Quaternions, octonions, and now, 16-ons and 2^n-ons; New kinds of numbers.

Warren D. Smith*
WDSmith@fastmail.fm

February 14, 2004

***Abstract* —**

"Cayley-Dickson doubling," starting from the real numbers, successively yields the complex numbers (dimension 2), quaternions (4), and octonions (8). Each contains all the previous ones as subalgebras. Famous Theorems, previously thought to be the last word, state that these are the full set of division (or normed) algebras with 1 over the real numbers. Their properties keep degrading: the complex numbers lose the ordering and self-conjugacy ($\overline{\overline{x}} = x$) properties of the reals; at the quaternions we lose commutativity; and at the octonions we lose associativity. If one keeps Cayley-Dickson doubling to get the 16-dimensional "sedenions," zero-divisors appear.

We introduce a *different* doubling process which also produces the complexes, quaternions, and octonions, but keeps going to yield 2^n-dimensional normed algebraic structures, for every $n > 0$. Each contains all the previous ones as subalgebras. We'll see how these evade the Famous Impossibility Theorems. They also lead to a rational "vector product" operation in $2^k - 1$ dimensions for each $k \geq 2$; this operation is impossible in other dimensions.

But properties continue to degrade. The 16-ons lose distributivity, right-cancellation $yx \cdot x^{-1} = y$, flexibility $a \cdot ba = ab \cdot a$, and antiautomorphism $\overline{ab} = \overline{b}\overline{a}$. The 32-ons lose the properties that the solutions of generic division problems necessarily exist and are unique, and they lose the "Trotter product limit formula." We introduce an important new notion to topology we call "generalized smoothness." The 2^n-ons are generalized smooth for $n \leq 4$.

All the 2^n-ons have 1 and obey numerous identities including weakenings of the distributive, associative, and antiautomorphism laws. In the case of 16-ons these weakened distributivity laws *characterize* them, i.e. our 16-ons are, in a sense, unique and best-possible. Our 2^n-ons are also unique, albeit in a much weaker sense. The 2^n-ons with $n \leq 4$ support a version of the fundamental theorem of algebra. Normed algebras (rational but not nec. distributive) over the reals are impossible in dimensions other than powers of 2.

Keywords — Quaternions, octonions, 16-ons, fundamental theorem of algebra, division, loops, non-distributive algebras, topology, generalized smoothness, Brouwer degree, vector fields on spheres, vector product, weak-linearity, left-alternative, Moufang and Bol laws, Schwartz-Zippel lemma, automatic verification of polynomial identities, Trotter product limit formula.

Contents

*Some of this research was done at DIMACS, Rutgers University, 96 Frelinghuysen Road, Piscataway NJ 08854-8018 and Temple University, math. dept. Wachman Hall, 1805 North Broad Street Philadelphia, PA 19122-6094.

1 Convenient table of properties of the 2^n-ons

1-ons=Reals.
2-ons=Complex numbers. Lose: $\overline{z} = z$ (the overline denotes conjugating, i.e. changing the sign of imaginary components); the ordering properties that both $\{z > 0, -z > 0, \text{ or } z = 0\}$ and $\{w > 0, z > 0 \text{ implies } w + z > 0, wz > 0\}$.
4-ons=Quaternions. Lose: commutativity $ab = ba$; the algebraic closedness property that every univariate polynomial equation has a root.
8-ons=Octonions. Lose: associativity $ab \cdot c = a \cdot bc$.
16-ons. Lose: right-alternativity $x \cdot yy = xy \cdot y$; right-cancellation $x = xy \cdot y^{-1}$; flexibility $x \cdot yx = xy \cdot x$; left-linearity $(b + c)a = ba + ca$; anti-automorphism $\overline{ab} = \overline{b}\overline{a}$, $(ab)^{-1} = b^{-1}a^{-1}$; left-linearity $(b + c)a = ba + ca$; continuity of the map $x \to xy$; Moufang and Bol identities (see EQs 10 & 11); diassociativity (see §5).
32-ons. Lose: generalized-smoothness of the map $x \to xy$; right-division properties that $xa = b$ has (generically) a solution x, and the uniqueness of such an x; the "fundamental theorem of algebra" that every polynomial having a unique "asymptotically dominant monomial" must have a root; Trotter's formula $\lim_{n\to\infty}[e^{x/n}e^{y/n}]^n = e^{x+y}$.
...
2^n-ons. Retain forever: Unique 2-sided multiplicative & additive identity elements 1 & 0; norm-multiplicativity $|xy|^2 = |x|^2|y|^2$; norm-subadditivity $|a + b| \leq |a| + |b|$; 2-sided inverse $a^{-1} = \overline{a}/|a|^2$ $(a \neq 0)$; $\overline{\overline{a}} = a$; $\overline{x \pm y} = \overline{x} \pm \overline{y}$; $(a^{-1})^{-1} = a$; $(\overline{a})^{-1} = \overline{a^{-1}}$; $|a|^2 = |\overline{a}|^2 = a\overline{a}$; left-alternativity $yy \cdot x = y \cdot yx$; left-cancellation $x = y^{-1} \cdot yx$; right-linearity $a(b+c) = ab+ac$; power-associativity $a^k a^\ell = a^{k+\ell}$; scaling $s \cdot ab = sa \cdot b = as \cdot b = a \cdot sb = a \cdot bs = ab \cdot s$ (s real); power-distributivity $(ra^k + sa^\ell)b = ra^k b + sa^\ell b$ (r, s real); vector product properties of $ab - \text{re}(ab)$ for pure-imaginary 2^n-ons a,b regarded as $(2^n - 1)$-vectors; numerous *weakened* associativity, commutativity, distributivity, antiautomorphism, and Moufang and Bol properties including 9-coordinate "niner" versions of most of those properties; contains 2^{n-1}-ons as subalgebra.

2 Introduction

Numbers [94] are commonly thought of as a dense infinite set of things, including "1" and "0," that one may add, subtract, multiply, and (except for division by 0) divide. The *real* numbers (and various subfields thereof, e.g. the rational, algebraic, and computable reals) are the prototypical example. It revolutionized analysis when it was understood that the reals are merely a 1-dimensional subfield of the 2-dimensional *complex* numbers. Effects which, so far, have been rather less revolutionary, were brought about by the discovery of the 4D *quaternions* and the 8D *octonions* – which continue the chain of inclusions begun by the complex numbers – and, in an entirely different direction, the surreals [66].

The purpose of this monograph is to present the 2^n-*ons* (pronunciation: "two-to-the-any-ons"), an infinite sequence of *normed* algebraic structures continuing the real⊂complex⊂quaternion⊂octonion inclusion chain[1].

The 2^n-ons (and in particular, the 16-ons) were commonly previously thought, incorrectly, to be impossible. The previous impossibility theorems (§13) still are presumably correct; our 2^n-ons simply evade them by disobeying their assumptions. Specifically: the 2^n-ons are *non*distributive and have a *dis*continuous multiplication map. Nevertheless, the 2^n-ons obey some remarkable weakened distributivity properties, and the 16-ons obey a remarkable new weakened-continuity property we call "generalized smoothness" (§22).

The 2^n-ons are defined recursively in terms of the 2^{n-1}-ons by EQ 68 and 69. (See also §16 & 32.1 for discussion of the "simplest" versions of that definition.)

The most important properties of the 2^n-ons for general n are the following (§10): Each has 1 and obeys $|ab|^2 = |a|^2|b|^2$, $|a|^2 = a\overline{a}$, $a \cdot ab = a^2 b$, $a \cdot a^{-1}b = b$, $a^2 + |a|^2 = 2a\,\mathrm{re}\,a$, $a^k a^\ell = a^{k+\ell}$, $a(b+c) = ab + ac$, $\overline{\overline{a}} = a$, $\overline{a \pm b} = \overline{a} \pm \overline{b}$, $(\overline{a})^{-1} = \overline{a^{-1}}$, and, letting $\langle x, y\rangle$ denote the 2^n-vector Euclidean inner product, $\langle xa, b\rangle = \langle a, \overline{x}b\rangle$, $\langle xa, xb\rangle = |x|^2\langle a, b\rangle$, and $\langle x, y\rangle = \langle \overline{x}, \overline{y}\rangle$. The following identities hold if either at least one of $\{a, b\}$ is a "niner" (last $2^n - 9$ coordinates= 0) or if "=" is reinterpreted to mean "the real parts are equal:" $ab \cdot a = a \cdot ba$, $ab \cdot a^{-1} = a \cdot ba^{-1}$, $ba \cdot a = b \cdot a^2$, $ba^{-1} \cdot a = b$, $\overline{ab} = \overline{b}\overline{a}$. All the coordinates of a 2^n-on are "imaginary" except for a single "real" coordinate (the overline denotes conjugation, i.e. changing the signs of all imaginary coordinates). If two purely imaginary (i.e., with real part 0) 2^n-ons are multiplied, and the real part of the result discarded, then this is a "vector product" for $(2^n - 1)$-dimensional vectors $\vec{a}$, $\vec{b}$, i.e. $\vec{a} \times \vec{b}$ is perpendicular to both $\vec{a}$ and $\vec{b}$, and its length is the same as the area of the parallelogram spanned by $\vec{a}$ and $\vec{b}$ (§25.2).

