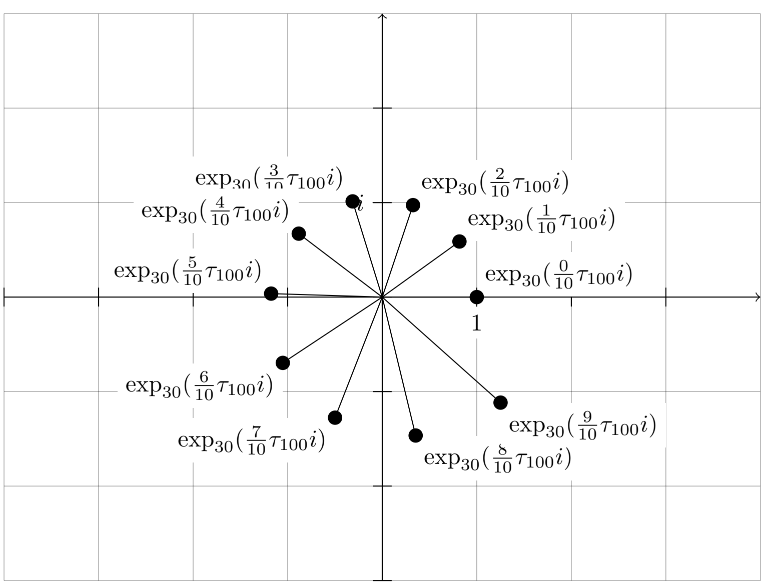
i. $= \|\exp_n(\frac{k}{K}\tau_m i)^K - \exp_n(k\tau_m i) + \exp_n(k\tau_m i) - 1\|^2$

ii. $\leq (\frac{a_2 K}{n} + \frac{a_3 n}{m} + \frac{b_3}{n})^2$

iii. $= (\frac{an}{m} + \frac{b}{n})^2$.

9. **Yield the tuple $\langle a,b,c,d,p\rangle$.**

Figure III:1



A plot of the list of complex numbers $\exp_{30}(\frac{[0{:}11]}{10}\tau_{100} i)$. Notice that when measurements are done relative to the complex number 1, $\exp_{30}(\frac{1}{10}\tau_{100} i)$ is roughly $\frac{1}{10}^{\text{th}}$ of a revolution, and also that each complex number has an angle that is roughly an integral multiple of that of $\exp_{30}(\frac{1}{10}\tau_{100} i)$.

Procedure III:73

Objective

Choose a two rationals M, N such that $0 < M$ and $N^2 < 12$. The objective of the following instructions is to construct rational numbers a, b such that $a > 0$, and a procedure, $p(x, n)$, to show that $\|\cos_n(x) - 1\|^2 \geq a^2$ when a rational number x and a positive integer n such that $M \leq |x| \leq N$ and $n > b$ are chosen.

Implementation

1. Let $a = \frac{M^2}{4}(1 - \frac{N^2}{12})$.
2. **Verify that $a > 0$.**
3. Let $b = 4$.
4. Let $p(x, n)$ be the following procedure:

(a) Using procedure III:36, verify that $(\cos_n(x) - 1)^2$

i. $= (\frac{1}{2}((1 + \frac{xi}{n})^n + (1 - \frac{xi}{n})^n) - 1)^2$

ii. $= (\frac{1}{2}(\sum_r^{[0:n+1]} \frac{n^r}{r!}(\frac{x}{n})^r i^r + \sum_r^{[0:n+1]} \frac{n^r}{r!}(\frac{x}{n})^r(-i)^r) - 1)^2$

iii. $= (\sum_r^{[0:\lfloor \frac{n}{2} \rfloor + 1]} \frac{n^{2r}}{(2r)!}(\frac{x}{n})^{2r}(-1)^r - 1)^2$

iv. $= (\sum_r^{[1:\lfloor \frac{n}{2} \rfloor + 1]} \frac{n^{2r}}{(2r)!}(\frac{x}{n})^{2r}(-1)^r)^2$

v. $= (\sum_r^{[1:\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \rfloor + 1]}(-\frac{n^{4r-2}}{(4r-2)!}(\frac{x}{n})^{4r-2} + \frac{n^{4r}}{(4r)!}(\frac{x}{n})^{4r}) - \frac{n^{2\lfloor \frac{n}{2} \rfloor}}{(2\lfloor \frac{n}{2} \rfloor)!}(\frac{x}{n})^{2\lfloor \frac{n}{2} \rfloor}[\lfloor \frac{n}{2} \rfloor \bmod 2 = 1])^2$

vi. $\geq (\sum_r^{[1:\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \rfloor + 1]} \frac{n^{4r-2}}{(4r-2)!}(\frac{x}{n})^{4r-2}(-1 + \frac{(n-4r+2)^2}{(4r)^2}(\frac{x}{n})^2))^2$

vii. $\geq (\sum_r^{[1:\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \rfloor + 1]} \frac{n^{4r-2}}{(4r-2)!}(\frac{x}{n})^{4r-2}(-1 + \frac{1}{(4r)^2}(x)^2))^2$

viii. $\geq (\sum_r^{[1:\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \rfloor + 1]} \frac{n^{4r-2}}{(4r-2)!}(\frac{x}{n})^{4r-2}(-1 + \frac{1}{12}x^2))^2$

ix. $\geq (\sum_r^{[1:\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \rfloor + 1]} \frac{n^{4r-2}}{(4r-2)!}(\frac{x}{n})^{4r-2}(-1 + \frac{N^2}{12}))^2$

x. $\geq (\frac{n^2}{2}(\frac{x}{n})^2(-1 + \frac{N^2}{12}))^2$

xi. $\geq (\frac{1}{4}x^2(-1 + \frac{N^2}{12}))^2$

xii. $\geq (\frac{M^2}{4}(-1 + \frac{N^2}{12}))^2$

xiii. $= a^2$

5. **Yield the tuple $\langle a, b, p \rangle$.**

Procedure III:74

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c such that $a > 0$, and a procedure, $p(n, m, k)$, to show that $\|\exp_n(\frac{k}{K}\tau_m i) - 1\|^2 \geq a^2$ when an integer k and positive integers n, m such that $0 < |k| \leq \frac{K}{2}$, $n > b$, and $m > c$ are chosen.

Implementation

1. Execute procedure III:64 and let $\langle a_1, c, p_1 \rangle$ receive.
2. Verify that $(\frac{a_1}{2})^2 < 12$.
3. Execute procedure III:63 and let $\langle a_2, p_2 \rangle$ receive.
4. Verify that $a_2 > 0$.
5. Execute procedure III:73 on $\langle \frac{a_2}{K}, \frac{a_1}{2} \rangle$ and let $\langle a, b, p_3 \rangle$ receive.
6. **Verify that $a > 0$.**
7. Let $p(n, m, k)$ be the following procedure:

(a) Verify that $1 \leq |k| \leq \frac{K}{2}$.

(b) Hence verify that $\frac{1}{K} \leq \frac{|k|}{K} \leq \frac{1}{2}$.

(c) Execute procedure p_1 on $\langle m \rangle$.

(d) Execute procedure p_2 on $\langle m \rangle$.

(e) Hence verify that $0 < \frac{a_2}{K} \leq \frac{1}{K}\tau_m \leq \frac{|k|}{K}\tau_m \leq \frac{1}{2}\tau_m \leq \frac{a_1}{2}$.

(f) Hence execute procedure p_3 on $\langle \frac{k}{K}\tau_m, n \rangle$.

(g) Hence verify that $(\cos_n(\frac{k}{K}\tau_m) - 1)^2 \geq a^2$.

(h) Using procedure III:36, verify that $\|\exp_n(\frac{k}{K}\tau_m i) - 1\|^2$

i. $\geq \mathrm{re}(\exp_n(\frac{k}{K}\tau_m i) - 1)^2$

ii. $= (\cos_n(\frac{k}{K}\tau_m) - 1)^2$

iii. $\geq a^2$

8. **Yield the tuple** $\langle a, b, c, p \rangle$**.**

Procedure III:75

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c such that $a > 0$, and a procedure, $p(n, m, j, k)$, to show that $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 \geq a^2$ when positive integers n, j, k, m such that $-K < j \leq k < K$, $0 < k - j \leq \frac{K}{2}$, $n \geq b$, and $m \geq c$ are chosen.

Implementation

1. Execute procedure III:64 and let $\langle a_1, b_1, p_1 \rangle$ receive.
2. Execute procedure III:30 on $\langle a_1 \rangle$ and let $\langle a_2, b_2, p_2 \rangle$ receive.
3. Execute procedure III:74 on $\langle K \rangle$ and let $\langle a_3, b_3, c_3, p_3 \rangle$ receive.
4. Execute procedure III:31 on $\langle a_1 \rangle$ and let $\langle a_4, b_4, p_4 \rangle$ receive.
5. Let $a = \frac{1}{2}a_2a_3$.
6. Let $b = \max(\frac{2a_4{a_1}^2}{a_2a_3}, b_3, b_4, b_2)$.
7. Let $c = \max(b_1, c_3)$.
8. Let $p(n, m, j, k)$ be the following procedure:

(a) Verify that $-K < j < K$.

(b) Hence verify that $-1 < \frac{j}{K} < 1$.

(c) Hence verify that $\|\frac{j}{K}\|^2 < 1$.

(d) Execute procedure p_1 on $\langle m \rangle$.

(e) Hence verify that $\|\frac{j}{K}\tau_m i\|^2 = \|\frac{j}{K}\|^2\|\tau_m\|^2 \leq \|\tau_m\|^2 \leq {a_1}^2$.

(f) Execute procedure p_2 on $\langle \frac{j}{K}\tau_m i, n \rangle$.

(g) Hence verify that $\|\exp_n(\frac{j}{K}\tau_m i)\|^2 \geq {a_2}^2 > 0$.

(h) Execute procedure p_3 on $\langle n, m, k - j \rangle$.

(i) Hence verify that $\|\exp_n(\frac{k-j}{K}\tau_m i) - 1\|^2 \geq {a_3}^2 > 0$.

(j) Verify that $0 < \frac{k-j}{K} \leq \frac{1}{2}$.

(k) Hence verify that $\|\frac{k-j}{K}\tau_m i\|^2 \leq \|\frac{k-j}{K}\|^2\|\tau_m\|^2 \leq \|\tau_m\|^2 \leq {a_1}^2$.

(l) Verify that $n \geq b \geq \frac{2a_4{a_1}^2}{a_2a_3}$.

(m) Execute procedure p_4 on $\langle \frac{k-j}{K}\tau_m i, \frac{j}{K}\tau_m i, n \rangle$.

(n) Hence verify that $\|\exp_n(\frac{k-j}{K}\tau_m i)\exp_n(\frac{j}{K}\tau_m i) - \exp_n(\frac{k-j}{K}\tau_m i + \frac{j}{K}\tau_m i)\|^2 \leq \frac{{a_4}^2\|\frac{k-j}{K}\tau_m i\|^2\|\frac{j}{K}\tau_m i\|^2}{n^2} \leq \frac{{a_4}^2{a_1}^4}{n^2} \leq (\frac{a_2a_3}{2})^2$.

(o) Hence using procedure III:19, verify that $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2$

i. $= \|\exp_n(\frac{k-j}{K}\tau_m i + \frac{j}{K}\tau_m i) - \exp_n(\frac{k-j}{K}\tau_m i)\exp_n(\frac{j}{K}\tau_m i) + \exp_n(\frac{k-j}{K}\tau_m i)\exp_n(\frac{j}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2$

ii. $= \|\exp_n(\frac{j}{K}\tau_m i)(\exp_n(\frac{k-j}{K}\tau_m i) - 1) - (\exp_n(\frac{k-j}{K}\tau_m i + \frac{j}{K}\tau_m i) - \exp_n(\frac{k-j}{K}\tau_m i)\exp_n(\frac{j}{K}\tau_m i))\|^2$

iii. $\geq (a_2a_3 - \frac{a_2a_3}{2})^2$

iv. $\geq a^2$.

9. **Yield the tuple** $\langle a, b, c, p \rangle$**.**

Procedure III:76

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c such that $a > 0$, and a procedure, $p(n, m, j, k)$, to show that $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 \geq a^2$ when positive integers n, j, k, m such that $0 \leq j \leq k < K$, $\frac{K}{2} \leq k - j < K$, $n \geq b$, and $\frac{m}{n} \geq c$ are chosen.

Implementation

1. Execute procedure III:75 on $\langle K \rangle$ and let $\langle a_1, b_1, c_1, p_1 \rangle$ receive.
2. Execute procedure III:64 and let $\langle a_2, b_2, p_2 \rangle$ receive.

3. Execute procedure III:71 on $\langle a_2, 4\rangle$ and let $\langle a_3, b_3, c_3, d_3, p_3\rangle$ receive.

4. Let $a = \frac{1}{2}a_1$.

5. Let $b = \max(\frac{4b_3}{a_1}, b_1, c_3)$.

6. Let $c = \max(\frac{4a_3}{a_1}, \frac{c_1}{b}, \frac{b_2}{b}, \frac{d_3}{b})$.

7. Let $p(n, m, j, k)$ be the following procedure:

(a) Verify that $-\frac{K}{2} \leq k - K < j < \frac{K}{2}$.

(b) Also verify that $0 < j - (k - K) \leq \frac{K}{2}$.

(c) Verify that $m \geq cn \geq \frac{c_1}{b}b = c_1$.

(d) Hence execute procedure p_1 on $\langle n, m, k - K, j\rangle$.

(e) Hence verify that $\|\exp_n(\frac{j}{K}\tau_m i) - \exp_n(\frac{k-K}{K}\tau_m i)\|^2 \geq {a_1}^2$.

(f) Verify that $m \geq cn \geq \frac{b_2}{b}b = b_2$.

(g) Execute procedure p_2 on $\langle m\rangle$.

(h) Hence verify that $\tau_m \leq a_2$.

(i) Hence verify that $\|\frac{k}{K}\tau_m i\|^2 = \|\frac{k}{K}\|^2\|\tau_m\|^2 \leq \|\tau_m\|^2 \leq {a_2}^2$.

(j) Also verify that $m \geq cn \geq \frac{d_3}{b}b = d_3$.

(k) Now execute procedure p_3 on $\langle \frac{k}{K}\tau_m i, n, m, -4\rangle$.

(l) Hence verify that $\|i^{-4}\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{k}{K}\tau_m i - \frac{4}{4}\tau_m i)\|^2 \leq (\frac{a_3 n}{m} + \frac{b_3}{n})^2 \leq (\frac{a_1}{2})^2$.

(m) Now verify that $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2$

i. $= \|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{k}{K}\tau_m i - \tau_m i) + \exp_n(\frac{k-K}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2$

ii. $\geq \frac{1}{2}\|\exp_n(\frac{k-K}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 - \|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{k}{K}\tau_m i - \tau_m i)\|^2$

iii. $\geq \frac{1}{2}{a_1}^2 - (\frac{a_1}{2})^2$

iv. $\geq a^2$.

8. **Yield the tuple** $\langle a, b, c, p\rangle$**.**

Procedure III:77

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c such that $a > 0$, and a procedure, $p(n, m, j, k)$, to show that $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 \geq a^2$ when positive integers n, j, k, m such that $0 \leq j \leq k < K$, $0 < k - j < K$, $n \geq b$, and $\frac{m}{n} \geq c$ are chosen.

Implementation

1. Execute procedure III:75 on $\langle K\rangle$ and let $\langle a_1, b_1, c_1, p_1\rangle$ receive.

2. Execute procedure III:76 on $\langle K\rangle$ and let $\langle a_2, b_2, c_2, p_2\rangle$ receive.

3. Let $a = \min(a_1, a_2)$.

4. **Verify that** $a > 0$**.**

5. Let $b = \max(b_1, b_2)$.

6. Let $c = \max(\frac{c_1}{b}, c_2)$.

7. Let $p(n, m, j, k)$ be the following procedure:

(a) If $k - j \leq \frac{K}{2}$, then do the following:

i. Verify that $m \geq cn \geq \frac{c_1}{b}b = c_1$.

ii. Execute procedure p_1 on $\langle n, m, j, k\rangle$.

iii. **Hence verify that** $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 \geq a_1 \geq a$**.**

(b) Otherwise if $k - j > \frac{K}{2}$, then do the following:

i. Execute procedure p_2 on $\langle n, m, j, k\rangle$.

ii. **Hence verify that** $\|\exp_n(\frac{k}{K}\tau_m i) - \exp_n(\frac{j}{K}\tau_m i)\|^2 \geq a_2 \geq a$**.**

8. **Yield the tuple** $\langle a, b, c, p\rangle$**.**

Declaration III:19

The phrase "complex polynomial" will be used to indicate that the declarations and procedures pertaining to polynomials are being used but with the provison that all uses of rational numbers therein are substituted with uses of complex numbers.

Procedure III:78

Objective

Choose a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(n, m)$, to construct a list of complex numbers z and a list of complex polynomials q such that,

1. $z_k = \exp_n(\frac{k}{K}\tau_m i)$ for $k \in [0 : K]$
2. $q_K = \lambda^K - 1$
3. $q_{K-1} = \sum_r^{[0:K]} \lambda^r$
4. $q_{k+1} = (\lambda - z_k)q_k + \Lambda(q_{k+1}, z_k)$ for $k \in [0 : K]$
5. $(q_k)_{\deg(q_k)} = 1$ for $k \in [0 : K + 1]$
6. $\Lambda(q_k, z_j) \equiv 0$ (err $\frac{an}{m} + \frac{b}{n}$) for $j \in [0 : k]$, for $k \in [0 : K + 1]$

when two positive integers n, m such that $n > c$ and $\frac{m}{n} > d$ are chosen.

Implementation

1. Execute procedure III:72 on $\langle K\rangle$ and let $\langle a_1, b_1, c_1, d_1, p_1\rangle$ receive.
2. Execute procedure III:77 on $\langle K\rangle$ and let $\langle a_2, b_2, c_2, p_2\rangle$ receive.
3. Let $a = \max(1, \frac{2}{a_2})^K a_1$.
4. Let $b = \max(1, \frac{2}{a_2})^K b_1$.
5. Let $c = \max(c_1, b_2)$.
6. Let $d = \max(d_1, c_2)$.
7. Let $p(n, m)$ be the following procedure:
   (a) **Let** $q_K = \lambda^K - 1$**.**
   (b) For $k \in [K : 0]$, do the following:
      i. **Let** $z_k = \exp_n(\frac{k}{K}\tau_m i)$**.**
      ii. Execute procedure p_1 on $\langle n, m, k\rangle$.
      iii. **Hence verify that** $\|\Lambda(q_K, z_k)\|^2 \leq (\frac{a_1 n}{m} + \frac{b_1}{n})^2$**.**
   (c) For $k \in [K : 0]$, do the following:
      i. Let $q_k = q_{k+1} \operatorname{div} (\lambda - z_k)$.
      ii. Let $r_k = q_{k+1} \bmod (\lambda - z_k)$.
      iii. Verify that $\deg(r_k) < \deg(\lambda - z_k) = 1$.
      iv. Hence verify that $\deg(r_k) = 0$.
      v. Verify that $q_{k+1} = (\lambda - z_k)q_k + r_k$.
      vi. **Hence verify that** $1 = (q_{k+1})_{\deg(q_{k+1})} = ((\lambda - z_k)q_k + r_k)_{\deg(q_{k+1})} = (q_k)_{\deg(q_k)}$**.**
      vii. Also verify that $\Lambda(q_{k+1}, z_k) = \Lambda(\lambda - z_k, z_k)\Lambda(q_k, z_k) + \Lambda(r_k, z_k) = (z_k - z_k)\Lambda(q_k, z_k) + r_k = r_k$.
      viii. **Hence verify that** $q_{k+1} = (\lambda - z_k)q_k + \Lambda(q_{k+1}, z_k)$**.**
      ix. Execute the auxilliary procedure on $\langle k, q_{k+1}, z\rangle$.
      x. Now using (cvii), verify that $(\lambda - 1)\sum_r^{[0:K]} \lambda^r$
         A. $= q_K$
         B. $= (\lambda - z_{K-1})q_{K-1} + \Lambda(q_K, z_{K-1})$
         C. $= (\lambda - 1)q_{K-1} + \Lambda(\lambda^K - 1, 1)$
         D. $= (\lambda - 1)q_{K-1}$.
      xi. **Hence verify that** $\sum_r^{[0:K]} \lambda^r = q_{K-1}$**.**
   (d) **Yield the tuple** $\langle z, q\rangle$**.**
8. **Yield the tuple** $\langle a, b, c, d, p\rangle$**.**

Auxilliary procedure

Objective Choose a non-negative integer k, a complex polynomial q_{k+1}, and a list of complex numbers z such that $z_j = \exp_n(\frac{j}{K}\tau_m i)$ and $\Lambda(q_{k+1}, z_j) \equiv 0$ (err $(\frac{2}{a_2})^{K-(k+1)}(\frac{a_1 n}{m} + \frac{b_1}{n})$) for $j \in [k+1 : 0]$. Let $q_k = q_{k+1} \operatorname{div} (\lambda - z_k)$. The objective of the following instructions is to show that $\Lambda(q_k, z_j) \equiv 0$ (err $(\frac{2}{a_2})^{K-k}(\frac{a_1 n}{m} + \frac{b_1}{n})$) (err $\frac{an}{m} + \frac{b}{n}$) for $j \in [k : 0]$.

Implementation

1. For $j \in [k : 0]$, do the following:
   (a) Verify that $\Lambda(q_{k+1}, z_j) = \Lambda(\lambda - z_k, z_j)\Lambda(q_k, z_j) + \Lambda(q_{k+1}, z_k)$.
   (b) Hence verify that $\Lambda(q_{k+1}, z_j) - \Lambda(q_{k+1}, z_k) = (z_j - z_k)\Lambda(q_k, z_j)$.
   (c) Execute procedure p_2 on $\langle n, m, \min(j, k), \max(j, k)\rangle$.

(d) Hence verify that $\|z_j - z_k\|^2 \geq {a_2}^2$.

(e) Hence verify that ${a_2}^2\|\Lambda(q_k, z_j)\|^2$

i. $\leq \|z_j - z_k\|^2\|\Lambda(q_k, z_j)\|^2$

ii. $= \|(z_j - z_k)\Lambda(q_k, z_j)\|^2$

iii. $= \|\Lambda(q_{k+1}, z_j) - \Lambda(q_{k+1}, z_k)\|^2$

iv. $\leq ((\frac{2}{a_2})^{K-k-1}(\frac{a_1 n}{m}+\frac{b_1}{n})+(\frac{2}{a_2})^{K-k-1}(\frac{a_1 n}{m}+\frac{b_1}{n}))^2$

v. $= (2(\frac{2}{a_2})^{K-k-1}(\frac{a_1 n}{m} + \frac{b_1}{n}))^2$

vi. $= {a_2}^2((\frac{2}{a_2})^{K-k}(\frac{a_1 n}{m} + \frac{b_1}{n}))^2$.

(f) **Hence verify that** $\|\Lambda(q_k, z_j)\|^2 \leq ((\frac{2}{a_2})^{K-k}(\frac{a_1 n}{m} + \frac{b_1}{n}))^2 \leq (\frac{an}{m} + \frac{b}{n})^2$**.**

Procedure III:79

Objective

Choose a rational number X and a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(x, n, m)$, to show that $\sum_r^{[0:K]} x^r \equiv \prod_r^{[1:K]}(x - \exp_n(\frac{r}{K}\tau_m i))$ (err $\frac{an}{m} + \frac{b}{n}$) when a complex number x and positive integers n, m such that $n > c$, $\frac{m}{n} > d$, and $\|x\|^2 \leq X$ are chosen.

Implementation

1. Execute procedure III:78 on $\langle K\rangle$ and let $\langle a_1, b_1, c_1, d_1, p_1\rangle$ receive.
2. Execute procedure III:64 and let $\langle a_2, b_2, p_2\rangle$ receive.
3. Execute procedure III:29 on $\langle a_2\rangle$ and let $\langle a_3, b_3, p_3\rangle$ receive.
4. Let $l = \sum_k^{[0:K-1]} \prod_j^{[k+1:K-1]}(X + a_3)$.
5. Let $a = a_1 l$.
6. Let $b = b_1 l$.
7. Let $c = \max(c_1, b_3)$.
8. Let $d = \max(d_1, b_2)$.
9. Let $p(x, n, m)$ be the following procedure:

(a) Execute procedure p_2 on $\langle m\rangle$.

