The Cayley-Dickson Construction in ACL2

John Cowles Ruben Gamboa
University of Wyoming
Laramie, WY
{cowles,ruben}@uwyo.edu

The **Cayley-Dickson Construction** is a generalization of the familiar construction of the complex numbers from pairs of real numbers. The complex numbers can be viewed as two-dimensional vectors equipped with a multiplication.

The construction can be used to construct, not only the two-dimensional Complex Numbers, but also the four-dimensional Quaternions and the eight-dimensional Octonions. Each of these vector spaces has a vector multiplication, $\mathbf{v}_1 \bullet \mathbf{v}_2$, that satisfies:

1. Each nonzero vector, $\mathbf{v}$, has a multiplicative inverse $\mathbf{v}^{-1}$.
2. For the Euclidean length of a vector $|\mathbf{v}|$, $|\mathbf{v}_1 \bullet \mathbf{v}_2| = |\mathbf{v}_1| \cdot |\mathbf{v}_2|$

Real numbers can also be viewed as (one-dimensional) vectors with the above two properties.

ACL2(r) is used to explore this question: Given a vector space, equipped with a multiplication, satisfying the Euclidean length condition 2, given above. Make pairs of vectors into "new" vectors with a multiplication. When do the newly constructed vectors also satisfy condition 2?

1 Cayley-Dickson Construction

Given a vector space, with vector addition, $\mathbf{v}_1 + \mathbf{v}_2$; vector minus $-\mathbf{v}$; a zero vector $\vec{0}$; scalar multiplication by real number a, $a \circ \mathbf{v}$; a unit vector $\vec{1}$; and vector multiplication $\mathbf{v}_1 \bullet \mathbf{v}_2$; satisfying the Euclidean length condition $|\mathbf{v}_1 \bullet \mathbf{v}_2| = |\mathbf{v}_1| \cdot |\mathbf{v}_2|$ (2).

Define the **norm** of vector $\mathbf{v}$ by $\|\mathbf{v}\| = |\mathbf{v}|^2$. Since $|\mathbf{v}_1 \bullet \mathbf{v}_2| = |\mathbf{v}_1| \cdot |\mathbf{v}_2|$ is equivalent to $|\mathbf{v}_1 \bullet \mathbf{v}_2|^2 = |\mathbf{v}_1|^2 \cdot |\mathbf{v}_2|^2$, the Euclidean length condition is equivalent to

$$\|\mathbf{v}_1 \bullet \mathbf{v}_2\| = \|\mathbf{v}_1\| \cdot \|\mathbf{v}_2\|.$$

Recall the **dot (or inner) product**, of n-dimensional vectors, is defined by

$$\begin{aligned}(x_1, \ldots, x_n) \odot (y_1, \ldots, y_n) &= x_1 \cdot y_1 + \cdots + x_n \cdot y_n \\ &= \sum_{i=1}^{n} x_i \cdot y_i\end{aligned}$$

Then Euclidean length and norm of vector $\mathbf{v}$ are given by

$$\begin{aligned}|\mathbf{v}| &= \sqrt{\mathbf{v} \odot \mathbf{v}} \\ \|\mathbf{v}\| &= \mathbf{v} \odot \mathbf{v}.\end{aligned}$$

Except for vector multiplication, it is easy to treat ordered pairs of vectors, $(\mathbf{v}_1; \mathbf{v}_2)$, as vectors:

1. $(\mathbf{v}_1; \mathbf{v}_2) + (\mathbf{w}_1; \mathbf{w}_2) = (\mathbf{v}_1 + \mathbf{w}_1; \mathbf{v}_2 + \mathbf{w}_2)$
2. $-(\mathbf{v}_1; \mathbf{v}_2) = (-\mathbf{v}_1; -\mathbf{v}_2)$

Warren Hunt Jr. and Anna Slobodova (Eds.):
ACL2 Theorem Prover and its Applications
EPTCS 249, 2017, pp. 18–29, doi:10.4204/EPTCS.249.2

3. zero vector: $(\vec{0};\vec{0})$
4. $a \circ (\mathbf{v}_1;\mathbf{v}_2) = (a \circ \mathbf{v}_1;\, a \circ \mathbf{v}_2)$
5. unit vector: $(\vec{1};\vec{0})$
6. $(\mathbf{v}_1;\mathbf{v}_2) \odot (\mathbf{w}_1;\mathbf{w}_2) = \{\mathbf{v}_1 \odot \mathbf{w}_1\} + \{\mathbf{v}_2 \odot \mathbf{w}_2\}$
7. $\|(\mathbf{v}_1;\mathbf{v}_2)\| = \|\mathbf{v}_1\| + \|\mathbf{v}_2\|$