The 16-ons continue the chain of property-degradation by losing the left-linear $(b+c)a = ba+ca$ *distributive* property. The 2^n-ons nevertheless obey $(b+c)a = ba+ca$ if either (1) b and c are niner, (2) a is niner, or (3) at least one of $\{a, b, c\}$ is real. We'll see in §14-16 that these and a few other weakened-distributivity properties *characterize* the 16-ons.

We show in §19-20 that one can *divide* any 2^n-on by any nonzero 2^n-on (on either side) to get an answer which, for 16-ons, generically *exists* and is *unique*. However these existence and uniqueness properties are irrevocably lost at the 32-ons. The "Trotter product limit formula" $\lim_{n\to\infty}[e^{x/n}e^{y/n}]^n = e^{x+y}$ (which underlies quantum mechanics) is another property of 16-ons x, y that is irrevocably lost at the 32-ons.

Those readers who are not pure mathematicians may ask: Of what *use* are the 2^n-ons? Nice division algebras are so exceedingly rare that it surely is worth investigating all properties of the few that exist (with the 16-ons being a new one) under the presumption that some use will be found for them all. This monograph, as the largest collection of facts and proofs about 2^n-ons, fills that need.

The quaternions played very important roles historically both in leading Maxwell to his electromagnetic equations, leading Gibbs to his 3-vector notation (cross-product, dot-product, etc.), and in fathering the entire discipline of abstract algebra – even if those roles were later largely forgotten after all of these things were redone without reference to quaternions. Known uses include: As we shall explain, the quaternions are a superior way to represent 3D and 4D rotations and Lorentz transformations. (Hence they have been used in special relativity, Newtonian mechanics, gyroscopes, aerospace engineering, computer graphics, etc.) Both the quaternions and octonions play fundamental roles in the theory of sphere packings in up to 9 dimensions [67], and hence have been used in the design of protocols for fast modems. The quaternions and octonions also play fundamental roles in the theories of Lie [144] and Jordan algebras [143], in the theory of loops [47], and in topology [2][37]. The quaternions also have been used in the best known explicit constructions [202] of fundamental combinatorial objects called "expanders" which underlie various parallel algorithms – e.g. all known asymptotically optimal parallel sorting algorithms [7] – and telephonic routing networks [30]. It also is possible that 2^n-ons will become important in theoretical physics, see open problem 4 in §30.

Along the way we'll

1. Prove new versions of the Fundamental Theorem of Algebra (§17 and 23),
2. Present new facts about quaternions and octonions,
3. Introduce a new notion called "generalized smoothness" into topology (now allowing topology to be used even for discontinuous maps),
4. Extend the "Schwartz-Zippel lemma" about computer verification of identities into the noncommutative and differential operator worlds (§11),
5. Present a useful "taxonomy of loop theory" (§26.2)
6. Show that some fundamental notions from Complex Analysis such as Cauchy Integral Formula and contour integrals have 2^n-onic analogues (§21.3),

and provide the answer to the trivia question "what mathematician was a 3000^+-ton ship named for?"

3 Notation

Nnac, nnacd: We shall employ the highly useful abbreviation *nnac* to mean (that some ring-multiplication is) "not

[1] The 2^n-ons may of course be either surrealized, or restricted to rational, algebraic, or computable subfields. Those are totally independent issues.

necessarily associative nor commutative." Indeed we sometimes even shall allow multiplication to be non-distributive, in which case we use "nnacd."

Abstract algebra: For basic definitions such as loop, group, ring, field, see elementary algebra books [145] and our §26.

"Algebras:" An n-dimensional nnacd-*algebra* A over a field F is the set of the n-tuples of elements of F, together with componentwise addition, subtraction, and scalar multiplication operations $x+y$, $x-y$, and $xs = sx$ for $s \in F$ and $x, y \in F^n$; and the key feature of A is that it has a vector-vector nnacd-*multiplication* operation, denoted by either xy or $x \cdot y$. Juxtaposition means the same as, but has higher precedence[2] than, dot: $yz \cdot t = (yz)t$. We shall mainly be interested in the real field $F = \mathbb{R}$; less frequently in the complex field $F = \mathbb{C}$, and still less frequently in finite fields such as $F = \mathrm{GF}_2$. (Actually, it is possible to start even from certain non-fields. See §26.5.) Our algebras also will usually have a "conjugation" operation denoted $\overline{x}$, obeying $\overline{\overline{x}} = x$ and $\overline{x \pm y} = \overline{x} \pm \overline{y}$, and an identity element 1. In that case $\overline{1} = 1$ and we often slightly abuse notation by writing merely s instead of $s1$.

Vectors: We denote the Euclidean inner product of two N-vectors over F by $\langle x, y\rangle = \sum_{j=0}^{N-1} x_j y_j$, and $|x|^2 = \sum_{j=0}^{N-1} x_j^2$. Thus $|x|^2 = \langle x, x\rangle$ and $\langle x, y\rangle = \langle y, x\rangle$ and $|a+b| \le |a| + |b|$.

"Iff," "wlog," "generic:" The following shorthands are often useful: "iff" means "if and only if." "Wlog" means "without loss of generality." A set of real numbers is "generic" if they obey no multivariate polynomial equation with integer coefficients (besides equations satisfied by every set of reals), i.e., are algebraically unrelated. More generally we may use "full measure" to mean "except perhaps for a set of measure zero."

re, im: We write $\mathrm{re}\, x = \langle x, 1\rangle$ and $\mathrm{im}\, x = x - \mathrm{re}\, x$. When $F = \mathbb{R}$, we shall always only be concerned with this conjugation operation: $\overline{x} = 2\,\mathrm{re}\, x - x$.

Matrices: M^{-1}, M^T, and M^H denote, respectively, the inverse, transpose, and complex-conjugate transpose (Hermitian adjoint) of a matrix M, and I denotes the identity matrix. A real matrix M is *orthogonal* if $M^T M = M M^T = I$, i.e. if it has orthonormal rows (and orthonormal columns). A complex matrix M is *unitary* if $M^H M = M M^H = I$. A matrix M is *s-scaled orthogonal* if M is s times an orthogonal matrix, so that $M^T M = s^2 I$.

Spheres: S^{n-1} denotes the $(n-1)$-dimensional manifold $|\vec{x}| = 1$ for $\vec{x} \in \mathbb{R}^n$.

Stereographic projection is the following rational bijective map between the unit sphere $|\vec{x}|^2 + z^2 = 1$ in $\mathbb{R}^n \times \mathbb{R}$ (i.e., S^n) and the hyperplane $\mathbb{R}^n \cup \infty$:

$$(\vec{x}, z) \to \frac{\vec{x}}{1-z}, \quad (\vec{0}, 1) \to \infty \tag{1}$$

whose inverse is

$$\vec{x} \to \left(\frac{2\vec{x}}{1+|\vec{x}|^2}, \frac{|\vec{x}|^2 - 1}{1+|\vec{x}|^2}\right). \tag{2}$$

Coordinates: When discussing elements of N-vectors, we shall number the coordinates from 0 to $N-1$. Starting at 0 has the advantages that (i) it is more compatible with the binary representation of integers when $N = 2^n$, and (ii) the index 0 automatically assumes a special status – useful since we shall make the 0th coordinate be the "real part" of a 2^n-on.

Mixing: We shall often mix notations commonly associated with n-vectors with notations commonly associated with n-dimensional algebra elements. E.g. x_5 means the 5th coordinate of $\vec{x}$. The special symbol e_k denotes the vector (or algebra element) whose kth coordinate is 1 and all of whose other coordinates are 0. We shall be constructing 2^n-ons in such a way that coordinates $0, \dots, 2^k - 1$ form a 2^k-on subalgebra, for[3] each k with $0 \le k < n$. 2^n-ons which are 0 in all coordinates except for the first 2^k, will thus be reals, complexes, quaternions, octonions, and 16-ons for $k = 0, 1, 2, 3, 4$ respectively. (Thus, for another example of notation-mixing, $e_0 = 1$.) It is also useful to call a 2^n-on which is zero in all but its first 9 coordinates (indices 0-8) a "niner."

Dimension: The "dimension" of a subset S of a d-dimensional manifold means its Haussdorf dimension, i.e., let S_r denote the locus of points distance$\le r$ from $S = S_0$; then

$$\dim(S) \stackrel{\text{def}}{=} \inf_{k,\, 0 \le k \le d} \{k \mid \lim_{r \to 0+} \mathrm{measure}(S_r) r^{k-d} < \infty\}. \tag{3}$$

4 Hamilton and the Quaternions

W.R. Hamilton discovered the quaternions on 16 October 1843, and described them in a letter he wrote to John T. Graves the next day.

