Exercises in Quantifier Manipulation

Roland Backhouse*
Diethard Michaelis†

February 6, 2006

Abstract

The Eindhoven quantifier notation is systematic, unlike standard mathematicial notation. This has the major advantage that calculations with quantified expressions become more straightforward because the calculational rules need be given just once for a great variety of different quantifiers.

We demonstrate the ease of calculation with finite quantifications by considering a number of examples. Two are simple warm-up exercises, using boolean equality as the quantifier. Three are taken from books of challenging mathematical problems, and one is a problem concocted by the authors to demonstrate the techniques.

1 Introduction

Quantifications, both logical ($\forall$, $\exists$) and arithmetic (Σ, Π, etc.) abound in program specifications, but the manipulation of quantified expressions is rarely discussed in any detail. (An important exception is [GKP89].) Moreover, many texts (in mathematics and computing) adopt different (unsystematic) notations for different quantifiers, obscuring the commonalities in their properties. Even worse, the dotdotdot ("...") notation is often used, leading inevitably to mistakes[1]. In contrast, the "Eindhoven" quantifier notation is a uniform notation for expressing quantifications over an arbitrary abelian monoid. It has been used since the early 1970s [Dij75, Dij76]. Initially, little or no explanation of the rules for manipulating quantifiers was given, except for some of the

*School of Computer Science and Information Technology, University of Nottingham, Nottingham NG8 1BB, England

†Beethovenstr. 55, 90513 Zirndorf, Germany

[1]The website "The most common errors in undergraduate mathematics" `www.vanderbilt.edu/~schectex/commerrs` reports "many errors" in the use of dotdotdot notation ("ellipses"). Of course, the error is the teacher's use of the notation, and should not be blamed on the student!

most basic (like empty range and range splitting [Gri81]). Backhouse [Bac86] compiled a list of rules for finite quantifications, partly based on the rules given by Knuth for summation [Knu68]; these were recently updated [Bac03] bringing the naming of the rules into line with that used elsewhere.

In this paper, we demonstrate the importance of manipulating quantifiers using a number of exercises drawn from books about challenging mathematical problems. Our calculations lead to straightforward solutions to the problems and, in one case, to a new theorem. The calculations are goal-directed and, we hope, may be of benefit to teaching the calculational method.

Full details of the notation and the rules we use are given in [Bac03].

2 Warm-up Exercises

A standard exercise is to prove that the parity of a sum of a finite bag of integers is odd equivales the number of odd elements is odd. This is a nice warm-up exercise in the use of the quantifier calculus:

$$
\begin{array}{cl}
 & even.\langle \Sigma k :: n_k \rangle \\
= & \{ \quad even \text{ distributes through summation} \quad \} \\
 & \langle \equiv k :: even.n_k \rangle \\
= & \{ \quad \text{trading, } even.n_k \equiv (odd.n_k \Rightarrow \mathsf{false}) \quad \} \\
 & \langle \equiv k : odd.n_k : \mathsf{false} \rangle \\
= & \{ \quad \mathsf{false} \equiv even.1 \quad \} \\
 & \langle \equiv k : odd.n_k : even.1 \rangle \\
= & \{ \quad even \text{ distributes through summation} \quad \} \\
 & even.\langle \Sigma k : odd.n_k : 1 \rangle \quad .
\end{array}
$$

The calculation uses two quantifiers: the familiar sum (Σ) quantifier, and the unfamiliar equivales ($\equiv$) quantifier. Possibly also unfamiliar is the distributivity of *even* over finite summation. This is a consequence of two properties:

$$even.0 \equiv \mathsf{true} \quad ,$$

(the unit of addition is mapped to the unit of equivales) and[2]

$$even.(m+n) \ \equiv \ even.m \ \equiv \ even.n$$

[2]Occurrences of the binary equivales symbol " $\equiv$ " and, later, inequivales " $\not\equiv$ " should be read associatively. Occurrences of the equality symbol " $=$ " should be read conjunctionally.

(binary addition is mapped to binary equivales). The "trading" rule for equivales (used in step 2) is like the trading rule for universal quantification. An implication, $P\Rightarrow$, in the term is "traded" into a conjunct, $P\wedge$, in the range. (Although we don't use it here, it is worth pointing out that the trading rule for inequivalence is like the trading rule for existential quantification — a conjunct is traded with a conjunct.)

