An example of goal-directed proof

Roland Backhouse*, Walter Guttmann†and Michael Winter‡

October 11, 2023

Abstract

We prove a non-trivial property of relations in a way that emphasises the creative process in its construction.

1 Introduction

In [BDGv22, theorem 139] it is proved that, for all relations R, the equivalence relation $R^* \cap (R^\cup)^*$ can be reformulated using the identity

$$R^* \cap (R^\cup)^* \;=\; (R \cap (R^\cup)^*)^* \quad .$$

This identity plays a significant role in algorithms which exploit the decomposition of a finite graph into an acyclic graph together with a collection of strongly connected components. (The relation R corresponds to the edge relation on nodes defined by the graph. Readers unfamiliar with the notation and/or property are referred to the appendix for a brief summary.) However, as observed in [BDGv22], the proof left a lot to be desired since it used the definition of the star operator (reflexive-transitive closure) as a sum of powers of R together with a quite complicated induction property. (Attempts we had made to apply fixed-point fusion had failed.)

Recently Guttmann formulated a proof using the inductive definition of R^* in point-free relation algebra. Winter made some improvements to Guttmann's proof.

Originally, the Guttmann-Winter proof was presented in the traditional mathematical style: a bottom-up proof that miraculously ends in the final step with the desired property. In this note, the proof has been rewritten in a way that emphasises the heuristics that were used to construct the proof. Some comments on how to present difficult proofs follow the calculations.

*School of Computer Science, University of Nottingham, Nottingham, UK

†Computer Science and Software Engineering , University of Canterbury, Christchurch, New Zealand

‡Department of Computer Science, Brock University, St. Catharines, ON, Canada

2 The Proof

The proof is by anti-symmetry of the equality relation. The inclusion

$$(R \cap (R^{\cup})^*)^* \ \subseteq \ R^* \cap (R^{\cup})^*$$

is straightforward: each step uses well-known properties and is self-evident[1]. The calculation doesn't deserve much attention. The opposite inclusion is much more difficult to prove and that is what this note is about.

The goal is to prove that

$$R^* \cap (R^{\cup})^* \ \subseteq \ (R \cap (R^{\cup})^*)^* \quad .$$

We aim to exploit the inductive definition of R^*. Because the other subexpressions are more complicated, we replace them by "S" and "T". The goal becomes to find conditions on S and T such that

$$R^* \cap S \ \subseteq \ T \quad .$$

The calculation is guided by the fact that the conditions must be satisfied by $(R^{\cup})^*$ and $(R \cap (R^{\cup})^*)^*$ but we may be lucky and find weaker conditions. (In fact, we don't.)

$$\begin{array}{ll}
 & R^* \cap S \ \subseteq \ T \\
= & \{ \quad \text{Heyting Galois connection} \quad \} \\
 & R^* \ \subseteq \ S \rightarrow T \\
\Leftarrow & \{ \quad \text{fixed-point definition of } R^* \quad \} \\
 & I \cup R \circ (S \rightarrow T) \ \subseteq \ S \rightarrow T \\
= & \{ \quad \text{Heyting Galois connection} \quad \} \\
 & (I \cup R \circ (S \rightarrow T)) \cap S \ \subseteq \ T \\
= & \{ \quad \text{distributivity} \quad \} \\
 & (I \cap S) \cup (R \circ (S \rightarrow T) \cap S) \ \subseteq \ T \\
= & \{ \quad \text{Galois connection defining ``}\cup\text{''} \quad \} \\
 & I \cap S \subseteq T \ \wedge \ R \circ (S \rightarrow T) \cap S \ \subseteq \ T \\
\Leftarrow & \{ \quad \text{introduce condition on } T \text{ in order to simplify ``}I \cap S\text{''} \quad \} \\
 & I \subseteq T \ \wedge \ R \circ (S \rightarrow T) \cap S \ \subseteq \ T \quad .
\end{array}$$

[1] See the appendix for a short summary of the properties that are needed to complete the proof.