The[4] complex numbers $a + ib$ are obtained from the reals by adjoining an additional special symbol i obeying $i^2 = -1$.

Hamilton instead adjoined *three* special symbols i, j, k, obeying $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, to the real numbers to get the quaternions $a + ib + jc + kd$. These have associative and distributive, but noncommutative, multiplication. The *conjugate* of the quaternion $q = a + ib + jc + kd$ is $\overline{q} = a - ib - jc - kd$, and its *norm* is $|q|^2 = q\overline{q} = \overline{q}q = a^2 + b^2 + c^2 + d^2$. Norms are multiplicative: $|ab|^2 = |a|^2 |b|^2$. The reciprocal (both the left and right inverse are the same) is $q^{-1} = \overline{q}/|q|^2$.

Hamilton and his followers, knowing the tremendous importance of complex numbers, naturally thought the quaternions would be even richer and more important. However, history has disappointed those hopes. One important reason is the 1850 theorem [166] of J.Liouville (1809-1882) that the only

[2] Some authors continue by defining $a : b$ and $a \dot{:} b$ to mean the same thing as $a \cdot b$, but with successively lower precedence.

[3] Warning. In §5 we give a "nice" construction of the octonions and in §8 of Cayley and Dickson's "sedenions," which do *not* have the property that the first 4 (respectively 8) coordinates form a quaternion (respectively octonion) subalgebra. Instead, the quaternion subalgebra $(1, i, j, k)$ of the octonions of §5 is in the coordinates corresponding to $(1, i_1, i_2, i_4)$; the octonion subalgebra of the sedenions of §8 is in the 8 coordinates $(1, s_1^+, s_2^+, \dots, s_7^+)$. We have departed from our usual coordinate-numbering convention in these sections *only*, purely because we want to show the most beautiful and symmetric possible constructions of the octonions anf Cayley-Dickson sedenions. You are also warned that the "sedenions" of Cayley and Dickson, described in §8, are entirely different from our "16-ons," described in §9.

[4] The theorem mentioned in §1 about the impossibility of "ordering" $\mathbb{C}$ is proven on page 68 of [94].

conformal mappings in dimensions ≥ 3 are spherical inversions; thus the exceedingly rich theory of "analytic" (which means the same thing as "complex-differentiable" and as "conformal") complex functions has no analogue in higher dimensions. Nevertheless, quaternions are far from useless. Special relativity, Lorentz transformations, and Maxwell's equations of electromagnetism may be reformulated quaternionically (or biquaternionically). The latter was done by Maxwell himself (see §21.3), but nowadays this is rare since it does not seem to bring any advantage. The quaternions inspired, and make useful, Gibbs's very used 3-vector "cross product" $\vec{a} \times \vec{b}$ notation and its relatives $\vec{\nabla} \times \vec{F}(\vec{x})$, etc. since the quaternion multiplication law (with quaternions now regarded as $\mathbb{R} \times \mathbb{R}^3$) may be written

$$(a, \vec{x})(b, \vec{y}) = (ab - \vec{x} \cdot \vec{y},\ a\vec{y} + b\vec{x} + \vec{x} \times \vec{y}). \tag{4}$$

They also were the source from which the great edifice of abstract algebra has sprung. (E.g., Hamilton was apparently the first to consider the "associative law" of multiplication.)

Rotations. One reason quaternions are useful is that they may be used to represent rotations [70]. Hamilton had been inspired by the fact that multiplication by a unit-norm complex number effects a *two*-dimensional rotation. Fact: any 3×3 rotation matrix may be represented as a unit-norm quaternion q (and exactly two such quaternions q and $-q$ work), with the rotation acting on a 3-vector $\vec{x}$ (regarded as a pure-imaginary quaternion x) via $x \to q^{-1}xq = \overline{q}xq$. Indeed (formula due to Olinde Rodrigues[5] in 1840), the q causing a rotation of angle θ counterclockwise about the axis $\vec{a}$ (with $|\vec{a}| = 1$) is given by the following beautiful formula

$$\pm q = (\cos\frac{\theta}{2}, \vec{a}\sin\frac{\theta}{2}) = \exp\frac{a\theta}{2} \tag{5}$$

where the rightmost expression denotes the quaternion-valued exponential (EQ 150) of the pure-imaginary unit-norm 3-component quaternion a. Note this is far nicer than employing a 3×3 rotation matrix since the axis and angle of the rotation are simply related to the transformation, and also because, e.g. the average of two rotation matrices is not a rotation matrix, whereas the average of two quaternions is still a quaternion.

Fact[6]: any 4×4 rotation matrix may be represented as a pair (a, b) of unit-norm quaternions (and exactly two such work; the negated pair is the other), acting on a 4-vector (regarded as a quaternion x) via $x \to axb$. Further, any unit-norm quaternion is the exponential (defined in EQ 150) of a pure-imaginary quaternion, so this 4D rotation instead may be written

$$x \to \exp(a)x\exp(b) \tag{6}$$

where a and b are pure-imaginary quaternions.

Although both of these facts are well known [71], we have not previously seen the fact that *five*-dimensional rotations may also be represented with quaternions.

To do that, we garner the extra dimension in a manner analogous to the way that complex numbers may be used to represent 3D rotations. To recall that: we stereographically project the surface of the unit sphere in $\mathbb{R}^3$ down to the plane $\mathbb{C}$, then perform a Möbius transformation $z \to \frac{az-b}{\overline{b}z+\overline{a}}$ where $|a|^2 + |b|^2 = 1$, then stereographically inverse-project back up onto the sphere.

Now, to perform rotations similarly in $\mathbb{R}^5$, we stereographically project the surface of a sphere in $\mathbb{R}^5$ into $\mathbb{R}^4$, regarded as the quaternions. Then we perform a quaternionic Moebius transformation $q \to (cq + d)^{-1}(aq + b)$ where $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$, and $\overline{a}b + \overline{c}d = 0$. Finally, we stereographically inverse-project back up onto the sphere. The 10 real degrees of freedom in a 5D rotation are thus made to correspond with the $10 = 16 - 2 - 4$ real degrees of freedom in 4 quaternions subject to 2 norm constraints and 1 quaternionic constraint.

It is also possible to represent "Lorentz transformations" via complex numbers, quaternions, and octonions ([21] page 147; [169] p.3761, and see our §8.4).

5 Graves, Cayley, Moufang, and the Octonions

Graves then discovered the octonions, also in 1843, and described them in a letter back to Hamilton on 26 December. Arthur Cayley soon rediscovered them and published them as an appendix to other work [55][7], and thus, unfortunately, they are often called the "Cayley numbers."[8]

They are obtained by adjoining *seven* special symbols $i_0, i_1, i_2, i_3, i_4, i_5, i_6$ to the reals[9]. The octonions are then $x = x_\infty + x_0 i_0 + x_1 i_1 + \cdots + x_6 i_6$. The multiplication law for $(i_{m+1}, i_{m+2}, i_{m+4})$ (indices m taken mod 7) is the same as for Hamilton's quaternions (i, j, k). For example, since $-kj = i$, we find by taking $m = 5$ that $-i_1 i_6 = i_5$. Again we define the conjugate $\overline{x}$ of an octonion x by negating all the i_m, and we define the norm $|x|^2 = x\overline{x} = \overline{x}x$ to be the sum of the squares of the x_m for $m \in \{0, 1, 2, 3, 4, 5, 6, \infty\}$.

[5] See §31.1 for information about Rodrigues.

[6] A.Cayley: Philos. Magaz. 7 (1854) and J.f. reine & angew. Math. 50 (1855).

[7] This was bizarre. Cayley's main thrust was to refute a certain Reverend Bronwin, who had pointed out errors in previous Cayley work on elliptic functions. However, Bronwin was right and Cayley wrong and hence this entire paper ultimately was omitted from Cayley's *collected papers*, except for the (completely unrelated) appendix Cayley had tacked on about his discovery of octonions!

[8] See footnote 3. Also, the sum-of-squares formula expressing the multiplicativity of the octonion norm had been found earlier by C.F.Degen in 1818.

[9] This very nice 7-cyclically symmetric presentation of the octonions dates back at least to E.Cartan & J.A.Shouten [53] in 1926.

[10] Also, the nice geometrical properties (correspondence to rotations) of quaternion multiplication are now lost, or at least diluted: Octonion multiplications $x \to ax$ and $x \to xa$, $|a|^2 = 1$, are 8D rotations, but certainly not the most general ones; and $x \to axa^{-1}$ are 7D rotations, since they preserve the subspace $\mathrm{re}x = 0$, but again these certainly are not the most general ones. Because a 7D rotation is described by 21 real degrees of freedom, one might hope that $x \to a(b(cxc^{-1})b^{-1})a^{-1}$ (which for $|a|^2 = |b|^2 = |c|^2 = 1$ also has 21 degrees of freedom) describes a general 7D rotation ($\mathrm{re}x = 0$). But that hope is not true. Similarly because a general 8D rotation is described by 28 real degrees of freedom, one might hope that 4 successive multiplications by unit-norm octonions might describe a general 8D rotation, but that hope too is in vain. (Indeed theorem 8 of section 8.4 of [68] states that a general octonion left-multiplication may be expressed as 7 consecutive octonion right-multiplications, but no fewer.) See our §28 for genuine (albeit comparatively messy) octonionic parameterizations of 7D and 8D rotations without any wasted degrees of freedom.

