

## Swapping the values of two variables

This short note explains a well-known programming trick that is rarely presented in a way that highlights the relevant properties of the operators involved in its solution. Our goal is to investigate the traditional solution, and see which properties of the operators that solution depends on, towards generalizing it.

The problem is how to swap the values of two variables without using another temporary one, and the solution that is usually presented assumes that the values can be represented as sequences of bits and exploits the bitwise exclusive-or operation (here denoted by  $\oplus$ ). Using the Guarded Command Language, it can be written as:

$$\begin{aligned} & \{ x = X \wedge y = Y \} \\ & x := x \oplus y ; \\ & y := x \oplus y ; \\ & x := x \oplus y \\ & \{ x = Y \wedge y = X \} . \end{aligned}$$

Now, in order to determine which properties of  $\oplus$  are involved and which other operators can be used, let's change  $\oplus$  to an arbitrary operator  $\otimes$  and present all the relevant annotations. Working back from the postcondition to the precondition yields:

$$\begin{aligned} & \{ x = X \wedge y = Y \} \\ & \{ (x \otimes y) \otimes ((x \otimes y) \otimes y) = Y \wedge (x \otimes y) \otimes y = X \} \\ & x := x \otimes y \\ & \{ x \otimes (x \otimes y) = Y \wedge x \otimes y = X \} \\ & y := x \otimes y \\ & \{ x \otimes y = Y \wedge y = X \} \\ & x := x \otimes y \\ & \{ x = Y \wedge y = X \} . \end{aligned}$$

In order to swap the values of  $x$  and  $y$ , we take the conjunction of the two initial assertions and we get the following implied conditions:

$$(x \otimes y) \otimes ((x \otimes y) \otimes y) = y \quad , \text{ and}$$

$$(x \otimes y) \otimes y = x \quad .$$

We want to find properties of the operator  $\otimes$  that make these conditions hold. Starting with the simpler condition, i.e. with the second one, and using square brackets to denote universal quantification over all free variables, we calculate:

$$\begin{aligned}
 & (x \otimes y) \otimes y \\
 = & \quad \{ \text{in order to isolate } x, \text{ let } \otimes \text{ be associative} \} \\
 & x \otimes (y \otimes y) \\
 = & \quad \{ \otimes \text{ is unitpotent, that is:} \\
 & \quad [ z \otimes z = 1_{\otimes} ] , \text{ where } 1_{\otimes} \text{ is the unit of } \otimes \} \\
 & x .
 \end{aligned}$$

The second condition is thus satisfied by assuming that  $\otimes$  is associative and unitpotent. The first condition can be calculated using the same properties:

$$\begin{aligned}
 & (x \otimes y) \otimes ((x \otimes y) \otimes y) \\
 = & \quad \{ \otimes \text{ is associative} \} \\
 & ((x \otimes y) \otimes (x \otimes y)) \otimes y \\
 = & \quad \{ \otimes \text{ is unitpotent} \} \\
 & y .
 \end{aligned}$$

Hence, the two properties of  $\otimes$  that validate the program presented are:

$\otimes$  is associative , and

$\otimes$  is unitpotent .

Clearly, the bitwise exclusive-or — or, as I prefer to call it, the bitwise inequivalence — is suitable. But note that the bitwise equivalence (usually denoted by  $\equiv$ ) is also suitable!

## Generalising $\otimes$

We now generalise  $\otimes$  by replacing each occurrence with a separate operator. The new program and corresponding annotation become:

$$\begin{aligned}
 & \{ x = X \wedge y = Y \} \\
 & \{ (x \otimes y) \oplus ((x \otimes y) \oplus y) = Y \wedge (x \otimes y) \oplus y = X \} \\
 & x := x \otimes y \\
 & \{ x \oplus (x \oplus y) = Y \wedge x \oplus y = X \}
 \end{aligned}$$

$$\begin{aligned}
& \mathbf{y} := \mathbf{x} \oplus \mathbf{y} \\
& \{ \mathbf{x} \ominus \mathbf{y} = \mathbf{Y} \wedge \mathbf{y} = \mathbf{X} \} \\
& \mathbf{x} := \mathbf{x} \ominus \mathbf{y} \\
& \{ \mathbf{x} = \mathbf{Y} \wedge \mathbf{y} = \mathbf{X} \} .
\end{aligned}$$

Again, the conjunction of the two initial assertions imply the following conditions:

$$(\mathbf{x} \otimes \mathbf{y}) \ominus ((\mathbf{x} \otimes \mathbf{y}) \oplus \mathbf{y}) = \mathbf{y} \quad , \text{ and}$$

$$(\mathbf{x} \otimes \mathbf{y}) \oplus \mathbf{y} = \mathbf{x} \quad .$$

As before, the goal is to investigate which properties of the operators make these conditions hold. Starting with the second condition, we calculate:

$$\begin{aligned}
& (\mathbf{x} \otimes \mathbf{y}) \oplus \mathbf{y} \\
= & \quad \{ \otimes \text{ associates with } \oplus \} \\
& \mathbf{x} \otimes (\mathbf{y} \oplus \mathbf{y}) \\
= & \quad \{ \oplus \text{ is unitpotent with respect to } \otimes , \text{ that is:} \\
& \quad [ \mathbf{z} \oplus \mathbf{z} = \mathbf{1}_{\otimes} ] , \text{ where } \mathbf{1}_{\otimes} \text{ is the unit of } \otimes \} \\
& \mathbf{x} .
\end{aligned}$$