Note that a special case for an empty bag does not need to be made. Even in this case, all quantifications are well defined; an equivales-quantification over an empty range is true.

It's useful to take this example a little further. Note that $\langle\Sigma k{:}\mathit{odd}.n_k{:}1\rangle$ is a count of the odd numbers in the bag. Sometimes, we want to count the number of values in a given finite range that satisfy a given property p. The following is useful.

$$
\begin{array}{ll}
 & \mathit{even}.\langle\Sigma k{:}p_k{:}1\rangle \\
= & \quad\{\quad \mathit{even} \text{ distributes through summation} \quad\} \\
 & \langle\equiv k : p_k : \mathit{even}.1\rangle \\
= & \quad\{\quad \text{trading, } \mathit{even}.1 \equiv \mathsf{false}\,,\ (q\Rightarrow\mathsf{false})\equiv q\equiv\mathsf{false} \quad\} \\
 & \langle\equiv k :: p_k \equiv \mathsf{false}\rangle \\
= & \quad\{\quad \text{associativity and symmetry} \quad\} \\
 & \langle\equiv k{::}p_k\rangle \ \equiv\ \langle\equiv k{::}\mathsf{false}\rangle \\
= & \quad\{\quad \mathsf{false} \equiv \mathit{even}.1\,,\ \text{distributivity} \quad\} \\
 & \langle\equiv k{::}p_k\rangle \ \equiv\ \mathit{even}.\langle\Sigma\, k{::}\,1\rangle \quad .
\end{array}
$$

In summary,

$$(1) \qquad \mathit{even}.\langle\Sigma k{:}p_k{:}1\rangle \ \equiv\ \langle\equiv k{::}p_k\rangle \ \equiv\ \mathit{even}.\langle\Sigma k{::}\,1\rangle \quad .$$

(In particular, p_k can be instantiated to $\mathit{odd}.n_k$.)

The equivales-quantifier will be used again later. Because it is unfamiliar, we offer the following exercise relating it to the different-from ($\not\equiv$) quantifier (more commonly known as exclusive-or).

The problem is to relate $\langle\equiv k{::}p_k\rangle$ to $\langle\not\equiv k{::}p_k\rangle$. Noting the distributivity laws: $\neg(p\equiv q)\equiv\neg p\not\equiv\neg q$, and $\neg\mathsf{true}\equiv\mathsf{false}$, negation distributes through an arbitrary finite equivales-quantification turning it into a different-from quantification. So,

$$
\begin{array}{ll}
 & \langle\not\equiv k{::}p_k\rangle \\
= & \quad\{\quad \text{double negation, distributivity} \quad\} \\
 & \neg\,\langle\equiv k{::}\neg p_k\rangle
\end{array}
$$

$$
\begin{array}{ll}
= & \{ \quad \text{definition of negation} \quad \} \\
& \langle \equiv k :: p_k \equiv \mathsf{false} \rangle \;\equiv\; \mathsf{false} \\
= & \{ \quad \text{associativity and symmetry of equivales} \quad \} \\
& \langle \equiv k :: p_k \rangle \;\equiv\; \langle \equiv k :: \mathsf{false} \rangle \;\equiv \mathsf{false} \\
= & \{ \quad \langle \equiv k :: \mathsf{false} \rangle = even.\langle \Sigma k :: 1 \rangle \,,\; odd \text{ is } \neg even \quad \} \\
& \langle \equiv k :: p_k \rangle \;\equiv odd.\langle \Sigma k :: 1 \rangle \quad .
\end{array}
$$

We conclude that

(2) $\quad \langle \not\equiv k :: p_k \rangle \;\equiv\; \langle \equiv k :: p_k \rangle \;\equiv\; odd.\langle \Sigma k :: 1 \rangle \quad .$

3 Even Numbers of Even Differences

The following exercise was designed by the authors to illustrate manipulations with quantifiers.

