

Math 351:03 — Fall 1999

MW4 SEC-217

Prof. Bumby

Solution to a messy problem. Exercise 1.2#14(e) was (incompletely) discussed in class. It was indicated that one way to see that the result is true is to examine the eight cases obtained by independently asking whether a point x belongs to each of the sets A, B, C . Since the answers to these questions determine whether x belongs to any set described in terms of A, B, C using the constructions of union and intersection, this gives a process for verifying that the set on the left of the desired identity contains exactly the same points as the set on the right. Although this works very well as a decision procedure, it does not give the feeling of being a *proof*. To remedy this, let me try to finish the approach that I started before suggesting that approach.

Analysis and synthesis. A mathematical proof is supposed to be written as a deductive argument. You are supposed to be able to follow it step by step and come away convinced that that the theorem has been proved; but if you are to write your own proofs, you also need to know how to discover that statements are true and to build the proof. At the very least, the proof must contain statements that reflect the statement of the desired result. If the result is difficult, the proof will contain a lot more. Solutions to exercises in a textbook may sometimes require a clever insight (particularly in *this* textbook), but should otherwise be expected to be straightforward.

For exercises in set notation, we may take as given the operations of union and intersection, and their interpretation using the words “or” and “and” with the usual properties of these words taken for granted. In keeping with the approach to *everything else* in this course, we should have used this interpretation to formulate our understanding of the operations on set as *axioms*, and based all subsequent proofs on these axioms. In trying to construct a proof in the style used in this section of the text, we will be forced to identify basic rules for interpreting operations on sets.

Forwards and Backwards. The finished proof will be written as a deduction, but the statement of the theorem tells us what the *last* line of the proof must be.

Examining this, it is often clear that there is only one way to prove that statement, so you can fill in more steps at the end of the proof. If the statement you are proving is an implication $A \implies B$, you also know that it will begin by asserting A and end by confirming that you have deduced B . Simple consequences of A should be recorded near the beginning of the proof. When you have exhausted all things that can be filled in easily at the beginning and end of the proof, you usually look for an important landmark in the middle. This is where you use your *insight* to identify how to connect the beginning and end of the proof.

Various techniques of proof like *division into cases* or *proof by contradiction* also lead to structuring the proof into pieces that are combined using the words that you always see in that type of proof.

Two inclusions are likely to be easier than one identity. This exercise asks us to prove the associative law for the *symmetric difference* operation defined by

$$A + B = (A - B) \cup (B - A). \tag{S}$$

The proof should be organized as a proof of

$$A + (B + C) \subseteq (A + B) + C \tag{1}$$

followed by a proof of

$$(A + B) + C \subseteq A + (B + C) \tag{2}$$

and ending with the statement that (1) and (2) show that the sets are equal because each contains the other. The proofs of the two statements will be similar (because of a symmetry in the form of the statements), but (depending on your audience) you may want to prove both without hinting that you used a mechanical process to change the first proof into the second.

Inclusion is implication. A statement of the form $X \subseteq Y$ is proved by introducing an arbitrary element x and proving $x \in X \implies x \in Y$. The proof leading to (1) must then begin:

- Let $x \in A + (B + C)$.

and end:

- Thus $x \in (A + B) + C$.

Depending on how long the proof is, you may need to remind the reader of where you began, but you should conclude by stating (1) and asserting that its proof is complete.

New symbols must be defined in terms of familiar ones. All we know about this operation $A + B$ is proved in this exercise, so, after quoting (S) the next line of the proof of (1) should say something like:

- Using (S), this means $x \in (A - (B + C)) \cup ((B + C) - A)$.

You then interpret the union of sets, and begin the division into cases. The word “or” signifies that you should divide into cases, and we have *name* those cases. Each case begin with one of the hypotheses separated by “or”, but it should end with the *whole* conclusion.

- Thus $x \in (A - (B + C))$ (case A) **or** $x \in ((B + C) - A)$ (case BC).

Each case is likely to prove only part of the conclusion. Before going too far, we should try to anticipate how the proof of each case will end. The line that we want to use as the last line of the proof of (1) also contains the new symbol $+$, so our proof is a proof of:

$$x \in ((A + B) - C) \text{ or } x \in (C - (A + B)).$$

If the case we are considering does not split into subcases, it is likely to lead to only one of these two possibilities. The possibility that is irrelevant in one case can be tacked on since we are only proving an implication. We should aim for only one of these cases in each part of the proof.

All remaining appearances of $+$ will also need to be expressed in terms of set union and set difference using (S), and this will lead to the subcases. For each case, we try to identify one way that the conclusion can hold and concentrate on proving that.

Splitting the second case. Let’s begin with case BC. The first two statements of that proof are:

$$\begin{aligned} x &\in B + C \\ x &\notin A \end{aligned}$$

but the $+$ in the first of these statements needs to be expressed in terms of more basic operations. As before, this leads to a division into case B, where $x \in B$, $x \notin C$, and our previous observation that $x \notin A$; and case C, where $x \in C$, $x \notin B$, and $x \notin A$.

One case can now be wrapped up. In case B, we have

$$x \in B - A \subseteq A + B$$

and $x \notin C$, giving $x \in ((A + B) - C)$, which has been found to be one way of reaching the desired conclusion.

One case leads to lemmas. Processing the information in case C introduces some general properties that are simple observations that may not have been noted before. They are also useful enough that we would like to use them without having to stop for a proof. They should be stated using new variables to name the sets to indicate that they apply more generally. These statements are:

- Negation Lemma: $(X - Y) \cap (X - Z) = X - (Y \cup Z) = (X - Y) - Z$.
- Union Lemma: $X + Y \subseteq X \cup Y$.
- Complement Lemma: If $Y \subseteq Z$, $X - Z \subseteq X - Y$.