Now, the first condition:

$$\begin{aligned}
& (\mathbf{x} \otimes \mathbf{y}) \ominus ((\mathbf{x} \otimes \mathbf{y}) \oplus \mathbf{y}) \\
= & \quad \{ \text{previous calculation} \} \\
& (\mathbf{x} \otimes \mathbf{y}) \ominus \mathbf{x} \\
= & \quad \{ \otimes \text{ is symmetric} \} \\
& (\mathbf{y} \otimes \mathbf{x}) \ominus \mathbf{x} \\
= & \quad \{ \otimes \text{ associates with } \ominus \} \\
& \mathbf{y} \otimes (\mathbf{x} \ominus \mathbf{x}) \\
= & \quad \{ \ominus \text{ is unitpotent with respect to } \otimes \} \\
& \mathbf{y} .
\end{aligned}$$

Note that the choices made in this calculation could be different. The final section of this note deals with a different and interesting one that leads to different properties. Now, from the two previous calculations we conclude that our new program is correct if the following properties hold:

- $\otimes$  is symmetric ,
- $\otimes$  associates with  $\oplus$  ,
- $\otimes$  associates with  $\ominus$  ,
- $\oplus$  is unitpotent with respect to  $\otimes$  , and
- $\ominus$  is unitpotent with respect to  $\otimes$  .

It is not difficult to see that, with respect to these conditions, operations  $\oplus$  and  $\ominus$  are identical. In fact, adopting these five properties, we can prove that  $\oplus$  and  $\ominus$  are the same operation:

$$\begin{aligned}
 & x \oplus y \\
 = & \quad \{ \text{unitpotency of } \ominus \text{ with respect to } \otimes, \\
 & \quad \text{since we want to introduce } \ominus \} \\
 & (x \oplus y) \otimes (y \ominus y) \\
 = & \quad \{ \otimes \text{ associates with } \ominus \} \\
 & ((x \oplus y) \otimes y) \ominus y \\
 = & \quad \{ \text{deferred proof obligation of } [ (x \oplus y) \otimes y = x ]; \\
 & \quad \text{see below } \} \\
 & x \ominus y .
 \end{aligned}$$

The assumption in the last step can be easily proved as follows:

$$\begin{aligned}
 & (x \oplus y) \otimes y \\
 = & \quad \{ \otimes \text{ is symmetric } \} \\
 & y \otimes (x \oplus y) \\
 = & \quad \{ \otimes \text{ associates with } \oplus \} \\
 & (y \otimes x) \oplus y
 \end{aligned}$$

$$\begin{aligned}
&= \{ \otimes \text{ is symmetric} \} \\
&\quad (x \otimes y) \oplus y \\
&= \{ \otimes \text{ associates with } \oplus \} \\
&\quad x \otimes (y \oplus y) \\
&= \{ \oplus \text{ is unitpotent with respect to } \otimes \} \\
&\quad x .
\end{aligned}$$

Thus we write both  $\oplus$  and  $\ominus$  as  $\oplus$  and our program becomes:

$$\begin{aligned}
&\{ x = X \wedge y = Y \} \\
&x := x \otimes y ; \\
&y := x \oplus y ; \\
&x := x \oplus y \\
&\{ x = Y \wedge y = X \} .
\end{aligned}$$

## A simple refinement

An immediate corollary is that if we have a group with an operation  $\otimes$  that is symmetric, and if we define the operator  $\oplus$  as

$$x \oplus y = x \otimes y^{-1} ,$$

where  $y^{-1}$  is the inverse of  $y$ , then the above properties will hold. We can take, for instance, real addition for  $\otimes$  and real subtraction for  $\oplus$ . This would yield the following program:

$$\begin{aligned}
&\{ x = X \wedge y = Y \} \\
&x := x + y ; \\
&y := x - y ; \\
&x := x - y \\
&\{ x = Y \wedge y = X \} .
\end{aligned}$$

## Eliminating the symmetry requirement

As said before, this section presents an alternative choice for the calculation of  $y$  presented in page 2. This choice eliminates the symmetry requirement for  $\otimes$  and leads to a different calculation:

$$\begin{aligned}
& (\mathbf{x} \otimes \mathbf{y}) \ominus ((\mathbf{x} \otimes \mathbf{y}) \oplus \mathbf{y}) \\
= & \{ \ominus \text{ associates with } \oplus \} \\
& ((\mathbf{x} \otimes \mathbf{y}) \ominus (\mathbf{x} \otimes \mathbf{y})) \oplus \mathbf{y} \\
= & \{ \ominus \text{ is unitpotent with respect to } \oplus \} \\
& \mathbf{y} .
\end{aligned}$$

We then conclude that  $\otimes$  does not need to be symmetric and that the program with three operations is correct if

- $\otimes$  associates with  $\oplus$  ,
- $\ominus$  associates with  $\oplus$  ,
- $\oplus$  is unitpotent with respect to  $\otimes$  , and
- $\ominus$  is unitpotent with respect to  $\oplus$  .

## Acknowledgments

I'd like to thank to my colleagues in the Nottingham Tuesday Morning Club, to Jeremy Weissmann and to Apurva Mehta for their comments, suggestions and corrections on earlier versions of this note.

João Fernando Ferreira  
July 10, 2007

School of Computer Science and Information Technology  
University of Nottingham, Jubilee Campus  
Wollaton Road, Nottingham  
NG8 1BB  
United Kingdom

joao@joaoferreira.org