Given that

$$\|\mathbf{v} \bullet \mathbf{w}\| = \|\mathbf{v}\| \cdot \|\mathbf{w}\|,$$

the problem is to define **multiplication of vector pairs** so that

$$\|(\mathbf{v}_1;\mathbf{v}_2) \bullet (\mathbf{w}_1;\mathbf{w}_2)\| = \|(\mathbf{v}_1;\mathbf{v}_2)\| \cdot \|(\mathbf{w}_1;\mathbf{w}_2)\|.$$

1.1 Examples

Complex multiplication. Think of the real numbers as one-dimensional vectors. Interpret ordered pairs of real numbers as complex numbers: For real a and b, $(a;b) = (\texttt{complex}\ a\ \ b) = a + b \cdot i$. For reals a_1, a_2 and b_1, b_2, complex multiplication is defined by

$$(a_1;a_2) \cdot (b_1;b_2) = ([a_1b_1 - a_2b_2]\,;\,[a_1b_2 + a_2b_1]) \tag{1}$$

and satisfies

$$\|(a_1;a_2) \cdot (b_1;b_2)\| = \|(a_1;a_2)\| \cdot \|(b_1;b_2)\|.$$

Quaternion multiplication. Think of the complex numbers as two-dimensional vectors. Interpret ordered pairs of complex numbers as William Hamilton's quaternions [1, 3, 2]: For complex $c = a_1 + a_2 \cdot i$ and $d = b_1 + b_2 \cdot i$,

$$\begin{aligned} (c;d) &= c + d \cdot j \\ &= a_1 + a_2 \cdot i + b_1 \cdot j + b_2 \cdot ij \\ &= a_1 + a_2 \cdot i + b_1 \cdot j + b_2 \cdot k. \end{aligned}$$

where $i \cdot j = k$.

For complex $c = a_1 + a_2 \cdot i$, $\bar{c} = a_1 - a_2 \cdot i$ is the **conjugate** of c.

For complex numbers $c_1 = a_1 + a_2 \cdot i$, $c_2 = a_3 + a_4 \cdot i$, $d_1 = b_1 + b_2 \cdot i$, and $d_2 = b_3 + b_4 \cdot i$, quaternion multiplication is defined by

$$\begin{aligned} (c_1;c_2) \cdot (d_1;d_2) &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) \\ &\quad + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j \\ &\quad + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k \\ &= (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i \\ &\quad - [(a_3b_3 + a_4b_4) + (-a_3b_4 + a_4b_3)i] \\ &\quad + [(a_1b_3 - a_2b_4) + (a_1b_4 + a_2b_3)i]j \\ &\quad + [(a_3b_1 + a_4b_2) + (-a_3b_2 + a_4b_1)i]j \\ &= (c_1d_1 - c_2\bar{d}_2) + (c_1d_2 + c_2\bar{d}_1)j \\ &= ([c_1d_1 - c_2\bar{d}_2];[c_1d_2 + c_2\bar{d}_1]) \end{aligned} \tag{2}$$

and satisfies

$$\|(c_1;c_2)\cdot(d_1;d_2)\| = \|(c_1;c_2)\|\cdot\|(d_1;d_2)\|.$$

Quaternion multiplication is completely determined by this table for the multiplication of i, j, and k:

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Quaternion multiplication is not commutative, since $i\cdot j = k$ and $j\cdot i = -k$. Quaternion multiplication is associative: $(q_1\cdot q_2)\cdot q_3 = q_1\cdot(q_2\cdot q_3)$.

Octonion multiplication. Think of the quaternions as four-dimensional vectors. Interpret ordered pairs of quaternions as John Graves's and Arthur Cayley's octonions [1, 3, 2]: For quaternions $q = a_1 + a_2\cdot i + a_3\cdot j + a_4\cdot k$ and $r = b_1 + b_2\cdot i + b_3\cdot j + b_4\cdot k$,

$$\begin{aligned}(q;r) &= q + r\cdot\ell \\ &= a_1 + a_2\cdot i + a_3\cdot j + a_4\cdot k \\ &\quad + b_1\cdot\ell + b_2\cdot i\ell + b_3\cdot j\ell + b_4\cdot k\ell \\ &= a_1 + a_2\cdot i + a_3\cdot j + a_4\cdot k \\ &\quad + b_1\cdot\ell + b_2\cdot I + b_3\cdot J + b_4\cdot K.\end{aligned}$$

where $i\cdot\ell = I$, $j\cdot\ell = J$, and $k\cdot\ell = K$

For quaternion $q = a_1 + a_2\cdot i + a_3\cdot j + a_4\cdot k$, $\bar{q} = a_1 - a_2\cdot i - a_3\cdot j - a_4\cdot k$ is the **conjugate** of q.

