Calculational proof design; an experiment

In this note, all variables are -at least to begin with- of the same, as yet anonymous type. There are two predicates, tri and col on unordered triples, i.e. for all α, β, γ

$$\begin{aligned} &tri.\alpha.\beta.\gamma \equiv tri.\beta.\gamma.\alpha \\ &tri.\alpha.\beta.\gamma \equiv tri.\gamma.\beta.\alpha \\ &col.\alpha.\beta.\gamma \equiv col.\beta.\gamma.\alpha \\ &col.\alpha.\beta.\gamma \equiv col.\gamma.\beta.\alpha \end{aligned}$$

These predicates satisfy a few laws, which I shall introduce when I need them. (Whether these laws are axioms or theorems is currently irrelevant.)

We would like to design a proof of the

Theorem Let p,q,r,s satisfy

(0) $tri.p.q.r \wedge tri.q.r.s \wedge tri.r.s.p \wedge tri.s.p.q$;

let x,y,z satisfy in some order equations

(1) α: $col.p.q.\alpha \wedge col.r.s.\alpha$,
α: $col.p.r.\alpha \wedge col.q.s.\alpha$
α: $col.p.s.\alpha \wedge col.q.r.\alpha$;

then $tri.x.y.z$ holds .

(End of Theorem.)

Remark Since the demonstrandum x,y,z is symmetric in x,y,z, we can postpone the choice which of these three solves which of the equations (1). (End of Remark.)

So we need a law that allows us to conclude tri, and I give you one such law: for all $\alpha,\beta,\gamma,\delta$

(2) $\alpha\neq\beta \wedge \mathrm{col}.\alpha.\beta.\gamma \wedge \mathrm{tri}.\alpha.\gamma.\delta \Rightarrow \mathrm{tri}.\alpha.\beta.\delta$.

Remark Although col and tri are predicates on unordered triples, I found it — in order to come to grips with the "symbol dynamics" — essential to choose carefully how to formulate (2), and to stick to that formulation. Without that discipline, I got totally confused. Notice (i) that it is the left-most argument α that occurs in all 4 atoms, and (ii) that the occurrence of β,γ,δ in the last 3 atoms reflects a transitivity structure. (End of Remark.)

The first thing we are going to do is to design our appeals to (2), which allows us to conclude one tri from another. In order to carry out our analysis, we call p,q,r,s our "sources" and x,y,z our "targets" — in this context

meaningless identifiers_ .

We now note that
(i) our demonstrandum is a tri on 3 targets (type TTT)
(ii) we are only given -see (0)- tri-atoms on 3 sources (type SSS)
(iii) the two tri-atoms in (antecedent and consequent of) (2) have 2 arguments in common.
These observations imply that we need intermediate tri-atoms of types TSS and TTS, i.e. at least three appeals to (2).

An appeal to (2) with tri.α.β.δ of type TTT and tri.α.γ.δ of type TST would have in the antecedent col.α.β.γ of type TTS, whereas the only given col-atoms -see (1)- are of type SST. That is a problem, but since we are given no way of concluding a col-atom, the only thing we can do is to postulate it. To minimize our commitment, we introduce a new variable t, which could be neither source nor target. Instantiating (2) with

(3) $\qquad \alpha, \beta, \gamma, \delta := x, y, t, z$

we get

(4) $x \neq y \wedge col.x.y.t \wedge tri.x.t.z \Rightarrow tri.x.y.z$.

In instantiation (3), component $\gamma := t$ is essential; how x, y, z have been distributed over α, β, δ is irrelevant.

Our next appeal to (2) has to conclude $tri.x.t.z$, and in view of our goal of using (0), $tri.\alpha.\gamma.\delta$ should be of type TTS. This settles $\beta := t$ and, for our source choosing p say, $\gamma := p$. For the other two, we have to choose between $\alpha, \delta := x, z$ and $\alpha, \delta := z, x$. We choose the latter —and shall say in a moment why— and obtain with instantiation from (2)

(5) $$\alpha, \beta, \gamma, \delta := z, t, p, x$$

(6) $z \neq t \wedge col.z.t.p \wedge tri.z.p.x \Rightarrow tri.z.t.x$.

Remark At this stage, the choice between $\alpha, \delta := x, z$ and $\alpha, \delta := z, x$ is guided by the following consideration. With the choice made we must hope —see (2) and (4)— that auxiliary t can be chosen so as to satisfy

(7) $$col.x.y.t \wedge col.z.t.p \quad ,$$

a 5-variable relation, apart from the specif variables involved of the familiar shape of equations (1). Thanks to laws not men-

tioned yet, the rejected alternative has unacceptable consequences.