(b) Hence verify that $\tau_m \leq a_2$.

(c) Execute procedure p_1 on $\langle n, m\rangle$ and let $\langle z, t\rangle$ receive.

(d) For $j \in [1 : K]$, do the following:

i. Verify that $\|\frac{j}{K}\tau_m i\|^2 = \|\frac{j}{K}\|^2\|\tau_m\|^2 \leq \|\tau_m\|^2 \leq a_2$.

ii. Execute procedure p_3 on $\langle \frac{j}{K}\tau_m i, n\rangle$.

iii. Hence verify that $\|z_j\|^2 = \|\exp_n(\frac{j}{K}\tau_m i)\|^2 \leq a_3$.

(e) Hence verify that $\|\sum_r^{[0:K]} x^r - \prod_r^{[1:K]}(x - z_r)\|^2$

i. $= \|\Lambda(\sum_r^{[0:K]} \lambda^r, x) - \prod_r^{[1:K]}(x - z_r)\|^2$

ii. $= \|\Lambda(t_{K-1}, x) - \prod_r^{[1:K]}(x - z_r)\|^2$

iii. $= \|\Lambda(\prod_j^{[0:K-1]}(\lambda - z'_j) + \sum_k^{[0:K-1]} \Lambda(t_{k+1}, z'_k)\prod_j^{[k+1:K-1]}(\lambda - z'_j), x) - \prod_r^{[1:K]}(x - z_r)\|^2$

iv. $= \|\prod_j^{[0:K-1]}(x - z'_j) + \sum_k^{[0:K-1]} \Lambda(t_{k+1}, z'_k)\prod_j^{[k+1:K-1]}(x - z'_j) - \prod_r^{[1:K]}(x - z_r)\|^2$

v. $= \|\sum_k^{[0:K-1]} \Lambda(t_{k+1}, z'_k)\prod_j^{[k+1:K-1]}(x - z'_j)\|^2$

vi. $\leq (\sum_k^{[0:K-1]}(\frac{a_1 n}{m} + \frac{b_1}{n})\prod_j^{[k+1:K-1]}(X + a_3))^2$

vii. $= ((\frac{a_1 n}{m} + \frac{b_1}{n})\sum_k^{[0:K-1]}\prod_j^{[k+1:K-1]}(X + a_3))^2$

viii. $= (\frac{an}{m} + \frac{b}{n})^2$.

10. **Yield the tuple** $\langle a, b, c, d, p\rangle$**.**

Procedure III:80

Objective

Choose a rational number X and a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(x, n, m)$, to show that $x^K - 1 \equiv \prod_r^{[0:K]}(x - \exp_n(\frac{r}{K}\tau_m i))$ (err $\frac{an}{m} + \frac{b}{n}$) when a complex number x and positive integers n, m such that $n > c$, $\frac{m}{n} > d$, and $\|x\|^2 \leq X$ are chosen.

Implementation

1. Execute procedure III:79 on $\langle X, K\rangle$ and let $\langle a_1, b_1, c, d, p_1\rangle$ receive.
2. Let $a = (X+1)a_1$.
3. Let $b = (X+1)b_1$.
4. Let $p(x, n, m)$ be the following procedure:
   (a) Execute procedure p_1 on $\langle x, n, m\rangle$.
   (b) Hence verify that $\|\sum_r^{[0:K]} x^r - \prod_r^{[1:K]}(x - \exp_n(\frac{r}{K}\tau_m i))\|^2 \le (\frac{a_1 n}{m} + \frac{b_1}{n})^2$.
   (c) Hence verify that $\|x^K - 1 - \prod_r^{[0:K]}(x - \exp_n(\frac{r}{K}\tau_m i))\|^2$
      i. $= \|(x-1)\sum_r^{[0:K]} x^r - (x-1)\prod_r^{[1:K]}(x - \exp_n(\frac{r}{K}\tau_m i))\|^2$
      ii. $= \|x-1\|^2 \|\sum_r^{[0:K]} x^r - \prod_r^{[1:K]}(x - \exp_n(\frac{r}{K}\tau_m i))\|^2$
      iii. $\le (X+1)^2(\frac{a_1 n}{m} + \frac{b_1}{n})^2$
      iv. $= (\frac{an}{m} + \frac{b}{n})^2$.
5. **Yield the tuple $\langle a, b, c, d, p\rangle$.**

Procedure III:81

Objective

Choose a rational number X and a positive integer K. The objective of the following instructions is to construct rational numbers a, b, c, d, and a procedure, $p(x, n, m)$, to show that $\exp_K(x) - 1 \equiv x\prod_r^{[1:K]}(1 - \frac{x}{K(\exp_n(\frac{r}{K}\tau_m i)-1)})$ (err $\frac{an}{m} + \frac{b}{n}$) when a complex number x and positive integers n, m such that $n > c$, $\frac{m}{n} > d$, and $\|x\|^2 \le X$ are chosen.

Implementation

1. Execute procedure III:80 on $\langle 1 + \frac{X}{K}, K\rangle$ and let $\langle a_1, b_1, c_1, d_1, p_1\rangle$ receive.
2. Execute procedure III:79 on $\langle 1, K\rangle$ and let $\langle a_2, b_2, c_2, d_2, p_2\rangle$ receive.
3. Execute procedure III:77 on $\langle K\rangle$ and let $\langle a_3, b_3, c_3, p_3\rangle$ receive.
4. Let $l = \frac{X}{K}(1 + \frac{X}{Ka_3})^{K-1}$.
5. Let $a = a_1 + la_2$.
6. Let $b = b_1 + lb_2$.
7. Let $c = \max(c_1, c_2, b_3)$.
8. Let $d = \max(d_1, d_2, c_3)$.
9. Let $p(x, n, m)$ be the following procedure:
   (a) Verify that $\|1 + \frac{x}{K}\|^2 \le (1 + \frac{X}{K})^2$.
   (b) Hence execute procedure p_1 on $\langle 1+\frac{x}{K}, n, m\rangle$.
   (c) Hence verify that $\|(1+\frac{x}{K})^K - 1 - \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i))\|^2 \le (\frac{a_1 n}{m} + \frac{b_1}{n})^2$.
   (d) Execute procedure p_2 on $\langle 1, n, m\rangle$.
   (e) Hence verify that $\|K - \prod_r^{[1:K]}(1 - \exp_n(\frac{r}{K}\tau_m i))\|^2 = \sum_r^{[0:K]} 1^r - \prod_r^{[1:K]}(1 - \exp_n(\frac{r}{K}\tau_m i))\|^2 \le (\frac{a_2 n}{m} + \frac{b_2}{n})^2$.
   (f) For $j \in [1:K]$, do the following:
      i. Execute procedure p_3 on $\langle n, m, 0, j\rangle$.
      ii. Hence verify that $\|\exp_n(\frac{j}{K}\tau_m i) - 1\|^2 \ge {a_3}^2$.
      iii. Let $z_j = K(\exp_n(\frac{j}{K}\tau_m i) - 1)$.
   (g) Hence verify that $\|\exp_K(x) - 1 - x\prod_r^{[1:K]}(1 - \frac{x}{z_r})\|^2$
      i. $= \|\exp_K(x) - 1 - \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i)) + \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i)) - x\prod_r^{[1:K]}(1 - \frac{x}{z_r})\|^2$
      ii. $= \|\exp_K(x) - 1 - \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i)) + \frac{x}{K}\prod_r^{[1:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i)) - x\prod_r^{[1:K]}(1 - \frac{x}{z_r})\|^2$
      iii. $= \|\exp_K(x) - 1 - \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i)) + \frac{x}{K}\prod_r^{[1:K]}(1 - \exp_n(\frac{r}{K}\tau_m i))\prod_r^{[1:K]}(1 - \frac{x}{z_r}) - x\prod_r^{[1:K]}(1 - \frac{x}{z_r})\|^2$
      iv. $= \|(\exp_K(x) - 1 - \prod_r^{[0:K]}(1 + \frac{x}{K} - \exp_n(\frac{r}{K}\tau_m i))) + \frac{x}{K}\prod_r^{[1:K]}(1 - \frac{x}{z_r})(\prod_r^{[1:K]}(1 - \exp_n(\frac{r}{K}\tau_m i)) - K)\|^2$
      v. $\le ((\frac{a_1 n}{m} + \frac{b_1}{n}) + \frac{X}{K}(\prod_r^{[1:K]}(1 + \frac{X}{Ka_3}))(\frac{a_2 n}{m} + \frac{b_2}{n}))^2$
      vi. $= ((\frac{a_1 n}{m} + \frac{b_1}{n}) + \frac{X}{K}(1 + \frac{X}{Ka_3})^{K-1}(\frac{a_2 n}{m} + \frac{b_2}{n}))^2$
      vii. $= (\frac{an}{m} + \frac{b}{n})^2$.
10. **Yield the tuple $\langle a, b, c, d, p\rangle$.**

Part IV

Differential Arithmetic

Declaration IV:0

The notation $\Delta_{x=y}^{z} f(x)$, where x, z are complex numbers such that $z \neq 0$ and $f[x]$ is a function of x, will be used as a shorthand for $\frac{f(y+z)-f(y)}{z}$.

Procedure IV:0

Objective

Choose two functions $f[x], g[x]$ and two complex numbers y, z such that $z \neq 0$. The objective of the following instructions is to show that $\Delta_{x=y}^{z}(f(x) + g(x)) = \Delta_{x=y}^{z} f(x) + \Delta_{x=y}^{z} g(x)$.

Implementation

1. Verify that $\Delta_{x=y}^{z}(f(x) + g(x))$
   (a) $= \frac{(f(y+z)+g(y+z))-(f(y)+g(y))}{z}$
   (b) $= \frac{f(y+z)-f(y)}{z} + \frac{g(y+z)-g(y)}{z}$
   (c) $= \Delta_{x=y}^{z} f(x) + \Delta_{x=y}^{z} g(x)$.

Procedure IV:1

Objective

Choose a functions $f[x]$ and complex numbers a, y, z such that $z \neq 0$. The objective of the following instructions is to show that $\Delta_{x=y}^{z}(af(x)) = a\,\Delta_{x=y}^{z} f(x)$.

Implementation

1. Verify that $\Delta_{x=y}^{z}(af(x))$
   (a) $= \frac{af(y+z)-af(y)}{z}$
   (b) $= a\frac{f(y+z)-f(y)}{z}$
   (c) $= a\,\Delta_{x=y}^{z} f(x)$.

Procedure IV:2

Objective

Choose the following:

1. A procedure $q_0(x, n)$ to show that $\|p_n'(x)\|^2 \leq {a_0}^2$ when a complex number x and a positive integer n such that $P(x)$ and $n > b_0$ are chosen.
2. A procedure $q_1(x, n, \delta)$ to show that $\|\frac{p_n(x+\delta)-p_n(x)}{\delta} - p_n'(x)\|^2 \leq (\frac{a_1}{n} + b_1\{\delta\})^2$

Implementation

Procedure IV:3

Objective

Choose the following:

1. A procedure $q_0(x, n)$ to show that $\|p_n'(x)\|^2 \leq {a_0}^2$ when a complex number x and a positive integer n such that $P(x)$, and $n > b_0$ are chosen
2. A procedure $q_1(x, n, \delta)$ to show that $\Delta_{y=x}^{+\delta} p_n(y) \equiv p_n'(x)$ (err $\frac{a_1}{n} + b_1\{\delta\}$) when two complex numbers x, δ and a positive integer n such that $P(x)$, $n > b_0$, and $\|\delta\|^2 < {c_1}^2$ are chosen
3. A procedure $q_2(x, n)$ to show that $\|t_n'(x)\|^2 \leq {a_2}^2$ when a complex number x and a positive integer n such that $R(x)$, and $n > b_2$ are chosen
4. A procedure $q_3(x, n, \delta)$ to show that $\Delta_{y=x}^{+\delta} t_n(y) \equiv t_n'(x)$ (err $\frac{a_3}{n} + b_3\{\delta\}$) when two complex numbers x, δ and a positive integer n such that $R(x)$, $n > b_2$, and $\|\delta\|^2 < {c_3}^2$ are chosen
5. A procedure $q_4(x, n)$ to show that $P(t_n(x))$ when a complex number x and a positive integer n such that $R(x)$ and $n > b_2$ are chosen

The objective of the following instructions is to construct the following:

1. Rational numbers a_5, b_5, a_6, b_6, c_6.
2. A procedure $q_5(x, n)$ to show that $\|p'_n(t_n(x))t'_n(x)\|^2 \leq a_5{}^2$ when a complex number x such that $R(x)$, and $n > b_5$ are chosen.
3. A procedure $q_6(x, n, \delta)$ to show that $\Delta_{y=x}^{x+\delta} p_n(t_n(y)) \equiv p'_n(t_n(x))t'_n(x)$ (err $\frac{a_6}{n} + b_6\{\delta\}$) when two complex numbers x, dx such that $R(x)$, $n > b_5$, and $\|\delta\|^2 < c_6{}^2$ are chosen.

Implementation

1. Let $a_5 = a_0 a_2$.
2. Let $b_5 = \max(b_0, b_2)$.
3. Let $a_6 = a_1 a_3 + a_1 a_2 + a_0 a_3$.
4. Let $b_6 = a_1 b_3 + b_1 a_3 + 2 b_1 b_3 c_6 + b_1 a_2 + a_0 b_3$.
5. Let $c_6 = \min(c_3, \frac{c_1}{a_3 + 2 b_3 c_3 + a_2})$.
6. Let $q_5(x, n, \delta)$ be the following procedure:
   (a) Execute procedure q_3 on $\langle x, n, \delta \rangle$.
   (b) Hence verify that $\|\frac{t_n(x+\delta) - t_n(x)}{\delta} - t'_n(x)\|^2 \leq (\frac{a_3}{n} + b_3\{\delta\})^2$.
   (c) Execute procedure q_4 on $\langle x, n \rangle$.
   (d) Hence verify that $\|t'_n(x)\|^2 \leq a_2{}^2$.
   (e) Verify that $\{\delta\}^2 \leq 2\|\delta\|^2 \leq 4c_6{}^2$.
   (f) Hence verify that $\{\delta\} \leq 2c_6 \leq 2c_3$.
   (g) Verify that $\|t_n(x + \delta) - t_n(x)\|^2$
      i. $= \|\frac{t_n(x+\delta) - t_n(x)}{\delta}\|^2 \|\delta\|^2$
      ii. $= \|\frac{t_n(x+\delta) - t_n(x)}{\delta} - t'_n(x) + t'_n(x)\|^2 \|\delta\|^2$
      iii. $\leq (\frac{a_3}{n} + b_3\{\delta\} + a_2)^2 \|\delta\|^2$
      iv. $\leq (a_3 + 2 b_3 c_3 + a_2)^2 c_6{}^2$
      v. $\leq c_1{}^2$.
   (h) Execute procedure q_4 on $\langle x, n \rangle$.
   (i) Hence verify that $P(t_n(x))$.
   (j) Execute procedure q_1 on $\langle t_n(x), n, t_n(x+\delta) - t_n(x) \rangle$.
   (k) Hence verify that $\|\frac{p_n(t_n(x) + (t_n(x+\delta) - t_n(x))) - p_n(t_n(x))}{t_n(x+\delta) - t_n(x)} - p'_n(t_n(x))\|^2 \leq (\frac{a_1}{n} + b_1\{\delta\})^2$.
   (l) Execute procedure q_0 on $\langle t_n(x), n \rangle$.
   (m) Hence verify that $\|p'_n(t_n(x))\|^2 \leq a_0{}^2$.
   (n) Verify that $\|\frac{p(t(x+\delta)) - p(t(x))}{\delta} - p'(t(x))t'(x)\|^2$
      i. $= \|\frac{p(t(x) + (t(x+\delta) - t(x))) - p(t(x))}{t(x+\delta) - t(x)} \cdot \frac{t(x+\delta) - t(x)}{\delta} - p'(t(x))t'(x)\|^2$
      ii. $= \|(\frac{p(t(x) + (t(x+\delta) - t(x))) - p(t(x))}{t(x+\delta) - t(x)} - p'(t(x))) \cdot \frac{t(x+\delta) - t(x)}{\delta} + p'(t(x))(\frac{t(x+\delta) - t(x)}{\delta} - t'(x))\|^2$
      iii. $= \|(\frac{p(t(x) + (t(x+\delta) - t(x))) - p(t(x))}{t(x+\delta) - t(x)} - p'(t(x))) \cdot (\frac{t(x+\delta) - t(x)}{\delta} - t'(x)) + (\frac{p(t(x) + (t(x+\delta) - t(x))) - p(t(x))}{t(x+\delta) - t(x)} - p'(t(x))) \cdot t'(x) + p'(t(x))(\frac{t(x+\delta) - t(x)}{\delta} - t'(x))\|^2$
      iv. $\leq ((\frac{a_1}{n} + b_1\{\delta\})(\frac{a_3}{n} + b_3\{\delta\}) + (\frac{a_1}{n} + b_1\{\delta\})a_2 + a_0(\frac{a_3}{n} + b_3\{\delta\}))^2$
      v. $\leq (\frac{a_6}{n} + b_6\{\delta\})^2$.
7. Let $q_6(x, n)$ be the following procedure:
   (a) Execute procedure q_4 on $\langle x, n \rangle$.
   (b) Hence verify that $P(t_n(x))$.
   (c) Execute procedure q_0 on $\langle t_n(x), n \rangle$.
   (d) Hence verify that $\|p'_n(t_n(x))\|^2 \leq a_0{}^2$.
   (e) Execute procedure q_2 on $\langle x, n \rangle$.
   (f) Hence verify that $\|t'_n(x)\|^2 \leq a_2{}^2$.
   (g) Hence verify that $\|p'_n(t_n(x))t'_n(x)\|^2 \leq (a_0 a_2)^2 = a_5{}^2$.
8. **Yield the tuple $\langle a_5, b_5, a_6, b_6, c_6, q_5, q_6 \rangle$.**

Procedure IV:4

Objective

Choose the following:

1. A procedure $q_0(x, n)$ to show that $\|p_n(x)\|^2 \leq a_0{}^2$ when a complex number x and a positive integer n such that $P(x)$ and $n > b_0$ are chosen.
2. A procedure $q_1(x, n)$ to show that $\|p'_n(x)\|^2 \leq a_1{}^2$ when a complex number x and a positive integer n such that $P(x)$ and $n > b_0$ are chosen.

3. A procedure $q_2(x, n, \delta)$ to show that $\Delta_{y=x}^{+\delta} p_n(y) \equiv p'_n(x)$ (err $\frac{a_2}{n} + b_2\{\delta\}$) when two complex numbers x, δ and a positive integer n such that $P(x)$, $n > b_0$, and $\|\delta\|^2 < {c_2}^2$ are chosen.

4. A procedure $q_3(x, n)$ to show that $\|t_n(x)\|^2 \leq {a_3}^2$ when a complex number x and a positive integer n such that $R(x)$ and $n > b_3$ are chosen.

5. A procedure $q_4(x, n)$ to show that $\|t'_n(x)\|^2 \leq {a_4}^2$ when a complex number x and a positive integer n such that $R(x)$ and $n > b_3$ are chosen.

6. A procedure $q_5(x, n, \delta)$ to show that $\Delta_{y=x}^{+\delta} t_n(y) \equiv t'_n(x)$ (err $\frac{a_5}{n} + b_5\{\delta\}$) when two complex numbers x, δ and a positive integer n such that $R(x)$, $n > b_3$, and $\|\delta\|^2 < {c_5}^2$ are chosen.

The objective of the following instructions is to construct the following:

1. Rational numbers a_6, b_6, a_7, b_7, c_7.

2. A procedure $q_6(x, n)$ to show that $\|p_n(x)t'_n(x) + p'_n(x)t_n(x)\|^2 \leq {a_6}^2$ when a complex number x and a positive integer n such that $P(x)$, $R(x)$, and $n > b_6$ are chosen.

3. A procedure $q_7(x, n, \delta)$ to show that $\Delta_{y=x}^{+\delta}(p_n(y)t_n(y)) \equiv p_n(x)t'_n(x) + p'_n(x)t_n(x)$ (err $\frac{a_7}{n} + b_7\{\delta\}$) when two complex numbers x, δ such that $P(x)$, $R(x)$, $n > b_6$, and $\|\delta\|^2 < {c_7}^2$ are chosen.

Implementation

1. Let $a_6 = a_0a_4 + a_1a_3$.

2. Let $b_6 = \max(b_0, b_3)$.

3. Let $a_7 = a_0a_5 + a_6a_2$.

4. Let $b_7 = a_2a_5 + a_1a_5 + a_4a_2 + a_1a_4 + a_0b_5 + a_6b_2 + 2c_7(a_2b_5 + b_2a_5 + a_1b_5 + a_4b_2) + 4b_2b_5{c_7}^2$.

5. Let $c_7 = \min(c_2, c_5)$.

6. Let $q_7(x, n, \delta)$ be the following procedure:

(a) Verify that $\{\delta\}^2 \leq 2\|\delta\|^2 \leq 4{c_7}^2$.

(b) Hence verify that $\{\delta\} \leq 2c_7$.

(c) Execute procedure q_2 on $\langle x, n, \delta \rangle$.

(d) Hence verify that $\|\frac{p_n(x+\delta)-p_n(x)}{\delta} - p'_n(x)\|^2 \leq (\frac{a_2}{n} + b_2\{\delta\})^2$.

(e) Execute procedure q_1 on $\langle x, n \rangle$.

(f) Hence verify that $\|p'_n(x)\|^2 \leq {a_1}^2$.

(g) Execute procedure q_5 on $\langle x, n, \delta \rangle$.

(h) Hence verify that $\|\frac{t_n(x+\delta)-t_n(x)}{\delta} - t'_n(x)\|^2 \leq (\frac{a_5}{n} + b_5\{\delta\})^2$.

(i) Execute procedure q_4 on $\langle x, n \rangle$.

(j) Hence verify that $\|t'_n(x)\|^2 \leq {a_4}^2$.

(k) Execute procedure q_0 on $\langle x, n \rangle$.

(l) Hence verify that $\|p_n(x)\|^2 \leq {a_0}^2$.

(m) Execute procedure q_3 on $\langle x, n \rangle$.

(n) Hence verify that $\|t_n(x)\|^2 \leq {a_6}^2$.

(o) Hence verify that $\|\frac{p_n(x+\delta)t_n(x+\delta)-p_n(x)t_n(x)}{\delta} - p_n(x)t'_n(x) - p'_n(x)t_n(x)\|^2$

i. $= \|p_n(x+\delta) \cdot \frac{t_n(x+\delta)-t_n(x)}{\delta} + t_n(x) \cdot \frac{p_n(x+\delta)-p_n(x)}{\delta} - p_n(x)t'_n(x) - p'_n(x)t_n(x)\|^2$

ii. $= \|\delta \cdot \frac{p_n(x+\delta)-p_n(x)}{\delta} \cdot \frac{t_n(x+\delta)-t_n(x)}{\delta} + p_n(x) \cdot \frac{t_n(x+\delta)-t_n(x)}{\delta} - p_n(x)t'_n(x) + t_n(x)(\frac{p_n(x+\delta)-p_n(x)}{\delta} - p'_n(x))\|^2$

iii. $= \|\delta(\frac{p_n(x+\delta)-p_n(x)}{\delta} - p'_n(x))(\frac{t_n(x+\delta)-t_n(x)}{\delta} - t'_n(x)) + \delta p'_n(x)(\frac{t_n(x+\delta)-t_n(x)}{\delta} - t'_n(x)) + \delta t'_n(x)(\frac{p_n(x+\delta)-p_n(x)}{\delta} - p'_n(x)) - \delta p'_n(x)t'_n(x) + p_n(x)(\frac{t_n(x+\delta)-t_n(x)}{\delta} - t'_n(x)) + t_n(x)(\frac{p_n(x+\delta)-p_n(x)}{\delta} - p'_n(x))\|^2$

iv. $\leq (\{\delta\}(\frac{a_2}{n} + b_2\{\delta\})(\frac{a_5}{n} + b_5\{\delta\}) + \{\delta\}a_1(\frac{a_5}{n} + b_5\{\delta\}) + \{\delta\}a_4(\frac{a_2}{n} + b_2\{\delta\}) + \{\delta\}a_1a_4 + a_0(\frac{a_5}{n} + b_5\{\delta\}) + a_6(\frac{a_2}{n} + b_2\{\delta\}))^2$

v. $\leq (\frac{a_7}{n} + b_7\{\delta\})^2$.