For quaternions q_1, q_2, r_1, and r_2, octonion multiplication is defined by

$$\begin{aligned}(q_1;q_2)\cdot(r_1;r_2) &= (q_1 + q_2\cdot\ell)\cdot(r_1 + r_2\cdot\ell) \\ &= (q_1r_1 - \bar{r}_2q_2) + (r_2q_1 + q_2\bar{r}_1)\cdot\ell \\ &= ([q_1r_1 - \bar{r}_2q_2];[r_2q_1 + q_2\bar{r}_1]) \qquad (3)\end{aligned}$$

and satisfies

$$\|(q_1;q_2)\cdot(r_1;r_2)\| = \|(q_1;q_2)\|\cdot\|(r_1;r_2)\|.$$

Octonion multiplication is completely determined by this table for the multiplication of i, j, k, ℓ, I, J, and K:

	i	j	k	ℓ	I	J	K
i	-1	k	$-j$	I	$-\ell$	$-K$	J
j	$-k$	-1	i	J	K	$-\ell$	$-I$
k	j	$-i$	-1	K	$-J$	I	$-\ell$
ℓ	$-I$	$-J$	$-K$	-1	i	j	k
I	ℓ	$-K$	J	$-i$	-1	$-k$	j
J	K	ℓ	$-I$	$-j$	k	-1	$-i$
K	$-J$	I	ℓ	$-k$	$-j$	i	-1

Since the octonions contain the quaternions, octonion multiplication is also not commutative. Octonian multiplication is not associative, since $\ell\cdot(I\cdot J) = K$ and $(\ell\cdot I)\cdot J = -K$.

Complex (1), quaternion (2), and octonion (3) multiplication suggest these possible definitions for vector multiplication:

$$(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2) = ([\mathbf{v}_1\mathbf{w}_1-\mathbf{v}_2\mathbf{w}_2];[\mathbf{v}_1\mathbf{w}_2+\mathbf{v}_2\mathbf{w}_1]) \quad (4)$$

$$(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2) = ([\mathbf{v}_1\mathbf{w}_1-\mathbf{v}_2\bar{\mathbf{w}}_2];[\mathbf{v}_1\mathbf{w}_2+\mathbf{v}_2\bar{\mathbf{w}}_1]) \quad (5)$$

$$(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2) = ([\mathbf{v}_1\mathbf{w}_1-\bar{\mathbf{w}}_2\mathbf{v}_2];[\mathbf{w}_2\mathbf{v}_1+\mathbf{v}_2\bar{\mathbf{w}}_1]) \quad (6)$$

When the $\mathbf{v}_i$ and $\mathbf{w}_i$ are real numbers, all three definitions are equivalent, since real multiplication is commutative and the conjugate of real a, $\bar{a}$, is just a.

When the $\mathbf{v}_i$ and $\mathbf{w}_i$ are complex numbers, the last two definitions are equivalent, since complex multiplication is commutative. However, when $\mathbf{v}_1 = 1+0\cdot i = \mathbf{w}_1$, $\mathbf{v}_2 = 0+1\cdot i$, and $\mathbf{w}_2 = 0+(-1\cdot i)$, the product given by equation (4) is the zero vector $([0+0\cdot i];[0+0\cdot i])$. So a vector product defined by (4) need not satisfy

$$\|(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2)\| = \|(\mathbf{v}_1;\mathbf{v}_2)\|\cdot\|(\mathbf{w}_1;\mathbf{w}_2)\|,$$

for complex inputs.

Since the quaternions contain the complex numbers, a vector product defined by (4) also will not be satisfactory for quaternion inputs. When $\mathbf{v}_1 = 0+(-1\cdot i)+0\cdot j+0\cdot k$, $\mathbf{v}_2 = 0+0\cdot i+1\cdot j+0\cdot k = \mathbf{w}_2$, and $\mathbf{w}_1 = 0+1\cdot i+0\cdot j+0\cdot k$, the product given by equation (5) is the zero vector $([0+0\cdot i+0\cdot j+0\cdot k];[0+0\cdot i+0\cdot j+0\cdot k])$. So a vector product defined by either (4) or (5) need not satisfy

$$\|(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2)\| = \|(\mathbf{v}_1;\mathbf{v}_2)\|\cdot\|(\mathbf{w}_1;\mathbf{w}_2)\|,$$

for quaternion inputs.

