Deductive reasoning and model-building: an algebraic perspective

In formal approaches to software development, two kinds of activity are prominent. One is concerned with exploiting automated reasoning, the other with using the computer in building and checking models to test hypotheses. These general principles are illustrated in the way that mathematicians have approached the study of algebraic structures such as *groups*.

Definition of a group, as given on p168 of Huth & Ryan:

A **group** is a tuple $(G,*,1)$, where $*: G\times G\to G$ is a function and $1 \in G$ such that

- G1: for every $x \in G$ there is some $y \in G$ such that $x*y = y*x = 1$ (any such y is called an inverse of x)
- G2: for all x,y,z in G, we have $x * (y * z) = (x * y) * z$; and
- G3: for all $x \in G$, we have $x*1 = 1*x = x$.

[The term *group multiplication* will be used below to refer to the function $*$.]

---

1. **Informal deduction from axioms:** Each element x has a unique inverse.

Proof: if y and z are both inverses for x, then
$x*y = y*x = 1$ and $x*z = z*x = 1$.
Hence: $y = 1*y = (z*x)*y = z*(x*y) = z*1 = z$

Definition: G is *commutative* if for all x,y in G, we have $x * y = y * x$.

---

2. **Informal deduction from axioms and additional hypothesis:** If each element $x \in G$ is such that $x*x = 1$, then G is commutative.

Consider the element $x * y$. It must be the case that $(x * y) * (x * y) = 1$.

This means that $x * (y * x) * y = 1$, which in turn means that
$x * x * (y * x) * y * y = x * y$. Since $x*x = 1$ and $y*y = 1$, the LHS of this expression simplifies to $y * x$, proving that x and y commute.

---

3. **Motivating model-building and model-checking:** Suppose that G is a group such that:

- every element of G can be expressed as a product of the two elements x and y in G;
- $x * x = 1$ and $y * y = 1$.

Does it follow that G is commutative?

The answer to this question is no. To reach this conclusion, it is necessary to construct a group that satisfies the stated conditions, but isn't commutative. Deduction from axioms can go some way to guiding this construction. For instance, since $x * x = 1$ and $y * y = 1$, any element in G that is expressed as a product of x's and y's can be expressed as a product in which x's and y's alternate. This means that all the elements of G have to expressible in at least one way as one of the family of products:
1, x, y, x*y, y*x, x*y*x, y*x*y, x*y*x*y, y*x*y*x, x *y*x*y*x, ...
[Note that the element 1 here is the *empty product* of "zero" x's and y's.]

It turns out that if we just consider this set of products with the multiplication $*$, then we already have an infinite group, where each element is represented by a distinct string in the above list, and the inverse of

an element is obtained by reversing that string. (Thus, for instance, the inverse of x∗y∗x is itself, whilst the inverse of x∗y∗x∗y is y∗x∗y∗x.) Checking that the group axioms hold for this structure is an exercise in *model-checking*.

Getting the computer to generate and check an infinite structure is of course rather problematic! In fact, in this case, there are finite examples of groups that satisfy the stated conditions but are not commutative. The smallest of these is the group where there are six distinct elements:
1, x, y, x∗y, y∗x, and x∗y∗x = y∗x∗y.

A mathematician would know that such a model existed from informal basic knowledge of groups. The above six element group structure arises as the symmetries of an equilateral triangle, where x corresponds to flipping the triangle over around the axis of symmetry passing through one vertex, and y to flipping the triangle over around the axis of symmetry passing through another vertex. The resulting group is known as the dihedral group D_3. The infinite group described above is known as the *infinite dihedral group*. For more background, you can consult other sources, such as the Wikipedia entry on dihedral groups.

The above discussion points to possible limitations in formal reasoning from axioms that may not be resolved by using computers. In fact, the famous results of Turing and Gödel confirm this decisively, showing that there are inherent limitations in automated reasoning that cannot be overcome. This is the background to the thinking of Emil Post, a mathematician who himself made a significant contribution to the study of unsolvable and undecidable problems.

In the conclusion to his paper 'Absolutely unsolvable problems and relatively undecidable propositions' - submitted to a mathematics periodical in 1941, but rejected, and not published until after his death! - Post writes:

> *... perhaps the greatest service the present account could render would stem from its stressing of its final conclusion that mathematical thinking is, and must be, essentially creative. It is to the writer's continuing amazement that ten years after Gödel's remarkable achievement current views on the nature of mathematics are thereby affected only to the point of seeing the need of many formal systems, instead of a universal one. Rather has it seemed to us to be inevitable that these developments will result in a reversal of the entire axiomatic trend of the late nineteenth and early twentieth centuries, with a return to meaning and truth. Postulational thinking will then remain as but one phase of mathematical thinking.*

In this module, we shall introduce a simple computer tool for model-checking - Alloy - that can be used to assist in the discovery of counterexamples such as we have illustrated above. Model-checking can be seen as an activity that aims to use the computer in a manner that fits in well with the shift in emphasis that Post is endorsing. Though using the computer is no substitute for human creativity and intuition, it can be very helpful in informal testing of conjectures and in generating examples to guide reflection and promote insight.