7. Let $q_6(x, n)$ be the following procedure:

(a) Execute procedure q_1 on $\langle x, n \rangle$.

(b) Hence verify that $\|p'_n(x)\|^2 \leq {a_1}^2$.

(c) Execute procedure q_4 on $\langle x, n \rangle$.

(d) Hence verify that $\|t'_n(x)\|^2 \leq {a_4}^2$.

(e) Execute procedure q_0 on $\langle x, n \rangle$.

(f) Hence verify that $\|p_n(x)\|^2 \leq {a_0}^2$.

(g) Execute procedure q_3 on $\langle x, n \rangle$.

(h) Hence verify that $\|t_n(x)\|^2 \leq {a_3}^2$.

(i) **Hence verify that** $\|p_n(x)t'_n(x) + p'_n(x)t_n(x)\|^2 \leq (a_0a_4 + a_1a_3)^2 = {a_6}^2$**.**

8. **Yield the tuple** $\langle a_6, b_6, a_7, b_7, c_7, q_6, q_7\rangle$**.**

Procedure IV:5

Objective

Choose a complex number x. The objective of the following instructions is to show that $|\mathrm{re}(x)| \leq \max(1, \|x\|^2)$.

Implementation

1. If $|\mathrm{re}(x)| < 1$, then do the following:

(a) **Verify that** $|\mathrm{re}(x)| < 1 \leq \max(1, \|x\|^2)$**.**

2. Otherwise do the following:

(a) **Verify that** $|\mathrm{re}(x)| \leq \mathrm{re}(x)^2 \leq \|x\|^2 \leq \max(1, \|x\|^2)$**.**

Procedure IV:6

Objective

Choose a rational number $D \geq 0$. The objective of the following instructions is to construct two rational numbers a, c and a procedure, $p(dx, n)$, to show that $\|\Delta_{x=0}^{+dx} \exp_n(x) - 1\|^2 \leq a\|dx\|^2$ when a complex number dx and a positive integer $n > c$ such that $\|dx\|^2 \leq D$ is chosen.

Implementation

1. Let $e = 2\max(1, D) + D$.

2. Execute procedure III:26 on $\langle e\rangle$ and let $\langle d, c, q\rangle$ receive.

3. Let $a = \max(1, d)$.

4. Let $p(dx, n)$ be the following procedure:

(a) Verify that $n > c$.

(b) Hence execute procedure q on $\langle D, n\rangle$.

(c) Hence verify that $\exp_n(D) \leq d$.

(d) Now using procedure II:29, procedure III:16 and procedure IV:5, verify that $\|\exp_n(dx) - 1 - dx\|^2$

i. $= \|(1 + \frac{dx}{n})^n - 1 - dx\|^2$

ii. $= \|\frac{dx}{n}\sum_r^{[0:n]}(1 + \frac{dx}{n})^r - n\frac{dx}{n}\|^2$

iii. $= \|\frac{dx}{n}\sum_r^{[0:n]}((1 + \frac{dx}{n})^r - 1)\|^2$

iv. $= \|\frac{dx}{n}\sum_r^{[0:n]}\frac{dx}{n}\sum_k^{[0:r]}(1 + \frac{dx}{n})^k\|^2$

v. $= \frac{\|dx\|^4}{n^4}\|\sum_r^{[0:n]}\sum_k^{[0:r]}(1 + \frac{dx}{n})^k\|^2$

vi. $\leq \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\|1 + \frac{dx}{n}\|^{2k}$

vii. $\leq \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\max(1, \|1 + \frac{dx}{n}\|^{2n})$

viii. $= \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\max(1, (1 + \frac{2\,\mathrm{re}(dx)}{n} + \frac{\|dx\|^2}{n^2})^n)$

ix. $\leq \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\max(1, (1 + \frac{2|\mathrm{re}(dx)|}{n} + \frac{\|dx\|^2}{n^2})^n)$

x. $\leq \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\max(1, (1 + \frac{e}{n})^n)$

xi. $\leq \frac{\|dx\|^4}{n^2}\sum_r^{[0:n]}\sum_k^{[0:r]}\max(1, d)$

xii. $\leq a\|dx\|^4$.

(e) **Therefore verify that** $\|\Delta_{x=0}^{+dx}\exp_n(x) - 1\|^2 \leq a\|dx\|^2$**.**

5. **Yield the tuple** $\langle a, c, p\rangle$**.**

Procedure IV:7

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct three rational numbers a, b, d, and a procedure, $p(x, dx, n)$, to show that $\|\Delta_{y=x}^{+dx}\exp_n(y) - \exp_n(x)\|^2 \leq \frac{a}{n^2} + b\|dx\|^2$ when two complex numbers x, dx and a positive integer $n > d$ such that $2(\|x\|^2 + \|dx\|^2) \leq X$ are chosen.

Implementation

1. Execute procedure III:31 on $\langle X\rangle$ and let $\langle e, f, q\rangle$ receive.
2. Execute procedure IV:6 on $\langle X\rangle$ and let $\langle h, j, r\rangle$ receive.
3. Execute procedure III:29 on $\langle X\rangle$ and let $\langle l, m, t\rangle$ receive.
4. Let $a = 2eX$.
5. Let $b = 2lh$.
6. Let $d = \max(f, j, m)$.
7. Let $p(x, dx, n)$ be the following procedure:
   (a) Verify that $n > d \geq f$.
   (b) Hence execute procedure q on $\langle x, dx, n\rangle$.
   (c) Therefore verify that $\|\exp_n(x)\exp_n(dx) - \exp_n(x + dx)\|^2 \leq \frac{e\|xdx\|^2}{n^2}$.
   (d) Verify that $n > d \geq j$.
   (e) Execute procedure r on $\langle dx, n\rangle$.
   (f) Therefore verify that $\|\frac{\exp_n(dx)-1}{dx} - 1\|^2 \leq h\|dx\|^2$.
   (g) Verify that $n > d \geq m$.
   (h) Execute procedure t on $\langle x, n\rangle$.
   (i) Therefore verify that $\|\exp_n(x)\|^2 \leq l$.
   (j) Using procedure III:16, verify that $\|\exp_n(x + dx) - \exp_n(x) - dx\exp_n(x)\|^2$
      i. $= \|\exp_n(x + dx) - \exp_n(x)\exp_n(dx) + \exp_n(x)\exp_n(dx) - \exp_n(x) - dx\exp_n(x)\|^2$
      ii. $\leq 2\|\exp_n(x + dx) - \exp_n(x)\exp_n(dx)\|^2 + 2\|\exp_n(x)\|^2\|\exp_n(dx) - 1 - dx\|^2$
      iii. $\leq \frac{2e\|x\|^2\|dx\|^2}{n^2} + 2lh\|dx\|^4$
      iv. $\leq \frac{2eX\|dx\|^2}{n^2} + 2lh\|dx\|^4$
   (k) **Therefore verify that** $\|\Delta_{y=x}^{+dx}\exp_n(y) - \exp_n(x)\|^2 \leq \frac{a}{n^2} + b\|dx\|^2$**.**
8. **Yield the tuple** $\langle a, b, d, p\rangle$**.**

Procedure IV:8

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct three rational numbers a, b, d and a procedure, $p(x, dx, n)$, to show that $\|\Delta_{y=x}^{+dx}\cos_n(y) + \sin_n(x)\|^2 \leq \frac{a}{n^2} + b\|dx\|^2$ when two complex numbers x, dx and a positive integer $n > d$ such that $2(\|x\|^2 + \|dx\|^2) \leq X$ are chosen.

Implementation

1. Execute procedure IV:7 on $\langle X\rangle$ and let $\langle a, b, d, q\rangle$.
2. Let $p(x, dx, n)$ be the following procedure:
   (a) Verify that $2(\|ix\|^2 + \|idx\|^2) = 2(\|x\|^2 + \|dx\|^2) \leq X$.
   (b) Verify that $\|idx\|^2 = \|dx\|^2 \leq X$.
   (c) Hence execute procedure q on $\langle ix, idx, n\rangle$.
   (d) Hence verify that $\|\frac{\exp_n(ix+idx)-\exp_n(ix)}{idx} - \exp_n(ix)\|^2 \leq \frac{a}{n^2} + b\|idx\|^2$.
   (e) Verify that $2(\|-ix\|^2 + \|-idx\|^2) = 2(\|x\|^2 + \|dx\|^2) \leq X$.
   (f) Verify that $\|-idx\|^2 = \|dx\|^2 \leq X$.
   (g) Hence execute procedure q on $\langle -ix, -idx, n\rangle$.
   (h) Hence verify that $\|\frac{\exp_n(-ix-idx)-\exp_n(-ix)}{-idx} - \exp_n(-ix)\|^2 \leq \frac{a}{n^2} + b\|-idx\|^2$.
   (i) Using procedure III:16, verify that $\|\cos_n(x + dx) - \cos_n(x) + \sin_n(x)dx\|^2$
      i. $= \|\frac{\exp_n(i(x+dx))+\exp_n(-i(x+dx))}{2} - \frac{\exp_n(ix)+\exp_n(-ix)}{2} + \frac{dx\exp_n(ix)-dx\exp_n(-ix)}{2i}\|^2$
      ii. $\leq \frac{\|\exp_n(ix+idx)-\exp_n(ix)-idx\exp_n(ix)\|^2}{2} + \frac{\|\exp_n(-ix-idx)-\exp_n(-ix)-(-idx)\exp_n(-ix)\|^2}{2}$
      iii. $\leq \frac{\|idx\|^2(\frac{a}{n^2}+b\|idx\|^2)}{2} + \frac{\|-idx\|^2(\frac{a}{n^2}+b\|-idx\|^2)}{2}$
      iv. $= \|dx\|^2(\frac{a}{n^2} + b\|dx\|^2)$.
   (j) **Therefore verify that** $\|\Delta_{y=x}^{+dx}\cos_n(y) + \sin_n(x)\|^2 \leq \frac{a}{n^2} + b\|dx\|^2$**.**
3. **Yield the tuple** $\langle a, b, d, p\rangle$**.**

Procedure IV:9

Objective

Choose a rational number $X \geq 0$. The objective of the following instructions is to construct three rational numbers a, b, d and a procedure, $p(x, dx, n)$, to show that $\|\Delta_{y=x}^{+dx} \sin_n(y) - \cos_n(x)\|^2 \leq \frac{a}{n^2} + b\|dx\|^2$ when two complex numbers x, dx and a positive integer $n > d$ such that $2(\|x\|^2 + \|dx\|^2) \leq X$ are chosen.

Implementation

Implementation is analogous to that of procedure IV:8.

Declaration IV:1

The notation $\int_r^R f(\#r, r, dr)$, where R is a non-empty list of complex numbers and $f[\#r, r, dr]$ is a function of $\#r, r, dr$, will be used as a shorthand for $\sum_t^{[0:|R|-1]} f(t, R_t, R_{t+1} - R_t)$.

Procedure IV:10

Objective

Choose two functions $f[\#r, r, dr], g[\#r, r, dr]$, and a non-empty list of complex numbers R. The objective of the following instructions is to show that $\int_r^R (f(\#r, r, dr) + g(\#r, r, dr)) = \int_r^R f(\#r, r, dr) + \int_r^R g(\#r, r, dr)$.

Implementation

1. Verify that $\int_r^R (f(\#r, r, dr) + g(\#r, r, dr))$
   (a) $= \sum_t^{[0:|R|-1]} (f(t, R_t, R_{t+1} - R_t) + g(t, R_t, R_{t+1} - R_t))$
   (b) $= \sum_t^{[0:|R|-1]} f(t, R_t, R_{t+1} - R_t) + \sum_t^{[0:|R|-1]} g(t, R_t, R_{t+1} - R_t)$
   (c) $= \int_r^R f(\#r, r, dr) + \int_r^R g(\#r, r, dr)$

Procedure IV:11

Objective

Choose a complex number a, a function $f[\#r, r, dr]$, and a non-empty list of complex numbers R. The objective of the following instructions is to show that $\int_r^R af(\#r, r, dr) = a \int_r^R f(\#r, r, dr)$.

Implementation

1. Verify that $\int_r^R af(\#r, r, dr)$
   (a) $= \sum_t^{[0:|R|-1]} af(t, R_t, R_{t+1} - R_t)$
   (b) $= a \sum_t^{[0:|R|-1]} f(t, R_t, R_{t+1} - R_t)$
   (c) $= a \int_r^R f(\#r, r, dr)$

Procedure IV:12

Objective

Choose a function $f[r]$ and two non-empty lists of complex numbers R, S such that $R_{|R|-1} = S_0$. The objective of the following instructions is to show that $\int_r^{R \frown S} f(r)dr = \int_r^R f(r)dr + \int_r^S f(r)dr$.

Implementation

1. Let $T = R \frown S$.
2. Verify that $\int_r^T f(r)dr$
   (a) $= \sum_t^{[0:|T|-1]} f(T_t)(T_{t+1} - T_t)$
   (b) $= \sum_t^{[0:|R|-1]} f(T_t)(T_{t+1} - T_t) + \sum_t^{[|R|-1:|R|]} f(T_t)(T_{t+1} - T_t) + \sum_t^{[|R|:|T|-1]} f(T_t)(T_{t+1} - T_t)$
   (c) $= \sum_t^{[0:|R|-1]} f(R_t)(R_{t+1} - R_t) + f(T_{|R|-1})(T_{|R|} - T_{|R|-1}) + \sum_t^{[|R|:|T|-1]} f(S_{t-|R|})(S_{t+1-|R|} - S_{t-|R|})$
   (d) $= \sum_t^{[0:|R|-1]} f(R_t)(R_{t+1} - R_t) + f(T_{|R|-1})(S_0 - R_{|R|-1}) + \sum_t^{[0:|S|-1]} f(S_t)(S_{t+1} - S_t)$
   (e) $= \int_r^R f(r)dr + \int_r^S f(r)dr$.

Procedure IV:13

Objective

Choose a function $f[r]$ and a list of complex numbers R. The objective of the following instructions is to show that $\|\int_r^R f(r)dr\|^2 \leq (|R|-1)^2 \max(\|\Delta R\|^2) \max(\|f(R_{[0:|R|-1]})\|^2)$

Implementation

1. Verify that $\|\int_r^R f(r)dr\|^2$
   (a) $\leq (|R|-1) \int_r^R \|f(r)\|^2 \|dr\|^2$
   (b) $\leq (|R|-1) \int_r^R \max(\|f(R_{[0:|R|-1]})\|^2) \max(\|\Delta R\|^2)$
   (c) $\leq (|R|-1)^2 \max(\|f(R_{[0:|R|-1]})\|^2) \max(\|\Delta R\|^2)$.

Procedure IV:14

Objective

Choose a list of functions F and a list of complex numbers R such that $F_0(R_1) = F_1(R_1), F_1(R_2) = F_2(R_2), \cdots, F_{|R|-3}(R_{|R|-2}) = F_{|R|-2}(R_{|R|-2})$. The objective of the following instructions is to show that $\int_r^R dr\, \Delta_{z=r}^{dr} F_{\#r}(z) = F_{|R|-2}(R_{|R|-1}) - F_0(R_0)$.

Implementation

1. Verify that $\int_r^R dr\, \Delta_{z=r}^{dr} F_{\#r}(z)$
   (a) $= \int_r^R dr(\frac{F_{\#r}(r+dr) - F_{\#r}(r)}{dr})$
   (b) $= \int_r^R (F_{\#r}(r+dr) - F_{\#r}(r))$
   (c) $= \sum_k^{[0:|R|-1]} (F_k(R_{k+1}) - F_k(R_k))$
   (d) $= -F_0(R_0) + \sum_k^{[0:|R|-2]} (F_k(R_{k+1}) - F_{k+1}(R_{k+1})) + F_{|R|-2}(R_{|R|-1})$
   (e) $= -F_0(R_0) + \sum_k^{[0:|R|-2]} 0 + F_{|R|-2}(R_{|R|-1})$
   (f) $= F_{|R|-2}(R_{|R|-1}) - F_0(R_0)$.

Declaration IV:2

The notation ΔX, where X is a list, will be used as a shorthand for $\langle X_1 - X_0, X_2 - X_1, \cdots, X_{|X|-1} - X_{|X|-2} \rangle$.

Part V

Matrix Arithmetic

Declaration V:0

The phrase "matrix" will be used as a shorthand for a list of equally lengthed lists of polynomials. In particular, the phrase "$m \times n$ matrix" will be used as a shorthand for a length-m list of length-n lists of polynomials.

Declaration V:1

The notation $A_{I,J}$, where A is a matrix and I, J are lists of indicies, will be used as a shorthand for $\langle (A_j)_J \text{ for } j \in I\rangle$.

Declaration V:2

The phrase "$A = B$", where A, B are $m \times n$ matrices, will be used as a shorthand for "$A_{i,j} = B_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$".

Procedure V:0

Objective

Choose an $m \times n$ matrix A. The objective of the following instructions is to show that $A = A$.

Implementation

1. Verify that $A_{i,j} = A_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
2. **Hence verify that** $A = A$**.**

Procedure V:1

Objective

Choose two $m \times n$ matrices A, B such that $A = B$. The objective of the following instructions is to show that $B = A$.

Implementation

1. Verify that $A_{i,j} = B_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
2. Hence verify that $B_{i,j} = A_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
3. **Hence verify that** $B = A$**.**

Procedure V:2

Objective

Choose three $m \times n$ matrices A, B, C such that $A = B$ and $B = C$. The objective of the following instructions is to show that $A = C$.

Implementation

1. Verify that $A_{i,j} = B_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
2. Verify that $B_{i,j} = C_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
3. Hence verify that $A_{i,j} = C_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
4. **Hence verify that** $A = C$**.**

Declaration V:3

The notation $A + B$, where A, B are $m \times n$ matrices, will be used as a shorthand for the list $\langle\langle A_{i,j} + B_{i,j} \text{ for } j \in [0 : n]\rangle \text{ for } i \in [0 : m]\rangle$.

Procedure V:3

Objective

Choose four $m \times n$ matrices A, B, C, D such that $A = C$ and $B = D$. The objective of the following instructions is to show that $A + B = C + D$.

Implementation

1. Verify that $A_{i,j} = C_{i,j}$ for $j \in [0:n]$, for $i \in [0:m]$.
2. Verify that $B_{i,j} = D_{i,j}$ for $j \in [0:n]$, for $i \in [0:m]$.
3. Hence verify that $A + B$
   (a) $= \langle\langle A_{i,j} + B_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (b) $= \langle\langle C_{i,j} + D_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (c) $= C + D$.

Procedure V:4

Objective

Choose three $m \times n$ matrices A, B, C. The objective of the following instructions is to show that $(A + B) + C = A + (B + C)$.

Implementation

1. Verify that $(A + B) + C$
   (a) $= \langle\langle (A + B)_{i,j} + C_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (b) $= \langle\langle (A_{i,j} + B_{i,j}) + C_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (c) $= \langle\langle A_{i,j} + (B_{i,j} + C_{i,j})$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (d) $= \langle\langle A_{i,j} + (B + C)_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (e) $= A + (B + C)$.

Procedure V:5

Objective

Choose two $m \times n$ matrices A, B. The objective of the following instructions is to show that $A + B = B + A$.

Implementation

1. $A + B$
   (a) $= \langle\langle A_{i,j} + B_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (b) $= \langle\langle B_{i,j} + A_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (c) $= B + A$.

Declaration V:4

The notation $0_{m\times n}$ will contextually be used as a shorthand for the list $\langle\langle 0$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$ where the natural numbers m, n are determined by the context.

Procedure V:6

Objective

Choose an $m \times n$ matrix A. The objective of the following instructions is to show that $0 + A = A$.

Implementation

1. Verify that $0 + A$
   (a) $= 0_{m\times n} + A$
   (b) $= \langle\langle 0_{i,j} + A_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (c) $= \langle\langle 0 + A_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (d) $= \langle\langle A_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$
   (e) $= A$.

Declaration V:5

The notation $-A$, where A is an $m \times n$ matrix, will be used as a shorthand for the list $\langle\langle -A_{i,j}$ for $j \in [0:n]\rangle$ for $i \in [0:m]\rangle$.

Procedure V:7

Objective

Choose two $m \times n$ matrices A, B such that $A = B$. The objective of the following instructions is to show that $-A = -B$.

Implementation

1. Verify that $A_{i,j} = B_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
2. Hence verify that $-A$

   (a) $= \langle\langle -A_{i,j}$ for $j \in [0 : n]\rangle$ for $i \in [0 : m]\rangle$

   (b) $= \langle\langle -B_{i,j}$ for $j \in [0 : n]\rangle$ for $i \in [0 : m]\rangle$

   (c) $= -B$.

Procedure V:8

Objective

Choose a $m \times n$ matrix A. The objective of the following instructions is to show that $-A + A = 0$.

Implementation

1. Verify that $-A + A$

   (a) $\langle\langle (-A)_{i,j} + A_{i,j}$ for $j \in [0 : n]\rangle$ for $i \in [0 : m]\rangle$

   (b) $\langle\langle -(A_{i,j}) + A_{i,j}$ for $j \in [0 : n]\rangle$ for $i \in [0 : m]\rangle$

   (c) $\langle\langle 0$ for $j \in [0 : n]\rangle$ for $i \in [0 : m]\rangle$

   (d) $= 0$.

Declaration V:6

The notation AB, where A is an $m \times n$ matrix and B is an $n \times k$ matrix, will be used as a shorthand for the list $\langle\langle \sum_r^{[0:n]} A_{i,r}B_{r,j}$ for $j \in [0 : k]\rangle$ for $i \in [0 : m]\rangle$.

Procedure V:9

Objective

Choose two $m \times n$ matrices A, C and two $n \times k$ matrices B, D such that $A = C$ and $B = D$. The objective of the following instructions is to show that $AB = CD$.

Implementation

1. Verify that $A_{i,j} = C_{i,j}$ for $j \in [0 : n]$, for $i \in [0 : m]$.
2. Verify that $B_{i,j} = D_{i,j}$ for $j \in [0 : k]$, for $i \in [0 : n]$.
3. Hence verify that AB

   (a) $= \langle\langle \sum_r^{[0:n]} A_{i,r}B_{r,j}$ for $j \in [0 : k]\rangle$ for $i \in [0 : m]\rangle$

   (b) $= \langle\langle \sum_r^{[0:n]} C_{i,r}D_{r,j}$ for $j \in [0 : k]\rangle$ for $i \in [0 : m]\rangle$

   (c) $= CD$.

Procedure V:10

Objective

Choose an $m \times n$ matrix, A, an $n \times p$ matrix, B, and a $p \times q$ matrix, C. The objective of the following instructions is to show that $(AB)C = A(BC)$.

Implementation

1. Verify that $(AB)C$

   (a) $= \langle\langle \sum_r^{[0:p]} (AB)_{i,r}C_{r,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (b) $= \langle\langle \sum_r^{[0:p]} (\sum_l^{[0:n]} A_{i,l}B_{l,r})C_{r,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (c) $= \langle\langle \sum_r^{[0:p]} \sum_l^{[0:n]} A_{i,l}B_{l,r}C_{r,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (d) $= \langle\langle \sum_l^{[0:n]} \sum_r^{[0:p]} A_{i,l}B_{l,r}C_{r,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (e) $= \langle\langle \sum_l^{[0:n]} A_{i,l} \sum_r^{[0:p]} B_{l,r}C_{r,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (f) $= \langle\langle \sum_l^{[0:n]} A_{i,l}(BC)_{l,j}$ for $j \in [0 : q]\rangle$ for $i \in [0 : m]\rangle$

   (g) $= A(BC)$.

Declaration V:7

The notation $a_{m\times m}$, where $a \neq 0$ is a polynomial, will contextually be used as a shorthand for the list $\langle\langle a[i=j] \text{ for } j \in [0:m]\rangle \text{ for } i \in [0:m]\rangle$.

Procedure V:11

Objective

Choose an $m \times n$ matrix, A. The objective of the following instructions is to show that $1A = A$.