This leaves (6) as a possible way to define vector multiplication of ordered pairs of vectors. So a vector **conjugate**, $\bar{\mathbf{v}}$, is also required. Continuing the enumeration of vector pair operations given on page 2:

8. $\overline{(\mathbf{v}_1;\mathbf{v}_2)} = (\bar{\mathbf{v}}_1;-\mathbf{v}_2)$
9. $(\mathbf{v}_1;\mathbf{v}_2)\bullet(\mathbf{w}_1;\mathbf{w}_2) = ([\mathbf{v}_1\mathbf{w}_1-\bar{\mathbf{w}}_2\mathbf{v}_2];[\mathbf{w}_2\mathbf{v}_1+\mathbf{v}_2\bar{\mathbf{w}}_1])$

The enumerated list of items, $1,2,\cdots,9$, defining various operations on ordered pairs of vectors, is called the **Cayley-Dickson Construction** [4, 2].

1.2 Summary

- Start with the real numbers.
  Apply the Cayley-Dickson Construction to pairs of real numbers.
  Obtain a vector algebra isomorphic to the complex numbers.
- Apply the Cayley-Dickson Construction to pairs of complex numbers.
  Obtain a vector algebra isomorphic to the quaternions.
- Apply the Cayley-Dickson Construction to pairs of quaternions.
  Obtain a vector algebra isomorphic to the octonians.

Each of these vector spaces: real numbers, complex numbers, quaternions, and octonians, satisfy

$$\|\mathbf{v}_1\bullet\mathbf{v}_2\| = \|\mathbf{v}_1\|\cdot\|\mathbf{v}_2\|.$$

Futhermore, every vector $\mathbf{v}\neq\vec{0}$ has a multiplicative inverse:

$$\mathbf{v}^{-1} = \frac{1}{\|\mathbf{v}\|}\circ\bar{\mathbf{v}}$$

2 Composition Algebras

A **composition algebra** [1, 3] is a real vector space, with vector multiplication, a real-valued norm, and a real-valued dot product, satisfying this composition law

$$\|\mathbf{v}_1 \bullet \mathbf{v}_2\| = \|\mathbf{v}_1\| \cdot \|\mathbf{v}_2\|.$$

Use `encapsulate` to axiomatize, in ACL2(r), composition algebras.
ACL2(r) function symbols are needed for

- Vector Predicate. $\mathbf{Vp}(x)$ for "x is a vector."
- Zero Vector. $\vec{0}$
- Vector Addition. $\mathbf{v}_1 + \mathbf{v}_2$
- Vector Minus. $-\mathbf{v}$
- Scalar Multiplication. For real number a, $a \circ \mathbf{v}$
- Vector Multipication. $\mathbf{v}_1 \bullet \mathbf{v}_2$
- Unit Vector. $\vec{1}$
- Vector Norm. $\|\mathbf{v}\|$
- Vector Dot Product. $\mathbf{v}_1 \odot \mathbf{v}_2$
- Predicate with Quantifier. $\forall u[\mathbf{Vp}(u) \rightarrow u \odot x = 0]$
- Skolem Function. Witness function for Predicate with Quantifier

In addition to the usual closure axioms, the `encapsulate` adds these axioms to ACL2(r):

- Real Vector Space Axioms.

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow (x+y)+z = x+(y+z)$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow x+y = y+x$$

$$\mathbf{Vp}(x) \rightarrow \vec{0}+x = x$$

$$\mathbf{Vp}(x) \rightarrow x+(-x) = \vec{0}$$

$$[\texttt{Realp}(a) \wedge \texttt{Realp}(b) \wedge \mathbf{Vp}(x)] \rightarrow a \circ (b \circ x) = (a \cdot b) \circ x$$

$$\mathbf{Vp}(x) \rightarrow 1 \circ x = x$$

$$[\texttt{Realp}(a) \wedge \texttt{Realp}(b) \wedge \mathbf{Vp}(x)] \rightarrow (a+b) \circ x = (a \circ x) + (b \circ x)$$

$$[\texttt{Realp}(a) \wedge \mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow a \circ (x+y) = (a \circ x) + (a \circ y)$$

- Real Vector Algebra Axioms.