The introduced condition fits with our goal so we proceed with the second conjunct. We begin by seeking a condition on S that enables the elimination of "$S\rightarrow$". To this end, we calculate:

$$
\begin{array}{ll}
 & R\circ(S\rightarrow T) \cap S \\
\subseteq & \{ \quad \text{modularity rule} \quad \} \\
 & R\circ(S\rightarrow T \;\cap\; R^{\cup}\circ S) \\
\subseteq & \{ \quad \text{introduce assumption as prelude to cancellation:} \\
 & \qquad \bullet \quad R^{\cup}\circ S \subseteq S \;. \quad \} \\
 & R\circ(S\rightarrow T \;\cap\; S) \\
\subseteq & \{ \quad \text{(Heyting GC) cancellation} \quad \} \\
 & R\circ T \;\; .
\end{array}
$$

In this way, we have derived the property that, for all R, S and T,

(1) $\quad R\circ(S\rightarrow T) \cap S \;\subseteq\; R\circ T \quad \Leftarrow \quad R^{\cup}\circ S \subseteq S \;\; .$

We now continue the calculation.

$$
\begin{array}{ll}
 & R\circ(S\rightarrow T) \cap S \;\subseteq\; T \\
= & \{ \quad \text{the hardest step in the calculation: as a prelude to applying (1),} \\
 & \qquad \text{we exploit the idempotency of set-intersection} \quad \} \\
 & R\circ(S\rightarrow T) \;\cap\; S \cap S \;\subseteq\; T \\
\Leftarrow & \{ \quad \text{(1) and monotonicity} \quad \} \\
 & R^{\cup}\circ S \subseteq S \;\;\wedge\;\; R\circ T \cap S \;\subseteq\; T \\
\Leftarrow & \{ \quad \text{aiming for fixed-point definition of } T\text{, use modularity rule} \quad \} \\
 & R^{\cup}\circ S \subseteq S \;\;\wedge\;\; (R \cap S\circ T^{\cup})\circ T \;\subseteq\; T \\
\Leftarrow & \{ \quad \text{the left conjunct is satisfied by } S = (R^{\cup})^{*} \;\; ; \\
 & \qquad \text{we postpone introducing this as a condition} \\
 & \qquad \text{but note that, with this instantiation, } S = S\circ S \quad \} \\
 & \qquad R^{\cup}\circ S \subseteq S \;\;\wedge\;\; S = S\circ S \;\;\wedge\;\; T^{\cup} \subseteq S \\
 & \wedge \quad (R\cap S)\circ T \;\subseteq\; T \\
\Leftarrow & \{ \quad \text{fixed-point definition of star} \quad \} \\
 & \qquad R^{\cup}\circ S \subseteq S \;\;\wedge\;\; S = S\circ S \;\;\wedge\;\; T^{\cup} \subseteq S
\end{array}
$$

$$\wedge \quad T = (R\cap S)^*$$

$\Leftarrow \quad \{$ 1st conjunct: fixed-point definition of star

2nd conjunct: reflexivity and transitivity of $(R^\cup)^*$

3rd conjunct: $(R\cap(R^\cup)^*)^* \subseteq R^*$ and $(R^*)^\cup = (R^\cup)^*$ $\}$

$$S = (R^\cup)^* \;\wedge\; T = (R\cap(R^\cup)^*)^* \quad .$$

In the first calculation, we have proved that

$$R^*\cap S \;\subseteq\; T \quad\Leftarrow\quad I\subseteq T \;\wedge\; R\circ(S{\rightarrow}T)\cap S \;\subseteq\; T \quad ,$$

and, in the final calculation, we have proved that

$$R\circ(S{\rightarrow}T)\cap S \;\subseteq\; T \quad\Leftarrow\quad S = (R^\cup)^* \;\wedge\; T = (R\cap(R^\cup)^*)^* \quad .$$

Noting that $I \subseteq (R\cap(R^\cup)^*)^*$ (the condition on T determined by the first calculation), the conclusion of the combined calculations is thus

$$R^*\cap S \;\subseteq\; T \;\Leftarrow\; S = (R^\cup)^* \;\wedge\; T = (R\cap(R^\cup)^*)^* \quad ,$$

from which the desired inclusion immediately follows.