Implementation

1. Verify that $1A$
   (a) $= 1_m A$
   (b) $= \langle\langle\sum_r^{[0:m]} 1_{i,r}A_{r,j} \text{ for } j \in [0:n]\rangle \text{ for } i \in [0:m]\rangle$
   (c) $= \langle\langle\sum_r^{[0:m]}[i=r]A_{r,j} \text{ for } j \in [0:n]\rangle \text{ for } i \in [0:m]\rangle$
   (d) $= \langle\langle A_{i,j} \text{ for } j \in [0:n]\rangle \text{ for } i \in [0:m]\rangle$
   (e) $= A$.

Procedure V:12

Objective

Choose an $m \times n$ matrix A, and two $n \times k$ matrices B, C. The objective of the following instructions is to show that $A(B+C) = AB + AC$.

Implementation

1. $A(B+C)$
   (a) $= \langle\langle\sum_r^{[0:n]} A_{i,r}(B+C)_{r,j} \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle$
   (b) $= \langle\langle\sum_r^{[0:n]} A_{i,r}(B_{r,j}+C_{r,j}) \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle$
   (c) $= \langle\langle\sum_r^{[0:n]}(A_{i,r}B_{r,j}+A_{i,r}C_{r,j}) \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle$
   (d) $= \langle\langle\sum_r^{[0:n]} A_{i,r}B_{r,j} + \sum_r^{[0:n]} A_{i,r}C_{r,j} \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle$
   (e) $= \langle\langle\sum_r^{[0:n]} A_{i,r}B_{r,j} \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle + \langle\langle\sum_r^{[0:n]}\sum_r^{[0:n]} A_{i,r}C_{r,j} \text{ for } j \in [0:k]\rangle \text{ for } i \in [0:m]\rangle$
   (f) $= AB + AC$.

Declaration V:8

The phrase "row i of A" and the notation $A_{i,*}$, where A is an $m \times n$ matrix and $0 \leq i < m$, will be used as a shorthand for $A_{i,[0:n]}$.

Declaration V:9

The phrase "column i of A" and the notation $A_{*,i}$, where A is an $m \times n$ matrix and $0 \leq i < n$, will be used as a shorthand for $A_{[0:m],i}$.

Procedure V:13

Objective

Choose an $m \times 2$ matrix, A. Let $\deg(0) = \infty$. Let $k = \min(\deg(A_{0,0}), \deg(A_{0,1}))$ and $q = \deg(A_{0,0})$. The objective of the following instructions is to make $A_{0,1} = 0$, $\deg(A_{0,0}) \leq k$, and either leave $A_{*,0}$ unchanged or make $\deg(A_{0,0}) < q$ by a sequence of operations whereby, in each step a polynomial times either of the columns is added to the other.

Implementation

1. Let A be our working matrix.
2. While $A_{0,1} \neq 0$, do the following:
   (a) If $\deg(A_{0,0}) \leq \deg(A_{0,1})$, then:
      i. Subtract $\frac{(A_{0,1})_{\deg(A_{0,1})}}{(A_{0,0})_{\deg(A_{0,0})}}\lambda^{\deg(A_{0,1})-\deg(A_{0,0})}$ times $A_{0,0}$ from $A_{0,1}$.
      ii. Now verify that either $A_{0,1}$'s degree has decreased or $A_{0,1} = 0$.
   (b) Otherwise, do the following:
      i. Let $p = \frac{(A_{0,0})_{\deg(A_{0,0})}}{(A_{0,1})_{\deg(A_{0,1})}}\lambda^{\deg(A_{0,0})-\deg(A_{0,1})}$.
      ii. If $A_{0,0} = pA_{0,1}$, then do the following:
         A. Add $1-p$ times $A_{0,1}$ to $A_{0,0}$.

B. Verify that now $A_{0,0} = A_{0,1}$.

iii. Otherwise, do the following:

A. Verify that $A_{0,0} \neq pA_{0,1}$.

B. Add $-p$ times $A_{0,1}$ to $A_{0,0}$.

iv. Therefore verify that $A_{0,0} \neq 0$.

v. Also verify that $A_{0,0}$'s degree has decreased.

3. **Verify that $A_{0,1} = 0$.**

4. Verify that the changes to $A_{0,0}$, if any, have decreased its degree.

5. If both operations are well-defined, then do the following:

(a) Verify that all changes to $A_{0,1}$ but the last have decreased its degree.

(b) Verify that $\deg(A_{0,0}) \leq$ the degree of the penultimate value of $A_{0,1}$.

6. **Therefore verify that $\deg(A_{0,0}) \leq k$.**

7. If $A_{*,0}$ was changed, then do the following:

(a) Verify that $A_{0,0}$ was also changed.

(b) **Therefore verify that $\deg(A_{0,0}) < q$.**

8. **Yield the tuple $\langle A \rangle$.**

Declaration V:10

The phrase "matrix diagonal" will be used as a shorthand for matrix positions such that the row index equals the column index.

Declaration V:11

The phrase "diagonal matrix" will be used to refer to matrices with 0s in all off-diagonal positions.

Procedure V:14

Objective

Choose a $m \times n$ matrix, A. The objective of the following instructions is to transform A into an $m \times n$ diagonal matrix by a sequence of operations whereby either a polynomial times any of the columns is added to a different column, or a polynomial times any of the rows is added to a different row.

Implementation

1. If $m = 0$ or $n = 0$, then do the following:

(a) **Verify that A is an $m \times n$ diagonal matrix.**

(b) **Yield the tuple $\langle A \rangle$.**

2. Otherwise do the following:

3. Verify that $m > 0$ and $n > 0$.

4. Let A be our working matrix.

5. Now do the following:

(a) While $A_{0,[1:n]} \neq 0$, do the following:

i. Select the $m \times 2$ matrix whose top-right entry coincides with the last non-zero entry of the first row

ii. Apply procedure V:13 on this submatrix.

iii. Verify that the top-left and top-right entries of the submatrix are now non-zero and zero respectively.

iv. If $A_{*,0}$ was modified by (5aii), then do the following:

A. Verify that $\deg(A_{0,0})$ decreased.

B. Go back to (5).

(b) Now do the same operations as in (a), but this time with the operations themselves reflected across the matrix's diagonal.

6. Verify that $A_{0,[1:n]} = 0$.

7. Also verify that $A_{[1:m],0} = 0$.

8. Apply procedure V:14 on the submatrix $A_{[1:m],[1:n]}$.

9. Verify that (8)'s execution leaves the first row and column unchanged.

10. Also verify that $A_{[1:m],[1:n]}$ is now a $(m-1) \times (n-1)$ diagonal matrix.

11. **Therefore verify that A is now an $m \times n$ diagonal matrix.**

12. **Yield the tuple $\langle A \rangle$.**

Declaration V:12

The phrase "tilt matrix" will be used to refer to square matrices with only 1s on the diagonal, a single polynomial off the diagonal, and 0s everywhere else.

Procedure V:15

Objective

Choose a procedure, A, and two non-negative integers m, n. The objective of the following instructions is, once A has been executed, to construct a list of $m \times m$ tilts, M, and a list of $n \times n$ tilts, N such that $M_{|M|-1-i}$ equals 1_m after applying the i^{th} row operation carried out by A also on it, and N_i equals 1_n after applying the i^{th} row operation carried out by A also on it.

Implementation

1. Make an empty list, N.
2. Augment procedure A so that each time a polynomial x times a column i is added onto column j, an $n \times n$ matrix that only has 1s on its diagonal, and such that the only non-zero entry off its diagonal is x at position (i, j), is appended onto N.
3. Make an empty list, M.
4. Also augment procedure A so that each time a polynomial x times a row i is added onto row j, an $n \times n$ matrix that only has 1s on its diagonal, and such that the only non-zero entry off its diagonal is x at position (j, i), is prepended onto M.
5. Now run procedure A.
6. **Yield the tuple $\langle M, N \rangle$.**

Procedure V:16

Objective

Choose a $m \times n$ matrix, A. The objective of the following instructions is to show that $1_m A = A = A 1_n$.

Implementation

1. For $0 \leq r < m$, do the following:
   (a) For $0 \leq t < n$, do the following:
      i. Verify that $(1_m A)_{r,t} = \sum_u^{[0:m]} (1_m)_{r,u} A_{u,t} = (1_m)_{r,r} A_{r,t} = 1 * A_{r,t} = A_{r,t}$.
2. **Therefore verify that $1_m A = A$.**
3. For $0 \leq r < m$, do the following:
   (a) For $0 \leq t < n$, do the following:
      i. Verify that $(A 1_n)_{r,t} = \sum_u^{[0:m]} A_{r,u} (1_n)_{u,t} = A_{r,t} (1_n)_{t,t} = A_{r,t} * 1 = A_{r,t}$.
4. **Therefore verify that $A 1_n = A$.**

Declaration V:13

The notation A^{-1}, where A is a list of $m \times m$ tilts, will be used to refer to the result yielded by executing the following instructions:

1. Let A^{-1} be $\langle\rangle$.
2. For i in $[0 : |A|]$, do the following:
   (a) Let (j, k) be the position of the off diagonal entry of A_i.
   (b) Let B equal A_i but with entry (j, k) negated.
   (c) Now prepend B onto A^{-1}.
3. **Yield $\langle A^{-1} \rangle$.**

Procedure V:17

Objective

Choose a list of $m \times m$ tilts, A. The objective of the following instructions is to show that $A_* {A^{-1}}_* = 1_m$.

Implementation

1. Verify that $|A| = |A^{-1}|$.
2. For i in $[0 : |A|]$, do the following:
   (a) Let (j, k) be the position of the off diagonal entry of A_i.
   (b) Let $B = {A^{-1}}_{|A|-1-i}$.

(c) For r in $[0 : m]$ and $r \neq j$, do the following:

i. For t in $[0 : m]$, do the following:

A. Verify that $(A_i B)_{r,t} = \sum_u^{[0:m]} (A_i)_{r,u} B_{u,t} = (A_i)_{r,r} B_{r,t} = 1 * B_{r,t} = [r = t]$.

(d) For t in $[0 : m]$ and $t \neq k$, do the following:

i. Verify that $(A_i B)_{j,t} = \sum_u^{[0:m]} (A_i)_{j,u} B_{u,t} = (A_i)_{j,t} B_{t,t} = (A_i)_{j,t} * 1 = [j = t]$.

(e) Verify that $(A_i B)_{j,k} = \sum_u^{[0:m]} (A_i)_{j,u} B_{u,k} = (A_i)_{j,j} B_{j,k} + (A_i)_{j,k} B_{k,k} = 1 * B_{j,k} + (A_i)_{j,k} * 1 = B_{j,k} + (A_i)_{j,k} = 0$.

(f) Therefore verify that $A_i B = 1_m$.

3. Therefore using procedure V:10 and procedure V:16, verify that $A_* {A^{-1}}_*$

(a) $= A_0 \cdots A_{|A|-2} A_{|A|-1} {A^{-1}}_0 {A^{-1}}_1 \cdots {A^{-1}}_{|A|-1}$

(b) $= A_0 \cdots A_{|A|-3} A_{|A|-2} 1_m {A^{-1}}_1 {A^{-1}}_2 \cdots {A^{-1}}_{|A|-1}$

(c) $= A_0 \cdots A_{|A|-3} A_{|A|-2} {A^{-1}}_1 {A^{-1}}_2 \cdots {A^{-1}}_{|A|-1}$

(d) $\vdots$

(e) $= A_0 1_m {A^{-1}}_{|A|-1}$

(f) $= A_0 {A^{-1}}_{|A|-1}$

(g) $= 1_m$.

Procedure V:18

Objective

Choose a list of $m \times m$ tilts, A. The objective of the following instructions is to show that $(A^{-1})^{-1} = A$ and ${A^{-1}}_* A_* = 1_m$.

Implementation

1. **Verify that $(A^{-1})^{-1} = A$.**

2. **Therefore using procedure V:17, verify that ${A^{-1}}_* A_* = {A^{-1}}_* {(A^{-1})^{-1}}_* = 1_m$.**

Procedure V:19

Objective

Choose a 2×2 diagonal matrix, A. The objective of the following instructions is to construct polynomials u, v and transform A into a 2×2 diagonal matrix, A', such that $A'_{1,1} = uA'_{0,0}$ and $A_{0,0} = vA'_{0,0}$ by a sequence of operations whereby either a polynomial times any of the columns is added to a different column, or a polynomial times any of the rows is added to a different row.

Implementation

1. Add row 1 to row 0.

2. Now verify that $A_{0,1} = A_{1,1}$.

3. Set $A' = A$ and let A' be our working matrix.

4. Let $\langle M, N \rangle$ receive the results of executing procedure V:15 on the pair $\langle 2, 2 \rangle$ and the following procedure:

   (a) Execute procedure V:13 on A'.

5. Using (4), verify that M is empty.

6. Using (4) and (5), verify that $AN_* = M_* AN_* = A'$.

7. Using (6), verify that $A = A1_n = AN_* {N^{-1}}_* = A' {N^{-1}}_*$.

8. Using (4), verify that $A'_{0,1} = 0$.

9. **Using (4) and (7), verify that $A_{0,0} = A'_{0,0} {N^{-1}}_{*0,0} + A'_{0,1} {N^{-1}}_{*1,0} = A'_{0,0} {N^{-1}}_{*0,0}$.**

10. Using (4) and (7), verify that $A_{1,1} = A_{0,1} = A'_{0,0} {N^{-1}}_{*0,1} + A'_{0,1} {N^{-1}}_{*1,1} = A'_{0,0} {N^{-1}}_{*0,1}$.

11. Using (2), verify that $A_{1,0} = 0$.

12. Using (6) and (11), verify that $A'_{1,0} = A_{1,0} N_{*0,0} + A_{1,1} N_{*1,0} = A_{1,1} N_{*1,0} = A'_{0,0} {N^{-1}}_{*0,1} N_{*1,0}$.

13. **Using (6) and (11), verify that $A'_{1,1} = A_{1,0} N_{*0,1} + A_{1,1} N_{*1,1} = A_{1,1} N_{*1,1} = A'_{0,0} {N^{-1}}_{*0,1} N_{*1,1}$.**

14. Subtract ${N^{-1}}_{*0,1} N_{*1,0}$ times row 0 from row 1.

15. Now using (14) and (12), verify that $A'_{1,0} = 0$.

16. **Therefore verify that A' is a 2×2 diagonal matrix.**

17. **Let $A = A'$.**

18. **Yield $\langle N^{-1}{}_{*0,1} N_{*1,1}, N^{-1}{}_{*0,0} \rangle$.**

Procedure V:20

Objective

Choose a $m \times n$ matrix, A such that $\min(m, n) > 0$. The objective of the following instructions is to define a list of polynomials u and transform A into an $m \times n$ diagonal matrix such that $A_{k,k} = u_k A_{0,0}$ for k in $[0 : \min(m, n)]$ by a sequence of operations whereby either a polynomial times any of the columns is added to a different column, or a polynomial times any of the rows is added to a different row.

Implementation

1. Let $u = \langle 1 \rangle$.
2. Execute procedure V:14 on A.
3. Verify that A is an $m \times n$ diagonal matrix.
4. For j in $[1 : \min(m, n)]$, do the following:

   (a) Using (h), verify that $A_{k,k} = u_k A_{0,0}$ for k in $[0 : j]$.

   (b) Set $A' = A$.

   (c) Execute procedure V:19 on $A'_{\langle 0,j \rangle, \langle 0,j \rangle}$ and let $\langle u_j, v \rangle$ receive.

   (d) Using (c), verify that A and A' are the same modulo positions $\langle 0, 0 \rangle$ and $\langle j, j \rangle$.

   (e) Therefore verify that A' is an $m \times n$ diagonal matrix.

   (f) Also, using (c), verify that $A'_{j,j} = u_j A'_{0,0}$.

   (g) Also, for k in $[1 : j]$, do the following:

      i. Using (a), (c), and (d), verify that $A'_{k,k} = A_{k,k} = u_k A_{0,0} = u_k A'_{0,0} v$.

      ii. Set $u_k = u_k v$.

      iii. Hence verify that $A'_{k,k} = u_k A'_{0,0}$.

   (h) Therefore verify that $A_{k,k} = u_k A_{0,0}$ for k in $[0 : j + 1]$.

   (i) Now let $A = A'$.

5. **Hence using (4h), verify that $A_{k,k} = u_k A_{0,0}$ for k in $[0 : \min(m, n)]$.**

6. **Also, using (4e), verify that A is an $m \times n$ diagonal matrix.**

7. **Yield $\langle u \rangle$.**

Procedure V:21

Objective

Choose a $m \times n$ matrix, A, and a $n \times k$ matrix, B. Choose integers $0 \leq a < m$, $0 \leq b < n$, and $0 \leq c < k$. The objective of the following instructions is to show that

1. $(AB)_{[0:a],[0:c]} = A_{[0:a],[0:b]} B_{[0:b],[0:c]} + A_{[0:a],[b:n]} B_{[b:n],[0:c]}$
2. $(AB)_{[0:a],[c:k]} = A_{[0:a],[0:b]} B_{[0:b],[c:k]} + A_{[0:a],[b:n]} B_{[b:n],[c:k]}$
3. $(AB)_{[a:m],[0:c]} = A_{[a:m],[0:b]} B_{[0:b],[0:c]} + A_{[a:m],[b:n]} B_{[b:n],[0:c]}$
4. $(AB)_{[a:m],[c:k]} = A_{[a:m],[0:b]} B_{[0:b],[c:k]} + A_{[a:m],[b:n]} B_{[b:n],[c:k]}$.

Implementation

1. For each $0 \leq i < a$, do the following:

   (a) For each $0 \leq j < c$, do the following:

      i. Verify that $(AB)_{i,j} = \sum_p^{[0:n]} A_{i,p} B_{p,j} = \sum_p^{[0:b]} A_{i,p} B_{p,j} + \sum_p^{[b:n]} A_{i,p} B_{p,j} = \sum_p^{[0:b]} (A_{[0:a],[0:b]})_{i,p} (B_{[0:b],[0:c]})_{p,j} + \sum_p^{[0:n-b]} (A_{[0:a],[b:n]})_{i,p} (B_{[b:n],[0:c]})_{p,j} = (A_{[0:a],[0:b]} B_{[0:b],[0:c]})_{i,j} + (A_{[0:a],[b:n]} B_{[b:n],[0:c]})_{i,j}$.

2. **Therefore verify that $(AB)_{[0:a],[0:c]} = A_{[0:a],[0:b]} B_{[0:b],[0:c]} + A_{[0:a],[b:n]} B_{[b:n],[0:c]}$.**

3. **Using computations analogous to (1) and (2), show items (2), (3), and (4) of the objective.**

Declaration V:14

The phrase "number of rows of A" and the notation rows(A), where A is an $m \times n$ matrix, will be used as a shorthand for m.

Declaration V:15

The phrase "number of columns of A" and the notation cols(A), where A is an $m \times n$ matrix, will be used as a shorthand for n.

Declaration V:16

The notation diag(C), where C is a list of rational square matrices, will be used to refer to the result yielded by executing the following instructions:

1. Let E be a 0×0 matrices.
2. Now for i in $[0 : |C|]$:
   (a) Add $\text{cols}(C_i)$ columns filled with zeros to the right end of E.
   (b) Add $\text{rows}(C_i)$ rows filled with zeros to the bottom end of E.
   (c) Set the bottom-right corner of E equal to C_i.
3. **Yield the tuple $\langle E \rangle$.**

Procedure V:22

Objective

Choose a $m \times n$ matrix, A. Let $A_{-1,-1} = 1$. The objective of the following instructions is to construct the list of polynomials v and transform A into an $m \times n$ diagonal matrix such that $A_{k,k} = v_k A_{k-1,k-1}$ for k in $[0 : \min(m, n)]$ by a sequence of operations whereby either a polynomial times any of the columns is added to a different column, or a polynomial times any of the rows is added to a different row.

Implementation

1. If $\min(m, n) = 0$, then do the following:
   (a) **Verify that A is an $m \times n$ diagonal matrix.**
   (b) **Yield $\langle\rangle$.**
2. Otherwise do the following:
   (a) Apply procedure V:20 on A, and let $\langle u \rangle$ receive.
   (b) Verify that A is an $m \times n$ diagonal matrix.
   (c) Verify that $A_{k,k} = u_k A_{0,0}$ for k in $[0 : \min(m, n)]$.
   (d) Let B, C be an $(m-1) \times (n-1)$ diagonal matrix with $u_{1:|u|}$ on the diagonal.
   (e) Let $\langle M, N \rangle$ receive the results of executing procedure V:15 on the pair $\langle m-1, n-1 \rangle$ and the following procedure:
      i. Execute procedure V:22 on C and let $\langle w \rangle$ receive.
   (f) Therefore verify that C is an $(m-1) \times (n-1)$ diagonal matrix.
   (g) Also verify that $C = M_* B N_*$.
   (h) Let $C_{-1,-1} = 1$.
   (i) Now using (ei), verify that $C_{k,k} = w_k C_{k-1,k-1}$ for k in $[0 : \min(m, n) - 1]$.
   (j) Therefore using (c), verify that $A_{0,0} C = M_*(A_{0,0} B) N_* = M_* A_{[1:m],[1:n]} N_*$.
   (k) Premultiply A by $\text{diag}(1, M_k)$ for k in $[|M| : 0]$.
   (l) Postmultiply A by $\text{diag}(1, N_k)$ for k in $[0 : |N|]$.
   (m) Now verify that $A_{[1:m],[1:n]} = A_{0,0} C$.
   (n) Now let $u = \langle A_{0,0} \rangle ^\frown w$.
   (o) **Therefore verify that $A_{k,k} = u_k A_{k-1,k-1}$ for k in $[0 : \min(m, n)]$.**
   (p) **Yield the tuple $\langle u \rangle$.**

Declaration V:17

The notation det(A), where A is a $m \times m$ matrix, will be used to refer to the result yielded by executing the following instructions:

1. If $m = 0$, then do the following:

(a) **Yield the tuple $\langle 1 \rangle$.**

2. Otherwise, do the following:

(a) Let $h_r = A_{[0:r]\frown[r+1,m],[1:m]}$ for r in $[0 : m]$.

(b) **Yield the tuple $\langle \sum_r^{[0:m]} (-1)^r A_{r,0} \det(h_r) \rangle$.**

Procedure V:23

Objective

Choose a polynomial p. Choose two $1 \times m$ matrices, B and C. Choose an integer $0 \leq i < m$. Choose a $m \times m$ matrix, A, such that its i^{th} row is $B + pC$. Let A' be A but with the i^{th} row replaced by B and let A'' be A but with the i^{th} row replaced by C. The objective of the following instructions is to show that $\det(A) = \det(A') + p\det(A'')$.

Implementation

1. If $m = 1$, then do the following:

(a) Verify that $i = 0$.

(b) **Therefore verify that $\det(A) = A_{0,0} = B_{0,0} + pC_{0,0} = \det(A') + p\det(A'')$.**

2. Otherwise, do the following:

(a) For r in $[0 : i]$, do the following:

i. Verify that $(A_{[0:r]\frown[r+1:m],[1:m]})_{i-1,*} = B + pC$.

ii. Verify that $A'_{[0:r]\frown[r+1:m],[1:m]}$ is $A_{[0:r]\frown[r+1:m],[1:m]}$ with row $i-1$ replaced by B.

iii. Verify that $A''_{[0:r]\frown[r+1:m],[1:m]}$ is $A_{[0:r]\frown[r+1:m],[1:m]}$ with row $i-1$ replaced by C.

iv. Execute procedure V:23 on $\langle p, B, C, i-1, A_{[0:r]\frown[r+1:m],[1:m]} \rangle$.

v. Therefore verify that $\det(A_{[0:r]\frown[r+1:m],[1:m]}) = \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]})$.

(b) For r in $[i+1 : m]$, do the following:

i. Verify that $(A_{[0:r]\frown[r+1:m],[1:m]})_{i,*} = B + pC$.

ii. Verify that $A'_{[0:r]\frown[r+1:m],[1:m]}$ is $A_{[0:r]\frown[r+1:m],[1:m]}$ with row i replaced by B.

iii. Verify that $A''_{[0:r]\frown[r+1:m],[1:m]}$ is $A_{[0:r]\frown[r+1:m],[1:m]}$ with row i replaced by C.

iv. Execute procedure V:23 on $\langle p, B, C, i, A_{[0:r]\frown[r+1:m],[1:m]} \rangle$.

v. Therefore verify that $\det(A_{[0:r]\frown[r+1:m],[1:m]}) = \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]})$.