$$\vec{1} \neq \vec{0}$$

$$[\mathtt{Realp}(a) \wedge \mathtt{Realp}(b) \wedge \mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow$$
$$x \bullet [(a \circ y) + (b \circ z)] = [a \circ (x \bullet y)] + [b \circ (x \bullet z)]$$

$$[\mathtt{Realp}(a) \wedge \mathtt{Realp}(b) \wedge \mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow$$
$$[(a \circ x) + (b \circ y)] \bullet z = [a \circ (x \bullet z)] + [b \circ (y \bullet z)]$$

$$\mathbf{Vp}(x) \rightarrow [(\vec{1} \bullet x = x) \wedge (x \bullet \vec{1} = x)]$$

- Vector Norm and Dot Product Axioms.

$$\mathbf{Vp}(x) \rightarrow [\mathtt{Realp}(\|x\|) \wedge \|x\| \geq 0]$$

$$\mathbf{Vp}(x) \rightarrow [(\|x\| = 0) = (x = \vec{0})]$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow \|x \bullet y\| = \|x\| \cdot \|y\|$$

$$x \odot y = \frac{1}{2} \cdot [\|x + y\| - \|x\| - \|y\|]$$

$$[\mathtt{Realp}(a) \wedge \mathtt{Realp}(b) \wedge \mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow$$
$$[(a \circ x) + (b \circ y)] \odot z = [a \cdot (x \odot z)] + [b \cdot (y \odot z)]$$

$$\forall u [\mathbf{Vp}(u) \rightarrow u \odot x = 0] =$$
$$[\mathtt{let}\ u\ \text{be}\ \mathtt{witness}(x)][\mathbf{Vp}(u) \rightarrow u \odot x = 0]$$

$$\forall u [\mathbf{Vp}(u) \rightarrow u \odot x = 0] \rightarrow [\mathbf{Vp}(u) \rightarrow u \odot x = 0]$$

$$(\mathbf{Vp}(x) \wedge \forall u [\mathbf{Vp}(u) \rightarrow u \odot x = 0]) \rightarrow x = \vec{0}$$

The ACL2(r) theory of composition algebras includes the following theorems and definitions:

- Scaling Laws.

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow (x \bullet y) \odot (x \bullet z) = \|x\| \cdot (y \odot z)$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow (x \bullet z) \odot (y \bullet z) = (x \odot y) \cdot \|z\|$$

- Exchange Law.

$$[\mathbf{Vp}(u) \wedge \mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow [(u \bullet y) \odot (x \bullet z)] + [(u \bullet z) \odot (x \bullet y)] = 2 \cdot (u \odot x) \cdot (y \odot z)$$

- Conjugate Definition.

$$\bar{x} = ([2 \cdot (x \odot \vec{1})] \circ \vec{1}) + (-x)$$

- Conjugate Laws.

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow y \odot (\bar{x} \bullet z) = z \odot (x \bullet y)$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \mathbf{Vp}(z)] \rightarrow x \odot (z \bullet \bar{y}) = z \odot (x \bullet y)$$

$$\mathbf{Vp}(x) \rightarrow \bar{\bar{x}} = x$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow \overline{x \bullet y} = \bar{y} \bullet \bar{x}$$

- Inverse Definition.

$$x^{-1} = \frac{1}{\|x\|} \circ \bar{x}$$

- Inverse Law.

$$[\mathbf{Vp}(x) \wedge x \neq \vec{0}] \rightarrow [x^{-1} \bullet x = \vec{1} \wedge x \bullet x^{-1} = \vec{1}\,]$$

- Alternative Laws. Special versions of associativity.

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow x \bullet (x \bullet y) = (x \bullet x) \bullet y$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow (y \bullet x) \bullet x = y \bullet (x \bullet x)$$

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow (x \bullet y) \bullet x = x \bullet (y \bullet x)$$

- Other Theorems.

$$[\mathbf{Vp}(x) \wedge \mathbf{Vp}(y)] \rightarrow ([x \bullet y = \vec{0}] = [(x = \vec{0}) \vee (y = \vec{0})])$$

$$(\mathbf{Vp}(x) \wedge \mathbf{Vp}(y) \wedge \forall u[\mathbf{Vp}(u) \rightarrow u \odot x = u \odot y]) \rightarrow x = y$$

$$\|x\| = x \odot x$$

3 Composition Algebra Doubling.

Use `encapsulate` to axiomatize, in ACL2(r), two composition algebras, with vector predicates $V_1 p$ and $V_2 p$. The vectors satisfying $V_2 p$ are `ordered pairs` of elements satisfying $V_1 p$. Both algebras, individually, satisfy all the axioms (and also all theorems) of the previous section. These additional axioms connect the various vector operations of the two spaces:

- Additional Axioms.

