The quartet spaces of G. ’t Hooft

Wim H. Hesselink, whh525
Johann Bernoulli Institute for Mathematics and Computer Science
University of Groningen, the Netherlands

October 20, 2017

Abstract

In 1964, G. ’t Hooft postulated three axioms, and proved that every nonempty finite model of them has $4^n$ elements. This note confirms this by showing that every nonempty model can be made into a vector space over the field with four elements. For every pair of different elements $x$ and $y$, the quartet of $x$ and $y$ is the affine line through $x$ and $y$ in this vector space.

1 Introduction

In 1964, when I was an undergraduate in physics at Utrecht University in the Netherlands, the now famous physicist Gerard ’t Hooft was one of us. When our professor Freudenthal taught us the axioms of linear spaces, ’t Hooft postulated an axiom system out of the blue. He called the models of his axiom system quartet spaces because they are compositions of quartets, models with four elements. Indeed, he proved that every nonempty finite model has $4^n$ elements for some natural number $n$, and that such models exist for all $n$.

He never published this. Around 1966, I wrote about his quartet spaces in our undergraduate newsletter WisFysVaria. In the present note I present his axiom system and show that every nonempty model of it is in some sense a vector space over the field with four elements.

2 Axioms for quartet spaces

Let a $*$-space be a set $Q$ with a binary operation $*$ between its elements. ’t Hooft defined a quartet space $Q$ to be a $*$-space $Q$ that satisfies the axioms

(A0) $x * y = z$ implies $y * z = x$ ,
(A1) $x * (y * z) = z * (y * x)$ ,
(A2) $x * x = x$ ,

for all $x, y, z \in Q$.

Recall that a $*$-space $Q$ is called commutative and associative if it satisfies the respective axioms

(com) $x * y = y * x$ ,
(ass) $x * (y * z) = (x * y) * z$ .

In general, a quartet space is neither commutative nor associative. Therefore, we have to be careful with the order and the association of the operands.

If Axiom (A0) is applied twice, it yields

(0) $x * y = z$ implies $z * x = y$ .
Elimination of \( z \) from the implications (A0) and (0) gives the equalities

\[
y \ast (x \ast y) = x \quad \text{and} \quad (x \ast y) \ast x = y.
\]

Axiom (A1) has a mirror version

\[
(x \ast y) \ast z = (z \ast y) \ast x.
\]

This formula follows from the axioms (A0) and (A1) because

\[
(x \ast y) \ast z = \begin{cases} 
\text{take } b = z \ast y, \text{ so that } z = y \ast b \text{ by (A0)} \\
(x \ast y) \ast (y \ast b) \\
\text{(A1) with } x := x \ast y \text{ and } z := b \\
b \ast (y \ast (x \ast y)) \\
\{ \text{value of } b, \text{ and (1) with } x \text{ and } y \text{ interchanged} \} \\
(z \ast y) \ast x.
\end{cases}
\]

A less obvious consequence is:

\[
(w \ast x) \ast (y \ast z) = (w \ast y) \ast (x \ast z).
\]

Formula (3) follows from Axiom (A1) because

\[
(w \ast x) \ast (y \ast z) = \begin{cases} 
\text{(A1) with } x := w \ast x \\
z \ast (y \ast (w \ast x)) \\
\text{(A1) with } x := y, y := w, z := x \\
z \ast (x \ast (w \ast y)) \\
\text{(A1) with } x := z, y := x, z := w \ast y \\
(w \ast y) \ast (x \ast z).
\end{cases}
\]

I cannot reconstruct the proofs of 50 years ago, but I recall that the key was the triple operator \([ , , ]\) given by

\[
[x, y, z] = (x \ast y) \ast (z \ast x).
\]

Formula (3) directly implies \([x, y, z] = [x, z, y]\). A more difficult property is \([x, y, z] = [y, z, x]\). Although it is not used below, this property is proved in

\[
(x \ast y) \ast (z \ast x) = (y \ast z) \ast (x \ast y) \\
\equiv \begin{cases} 
\text{(A2), twice} \\
(x \ast (y \ast y)) \ast (z \ast x) = (y \ast z) \ast ((x \ast x) \ast y) \\
\text{(A1) and Formula (2)} \\
(y \ast (x \ast x)) \ast (z \ast x) = (y \ast z) \ast ((y \ast x) \ast x) \\
\text{Formula (3) with } w := y, x := y \ast x, y := z, z := x \end{cases} \text{ true}.
\]

It follows that \([x, y, z]\) is invariant under all permutations of its three arguments.