Again norms are multiplicative: $|ab|^2 = |a|^2|b|^2$. Multiplication is now neither commutative nor, unfortunately[10], associative (e.g. $i_1i_2 \cdot i_3 = i_4i_3 = -i_6 \neq i_6 = i_1i_5 = i_1 \cdot i_2i_3$).

Fortunately octonion multiplication obeys[11] a weakened associativity property, the left and right "alternative" laws

$$xx \cdot y = x \cdot xy, \quad xy \cdot y = x \cdot yy. \tag{7}$$

Thanks to distributivity and $x^{-1} = \overline{x}|x|^{-2}$, these imply and are implied by the (usually more useful) left and right "cancellation" laws

$$y = x^{-1}x \cdot y = x^{-1} \cdot xy, \quad yx \cdot x^{-1} = y \cdot xx^{-1} = y. \tag{8}$$

Because of these laws, the octonions again form a division ring with $c^{-1} = \overline{c}/|c|^2$. (That is, the cancellation laws allow us to divide, i.e. solve $ax = b$ for x, by left-multiplying both sides by a^{-1}; similarly we may solve $xa = b$.)

For other interesting representations of the octonions, see [73][99].

In any Moufang loop ("Moufang's theorem" [181][114]) or in any alternative nnac-ring ("generalized Artin's theorem" – see the first corollary in the appendix of [49]) it is known[12] that:

1. The multiplication is[13]: "flexible"
$$xy \cdot x = x \cdot yx; \tag{9}$$
2. The left and right "Bol laws" [36][160][217][14] hold
$$(x \cdot yx)z = x(y \cdot xz) \qquad \text{(left)}, \tag{10}$$
$$z(xy \cdot x) = (zx \cdot y)x \qquad \text{(right)};$$
3. The left, middle, and right "Moufang laws" hold[15], i.e., respectively:
$$(xy \cdot x)z = x(y \cdot xz) \qquad \text{(left)}, \tag{11}$$
$$x(yz \cdot x) = xy \cdot zx = (x \cdot yz)x \qquad \text{(middle)}, \tag{12}$$
$$(xy \cdot z)y = x(y \cdot zy) \qquad \text{(right)}; \tag{13}$$
4. Reciprocals (whenever they exist) are automatically two sided[16]: $x^{-1}x = xx^{-1} = 1$.
5. Multiplication is "power associative," i.e. x^n has an unambiguous meaning (no matter how one parenthesizes) for every integer $n \geq 0$, and indeed for every integer n of either sign if x^{-1} exists, i.e. the subloop (subring) generated by any *one* element is associative;
6. More generally, alternativity implies (and is implied by) "diassociativity:" the subring (or subloop) generated by any two elements a and b, is associative; and any a, b, c that associate in some order generate an associative subring or subloop. In the octonions, this subalgebra is isomorphic to the quaternions (or, in degenerate cases, to a subalgebra of the quaternions).

The question of just which properties follow from which Moufang or alternative (or other) axioms in loops or nnac-rings is discussed in greater detail in §26.

The octonions also obey *unambiguity of similitude*

$$x^{-1}y \cdot x = x^{-1} \cdot yx, \tag{14}$$

and *anti-automorphism*

$$\overline{a}\overline{b} = \overline{ba} \tag{15}$$

and consequently obey $a^{-1}b^{-1} = (ba)^{-1}$.

6 Moufang-like laws for octonions

Theorem 1 (Moufang-like laws). *If a, x, y are octonions (and $a \neq 0$ if necessary, i.e. in the equations containing a^{-1}), then they obey the following 17 equations (some including multiple equalities). However, in general, no two of these 17 functions are equal.*

$$(x \cdot ya)a^{-1} = xa \cdot a^{-1}y = a(a^{-1}x \cdot y) \tag{16}$$
$$(x \cdot a^{-1}ya)a^{-1} = a(a^{-1}x \cdot a^{-1}y) \tag{17}$$
$$a^{-1}(xa \cdot y) = a^{-1}x \cdot ay \tag{18}$$
$$a(a^{-1}xa \cdot y) = (xa \cdot ya)a^{-1} \tag{19}$$
$$(a^{-1}xa \cdot ya^{-1})a = a^{-1}(xa \cdot y) = (a^{-1}x \cdot ay) \tag{20}$$
$$(ax \cdot ya)a^{-1} = a \cdot xy \tag{21}$$
$$xa \cdot a^{-1}ya = a(a^{-1}x \cdot ya) \tag{22}$$
$$a(xa^{-1} \cdot ya^{-1}) = (axa^{-1} \cdot y)a^{-1} \tag{23}$$
$$a^{-1}(ax \cdot ay) = (x \cdot aya^{-1})a \tag{24}$$
$$a(x \cdot aya^{-1}) = (ax \cdot ay)a^{-1} \tag{25}$$
$$xy \cdot a = a^{-1}(ax \cdot ya) \tag{26}$$
$$xa \cdot ya^{-1} = a(a^{-1}x \cdot aya^{-1}) = (x \cdot ay)a^{-1} \tag{27}$$

[11] Octonion alternativity was conjectured by E.Artin and first shown by Max Zorn [262]. Adem ([5] appendix) gave a slick proof, resembling his other one we mention in footnote 24 of the theorem (originally due to Albert [9]) that the Cayley-Dickson double (see §8.1) of a linear algebra A is alternative if and only if A is associative.

[12] K.Kunen [159] showed that in a *loop ring* in which $1 + 1 \neq 0$ (and hence in its underlying loop) left and right alternativity imply each other. But this is not true in general rings, nor in loops whose loop rings have characteristic 2. Kunen in another paper [160] showed that any quasigroup satisfying any Moufang identity, must be a Moufang loop, i.e. must have a 2-sided identity. Both of Kunen's proofs were discovered with aid from proof-finding computer programs.

[13] Actually, in the presence of the distributive law, any two of the three laws {left-alternativity, right-alternativity, flexibility} implies the third. But this is untrue in a loop.

[14] It was shown by Robinson [217] that *loops* obeying either the left Bol (or the right Bol) identity, are power-associative. Left Bol loops are left-alternative, see figure 26.3.

[15] Any one among Moufang's four = signs suffice ([47] p.115-120, [181]), in a ring or loop, to imply the three others and hence left and right alternativity and cancellation, flexibility, and left and right Bol. Also, a loop is Moufang iff both the left and right Bol laws hold. In a Moufang loop $a^{-1}b^{-1} = (ba)^{-1}$. Different authors disagree on what the precise statements of the "Bol" and "Moufang" identities are. We are following Kunen [160]. Under Kunen's convention, the left and right Bol identities do *not* imply each other in a loop, although they do in a ring. Of course if multiplication is flexible, as it is in the octonions, the distinction between the Bol and Moufang identities vanishes.

[16] To draw this conclusion, left- and right-cancellation alone suffice; flexibility and distributivity are not needed.

$$(xa \cdot ya^{-1})a = x \cdot ay \tag{28}$$
$$(ax \cdot a^{-1}y)a = axa^{-1} \cdot ya \tag{29}$$
$$(ax \cdot ya^{-1})a = axa^{-1} \cdot ay \tag{30}$$
$$(axa^{-1} \cdot a^{-1}ya)a^{-1} = a(xa^{-1} \cdot a^{-1}y) \tag{31}$$
$$a(xa^{-1} \cdot aya^{-1}) = (axa^{-1} \cdot ay)a^{-1} = ax \cdot ya^{-1} \tag{32}$$

Proof: These were established by computer, see §11. Q.E.D.

6.1 Miscellaneous facts about octonions

Theorem 2 (Reflections). *Let* $\text{refl}[\vec{x}]$ *denote the map*

$$\text{refl}[\vec{x}](\vec{t}) \overset{\text{def}}{=} \vec{t} - \frac{2\langle \vec{x}, \vec{t}\rangle}{|\vec{x}|^2}\vec{x} \tag{33}$$

mapping an 8-vector $\vec{t}$ *to its reflection in the hyperplane normal to* $\vec{x}$ *and containing the origin. Let* a *be a unit-norm octonion. Then (viewing octonions as 8-vectors),* $-\text{refl}[a](\overline{y}) = a \cdot ya$*, while* $-\text{refl}[a](y) = \overline{\overline{a}y \cdot \overline{a}} = a \cdot \overline{y}a$.