3 Specific Comments

Before making more general remarks, some comments on the calculation are in order.

The central problem in both calculations is how to deal with the occurrence of the intersection operator ("$\cap$") on the lower side of an inclusion ("$\subseteq$").

The first calculation is quite straightforward and relatively self-evident: R^* is by definition a least fixed point and it is very common to use fixed-point induction to establish less obvious properties. (Formally, fixed-point induction is the rule that a least fixed point is a least prefix point. In this case, the rule used is that, for all R and T,

$$R^*\subseteq T \;\Leftarrow\; I\cup R\circ T \subseteq T \quad .$$

There is a choice of which fixed-point definition of R^* to use should the calculation fail.) The combination of fixed-point induction with the use of a Galois connection is also very common. In this case, the Galois connection is, for all R, S and T,

$$R\cap S \subseteq T \quad\equiv\quad R \subseteq S{\rightarrow}T \quad .$$

We have called it the "Heyting Galois connection" because it is essentially the same as the adjunction between $\wedge p$ and $p\Rightarrow$ (for all predicates p) in intuitionistic logic, the formalisation of which is generally attributed to Heyting. The problem of the intersection operator is resolved by simply "shunting" it out of the way and then "shunting" it back. The remaining steps are relatively self-evident. Since the goal is to rewrite T as U^* for some U, the introduction of the condition $I\subseteq T$ on T is an obvious step to take.

The second calculation is also relatively straightforward. The issue that must be resolved is that the initial calculation has introduced "$S\to$" on the left side of an inclusion. It is vital that this is eliminated. The Heyting Galois connection suggests a line of attack: specifically, we have the cancellation rule: for all S and T,

$$(S\to T)\cap S \subseteq T \ \ .$$

Aiming to apply cancellation, the calculation begins by applying the modularity rule. In this way, (1) is easily derived.

Undoubtedly, the hardest step of all is the first step of the third calculation: the step in which idempotency of set intersection is applied to replace "$\cap S$" by "$\cap S\cap S$". Effectively, instead of (1), the equivalent property

(2) $$R\circ(S\to T)\cap S \subseteq R\circ T\cap S \quad\Leftarrow\quad R^{\cup}\circ S\subseteq S$$

has been applied. In fact, (2) can be further strengthened by replacing the inclusion on the consequent by an equality since

$$\begin{array}{ll}
 & R\circ T\cap S \subseteq R\circ(S\to T)\cap S \\
= & \{ \quad \text{Galois connection defining intersection} \quad \} \\
 & R\circ T\cap S \subseteq R\circ(S\to T) \ \wedge\ R\circ T\cap S \subseteq S \\
= & \{ \quad X\cap S\subseteq S \text{ with } X:=R\circ T \quad \} \\
 & R\circ T\cap S \subseteq R\circ(S\to T) \\
\Leftarrow & \{ \quad R\circ T\cap S \subseteq R\circ T \quad \} \\
 & R\circ T \subseteq R\circ(S\to T) \\
\Leftarrow & \{ \quad \text{monotonicity of composition} \quad \} \\
 & T \subseteq S\to T \\
= & \{ \quad \text{Heyting Galois connection} \quad \} \\
 & T\cap S \subseteq T \\
= & \{ \quad \text{property of intersection} \quad \} \\
 & \mathsf{true} \ \ .
\end{array}$$

Thus, by antisymmetry of the subset ordering together with (2),

(3) $$R\circ(S\to T)\cap S = R\circ T\cap S \quad\Leftarrow\quad R^{\cup}\circ S\subseteq S \ \ .$$

Although the stronger property (3) is not used directly, its derivation provides a useful safety check: because we have derived an equality, we know that simplifying the expression "$R \circ (S \rightarrow T) \cap S$" to "$R \circ T \cap S$" does not incur any loss of information (so long as the condition $R^{\cup} \circ S \subseteq S$ is satisfied). This is the raison d'être for the use of the idempotence of set intersection.

4 General Comments

So much for the details of the calculation; now more general comments.