(c) Therefore using (av) and (bv), verify that $\det(A)$

i. $= \sum_r^{[0:m]} (-1)^r A_{r,0} \det(A_{[0:r]\frown[r+1:m],[1:m]})$

ii. $= \sum_r^{[0:i]} (-1)^r A_{r,0} \det(A_{[0:r]\frown[r+1:m],[1:m]}) + (-1)^i A_{i,0} \det(A_{[0:i]\frown[i+1:m],[1:m]}) + \sum_r^{[i+1:m]} (-1)^r A_{r,0} \det(A_{[0:r]\frown[r+1:m],[1:m]})$

iii. $= \sum_r^{[0:i]} (-1)^r A_{r,0} (\det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]})) + (-1)^i (A'_{i,0} + pA''_{i,0}) \det(A_{[0:i]\frown[i+1:m],[1:m]}) + \sum_r^{[i+1:m]} (-1)^r A_{r,0} (\det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]}))$

iv. $= \sum_r^{[0:i]} (-1)^r A_{r,0} \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + (-1)^i A'_{i,0} \det(A_{[0:i]\frown[i+1:m],[1:m]}) + \sum_r^{[i+1:m]} (-1)^r A_{r,0} \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + \sum_r^{[0:i]} (-1)^r A_{r,0} p\det(A''_{[0:r]\frown[r+1:m],[1:m]}) + (-1)^i pA''_{i,0} \det(A_{[0:i]\frown[i+1:m],[1:m]}) + \sum_r^{[i+1:m]} (-1)^r A_{r,0} p\det(A''_{[0:r]\frown[r+1:m],[1:m]})$

v. $= \sum_r^{[0:m]} (-1)^r A'_{r,0} \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\sum_r^{[0:m]} (-1)^r A''_{r,0} \det(A''_{[0:r]\frown[r+1:m],[1:m]})$

vi. $= \det(A') + p\det(A'')$.

Procedure V:24

Objective

Choose a polynomial p. Choose two $m \times 1$ matrices, B and C. Choose an integer $0 \leq i < m$. Choose a $m \times m$ matrix, A, such that its i^{th} column is $B + pC$. Let A' be A but with the i^{th} column replaced by B and let A'' be A but with the i^{th} column replaced by C. The objective of the following instructions is to show that $\det(A) = \det(A') + p\det(A'')$.

Implementation

1. If $i = 0$, then verify that $\det(A)$

(a) $= \sum_r^{[0:m]}(-1)^r A_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

(b) $= \sum_r^{[0:m]}(-1)^r (B+pC)_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

(c) $= \sum_r^{[0:m]}(-1)^r (B)_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]}) + \sum_r^{[0:m]}(-1)^r (pC)_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

(d) $= \sum_r^{[0:m]}(-1)^r (B)_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]}) + p\sum_r^{[0:m]}(-1)^r (C)_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

(e) $= \sum_r^{[0:m]}(-1)^r (A')_{r,0}\det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\sum_r^{[0:m]}(-1)^r (A'')_{r,0}\det(A''_{[0:r]\frown[r+1:m],[1:m]})$

(f) $= \det(A') + p\det(A'')$

2. Otherwise, do the following:

(a) For r in $[0:m]$, do the following:

i. Execute procedure V:24 on $\langle p, B_{[0:r]\frown[r+1:m],0}, C_{[0:r]\frown[r+1:m],0}, i-1, A_{[0:r]\frown[r+1:m],[1:m]}\rangle$.

ii. Therefore verify that $\det(A_{[0:r]\frown[r+1:m],[1:m]}) = \det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]})$.

(b) Therefore using (a), verify that $\det(A)$

i. $= \sum_r^{[0:m]}(-1)^r A_{r,0}\cdot\det(A_{[0:r]\frown[r+1:m],[1:m]})$

ii. $= \sum_r^{[0:m]}(-1)^r A_{r,0}(\det(A'_{[0:r]\frown[r+1:m],[1:m]}) + p\det(A''_{[0:r]\frown[r+1:m],[1:m]}))$

iii. $= \sum_r^{[0:m]}(-1)^r A'_{r,0}\det(A'_{[0:r]\frown[r+1:m],[1:m]}) + \sum_r^{[0:m]}(-1)^r A''_{r,0}p\det(A''_{[0:r]\frown[r+1:m],[1:m]})$

iv. $= \det(A') + p\det(A'')$.

Procedure V:25

Objective

Choose a $m \times m$ matrix, A. Choose an integer $0 < i < m$. Let A' be A with rows $i-1$ and i swapped. The objective of the following instructions is to show that $\det(A') = -\det(A)$.

Implementation

1. If $m = 2$, then do the following:

(a) Verify that $i = 1$.

(b) Therefore verify that $\det(A') = A'_{0,0}A'_{1,1} - A'_{1,0}A'_{0,1} = A_{1,0}A_{0,1} - A_{0,0}A_{1,1} = -\det(A)$.

2. Otherwise do the following:

(a) For r in $[0:i-1]$, do the following:

i. Verify that $A_{[0:r]\frown[r+1:m],[1:m]}$ is the same as $A'_{[0:r]\frown[r+1:m],[1:m]}$ but with rows $i-2$ and $i-1$ swapped.

ii. Execute procedure V:25 on $\langle A_{[0:r]\frown[r+1:m],[1:m]}, i-1\rangle$.

iii. Hence verify that $\det(A'_{[0:r]\frown[r+1:m],[1:m]}) = -\det(A_{[0:r]\frown[r+1:m],[1:m]})$.

(b) For r in $[i+1:m]$, do the following:

i. Verify that $A_{[0:r]\frown[r+1:m],[1:m]}$ is the same as $A'_{[0:r]\frown[r+1:m],[1:m]}$ but with rows $i-1$ and i swapped.

ii. Execute procedure V:25 on $\langle A_{[0:r]\frown[r+1:m],[1:m]}, i\rangle$.

iii. Hence verify that $\det(A'_{[0:r]\frown[r+1:m],[1:m]}) = -\det(A_{[0:r]\frown[r+1:m],[1:m]})$.

(c) Verify that $\det(A)$

i. $= \sum_r^{[0:m]}(-1)^r A_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

ii. $= \sum_r^{[0:i-1]}(-1)^r A_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]}) + (-1)^{i-1}A_{i-1,0}\det(A_{[0:i-1]\frown[i:m],[1:m]}) + (-1)^i A_{i,0}\det(A_{[0:i]\frown[i+1:m],[1:m]}) + \sum_r^{[i+1:m]}(-1)^r A_{r,0}\det(A_{[0:r]\frown[r+1:m],[1:m]})$

iii. $= -\sum_r^{[0:i-1]}(-1)^r A'_{r,0}\det(A'_{[0:r]\frown[r+1:m],[1:m]}) - (-1)^i A'_{i,0}\det(A'_{[0:i]\frown[i+1:m],[1:m]}) - (-1)^{i-1}A'_{i-1,0}\det(A'_{[0:i-1]\frown[i:m],[1:m]}) - \sum_r^{[i+1:m]}(-1)^r A'_{r,0}\det(A'_{[0:r]\frown[r+1:m],[1:m]})$

iv. $= -\sum_r^{[0:m]}(-1)^r A'_{r,0}\det(A'_{[0:r]\frown[r+1:m],[1:m]})$

v. $= -\det(A')$.

Procedure V:26

Objective

Choose a $m \times m$ matrix, A. Choose an integer $0 < i < m$. Let A' be A with columns $i-1$ and i swapped. The objective of the following instructions is to show that $\det(A') = -\det(A)$.

Implementation

1. If $i = 1$, then verify that $\det(A)$
   (a) $= \sum_r^{[0:m]} (-1)^r A_{r,0} \det(A_{[0:r]\frown[r+1:m],[1:m]})$
   (b) $= \sum_r^{[0:m]} (-1)^r A_{r,0} \sum_t^{[r+1:m]} (-1)^{t-1} A_{t,1} * \det(A_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m]}) + \sum_t^{[0:m]} (-1)^t A_{t,0} \sum_r^{[0:t]} (-1)^r A_{r,1} * \det(A_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m+1]})$
   (c) $= \sum_t^{[0:m]} (-1)^{t-1} A_{t,1} \sum_r^{[0:t]} (-1)^r A_{r,0} * \det(A_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m+1]}) + \sum_r^{[0:m]} (-1)^r A_{r,1} \sum_t^{[r+1:m]} (-1)^t A_{t,0} * \det(A_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m+1]})$
   (d) $= \sum_t^{[0:m]} (-1)^{t-1} A'_{t,0} \sum_r^{[0:t]} (-1)^r A'_{r,1} * \det(A'_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m+1]}) + \sum_r^{[0:m]} (-1)^r A'_{r,0} \sum_t^{[r+1:m]} (-1)^t A'_{t,1} * \det(A'_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m]})$
   (e) $= -(\sum_r^{[0:m]} (-1)^r A'_{r,0} \sum_t^{[r+1:m]} (-1)^{t-1} A'_{t,1} * \det(A'_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m]}) + \sum_t^{[0:m]} (-1)^t A'_{t,0} \sum_r^{[0:t]} (-1)^r A'_{r,1} * \det(A'_{[0:r]\frown[r+1:t]\frown[t+1:m],[2:m]}))$
   (f) $= -\det(A')$.
2. Otherwise do the following:
   (a) Verify that $i > 1$.
   (b) For r in $[0 : m]$, do the following:
      i. Execute procedure V:26 on $\langle i-1, A_{[0:r]\frown[r+1:m],[1:m]}\rangle$.
      ii. Therefore verify that $\det(A_{[0:r]\frown[r+1:m],[1:m]}) = -\det(A'_{[0:r]\frown[r+1:m],[1:m]})$.
   (c) Therefore using (bii), verify that $\det(A) = \sum_r^{[0:m]} (-1)^r A_{r,0} \cdot \det(A_{[0:r]\frown[r+1:m],[1:m]}) = \sum_r^{[0:m]} (-1)^r A'_{r,0} \cdot (-\det(A'_{[0:r]\frown[r+1:m],[1:m]})) = -\det(A')$.

Procedure V:27

Objective

Choose integers $0 < i < m$. Choose a $m \times m$ matrix, A, such that columns $i-1$ and i are the same. The objective of the following instructions is to show that $\det(A) = 0$.

Implementation

1. Let A' be A with columns $i-1$ and i swapped.
2. Execute procedure V:26 on $\langle A, i\rangle$.
3. Also, verify that $A' = A$.
4. Therefore verify that $\det(A) = \det(A') = -\det(A)$.
5. **Therefore verify that $\det(A) = 0$.**

Procedure V:28

Objective

Choose integers $0 < i < m$. Choose a $m \times m$ matrix, A, such that rows $i-1$ and i are the same. The objective of the following instructions is to show that $\det(A) = 0$.

Implementation

Instructions are analogous to those of procedure V:27.

Procedure V:29

Objective

Choose integers $0 \le i < m$. Choose an integer $-i \le j < m-i$. Choose a $m \times m$ matrix, A. Let A' be A but with column i moved j places. The objective of the following instructions is to show that $\det(A') = (-1)^j \det(A)$.

Implementation

1. Let $B = \langle A \rangle$.
2. For k in $[i : i + j]$, do the following:
   (a) Let $B_{|B|}$ be the result of swapping columns k and $k + 1$ of $B_{|B|-1}$.
   (b) Using procedure V:26, verify that $\det(B_{|B|-1}) = -\det(B_{|B|-2})$.
3. Verify that $A' = B_{|B|-1}$.
4. **Therefore verify that** $\det(A') = \det(B_{|B|-1}) = (-1)^1 \det(B_{|B|-2}) = \cdots = (-1)^j \det(B_0) = (-1)^j \det(A)$**.**

Procedure V:30

Objective

Choose integers $0 \leq i < m$. Choose an integer $-i \leq j < m - i$. Choose a $m \times m$ matrix, A. Let A' be A but with row i moved j places. The objective of the following instructions is to show that $\det(A') = (-1)^j \det(A)$.

Implementation

Instructions are analogous to those of procedure V:29.

Declaration V:18

The notation $C_k(A)$, where A is a $m \times n$ matrix and k is an integer such that $0 \leq k \leq \min(m, n)$, will be used to refer to the $\binom{m}{k} \times \binom{n}{k}$ matrix with the following specification:

1. The rows are labeled by the colexicographically sorted list of increasing length-k sequences whose elements are picked from $[0 : m]$.
2. The columns are labeled by the colexicographically sorted list of increasing length-k sequences whose elements are picked from $[0 : n]$.
3. For each row label I: For each column label J: The entry at position (I, J) is $\det(A_{I,J})$.

Declaration V:19

The notation $A_{\underline{I},\underline{J}}$ will be used to refer to the entry of A with row label I and column label J.

Procedure V:31

Objective

Choose two integers $0 \leq k \leq m$. The objective of the following instructions is to show that $C_k(1_m) = 1_{\binom{m}{k}}$.

Implementation

1. For each row label I of $C_k(1_m)$, for each column label J of $C_k(1_m)$, do the following:
   (a) If $I = J$, then do the following:
      i. Verify that $((1_m)_{I,J})_{i,j} = ((1_m)_{J,J})_{i,j} = (1_m)_{J_i,J_j} = [J_i = J_j] = [i = j]$ for $0 \leq i < k$, for $0 \leq j < k$.
      ii. Therefore verify that $(C_k(1_m))_{\underline{I},\underline{J}} = 1_k$.
      iii. **Therefore verify that** $(C_k(1_m))_{\underline{I},\underline{J}} = \det((1_m)_{I,J}) = \det(1_k) = 1$**.**
   (b) Otherwise, do the following:
      i. Verify that $I \neq J$.
      ii. Let i be the index of an element of I that is not an element of J.
      iii. Now verify that $(1_m)_{I_i,j} = [I_i = j] = 0$, for each j in J.
      iv. Therefore verify that $((1_m)_{I,J})_{i,*} = 0_{1 \times k}$.
      v. **Therefore verify that** $(C_k(1_m))_{\underline{I},\underline{J}} = \det((1_m)_{I,J}) = 0$**.**
2. **Therefore verify that** $C_k(1_m) = 1_{\binom{m}{k}}$**.**

Procedure V:32

Objective

Choose an integer $0 \leq k \leq \min(m, n)$. Choose a $m \times m$ tilt, A, such that the off diagonal entry is the polynomial p at (i, j). Also choose a $m \times n$

matrix, B. The objective of the following instructions is to construct a $\binom{m}{k} \times \binom{m}{k}$ matrix D such that $C_k(AB) = DC_k(B)$.

Implementation

1. Let $D = C_k(1_m) = 1_{\binom{m}{k}}$.
2. Verify that AB equals B, but with its row i having p times B's row j added to it.
3. Go through the row labels, I, of $C_k(AB)$ and do the following:
   (a) If $i \notin I$, then do the following:
      i. Verify that $(AB)_{I,*} = B_{I,*}$.
      ii. Therefore for each column label J, verify that $C_k(AB)_{\underline{I},\underline{J}} = \det((AB)_{I,J}) = \det(B_{I,J}) = C_k(B)_{\underline{I},\underline{J}}$.
      iii. **Therefore verify that** $(C_k(AB))_{\underline{I},*} = (C_k(B))_{\underline{I},*}$**.**
   (b) Otherwise, if $i \in I$, then:
      i. Let I' be I but with an in-place replacement of i by j.
      ii. For each column label J: Using procedure V:24, verify that $C_k(AB)_{\underline{I},\underline{J}} = \det((AB)_{I,J}) = \det(B_{I,J}) + p * \det(B_{I',J})$.
      iii. If $j \in I$, then do the following:
         A. Verify that the sequence I' contains two js.
         B. For each column label J: Using procedure V:28 verify that $\det(B_{I',J}) = 0$.
         C. Therefore for each column label J: verify that $C_k(AB)_{\underline{I},\underline{J}} = \det(B_{I,J}) = C_k(B)_{\underline{I},\underline{J}}$.
         D. **Therefore verify that** $C_k(AB)_{\underline{I},*} = C_k(B)_{\underline{I},*}$**.**
      iv. Otherwise if $j \notin I$, do the following:
         A. Let l be the signed number of places that the j introduced above needs to be moved in order to make I' an increasing sequence.
         B. Let I'' be obtained from I' by moving the integer j in I' by l places.
         C. For each column label J: Using procedure V:30, verify that $\det(B_{I',J}) = (-1)^l \det(B_{I'',J})$.
         D. Therefore for each column label J: Verify that $C_k(AB)_{\underline{I},\underline{J}} = \det(B_{I,J}) + p * \det(B_{I',J}) = \det(B_{I,J}) + (-1)^l p * \det(B_{I'',J})$.
         E. Verify that I'' is a row label of $C_k(B)$.
         F. Therefore for each column label J: Verify that $C_k(AB)_{\underline{I},\underline{J}} = \det(B_{I,J}) + (-1)^l p * \det(B_{I'',J}) = C_k(B)_{\underline{I},\underline{J}} + (-1)^l p * C_k(B)_{\underline{I''},\underline{J}}$.
         G. **Therefore verify that** $(C_k(AB))_{\underline{I},*} = (C_k(B))_{\underline{I},*} + (-1)^l p (C_k(B))_{\underline{I''},*}$**.**
         H. **Set** $D_{\underline{I},\underline{I''}}$ **to** $(-1)^l p$**.**
   (c) **Therefore verify that** $C_k(AB)_{\underline{I},*} = D_{\underline{I},*} C_k(B)$**.**
4. **Therefore verify that** $C_k(AB) = DC_k(B)$**.**
5. **Yield** $\langle D \rangle$**.**

Procedure V:33

Objective

Choose an $m \times n$ diagonal matrix, A. Also choose an $n \times n$ matrix, B. Also choose an integer $0 \le k \le \min(m,n)$. The objective of the following instructions is to construct an $\binom{m}{k} \times \binom{n}{k}$ diagonal matrix D such that $C_k(AB) = DC_k(B)$.

Implementation

1. Let $D = C_k(0_{m \times n}) = 0_{\binom{m}{k} \times \binom{n}{k}}$.
2. Verify that AB equals $B_{[0:\min(m,n)],*}$ with each row i multiplied by $A_{i,i}$.
3. Go through the row labels, I, of $C_k(AB)$ and do the following:
   (a) If $I_k < \min(m,n)$, then do the following:
      i. Verify that every element of I is less than $\min(m,n)$.
      ii. Let $A_0 = A$.

iii. For i in $[0:k]$: Let A_{i+1} equal A_i but with position (I_i, I_i) set to 1.

iv. For each column label J: Repeatedly using procedure V:24, verify that $C_k(AB)_{\underline{I},\underline{J}}$

A. $= \det((AB)_{I,J})$

B. $= \det((A_0B)_{I,J})$

C. $= A_{I_0,I_0} \det((A_1B)_{I,J})$

D. $= A_{I_0,I_0}A_{I_1,I_1} \det((A_2B)_{I,J})$

E. $\vdots$

F. $= A_{I_0,I_0}A_{I_1,I_1} \cdots A_{I_{k-1},I_{k-1}} \det((A_kB)_{I,J})$

G. $= A_{I_0,I_0}A_{I_1,I_1} \cdots A_{I_{k-1},I_{k-1}} \det(B_{I,J})$

H. $= A_{I_0,I_0}A_{I_1,I_1} \cdots A_{I_{k-1},I_{k-1}} C_k(B)_{\underline{I},\underline{J}}$.

v. **Therefore verify that $(C_k(AB))_{\underline{I},*} = A_{I_1,I_1}A_{I_1,I_1} \cdots A_{I_k,I_k} * (C_k(B))_{\underline{I},*}$.**

vi. **Set $D_{\underline{I},\underline{I}}$ to $A_{I_0,I_0}A_{I_1,I_1} \cdots A_{I_{k-1},I_{k-1}}$.**

(b) Otherwise if $I_k \geq \min(m,n)$, then do the following:

i. Using the precondition, verify that $A_{I_k,*} = 0_{1\times n}$.

ii. Therefore verify that $(AB)_{I_k,*} = 0_{1\times n}$.

iii. Therefore verify that $((AB)_{I,*})_{k,*} = 0_{1\times n}$.

iv. Therefore for each column label J: verify that $C_k(AB)_{\underline{I},\underline{J}} = \det((AB)_{I,J}) = 0$.

v. **Therefore verify that $(C_k(AB))_{\underline{I},*}$ is zero.**

(c) **Therefore verify that $C_k(AB)_{\underline{I},*} = D_{\underline{I},*}C_k(B)$.**

4. **Verify that D is diagonal.**
5. **Verify that $C_k(AB) = DC_k(B)$.**
6. **Yield $\langle D \rangle$.**

Procedure V:34

Objective

Choose an integer $0 \leq k \leq \min(m,n)$. Choose a $m \times m$ tilt, A. Also choose a $m \times n$ matrix, B. The objective of the following instructions is to show that $C_k(AB) = C_k(A)C_k(B)$.

Implementation

1. Execute procedure V:32 on matrices A and 1_m and let $\langle D \rangle$ receive.
2. Using procedure V:31, verify that $C_k(A) = C_k(A1_m) = DC_k(1_m) = D1_{\binom{m}{k}} = D$.
3. Execute procedure V:32 on $\langle A, B \rangle$ and let $\langle D' \rangle$ receive.
4. Verify that $D' = D = C_k(A)$.
5. **Therefore verify that $C_k(AB) = D'C_k(B) = C_k(A)C_k(B)$.**

Procedure V:35

Objective

Choose an integer $0 \leq k \leq \min(m,n)$. Choose an $n\times n$ tilt, A. Also choose a $m\times n$ matrix, B. The objective of the following instructions is to show that $C_k(BA) = C_k(B)C_k(A)$.

Implementation

Instructions are analogous to those of procedure V:34.

Procedure V:36

Objective

Choose an integer $0 \leq k \leq \min(m,n)$. Choose an $m \times n$ diagonal matrix, A. Also choose a $n \times n$ matrix, B. The objective of the following instructions is to show that $C_k(AB) = C_k(A)C_k(B)$.

Implementation

Instructions are analogous to those of procedure V:34.

Procedure V:37

Objective

Choose a $m \times n$ matrix, A. Let $D_{-1,-1} = 1$. The objective of the following instructions is to construct a list of $m \times m$ tilts, M, an $m \times n$ diagonal matrix, D, a list of polynomials, v, and a list of $n \times n$ tiltss, N, such that $M_* A N_* = D$, $A = {M^{-1}}_* D {N^{-1}}_*$, and $D_{i,i} = v_i D_{i-1,i-1}$ for i in $[0 : \min(m, n)]$.

Implementation

1. Let D be a copy of A.
2. Let $\langle M, N\rangle$ receive the results of executing procedure V:15 on the pair $\langle m, n\rangle$ and the following procedure:
   (a) Execute procedure V:22 on the matrix D and let $\langle v\rangle$ receive.
3. **Verify that** $D_{i,i} = v_i D_{i-1,i-1}$ **for** i **in** $[0 : \min(m, n)]$**.**
4. **Verify that** $M_* A N_* = D$**.**
5. Hence verify that $A = 1_m A 1_n = {M^{-1}}_* M_* A N_* {N^{-1}}_* = {M^{-1}}_* D {N^{-1}}_*$.
6. **Yield the tuple** $\langle M, D, v, N\rangle$**.**

Procedure V:38

Objective

Choose integers $0 \le k \le \min(m, n, p)$. Choose a $m \times n$ matrix, A. Also choose a $n \times p$ matrix, B. The objective of the following instructions is to show that $C_k(AB) = C_k(A)C_k(B)$.

Implementation

1. Execute procedure V:37 on A and let $\langle M, D, , N\rangle$ receive.
2. Using repeated applications of procedure V:36, verify that $C_k(AB)$
   (a) $= C_k({M^{-1}}_0 \cdots {M^{-1}}_{|M|-1} D {N^{-1}}_0 \cdots {N^{-1}}_{|N|-1} B)$
   (b) $= C_k({M^{-1}}_0) \cdots C_k({M^{-1}}_{|M|-1}) * C_k(D) * C_k({N^{-1}}_0) \cdots C_k({N^{-1}}_{|N|-1}) C_k(B)$
   (c) $= C_k({M^{-1}}_0 \cdots {M^{-1}}_{|M|-1} D {N^{-1}}_0 \cdots {N^{-1}}_{|N|-1}) C_k(B)$
   (d) $= C_k(A)C_k(B)$.

