Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-01

Counting Integral Points

How many integral points are in the following triangle?

$$\begin{array}{ccc} (0,n) & & \\ | & \diagdown & \\ (0,0) & — & (n,0) \end{array}$$

Express that number as a sum!

$$\sum_{x=?}^{?} ?$$

How many integral points are in the circle of radius n around $(0,0)$?

?

$$\begin{array}{ll} & 7 \cdot 8 \\ = & \langle \text{ Evaluation } \rangle \\ & (10-3)\cdot(12-4) \\ \leq & \langle \text{ Fact: } 3 \leq 4 \text{ } \rangle \\ & (10-4)\cdot(12-4) \\ \leq & \langle \text{ Fact: } 4 \leq 5 \text{ } \rangle \\ & (10-4)\cdot(12-5) \\ = & \langle \text{ Evaluation } \rangle \\ & 6 \cdot 7 \\ = & \langle \text{ Evaluation } \rangle \\ & 42 \end{array}$$

This proves: $7 \cdot 8 \leq 42$

Plan for Today

- **Sum and Product Quantification** (special case of Textbook Chapter 8)
- Extending the calculational proof format to transitive operators
- Monotonicity

Counting Integral Points

How many integral points are in the triangle $\begin{array}{ccc} (0,n) & & \\ | & \diagdown & \\ (0,0) & — & (n,0) \end{array}$?

$$
\begin{array}{ll}
 & \sum_{x=0}^{n} (n - x + 1) \\
= & \langle \text{ Summing 1 values } \rangle \\
 & \sum_{x=0}^{n} (\sum_{y=0}^{n-x} 1) \\
= & \langle \text{ Switch to LADM notation } \rangle \\
 & (\sum x \mid 0 \le x \le n \bullet (\sum y \mid 0 \le y \le n - x \bullet 1)) \\
= & \langle \text{ Nesting } \rangle \\
 & (\sum x, y \mid 0 \le x \le n \land 0 \le y \le n - x \bullet 1) \\
= & \langle \text{ Isotonicity of } + \rangle \\
 & (\sum x, y \mid 0 \le x \le n \land x \le x + y \le n \bullet 1) \\
= & \langle \text{ Def. of } \Rightarrow \text{ (3.60) with Transitivity of } \le \rangle \\
 & (\sum x, y \mid 0 \le x \le x + y \le n \bullet 1) \\
= & \langle \text{ Making implied integer type explicit } \rangle \\
 & (\sum x, y : \mathbb{Z} \mid 0 \le x \le x + y \le n \bullet 1) \\
= & \langle \text{ Switching to natural numbers } \rangle \\
 & (\sum x, y : \mathbb{N} \mid x + y \le n \bullet 1)
\end{array}
$$

Counting Integral Points

How many integral points are in the triangle $\begin{array}{ccc} (0,n) & & \\ | & \diagdown & \\ (0,0) & — & (n,0) \end{array}$?

$$(\sum x, y : \mathbb{N} \mid x + y \le n \bullet 1)$$

How many integral points are in the circle of radius n around $(0,0)$?

$$(\sum x, y : \mathbb{Z} \mid x \cdot x + y \cdot y \le n \cdot n \bullet 1)$$

Sum Quantification Examples

$(\sum k : \mathbb{N} \mid k < 5 \bullet k)$

- "The sum of all natural numbers less than five"

$(\sum k : \mathbb{N} \mid k < 5 \bullet k \cdot k)$

- "For all natural numbers k that are less than 5, adding up the value of $k \cdot k$"
- "The sum of all squares of natural numbers less than five"

$(\sum x, y : \mathbb{N} \mid x \cdot y = 120 \bullet 2 \cdot (x + y))$

- "For all natural numbers x and y with product 120, adding up the value of $2 \cdot (x + y)$"
- "The sum of the perimeters of all integral rectangles with area 120"

Product Quantification Examples

- "The factorial of n is the product of all positive integers up to n"

  $$factorial : \mathbb{N} \to \mathbb{N}$$
  $$factorial\ n = (\prod k : \mathbb{N} \mid 0 < k \leq n \bullet k)$$