Since the earliest days of the development of "correct-by-construction" program design techniques, goal-directed reasoning has always been a central theme of "program calculation". For example, "programming as a goal-oriented activity" was a specific topic in Gries's textbook "The Science of Programming" [Gri81, chapter 14], and broadening the theme to the mathematics of program construction was the topic of Van Gasteren's thesis [vG90]. Goal-directed reasoning is also evident in many of Dijkstra's "EWD"s (available from the University of Texas) and many other publications of the last fifty years.

In contrast, the standard mathematical style is "bottom-up". That is evident from the fact that mathematicians almost always use *only-if* arguments (implication) as opposed to *if* arguments (follows-from). In our view, it is extremely important that the more challenging calculations are presented in a goal-directed way, as we have tried to do above. It is important because it helps to teach the creative process underlying the mathematics of program construction. Of course, when a new theory is being developed the work proceeds in a bottom-up fashion: one identifies the more straightforward properties and builds up to properties that are not so obvious. But each step in the process is an exploration. One seeks properties of a certain type (for example, distributivity properties) but the exact form of the properties is not known at the outset. It is vital that we develop a style of calculation that exposes the creative process and that we communicate this process to our students.

Many calculations are, of course, straightforward and don't merit much discussion. Less interesting calculations are ones where each step *simplifies* the expression under consideration (in some sense of the word "simplify"). In contrast, the calculation above involves several *complification* steps. In particular, the step we have singled out as the hardest of all is a complification step: idempotency is used in the derivation of (1) to replace an expression of the form $X \cap S$ by $X \cap S \cap S$. Idempotency is normally presented as a simplification rule whereby the number of occurrences of the operator in question is reduced. In order to foster creative calculation, it is also vital to avoid an undue bias in the presentation of equational properties; equality is after all a symmetric operator.

In summary, what we have presented is, in our view, a very good example of a non-trivial calculation that deserves careful study. We hope that, in future, more effort is spent in research publications and textbooks on elucidating the process of creative calculation. Historically one argument against calculations in the style above is the need to save space. But modern technology —the much reduced reliance on "hard copy"— makes this argument much less relevant.

References

[BDGv22] Roland Backhouse, Henk Doornbos, Roland Glück, and Jaap van der Woude. Components and acyclicity of graphs. An exercise in combining precision with concision. *Journal of Logical and Algebraic Methods in Programming*, 124:100730, 2022.

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

[vG90] Antonetta J.M. van Gasteren. *On the Shape of Mathematical Arguments.* Number 445 in LNCS. Springer-Verlag, 1990.

Appendix

In the proof we use a number of properties without specific mention. These properties will be well-known to readers well-versed in relation algebra but for others may not be so. For this reason, we give a very brief summary of the relevant properties.

Variables R, S and T in the proof all denote homogeneous binary relations. The set notation we use ("$\subseteq$", "$\cap$" and "$\cup$") has its standard meaning and we do assume familiarity with the properties of the set operators. (Some readers may not be familiar with the Heyting Galois connection: the existence of an upper adjoint of $\cap S$ (for all S) is a consequence of the universal distributivity of set-intersection over set-union.)

Relation composition and converse are denoted by "$\circ$" and "$^{\cup}$", respectively, and the identity relation is denoted by I. All of intersection, union, composition and converse are monotonic with respect to the subset ordering. Also, the logical operator "$\wedge$" is monotonic with respect to the "$\Leftarrow$" relation.

An example of a step that uses a number of the above properties without specific mention is the final step in the initial calculation. In full detail, we use the fact that $I{\cap}S \subseteq I$, that the subset relation is transitive (so $I{\cap}S \subseteq I \wedge I \subseteq T \;\Rightarrow\; I{\cap}S \subseteq T$) and that "$\wedge$" is monotonic with respect to the "$\Leftarrow$" relation. Monotonicity of composition is used when the cancellation rule for the Heyting Galois connection is applied.