Suppose $\{n_k \mid 0 \leq k < M\}$ is a bag of integers. Consider the bag of *differences*

$$\{n_j - n_k \mid j < k\} \quad .$$

(For brevity, we assume throughout that the type of dummies j and k is the set of the first M natural numbers.) The question is: how can we evaluate whether the number of even differences is even with minimal effort? To resolve this question, we try to simplify the specification:

$$even.\langle \Sigma j,k \;:\; j < k \wedge even.(n_j - n_k) \;:\; 1 \rangle \quad .$$

We begin our calculation with a use of the warm-up exercises.

$$
\begin{array}{ll}
& even.\langle \Sigma j,k \;:\; j < k \wedge even.(n_j - n_k) \;:\; 1 \rangle \\
= & \{ \quad (1) \quad \} \\
& \langle \equiv j,k : j < k : even.n_j \;\equiv\; even.n_k \rangle \;\equiv\; even.\langle \Sigma j,k : j < k : 1 \rangle \\
= & \{ \quad \text{distributivity of } even \text{ over summation} \quad \} \\
& even.\langle \Sigma j,k : j < k : n_j + n_k \rangle \;\equiv\; even.\left\langle \Sigma j,k : j < k : \tfrac{1}{2} + \tfrac{1}{2} \right\rangle \quad .
\end{array}
$$

We now calculate the value of $\langle \Sigma j,k : j < k : n_j + n_k \rangle$. (The value of $\left\langle \Sigma j,k : j < k : \frac{1}{2} + \frac{1}{2} \right\rangle$ is easily seen to be the sum of the first M natural numbers, which is well known to be $\frac{1}{2} \times (M-1) \times M$. It is amusing to note, however, that it is a special case of the first summation, as made obvious by the way it has been written. The calculation below is an attractive way of deriving the standard formula.)

$$
\begin{array}{ll}
 & \langle \Sigma j,k : j<k : n_j + n_k \rangle \\
= & \{ \quad \text{aiming to eliminate the awkward range restriction,} \\
 & \quad\;\; \text{we exploit symmetry of addition} \quad \} \\
 & \frac{1}{2} \times \langle \Sigma j,k : j<k \vee k<j : n_j + n_k \rangle \\
= & \{ \quad j<k \vee k<j \;\equiv\; \neg(j=k) \text{ , range splitting} \quad \} \\
 & \frac{1}{2} \times (\langle \Sigma j,k :: n_j + n_k \rangle \;-\; \langle \Sigma j,k : j=k : n_j + n_k \rangle) \\
= & \{ \quad \text{associativity and symmetry, one-point rule} \quad \} \\
 & \frac{1}{2} \times (\langle \Sigma j,k :: n_j \rangle \;+\; \langle \Sigma j,k :: n_k \rangle \;-\; \langle \Sigma j :: 2 \times n_j \rangle) \\
= & \{ \quad \text{dummy renaming and distributivity} \quad \} \\
 & \frac{1}{2} \times 2 \times (\langle \Sigma j,k :: n_j \rangle \;-\; \langle \Sigma j :: n_j \rangle) \\
= & \{ \quad \text{arithmetic, nesting and associativity and symmetry} \quad \} \\
 & \langle \Sigma j :: \langle \Sigma k :: n_j \rangle \;-\; n_j \rangle \\
= & \{ \quad \text{distributivity (of product over addition)} \quad \} \\
 & \langle \Sigma j :: n_j \times (\langle \Sigma k :: 1 \rangle \;-\; 1) \rangle \\
= & \{ \quad \text{range of } k \text{ is } 0 \le k < M \text{, distributivity} \quad \} \\
 & (M-1) \times \langle \Sigma j :: n_j \rangle \quad .
\end{array}
$$

Consequently,

$$
even.\langle \Sigma j,k : j<k : n_j + n_k \rangle \quad \equiv \quad odd.M \vee even.\langle \Sigma j :: n_j \rangle \quad .
$$

Similarly, we have:

$$
\begin{array}{ll}
 & even.\langle \Sigma j,k : j<k : 1 \rangle \\
= & \{ \quad \text{above with } n_j = \frac{1}{2} \text{, or standard formula} \quad \} \\
 & even.(\frac{1}{2} \times (M-1) \times M) \\
= & \{ \quad \text{case analysis on } even.M \quad \} \\
 & even.\lfloor \frac{M}{2} \rfloor \quad .
\end{array}
$$

Substituting, we have determined that

$$
\begin{array}{ll}
 & even.\langle \Sigma j,k : j<k \wedge even.(n_j - n_k) : 1 \rangle \\
\equiv & odd.M \vee even.\langle \Sigma j : odd.n_j : 1 \rangle \quad \equiv \quad even.\lfloor \frac{M}{2} \rfloor \quad .
\end{array}
$$