Procedure V:39

Objective

Choose a $m \times m$ matrix, A. Let D be a copy of A. Execute procedure V:22 on D. The objective of the following instructions is to show that $\det(A)$ is the product of the diagonal entries of D.

Implementation

1. Execute procedure V:37 on A and let $\langle M, D, , N\rangle$ receive.
2. Using procedure V:38, verify that $\det(A)$
   (a) $= C_m(A)$
   (b) $= C_m({M^{-1}}_0 \cdots {M^{-1}}_{|M|-1} D {N^{-1}}_0 \cdots {N^{-1}}_{|N|-1})$
   (c) $= C_m({M^{-1}}_0) \cdots C_m({M^{-1}}_{|M|-1}) C_m(D) C_m({N^{-1}}_0) \cdots C_m({N^{-1}}_{|N|-1})$
   (d) $= 1 \cdots 1 C_m(D) 1 \cdots 1 = C_m(D)$
   (e) $= \det(D)$
   (f) $= \prod_r^{[0:m]} D_{r,r}$.

Declaration V:20

The notation A^T, where A is a $m \times n$ matrix, will be used to refer to the $n \times m$ matrix such that ${A^T}_{i,j} = A_{j,i}$ for i in $[0 : n]$, for j in $[0 : m]$.

Procedure V:40

Objective

Choose a $m \times n$ matrix, A, and a $n \times k$ matrix, B. The objective of the following instructions is to show that $B^T A^T = (AB)^T$.

Implementation

1. Verify that $B^T A^T$ and $(AB)^T$ have dimensions $k \times m$.
2. For i in $[0:k]$: For j in $[0:m]$:
   (a) Verify that $(B^T A^T)_{i,j} = \sum_l^{[0:n]} B_{l,i} A_{j,l} = \sum_l^{[0:n]} A_{j,l} B_{l,i} = (AB)_{j,i} = ((AB)^T)_{i,j}$.
3. **Therefore verify that $B^T A^T = (AB)^T$.**

Procedure V:41

Objective

Choose a $m \times m$ matrix, A. The objective of the following instructions is to show that $\det(A^T) = \det(A)$.

Implementation

1. Execute procedure V:37 on A and let $\langle M, D, , N\rangle$ receive.
2. Therefore using procedures procedure V:39 and procedure V:40, verify that $\det(A^T)$
   (a) $= \det((M^{-1}{}_0 \cdots M^{-1}{}_{|M|-1} D N^{-1}{}_0 \cdots N^{-1}{}_{|N|-1})^T)$
   (b) $= \det((N^{-1}{}_{|N|-1})^T \cdots (N^{-1}{}_0)^T D^T (M^{-1}{}_{|M|-1})^T \cdots (M^{-1}{}_0)^T)$
   (c) $= \det(D^T)$
   (d) $= \det(D)$
   (e) $= \det(M^{-1}{}_0 \cdots M^{-1}{}_{|M|-1} D N^{-1}{}_0 \cdots N^{-1}{}_{|N|-1})$
   (f) $= \det(A)$.

Procedure V:42

Objective

Choose a $m \times n$ matrix, A, and an integer $0 \leq k \leq \min(m, n)$. The objective of the following instructions is to show that $C_k(A)^T = C_k(A^T)$.

Implementation

1. For each row label I of $C_k(A^T)$, do the following:
   (a) For each column label J of $C_k(A^T)$, do the following:
      i. Using procedure V:41, verify that $(C_k(A^T))_{\underline{I},\underline{J}} = \det((A^T)_{I,J}) = \det(A_{J,I}) = (C_k(A))_{\underline{J},\underline{I}}$.
2. **Therefore verify that $(C_k(A))^T = (C_k(A^T))$.**

Procedure V:43

Objective

Choose a $m \times n$ rational matrix, A, and a $m \times p$ rational matrix, B. Execute procedure V:37 on A and let $\langle M, D, , N\rangle$ receive the result. If the indices of the rows of D that are entirely zero are also the indices of the rows of $M_* B$ that are entirely zero, then the objective of the following instructions is to construct a $n \times p$ rational matrix E such that $AE = B$.

Implementation

1. Verify that $A = M^{-1}{}_* D N^{-1}{}_*$.
2. Verify that $M^{-1}{}_*$, D, and $N^{-1}{}_*$ are rational matrices.
3. Let C be an $n \times p$ matrix with its i^{th} row given as follows:
   (a) If $D_{i,i} \neq 0$, then do the following:
      i. Let row i be row i of $M_* B$ divided by $D_{i,i}$.
   (b) Otherwise, do the following:
      i. **Choose p rational numbers to fill up the row.**
4. Verify that $DC = M_* B$.
5. Let E be $N_* C$.
6. **Therefore using procedure V:17, verify that $AE = M^{-1}{}_* D N^{-1}{}_* E = M^{-1}{}_* D N^{-1}{}_* N_* C = M^{-1}{}_* D 1_n C = M^{-1}{}_* DC = M^{-1}{}_* M_* B = 1_m B = B$.**

7. **Yield the tuple $\langle E \rangle$.**

Declaration V:21

The notation $A\backslash B$ will be used to refer to the result yielded by executing procedure V:43 on $\langle A, B \rangle$.

Procedure V:44

Objective

Choose a $m \times n$ rational matrix, A, and a $p \times n$ rational matrix, B. Execute procedure V:37 on A and let $\langle M, D, , N \rangle$ receive the result. If the indices of the columns of D that are entirely zero are also the indices of the columns of BN_* that are entirely zero, then the objective of the following instructions is to construct a $p \times m$ rational matrix E such that $EA = B$.

Implementation

Instructions are analogous to those of procedure V:43.

Declaration V:22

The notation A/B will be used to refer to the result yielded by executing procedure V:44 on $\langle A, B \rangle$.

Procedure V:45

Objective

Choose a $m \times n$ rational matrix, A, a $n \times p$ rational matrix, E, and a $m \times p$ rational matrix, B such that $AE = B$. Execute procedure V:37 on A and let $\langle M, D, , N \rangle$ receive the result. If the indices of the rows of D that are entirely zero are not also the indices of the rows of M_*B that are entirely zero, then the objective of the following instructions is to show that $0 \neq 0$.

Implementation

1. Verify that $M^{-1}{}_*DN^{-1}{}_*E = AE = B$.
2. Therefore verify that $DN^{-1}{}_*E = M_*B$.
3. Let i be an integer such that $D_{i,*}$ is zero and yet $(M_*B)_{i,*}$ is not zero.
4. Verify that $D_{i,*} = D_{i,*}N^{-1}{}_*E = (DN^{-1}{}_*E)_{i,*} = (M_*B)_{i,*}$.
5. Let j be an integer such that $(M_*B)_{i,j} \neq 0$.
6. **Now verify that $0 = D_{i,j} = (M_*B)_{i,j} \neq 0$.**

Procedure V:46

Objective

Choose a $p \times m$ rational matrix, E, a $m \times n$ rational matrix, A, and a $p \times n$ rational matrix, B such that $EA = B$. Execute procedure V:37 on A and let $\langle M, D, , N \rangle$ receive the result. If the indices of the columns of D that are entirely zero are not also the indices of the columns of BN_* that are entirely zero, then the objective of the following instructions is to show that $0 \neq 0$.

Implementation

Instructions are analogous to those of procedure V:45.

Procedure V:47

Objective

Choose two $m \times m$ rational matrices, A and B, such that $AB = 1_m$. The objective of the following instructions is to show that either $0 = 1$ or $BA = 1_m$.

Implementation

1. Execute procedure V:37 on B and let $\langle M, D, , N \rangle$ receive the result.
2. Verify that $B = M^{-1}{}_*DN^{-1}{}_*$.
3. If D has a zero on its diagonal, then do the following:

   (a) Using procedure V:39, verify that $\det(1_m) = \det(AB) = \det(A)\det(B) = \det(A)\det(D) = \det(A) * 0 = 0$.

(b) Also verify that $\det(1_m) = 1^m = 1$.

(c) Therefore verify that $0 = 1$.

(d) **Abort procedure.**

4. Otherwise do the following:

(a) Verify that D does not have a zero on its diagonal.

(b) Verify that $B\backslash 1_m = 1_m(B\backslash 1_m) = AB(B\backslash 1_m) = A(B(B\backslash 1_m)) = A1_m = A$.

(c) **Therefore verify that $BA = B(B\backslash 1_m) = 1_m$.**

Procedure V:48

Objective

Choose an $m\times m$ matrix, M, and an $m\times m$ rational matrix, B. The objective of the following instructions is to construct a $m\times m$ matrix, Q, and a $m\times m$ rational matrix, R, such that $M = (\lambda 1_m - B)Q + R$.

Implementation

1. Let $M_0\lambda^b + M_1\lambda^{b-1} + \cdots + M_b\lambda^0 = M$, where the M_i are $m \times m$ rational matrices.
2. Now let $R = B^b M_0 + B^{b-1}M_1 + \cdots + B^0 M_b$.
3. Let $Q = \sum_k^{[1:b]}(\lambda^{k-1}1_m B^0 + \lambda^{k-2}1_m B^1 + \cdots + \lambda^0 1_m B^{k-1})M_k$.
4. Verify that $M - R = (\lambda 1_m - B)\sum_k^{[1:b]}(\lambda^{k-1}1_m B^0 + \lambda^{k-2}1_m B^1 + \cdots + \lambda^0 1_m B^{k-1})M_k = (\lambda 1_m - B)Q$.
5. **Verify that $M = (\lambda 1_m - B)Q + R$.**
6. **Yield the tuple $\langle Q, R\rangle$.**

Procedure V:49

Objective

Choose an $m\times m$ matrix, M, and an $m\times m$ rational matrix, B. The objective of the following instructions is to construct a $m\times m$ matrix, Q, and a $m\times m$ rational matrix, R, such that $M = Q(\lambda 1_m - B) + R$.

Implementation

The instructions are analogous to those of procedure V:48.

Procedure V:50

Objective

Choose two $m \times m$ rational matrices, B, A, and two lists of $m \times m$ tilts such that $\lambda 1_m - B = M(\lambda 1_m - A)N$. The objective of the following instructions is to either show that $0 = 1$ or to construct $m\times m$ rational matrices R_1 and R_3 such that $1_m = R_1 R_3$ and $B = R_1 A R_3$.

Implementation

1. Verify that $(\lambda 1_m - B)N^{-1} = M(\lambda 1_m - A)NN^{-1} = M(\lambda 1_m - A)1_m = M(\lambda 1_m - A)$.
2. Execute procedure V:49 on $\langle M, B\rangle$ and let $\langle Q_1, R_1\rangle$ receive.
3. Verify that $M = (\lambda 1_m - B)Q_1 + R_1$.
4. Execute procedure V:49 on $\langle N^{-1}, A\rangle$ and let $\langle Q_2, R_2\rangle$ receive.
5. Verify that $N^{-1} = Q_2(\lambda 1_m - A) + R_2$.
6. By substituting M and N^{-1} into (2), verify that $(\lambda 1_m - B)(Q_2(\lambda 1_m - A) + R_2) = ((\lambda 1_m - B)Q_1 + R_1)(\lambda 1_m - A)$.
7. By rearranging both sides, verify that $(\lambda 1_m - B)(Q_2 - Q_1)(\lambda 1_m - A) = R_1(\lambda 1_m - A) - (\lambda 1_m - B)R_2$.
8. By equating the coefficients of different powers of λ both sides, verify that $Q_2 - Q_1 = 0_{m\times m}$.
9. Verify that $R_1(\lambda 1_m - A) - (\lambda 1_m - B)R_2 = (\lambda 1_m - B)(Q_2 - Q_1)(\lambda 1_m - A) = (\lambda 1_m - B)0_{m\times m}(\lambda 1_m - A) = 0_{m\times m}$.
10. Therefore by adding $(\lambda 1_m - B)R_2$ to both sides, verify that $\lambda R_1 - R_1 A = R_1(\lambda 1_m - A) = (\lambda 1_m - B)R_2 = \lambda R_2 - BR_2$.
11. By equating the coefficients of λ on both sides, verify that $R_1 = R_2$.
12. Therefore verify that $R_1 A = BR_1$.

13. Execute procedure V:49 on $\langle M^{-1}, A\rangle$ and let $\langle Q_3, R_3\rangle$ receive.
14. Verify that $M^{-1} = (\lambda 1_m - A)Q_3 + R_3$.
15. Verify that $1_m = MM^{-1} = ((\lambda 1_m - B)Q_1 + R_1)M^{-1} = (\lambda 1_m - B)Q_1M^{-1} + R_1M^{-1} = (\lambda 1_m - B)Q_1M^{-1} + R_1(\lambda I - A)Q_3 + R_1R_3 = (\lambda 1_m - B)Q_1M^{-1} + (\lambda I - B)R_1Q_3 + R_1R_3 = (\lambda 1_m - B)(Q_1M^{-1} + R_1Q_3) + R_1R_3$.
16. By equating the powers of λ on both sides, verify that $Q_1M^{-1} + R_1Q_3 = 0$.
17. By substituting zero for $Q_1M^{-1} + R_1Q_3$, **verify that** $1_m = (\lambda 1_m - B)0_{m\times m} + R_1R_3 = R_1R_3$**.**
18. **Therefore using procedure V:47, verify that** $R_3R_1 = 1_m$**.**
19. **Also, verify that** $B = B1_m = BR_1R_3 = R_1AR_3$**.**
20. **Yield the pair** (R_1, R_3)**.**

Procedure V:51

Objective

Choose a $m \times n$ matrix, A. Choose two integers $0 \le i, j < m$ such that $i \ne j$. The objective of the following instructions is to negate row i and swap it with row j using only elementary row operations.

Implementation

1. Let A be our working matrix.
2. Subtract row j from row i.
3. Add row i to row j.
4. Subtract row j from row i.
5. **Verify that the** i^{th} **row has been negated and swapped with the** j^{th} **row.**

Procedure V:52

Objective

Choose a $m \times n$ matrix, A. Choose two integers $0 \le i, j < n$ such that $i \ne j$. The objective of the following instructions is to negate column i and swap it with row j using only elementary column operations.

Implementation

The instructions are analogous to those of procedure V:51.

Procedure V:53

Objective

Choose an $m \times n$ diagonal matrix, A. Choose two integers $0 \le i, j < \min(m, n)$ such that $i \ne j$. The objective of the following instructions is to swap $B_{i,i}$ and $B_{j,j}$ using only elementary row and column operations.

Implementation

1. Let A be our working matrix.
2. Use procedure V:52 to negate the i^{th} row and swap it with the j^{th} row.
3. Use procedure V:52 to negate the i^{th} column and swap it with the j^{th} column.
4. **Therefore, overall verify that** $B_{i,i}$ **and** $B_{j,j}$ **have been swapped.**

Procedure V:54

Objective

Choose an $m \times n$ diagonal matrix, A. Choose two integers $0 \le i, j < \min(m, n)$ such that $i \ne j$. Choose a rational $k \ne 0$. The objective of the following instructions is to multiply $B_{i,i}$ by k and $B_{j,j}$ by $\frac{1}{k}$ using only elementary row and column operations.

Implementation

1. Let A be our working matrix.
2. Add k times row i to row j.
3. Subtract $\frac{1}{k}$ times row j from row i.
4. Add k times row i to row j.

5. Verify that the i^{th} row has been scaled by k, the j^{th} row by $-\frac{1}{k}$, and that both these rows are swapped.
6. Use procedure V:52 to negate the i^{th} row and swap it with the j^{th} row.
7. **Therefore, overall verify that $B_{i,i}$ has been multiplied by k, and $B_{j,j}$ by $\frac{1}{k}$.**

Procedure V:55

Objective

Choose a $m \times m$ rational matrix, A. Execute procedure V:22 on the polynomial matrix $\lambda I - A$ and let $\langle B \rangle$ be the result. The objective of the following instructions is to show that either none of the diagonal entries of B are equal to zero, or $1 = 0$.

Implementation

1. Verify that $\det(\lambda I - A)$ is a monic polynomial of degree m.
2. Therefore using procedure V:39, verify that $\det(B) = \det(\lambda I - A)$.
3. Therefore verify that $\det(B)$ is a monic polynomial of degree m.
4. If any of the diagonal entries of B equal zero, then do the following:
   (a) Verify that $\det(B) = B_{0,0}B_{1,1}\cdots B_{m-1,m-1} = 0$.
   (b) Therefore using (3) and (4a), verify that $1 = 0$.
   (c) **Abort procedure.**
5. Otherwise do the following:
   (a) **Verify that none of the diagonal entries of B equal zero.**

Procedure V:56

Objective

Choose a positive integer m and an $m \times m$ rational matrix, A. Execute procedure V:37 on the polynomial matrix $\lambda 1_m - A$ and let $\langle , B, v, \rangle$ be the result. The objective of the following instructions is to either show that $0 < 0$ or to construct an integer a such that $\sum_i^{[a:m]} \deg(B_{i,i}) = m$, $\deg(B_{i,i}) > 0$ for i in $[a : m]$, and $\deg(B_{i,i}) = 0$ for i in $[0 : a]$.

Implementation

1. Execute procedure V:55 on A.
2. If $\deg(B_{i,i}) = 0$ for i in $[0 : m]$, then do the following:
   (a) Verify that $\det(\lambda 1_m - A) = \det(B) = B_{0,0}B_{1,1}\cdots B_{m-1,m-1}$.
   (b) **Therefore verify that $0 < m = \deg(\det(\lambda 1_m - A)) = \deg(B_{0,0}B_{1,1}\cdots B_{m-1,m-1}) = 0 + 0 + \cdots + 0 = 0$.**
   (c) **Abort procedure.**
3. Otherwise do the following:
   (a) Let $0 \le a < m$ be the least integer such that $\deg(B_{a,a}) > 0$.
   (b) **Verify that $\deg(B_{i,i}) = 0$ for i in $[0 : a]$.**
   (c) **Verify that $\sum_i^{[a:m]} \deg(B_{i,i}) = \sum_i^{[0:m]} \deg(B_{i,i}) = \deg(B_{0,0}B_{1,1}\cdots B_{m-1,m-1}) = \deg(\det(B)) = \deg(\lambda 1_m - A) = m$.**
   (d) For i in $[a + 1 : m]$, do the following:
      i. Verify that $B_{i,i} = u_i B_{i-1,i-1}$.
      ii. Verify that $B_{i,i} \neq 0$.
      iii. Therefore verify that $u_i \neq 0$.
      iv. **Therefore verify that $\deg(B_{i,i}) = \deg(u_i B_{i-1,i-1}) \ge \deg(B_{i-1,i-1}) > 0$.**
   (e) **Yield the tuple $\langle a \rangle$.**

Declaration V:23

The notation $(e_i)_{k\times 1}$ will be used to refer to the $k \times 1$ rational matrix such that its i^{th} entry, 1, is the only non-zero entry.

Declaration V:24

The notation $\mathrm{mat}_t(p)$ will be used as a shorthand for $\sum_j^{[0:t]} p_j e_j$.

Declaration V:25

The notation comp(p), where $p \neq 0$ is a monic polynomial such that $\deg(p) > 0$, will be used as a shorthand for the $\deg(p) \times \deg(p)$ rational matrix of the following constitution:

1. Its first $\deg(p) - 1$ columns equal the last $\deg(p) - 1$ columns of 1_k.
2. Its last column is $-\text{mat}_{\deg(p)}(p)$.

Procedure V:57

Objective

Choose a monic polynomial, p such that $\deg(p) > 0$. Let $k = \deg(p)$. Choose a $k \times k$ matrix, D, such that $D = \lambda 1_k - \text{comp}(p)$. The objective of the following instructions is to transform D into $\text{diag}(1, \cdots, 1, p)$ by a sequence of elementary operations.

Implementation

1. Let the matrix D be our working matrix.
2. For i in $[k : 1]$, add λ times row i to row $i - 1$.
3. Verify that D's first $k-1$ columns are now the last $k - 1$ columns of -1_k.
4. Verify that D's last column is p followed by some other polynomials.
5. For i in $[1 : k]$, subtract $D_{i,k-1}$ times column $i - 1$ from column $k - 1$.
6. Verify that D's last column is now p followed by zeros.
7. For i in $[1 : k]$, negate row $i - 1$ and exchange it with row i using procedure V:52.
8. **Therefore verify that $D = \text{diag}(1, \cdots, 1, p)$.**

Procedure V:58

Objective

Choose a positive integer m and an $m \times m$ rational matrix, A. Execute procedure V:15 on the polynomial matrix $\lambda 1_m - A$ and let $\langle , B, , \rangle$ receive the result. Execute procedure V:56 on A and let $\langle a \rangle$ receive the result. Let $E_i = \text{comp}(\text{mon}(B_{a+i,a+i}))$ for i in $[0 : m - a]$. The objective of the following instructions is to first show that $\text{cols}(\text{diag}(E)) = m$, and second to apply a sequence of elementary operations on $\lambda 1_m - \text{diag}(E)$ to obtain the matrix B.

Implementation

1. Verify that the diagonal of B comprises a rationals followed by $B_{a,a}, B_{a+1,a+1}, \cdots, B_{m-1,m-1}$.
2. **Using procedure V:57, verify that** $\text{cols}(\text{diag}(E)) = \sum_i^{[0:|E|]} \text{cols}(E_i) = \sum_i^{[0:|E|]} \text{cols}(\text{comp}(\text{mon}(B_{a+i,a+i}))) = \sum_i^{[0:|E|]} \deg(\text{mon}(B_{a+i,a+i})) = \sum_i^{[0:m-a]} \deg(B_{a+i,a+i}) = \sum_i^{[a:m]} \deg(B_{i,i}) = m$**.**
3. Let $F = \lambda 1_m - \text{diag}(E)$.
4. Now for i in $[0 : |E|]$:
   (a) Let $j = \sum_r^{[0:i]} \text{cols}(E_r)$.
   (b) Let $k = j + \text{cols}(E_i)$.
   (c) Apply procedure V:57 on the tuple $\langle \text{mon}(B_{a+i,a+i}), F_{[j:k],[j:k]} \rangle$.
5. Now verify that F is an $m \times m$ diagonal rational matrix.
6. Also verify that the diagonal of F comprises $\text{mon}(B_{a,a}), \text{mon}(B_{a+1,a+1}), \cdots, \text{mon}(B_{m-1,m-1})$ and a 1s.
7. Rearrange the diagonal of F so that $\text{mon}(B_{i,i})$ is at the i^{th} position on the diagonal for i in $[a : m]$ by doing pairwise swaps. In general, swap the i^{th} and j^{th} diagonal entries using procedure V:53.
8. For i in $[0 : m - 1]$, do the following:
   (a) Let $k = \frac{(B_{i,i})_{\deg(B_{i,i})}}{(F_{i,i})_{\deg(F_{i,i})}}$.
   (b) Scale $B_{i,i}$ by k and $B_{i+1,i+1}$ by $\frac{1}{k}$ using procedure V:54.
   (c) Now verify that $F_{i,i} = B_{i,i}$.
9. Now verify that $\det(F)_m = \det(\lambda 1_m - \text{diag}(E))_m = 1 = \det(\lambda 1_m - A)_m = \det(B)_m$.
10. Therefore verify that $(F_{m,m})_{\deg(F_{m,m})}$

(a) $= \frac{\det(F)_m}{(\det(F_{[1:m],[1:m]}))_{m-\deg(F_{m,m})}}$

(b) $= \frac{\det(B)_m}{(\det(B_{[1:m],[1:m]}))_{m-\deg(B_{m,m})}}$

(c) $= (B_{m,m})_{\deg(B_{m,m})}$.

11. Therefore verify that $F_{m,m} = B_{m,m}$.
12. **Therefore verify that $F = B$.**

Procedure V:59

Objective

Choose a $m \times m$ rational matrix, A. Execute procedure V:56 on A and let $\langle a\rangle$ receive the result. Let $E_i = \text{comp}(\text{mon}(B_{a+i,a+i}))$ for i in $[0 : m-a]$. The objective of the following instructions is to either show that $0 = 1$ or to construct $m \times m$ rational matrices R, T such that $A = R\,\text{diag}(E)T$, $RT = 1_m$, and $TR = 1_m$.