For the instantiation of γ with a source we were free to select p ; note that (0) and (1) are symmetric in p,q,r,s. (End of Remark)

Our third appeal to (2) should conclude $tri.z.p.x$ and now $tri.\alpha.\gamma.\delta$ should be of type TSS , i.e. γ has to be instantiated with a next source - say q : we are free - and β with a target, more precisely with either x or z . In view of (1), we want $col.\alpha.\beta.\gamma$ to be of type SST , and with β a target, we conclude that α should be instantiated with source p. We hope that the choice between $\beta,\delta := z,x$ and $\beta,\delta := x,z$ does not matter, and with instantiation

(8) $$\alpha,\beta,\gamma,\delta := p,x \quad q,z$$

we obtain from (2)

(9) $$p \neq z \wedge col.p.x.q \wedge tri.p.q.z \Rightarrow tri.p.x.z$$

The occurrence of $col.p.x.q$ makes us decide that x satisfy the first equation of (1), hence

(10) $$col.p.q.x \wedge col.r.s.x \quad .$$

Our final appeal to (2) should conclude tri.p.q.z from, say tri.p.q.r. For the instantiation that settles $\beta, \gamma := z, r$; we still have to choose between $\alpha, \delta := p, q$ and $\alpha, \delta := q, p$. We hope that the choice does not matter and take the latter: with the initiation

(11) $\quad \alpha, \beta, \gamma, \delta := q, z, r, p$

we obtain from (2)

(12) $q \neq z \wedge \text{col.}q.z.r \wedge \text{tri.}q.r.p \Rightarrow \text{tri.}q.z.p$,

and the occurrence of col.q.z.r makes us decide that z satisfies the third equation of (1); in summary (1) is replaced by - see (10) -

(13)
$$\begin{aligned} &\text{col.}p.q.x \wedge \text{col.}r.s.x \\ &\text{col.}p.r.y \wedge \text{col.}q.s.y \\ &\text{col.}p.s.z \wedge \text{col.}q.r.z \end{aligned} \quad .$$

Having dealt with the tri-atoms and the ensuing col-atoms we are left with the obligation to show

- $x \neq y$ (from (4))
- $z \neq t$ (from (6))
- $p \neq z$ (from (9))
- $q \neq z$ (from (12))

but, so far, we have no way of concluding

a difference. Fortunately, there is a law allowing us to do so:

(14) $\quad col.\alpha.\beta.\gamma \wedge tri.\beta.\gamma.\delta \Rightarrow \alpha \neq \delta$

We deal with the last two remaining obligations first:

- $q \neq z$
  $\Leftarrow$ {(14) with $\alpha,\beta,\gamma,\delta := z,s,p,q$}
  $col.z.s.p \wedge tri.s.p.q$
  $=$ {(13); (0)}
  true

- $p \neq z$
  $\Leftarrow$ {(14) with $\alpha,\beta,\gamma,\delta := z,q,r,p$}
  $col.z.q.r \wedge tri.q.r.p$
  $=$ {(13); (0)}
  true

The above are two instances of the general theorem that any source differs from any target.

Now we deal with the first of the remaining obligations

- $x \neq y$
  $\Leftarrow$ {(14) with $\alpha,\beta,\gamma,\delta := x,p,q,y$}
  $col.x.p.q \wedge tri.p.q.y$
  $=$ {(13)}
  $tri.p.y.q$

$\Leftarrow$ {(2) with $\alpha, \beta, \gamma, \delta := p, y, r, q$}
$p \neq y \wedge \mathrm{col}.p.y.r \wedge \mathrm{tri}.p.r.q$
$=$ {any source differs from any target; (13); (0)}
true

* * *

But with our last proof obligation, viz. $z \neq t$, we run into trouble. What we need is the existence of a t satisfying – see (7)

(15) $z \neq t \wedge \mathrm{col}.x.y.t \wedge \mathrm{col}.z.t.p$.

