The Cayley-Dickson Construction in ACL2

John Cowles and Ruben Gamboa

Department of Computer Science
University of Wyoming
Laramie, Wyoming 82071

{cowles,ruben}@uwyo.edu

May 22-23, 2017

UNIVERSITY OF WYOMING

Cayley-Dickson Construction

How to define a multiplication for vectors?

- Generalize the construction of complex numbers from pairs of real numbers.
- View complex numbers as two dimensional vectors equipped with a multiplication.

Desirable properties for a vector multiplication

zero vector: $\mathbf{v} \bullet \vec{\mathbf{0}} = \vec{\mathbf{0}}$

unit vector: $\vec{\mathbf{1}} \bullet \mathbf{v} = \mathbf{v}$

inverse for nonzero vectors: $\mathbf{v}^{-1} \bullet \mathbf{v} = \vec{\mathbf{1}}$

associative: $(\mathbf{v}_1 \bullet \mathbf{v}_2) \bullet \mathbf{v}_3 = \mathbf{v}_1 \bullet (\mathbf{v}_2 \bullet \mathbf{v}_3)$

Use **zero vector**, **unit vector**, **associative** and **inverse for nonzero vectors** properties to prove:

closure for nonzero vectors:

$$(\mathbf{v_1} \neq \vec{\mathbf{0}} \wedge \mathbf{v_2} \neq \vec{\mathbf{0}}) \rightarrow \mathbf{v_1} \bullet \mathbf{v_2} \neq \vec{\mathbf{0}}$$

Prove

$$(\mathbf{v_1} \bullet \mathbf{v_2} = \vec{\mathbf{0}} \wedge \mathbf{v_1} \neq \vec{\mathbf{0}}) \rightarrow \mathbf{v_2} = \vec{\mathbf{0}}$$

Prove

$$(\mathbf{v_1} \bullet \mathbf{v_2} = \vec{\mathbf{0}} \wedge \mathbf{v_1} \neq \vec{\mathbf{0}}) \rightarrow \mathbf{v_2} = \vec{\mathbf{0}}$$

Assume $\mathbf{v_1} \bullet \mathbf{v_2} = \vec{\mathbf{0}} \wedge \mathbf{v_1} \neq \vec{\mathbf{0}}$. Then

$$\begin{aligned}
\mathbf{v_2} &= \vec{\mathbf{1}} \bullet \mathbf{v_2} \\
&= (\mathbf{v_1^{-1}} \bullet \mathbf{v_1}) \bullet \mathbf{v_2} \\
&= \mathbf{v_1^{-1}} \bullet (\mathbf{v_1} \bullet \mathbf{v_2}) \\
&= \mathbf{v_1^{-1}} \bullet \vec{\mathbf{0}} \\
&= \vec{\mathbf{0}}
\end{aligned}$$

Recall the construction of complex numbers from pairs of real numbers.

Interpret pairs of real numbers as complex numbers:

For real **v** and **w**,

$$(\mathbf{v}\,;\mathbf{w}) = (\text{complex } \mathbf{v}\ \ \mathbf{w}) = \mathbf{v} + \mathbf{w} \cdot \boldsymbol{i}$$

Complex multiplication. Think of the real numbers as one dimensional vectors.

For reals $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{w}_1, \mathbf{w}_2$, complex multiplication is defined by

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

Satisfies **zero vector**, **unit vector**, **inverse for nonzero vectors**, and **associative**, properties.

Repeat this same construction using pairs of **complex numbers** (instead of pairs of **reals**).

For **complex** $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{w}_1, \mathbf{w}_2$, multiplication of **pairs** is defined by

$$\begin{aligned}(\mathbf{v_1}; \mathbf{v_2}) \bullet (\mathbf{w_1}; \mathbf{w_2}) = \\ \quad ([\mathbf{v_1 w_1} - \mathbf{v_2 w_2}] \,;\, [\mathbf{v_1 w_2} + \mathbf{v_2 w_1}])\end{aligned}$$

This multiplication is **associative.**

$$\vec{\mathbf{0}} = ((\text{complex } \mathbf{0}\ \mathbf{0})\,;\,(\text{complex } \mathbf{0}\ \mathbf{0}))$$

$$\vec{\mathbf{1}} = ((\text{complex } \mathbf{1}\ \mathbf{0})\,;\,(\text{complex } \mathbf{0}\ \mathbf{0}))$$

This property **fails**:

closure for nonzero vectors:

$$(\mathbf{v_1} \neq \vec{\mathbf{0}} \wedge \mathbf{v_2} \neq \vec{\mathbf{0}}) \rightarrow \mathbf{v_1} \bullet \mathbf{v_2} \neq \vec{\mathbf{0}}$$

