

Monotonicity in Calculational Proofs

David Gries
Computer Science, Cornell University

May 1999

Abstract

We discuss the use of weakening and strengthening steps in calculational proofs. We present a metatheorem concerning monotonicity of positions in a formula that should have a more prominent place in the teaching of such proofs and give supporting examples.

Introduction

In making a calculational step like¹

$$\begin{array}{l} (\forall x \mid: P \wedge R) \\ \Rightarrow \quad \langle \text{Weakening } P \Rightarrow P \vee Q \rangle \\ (\forall x \mid: (P \vee Q) \wedge R) \end{array}$$

we are implicitly using the fact that the occurrence of variable P that is being replaced is in a monotonic position —weakening that position weakens the whole formula. To make the proof more precise and complete, the fact should be made explicit. A long-known but basically forgotten theorem can be used for this purpose; we show how this theorem is used in several calculational proofs.

Monotonicity

A function f is *monotonic* in its argument if $x \Rightarrow y$ implies $f.x \Rightarrow f.y$ (for all x, y). It is *antimonotonic* if $x \Rightarrow y$ implies $f.x \Leftarrow f.y$ (for all x, y).

The following facts are well-known: \vee and \wedge are monotonic in each of their operands, negation is antimonotonic in its operand, \Rightarrow is monotonic in its consequent and antimonotonic in its antecedent, $(\forall x \mid R : P)$ is monotonic in P but antimonotonic in R , and $(\exists x \mid R : P)$ is monotonic in both P and R . Formally, we have:

- (1) **Monotonic** \vee : $(P \Rightarrow Q) \Rightarrow (P \vee R \Rightarrow Q \vee R)$
Monotonic \wedge : $(P \Rightarrow Q) \Rightarrow (P \wedge R \Rightarrow Q \wedge R)$

¹We are dealing with a calculational predicate logic with equality, using the notation of [3].

- (2) **Antimonotonic \neg :** $(P \Rightarrow Q) \Rightarrow (\neg P \Leftarrow \neg Q)$
Monotonic consequent: $(P \Rightarrow Q) \Rightarrow ((R \Rightarrow P) \Rightarrow (R \Rightarrow Q))$
Antimonotonic antecedent: $(P \Rightarrow Q) \Rightarrow ((P \Rightarrow R) \Leftarrow (Q \Rightarrow R))$
Antimonotonic \forall -range: $(\mathbb{P} \Rightarrow Q) \Rightarrow ((\forall x \mid P : R) \Leftarrow (\forall x \mid Q : R))$
Monotonic \forall -body: $(P \Rightarrow Q) \Rightarrow ((\forall x \mid R : P) \Rightarrow (\forall x \mid R : Q))$
Monotonic \exists -range: $(P \Rightarrow Q) \Rightarrow ((\exists x \mid P : R) \Rightarrow (\exists x \mid Q : R))$
(3) **Monotonic \exists -body:** $(P \Rightarrow Q) \Rightarrow ((\exists x \mid R : P) \Rightarrow (\exists x \mid R : Q))$

But which of the following two formulas is valid, if either?

$$(\forall x \mid \neg P : S) \Rightarrow (\forall x \mid \neg(P \vee Q) : S)$$

$$(\forall x \mid \neg P : S) \Leftarrow (\forall x \mid \neg(P \vee Q) : S)$$

The answer is given by the following definition and theorem. ($E[z := P]$ denotes capture-avoiding substitution: $E[z := P]$ is a copy of expression E in which all occurrences of variable z have been replaced by expression P , with names of dummies (bound variables) being first replaced to avoid capture.)

- (4) **Definition.** Consider an occurrence of free variable z in a formula E (but not within an operand of \equiv). The position of z within E is called *monotonic* if it is nested within an even number of negations, antecedents, and ranges of universal quantifications; otherwise, it is *antimonotonic*.
- (5) **Metatheorem Monotonicity.** Suppose $P \Rightarrow Q$ is a theorem. Let expression E contain exactly one occurrence² of free variable z . Then:

- (a) Provided the position of z in E is monotonic,
 $E[z := P] \Rightarrow E[z := Q]$ is a theorem.
(b) Provided the position of z in E is antimonotonic,
 $E[z := P] \Leftarrow E[z := Q]$ is a theorem.