Suppose we had an existence proof of a t satisfying (7). To satisfy (15), we would then have to show that $t = z$ does not satisfy (7), i.e.

$$\neg(\mathrm{col}.x.y.z \wedge \mathrm{col}.z.z.p) \quad ;$$

the above, however, reduces to our original demonstrandum

$$\mathrm{tri}.x.y.z$$

thanks two further laws

(16) $\mathrm{col}.\alpha.\alpha.\beta$

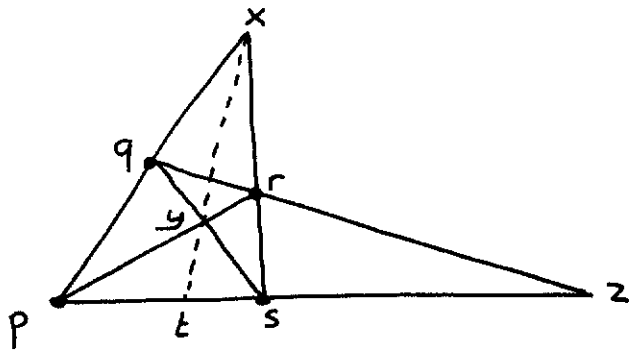
(17) $\mathrm{col}.\alpha.\beta.\gamma \equiv \mathrm{tri}.\alpha.\beta.\gamma$.

The type of axiom that is missing postulates

the existence of solutions that differ from parameters occurring in the equations. In what I saw (Pasch, Peano, Veblen, Hilbert), such existence axioms do occur.

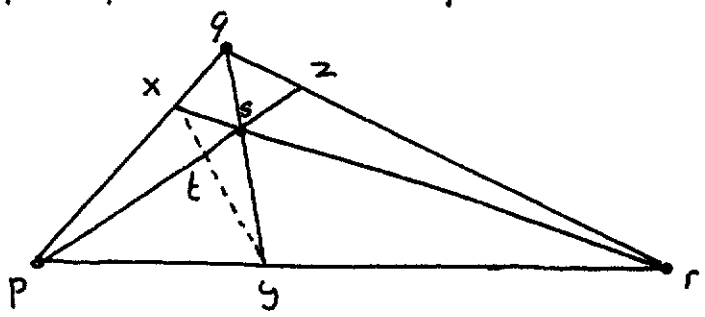
* * *

All this has been triggered by the study of (the beginnings of) axiomatizations of plane geometry - in Hilbert's "Foundations of Geometry" and Coxeter's "Introduction to Geometry" - . The proofs I encountered were verbal and pictorial and often I could not convince myself that the arguments were complete. I can now give you a picture illustrating the above argument



with "col" meaning "collinear" and "tri" standing for "triangular". But you must take my word for it that this picture was only drawn after the above proofs were designed: the whole point of the experiment was to try out the feasibility of proof design without leaning on the pictorial crutch.

The trouble with pictures, of course, is that the don't state the extent to which they are overspecific. Look, for instance, at



This is "the same picture" as the previous one!

Remark The trouble could really be serious. In the existence axiomatizations I saw, the notion "between" plays a central role. In the one picture t lies between x and y, in the other it does not. (End of Remark)

I was also interested in the calculational consequences of the fact that, while having variables of only one type – "points", say –, I had no expressions of that type. After the fact, I think that the consequences are minor.

Before I started on this, I did not know which predicates to use; the decision to introduce both col and tri helped a lot.

Though (17) clearly states that one of the two predicates is superfluous, we leave open which one. It was also a surprise to see that (17) played no role beyond making law (14) a derivable theorem:

$$
\begin{array}{ll}
 & \mathrm{col}.\alpha.\beta.\gamma \wedge \mathrm{tri}.\beta.\gamma.\delta \\
\Rightarrow & \quad \{\ \text{pred. calc.}\ \} \\
 & \mathrm{col}.\alpha.\beta.\gamma \equiv \mathrm{tri}.\beta.\gamma.\delta \\
= & \quad \{\ (17)\ \} \\
 & \mathrm{col}.\alpha.\beta.\gamma \not\equiv \mathrm{col}.\delta.\beta.\gamma \\
\Rightarrow & \quad \{\ \text{Zinbiel}\ \} \\
 & \alpha \neq \delta \quad .
\end{array}
$$

I have been wondering whether, instead of what we have done, these predicates should rather be defined on unordered triples or, even more general, on sets. Thanks to this exercise I know that those alternatives deserve to be rejected: in law (2) – a linchpin of the whole argument – the consequent is symmetric in α, β, δ, but the antecedent is not. Finding the proper instantiation of (2) was, in fact, in each appeal to it the major and not trivial decision.

Nuenen, 21 December 1995

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188, USA