- "The product of all odd natural numbers below 50."

  $$(\prod k : \mathbb{N} \mid 2 \cdot k + 1 < 50 \bullet 2 \cdot k + 1)$$
  $$(\prod k : \mathbb{N} \mid k < 25 \bullet 2 \cdot k + 1)$$
  $$(\prod n : \mathbb{N} \mid \neg(2 \mid n) \wedge n < 50 \bullet n)$$

Sum and Product Quantification

$(\sum x \mid R \bullet E)$

- "For all x satisfying R, summing up the value of E"
- "The sum of all E for x with R"

$(\sum x : T \bullet E)$

- "For all x of type T, summing up the value of E"
- "The sum of all E for x of type T"

$(\prod x \mid R \bullet E)$

- "The product of all E for x with R"

$(\prod x : T \bullet E)$

- "The product of all E for x of type T"

General Shape of Sum and Product Quantifications

$$(\sum x : t_1;\ y, z : t_2 \mid R \bullet E)$$
$$(\prod x : t_1;\ y, z : t_2 \mid R \bullet E)$$

- Any number of **variables** x, y, z can be quantified over
- The quantified variables may have **type annotations** (which act as **type declarations**)
- Expression $R : \mathbb{B}$ is the **range** of the quantification
- Expression E is the **body** of the quantification
- E will have a number type ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)
- Both R and E may refer to the **quantified variables** x, y, z
- The type of the whole quantification expression is the type of E.

Expanding Sum and Product Quantification

Sum quantification ($\sum$) is **"addition (+) of arbitrarily many terms"**:

$$
\begin{aligned}
& (\ \textstyle\sum i \ \mid\ 5 \le i < 9 \bullet i \cdot (i+1)\ ) \\
= \ & \langle \text{ Quantification expansion } \rangle \\
& (i \cdot (i+1))[i := 5] \quad + \quad (i \cdot (i+1))[i := 6] \quad + \quad (i \cdot (i+1))[i := 7] \quad + \quad (i \cdot (i+1))[i := 8] \\
= \ & \langle \text{ Substitution } \rangle \\
& 5 \cdot (5+1) \quad + \quad 6 \cdot (6+1) \quad + \quad 7 \cdot (7+1) \quad + \quad 8 \cdot (8+1)
\end{aligned}
$$

Product quantification ($\prod$) is **"multiplication ($\cdot$) of arbitrarily many factors"**:

$$
\begin{aligned}
& (\ \textstyle\prod i \ \mid\ 0 \le i < 4 \bullet 5 \cdot i + 1\ ) \\
= \ & \langle \text{ Quantification expansion } \rangle \\
& (5 \cdot i + 1)[i := 0] \quad \cdot \quad (5 \cdot i + 1)[i := 1] \quad \cdot \quad (5 \cdot i + 1)[i := 2] \quad \cdot \quad (5 \cdot i + 1)[i := 3] \\
= \ & \langle \text{ Substitution } \rangle \\
& (5 \cdot 0 + 1) \quad \cdot \quad (5 \cdot 1 + 1) \quad \cdot \quad (5 \cdot 2 + 1) \quad \cdot \quad (5 \cdot 3 + 1)
\end{aligned}
$$

LADM/CalcCheck Quantification Notation

Conventional sum quantification notation: $\displaystyle\sum_{i=1}^{n} e \quad = \quad e[i := 1] + \ldots + e[i := n]$

The textbook uses a different, but systematic **linear** notation:

$$(\textstyle\sum i \ \mid\ 1 \le i \le n : e) \qquad \text{or} \qquad (+ i \ \mid\ 1 \le i \le n : e)$$

We use a variant with a "spot" "•" instead of the colon ":" and only use "big" operators:

$$(\textstyle\sum i \ \mid\ 1 \le i \le n \bullet e)$$

Reasons for using this linear quantification notation:

- Clearly delimited introduction of **quantified variables** (**dummies**)
- **Arbitrary** Boolean expressions can define the **range** of the quantified variables
  $$(\textstyle\sum i \ \mid\ 1 \le i \le 7 \wedge \mathit{even}\ i \bullet i) = 2 + 4 + 6$$
- Extends easily to multiple quantified variables:
  $$(\textstyle\sum i, j : \mathbb{Z} \ \mid\ 1 \le i < j \le 4 \bullet i/j) = 1/2 + 1/3 + 1/4 + 2/3 + 2/4 + 3/4$$

?

$$
\begin{aligned}
& 7 \cdot 8 \\
= \ & \langle \text{ Evaluation } \rangle \\
& (10 - 3) \cdot (12 - 4) \\
\le \ & \langle \text{ Fact: } 3 \le 4 \ \rangle \\
& (10 - 4) \cdot (12 - 4) \\
\le \ & \langle \text{ Fact: } 4 \le 5 \ \rangle \\
& (10 - 4) \cdot (12 - 5) \\
= \ & \langle \text{ Evaluation } \rangle \\
& 6 \cdot 7 \\
= \ & \langle \text{ Evaluation } \rangle \\
& 42
\end{aligned}
$$

This proves: $7 \cdot 8 \le 42$

Calculational Proof Format

$$
\begin{array}{ll}
 & E_0 \\
= & \langle \text{ Explanation of why } E_0 = E_1 \text{ } \rangle \\
 & E_1 \\
= & \langle \text{ Explanation of why } E_1 = E_2 \text{ } \rangle \\
 & E_2 \\
= & \langle \text{ Explanation of why } E_2 = E_3 \text{ } \rangle \\
 & E_3
\end{array}
$$

This is a proof for:

$$E_0 = E_3$$

Calculational Proof Format

$$
\begin{array}{ll}
 & E_0 \\
= & \langle \text{ Explanation of why } E_0 = E_1 \text{ } \rangle \\
 & E_1 \\
= & \langle \text{ Explanation of why } E_1 = E_2 \text{ — with comment } \rangle \\
 & E_2 \\
= & \langle \text{ Explanation of why } E_2 = E_3 \text{ } \rangle \\
 & E_3
\end{array}
$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 = E_1 \qquad \wedge \qquad E_1 = E_2 \qquad \wedge \qquad E_2 = E_3$$

Because $=$ is **transitive**, this justifies:

$$E_0 = E_3$$

Calculational Proof Format

$$
\begin{array}{ll}
 & E_0 \\
\leq & \langle \text{ Explanation of why } E_0 \leq E_1 \text{ } \rangle \\
 & E_1 \\
\leq & \langle \text{ Explanation of why } E_1 \leq E_2 \text{ — with comment } \rangle \\
 & E_2 \\
\leq & \langle \text{ Explanation of why } E_2 \leq E_3 \text{ } \rangle \\
 & E_3
\end{array}
$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 \leq E_1 \qquad \wedge \qquad E_1 \leq E_2 \qquad \wedge \qquad E_2 \leq E_3$$

Because $\leq$ is **transitive**, this justifies:

$$E_0 \leq E_3$$

Calculational Proof Format

$$\begin{array}{ll} & E_0 \\ \leq & \langle \text{ Explanation of why } E_0 \leq E_1 \text{ } \rangle \\ & E_1 \\ = & \langle \text{ Explanation of why } E_1 = E_2 \text{ — with comment } \rangle \\ & E_2 \\ \leq & \langle \text{ Explanation of why } E_2 \leq E_3 \text{ } \rangle \\ & E_3 \end{array}$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 \leq E_1 \quad \wedge \quad E_1 = E_2 \quad \wedge \quad E_2 \leq E_3$$

Because $\leq$ is **transitive**(and because of Leibniz), this justifies:

$$E_0 \leq E_3$$

Calculational Proof Format

$$\begin{array}{ll} & E_0 \\ \Rightarrow & \langle \text{ Explanation of why } E_0 \Rightarrow E_1 \text{ } \rangle \\ & E_1 \\ \equiv & \langle \text{ Explanation of why } E_1 \equiv E_2 \text{ — with comment } \rangle \\ & E_2 \\ \Rightarrow & \langle \text{ Explanation of why } E_2 \Rightarrow E_3 \text{ } \rangle \\ & E_3 \end{array}$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$(E_0 \Rightarrow E_1) \quad \wedge \quad (E_1 \equiv E_2) \quad \wedge \quad (E_2 \Rightarrow E_3)$$