We can state (a) and (b) as inference rules:

- (6) **Monotonicity:** Provided the position of z in E is monotonic,

$$\frac{P \Rightarrow Q}{E[z := P] \Rightarrow E[z := Q]}$$

- (7) **Antimonotonicity:** Provided the position of z in E is antimonotonic,

$$\frac{P \Rightarrow Q}{E[z := P] \Leftarrow E[z := Q]}$$

²Actually, E can contain more than one occurrence of z , as long as all its positions are monotonic or all its positions are antimonotonic.

Sketch of proof of (5). The proof is by induction on the structure of expression E . One can reduce the case analysis by first manipulating E so that one has to deal only with formulas that contain variables, constants, negations, disjunctions in which z is not in the second operand, and existential quantifications with range *true*. Thus, perform the following steps, in order:

- Replace $(\forall x \mid F1 : F2)$ by $\neg(\exists x \mid F1 : \neg F2)$.
- Replace $(\exists x \mid F1 : F2)$ by $(\exists x \mid : F1 \wedge F2)$.
- Replace $F1 \not\Leftarrow F2$ by $\neg(F1 \Leftarrow F2)$.
- Replace $F1 \Leftarrow F2$ by $F2 \Rightarrow F1$.
- Replace $F1 \not\Rightarrow F2$ by $\neg(F1 \Rightarrow F2)$.
- Replace $F1 \Rightarrow F2$ by $\neg F1 \vee F2$.
- Replace $F1 \wedge F2$ by $\neg(\neg F1 \vee \neg F2)$.
- If z is in the second operand $F2$ of $F1 \vee F2$, replace $F1 \vee F2$ by $F2 \vee F1$.

These manipulations do not change the monotonicity of the position of z . Now, comes a straightforward proof by induction on the structure of the more restricted expressions E , which will rely on monotonic/antimonotonic properties (1), (2), and (3). \square

Incidentally, when teaching calculational logic and induction, this inductive proof is a nice exercise for students.

A convention for citing monotonicity

In a weakening/strengthening step of a calculation, the hint should explain why the step is sound. Here is a simple example, where it is presumed that Weakening was proved earlier.

$$\Rightarrow \frac{P}{\langle \text{Weakening}, P \Rightarrow P \vee Q \rangle} P \vee Q$$

But in the following example, the hint is not precise. This is because the soundness of the step depends not only on Weakening but also on Monotonic \wedge .

$$\Rightarrow \frac{P \wedge R}{\langle \text{Weakening}, P \Rightarrow P \vee Q \rangle} (P \vee Q) \wedge R$$

We seek a uniform way of substantiating steps like the above one. Rather than rely directly on all the individual monotonicity properties (1)–(3), it is easier to rely on inference rules (6) and (7), which can be used to substantiate all such weakening/strengthening steps.

We suggest the use of “Monotonic:” and “Antimonotonic:” to show reliance on these inference rules, as shown below. The word “Monotonic” suggests that a monotonic position is being replaced; “Antimonotonic” suggests that an antimonotonic position is being replaced. In the examples given below, to the right we have shown how the formulas can be rewritten in terms of variable z , so that the use of the inference rules is more easily seen.

$$\begin{array}{ll}
(\forall x \mid P \wedge R) & \quad \quad \quad \neg(\forall x \mid z \wedge R)[z := P] \\
\Rightarrow \quad \langle \text{Monotonic: Weakening } P \Rightarrow P \vee Q \rangle & \\
(\forall x \mid (P \vee Q) \wedge R) & \quad \quad \quad \neg(\forall x \mid z \wedge R)[z := P \vee Q] \\
\\
\neg(\forall x \mid \neg P \wedge R : S) & \quad \quad \quad \neg\neg(\forall x \mid \neg z \wedge R : S)[z := P] \\
\Leftarrow \quad \langle \text{Antimonotonic: Weakening } P \Rightarrow P \vee Q \rangle & \\
\neg(\forall x \mid \neg(P \vee Q) \wedge R : S) & \quad \quad \quad \neg\neg(\forall x \mid \neg z \wedge R : S)[z := P \vee Q]
\end{array}$$

Examples of the use of monotonicity

When dealing with theorems of propositional logic, monotonicity is not needed at all; as [3] shows, all proofs can be done easily without weakening/strengthening steps. However, for predicate logic proofs, weakening/strengthening steps are very useful, as the following examples show. These calculational proofs, using monotonicity/antimonotonicity, are surprisingly simple, especially compared to similar proofs in other proof systems. Each step of the proof is guided by the shapes of the current formula and goal. The theorems used in these proofs are from [3].