We conclude that, when M is even, the evenness of the number of even differences is determined by first determining whether the number of odd numbers is even, and then comparing this boolean for equality with $even.\lfloor\frac{M}{2}\rfloor$. That is, we evaluate:

$$even.\langle\Sigma j : odd.n_j : 1\rangle \;\equiv\; even.\lfloor\tfrac{M}{2}\rfloor \quad .$$

In the case that M is odd, the answer is independent of the numbers in the bag; it is simply

$$even.\lfloor\tfrac{M}{2}\rfloor \quad .$$

An interesting feature of this example is that we have chosen to simplify summations rather than to use the equivales quantifier. The crucial step of eliminating the awkward range restriction, $j<k$, exploits a property of addition that has no counterpart for equivales. This extra degree of calculational freedom significantly enhances the elegance of the calculation.

4 1906 Hungarian Contest Problem

Exercise [Zei99, 3.4.8] is a special case of the following.

Suppose a bag of M numbers is given. Let a and b be both arbitrary arrangements of the bag. Prove that, if M is odd, the product

$$(a_1-b_1)(a_2-b_2)(a_3-b_3)\ldots(a_M-b_M)$$

is an even number. (In [Zei99, 3.4.8], the bag is the set of numbers 1, 2, ..., M.)

The calculational solution is as follows.

$$\begin{array}{ll}
 & even.\langle\Pi k :: a_k - b_k\rangle \\
= & \{ \quad even \text{ distributes through product and summation} \quad \} \\
 & \langle\exists k :: even.a_k \equiv even.b_k\rangle \\
\Leftarrow & \{ \quad \text{discussed below} \quad \} \\
 & \langle\not\equiv k :: even.a_k \equiv even.b_k\rangle \\
= & \{ \quad (2) \quad \} \\
 & \langle\equiv k :: even.a_k \equiv even.b_k\rangle \;\equiv\; odd.\langle\Sigma k :: 1\rangle \\
= & \{ \quad \text{associativity and symmetry of equivalence} \quad \} \\
 & \langle\equiv k :: even.a_k\rangle \;\equiv\; \langle\equiv k :: even.b_k\rangle \;\equiv\; odd.\langle\Sigma k :: 1\rangle \\
= & \{ \quad a \text{ and } b \text{ are rearrangements of the same bag} \quad \} \\
 & odd.\langle\Sigma k :: 1\rangle \quad .
\end{array}$$

The second step of this calculation is the most risky because it is a strengthening step. It is suggested by the goal of separating the two operands of the equivalence in the term of the quantification. Formally, the property used is that, for all predicates p,

(3) $\langle \exists k :: p_k \rangle \;\Leftarrow\; \langle \not\equiv k :: p_k \rangle$

In words, (3) is read as an inclusive-or is weaker than an exclusive-or. Its truth is established by observing that the contrapositive law, $\langle \forall k :: p_k \rangle \;\Rightarrow\; \langle \equiv k :: p_k \rangle$ for all predicates p, is an immediate consequence of Leibniz's rule. (Substitute true for p_k in the right side of the implication.)

A special case of (3) is

(4) $\langle \exists k :: even.n_k \rangle \quad \Leftarrow \quad even.\langle \Sigma k :: n_k \rangle \wedge odd.\langle \Sigma k :: 1 \rangle$.

(Take p_k to be $even.n_k$ and use distributivity of $even$ through summation and (2). The property is better known in the contrapositive form: the sum of an odd number of odd numbers is odd.) In this way, our proof is directly comparable to Zeitz's solution 2 [Zei99, 3.4.8]. The difference is that Zeitz's solution has a "rabbit"[3]: an (implicit) proof by contradiction is used in order to replace multiplication by addition. Our solution replaces disjunction by equivales, but the replacement is suggested directly by the shape of the formulae.

5 Summing Absolute Differences

In this section and the next, we consider two problems taken from [SA03] that involve sums of absolute differences. We present calculational solutions. Our calculations lead to theorems that are stronger than those stated in [SA03].