Because $\Rightarrow$ is **transitive**(and because of Leibniz), this justifies:

$$E_0 \Rightarrow E_3$$

Calculational Proof Format

$$\begin{array}{ll} & E_0 \\ \leq & \langle \text{ Explanation of why } E_0 \leq E_1 \text{ } \rangle \\ & E_1 \\ = & \langle \text{ Explanation of why } E_1 = E_2 \text{ — with comment } \rangle \\ & E_2 \\ < & \langle \text{ Explanation of why } E_2 < E_3 \text{ } \rangle \\ & E_3 \end{array}$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 \leq E_1 \quad \wedge \quad E_1 = E_2 \quad \wedge \quad E_2 < E_3$$

Because $<$ is **transitive**, and because $\leq$ is the reflexive closure of $<$, this justifies:

$$E_0 < E_3$$

Calculational Proof Format

$$
\begin{array}{ll}
 & E_0 \\
\leq & \langle \text{ Explanation of why } E_0 \leq E_1 \text{ } \rangle \\
 & E_1 \\
= & \langle \text{ Explanation of why } E_1 = E_2 \text{ — with comment } \rangle \\
 & E_2 \\
\geq & \langle \text{ Explanation of why } E_2 \geq E_3 \text{ } \rangle \\
 & E_3
\end{array}
$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 \leq E_1 \qquad \wedge \qquad E_1 = E_2 \qquad \wedge \qquad E_2 \geq E_3$$

This justifies nothing about the relation between E_0 and E_3 !

?

$$
\begin{array}{ll}
 & 7 \cdot 8 \\
= & \langle \text{ Evaluation } \rangle \\
 & (10 - 3) \cdot (12 - 4) \\
\leq & \langle \text{ Fact: } 3 \leq 4 \text{ } \rangle \\
 & (10 - 4) \cdot (12 - 4) \\
\leq & \langle \text{ Fact: } 4 \leq 5 \text{ } \rangle \\
 & (10 - 4) \cdot (12 - 5) \\
= & \langle \text{ Evaluation } \rangle \\
 & 6 \cdot 7 \\
= & \langle \text{ Evaluation } \rangle \\
 & 42
\end{array}
$$

This proves: $7 \cdot 8 \leq 42$

Leibniz is Special to Equality

How about the following?

$$
\begin{array}{ll}
 & x - 3 \\
\leq & \langle \text{ Fact: } 3 \leq 4 \text{ } \rangle \\
 & x - 4
\end{array}
$$

Remember:

(1.5) **Leibniz:** $\dfrac{X \;=\; Y}{E[z := X] \;=\; E[z := Y]}$

Leibniz is available <u>only for equality</u>

Order Relations

- Let T be a type.
- A relation $\_\leq\_$ on T is called:
  - **reflexive** iff $x \leq x$ is a theorem
  - **transitive** iff $x \leq y \Rightarrow y \leq z \Rightarrow x \leq z$ is a theorem
  - **antisymmetric** iff $x \leq y \Rightarrow y \leq x \Rightarrow x = y$ is a theorem
  - an **order** (or **ordering**) iff it is reflexive, transitive, and antisymmetric
- Orders you are familiar with:

$$\begin{array}{lcccccc}
_=_ & : & T & \to & T & \to & \mathbb{B} \\
\leq & : & \mathbb{Z} & \to & \mathbb{Z} & \to & \mathbb{B} \\
\geq & : & \mathbb{Z} & \to & \mathbb{Z} & \to & \mathbb{B} \\
\leq & : & \mathbb{N} & \to & \mathbb{N} & \to & \mathbb{B} \\
\geq & : & \mathbb{N} & \to & \mathbb{N} & \to & \mathbb{B} \\
_|_ & : & \mathbb{N} & \to & \mathbb{N} & \to & \mathbb{B} \\
\equiv & : & \mathbb{B} & \to & \mathbb{B} & \to & \mathbb{B} \\
\Rightarrow & : & \mathbb{B} & \to & \mathbb{B} & \to & \mathbb{B} \\
\subseteq & : & set(T) & \to & set(T) & \to & \mathbb{B}
\end{array}$$