$$x +_2 y = ([\mathtt{car}(x) +_1 \mathtt{car}(y)]; [\mathtt{cdr}(x) +_1 \mathtt{cdr}(y)])$$

$$a \circ_2 x = ([a \circ_1 \mathtt{car}(x)]; [a \circ_1 \mathtt{cdr}(x)])$$

$$[V_1 p(x) \wedge V_1 p(y)] \rightarrow (x; \vec{0}_1) \bullet_2 (y; \vec{0}_1) = ([x \bullet_1 y]; \vec{0}_1)$$

$$V_1 p(x) \rightarrow ([\|(x; \vec{0}_1)\|_2 = \|x\|_1] \wedge [\|(\vec{0}_1; x)\|_2 = \|x\|_1])$$

$$[V_1 p(x) \wedge V_1 p(y)] \rightarrow (x; \vec{0}_1) \odot_2 (\vec{0}_1; y) = 0$$

$$\vec{1}_2 = (\vec{1}_1; \vec{0}_1)$$

$$V_1 p(x) \rightarrow (x; \vec{0}_1) \bullet_2 (\vec{0}_1; \vec{1}_1) = (\vec{0}_1; x)$$

Since both $V_1 p$ and $V_2 p$ are composition algebras,

$$\begin{aligned} &[V_1 p(v_1) \wedge V_1 p(v_2) \wedge V_1 p(w_1) \wedge V_1 p(w_2)] \rightarrow \\ &\quad [\,\|v_1 \bullet_1 v_2\|_1 = \|v_1\|_1 \cdot \|v_2\|_1 \wedge \\ &\quad \|(v_1; w_1) \bullet_2 (v_2; w_2)\|_2 = \|(v_1; w_1)\|_2 \cdot \|(v_2; w_2)\|_2\,]. \end{aligned}$$

Among the consequences of these `encapsulated` axioms, ACL2(r) verifies:

- Dot Product Doubling.

$$\begin{aligned} &[V_1 p(v_1) \wedge V_1 p(v_2) \wedge V_1 p(w_1) \wedge V_1 p(w_2)] \rightarrow \\ &\quad (v_1; v_2) \odot_2 (w_1; w_2) = [v_1 \odot_1 w_1] + [v_2 \odot_1 w_2] \end{aligned}$$

- Conjugation Doubling.

$$[V_1 p(v_1) \wedge V_1 p(v_2)] \rightarrow \overline{(v_1; v_2)} = (\bar{v}_1; -v_2)$$

- Product Doubling.

$$\begin{aligned} &[V_1 p(v_1) \wedge V_1 p(v_2) \wedge V_1 p(w_1) \wedge V_1 p(w_2)] \rightarrow \\ &\quad (v_1; v_2) \bullet_2 (w_1; w_2) = \\ &\quad (\{[v_1 \bullet_1 w_1] - [\bar{w}_2 \bullet_1 v_2]\}; \{[w_2 \bullet_1 v_1] +_1 [v_2 \bullet_1 \bar{w}_1]\}) \end{aligned}$$

- Norm Doubling.
$$[V_1p(v_1) \wedge V_1p(v_2)] \to \|(v_1;v_2)\|_2 = \|v_1\|_1 + \|v_2\|_1$$
- Associativity of $\bullet_1$.
$$[V_1p(v_1) \wedge V_1p(v_2) \wedge V_1p(v_3)] \to [v_1 \bullet_1 v_2] \bullet_1 v_3 = v_1 \bullet_1 [v_2 \bullet_1 v_3]$$

The above doubling theorems match the definitions used in the Cayley-Dickson Construction for making ordered pairs of V_1p vectors into V_2p vectors. Furthermore, if both the V_2p ordered pairs and the the component V_1p vectors form composition algebras, then the component V_1p algebra has an associative multiplication.

In addition, ACL2(r) verifies that if the component V_1p vectors form a composition algebra with an associative multiplication, then the Cayley-Dickson Construction makes the V_2p ordered pairs into a composition algebra.

3.1 Summary

ACL2(r) verifies:

- Start with a composition algebra V_1p.
- Let V_2p be the set of ordered pairs of elements from V_1p.
- Then
  1. (a) If V_2p is also a composition algebra, then V_1p-multiplication is associative.
     (b) If V_1p-multiplication is associative, then V_2p can be made into a composition algebra.
  2. (a) If V_2p is a composition algebra with associative multiplication, then V_1p-multiplication is associative and commutative.
     (b) If V_1p-multiplication is associative and commutative, then V_2p can be made into a composition algebra with associative multiplication.
  3. (a) If V_2p is a composition algebra with associative and commutative multiplication, then V_1p-multiplication is also associative and commutative, and V_1p-conjugation is trivial.
     (b) If V_1p-multiplication is associative and commutative, and V_1p-conjugation is trivial, then V_2p can be made into a composition algebra with associative and commutative multiplication.