Example:

$$\begin{aligned} &((\text{complex } \mathbf{1}\ \mathbf{0})\ ;\ (\text{complex } \mathbf{0}\ \mathbf{1})) \\ &\quad \bullet \quad ((\text{complex } \mathbf{1}\ \mathbf{0})\ ;\ (\text{complex } \mathbf{0}\ \ -\mathbf{1})) = \vec{\mathbf{0}} \end{aligned}$$

No multiplicative inverse for this vector:

$$((\text{complex } \mathbf{1}\ \mathbf{0})\ ;\ (\text{complex } \mathbf{0}\ \mathbf{1})) \neq \vec{\mathbf{0}}$$

Generalize "complex" multiplication of **pairs**:

$$(\mathbf{v_1}; \mathbf{v_2}) \bullet (\mathbf{w_1}; \mathbf{w_2}) = \\ ([\mathbf{v_1 w_1} - \mathbf{v_2 w_2}]\,;\ [\mathbf{v_1 w_2} + \mathbf{v_2 w_1}])$$

into **"Cayley-Dickson"** multiplication of **pairs**:

For **complex** $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{w}_1, \mathbf{w}_2$,

$$(\mathbf{v_1}; \mathbf{v_2}) \bullet (\mathbf{w_1}; \mathbf{w_2}) = \\ ([\mathbf{v_1 w_1} - \bar{\mathbf{w}}_2 \mathbf{v_2}]\,;\ [\mathbf{w_2 v_1} + \mathbf{v_2} \bar{\mathbf{w}}_1])$$

Here $\bar{\mathbf{w}}$ is the complex conjugate of $\mathbf{w}$.

Pairs of complex numbers with **Cayley-Dickson** multiplication:

$$(\mathbf{v_1} ; \mathbf{v_2}) \bullet (\mathbf{w_1} ; \mathbf{w_2}) = \\ ([\mathbf{v_1 w_1} - \bar{\mathbf{w}}_2 \mathbf{v_2}] ; [\mathbf{w_2 v_1} + \mathbf{v_2} \bar{\mathbf{w}}_1])$$

Satisfies **zero vector**, **unit vector**, **inverse for nonzero vectors**, and **associative** properties.

Vector space, of these pairs, is (isomorphic to) William Hamilton's **Quaternions.**

Cayley-Dickson Construction

Given a vector space, with multiplication, and with a unary **conjugate** operation, $\bar{\mathbf{v}}$.

Form “new” **Cayley-Dickson** vectors:
Pairs of “old” vectors $(\mathbf{v}_1; \mathbf{v}_2)$

Cayley-Dickson multiplication:

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

Cayley-Dickson conjugation:

$$\overline{(\mathbf{v}_1; \mathbf{v}_2)} = (\bar{\mathbf{v}}_1; -\mathbf{v}_2)$$

Cayley-Dickson Construction

Start with (1-dimensional) reals.

Real conjugate defined by

$$\bar{\mathbf{v}} = (\text{identity } \mathbf{v}) = \mathbf{v}$$

Use **Cayley-Dickson Construction** on pairs of reals:

Obtain (2-dimensional) complex numbers

Cayley-Dickson Construction

Use **Cayley-Dickson Construction** on pairs of complex numbers:

Obtain (4-dimensional) quaternions.

Cayley-Dickson Construction

Use **Cayley-Dickson Construction** on pairs of quaternions:

Obtain (8-dimensional) vector space (isomorphic to) Grave's & Cayley's **Octonians.**

Satisfies **zero vector**, **unit vector**, and **inverse for nonzero vectors** properties**.**

Fails to be **associative**, but
satisfies **closure for nonzero vectors.**

Cayley-Dickson Construction

Use **Cayley-Dickson Construction** on pairs of octonians:

Obtain (16-dimensional) vector space (isomorphic to) the **Sedenions.**

Satisfies **zero vector**, **unit vector**, and **inverse for nonzero vectors** properties**.**

Fails to be **associative.**
Fails **closure for nonzero vectors**.

Composition Algebras

Each of these vector spaces:

Reals, **Complex Numbers**,
Quaternions, and **Octonions**

has a vector multiplication, $\mathbf{v}_1 \bullet \mathbf{v}_2$, satisfying:

For the Euclidean length of a vector $|\mathbf{v}|$,

$$|\mathbf{v_1} \bullet \mathbf{v_2}| = |\mathbf{v_1}| \cdot |\mathbf{v_2}|$$

Composition Algebras

Define the **norm** of vector **v**:

$$\|\mathbf{v}\| = |\mathbf{v}|^2$$

Reformulate

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

with equivalent

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

.