Implementation

1. Execute procedure V:37 on the polynomial matrix $\lambda 1_m - A$ and let $\langle P, B, , Q\rangle$ be the result.
2. Verify that $P_*(\lambda 1_m - A)Q_* = B$.
3. Verify that $\lambda 1_m - A = P^{-1}{}_* B Q^{-1}{}_*$.
4. Let Z be a variant of procedure V:37 where every occurence of procedure V:22 in its instructions is replaced with procedure V:58, and where every mention of v is ignored.
5. Execute procedure Z on the matrix $\lambda 1_m - \text{diag}(E)$ and let $\langle M, , , N\rangle$ receive the result.
6. Verify that $M_*(\lambda 1_m - \text{diag}(E))N_* = B$.
7. Verify that $\lambda 1_m - A = P^{-1}{}_* B Q^{-1}{}_* = P^{-1}{}_* M(\lambda 1_m - \text{diag}(E))NQ^{-1}{}_*$.
8. Execute procedure V:50 on the matrices $\langle A, P^{-1}M, \text{diag}(E), NQ^{-1}\rangle$. Let the tuple $\langle R, T\rangle$ be the result.
9. **Verify that $A = R\,\text{diag}(E)T$.**
10. **Verify that $RT = 1_m$.**
11. **Verify that $TR = 1_m$.**
12. **Yield the tuple $\langle R, E, T\rangle$.**

Procedure V:60

Objective

Choose two polynomials a, b and an $m \times m$ matrix C such that $a = b$. The objective of the following instructions is to show that $\Lambda(a, C) = \Lambda(b, C)$.

Implementation

Implementation is analogous to that of procedure II:34.

Procedure V:61

Objective

Choose two polynomials a, b and an $m \times n$ matrix C. The objective of the following instructions is to show that $\Lambda(a + b, C) = \Lambda(a, C) + \Lambda(b, C)$.

Implementation

Implementation is analogous to that of procedure II:39.

Procedure V:62

Objective

Choose a polynomial a and an $m \times m$ matrix B. The objective of the following instructions is to show that $\Lambda(-a, B) = -\Lambda(a, B)$.

Implementation

Implementation is analogous to that of procedure II:45.

Procedure V:63

Objective

Choose two polynomials a, b and an $m \times m$ matrix C. The objective of the following instructions is to show that $\Lambda(ab, C) = \Lambda(a, C)\Lambda(b, C)$.

Implementation

Implementation is analogous to that of procedure II:48.

Procedure V:64

Objective

Choose a polynomial, r, and $m \times m$ rational matrices, R, A, S such that $SR = 1_m$. The objective of the following instructions is to show that $\Lambda(r, RAS) = R\Lambda(r, A)S$.

Implementation

1. Verify that $\Lambda(r, RAS)$
   (a) $= \sum_j^{[0:|r|]} r_j (RAS)^j$
   (b) $= \sum_j^{[0:|r|]} r_j RA^j S$
   (c) $= R(\sum_j^{[0:|r|]} r_j A^j)S$
   (d) $= R\Lambda(r, A)S$.

Procedure V:65

Objective

Choose a list of $m \times m$ rational matrices, A, and a polynomial, r. The objective of the following instructions is to show that $\Lambda(r, \mathrm{diag}(A)) = \mathrm{diag}(\Lambda(r, A))$.

Implementation

1. For $i = 0$ up to $i = t$, by repeated applications of procedure V:21, verify that $\mathrm{diag}(A)^i$ evaluates to $\mathrm{diag}(A^i)$.
2. Therefore verify that $\Lambda(r, \mathrm{diag}(A))$
   (a) $= \sum_j^{[0:|r|]} r_j \,\mathrm{diag}(A)^j$
   (b) $= \sum_j^{[0:|r|]} r_j \,\mathrm{diag}(A^j)$
   (c) $= \sum_j^{[0:|r|]} \mathrm{diag}(r_j A^j)$
   (d) $= \mathrm{diag}(\sum_j^{[0:|r|]} r_j A^j)$
   (e) $= \mathrm{diag}(\Lambda(r, A))$.

Procedure V:66

Objective

Choose a $m \times m$ rational matrix, A, and a polynomial, r. Execute procedure V:59 on the matrix A and let the tuple $\langle R_1, E, R_3\rangle$ receive the result. The objective of the following instructions is to show that $\Lambda(r, A) = R_1 \,\mathrm{diag}(\Lambda(r, E))R_3$.

Implementation

1. Verify that $R_3 R_1 = 1_m$.
2. Using procedure V:64, verify that $\Lambda(r, A) = \Lambda(r, R_1 \,\mathrm{diag}(E)R_3) = R_1\Lambda(r, \mathrm{diag}(E))R_3$.
3. Using procedure V:65, verify that $\Lambda(r, \mathrm{diag}(E)) = \mathrm{diag}(\Lambda(r, E))$.
4. **Therefore verify that** $\Lambda(r, A) = R_1 \,\mathrm{diag}(\Lambda(r, E))R_3$**.**

Procedure V:67

Objective

Choose a monic polynomial $p \neq 0$ such that $\deg(p) > 0$. The objective of the following instructions is to show that $\Lambda(p, \mathrm{comp}(p)) = 0_{\deg(p)\times\deg(p)}$.

Implementation

1. Let $G = \mathrm{comp}(p)$.
2. For i in $[0 : \deg(p)]$, verify that $G^i e_0 = G^{i-1}e_1 = \cdots = G^0 e_i = e_i$.
3. Therefore, for $i \in [0 : \deg(p)]$, do the following:
   (a) Using (1), verify that $\Lambda(p, G)e_i$
      i. $= (\sum_j^{[0:|p|]} p_j G^j)e_i$
      ii. $= (\sum_j^{[0:|p|]} p_j G^j)G^i e_0$
      iii. $= G^i(GG^{\deg(p)-1} + \sum_j^{[0:\deg(p)]} p_j G^j)e_0$
      iv. $= G^i(Ge_{\deg(p)-1} + \sum_j^{[0:\deg(p)]} p_j e_j)$

v. $= G^i 0_{\deg(p)\times 1}$

vi. $= 0_{\deg(p)\times 1}$.

4. **Therefore verify that** $\Lambda(p, \mathrm{comp}(p)) = \Lambda(p, G) = 0_{\deg(p)\times\deg(p)}$**.**

Declaration V:26

The notation last_A, where A is an $m \times m$ rational matrix, will be used as a shorthand for the polynomial yielded by executing the following instructions:

1. Execute procedure V:37 on the polynomial matrix $\lambda 1_m - A$ and let the tuple $\langle , B, , \rangle$ receive the result.
2. Yield $\langle B_{m-1,m-1} \rangle$.

Procedure V:68

Objective

Choose a $m \times m$ rational matrix, A. The objective of the following instructions is to show that either $1 = 0$ or $\mathrm{last}_A \neq 0$.

Implementation

1. Execute procedure V:55 on A.
2. **Therefore verify that** $\mathrm{last}_A \neq 0$**.**

Procedure V:69

Objective

Choose a $m \times m$ rational matrix, A. The objective of the following instructions is to either show that $0 < 0$ or to show that $\Lambda(\mathrm{last}_A, A) = 0_{m\times m}$.

Implementation

1. Execute procedure V:37 on the matrix A and let the tuple $\langle M, B, v, N \rangle$ receive the result.
2. Execute procedure V:56 on A and let $\langle a \rangle$ receive.
3. Execute procedure V:59 on A and let $\langle R, E, T \rangle$ receive.
4. For j in $[0 : |E|]$:
   (a) Verify that $E_j = \mathrm{comp}(\mathrm{mon}(B_{a+j,a+j}))$.
   (b) Verify that $\mathrm{last}_A = B_{m-1,m-1} = B_{a+j,a+j} \prod_r^{[a+j+1:m]} v_r$.
   (c) Let $k = \deg(\mathrm{mon}(B_{a+j,a+j}))$.
   (d) Therefore using procedure V:67 verify that $\Lambda(\mathrm{last}_A, E_j) = \Lambda(B_{m-1,m-1}, E_j) = \Lambda(B_{a+j,a+j}, \mathrm{comp}(\mathrm{mon}(B_{a+j,a+j}))) \prod_r^{[a+j+1:m]} \Lambda(v_r, E_j) = 0_{k\times k} \prod_r^{[a+j+1:m]} \Lambda(v_r, E_j) = 0_{k\times k}$.
5. **Therefore using procedure V:66 verify that** $\Lambda(\mathrm{last}_A, A) = R\,\mathrm{diag}(\Lambda(\mathrm{last}_A, E))T = R\,\mathrm{diag}(\Lambda(B_{m-1,m-1}, E))T = R 0_{m\times m} T = 0_{m\times m}$**.**

Procedure V:70

Objective

Choose a monic polynomial p such that $\deg(p) > 0$. Choose a polynomial $g \neq 0$ such that $\deg(g) < \deg(p)$. The objective of the following instructions is to show that $\Lambda(g, \mathrm{comp}(p)) \neq 0_{\deg(p)\times\deg(p)}$.

Implementation

1. Let $G = \mathrm{comp}(p)$.
2. Therefore using declaration V:25, verify that $\Lambda(g, G)e_0 = (\sum_j^{[0:\deg(g)+1]} g_j G^j)e_0 = \sum_j^{[0:\deg(g)+1]} g_j e_j \neq 0_{\deg(p)\times 1}$.
3. **Therefore verify that** $\Lambda(g, G) \neq 0_{\deg(p)\times\deg(p)}$**.**

Procedure V:71

Objective

Choose a polynomial g and a monic polynomial p such that $\deg(p) = \deg(g) > 0$ and $\Lambda(g, \mathrm{comp}(p)) = 0_{\deg(g)\times\deg(g)}$. The objective of the following instructions is to show that $g = g_{\deg(g)} p$.

Implementation

1. Let $G = \mathrm{comp}(p)$.
2. Using declaration V:25, verify that $0_{\deg(g)\times 1} = \Lambda(g,G)e_0 = (\sum_j^{[0:|g|]} g_j G^j)e_0 = g_{\deg(g)} G e_{\deg(g)-1} + \sum_j^{[0:\deg(g)]} g_j e_j$.
3. Therefore for i in $[0 : \deg(g)]$, do the following:
   (a) Verify that $0 = (g_{\deg(g)} G e_{\deg(g)-1} + \sum_j^{[0:\deg(g)]} g_j e_j)_{i,0}$.
   (b) Therefore using declaration V:25, verify that $-g_{\deg(g)} p_i + g_i = 0$.
   (c) Therefore verify that $g_i = g_{\deg(g)} p_i$.
4. **Therefore verify that $g = g_{\deg(g)} p$.**

Procedure V:72

Objective

Choose a $m \times m$ rational matrix, A. Choose a polynomial $p \neq 0$, such that $\Lambda(p, A) = 0_{m\times m}$. The objective of the following instructions is to either show that $0 \neq 0$ or to construct a polynomial f such that $p = f \,\mathrm{last}_A$.

Implementation

1. Let F be the 1×2 matrix $\langle\langle p, \mathrm{last}_A\rangle\rangle$.
2. Execute procedure V:37 on F and let $\langle M, D, , N\rangle$ receive the result.
3. Verify that $D_{0,0} \neq 0$.
4. Let $g = D_{0,0}$.
5. Verify that $F = M^{-1}{}_* D N^{-1}{}_* = D N^{-1}{}_*$.
6. Verify that $\mathrm{last}_A = F_{0,1} = D_{0,0} N^{-1}{}_{*0,1} + D_{0,1} N^{-1}{}_{*1,1} = D_{0,0} N^{-1}{}_{*0,1} = g N^{-1}{}_{*0,1}$.
7. Therefore verify that $N^{-1}{}_{*0,1} \neq 0$.
8. Let $u = \deg(\mathrm{last}_A)$.
9. Now verify that $u = \deg(\mathrm{last}_A) = \deg(D_{0,0} N^{-1}{}_{*0,1}) \geq \deg(D_{0,0}) = \deg(g)$.
10. Verify that $D = M_* F N_* = F N_*$.
11. Therefore verify that $g = D_{0,0} = N_{*0,0} p + N_{*1,0} \,\mathrm{last}_A$.
12. Therefore using procedure V:67, verify that $\Lambda(g, A) = \Lambda(N_{*0,0}, A)\Lambda(p, A) + \Lambda(N_{*1,0}, A)\Lambda(\mathrm{last}_A, A) = \Lambda(N_{*0,0}, A)0_{m\times m} + \Lambda(N_{*1,0}, A)0_{m\times m} = 0_{m\times m}$.
13. Execute procedure V:59 on the matrix A and let the tuple $\langle R_1, E, R_3\rangle$ receive the result.
14. Using procedure V:66, and procedure V:59, verify that $\mathrm{diag}(\Lambda(g, E)) = 1_m \,\mathrm{diag}(\Lambda(g, E))1_m = R_3 R_1 \,\mathrm{diag}(\Lambda(g, E))R_3 R_1 = R_3 \Lambda(g, A)R_1 = R_3 0_{m\times m} R_1 = 0_{m\times m}$.
15. Let $G = \mathrm{comp}(\mathrm{mon}(\mathrm{last}_A))$.
16. Verify that $\Lambda(g, G) = \Lambda(g, E_{|E|-1}) = \mathrm{diag}(\Lambda(g, E))_{[m-u:m],[m-u:m]} = 0_{u\times u}$.
17. If $\deg(g) < u$, then:
    (a) Using procedure V:70, verify that $\Lambda(g, G) \neq 0_{u\times u}$.
    (b) **Therefore using (16), verify that $0_{u\times u} = \Lambda(g, G) \neq 0_{u\times u}$.**
    (c) **Abort procedure.**
18. Otherwise, do the following:
    (a) Verify that $\deg(g) = u$.
    (b) Using procedure V:71, verify that $g = g_{\deg(g)} \,\mathrm{last}_A$.
    (c) **Therefore verify that $p = F_{0,0} = D_{0,0} N^{-1}{}_{*0,0} + D_{0,1} N^{-1}{}_{*1,0} = N^{-1}{}_{*0,0} g + N^{-1}{}_{*1,0} * 0 = N^{-1}{}_{*0,0} g = N^{-1}{}_{*0,0} g_{\deg(g)} \,\mathrm{last}_A$.**
    (d) **Yield the tuple $\langle N^{-1}{}_{*0,0} g_{\deg(g)}\rangle$.**

Procedure V:73

Objective

Choose an $m \times n$ rational matrix, A, and an $n \times m$ rational matrix, B, such that $AB = 1_m$. The objective of the following instructions is to show that either $0 = 1$ or every column of B is non-zero.

Implementation

1. If any column i of B, Be_i, is equal to zero, then:
   (a) Verify that $0_{n\times 1} = A0_{n\times 1} = A(Be_i) = (AB)e_i = 1_m e_i = e_i$.
   (b) **Therefore verify that 0=1.**
   (c) **Abort procedure.**

Procedure V:74

Objective

Choose a $m \times m$ rational matrix, A. Choose a polynomial p such that $p \neq 0$, $\Lambda(p, A) = 0$, and $\deg(p) < \deg(\mathrm{last}_A)$. The objective of the following instructions is to show that $0 < 0$.

Implementation

1. Execute procedure V:72 on A and p and let f receive.
2. Now verify that $p = f\,\mathrm{last}_A$.
3. Now using the precondition and (2), verify that $f \neq 0$ and $\mathrm{last}_A \neq 0$.
4. **Therefore using the precondition, (2), and (3), verify that** $\deg(\mathrm{last}_A) > \deg(p) = \deg(f\,\mathrm{last}_A) \geq \deg(\mathrm{last}_A)$**.**
5. **Abort procedure.**

Declaration V:27

The notation $\mathrm{pows}(A)$, where A is a $m \times m$ rational matrix, will be used as a shorthand for the result yielded by executing the following instructions:

1. Let $t = \deg(\mathrm{last}_A)$.
2. Make an $m^2 \times t$ matrix, B, whose i^{th} column is the sequential concatenation of the columns of A^i.
3. **Yield** $\langle B\rangle$**.**

Procedure V:75

Objective

Choose a $m \times m$ rational matrix, A. Execute procedure V:37 on $\mathrm{pows}(A)$ and let the tuple $\langle M, D, , N\rangle$ receive the result. Let $t = \mathrm{cols}(\mathrm{pows}(A))$. The objective of the following instructions is to show that either $0 < 0$ or to show that $C_t(D) = C_t(D)_{0,0} e_0 \neq 0$.

Implementation

1. Execute procedure V:37 on $\mathrm{pows}(A)$ and let the tuple $\langle M, D, , N\rangle$ receive the result.
2. Verify that $M_* \,\mathrm{pows}(A) N_* = D$.
3. Using procedure V:17, verify that $M^{-1}{}_* M_* \,\mathrm{pows}(A) N_* = 1_{m^2} \,\mathrm{pows}(A) N_* = \mathrm{pows}(A) N_* = M^{-1}{}_* D$.
4. If $C_t(D)_{0,0} = 0$, then:
   (a) Verify that for some $0 \leq i < t$, $D_{i,i} = 0$.
   (b) Therefore verify that $De_i = 0_{m^2\times 1}$.
   (c) Therefore verify that $\mathrm{pows}(A)(Ne_i) = (\mathrm{pows}(A)N)e_i = (M^{-1}D)e_i = M^{-1}(De_i) = 0_{m^2\times 1}$.
   (d) Let $p = N_{0,i}\lambda^0 + N_{1,i}\lambda^1 + \cdots + N_{t-1,i}\lambda^{t-1}$.
   (e) Therefore verify that $\Lambda(p, A) = 0_{m\times m}$.
   (f) Execute procedure V:73 on $N^{-1}{}_*$ and N_*.
   (g) Therefore verify that $p \neq 0$.
   (h) Execute procedure V:74 on A and p.
   (i) **Abort procedure.**
5. Otherwise, do the following:
   (a) Execute procedure V:33 on $\langle D, 1_t, t\rangle$ and let E receive.
   (b) Verify that $C_t(D) = C_t(D1_t) = EC_t(1_t) = E * 1 = E$.
   (c) Verify that E is a $\binom{m^2}{t} \times \binom{t}{t}$ diagonal matrix.
   (d) Therefore verify that $C_t(D)$ is a $\binom{m^2}{t} \times 1$ diagonal matrix.
   (e) **Therefore verify that** $C_t(D) = C_t(D)_{0,0} e_0 \neq 0$**.**

Procedure V:76

Objective

Choose a $m \times m$ rational matrix, A. Let $t = \mathrm{cols}(\mathrm{pows}(A))$. The objective of the following instructions is to show that either $0 < 0$ or to show that $C_t(\mathrm{pows}(A)) \neq 0$.

Implementation

1. Execute procedure V:37 on $\mathrm{pows}(A)$ and let the tuple $\langle M, D, , N\rangle$ receive the result.
2. Verify that $\mathrm{pows}(A) = {M^{-1}}_* D {N^{-1}}_*$.
3. Execute procedure V:73 on $C_t(M_*)$, $C_t({M^{-1}}_*)$.
4. Hence verify that all columns of $C_t({M^{-1}}_*)$ are non-zero.
5. Execute procedure V:75 on A.
6. Verify that $C_t(D) = C_t(D)_{0,0} e_0 \neq 0$.
7. Therefore verify that $C_t(D)_{0,0} \neq 0$.
8. Execute procedure V:73 on $C_t(N_*), C_t({N^{-1}}_*)$.
9. Hence verify that $C_t(N^{-1}) \neq 0$.
10. **Verify that** $C_t(\mathrm{pows}(A)) = C_t({M^{-1}}_* D {N^{-1}}_*) = C_t({M^{-1}}_*) C_t(D) C_t({N^{-1}}_*) = C_t({M^{-1}}_*) C_t(D)_{0,0} e_0 C_t({N^{-1}}_*) = C_t(D)_{0,0} C_t({N^{-1}}_*) C_t({M^{-1}}_*) e_0 \neq 0_{\binom{m^2}{t} \times 1}$.

Declaration V:28

The notation $\mathrm{tr}(A)$, where A is a square matrix, will be used as a shorthand for the sum of its diagonal entries.

Procedure V:77

Objective

Choose two $m \times m$ matrices A, B. The objective of the following instructions is to show that $\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B)$.

Implementation

1. Verify that $\mathrm{tr}(A+B)$
   (a) $= \sum_r^{[0:m]} (A+B)_{r,r}$
   (b) $= \sum_r^{[0:m]} (A_r + B_r)_{r,r}$
   (c) $= \sum_r^{[0:m]} A_{r,r} + \sum_r^{[0:m]} B_{r,r}$
   (d) $= \mathrm{tr}(A) + \mathrm{tr}(B)$.

Procedure V:78

Objective

Choose a polynomial b and an $m \times m$ matrix A. The objective of the following instructions is to show that $\mathrm{tr}(bA) = b\,\mathrm{tr}(A)$.

Implementation

1. Verify that $\mathrm{tr}(bA)$
   (a) $= \mathrm{tr}(b_{m\times m} A)$
   (b) $= \sum_r^{[0:m]} (b_{m\times m} A)_{r,r}$
   (c) $= \sum_r^{[0:m]} \sum_t^{[0:m]} (b_{m\times m})_{r,t} A_{t,r}$
   (d) $= \sum_r^{[0:m]} (b_{m\times m})_{r,r} A_{r,r}$
   (e) $= \sum_r^{[0:m]} b A_{r,r}$
   (f) $= b \sum_r^{[0:m]} A_{r,r}$
   (g) $= b\,\mathrm{tr}(A)$.

Procedure V:79

Objective

Choose an $m \times n$ matrix A and an $n \times m$ matrix B. The objective of the following instructions is to show that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Implementation

1. Verify that $\mathrm{tr}(AB)$
   (a) $= \sum_r^{[0:m]} (AB)_{r,r}$
   (b) $= \sum_r^{[0:m]} \sum_t^{[0:n]} A_{r,t} B_{t,r}$

(c) $= \sum_t^{[0:n]} \sum_r^{[0:m]} B_{t,r} A_{r,t}$

(d) $= \sum_t^{[0:n]} (BA)_{t,t}$

(e) $= \mathrm{tr}(BA)$.

Procedure V:80

Objective

Choose an $m \times n$ matrix A such that $A \neq 0$. The objective of the following instructions is to show that $\mathrm{tr}(A^T A) > 0$.

Implementation

1. Verify that $\mathrm{tr}(A^T A)$

(a) $= \sum_r^{[0:n]} (A^T A)_{r,r}$

(b) $= \sum_r^{[0:n]} \sum_t^{[0:m]} (A^T)_{r,t} A_{t,r}$

(c) $= \sum_r^{[0:n]} \sum_t^{[0:m]} A_{t,r} A_{t,r}$

(d) $= \sum_r^{[0:n]} \sum_t^{[0:m]} (A_{t,r})^2$

(e) > 0.

Declaration V:29

The phrase "symmetric matrix" will be used to refer to matrices A such that "$A^T = A$".

Procedure V:81

Objective

Choose a symmetric $m \times m$ rational matrix, A. Let $t = \deg(\mathrm{last}_A)$. Choose two polynomials u, w such that $\deg(u) < t$ and $\deg(w) < t$. The objective of the following instructions is to show that $\mathrm{tr}(\Lambda(uw, A)) = \mathrm{mat}(u)^T \mathrm{pows}(A)^T \mathrm{pows}(A) \mathrm{mat}_t(w)$.