It is useful to "lift" a binary operator $\oplus$ on numbers to bags of equal size by defining, for bags a and c, each of size m,

$$a \oplus c \;=\; \langle \mathrm{BAG}\; i : 0 \le i < m : a_i \oplus c_i \rangle \quad .$$

We extend unary operators to bags (in particular, the absolute value operator) in the same way. Thus, $|a-c|$ denotes the bag of absolute differences

$$\langle \mathrm{BAG}\; i : 0 \le i < m : |a_i - c_i| \rangle \quad .$$

Quantifiers are functions from bags to values. For example, the sum quantifier, "Σ", maps a bag of numbers to a number. Combined with lifting, this gives the concise notation $\Sigma|a-c|$ for $\langle \Sigma i : 0 \le i < m : |a_i - c_i| \rangle$.

This section's problem is as follows. The numbers $1, 2, 3, \ldots 2{\times}N$ are divided over two sequences a and b, each of length N, in such a way that a is increasing and b is decreasing. Prove that

[3] Zeitz's solution begins with the words "The crux move: consider the *sum* of the terms".

$$\Sigma|a-b| \;=\; N^2 \quad .$$

The first step in the solution is to "disentangle" summation and absolute values. Let a and b be arbitrary equal-length sequences of numbers. Then

$$
\begin{array}{ll}
 & \Sigma|a-b| \\
= & \quad \{ \quad \text{definition of absolute value} \quad \} \\
 & \Sigma((a{\uparrow}b) - (a{\downarrow}b)) \\
= & \quad \{ \quad \text{associativity and symmetry of summation,} \\
 & \quad\quad\;\; \text{distributivity of negation over sum} \quad \} \\
 & \Sigma(a{\uparrow}b) - \Sigma(a{\downarrow}b) \quad .
\end{array}
$$

In summary, for arbitrary sequences a and b of equal length,

(5) $\quad \Sigma|a-b| \;=\; \Sigma(a{\uparrow}b) - \Sigma(a{\downarrow}b) \quad .$

Except for their having equal length, the above calculation makes no assumption about the sequences a or b . We now take this information into account.

Suppose i and j index elements of the sequences. Then

$$
\begin{array}{ll}
 & a_i{\downarrow}b_i \;<\; a_j{\uparrow}b_j \\
= & \quad \{ \quad \text{distributivity of } (<x) \text{ over minimum,} \\
 & \quad\quad\;\; \text{and } (x<) \text{ over maximum (for any } x) \quad \} \\
 & a_i < a_j \;\vee\; a_i < b_j \;\vee\; b_i < a_j \;\vee\; b_i < b_j \\
= & \quad \{ \quad a \text{ is increasing, } b \text{ is decreasing} \quad \} \\
 & i<j \;\vee\; (a_i < b_j \;\vee\; b_i < a_j) \;\vee\; j<i \\
\Leftarrow & \quad \{ \quad \langle \forall\, k :: a_k \neq b_k \rangle \;\text{. I.e. } \langle \forall\, k :: a_k < b_k \;\vee\; b_k < a_k \rangle \quad \} \\
 & i<j \;\vee\; i=j \;\vee\; j<i \\
= & \quad \{ \quad \text{inequalities} \quad \} \\
 & \mathsf{true} \quad .
\end{array}
$$

The conclusion is that

(6) $\quad \langle \forall\, i,j :: a_i{\downarrow}b_i \;<\; a_j{\uparrow}b_j \rangle$

where dummies i and j range over indexes of a and b . The significance of (6) is that $\Sigma(a{\uparrow}b)$ is the sum of the N largest elements in the concatenation of the two sequences (where N is the length of sequence a), and $\Sigma(a{\downarrow}b)$ is the sum of the N smallest elements. Thus, combining (6) with (5), we get the following theorem.

Theorem 7 Suppose $2{\times}N$ distinct numbers are divided over two sequences a and b, each of length N, in such a way that a is increasing and b is decreasing. Then, $\Sigma|a{-}b|$ is the difference between

- the sum of the N largest

and

- the sum of the N smallest

of the given numbers.

□

Applying this theorem to the case that the numbers are 1, 2, 3, ..., $2{\times}N$, using the well-known formula for the sum of 1, 2, 3, ..., n, we get that $\Sigma|a{-}b|$ is

$$(\tfrac{1}{2}{\times}(2{\times}N){\times}(2{\times}N+1) - \tfrac{1}{2}{\times}N{\times}(N{+}1)) - \tfrac{1}{2}{\times}N{\times}(N{+}1) \quad ,$$

which simplifies to N^2. (Note that N may be zero.)