Composition Algebras

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

$$(x_1, \ldots, x_n) \odot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i \cdot y_i$$

Then **norm** and **dot product** are related:

$$\begin{array}{rcl} |\mathbf{v}| & = & \sqrt{\mathbf{v} \odot \mathbf{v}} \\ ||\mathbf{v}|| & = & \mathbf{v} \odot \mathbf{v} \end{array}$$

Also

$$\mathbf{v} \odot \mathbf{w} = \frac{1}{2} \cdot (||\mathbf{v} + \mathbf{w}|| - ||\mathbf{v}|| - ||\mathbf{w}||)$$

A **Composition Algebra** is

- a real vector space
- with vector multiplication
- with a real-valued **norm**
- satisfies this **composition law**

$$\|\mathbf{v_1} \bullet \mathbf{v_2}\| = \|\mathbf{v_1}\| \cdot \|\mathbf{v_2}\|$$

Composition Algebras

In a composition algebra $\boldsymbol{Vp}$:

Define a real-valued **dot** product by

$$\mathbf{v} \odot \mathbf{w} = \frac{1}{2} \cdot (\|\mathbf{v} + \mathbf{w}\| - \|\mathbf{v}\| - \|\mathbf{w}\|)$$

Assume this dot product satisfies

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

Composition Algebras

Use **encapsulate** to axiomatize the algebras.

These unary operations can be defined:

- conjugate
- multiplicative inverse

Composition Algebras

The **ACL2(r)** theory includes these theorems:

- multiplicative closure for nonzero vectors
- nonzero vectors have multiplicative inverses
- $\|\mathbf{v}\| = \mathbf{v} \odot \mathbf{v}$

Composition Algebras

Remember the **octonions**:

- 8-dimensional Composition Algebra
- vector multiplication is **not** associative

Vector Multiplication Associativity **not** a theorem of Composition Algebra Theory.

Composition Algebras

Start with a composition algebra $\boldsymbol{V_1p}$.

Let $\boldsymbol{V_2p}$ be the set of pairs of elements from $\boldsymbol{V_1p}$.

ACL2(r) verifies:

If $\boldsymbol{V_1p}$-multiplication is **associative**, then $\boldsymbol{V_2p}$ can be made into a composition algebra.

Use the **Cayley-Dickson Construction**.

Composition Algebras

Start with a composition algebra $\boldsymbol{V_1 p}$.

Let $\boldsymbol{V_2 p}$ be the set of pairs of elements from $\boldsymbol{V_1 p}$.

ACL2(r) verifies:

If $\boldsymbol{V_2 p}$ is also a composition algebra,

then $\boldsymbol{V_1 p}$-multiplication is **associative.**

Composition Algebras

Start with a composition algebra $\boldsymbol{V_1 p}$.

Let $\boldsymbol{V_2 p}$ be the set of pairs of elements from $\boldsymbol{V_1 p}$.

ACL2(r) verifies **Conjugation Doubling**:

If $\boldsymbol{V_2 p}$ is also a composition algebra,

then in $\boldsymbol{V_2 p}$

$$\overline{(\mathbf{v}_1; \mathbf{v}_2)} = (\bar{\mathbf{v}}_1; -\mathbf{v}_2)$$

Composition Algebras

Conjugation Doubling:

$$\overline{(\mathbf{v}_1; \mathbf{v}_2)} = (\bar{\mathbf{v}}_1; -\mathbf{v}_2)$$

Matches conjugation used in **Cayley-Dickson Construction.**

Composition Algebras

Start with a composition algebra $\boldsymbol{V_1 p}$.

Let $\boldsymbol{V_2 p}$ be the set of pairs of elements from $\boldsymbol{V_1 p}$.

ACL2(r) verifies **Product Doubling**:

If $\boldsymbol{V_2 p}$ is also a composition algebra,

then in $\boldsymbol{V_2 p}$

$$\begin{aligned}(\mathbf{v_1};\mathbf{v_2}) \bullet_2 (\mathbf{w_1};\mathbf{w_2}) = \\ ([\mathbf{v_1} \bullet_1 \mathbf{w_1} - \bar{\mathbf{w}}_2 \bullet_1 \mathbf{v_2}]\,;\,[\mathbf{w_2} \bullet_1 \mathbf{v_1} + \mathbf{v_2} \bullet_1 \bar{\mathbf{w}}_1])\end{aligned}$$

Composition Algebras

Product Doubling:

$$(\mathbf{v}_1 ; \mathbf{v}_2) \bullet_2 (\mathbf{w}_1 ; \mathbf{w}_2) = \\ ([\mathbf{v}_1 \bullet_1 \mathbf{w}_1 - \bar{\mathbf{w}}_2 \bullet_1 \mathbf{v}_2] ; [\mathbf{w}_2 \bullet_1 \mathbf{v}_1 + \mathbf{v}_2 \bullet_1 \bar{\mathbf{w}}_1])$$

Matches product used in **Cayley-Dickson Construction.**