Proof: [17] In the octonions this may be proven by computer as in §11. More generally: in *Cayley-Dickson algebras* (defined next section) we have

$$2\langle a, b\rangle = a\overline{b} + b\overline{a} = \overline{a}b + \overline{b}a \tag{34}$$

(by EQ 49 with $x = a + b$) so that

$$2a\langle a, b\rangle = a \cdot \overline{a}b + a \cdot \overline{b}a. \tag{35}$$

Hence the reflection law

$$a \cdot \overline{b}a = 2a\langle a, b\rangle - b = -\text{refl}[a](b) \tag{36}$$

has precisely the same validity in the Cayley-Dickson algebras as does the left-cancellation property $a \cdot \overline{a}b = |a|^2 b$. Since left-cancellation holds in the octonions, the second identity in our theorem is proven in the octonions – and the first identity is the same except $\overline{y}$ is used instead of y. (See also the generalization of this in theorem 34.) Q.E.D.

Remark. Here are 5 important special cases of theorem 2 (in all cases $|t| = 1$):

$$\text{refl}[t](0) = 0, \quad \text{refl}[t](t) = -t, \quad \text{refl}[1](y) = -\overline{y}, \tag{37}$$
$$\text{refl}[t](1) = -t^2, \quad \text{refl}[t](\overline{t}) = -t^3. \tag{38}$$

Theorem 3 (Companions). *Let* $T(z)$ *be an* $SO(8)$ *transformation of the octonion (regarded as an 8-vector)* z*. Then there exist unique (up to an overall sign change) unit-norm octonions* a, b *such that* $T(xy) = T(x)a \cdot bT(y)$.

Proof: This is shown in sections 8.1 and 8.7 of [68]. Conway and D.Smith call a and b the "companions" of T. Q.E.D.

7 Famous Impossibility theorems

Over the 100-year period 1880-1980, a great number of theorems were shown, all demonstrating in some way the uniqueness of the reals, complexes, quaternions, and octonions. Important contributors to this battle include Frobenius, Hurwitz, Radon, Bruck, Albert, Kaplansky, Kleinfeld, Zorn, Wright, and Skornyakov (algebraicists) and Hopf, Adams, Bott, Kervaire, and Milnor (topologists). Here is a list (surveys=[94][147][225][259]):

Theorem 4 (6 Famous Impossibility theorems). *The following 6 theorems hold.*

1. There are exactly 4 nnac-algebras with unit element 1 over the real numbers which have a multiplicative, non-negative-real valued, norm, namely: the reals, complexes, quaternions and octonions [94][134][147].

   • The demand that there be a unit element 1 may be replaced [101] by demanding power-associativity for powers ≤ 4.

   • Even if the demand for a unit element is dropped, then dimensions 1,2,4,8 are still the only possibilities, but [10][94] certain other algebras (which are related by orthogonal transformations to the quaternions and octonions) become available in dimensions 4 and 8. Some of these [14] have only a left-identity and some do not even have a 1-sided identity (nor do they have 2-sided inverses)[18].
2. These are also the only finite dimensional alternative (EQ 7) nnac division algebras over the reals [49][263].

   • This is still true if the word "alternative" is replaced by the weaker word "right-alternative," and also [12] even if the word "division" is replaced by the word "semisimple[19]."

   • E.K.Loginov [168] claims to have shown that any simply connected analytic Moufang loop must be embedded in the invertible elements of an alternative algebra over $\mathbb{R}$. If this is accepted then the only such loop (besides groups) with spherical topology is the unit-norm octonions.

   • The flexible division algebras over the reals have been classified [28] and have dimensions $1, 2, 4, 8$ only.

[17] This theorem was mentioned in §6.6 of [68], however their theorem statement was incorrect – their two reflections were performed in the wrong order and they forgot to negate.

[18] I. Kaplansky [148] analyses arbitrary dimensional (including infinite dimensional) algebras A, over arbitrary fields F, such that A has a quadratic, multiplicative norm. He claims (theorem page 957) that if the norm is "nonsingular," then:
(a) A is alternative.
(b) A has dimension$\in \{1, 2, 4, 8\}$, *or* $\text{char}F = 2$ and A is a "purely inseparable field over F."
(c) A is simple, *or* A is $F \oplus F$ (direct sum).
(d) The norm is $\overline{x}x$ where $\overline{x}$ is an involution.

Unfortunately, over GF_2 the *Euclidean* norm is "singular," since $|x + y|^2 - |x|^2 - |y|^2 \equiv 0 \bmod 2$, so that Kaplansky's results are not of interest to us. If we insist on using the Euclidean norm over GF_2, counterexamples to Kaplansky's theorem result: Let $F = GF_2$ and let A be n-dimensional (for any n). Define the multiplication as follows: The product of the binary n-bit word with a 1 in position j, times the binary n-bit word with a 1 in position k, is w_{jk}, where the w_{jk} are any binary words, with odd parity, we please. (We can cause 1 to exist by making $w_{0k} = w_{k0} = e_k$.) This algebra has multiplicative Euclidean norm (which is just the parity of the number of 1-bits). However, it is in general *not* a field, *not* alternative, *not* simple, and *not* $GF_2 \oplus GF_2$, and there is *not* any suitable involution $\overline{x}$. Also, see the theorem in §31.2, where we construct unital algebras A over any field F with $\text{char}F = 2$, of any dimension $n = \dim A$ with $n \bmod 6 \in \{2, 4\}$. These A are much more to Kaplansky's liking since they *are* alternative and commutative. However, they still violate his theorem since they are not fields, since the multiplication is, in general, non-associative. We conclude that n-dimensional composition algebras over GF_2 exist for every dimension n.

[19] "Simple" means: has no nontrivial ideals. "Semisimple" means has no nilpotent ideals besides $\{0\}$.

3. Any nnac *division* algebra over the reals, or indeed, any continuous map from $S^{n-1} \times S^{n-1} \to S^{n-1}$ with a 2-sided identity, is 1, 2, 4 or 8 dimensional [1][2]. (Warning [81][191][28]: other 8-dimensional division algebras over the reals exist besides the octonions; and division algebras over fields F with $F \neq \mathbb{R}$ exist with dimension$\notin \{1, 2, 4, 8\}$.)
4. Definition [98]: a vector "cross product" $\vec{a} \times \vec{b} \in \mathbb{R}^n$ for $\vec{a}, \vec{b} \in \mathbb{R}^n$ obeys
orthogonality:
$$\langle \vec{a} \times \vec{b}, a\rangle = \langle \vec{a} \times \vec{b}, b\rangle = 0 \quad (39)$$
and **length=area relation:**
$$|\vec{a} \times \vec{b}|^2 = |\vec{a}|^2|\vec{b}|^2 - \langle \vec{a}, \vec{b}\rangle^2 = \det \begin{pmatrix} \langle \vec{a}, \vec{a}\rangle & \langle \vec{a}, \vec{b}\rangle \\ \langle \vec{b}, \vec{a}\rangle & \langle \vec{b}, \vec{b}\rangle \end{pmatrix} \quad (40)$$
Then: A bilinear vector product exists in $\mathbb{R}^n$ iff $n = 3$ or $n = 7$.
• The word "bilinear" may be replaced by "continuous" in this theorem [97][98]. See also [179].
5. There are exactly four "real homogeneous algebras" over $\mathbb{R}$ (i.e. algebras with an automorphism group transitive on 1D subspaces, i.e. that allows mapping any nonzero vector to any other up to a proportionality) namely [84]:
   (a) $\mathbb{R}$ itself,
   (b) the pure imaginary quaternions with truncated (or equivalently Lie) multiplication (i.e. 3-vectors under cross product),
   (c) pure imaginary octonions with truncated (or equivalently Lie) multiplication (the 7D vector cross product), and
   (d) $\mathbb{C}^3$ under 3-vector cross product of the complex-conjugated 3-vectors, i.e. the pure-imaginary biquaternions[20] under Lie (or equivalently truncated) multiplication.
6. Any sum-of-squares identity (over any field F with char$F \neq 2$)
$$(\sum_{j=1}^{n} x_j^2)(\sum_{k=1}^{n} y_k^2) = (\sum_{\ell=1}^{n} z_\ell^2), \quad (41)$$
where the z_ℓ are given *bilinear* functions of the x_j and y_k, must have $n \in \{1, 2, 4, 8\}$ and must be the same (up to orthogonal linear transformations) as the norm-multiplicativity identity for the reals, complexes, quaternions, and octonions (A.Hurwitz's theorem [147][134]; see also claim 10 in our proof of our theorem 60). If EQ 41 holds over F, and -1 is not a sum of n squares in F, and if the z_ℓ are *rational* functions of the x_j and y_k over F, then n must[21] be a power of 2.
• An immediate corollary is: If the z_ℓ are rational functions of the x_j and y_k such that EQ 41 is valid over $\mathbb{R}$, then n is a power of 2.
• The analogous power-of-2-only theorem is *not* true over the *complex* numbers (nor in any field in which a sum of nonzero squares can be zero), because one may always add k more squares whose sum is 0 (e.g. the kth roots of unity) on to every sum, for any $k \geq 2$.