Our calculation does not presuppose a knowledge of the answer. The most crucial step is the first one, in which the arithmetic involved in calculating absolute differences is disentangled from summation of a sequence. The symmetry between minimum and maximum in (5) suggests the calculation that follows it.

6 A De Morgan-Like Theorem

For our final exercise, we consider the following problem [SA03].

An arbitrary set of $m{+}n$ *numbers is divided into two arbitrary groups* a_1, a_2, ..., a_m *and* b_1, b_2, ..., b_n, *and the numbers in each group arranged in ascending order*

$$a_1 < a_2 < \ldots < a_m \quad , \quad b_1 < b_2 < \ldots < b_n \quad .$$

Then the same numbers are again divided into two arbitrary groups c_1, c_2, ..., c_m *and* d_1, d_2, ..., d_n, *and the numbers in each group arranged in ascending order*

$$c_1 < c_2 < \ldots < c_m \quad , \quad d_1 < d_2 < \ldots < d_n \quad .$$

Prove the equality

$$|a_1{-}c_1| + |a_2{-}c_2| + \ldots + |a_m{-}c_m| \;=\; |b_1{-}d_1| + |b_2{-}d_2| + \ldots + |b_n{-}d_n| \quad .$$

Our solution to the problem involves identifying a novel theorem on ascending sequences. We also eliminate the requirement that all the numbers are distinct. This leads to novel applications (omitted here for brevity).

We assume that we are given a finite bag U of numbers. We assume that the elements of the bag are (totally) ordered by the relation $\preceq$. If c is a subbag of U, we use $\#c$ to denote its size. The complement of c (in U) is denoted $\overline{c}$. For all i, $0 \leq i < \#c$, the ith element of c in the resulting ordered sequence is denoted by $c.i$. Formally, we have, for all subbags c of U,

(8) $\langle \forall j,k : 0 \leq j \leq k < \#c : c.j \preceq c.k \rangle$.

When U is a set (i.e. there are no duplicates in the bag), we have the stronger: for all subsets c of U,

(9) $\langle \forall j,k : 0 \leq j < \#c \wedge 0 \leq k < \#c : j < k \equiv c.j \prec c.k \rangle$.

As in section 5, we "lift" operators to map sequences to sequences. In general, it is not the case that the indexing function $(.i)$ distributes through lifted operators. For example, $|a-c|.i$ need not be equal to $|a.i - c.i|$. It is the case, however, for minimum and maximum (with respect to $\preceq$), because they are monotonic. This is important.

We are now in a position to reformulate the problem: An arbitrary bag U of numbers is split into subbags a and $\overline{a}$. The same bag U is split again into b and $\overline{b}$, where $\#a = \#b$. Prove that

(10) $\Sigma |a-b| \;=\; \Sigma |\overline{a}-\overline{b}|$.

Before beginning the calculation, we observe two complications:

- In general, the two sums range over different numbers of elements.
- Order (absolute value) and arithmetic (addition and subtraction) are heavily entangled.

The first step is thus to improve the situation:

$$\begin{array}{ll}
 & \Sigma |a-b| \;=\; \Sigma |\overline{a}-\overline{b}| \\
= & \qquad \{ \quad \text{definition of absolute value} \quad \} \\
 & \langle \Sigma i :: a.i \uparrow b.i - a.i \downarrow b.i \rangle \;=\; \langle \Sigma i :: \overline{a}.i \uparrow \overline{b}.i - \overline{a}.i \downarrow \overline{b}.i \rangle \\
= & \qquad \{ \quad \text{for all } i,\ (.i) \text{ distributes through max and min,} \\
 & \qquad\qquad \text{associativity and symmetry of addition} \quad \} \\
 & \Sigma(a \uparrow b) \;-\; \Sigma(a \downarrow b) \;=\; \Sigma(\overline{a} \uparrow \overline{b}) \;-\; \Sigma(\overline{a} \downarrow \overline{b}) \\
= & \qquad \{ \quad \text{arithmetic} \quad \} \\
 & \Sigma(a \uparrow b) \;+\; \Sigma(\overline{a} \downarrow \overline{b}) \;=\; \Sigma(\overline{a} \uparrow \overline{b}) \;+\; \Sigma(a \downarrow b) \quad .
\end{array}$$