Implementation

1. Verify that $\mathrm{tr}(\Lambda(uw, A))$

(a) $= \mathrm{tr}(\Lambda(u, A)\Lambda(w, A))$

(b) $= \mathrm{tr}((\sum_p^{[0:t]} u_p A^p)(\sum_q^{[0:t]} w_q A^q))$

(c) $= \mathrm{tr}(\sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q A^p A^q)$

(d) $= \sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q \,\mathrm{tr}(A^p A^q)$

(e) $= \sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q \sum_e^{[0:m]} \sum_f^{[0:m]} {A^p}_{e,f} \cdot {A^q}_{f,e}$

(f) $= \sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q \sum_e^{[0:m]} \sum_f^{[0:m]} {A^p}_{f,e} \cdot {A^q}_{f,e}$

(g) $= \sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q \sum_g^{[0:m^2]} \mathrm{pows}(A)_{g,p} \mathrm{pows}(A)_{g,q}$

(h) $= \sum_p^{[0:t]} \sum_q^{[0:t]} u_p w_q (\mathrm{pows}(A)^T \mathrm{pows}(A))_{p,q}$

(i) $= \sum_p^{[0:t]} u_p (\mathrm{pows}(A)^T \mathrm{pows}(A) \mathrm{mat}_t(w))_p$

(j) $= \mathrm{mat}_t(u)^T \mathrm{pows}(A)^T \mathrm{pows}(A) \mathrm{mat}_t(w)$

Declaration V:30

The notation sel_A, where A is an $m \times m$ rational matrix, will be used as a shorthand for the result yielded by executing the following instructions:

1. Using procedure V:42, procedure V:76, and procedure V:80, verify that $C_t(\mathrm{pows}(A)^T \mathrm{pows}(A)) = C_t(\mathrm{pows}(A)^T) C_t(\mathrm{pows}(A)) = C_t(\mathrm{pows}(A))^T C_t(\mathrm{pows}(A)) = \mathrm{tr}(C_t(\mathrm{pows}(A))^T C_t(\mathrm{pows}(A))) > 0$.
2. Let $t = \deg(\mathrm{last}_A)$.
3. Let $H = (\mathrm{pows}(A)^T \mathrm{pows}(A)) \backslash e_{t-1}$.
4. **Yield** $\langle \frac{\sum_j^{[0:t]} H_{j,0} \lambda^j}{(\mathrm{last}_A)_t} \rangle$.

Procedure V:82

Objective

Choose a symmetric $m \times m$ rational matrix, A. Let $t = \deg(\mathrm{last}_A)$. Choose a polynomial u such that $\deg(u) < t$. The objective of the following instructions is to show that $\mathrm{tr}(\Lambda(u \,\mathrm{sel}_A, A)) = \frac{u_{t-1}}{(\mathrm{last}_A)_t}$.

Implementation

1. Using procedure V:81, verify that $\operatorname{tr}(\Lambda(u \operatorname{sel}_A, A))$
   (a) $= \operatorname{mat}(u)^T \operatorname{pows}(A)^T \operatorname{pows}(A) \operatorname{mat}_t(\operatorname{sel}_A)$
   (b) $= \frac{\operatorname{mat}(u)^T \operatorname{pows}(A)^T \operatorname{pows}(A)((\operatorname{pows}(A)^T \operatorname{pows}(A)) \backslash e_{t-1})}{(\operatorname{last}_A)_t}$
   (c) $= \frac{\operatorname{mat}(u)^T e_{t-1}}{(\operatorname{last}_A)_t}$
   (d) $= \frac{\operatorname{mat}(u)_{t-1,0}}{(\operatorname{last}_A)_t}$
   (e) $= \frac{u_{t-1}}{(\operatorname{last}_A)_t}$.

Procedure V:83

Objective

Choose a symmetric $m \times m$ rational matrix, A. The objective of the following instructions is to either show that $0 \neq 0$ or construct polynomials u, v such that $u \operatorname{last}_A + v \operatorname{sel}_A = 1$.

Implementation

1. Let $t = \deg(\operatorname{last}_A)$.
2. Let G be the 1×2 matrix $\langle\langle \operatorname{last}_A, \operatorname{sel}_A \rangle\rangle$.
3. Execute procedure V:37 on G and let the tuple $\langle M, D, , N \rangle$ receive.
4. Verify that $G = M^{-1}{}_* D N^{-1}{}_*$.
5. Verify that $\operatorname{last}_A \neq 0$.
6. Therefore verify that $D_{0,0} \neq 0$.
7. If $\deg(D_{0,0}) > 0$, then do the following:
   (a) Let $b = N^{-1}{}_{*0,0}$.
   (b) Verify that $\operatorname{last}_A = b D_{0,0}$.
   (c) Therefore verify that $b \neq 0$.
   (d) Let $z = \deg(b)$.
   (e) Verify that $t = \deg(\operatorname{last}_A) = \deg(b D_{0,0}) = \deg(b) + \deg(D_{0,0}) > \deg(b) = z$.
   (f) Let $c = N^{-1}{}_{*0,1}$.
   (g) Verify that $\operatorname{sel}_A = c D_{0,0}$.
   (h) Let $u = \lambda^{t-z-1} b$.
   (i) Execute procedure V:82 on A and u.
   (j) Hence verify that $(\operatorname{last}_A)_t \operatorname{tr}(\Lambda(u \operatorname{sel}_A, A)) = u_{t-1} = b_z \neq 0$.
   (k) Also verify that $\operatorname{tr}(\Lambda(u \operatorname{sel}_A, A))$
      i. $= \operatorname{tr}(\Lambda(\lambda^{t-z-1} b c D_{0,0}, A))$
      ii. $= \operatorname{tr}(\Lambda(\lambda^{t-z-1} c \operatorname{last}_A, A))$
      iii. $= \operatorname{tr}(\Lambda(\lambda^{t-z-1} c, A) \Lambda(\operatorname{last}_A, A))$
      iv. $= \operatorname{tr}(\Lambda(\lambda^{t-z-1} c, A) 0_{m \times m})$
      v. $= \operatorname{tr}(0_{m \times m})$
      vi. $= 0$.
   (l) **Therefore verify that $0 \neq 0$.**
   (m) **Abort procedure.**
8. Otherwise, do the following:
   (a) Verify that $\deg(D_{0,0}) = 0$.
   (b) Let $u = \frac{N_{0,0}}{D_{0,0}}$.
   (c) Let $v = \frac{N_{1,0}}{D_{0,0}}$.
   (d) **Verify that $u \operatorname{last}_A + v \operatorname{sel}_A = 1$.**
   (e) **Yield the tuple $\langle u, v \rangle$.**

Procedure V:84

Objective

Choose a symmetric $m \times m$ rational matrix A, where $m > 0$. Let $t = \deg(\operatorname{last}_A)$. The objective of the following instructions is to either show that $0 \neq 0$ or to construct lists of polynomials s, q such that

1. For $i = 0$ to $i = t$, $\deg(s_i) = i$.
2. For $i = 0$ to $i = t$, $\operatorname{sgn}((s_i)_i) = \operatorname{sgn}((s_t)_t)$.
3. For $i = 1$ to $i = t - 1$, $s_{i-1} + s_{i+1} = q_i s_i$.
4. $s_t = \operatorname{last}_A$.

Implementation

1. Let $s_t = \mathrm{last}_A$.
2. Execute procedure V:83 on A and let $\langle u, s_{t+1}\rangle$ receive the result.
3. Hence verify that $us_t + s_{t+1}\,\mathrm{sel}_A = 1$.
4. Let $q_t = s_{t+1} \operatorname{div} s_t$.
5. Let $s_{t-1} = s_{t+1} \bmod s_t$.
6. Verify that $s_{t+1} = q_t s_t + s_{t-1}$, where $\deg(s_{t-1}) < \deg(s_t) = t$.
7. Therefore verify that $us_t + (q_t s_t + s_{t-1})\,\mathrm{sel}_A = 1$.
8. Therefore verify that $\Lambda(s_{t-1}\,\mathrm{sel}_A, A) = \Lambda(us_t + (q_t s_t + s_{t-1})\,\mathrm{sel}_A, A) = \Lambda(1, A) = 1_m$.
9. Therefore using procedure V:82, verify that $\frac{(s_{t-1})_{t-1}}{(s_t)_t} = \mathrm{tr}(\Lambda(s_{t-1}\,\mathrm{sel}_A, A) = \mathrm{tr}(1_m) = m > 0$.
10. For $i \in [t : 1]$, do the following:
    (a) Let $q_i = (-s_{i+1}) \operatorname{div} (-s_i)$.
    (b) Let $s_{i-1} = (-s_{i+1}) \bmod (-s_i)$.
    (c) Verify that $\deg(q_i) = 1$.
    (d) Verify that $(q_i)_1 = \frac{(s_{i+1})_{i+1}}{(s_i)_i}$.
    (e) Also verify that $-s_{i+1} = -q_i s_i + s_{i-1}$.
    (f) Therefore verify that $q_i s_i = s_{i+1} + s_{i-1}$.
    (g) Therefore verify that $q_i s_i - s_{i+1} = s_{i-1}$.
    (h) Execute procedure II:76 on the tuple $\langle s, q, i-1\rangle$ and let $\langle p, j\rangle$ receive.
    (i) Verify that $s_{i-1} = ps_{t-1} + js_t$.
    (j) Verify that $\deg(p) = t - 1 - (i-1) = t - i$.
    (k) Verify that $\deg(j) = t - 2 - (i-1) = t - 1 - i$
    (l) Therefore verify that $\Lambda(s_{i-1}, A) = \Lambda(ps_{t-1} + js_t, A) = \Lambda(ps_{t-1}, A) + \Lambda(j, A)\Lambda(s_t, A) = \Lambda(ps_{t-1}, A) + \Lambda(j, A)0_{m\times m} = \Lambda(ps_{t-1}, A)$.
    (m) If $\Lambda(p, A) = 0$, then do the following:
        i. Execute procedure V:74 on A and p.
        ii. **Abort procedure.**
    (n) Otherwise, if $\Lambda(s_{i-1}, A) = 0_{m\times m}$, then do the following:
        i. Verify that $\Lambda(ps_{t-1}\,\mathrm{sel}_A, A) = \Lambda(ps_{t-1}, A)\Lambda(\mathrm{sel}_A, A) = \Lambda(s_{i-1}, A)\Lambda(\mathrm{sel}_A, A) = 0_{m\times m}\Lambda(\mathrm{sel}_A, A) = 0_{m\times m}$.
        ii. Verify that $\Lambda(ps_{t-1}\,\mathrm{sel}_A, A) = \Lambda(p, A)\Lambda(s_{t-1}\,\mathrm{sel}_A, A) = \Lambda(p, A)1_m = \Lambda(p, A) \neq 0_{m\times m}$.
        iii. Therefore verify that $0 \neq 0$.
        iv. **Abort procedure.**
    (o) Otherwise if $\Lambda(s_{i-1}\,\mathrm{sel}_A, A) = 0_{m\times m}$, then do the following:
        i. Verify that $\Lambda(s_{i-1}\,\mathrm{sel}_A\, s_{t-1}, A) = \Lambda(s_{i-1}\,\mathrm{sel}_A, A)\Lambda(s_{t-1}, A) = 0_{m\times m}\Lambda(s_{t-1}, A) = 0_{m\times m}$.
        ii. Verify that $\Lambda(s_{i-1}\,\mathrm{sel}_A\, s_{t-1}, A) = \Lambda(s_{i-1}, A)\Lambda(\mathrm{sel}_A\, s_{t-1}, A) = \Lambda(s_{i-1}, A)1_m = \Lambda(s_{i-1}, A) \neq 0_{m\times m}$.
        iii. Therefore verify that $0_{m\times m} \neq 0_{m\times m}$.
        iv. **Abort procedure.**
    (p) Otherwise, do the following:
        i. Verify that $\deg(s_{i-1}) < i$.
        ii. Verify that $\Lambda(s_{i-1}\,\mathrm{sel}_A, A) \neq 0_{m\times m}$.
        iii. Execute the auxilliary procedure on the tuple $(i-1, s_{i-1})$.
        iv. Hence using procedure V:80, verify that $\frac{(s_{i-1})_{i-1}}{(s_i)_i} = \mathrm{tr}(\Lambda({s_{i-1}}^2{\mathrm{sel}_A}^2, A)) = \mathrm{tr}((\Lambda(s_{i-1}\,\mathrm{sel}_A, A))^2) = \mathrm{tr}((\Lambda(s_{i-1}\,\mathrm{sel}_A, A))^T(\Lambda(s_{i-1}\,\mathrm{sel}_A, A))) > 0$.
        v. **Therefore verify that** $\mathrm{sgn}((s_{i-1})_{i-1}) = \mathrm{sgn}((s_i)_i)$.
11. Yield the tuple $\langle s_{[0:t+1]}, q_{[0:t]}\rangle$.

Auxilliary procedure

Objective Choose an integer $0 \leq k \leq t$ such that polynomial s_k is defined. Choose a polynomial g such that $\deg(g) \leq \min(k, t-1)$. The objective of the following instructions is to show that $\mathrm{tr}(\Lambda(gs_k{\mathrm{sel}_A}^2, A)) = \frac{g_k}{(s_{k+1})_{k+1}}$.

Implementation

1. If $k = t$, then verify that $\mathrm{tr}(\Lambda(gs_k\mathrm{sel}_A{}^2, A))$
  (a) $= \mathrm{tr}(\Lambda(gs_t\mathrm{sel}_A{}^2, A))$
  (b) $= \mathrm{tr}(\Lambda(g\mathrm{sel}_A{}^2, A)\Lambda(s_t, A))$
  (c) $= \mathrm{tr}(\Lambda(g\mathrm{sel}_A{}^2, A)0_{m\times m})$
  (d) $= 0$
  (e) $= \frac{g_k}{(s_{k+1})_{k+1}}$.
2. Otherwise if $k = t - 1$, then verify that $\mathrm{tr}(\Lambda(gs_k\mathrm{sel}_A{}^2, A))$
  (a) $= \mathrm{tr}(\Lambda(gs_{t-1}\mathrm{sel}_A{}^2, A))$
  (b) $= \mathrm{tr}(\Lambda(g\mathrm{sel}_A, A)\Lambda(s_{t-1}\mathrm{sel}_A, A))$
  (c) $= \mathrm{tr}(\Lambda(g\,\mathrm{sel}_A, A)1_m)$
  (d) $= \mathrm{tr}(\Lambda(g\,\mathrm{sel}_A, A))$
  (e) $=\frac{g_k}{(s_{k+1})_{k+1}}$.
3. Otherwise if $k < t - 1$, then do the following:
  (a) Verify that $\deg(gq_{k+1}) = k + 1 \leq t - 1$.
  (b) Execute the auxilliary procedure on the tuple $\langle k + 1, gq_{k+1}\rangle$.
  (c) Now verify that $\mathrm{tr}(\Lambda((gq_{k+1})s_{k+1}\mathrm{sel}_A{}^2, A)) = \frac{\frac{(s_{k+2})_{k+2}}{(s_{k+1})_{k+1}}g_k}{(s_{k+2})_{k+2}} = \frac{g_k}{(s_{k+1})_{k+1}}$.
  (d) Verify that $\deg(g) \leq k \leq t - 2$.
  (e) Execute the auxilliary procedure on the tuple $\langle k + 2, g\rangle$.
  (f) Now verify that $\mathrm{tr}(\Lambda(gs_{k+2}\mathrm{sel}_A{}^2, A)) = \frac{g_{k+2}}{(s_{k+3})_{k+3}} = \frac{0}{(s_{k+3})_{k+3}} = 0$.
  (g) Therefore verify that $\mathrm{tr}(\Lambda(gs_k\mathrm{sel}_A{}^2, A))$
    i. $= \mathrm{tr}(\Lambda(g(q_{k+1}s_{k+1} + s_{k+2})\mathrm{sel}_A{}^2, A))$
    ii. $= \mathrm{tr}(\Lambda(gq_{k+1}s_{k+1}\mathrm{sel}_A{}^2 + gs_{k+2}\mathrm{sel}_A{}^2, A))$
    iii. $= \mathrm{tr}(\Lambda(gq_{k+1}s_{k+1}\mathrm{sel}_A{}^2, A)+\Lambda(gs_{k+2}\mathrm{sel}_A{}^2, A))$
    iv. $= \mathrm{tr}(\Lambda(gq_{k+1}s_{k+1}\mathrm{sel}_A{}^2, A))+\mathrm{tr}(\Lambda(gs_{k+2}\mathrm{sel}_A{}^2, A))$
    v. $= \frac{g_k}{(s_{k+1})_{k+1}} + 0$
    vi. $= \frac{g_k}{(s_{k+1})_{k+1}}$.

Procedure V:85

Objective

Choose a symmetric $m \times m$ rational matrix, A. Let $t = \deg(\mathrm{last}_A)$. The objective of the following instructions is to either show that $0 < 0$ or to construct two lists of rational numbers c, d such that $c_0 < d_0 \leq c_1 < d_1 \leq \cdots \leq c_{t-1} < d_{t-1}$ and $0 \neq \mathrm{sgn}(\Lambda(\mathrm{last}_A, c_i)) = -\,\mathrm{sgn}(\Lambda(\mathrm{last}_A, d_i))$ for i in $[0 : t]$.

Implementation

1. Execute procedure V:84 on the matrix A and let the tuple $\langle s, q\rangle$ receive the result.
2. Execute procedure II:75 supplying the tuple $\langle s, q\rangle$. Let the tuple $\langle c, d\rangle$ receive the result.
3. **Verify that** $c_0 < d_0 \leq c_1 < d_1 \leq \cdots \leq c_{t-1} < d_{t-1}$**.**
4. **Verify that** $\mathrm{sgn}(\Lambda(\mathrm{last}_A, c_i)) = -\,\mathrm{sgn}(\Lambda(\mathrm{last}_A, d_i))$ **for** i **in** $[0 : t]$**.**
5. **Yield** $\langle c, d\rangle$**.**

Procedure V:86

Objective

Choose a symmetric $m \times m$ rational matrix, A. Let $t = \deg(\mathrm{last}_A)$. Execute procedure V:85 on A and let the tuple $\langle c, d\rangle$ receive the result. Execute procedure V:37 on A and let the tuple $\langle , , u, \rangle$ receive the result. The objective of the following instructions is to either show that $1 = -1$ or to construct a list of non-negative integers k such that $0 \neq \mathrm{sgn}(\Lambda(u_{k_i}, c_i)) = -\,\mathrm{sgn}(\Lambda(u_{k_i}, d_i))$ for i in $[0 : t]$.

Implementation

1. Verify that $\mathrm{last}_A = u_0u_1 \cdots u_{m-1}$.
2. For i in $[0 : t]$, do the following:
  (a) Using the precondition, verify that $0 \neq \mathrm{sgn}(\Lambda(\mathrm{last}_A, c_i)) = -\,\mathrm{sgn}(\Lambda(\mathrm{last}_A, d_i))$.
  (b) If $0 \in \mathrm{sgn}(\Lambda(u, c_i))$, then do the following:
    i. Verify that 0

A. $= \operatorname{sgn}(\Lambda(u_0, c_i)) \operatorname{sgn}(\Lambda(u_1, c_i)) \cdots \operatorname{sgn}(\Lambda(u_{m-1}, c_i))$

B. $= \operatorname{sgn}(\Lambda(u_0, c_i)\Lambda(u_1, c_i) \cdots \Lambda(u_{m-1}, c_i))$

C. $= \operatorname{sgn}(\Lambda(u_0 u_1 \cdots u_{m-1}, c_i))$

D. $= \operatorname{sgn}(\Lambda(\text{last}_A, c_i))$

E. $\neq 0$.

(c) If $0 \in \operatorname{sgn}(\Lambda(u, d_i))$, then do the following:

i. Verify that 0

A. $= \operatorname{sgn}(\Lambda(u_0, d_i)) \operatorname{sgn}(\Lambda(u_1, d_i)) \cdots \operatorname{sgn}(\Lambda(u_{m-1}, d_i))$

B. $= \operatorname{sgn}(\Lambda(u_0, d_i)\Lambda(u_1, d_i) \cdots \Lambda(u_{m-1}, d_i))$

C. $= \operatorname{sgn}(\Lambda(u_0 u_1 \cdots u_{m-1}, d_i))$

D. $= \operatorname{sgn}(\Lambda(\text{last}_A, d_i))$

E. $\neq 0$.

(d) If $\operatorname{sgn}(\Lambda(u_j, c_i)) = \operatorname{sgn}(\Lambda(u_j, d_i))$ for $j \in [0 : m]$, then do the following:

i. Verify that $\operatorname{sgn}(\Lambda(\text{last}_A, c_i))$

A. $= \operatorname{sgn}(\Lambda(u_0 u_1 \cdots u_{m-1}, c_i))$

B. $= \operatorname{sgn}(\Lambda(u_0, c_i)) \operatorname{sgn}(\Lambda(u_1, c_i)) \cdots \operatorname{sgn}(\Lambda(u_{m-1}, c_i))$

C. $= \operatorname{sgn}(\Lambda(u_0, d_i)) \operatorname{sgn}(\Lambda(u_1, d_i)) \cdots \operatorname{sgn}(\Lambda(u_{m-1}, d_i))$

D. $= \operatorname{sgn}(\Lambda(u_0 u_1 \cdots u_{m-1}, d_i))$

E. $= \operatorname{sgn}(\Lambda(\text{last}_A, d_i))$.

ii. **Therefore verify that $1 = -1$.**

iii. **Abort procedure.**

(e) Otherwise do the following:

i. **Let k_i be the least integer such that $0 \neq \operatorname{sgn}(\Lambda(u_{k_i}, c_i)) = -\operatorname{sgn}(\Lambda(u_{k_i}, d_i))$.**

3. **Yield $\langle k \rangle$.**

Procedure V:87

Objective

Choose a symmetric $m \times m$ rational matrix, A. Execute procedure V:37 on A and let the tuple $\langle, , u, \rangle$ receive the result. Execute procedure II:69 on A and let k receive. Let $t = \deg(\text{last}_A)$. Let $n_j = \sum_i^{[0:t]} [k_i = j]$ for j in $[0 : m]$. The objective of the following instructions is to either show that $0 < 0$, or to show that $n_i = \deg(u_i)$ for i in $[0 : m]$.

Implementation

1. Verify that $\sum_j^{[0:m]} n_j = \sum_j^{[0:m]} \sum_i^{[0:t]} [k_i = j] = \sum_i^{[0:t]} \sum_j^{[0:m]} [k_i = j] = \sum_i^{[0:t]} 1 = t$.
2. If for any i in $[0 : m]$, $n_i > \deg(u_i)$, then do the following:
   (a) Execute procedure II:69 on the polynomial u_i along with $\deg(u_i)+1$ of the distinct pairs $\langle c_l, d_l \rangle$ such that $k_l = i$.
   (b) **Abort procedure.**
3. Otherwise if for any i in $[0 : m]$, $n_i < \deg(u_i)$, then do the following:
   (a) Verify that $\sum_i^{[0:m]} n_j < \sum_i^{[0:m]} \deg(u_j) = t$.
   (b) Therefore using (1) and (a), verify that $\sum_i^{[0:m]} n_j < \sum_i^{[0:m]} n_j$.
   (c) **Abort procedure.**
4. Otherwise, do the following:
   (a) **For all i in $[0 : m]$, verify that $n_i = \deg(u_i)$.**

Procedure V:88

Objective

Choose a symmetric $m \times m$ rational matrix, A. Let $t = \deg(\text{last}_A)$. Execute procedure V:86 on the matrix A and let the tuple $\langle k \rangle$ receive the result. The objective of the following instructions is to either show that $0 < 0$ or to show that $\sum_i^{[0:t]} (m - k_i) = m$.

Implementation

1. Execute procedure V:37 on the matrix A and let the tuple $\langle, D, u, \rangle$.
2. Using procedure V:87, verify that $\sum_i^{[0:t]} (m - k_i)$
   (a) $= \sum_i^{[0:t]} \sum_j^{[0:m]} [k_i \leq j]$

(b) $= \sum_j^{[0:m]} \sum_i^{[0:t]} [k_i \leq j]$

(c) $= \sum_j^{[0:m]} \sum_i^{[0:t]} [k_i \leq j] \sum_l^{[0:m]} [k_i = l]$

(d) $= \sum_j^{[0:m]} \sum_l^{[0:m]} \sum_i^{[0:t]} [k_i \leq j][k_i = l]$

(e) $= \sum_j^{[0:m]} \sum_l^{[0:m]} \sum_i^{[0:t]} [l \leq j][k_i = l]$

(f) $= \sum_j^{[0:m]} \sum_l^{[0:m]} [l \leq j] \sum_i^{[0:t]} [k_i = l]$

(g) $= \sum_j^{[0:m]} \sum_l^{[0:m]} [l \leq j] \deg u_l$

(h) $= \sum_j^{[0:m]} \sum_l^{[0:j+1]} \deg u_l$

(i) $= \sum_j^{[0:m]} \deg D_{j,j}$

(j) $= m$

References

[1] Harold Edwards. *Linear Algebra*. Springer Science+Business Media, 1995.

[2] Hugh L. Montgomery, Ivan Niven, Herbert S. Zuckerman. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 1991.

[3] Ludwig Wittgenstein. *Philosophical Grammar*. Edited by Rush Rhees. Translated by Anthony Kenny. Basil Blackwell, Oxford, 1974.