Remark (Polynomials impossible). Unless $n \in \{1, 2, 4, 8\}$, sum of squares identities (EQ 41) are impossible with the z_ℓ defined by *polynomial* maps $S^{n-1} \times S^{n-1} \to S^{n-1}$; if the maps feature a 2-sided identity element "1." (Proof: Use Adams' results about smooth maps mentioned in part 3 of impossibility theorem 4. Second proof: if the z_ℓ are *polynomial* functions of the x_j and y_k, then they must in fact be *bilinear* functions, as may be seen by considering fully expanding both sides into monomials and matching the coefficients of the terms of highest degree.) Thus this monograph's decision to resort to *rational* maps in §9 was necessary.

• *Hurwitz's problem* [134] asks: What is the least integer $n = n(r, s)$ so that a sum of squares identity
$$(x_1^2 + \cdots + x_r^2)(y_1^2 + \cdots + y_s^2) = (z_1^2 + \cdots + z_n^2) \quad (42)$$
exists where the z_k are polynomial (and hence bilinear) functions of the x_i and y_j? It is known that $n(r, s)$ is always finite: indeed Hurwitz [135] and Radon [210] in their original papers had independently shown that the largest r such that $n(n, r) = n = u2^{4\alpha+\beta}$ with $0 \leq \alpha$, $0 \leq \beta \leq 3$, u odd, is
$$r = 8\alpha + 2^\beta. \quad (43)$$
Many later authors (cited in [234]) showed how to achieve the Hurwitz-Radon bound (EQ 43) with all-integer constructions in which all the coefficients in the bilinear forms are elements of $\{-1, 0, +1\}$. Many of these constructions arise from modifications and/or dimensional restrictions of the Cayley-Dickson multiplication formula we shall discuss in §8.1. If the polynomials $z_k(\vec{x}, \vec{y})$ are required to have *real* coefficients, then [163] if $\min\{r, s\} \leq 9$ the answer is defined recursively by
$$n(1, s) = s, \quad n(r, s) = n(s, r), \quad (44)$$
$$n(r, s) = 2^t \text{ if } 2^{t-1} < r, s \leq 2^t \quad (45)$$
and
$$n(r, s) = 2^t + n(r, s - 2^t) \text{ if } r \leq 2^t < s. \quad (46)$$

[20] See the discussion of "bions" in §8; our new 2^n-ons also have "bi" versions, discussed in §9.

[21] The theory behind this is primarily due to A.Pfister [199][211]. D.B.Shapiro remarks: "This statement immediately follows from the Cassels-Pfister Subform Theorem, as stated in Corollary A.2 on page 167 of my book [231]. The hypothesis of the theorem becomes statement (3) in that Corollary, where φ is the 'sum of n squares' quadratic form. That Corollary implies that φ is a Pfister form, which in this case is equivalent to saying that n is a 2-power.

The proof of the Subform Theorem and Corollary are not included in my book. They can be extracted from the earlier literature... I believe T.Y. Lam was the first to observe the Corollary in this form, and it was first stated in this nice way in my survey [232]." Q.E.D.

I also remark that there is an extremely simple proof by A.M.Legendre and B.L.van der Waerden that satisfying EQ 41 in the rationals is impossible when $n = 3$ (with the z_ℓ rational functions of the x_j's and y_k's), based on the fact that $3 = 1 + 1 + 1$ and $21 = 4^2 + 2^2 + 1$ are the sums of three squares, but $63 = 3 \cdot 21$ is not.

If the polynomials are required to have *integer* coefficients, then it is known [234] that the $n(r,s)$ given by the recurrence in EQ 44-46 yields a lower bound on the true $n(r,s)$ for *all* r,s (but it is only known to be tight when $\min\{r,s\} \le 9$), and table 7.1 gives the answer when $10 \le r,s \le 16$. Lam and Yiu conjectured that restricting to integer coefficients has no effect – i.e. the same $n(r,s)$ always result as in the case of real coefficients. That conjecture is known to be true when $\min\{r,s\} \le 9$, and all known upper bound records have been achieved via all-integer constructions.

$r\backslash s$	10	11	12	13	14	15	16
10	16	26	26	27	27	28	28
11	26	26	26	28	28	30	30
12	26	26	26	28	30	32	32
13	27	28	28	28	32	32	32
14	27	28	30	32	32	32	32
15	28	30	32	32	32	32	32
16	28	30	32	32	32	32	32

Figure 7.1. [163] The least possible number $n(r,s)$ of squares on right hand side of sum of squares identity EQ 42 where the z_k are polynomials in the x_i and y_j's with *integer* coefficients. [Additional upper bound constructions are given in [5][234], including $n(32,32) \le 116$.]

These impossibility theorems had widely been thought to "close the book" on our subject. However, we shall see that the book has at least one more chapter. Here is what happens to these 6 impossibility theorems:

1. We get nnacd-algebras of dimension 2^n (for *all* $n \ge 0$) with 1 and with multiplicative euclidean norm; and *only* dimensions 2^n are possible (for algebra definitions built of rational functions).
2. When $n \ge 4$ these are no longer alternative nor flexible. Indeed alternativity is *impossible* (for algebra definitions built of rational functions).
3. There are several possible definitions of "division" nnacd-algebras; under the weakest definition (no zero-divisors) all of ours are division algebras, but under the strongest (unique existence of solutions to any division problem), only the ones with $n \le 4$ are (and in the case $n = 4$, only under genericity assumptions).
4. We get a vector product in every dimension $2^n - 1$, $n \ge 1$. It is rational and (hence) discontinuous. Dimensions not of the form $2^n - 1$ are impossible (for vector products built of rational functions).
5. None of our new constructions are "homogeneous."
6. Our norm-multiplicativity identities are of the form EQ 41 for each $n = 2^m$ for each $m \ge 0$, with the z_ℓ being *rational* functions of the x_j's and y_k's.

8 Cayley, Dickson, sedenions, and bi"ons"

8.1 Cayley-Dickson doubling

The complexes, quaternions, and octonions may be constructed successively, starting from the reals, by a process called "Cayley-Dickson doubling" [81][80][79][227][147].

We start from some ring R which already has, predefined, a commutative and associative addition, a two sided identity "1," a nnac multiplication, and a self-inverse (i.e. $\overline{\overline{x}} = x$) R-linear ($\overline{x \pm y} = \overline{x} \pm \overline{y}$) anti-automorphic ($\overline{ab} = \overline{b}\,\overline{a}$) operation, called "conjugation," denoted by overlining: $x \to \overline{x}$. We now make a new ring, whose elements are *2-tuples* from the old ring, by defining tuple-addition as the usual elementwise addition, conjugation as

$$\overline{(a,b)} = (\overline{a}, -b), \tag{47}$$

and tuple-multiplication as

$$(a,\, b)\,(c,\, d) \;=\; (ac - d\overline{b},\; \overline{a}d + cb). \tag{48}$$

This is the **Cayley-Dickson doubling formula.** In the usual case, the initial ring is the real numbers with simply $\overline{x} = x$, and then we get, successively, the complexes, quaternions[22], and octonions. After the tth doubling, we get an algebra of dimension 2^t over R. We call these the *Cayley-Dickson algebras.* They keep going forever. It is tempting, but, we shall argue, *wrong*, to believe that the Cayley-Dickson doubling process is the "natural" one which keeps generating the "best possible" 2^t-dimensional algebras. In fact, we shall propose (EQ 68) a different and better doubling process.

8.2 The Sedenions

But for those who succumb to temptation, the next (16 dimensional) Cayley-Dickson algebra is called the sedenions. (Mnemonic: "CDions," for *C*ayley and *D*ickson.) Unfortunately, the sedenions (and all their successors) both have zero-divisors and hence do *not* have a multiplicative norm (see EQ 56), and have non-alternative and non-commutative multiplication. Sedenion multiplication still has the saving grace that it is power associative. (Proof: the powers of a sedenion are generated by *two* octonions, which, by Artin's theorem [cf. §5], necessarily generate a diassociative subalgebra. For other proofs see [226] and theorems 19 and 20.) The non-invertible sedenions are a measure-0 subset of the sedenions.

8.3 Properties of Cayley-Dickson algebras

All Cayley-Dickson algebras are "quadratic," i.e. obey

$$x^2 - 2\mathrm{re}(x)x + |x|^2 = 0 \tag{49}$$

([225] page 50) and "central simple," indeed

[22] Warning: Although representing 2^n-ons as ordered pairs (a,b) of 2^{n-1}-ons has the virtue of not introducing a ceaseless stream of new special $\sqrt{-1}$ symbols, it unfortunately risks creating the *wrong* impression that $a + ib = a + bi$, where i is the new $\sqrt{-1}$ symbol. (This is false for the octonions and their successors.) This monograph sticks to the "eyes left" convention $(a,b) = a + ib$. To convert between the two conventions for octonions, use $ix = \overline{x}i$, or more generally see (EQ 98). We also warn the reader that Cayley-Dickson doubling produces a different basis for the octonions than the "pretty" basis we gave in §5. The two are readily interconverted by merely reordering the basis elements: in the "pretty" basis the basic quaternions (i,j,k) are (i_1,i_2,i_4) and $i_0 i_n = i_{3n}$ where $n \in \{1,2,4\}$ and indices are mod 7. In the Cayley-Dickson basis (i,j,k) is (i_1,i_2,i_3) and $i_4 i_n = i_{n+4}$ where $n \in \{1,2,3\}$.