This is much better. Both sides have $\#\mathsf{U}$ summands, and they differ only by complementation. This suggests a bold step:

$$
\begin{array}{cl}
 & \Sigma(a{\uparrow}b) + \Sigma(\overline{a}{\downarrow}\overline{b}) \;=\; \Sigma(\overline{a}{\uparrow}\overline{b}) + \Sigma(a{\downarrow}b) \\
\Leftarrow & \{ \quad \Sigma\mathsf{U} \;=\; \Sigma(a{\uparrow}b) + \Sigma(\overline{a{\uparrow}b}) \;=\; \Sigma(\overline{a{\downarrow}b}) + \Sigma(a{\downarrow}b) \quad \} \\
 & \overline{a{\uparrow}b} = \overline{a}{\downarrow}\overline{b} \;\wedge\; \overline{a{\downarrow}b} = \overline{a}{\uparrow}\overline{b} \;\; .
\end{array}
$$

We have thus reduced the original problem to establishing the following theorem on increasing sequences.

Theorem 11 ("De Morgan's Rule") For all equal-length subbags a and b of a totally ordered bag U:

$$\overline{a{\uparrow}b} = \overline{a}{\downarrow}\overline{b} \quad \text{and} \quad \overline{a{\downarrow}b} = \overline{a}{\uparrow}\overline{b} \quad .$$

□

We first prove the theorem assuming that U is a set, and then show how to extend the proof to bags. Clearly, it suffices to prove just the first conjunct. (The second is obtained from the first by the replacements $a,b := \overline{a},\overline{b}$.)

We have:

$$
\begin{array}{cl}
 & \overline{a{\uparrow}b} = \overline{a}{\downarrow}\overline{b} \\
= & \{ \quad \#(\overline{a{\uparrow}b}) \;=\; \#(\overline{a}{\downarrow}\overline{b})\text{, complementation} \quad \} \\
 & \langle \forall i,j :: (a{\uparrow}b).i \neq (\overline{a}{\downarrow}\overline{b}).j \rangle \\
= & \{ \quad \text{monotonicity of min and max} \quad \} \\
 & \langle \forall i,j :: a.i{\uparrow}b.i \;\neq\; \overline{a}.j{\downarrow}\overline{b}.j \rangle \quad .
\end{array}
$$

Now consider arbitrary i and j. We show that $a.i{\uparrow}b.i \;=\; \overline{a}.j{\downarrow}\overline{b}.j$ implies false.

$$
\begin{array}{cl}
 & a.i{\uparrow}b.i \;=\; \overline{a}.j{\downarrow}\overline{b}.j \\
= & \{ \quad a.i \neq \overline{a}.j\,,\; b.i \neq \overline{b}.j \text{ (because } a \text{ and } b \text{ are sets)} \quad \} \\
 & \quad (a.i \preceq b.i = \overline{a}.j \preceq \overline{b}.j) \\
 & \vee \quad (b.i \preceq a.i = \overline{b}.j \preceq \overline{a}.j) \quad .
\end{array}
$$

By symmetry, it suffices to prove that just one of the two disjuncts implies false. We proceed with the first.

$$
\begin{array}{cl}
 & a.i \preceq b.i = \overline{a}.j \preceq \overline{b}.j \\
= & \{ \quad \text{disentangling } a \text{ from } b \quad \}
\end{array}
$$

$$\begin{array}{ll}
& a.i \preceq \overline{a}.j \ \wedge \ \overline{a}.j = b.i \ \wedge \ b.i \preceq \overline{b}.j \\
= & \{ \qquad a \text{ and } \overline{a} \text{ are disjoint, as are } b \text{ and } \overline{b} \quad \} \\
& a.i \prec \overline{a}.j \ \wedge \ \overline{a}.j = b.i \ \wedge \ b.i \prec \overline{b}.j \ .
\end{array}$$

The next step is crucial. The property $a.i \prec \overline{a}.j$ implies that $(i{+}1)+j$ elements of U are less than $\overline{a}.j$; similarly, the property $b.i \prec \overline{b}.j$ implies that $(\#b-1-i)+(\#\overline{b}-j)$ elements of U are greater than $b.i$. Formally:

$$\begin{array}{ll}
& a.i \prec \overline{a}.j \\
= & \{ \qquad (9) \text{ and transitivity of } \prec \quad \} \\
& \langle \forall k : k \leq i : a.k \prec \overline{a}.j \rangle \ \wedge \ \langle \forall k : k < j : \overline{a}.k \prec \overline{a}.j \rangle \\
\Rightarrow & \{ \qquad a \text{ and } \overline{a} \text{ are disjoint subsets of } U \quad \} \\
& \langle \Sigma k : U.k \prec \overline{a}.j : 1 \rangle \ \geq \ (i{+}1)+j \ .
\end{array}$$