In [3], the One-point rule is an axiom and Instantiation is a theorem:

(8) **One-point rule:** Provided x does not occur free in E ,

$$(\forall x \mid x = E : P) \equiv P[x := E]$$

Instantiation: $(\forall x \mid P) \Rightarrow P[x := E]$

We prove Instantiation. Let z be a variable that does not occur free in P or E . We have:

$$\begin{array}{l}
(\forall x \mid \text{true} : P) \\
= \quad \langle \text{Dummy renaming } \neg z \text{ not free in } P \rangle \\
(\forall z \mid \text{true} : P[x := z]) \\
\Rightarrow \quad \langle \text{Antimonotonic: } \text{true} \Leftarrow z = E \rangle
\end{array}$$

$$\begin{aligned}
& (\forall z \mid z = E : P[x := z]) \\
= & \quad \langle \text{One-point rule} \rangle \\
& P[x := z][z := E] \\
= & \quad \langle \text{Property of textual substitution — } z \text{ is not free in } P \rangle \\
& P[x := E]
\end{aligned}$$

The next two examples concern proving English arguments sound by formalizing them and proving their formalizations. Consider the following statement.

All men are mortal. Socrates is a man. Therefore, Socrates is mortal.

We introduce two predicates.

man.m: person *m* is a man.
mortal.m: person *m* is mortal.

We formalize the statement as follows, with *S* standing for Socrates, and prove the formalization.

$$\begin{aligned}
& (\forall m \mid : \textit{man.m} \Rightarrow \textit{mortal.m}) \wedge \textit{man.S} \Rightarrow \textit{mortal.S} \\
& \Rightarrow \quad \langle \text{Monotonic: Instantiation, with } S \text{ for } m \rangle \\
& \quad (\textit{man.m} \Rightarrow \textit{mortal.m}) \wedge \textit{man.S} \\
& \Rightarrow \quad \langle \text{Modus ponens} \rangle \\
& \quad \textit{mortal.S}
\end{aligned}$$

Here is a second proof, which transforms the whole formula into a known theorem. It relies on inference rule Modus ponens, $P \Leftarrow Q, Q \longrightarrow P$.

$$\begin{aligned}
& (\forall m \mid : \textit{man.m} \Rightarrow \textit{mortal.m}) \wedge \textit{man.S} \Rightarrow \textit{mortal.S} \\
\Leftarrow & \quad \langle \text{Antimonotonic: Instantiation, with } S \text{ for } m \rangle \\
& (\textit{man.S} \Rightarrow \textit{mortal.S}) \wedge \textit{man.S} \Rightarrow \textit{mortal.S} \quad \text{—Modus ponens}
\end{aligned}$$

Now consider the English statement.

None but those with hearts can love. Some liars are heartless. Therefore, some liars cannot love.

Using *hh.p* for “*p* has a heart”, *cl.p* for “*p* can love”, and *li.p* for “*p* is a liar”, we formalize this as

$$(\forall p \mid : \textit{cl.p} \Rightarrow \textit{hh.p}) \wedge (\exists p \mid : \textit{li.p} \wedge \neg \textit{hh.p}) \Rightarrow (\exists p \mid : \textit{li.p} \wedge \neg \textit{cl.p}) \quad .$$

We prove this formula.

$$\begin{aligned}
& (\forall p \mathbf{I}: cl.p \Rightarrow hh.p) \wedge (\exists p \mathbf{I}: li.p \wedge \neg hh.p) \\
= & \quad \langle \text{Distributivity of } \wedge \text{ over } \exists \text{ —to get} \\
& \quad \text{same outer quantification as in consequent} \rangle \\
& (\exists p \mathbf{I}: (\forall p \mathbf{I}: cl.p \Rightarrow hh.p) \wedge li.p \wedge \neg hh.p) \\
\Rightarrow & \quad \langle \text{Monotonic: Instantiation} \rangle \\
& (\exists p \mathbf{I}: (cl.p \Rightarrow hh.p) \wedge li.p \wedge \neg hh.p) \\
= & \quad \langle \text{Contrapositive} \rangle \\
& (\exists p \mathbf{I}: (\neg hh.p \Rightarrow \neg cl.p) \wedge li.p \wedge \neg hh.p) \\
\Rightarrow & \quad \langle \text{Monotonic: Modus ponens} \rangle \\
& (\exists p \mathbf{I}: \neg cl.p \wedge li.p)
\end{aligned}$$