3.1.1 A last example

Apply the Cayley-Dickson Construction to pairs of octonions. Think of the octonions as eight-dimensional vectors. Interpret ordered pairs of octonions as sixteen-dimensional vectors called Sedenions [5]: For octonians

$$\begin{aligned} o &= a_1 + a_2 \cdot i + a_3 \cdot j + a_4 \cdot k + a_5 \cdot \ell + a_6 \cdot I + a_7 \cdot J + a_8 \cdot K \\ p &= b_1 + b_2 \cdot i + b_3 \cdot j + b_4 \cdot k + b_5 \cdot \ell + b_6 \cdot I + b_7 \cdot J + b_8 \cdot K, \end{aligned}$$

$$\begin{aligned} (o;p) &= o + p \cdot L \\ &= a_1 + a_2 \cdot i + a_3 \cdot j + a_4 \cdot k + a_5 \cdot \ell + a_6 \cdot I + a_7 \cdot J + a_8 \cdot K \\ &\quad + b_1 \cdot L + b_2 \cdot iL + b_3 \cdot jL + b_4 \cdot kL + b_5 \cdot \ell L + b_6 \cdot IL \\ &\quad + b_7 \cdot JL + b_8 \cdot KL. \end{aligned}$$

For octonion

$$\begin{aligned} o &= a_1 + a_2 \cdot i + a_3 \cdot j + a_4 \cdot k + a_5 \cdot \ell + a_6 \cdot I + a_7 \cdot J + a_8 \cdot K, \\ \bar{o} &= a_1 - a_2 \cdot i - a_3 \cdot j - a_4 \cdot k - a_5 \cdot \ell - a_6 \cdot I - a_7 \cdot J - a_8 \cdot K \end{aligned}$$

is the **conjugate** of o.

For octonions o_1, o_2, p_1, and p_2, sedenion multiplication is defined by

$$\begin{aligned} (o_1;o_2) \cdot (p_1;p_2) &= (o_1 + o_2 \cdot L) \cdot (p_1 + p_2 \cdot L) \\ &= (o_1 p_1 - \bar{p}_2 o_2) + (p_2 o_1 + o_2 \bar{p}_1) \cdot L \\ &= ([o_1 p_1 - \bar{p}_2 o_2];[p_2 o_1 + o_2 \bar{p}_1]) \end{aligned}$$

Recall the octonians have a **non**-trivial conjugate and octonian multiplication is **not** commutative and also **not** associative. The octonions form a composition algebra, so that for octonions o and p, $\|o \cdot p\| = \|o\| \cdot \|p\|$.

By item 1(a) listed above about composition algebras, since octonian multiplication is not associative, the sedenions is not a composition algebra. In fact, the sedenion product of nonzero vectors could be the zero vector. For example, let o_1, o_2, p_1, and p_2 be these otonions:

$$\begin{aligned} o_1 &= 0 + 0 \cdot i + 0 \cdot j + 1 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K \\ o_2 &= 0 + 0 \cdot i + 1 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K \\ p_1 &= 0 + 0 \cdot i + 0 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 1 \cdot J + 0 \cdot K \\ p_2 &= 0 + 0 \cdot i + 0 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + (-1 \cdot K). \end{aligned}$$

Then

$$\begin{aligned} &(o_1 + o_2 \cdot L) \cdot (p_1 + p_2 \cdot L) = \\ &\quad (0 + 0 \cdot i + 0 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K) \\ &\quad + (0 + 0 \cdot i + 0 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K) \cdot L. \end{aligned}$$

So

$$\|(o_1 + o_2 \cdot L) \cdot (p_1 + p_2 \cdot L)\| = 0,$$

but

$$\|(o_1 + o_2 \cdot L)\| = 2 = \|(p_1 + p_2 \cdot L)\|,$$

and

$$\|(o_1 + o_2 \cdot L) \cdot (p_1 + p_2 \cdot L)\| \neq \|(o_1 + o_2 \cdot L)\| \cdot \|(p_1 + p_2 \cdot L)\|.$$