Theorem 5 (Centers of Cayley-Dickson algebras). **Commutative center:** *$rx = xr$ for all quaternions x, iff r is real. This is also true in every Cayley-Dickson 2^n-on linear algebra for each $n \ge 2$. (But for $n \le 1$, the whole algebra is commutative.)*
Associative center: *If $x \cdot ry = xr \cdot y$ for all octonions x, y, then r is real. This is also true in every Cayley-Dickson 2^n-on linear algebra for each $n \ge 3$. (But for $n \le 2$, the whole algebra is associative.)*

Proof: [23] Claim 1 is a consequence of Schafer's theorem ([225] page 50) that the Cayley-Dickson algebras are central simple. Claim 2, in the octonions, is theorem 1 in section 8.1 of [68], and a proof of it for $n > 3$, by induction on n, is lemma 1.1 of [92]. Q.E.D.

Corollary 6 (Centers of 2^n-ons). *The same is true with our 2^n-ons instead of the Cayley-Dickson algebras.*

Proof: We have not yet defined the 2^n-ons, but all that is needed for the present purpose are the facts that $xr = rx$ and and $x \cdot ry = xr \cdot y$ for real r if x, y are 2^n-ons, and the fact that the 2^n-ons contain the quaternions (if $n \ge 2$) and the octonions (if $n \ge 3$) as subalgebras. Q.E.D.

The Cayley-Dicksons all obey both the flexible identity $xy \cdot x = x \cdot yx$ [226][24]and the "Jordan identity" $xy \cdot x^2 = x \cdot yx^2$, i.e., the noncommutative ones are "non-commutative Jordan algebras" in the terminology of Schafer ([225] page 141); see [9][45][226]. Therefore *all* the Cayley-Dickson algebras are strictly power-associative, since all non-commutative Jordan algebras are ([227] page 141). In fact every multilinear identity of degree≤ 5 which is obeyed in the sedenions [41][125] also is obeyed in every flexible quadratic algebra, in particular in every higher Cayley-Dickson algebra. Thus in this sense, the Cayley-Dickson algebras "stop getting worse" once we reach the sedenions.

Although the Cayley-Dickson algebras no longer have a multiplicative norm when $n \ge 4$, and no longer are commutative when $n \ge 2$, they nevertheless obey

Lemma 7 (Weakened norm-multiplicativity/ commutativity property). *If x and y are elements of a Cayley-Dickson algebra, then*

$$|xy| = |yx|. \tag{50}$$

Proof: This is the third equation of lemma 1.4.2 of [149]. Q.E.D.

We have not seen previously, so we prove it ourselves:

Theorem 8 (Cayley-Dickson antiautomorphism). *All the* Cayley-Dickson *2^n-dimensional algebras enjoy the anti-automorphism identity $\overline{t}\,\overline{y} = \overline{yt}$.*
Proof by induction on n: Obviously it is true when $n = 0$. Doubling via EQ 48 yields

$$\overline{(a, b)}\;\overline{(c, d)} = (\overline{a}, -b)(\overline{c}, -d) = (\overline{ac} - d\overline{b},\ -ad - \overline{c}b) \tag{51}$$

whereas by the inductive hypothesis and EQ 47

$$\overline{(c, d)(a, b)} = \overline{(ca - b\overline{d}, \overline{c}b + ad)} = (\overline{ac} - d\overline{b},\ -ad - \overline{c}b). \tag{52}$$

Q.E.D.

8.4 The "bi-ons"

If, instead of starting our successive doublings from the real field, we begin it from the *complex* field (but now regarding the Cayley-Dickson conjugate $\overline{z}$ of a complex number as z *itself*), then we get, successively, the "bi-complex numbers," the "biquaternions," the "bioctonions," the "bisedenions," and so on.

Notation: It is useful to introduce the new symbol $I = \sqrt{-1} \ne i, j, k$ to be the $\sqrt{-1}$ from the underlying complex field, which is different from the $\sqrt{-1}$ symbols arising in Cayley-Dickson doubling. Also, the operation of negating I (complex conjugation) is best denoted $x \to x^*$ to distinguish it from the usual Cayley-Dickson conjugation $x \to \overline{x}$. These two kinds of conjugation commute.

The bi-ons are slightly less attractive than their non-bi cousins. They have the same commutativity and associativity properties as their non-bi cousins (e.g., the bioctonions are noncommutative, alternative, and nonassociative; the bisedenions are power-associative, all of the bi's are flexible, etc.) and obey the same polynomial identities. And in the 2, 4, and 8 complex-dimensional cases we still have a multiplicative norm $|q|^2$, which now, however, is a complex rather than real number. But none of the bi-ons are division algebras, because an inverse $q^{-1} = \overline{q}/|q|^2$ might not exist, even if $q \ne 0$, because the norm $|q|^2$, which now is the sum of squares of 2^k *complex* numbers, $k \ge 1$, can be zero even if those numbers are nonzero, e.g. $1^2 + I^2 = 0$. Nevertheless, the set of q with $|q|^2 = 0$ always has measure zero in complex 2^k-space, so that inversion *usually* remains possible.

As was arguably realized by C.F.Gauss before Hamilton's discovery of the quaternions, the biquaternions are isomorphic to the 2×2 complex matrices $\mathbb{C}^{2\times 2}$ and their norm is simply the determinant; the isomorphism is

$$a + ib + jc + kd \approx \begin{pmatrix} a + ib & -c - id \\ c - id & a - ib \end{pmatrix}. \tag{53}$$

Price [208] gives much of the credit for the invention and early development of the bicomplex numbers to Corrado Segre (1860-1924). Segre ([230]; [208] p.vi) noted

Theorem 9 (Segre). *The bicomplex numbers are algebraically isomorphic to $\mathbb{C} \oplus \mathbb{C}$.*

[23] These are also proven as lemmas 1.4.3 and 1.4.4 of [149].

[24] A sketch of a different, and simpler, proof of flexibility: $\langle ab \cdot a - a \cdot ba, 1\rangle = \langle ab, \overline{a}\rangle - \langle ba, \overline{a}\rangle = \langle b, \overline{a}^2\rangle - \langle b, \overline{a}^2\rangle = 0$ so $ab \cdot a - a \cdot ba$ must be pure-imaginary. But, with the aid of our theorem 8, its conjugate may easily be seen to be equal to it, so it must be 0. Q.E.D. Yet another simple proof (by induction on n) is lemma 4.3.3 of [149]. Still another slick proof, due to Adem ([5] appendix) proves that *the Cayley-Dickson-double of a linear algebra A is flexible if and only if A is itself flexible.* The "only if" direction is trivial (since A is a subalgebra). The "if" part relies on the facts that (using the associator notation of EQ 197) (1) in any flexible algebra $(x, y, z) + (z, y, x) = 0$ ([225] p.28), and (2) within the Cayley-Dickson double of an algebra A, the identity $(x, y, x) = ((a, b, a) - (a, \beta, \alpha) - (\alpha, \beta, a) + (b, \alpha, \alpha) + (\alpha, \alpha, b); 0)$ holds where $x = (a; \alpha)$ and $y = (b; \beta)$ and where we have written elements of the doubled algebra as 2-tuples $(p; q)$ from A. From these Adem concludes that $(x, y, x) = 0$, proving flexibility of the doubled algebra.

Proof: A bicomplex number $x_1 + i_1x_2 + i_2x_3 + i_1i_2x_4$ (for two commuting $\sqrt{-1}$ symbols i_1 and i_2) may be written in the form $Aj + Bk$ where $j = (1+i_1i_2)/2$ and $k = (1-i_1i_2)/2$ obey $j^2 = j$, $k^2 = k$, and $jk = kj = 0$, where A,B are complex numbers that are real-linear combinations of 1 and i_1: $A = x_1 - x_4 + (x_2 + x_3)i_1$, $B = x_1 + x_4 + (x_2 - x_3)i_1$. Thus re-expressing the bicomplex numbers in Segre's basis makes it obvious they really are just $\mathbb{C} \oplus \mathbb{C}$, i.e. they are 2-tuples of complex numbers added and multiplied componentwise. Q.E.D.

As we have described in EQs 5-6, quaternions are very useful for representing 3D and 4D *rotations*. The biquaternionic analogue is the representation of $(3 + 1)$-dimensional *Lorentz transformations* via

$$q \to LqL^*, \quad L = \exp(I\frac{b}{2})\exp(\frac{r}{2}). \tag{54}$$

Here q is a special relativity[25] 4-vector $q = t + ix + jy + kz$, and the Lorentz transformation is the product of a *boost* $b = b_xi + b_yj + b_zk$ with a speed of $\tanh|\vec{b}|$, times a 3D rotation (as in EQ 5) through angle $\theta = |\vec{r}|$ radians with axis in the same direction as $r = r_xi + r_yj + r_zk$. Lorentz transformations applied to ordinary quaternions q (i.e. ones not involving I) preserve the absence of I and preserve the quaternionic norm $|q|$.