Similarly,

$$\begin{array}{ll}
& b.i \prec \overline{b}.j \\
= & \{ \qquad (9) \text{ and transitivity of } \prec \quad \} \\
& \langle \forall k : i < k : b.i \prec b.k \rangle \ \wedge \ \langle \forall k : j \leq k : b.i \prec \overline{b}.k \rangle \\
\Rightarrow & \{ \qquad b \text{ and } \overline{b} \text{ are disjoint subsets of } U \quad \} \\
& \langle \Sigma k : b.i \prec U.k : 1 \rangle \ \geq \ (\#b-1-i)+(\#\overline{b}-j) \ .
\end{array}$$

We now combine these two counts with the middle conjunct: $\overline{a}.j = b.i$.

$$\begin{array}{ll}
& a.i \prec \overline{a}.j \ \wedge \ \overline{a}.j = b.i \ \wedge \ b.i \prec \overline{b}.j \\
\Rightarrow & \{ \qquad \text{above, Leibniz} \quad \} \\
& \langle \Sigma k : U.k \prec b.i \vee b.i \prec U.k : 1 \rangle \ \geq \ (i{+}1)+j+(\#b-1-i)+(\#\overline{b}-j) \\
= & \{ \qquad \text{arithmetic, } \#b+\#\overline{b} = \#U \quad \} \\
& \langle \Sigma k : U.k \neq b.i : 1 \rangle \ \geq \ \#U \\
= & \{ \qquad b.i \text{ is an element of } U \quad \} \\
& \mathsf{false} \ .
\end{array}$$

This completes the proof of theorem 11, assuming that U is a set. Given a bag U, this lemma can be applied to the sets of pairs $(U.i, i)$ ordered lexicographically by $(x,i) \succeq (y,j)$ equivales $x \succ y \vee (x = y \wedge i \geq j)$.

It is interesting to compare our calculation with the argument given by Savchev and Andreescu [SA03]. Their argument starts immediately with induction and a subsequent case analysis. Our calculation is driven by heuristic principles, which lead to the discovery of the much more general De Morgan-like theorem. Their argument has 10 lines of displayed formulae (including 16 occurrences of ellipsis dots) and 20 lines of printed text. Ours is much more detailed, but has just 16 calculation steps, and a similar amount of text (including the hints accompanying calculation steps). Their argument assumes that $\mathcal{U}$ is a set, and is split into *non-empty* subsets; our calculation assumes that $\mathcal{U}$ is a bag, that is split arbitrarily.

7 Conclusion

Manipulating quantified expressions is an important calculational skill. Elsewhere, Knuth, Patashink and Graham [GKP89] also emphasise its importance and give several examples of non-trivial calculations with the Sigma quantifier. We have provided further evidence for the importance of the skill by tackling a number of challenging mathematical exercises.

Acknowledgements We are grateful to Wim Feijen for bringing the problems in [SA03] to our attention, and to Jeremy Weissmann for comments on an earlier presentation of section 5.

References

[Bac86] R.C. Backhouse. *Program Construction and Verification.* Prentice-Hall International, 1986.

[Bac03] Roland Backhouse. *Program Construction. Calculating Implementations From Specifications.* John Wiley Sons, Ltd., 2003.

[Dij75] Edsger W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Communications of the ACM*, 18:453–457, 1975.

[Dij76] Edsger W. Dijkstra. *A Discipline of Programming.* Prentice-Hall, 1976.

[GKP89] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics.* Addison-Wesley, 1989.

[Gri81] David Gries. *The Science of Programming.* Springer-Verlag, 1981.

[Knu68] Donald E. Knuth. *The Art of Computer Programming.*, volume Vol. I: Fundamental Algorithms. Addison-Wesley Publishing Co., Menlo Park, 1968.

[SA03] Svetoslav Savchev and Titu Andreescu. *Mathematical Miniatures*, volume 43 of *Anneli Lax New Mathematical Library*. The Mathematical Association of America, 2003.

[Zei99] Paul Zeitz. *The Art and Craft of Problem Solving*. John Wiley & Sons Inc., 1999.