All nonzero sedenions have multiplicative inverses. For example,

$$\begin{aligned} &(o_1 + o_2 \cdot L)^{-1} = \\ &\quad (0 + 0 \cdot i + 0 \cdot j + (-\frac{1}{2} \cdot k) + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K) \\ &\quad + (0 + 0 \cdot i + (-\frac{1}{2} \cdot j) + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + 0 \cdot K) \cdot L \\ &(p_1 + p_2 \cdot L)^{-1} = \\ &\quad (0 + 0 \cdot i + 0 \cdot j + 0 \cdot k) + 0 \cdot \ell + 0 \cdot I + (-\frac{1}{2} \cdot J) + 0 \cdot K) \\ &\quad + (0 + 0 \cdot i + 0 \cdot j + 0 \cdot k + 0 \cdot \ell + 0 \cdot I + 0 \cdot J + (\frac{1}{2} \cdot K)) \cdot L \end{aligned}$$

A ACL2(r) Books

A.1 `cayley1.lisp`

The Reals form a (1-dimensional) composition algebra.

A.2 `cayley1a.lisp`

Cons pairs of Reals form a (2-dimensional) composition algebra.
This algebra is (isomorphic to) the Complex Numbers.

A.3 `cayley1b.lisp`

Cons pairs of Complex Numbers form a (4-dimensional) composition algebra.
This algebra is (isomorphic to) the Quaternions.

3-Dimensional Vector Cross Product and 3-Dimensional Dot Product are related to 4-Dimensional Quaternion Multiplication.

A.4 `cayley1c.lisp`

Cons pairs of Quaternions form a (8-dimensional) composition algebra.
This algebra is (isomorphic to) the Octonions.

7-Dimensional Vector Cross Product and 7-Dimensional Dot Product are related to 8-Dimensional Octonion Multiplication.

A.5 `cayley1d.lisp`

Cons pairs of Octonions form a (16-dimensional) algebra.
This algebra is (isomorphic to) the Sedenions.

This algebra is not a composition algebra, but all nonzero Sedenions have multiplicative inverses.

A.6 `cayley2.lisp`

Axioms and theory of composition algebras.

A.7 `cayley2.lisp`

In composition algebras, $\|v\| = v \odot v$.

A.8 `cayley3.lisp`

Start with a composition algebra V1. Let V2 be the set of ordered pairs of elements from V1.

If V2 is also a composition algebra, then V1-multiplication is associative.

A.9 `cayley3a.lisp`

Start with a composition algebra V. Let V2 be the set of ordered pairs of elements from V.

If V-multiplication is associative, then V2 can be made into a composition algebra.

A.10 `cayley4.lisp`

Start with a composition algebra V1. Let V2 be the set of ordered pairs of elements from V1.

If V2 is a composition algebra with associative multiplication, then V1-multiplication is associative and commutative.

A.11 `cayley4a.lisp`

Start with a composition algebra V. Let V2 be the set of ordered pairs of elements from V.

If V-multiplication is associative and commutative, then V2 can be made into a composition algebra with associative multiplication.

A.12 `cayley5.lisp`

Start with a composition algebra V1. Let V2 be the set of ordered pairs of elements from V1.

If V2 is a composition algebra with associative and commutative multiplication, then V1-multiplication is associative and commutative, and V1-conjugation is trivial.

A.13 `cayley5a.lisp`

Start with a composition algebra V. Let V2 be the set of ordered pairs of elements from V.

If V-multiplication is associative and commutative, and V-conjugation is trivial, then V2 can be made into a composition algebra with associative and commutative multiplication.

References

[1] J.H. Conway & D.A. Smith (2003): *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*. AK Peters.

[2] Princeton Companion Group (2008): *Quaternions, Octonians, and Normed Division Algebras*. In Timothy Gowers, editor: *The Princeton Companion to Mathematics*, Princeton University Press, doi:10.1515/9781400830398.

[3] M. Koecher & R. Remmert (1991): *Chapter 7, Hamilton's Quaternions; Chapter 9, CAYLEY Numbers or Alternative Division Algebras; Chapter 10, Section 1, Composition Algebras*. In F. Hirzebruch M. Koecher K. Mainzer J. Neukirch A. Prestel H.-D. Ebbinghaus, H. Hermes & R. Remmert, editors: *Numbers*, Springer-Verlag, doi:10.1007/978-1-4612-1005-4.

[4] Wikipedia (2016): *Cayley-Dickson construction: From Wikipedia, the free encyclopedia*. Available at `https://en.wikipedia.org/wiki/Cayley-Dickson_construction`.

[5] Wikipedia (2016): *Sedenion: From Wikipedia, the free encyclopedia*. Available at `https://en.wikipedia.org/wiki/Sedenion`.