In [4], Carroll Morgan derives a nice proof of

$$(9) \quad (\exists x \mathbf{I}: (\forall y \mathbf{I}: P)) \Rightarrow (\forall y \mathbf{I}: (\exists x \mathbf{I}: P)) \quad .$$

Wim Feijen [2] presents convincing heuristics for the development of the proof. Here is the proof. Note that it uses Metatheorem Monotonicity, twice, although neither Morgan nor Feijen cite it.

$$\begin{aligned}
& (\exists x \mathbf{I}: (\forall y \mathbf{I}: P)) \\
\Rightarrow & \quad \langle \text{Monotonic: } R \Rightarrow (\forall y \mathbf{I}: R), \text{ provided } y \text{ doesn't occur free in } R \\
& \quad \text{—introduce the necessary universal quantification over } y \rangle \\
& (\forall y \mathbf{I}: (\exists x \mathbf{I}: (\forall y \mathbf{I}: P))) \\
\Rightarrow & \quad \langle \text{Monotonic: Instantiation —Eliminate universal quantification} \rangle \\
& (\forall y \mathbf{I}: (\exists x \mathbf{I}: P))
\end{aligned}$$

When we generalize (9) to allow ranges other than *true*, the proof becomes more complicated. Below, we prove:

$$(10) \quad \text{Provided } x \text{ not free in } Q \text{ and } y \text{ not free in } R, \\ (\exists x \mathbf{I} \mid R : (\forall y \mathbf{I} \mid Q : P)) \Rightarrow (\forall y \mathbf{I} \mid Q : (\exists x \mathbf{I} \mid R : P))$$

Since x does not occur free in the consequent, by Metatheorem Witness (9.30) of [3], (10) can be proved by proving instead

$$R \wedge (\forall y \mathbf{I} \mid Q : P) \Rightarrow (\forall y \mathbf{I} \mid Q : (\exists x \mathbf{I} \mid R : P)) \quad ,$$

which we now do:

$$\begin{aligned}
& R \wedge (\forall y \mathbf{I} \mid Q : P) \\
\Rightarrow & \quad \langle \wedge \text{ over } \forall, \text{ since } y \text{ not free in } R \rangle \\
& (\forall y \mathbf{I} \mid Q : R \wedge P) \\
\Rightarrow & \quad \langle \text{Monotonic: } \exists \text{-Introduction} \rangle \\
& (\forall y \mathbf{I} \mid Q : (\exists x \mathbf{I} : R \wedge P)) \\
= & \quad \langle \text{Trading} \rangle \\
& (\forall y \mathbf{I} \mid Q : (\exists x \mathbf{I} \mid R : P))
\end{aligned}$$

Discussion

Monotonicity properties (1)–(3), as well as metatheorem Monotonicity, are well-known. They can be found, in one guise or another, in several texts on logic. But the two major books that deal with the calculational approach do a bad job of explaining how monotonicity/antimonotonicity is to be used. On page 61 of [1], Dijkstra and Scholten discuss the monotonic properties of negation and implication. But they don't state the general theorem (5) and they don't give a convention for indicating its use. On page 93 of [1], a hint explicitly states the use of monotonicity of \wedge and \exists in a weakening step, but on pages 73 and 77, monotonicity of \forall -body is used without mention. We think the authors just didn't anticipate the frequent use of monotonicity and the problem readers would have with it if it were not well explained.

Gries and Schneider [3] also don't treat monotonicity well, and this has resulted in confusion among students about monotonicity and its use. The next edition of [3] is expected to use the approach of this note in order to eliminate the confusion.

The message of this little article is meant to be the apparent simplicity and brevity of many proofs in the calculational system when the right tools, like metatheorem Monotonicity, are available.

References

- [1] Edsger W. Dijkstra and Carel S. Scholten. *Predicate Calculus and Program Semantics*. Springer Verlag, New York, 1990.
- [2] Wim H.J. Feijen. $\exists\forall \Rightarrow \forall\exists$. WHJ189, September 1994.
- [3] David Gries and Fred B. Schneider. *A Logical Approach to Discrete Math*. Springer Verlag, New York 1993.
- [4] Carroll Morgan. Email communications in September 1995.