## 3 Reduction to linear algebra

't Hooft developed an independent theory of quartet spaces, but it seems to be more illuminating to relate the quartet spaces to more familiar algebraic theories.

To show that the axioms of the previous section are satisfiable and independent, let \( R \) be an associative ring with \( 1 \neq 0 \), and with two fixed elements \( a, b \in R \).

Define the operation \( \ast \) on \( R \) by \( x \ast y = ax + by \) for all \( x, y \in R \). It is easy to verify that the operation \( \ast \) on \( R \) satisfies Formula (3) if and only if \( ab = ba \). It...
satisfies Axiom (A0) if and only if \( a + b^2 = 0 \) and \( ba = 1 \). This implies that \( ab = ba \).

Operation \(*\) on \( R \) satisfies Axiom (A1) if and only if \( a = b^2 \). It satisfies Formula (2) if and only if \( b = a^2 \). This implies that Formula (2) does not follow from Axiom (A1) alone. Operation \(*\) on \( R \) satisfies Axiom (A2) if and only if \( a + b = 1 \).

It follows that the \(*\)-space \( (R, *) \) is a quartet space if and only if \( 1 + 1 = 0 \) and \( a = b^2 \) and \( a + b = 1 \). In fact, these three equations together imply that \( b^3 = 1 \). They also imply that the ring generated by 1, \( a \), and \( b \) is the Galois field \( \mathbb{F}_4 \), the field with the four (different) elements: 0, 1, \( a \), \( b \).

More generally, let \( V \) be a vector space over this field \( \mathbb{F}_4 \). The space \( V \) can be made into a quartet space by defining \( x * y = ax + by \) for all \( x, y \in V \). If \( x \) and \( y \) are different, there is a unique line in \( V \) through the points \( x \) and \( y \), and this line is the set \( \{ x, y, x * y, y * x \} \). Such a set was called a quartet by 't Hooft.

Our main result expresses that, conversely, every nonempty quartet space is obtained in this way.

**Theorem 1** Let \( Q \) be a nonempty quartet space. Then \( Q \) has a structure of a vector space over \( \mathbb{F}_4 \) such that \( x * y = ax + by \) for all \( x, y \in Q \).

**Proof.** The proof relies on a mathematical form of symmetry breaking: as the set \( Q \) is nonempty, we can choose an arbitrary element \( e \in Q \) as a base point. We define addition in \( Q \) by \( x + y = (e * x) * (y * e) \). Formula (3) implies that \(+\) is commutative. For elements \( x \) and \( y \), we have

\[
e * (x + y) = (y * e) * x
\]

because

\[
e * (x + y) \\
= \{ \text{definition} \} e * ((e * x) * (y * e)) \\
= \{ \text{(A1)} \} (y * e) * ((e * x) * e) \\
= \{ (0) \} (y * e) * x.
\]

It follows that

\[
(x + y) + z = (z + y) + x
\]

\[
\equiv \{ \text{definition +, twice} \}
(e * (x + y)) * (z * e) = (e * (z + y)) * (x * e)
\]

\[
\equiv \{ \text{(4), twice} \}
((y * e) * x) * (z * e) = ((y * e) * z) * (x * e)
\]

\[
\equiv \{ \text{(3)} \} \text{true}.
\]

As addition is commutative, this implies that it is also associative.

