960605

Dear Martin,

Here are further thoughts about algebras for proofs,
raised by the book (yet another one...)

M. Darnel, Theory of Lattice-ordered Groups,
Dekker, New-York, 1995 [an expensive book :-( ]

On p.1, it says

"...we gather many results about the interplay of the order structure and the group structure...".

I feel this is central to us, computer scientists, in many ways:

- The group (or semigroup) structure serves to compose things, such as programs and proofs.
- The order (viz. lattice or semilattice) structure serves to support refinements, in programs as well as in proofs.

The use of semigroups or monoids instead of groups, of semilattices instead of lattices, and of categories instead of lattices,
is a rather secondary issue in this general context.
It is thus not surprising that various people came up with related algebras, for apparently different applications. But the differences now appear to me somewhat superficial.

Thus, the role of residuation is technical. In a l-group ("l-thing" means "lattice-ordered thing"), we solve the equation

$$a \circ x = b$$

by $x = a' \circ b$.

where $a'$ is the inverse of $a$.

In an l-semigroup, we solve the inequation

$$a \circ x \rceil b$$

by $x = a \setminus b$

where $a \setminus b$ is the residual. As well-known,

$a' \circ b$ in l-groups
becomes
$a \setminus b$ in l-semigroups.

We may write $(a \to b)$ for $(a \setminus b)$. We can read this as

Give me "a", and I will give you "b"

as in a game.

Amusingly enough, the semigroup property

$$a \circ (a \setminus b) \rceil b$$

which can be read as modus ponens, amounts to
the group property

$$a \circ (a' \circ b) = b,$$

which is not a surprise.

The inversion operation can be interpreted as follows:

- In programs, it is program inversion, as studied by e.g. Gries.
- In proofs, it could be seen as transforming a top-down proof into its bottom-up version.

Of course, inversion is available in relation algebras.
If inversion is not assumed, we may just use ordered semigroups.

By the way, it is remarkable to see that classical works, such as the above book by Darnel, do not consider fixpoint equations at all; Tarski is out of the picture. For us, this is central.
On the other hand, the order structure is detailed in various ways, e.g. in archimedean l-groups; this could be relevant for dynamical systems, ...in my other life. (*)

It is also interesting to notice the mutual ignorance of researchers in this area. In the book

Baccelli et al., Synchronization and Linearity, Wiley, 1995,

mentioned in a previous mail, the discussion
about algebras related to dioids ignores category-based structures (including quantales) as well as lattice-ordered groups.
Conversely, Darnel does not even mention semigroups, monoids or categories.

Another point: I recently met J.-R. Abrial, and talked with him about proof refinement. He finds the principle quite attractive [and asks for documents...:-) ]. He made the following interesting observation: proof refinement should go hand in hand with program refinement. In other words, we could prove an abstract program by an abstract proof, and could refine both in parallel.

I am away from the 7th to the 14th.

Regards,

Michel

(*) and also for games?