The quantities X , Y , and Z that appear as *free variables* in these statements should be interpreted as if each statement began, “For all X , Y , and Z ...” (it doesn’t hurt to mention Z in this way in the Union Lemma, where it is otherwise ignored).

Each of these is proved by a simple consideration of how membership in X , Y and Z affects membership in the sets mentioned in the lemma.

Finishing another case. In case C , $x \in C$ and $x \notin A$, so $x \in C - A$. Similarly, $x \in C - B$. Thus the Negation Lemma (with $X = C$, $Y = A$ and $Z = B$) gives $x \in C - (A \cup B)$. The Union Lemma (with $X = A$ and $Y = B$) says that $A + B \subseteq A \cup B$, so the Complement Lemma (with $X = C$, $Y = A + B$ and $Z = A \cup B$) gives $x \in C - (A + B)$, finishing the proof of case C .

Splitting the remaining case. To begin case A , we need to interpret $x \in (A - (B + C))$ as

$$x \in \left(A - \left((B - C) \cup (C - B) \right) \right).$$

The Negation Lemma turns this into $x \in (A - (B - C))$ **and** $x \in (A - (C - B))$. To interpret this, we formulate the

- Double Negative lemma: $X - (Y - Z) = (X - Y) \cup (X \cap Y \cap Z)$.

which is again proved by considering the eight cases of membership in the three sets X , Y and Z independently.

Case A should then be divided into the cases where $x \in A \cap B \cap C$ and *everything else*. The first case is allowed by both applications of the Double Negative Lemma, $X = A$, $Y = B$, $Z = C$ or $X = A$, $Y = C$, $Z = B$. In the second case, this possibility is excluded, so the other option of the Double Negative Lemma holds with each assignment of values to X , Y , Z . Thus $x \in A - B$ **and** $x \in A - C$. The second form of the Negation Lemma gives $x \in (A - B) - C$. Since $A - B \subseteq A + B$, we can get one part of the conclusion from the

- Monotonicity Lemma: If $X \subseteq Y$, then $X - Z \subseteq Y - Z$.

The last case. To deal with $x \in A \cap B \cap C$, we show that $A \cap B \cap C \subseteq (C - (A + B))$. To show this directly, we need to show that, if $x \in C$ and $x \in A \cap B$ then $x \notin A + B$ (since it is known that $x \in C$). However, if $x \in A + B$ and $x \in A$, then we must have $x \notin B$, contradicting the assumption that $x \in C$.

Conclusion. All pieces of the proof of one conclusion have now been discovered. They need to be rearranged to form a deductive argument with the lemmas that we extracted given before starting the main proof. With a little more work, another lemma might be extracted from the last case, but we can leave that as a special argument. The reverse inclusion then needs to be proved. It will look exactly like the proof of the forward inclusion.

Why was this so difficult? Set theory has some paradoxes. If you are too careless in allowing sets to be defined by properties, you can come up with a description for which there are things for which it cannot be decided whether they have the property or not. An extremely cautious way to avoid such paradoxes is to only allow members of a known set to be tested for having some property. This allows the set $X - Y$ to appear, but avoids having an absolute “property of not being in Y ”. In the last case, a special argument was given because of loss of patience with this extreme caution.

A related matter is that we have introduced the symbol \cup for the union of sets, but the only rules we have for working with this place no restriction on the intersection of the sets. Our informal language for talking about sets includes the concept of *disjoint union*. If you can break a set into pieces such that a point of the set lies in exactly one piece, then an argument based on a division into cases can be made a lot sharper. Within each case, it may even be possible to give an efficient proof of an equivalence. If you look closely at the above analysis, we find that unraveling the definition (S) splits the set into two sets and then splits each of these into two sets. The different ways of associating the operation give two independent ways of performing this construction.

Finally, we jumped into proving something without first proving a lot of easier properties that could be used as axioms. Some of this was corrected as we went through the proof by extracting lemmas and giving them colorful names, but we don't have a neat set of axioms that allow a systematic development of the basic properties of the operations we want to perform on sets. However, the collection of all properties proved in exercise 1.2#13, shows that the operations defined there behave very much like we expect an addition and multiplication to behave (although (d) is a little disturbing, and (c) is curious). This suggests that these operations should be taken as the basic ones and $A \cup B$ defined as $A + B + A \cdot B$.

Where's the proof? After all this talk about how to prove the result, a proof was never given. Well, yes and no. The steps of the proof were identified and instructions were included to allow them to be arranged in order to form a deductive argument, so *doing* that would show nothing new.

Another reason for abandoning the proof is that there is a short proof using the decision procedure that applies more generally to analyze any statement about a finite number of sets. Since the best we could come up with would be two proofs of inclusions, each involving four cases, a mechanical process involving only eight cases seems more attractive.

Why was this written? You will see enough proofs, but it is rare that you get to examine the process of discovering a proof. It is easy to see that a deductive argument does what it claims to do, but good proofs can hide the analysis that led to their discovery. If you are going to *do* mathematics, you need to do more than string proofs together in the hope of eventually reaching something interesting. To solve a problem, you sometimes need to imagine a proof written out in full detail so you can think about what will appear in the *middle* of the proof. Proofs in algebra are often so tightly structured that this can be done.

Another purpose of this essay is to highlight the concept of *lemma*. Although the main flow of a deductive proof is one step after another, the steps don't always build on their immediate predecessor. Parts of the proof that are used several times, or introduced as one of many pieces that will be combined later, need to have a label. Extracting such statements from a proof means that the main proof can be shorter, more direct, and easier to understand.