Monotonicity, Isotonicity, Antitonicity

- Let $\_\leq\_$ be an order on T
- Let $f : T \to T$ be a function on T
- Then f is called
  - **monotonic** iff $x \leq y \Rightarrow f\ x \leq f\ y$ is a theorem
  - **isotonic** iff $x \leq y \equiv f\ x \leq f\ y$ is a theorem
  - **antitonic** iff $x \leq y \Rightarrow f\ y \leq f\ x$ is a theorem
- Examples:
  - suc _ : $\mathbb{N} \to \mathbb{N}$ is isotonic
  - pred : $\mathbb{N} \to \mathbb{N}$ is monotonic, but not isotonic
  - $\_+\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is isotonic in the first argument:
    $x \leq y \equiv x + z \leq y + z$ is a theorem
  - $\_+\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is isotonic in the second argument:
    $x \leq y \equiv z + x \leq z + y$ is a theorem
  - $\_-\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is **monotonic in the first argument**:
    $x \leq y \Rightarrow x - z \leq y - z$ is a theorem
  - $\_-\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is **antitonic in the second argument**:
    $x \leq y \Rightarrow z - y \leq z - x$ is a theorem

Example Application of "Isotonicity of +"

- $\_+\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is isotone in the first argument:
  $x \leq y \equiv x + z \leq y + z$ is a theorem

```
Calculation:
    2 + n
  ≤⟨ “Isotonicity of +” with Fact `2 ≤ 3` ⟩
    3 + n
```

This step can be justified without "with" as follows:

```
Calculation:
    2 + n ≤ 3 + n
  ≡⟨ “Identity of ≡” ⟩
    true  ≡  2 + n ≤ 3 + n
  ≡⟨ Fact `2 ≤ 3` ⟩
    2 ≤ 3  ≡  2 + n ≤ 3 + n
      — This is “Isotonicity of +”
```

Example Application of "Monotonicity of –"

- $\_-\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is **monotone in the first argument**:
  $x \leq y \quad \Rightarrow \quad x - z \leq y - z$ is a theorem

---

```
Calculation:
    12 - n
  ≤⟨ “Monotonicity of -” with Fact `12 ≤ 20` ⟩
    20 - n
```

This step can be justified without "with" as follows:

```
Calculation:
    12 - n  ≤  20 - n
  ≡⟨ “Left-identity of ⇒” ⟩
    true  ⇒  (12 - n  ≤  20 - n)
  ≡⟨ Fact `12 ≤ 20` ⟩
    (12 ≤ 20)  ⇒  (12 - n  ≤  20 - n)
  — This is “Monotonicity of -”
```

Example Application of "Antitonicity of –"

- $\_-\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is **antitone in the second argument**:
  $x \leq y \quad \Rightarrow \quad z - y \leq z - x$ is a theorem

---

```
Calculation:
    m - 3
  ≤⟨ “Antitonicity of -” with Fact `2 ≤ 3` ⟩
    m - 2
```

Multiplication on $\mathbb{N}$ is Monotonic…

```
Calculation:
    42
  =⟨ Evaluation ⟩
    6 · 7
  =⟨ Evaluation ⟩
    (10 - 4) · (12 - 5)
  ≤⟨ “Monotonicity of ·”
        with “Antitonicity of -” with Fact `3 ≤ 4`
    ⟩
    (10 - 3) · (12 - 5)
  ≤⟨ “Monotonicity of ·”
        with “Antitonicity of -” with Fact `4 ≤ 5`
    ⟩
    (10 - 3) · (12 - 4)
  =⟨ Evaluation ⟩
    7 · 8
  =⟨ Evaluation ⟩
    56
```