Converse is defined by the Galois connection, for all R and S,

$$R^{\cup} \subseteq S \;\equiv\; R \subseteq S^{\cup}$$

together with the distributivity property, for all R and S,

$$(R{\circ}S)^{\cup} \;=\; S^{\cup} \circ R^{\cup}$$

and the property that

$$I^{\cup} = I \quad .$$

The modularity rule (aka the Dedekind rule) is used in both its forms: for all R, S and T,

$$R{\circ}S \cap T \;\subseteq\; R{\circ}(S \cap R^{\cup} \circ T)$$

and its symmetric counterpart

$$R \cap S{\circ}T \;\subseteq\; (R \circ T^{\cup} \cap S){\circ}T \quad .$$

The rule is important because composition does not distribute over intersection: it gives a handle on expressions involving both operators where the intersection is on the lower side of a set inclusion.

R^* denotes the reflexive, transitive closure of R. The inductive definition of R^* used here[2] is the property that, for all T,

$$R^* \subseteq T \;\Leftarrow\; I \cup R{\circ}T \subseteq T \quad .$$

That is, R^* is the least prefix point of the function mapping T to $I \cup R{\circ}T$. We don't directly use the fact that R^* is a fixed point of this function but we do use the (derived) properties that, for all R,

$$I \subseteq R^* \quad\wedge\quad (R^*)^* \;=\; R^* \quad\wedge\quad R^* \circ R^* \;=\; R^* \quad\wedge\quad (R^{\cup})^* = (R^*)^{\cup} \quad .$$

We also use the fact that the star operator is monotonic with respect to the subset ordering. As an example of the explicit use of these properties we present the proof of the omitted inclusion:

$$(R \cap (R^{\cup})^*)^* \;\subseteq\; R^* \cap (R^{\cup})^*$$

$$= \qquad \{ \qquad \text{Galois connection defining intersection} \qquad \}$$

$$(R \cap (R^{\cup})^*)^* \subseteq R^* \quad\wedge\quad (R \cap (R^{\cup})^*)^* \subseteq (R^{\cup})^*$$

[2] An alternative fixed-point definition —alluded to in the text— is the direct formalisation of the property that R^* is the least reflexive, transitive relation that contains R.

$$
\begin{array}{ll}
\Leftarrow & \{ \quad \text{1st conjunct: star is monotonic} \\
& \quad\;\; \text{2nd conjunct: } (R^*)^* = R^* \text{ (with } R{:=}R^\cup\text{) and star is monotonic} \quad \} \\
& R\cap(R^\cup)^* \subseteq R \quad\wedge\quad R\cap(R^\cup)^* \subseteq (R^\cup)^* \\
= & \{ \quad \text{Galois connection defining intersection} \quad \} \\
& R\cap(R^\cup)^* \subseteq R\cap(R^\cup)^* \\
= & \{ \quad \text{reflexivity of the subset relation} \quad \} \\
& \mathsf{true} \;\; .
\end{array}
$$

It is mentioned in the introduction that the identity we have proved is central to a number of algorithms that exploit graph theory. In such algorithms, the relation R is the edge relation on nodes of a finite graph: specifically, two nodes u and v are related by R iff there is an edge in the corresponding graph from u to v. Conversely, two nodes u and v are related by $R^\cup$ iff there is an edge in the graph from v to u. The graph corresponding to $R^\cup$ is thus the graph obtained by reversing the edges of the graph corresponding to R. Nodes u and v are related by R^* iff there is a path from u to v in the graph, and by $(R^\cup)^*$ iff there is a path from u to v in the graph formed of reversed edges. (Equivalently, u and v are related by $(R^\cup)^*$ if there is a path from v to u in the graph. Formally, the equivalence is expressed by the identity $(R^\cup)^* = (R^*)^\cup$.)

The relation $R^*\cap(R^\cup)^*$ holds between nodes u and v if there is both a path from u to v and a path from v to u in the corresponding graph. Thus $R^*\cap(R^\cup)^*$ is the equivalence relation that holds between nodes u and v when both are in the same strongly connected component of the graph.

The relation $R\cap(R^\cup)^*$ holds between nodes u and v iff there is an edge from u to v and a path from v to u. The proven identity thus states that nodes u and v are strongly connected iff there is a path from u to v in the graph corresponding to this relation. This insight is fundamental to algorithms that determine the strongly connected components of a graph as well as the decomposition of a graph into its strongly connected components together with an acyclic graph connecting such components.