Special rules are \( e + x = x \) and \( x + x = e \) for every \( x \in Q \), as proved in

\[
e + x
\]

\[
= \{ \text{definition of +} \} (e * e) * (x * e)
\]

\[
= \{ \text{(A2) for } x := e \} e * (x * e)
\]

\[
= \{ \text{(A0)} \} x.
\]

\[
x + x
\]

\[
= \{ \text{definition of +} \} (e * x) * (x * e)
\]

\[
= \{ \text{(A1)} \} e * (x * (e * x))
\]

\[
= \{ \text{(A0)} \} e * e
\]

\[
= \{ \text{(A2) for } x := e \} e.
\]

3
This implies that \((Q, +)\) is an additive group with neutral element \(e\). Moreover, every element is its own inverse. Therefore, \((Q, +)\) is a vector space over the field \(\mathbb{F}_2\) with two elements.

The group \((Q, +)\) has additional structure, viz. functions \(\beta, \alpha : Q \to Q\) given by \(\beta(x) = e * x\) and \(\alpha(x) = x * e\). These functions are additive. This is proved for \(\beta\) in

\[
\beta(x + y) = \beta(x) + \beta(y)
\]

\[
\equiv \{ \text{def. } \beta, + \} e * ((e * x) * (y * e)) = (e * (e * x)) * ((e * y) * e)
\]

\[
\equiv \{ (A1), \text{twice} \} (y * e) * ((e * x) * e) = (x * (e * e)) * ((e * y) * e)
\]

\[
\equiv \{ (0), \text{twice, (A2)} \text{ for } x := e \} (y * e) * x = (x * e) * y
\]

\[
\equiv \{ (2) \} \text{ true}.
\]

The proof for \(\alpha\) is similar. The operation \(*\) can be expressed in terms of \(+\), \(\alpha\), \(\beta\), because, by \((A0)\) and \((0)\), it holds that

\[
\alpha(x) + \beta(y) = (e * (x * e)) * ((e * y) * e) = x * y.
\]

Axiom \((A0)\) and formula \((0)\) imply that \(\alpha\) and \(\beta\) are each others inverse. In particular, they commute. Using the Axiom \((A1)\), we find that \(\alpha = \beta \circ \beta\), and hence \(\beta^3 = 1\), the identity function. Finally, Axiom \((A2)\) implies that \(\alpha + \beta = 1\). Therefore, \(Q\) becomes a vector space over \(\mathbb{F}_4\) by defining \(ax = \alpha(x)\) and \(bx = \beta(x)\) for all \(x \in Q\).

This result shows that the three axioms of ’t Hooft characterise the vector spaces over the field with four elements up to the choice of an origin. In particular, every finite model has \(4^n\) elements for some natural number \(n\). It is surprising that three simple axioms induce so much structure.

4 Axiom \((A2)\) is almost superfluous

If we remove the third axiom, we can do almost as much. Let a \(*\)-space \(Q\) be called a pre-quartet space if it satisfies the axioms \((A0)\) and \((A1)\).

Let \(Q\) be an arbitrary nonempty pre-quartet space. As their proofs do not use Axiom \((A2)\), the Formulas \((0), (1), (2), (3)\) are valid in \(Q\). Every square \(x^2 = x * x\) in \(Q\) is idempotent, i.e., \(x^2 * x^2 = x^2\), because

\[
(x * x) * (x * x)
\]

\[
= \{ (A1) \} x * (x * (x * x))
\]

\[
= \{ (1) \} x * x.
\]

As \(Q\) has some idempotent elements, we can choose an idempotent element \(e \in Q\) as a base point. Now the remainder of the proof of Theorem 1 is applicable, because Axiom \((A2)\) is used only in proving that \(e^3 = e\), except in the last sentences in the proof of \(\alpha + \beta = 1\). Therefore, instead of the field \(\mathbb{F}_4\), we end up with the commutative ring \(B = \mathbb{F}_2[\beta]\) with the relation \(\beta^3 = 1\). The result is therefore that \(Q\) can be regarded as a module over the ring \(B\). The ring \(B\) is isomorphic to the Cartesian product \(\mathbb{F}_4 \times \mathbb{F}_2\). It follows that \(Q\) is isomorphic to a Cartesian product of a vector space over \(\mathbb{F}_4\), and a vector space over \(\mathbb{F}_2\); the first with the quartet operation \(x * y = ax + by\), the second with the operation \(x * y = x + y\). Axiom \((A2)\) thus serves to remove the uninteresting part of the pre-quartet space.