

The dangers of preserving symmetry

We are asked to show that a group is symmetric —that is, satisfies

$$(0) \quad x * y = y * x \quad , \quad \text{for all } x , y \text{ —}$$

whenever it satisfies

$$(1) \quad x * x = e \quad , \quad \text{for all } x \quad ,$$

where e is the identity element of the group.

Since formula (0) is as symmetrical as we could like it to be, one might think that an ideal proof of (0) should respect that symmetry, say by transforming (0) directly into **true**. The reader is invited to try his hand at such an approach; however, the only reasonable, symmetry-preserving ideas I could come up with yielded repetitive manipulations which had to be applied to both sides of the equality, manipulations which in the end went in circles and amounted to nothing. I highly doubt a proof along such lines is possible.

One way to prove (0) is to observe for all x , y :

$$\begin{aligned} & x * y \\ = & \quad \{ \text{aiming to introduce } y \text{ into the left side of the equation, and (1)} \\ & \quad \text{can be used for this introduction, provided we can introduce } e ; \text{ we} \\ & \quad \text{can introduce } e \text{ with simple algebra } \} \\ & e * x * y \\ = & \quad \{ (1) , \quad x := y \quad \} \\ & (y * y) * x * y \\ = & \quad \{ \text{repeating with } x \text{ on the right side } \} \\ & y * y * x * y * x * x \\ = & \quad \{ (1) , \quad x := y * x \quad \} \\ & y * e * x \\ = & \quad \{ \text{algebra } \} \\ & y * x \quad . \end{aligned}$$

This is a nice proof, so much so that we have even proved the stronger result that (0) implies (1) for monoids — “groups without inverses” — . But notice that in this proof we broke the symmetry right from the start, by trying to transform one side of (0) into the other, rather than manipulating (0) directly.

* *

 *

What is happening here?

First, let us recall why, in general, we don't want to break symmetry. The first and second proofs in Netty van Gasteren's thesis are good examples of why we don't: Namely, by preserving symmetry, we suppress irrelevant distinctions, thereby shortening our arguments; while by breaking symmetry, we often have to treat cases separately, and case analysis can easily lead to an unmanageable mess.

However, this is only one side of the story. In EWD1311, by Edsger Dijkstra, the attempt to preserve symmetry forces Dijkstra to repeat the same argument four times. We see similar—even fatal!—consequences when trying to preserve symmetry in a proof of $(0) \Leftarrow \mathbf{true}$. And breaking symmetry may not always lead to case analysis: the problem under discussion is a perfect example.

More importantly, observe that the symmetry we see in (0) involves $*$, an operator whose symmetry we can only exploit after we prove (0) ! So because we *cannot* exploit symmetry in (0) , it becomes crucial to *break* the symmetry somewhere, hopefully early on in the proof. And indeed, choosing to break the symmetry by transforming one side of (0) into the other yields the fairly manageable proof above.

$$* \quad * \quad *$$

Now observe what happens if we break the symmetry of (0) while exploiting another symmetry hidden in formula (1) . Introducing the prefix operator \sim for the inverse, by algebra we can rewrite (1) as:

$$(1') \quad x = \sim x \quad ;$$

that is, there is a symmetry between elements of the group and their inverses.

With this in mind, there is really only one way to break the symmetry of (0) , by rewriting it as:

$$(0') \quad x * y * \sim x * \sim y = e \quad ,$$

which we prove as follows:

$$\begin{aligned} & x * y * \sim x * \sim y \\ = & \{ (1') \text{ twice; once with } x := x \text{ and once with } x := y \} \\ & x * y * x * y \\ = & \{ (1) \text{ with } x := x * y \} \\ & e \end{aligned}$$

This new proof still uses (1) three times, but look how mindless their applications have become, compared to those in the original proof! On the other hand, we have sacrificed generality for smoothness: by introducing inverses, our proof became simpler, but now no longer works for monoids.

* *

 *

One lesson to be learned here is that when inverses can be exploited,

$$(2) \quad x * y * \sim x * \sim y = e$$

may be a much better demonstrandum than (0) when trying to establish that $*$ is symmetric. To see this principle in action, suppose that we do not know (1), but instead we know there exists some endomorphism E on our group satisfying $E.x = \sim x$, for all x . Now that inverses have been brought into play, we prove (0) by proving (2):

$$\begin{aligned} & x * y * \sim x * \sim y \\ = & \quad \{ \text{defining property of } E, \text{ twice} \} \\ & x * y * E.x * E.y \\ = & \quad \{ \text{morphism property} \} \\ & x * y * E.(x * y) \\ = & \quad \{ \text{defining property of } E \} \\ & x * y * \sim(x * y) \\ = & \quad \{ \text{definition of inverse} \} \\ & e \quad . \end{aligned}$$

The other, larger, lesson to be learned, I think, is that one should be just as wary of preserving symmetry as of breaking it. The formulae that should be symmetrical are precisely those that deserve to be. In the original problem (0) was symmetrical, while (1) was not, and we could not find a really elegant solution until we turned that situation on its head.

Santa Cruz, 3-5 November 2004

Revised: Culver City, 29 August 2005

Jeremy Weissmann
11260 Overland Ave. #21A
Culver City, CA 90230
USA
jeremy@mathmeth.com