8.5 Nicest sedenion representation, and the zero-divisors

The nicest representation of[26] the sedenions probably is as follows. (This seems to be new, although similar-appearing representations have been exhibited before.)

Consider the following 35 triples from the 15-element set $\{\infty, 0^+, 1^+, 2^+, \dots, 6^+, 0^-, 1^-, 2^-, \dots, 6^-\}$:

$$\begin{gathered}(\infty, 0^+, 0^-), \quad (1^+, 2^+, 4^+), \\ (5^+, 6^-, 1^-), \quad (3^+, 5^-, 2^-), \quad (6^+, 3^-, 4^-)\end{gathered} \tag{55}$$

where all numbers are taken mod 7, so that each triple here really leads to 7 such triples, so these "5" triples are really 35. For example, the first triple shown leads to $(\infty, 1^+, 1^-)$, and the last triple shown leads to $(0^+, 4^-, 5^-)$, if we add 1 mod 7 to every number in them[27]. Amazing properties: if every number in every triple is *doubled* mod 7, the result is still the same design (with some triples cyclically shifted, but never order-reversed). Also note that $1, 2, 4$ are the nonzero squares, and $3, 5, 6$ are the nonsquares, mod 7.

Let the 15 special $\sqrt{-1}$ symbols, adjoined to the reals to create the sedenions, be called $s_\infty, s_0^\pm, s_1^\pm, \dots, s_6^\pm$. Now if (a, b, c) is one of our 35 magic triples, then regard the multiplication laws for (s_a, s_b, s_c) as the same as for the quaternions (i, j, k). Example: since $ji = -k$ we have from the triple $(5^+, 1^-, 6^-)$ that $s_1^- s_5^+ = -s_6^-$.

Note that the triple $(1^+, 2^+, 4^+)$ (in its 7 incarnations) *alone* suffices to generate the octonions (see §5) with basis $(1, s_0^+, s_1^+, \dots, s_6^+)$. On the other hand, $(\infty, 0^+, 0^-)$ merely yields 7 different quaternion subalgebras and does not alone yield any octonions. Each of the other 3 basic triples, e.g. $(5^+, 6^-, 1^-)$, acting alone yields nothing.

An example of zero-division in these sedenions is

$$(s_0^+ + s_1^-)(s_1^+ + s_0^-) = 0. \tag{56}$$

Indeed, Khalil & Yiu ([149] prop. 3.2.1, following [93]) showed

Lemma 10 (The zero divisions in the sedenions). *Octonion-pairs (a, b) regarded as sedenions (now* not *in our nice symmetric basis but rather in the usual Cayley-Dickson basis where the first 8 coordinates form an octonion subalgebra) are zero-divisors iff a and b obey $|a| = |b|$ and $\mathrm{re}\, a = \mathrm{re}\, b = \langle a, b\rangle = 0$.*

9 The new doubling process

The core idea behind our new construction is extremely simple. It is based on the observation that multiplying a real orthogonal matrix times a real vector preserves its Euclidean norm. Our plan to multiply 2^n-tuples w and x to get $z = wx$ is: Generate a $|w|$-scaled orthogonal matrix $M(w)$, then take $z = M(w)x$.

Consider[28] the following block matrix, made of four $n \times n$ blocks:

$$\boxed{M = \begin{pmatrix} A & -KBK \\ KB^TK & KB^TKA^TKB^{-T}K \end{pmatrix}}. \tag{57}$$

Here $K \overset{\text{def}}{=} \mathrm{diag}(1, -1, -1, \dots, -1, -1)$ is an $n \times n$ matrix obeying $K^T = K^{-1} = K^H = K$. If B is non-invertible, then we agree to use

$$M = \begin{pmatrix} A & -KBK \\ KB^TK & A^T \end{pmatrix} \tag{58}$$

instead of EQ 57.

Lemma 11 (Orthogonality). *If A is $|a|$ times an orthogonal matrix with determinant $+1$, and B is $|b|$ times an orthogonal matrix with determinant $+1$, then M in EQ 57 is $\sqrt{|a|^2 + |b|^2}$ times an orthogonal matrix with determinant $+1$.*

Proof: Simply multiply out $MM^T =$

$$\begin{bmatrix} A & -KBK \\ KB^TK & KB^TKA^TKB^{-T}K \end{bmatrix} \begin{bmatrix} A^T & KBK \\ -KB^TK & KB^{-1}KAKBK \end{bmatrix}$$

$$= \begin{pmatrix} (|a|^2 + |b|^2)I & 0 \\ 0 & (|a|^2 + |b|^2)I \end{pmatrix}. \tag{59}$$

The top-left diagonal block is $AA^T + BB^T = (|a|^2 + |b|^2)I$, and so is the bottom-left block. The top-right block is $AKBK - KBKKB^{-1}KAKBK = AKBK - AKBK = 0$.

[25] We employ units with lightspeed= 1.

[26] See footnote 3.

[27] The triples in EQ 55 form a solution to the famous "Kirkman schoolgirl problem." See §31.2 for information about Kirkman.

[28] There are 4 obvious variants of this Construction, which are shown in §27 to be inequivalent. Our choice (EQ 57) seems nicest.

So it works. In the particular case of non-invertible B, which happens iff $b = 0$, we have

$$M = \begin{pmatrix} A & 0 \\ 0 & A^T \end{pmatrix} \tag{60}$$

and $M^T M = |a|^2 I$ is even more trivial. The *scaled-orthogonality* claim is now proven, and we need only to prove the claim about positivity of the determinant.

The determinant of a real orthogonal matrix is necessarily ± 1. We reduce M to 2×2 block diagonal form via row operations:

$$\begin{aligned} \det(M) &= \det\left(AA^T + AKB^TKA^{-1}KBK\right) \\ &= \det\left(|a|^2 I + |b|^2 A[KBK]^{-1}A^{-1}[KBK]\right) \end{aligned} \tag{61}$$

Now note that the eigenvalues λ of the matrix in this lattermost determinant, all are of the form $\lambda = |a|^2 + |b|^2 r$ where r is a complex root of unity, and where each r is necessarily either real or a member of a complex-conjugate pair (both of whose members are represented). This makes it evident that if $|a|^2 > 2|b|^2$ then the product of all these eigenvalues must be a positive real, since all the terms in the product (once we agglomerate complex conjugate pairs) are. Hence it must (if M is scaled by $(|a|^2 + |b|^2)^{-1}$ to make it be orthogonal) be $+1$. (This of course is especially obvious in the case $|a| = 1$ and $|b| = 0$ when we just have $\det I = 1$.) Now note that the determinant of a matrix is a continuous function of its entries. Hence there is no way for it to jump from $+1$ to -1 as we smoothly move $(|a|^2, |b|^2)$ from $(1, 0)$ to whatever we want their final values to be. The positivity of the determinant is now proven. Q.E.D.

Doubling in action. We may begin with 1×1 real matrices $M(a) = a$ to get the algebra of real numbers. After doubling via EQ 57, we get the **complex** numbers (as 2-tuples of reals) via

$$M(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \tag{62}$$

These 2×2 real matrices are, in fact, a faithful representation of the complex numbers, i.e. $M(x)M(y) = M(xy)$, $M(x \pm y) = M(x) \pm M(y)$, etc. Also note that $M(\overline{z}) = M(z)^T$, $M(z^{-1}) = M(z)^{-1}$, and $\det M(z) = |z|^2 \geq 0$.

A second doubling yields the **quaternions** as 4-tuples of real numbers. In this particular case (because K commutes with our matrices M when both are 2×2), we could, alternatively, begin with 1×1 complex matrices $M(a) = a$ to get the algebra of complex numbers. After doubling, we would get the quaternions (as 2-tuples of complex numbers) via

$$M_c(a + jb) = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}. \tag{63}$$

These 2×2 complex matrices are, in fact, a faithful representation of the quaternions, i.e. $M_c(x)M_c(y) = M_c(xy)$, $M_c(x \pm y) = M_c(x) \pm M_c(y)$, etc. Also note that $M_c(\overline{q}) = M_c(q)^H$, $M_c(q^{-1}) = M_c(q)^{-1}$, and $\det M_c(q) = |q|^2$. If we instead adopt our usual procedure, we instead get 4×4 real matrices, which also faithfully represent the quaternions, and which obey $M(\overline{q}) = M(q)^T$, $M(q^{-1}) = M(q)^{-1}$, and $\det M(q) = |q|^4$.

After another doubling, we get[29] the **octonions** (as 2-tuples of quaternions, which we view as 8-tuples of real numbers) via

$$M(a, b) = \begin{pmatrix} A & -KBK \\ KB^TK & KB^TKA^TKB^{-T}K \end{pmatrix} \tag{64}$$

where A and B are respectively the 4×4 real matrices representing quaternions a and b. These matrices are the left-representation of the octonions. For much information about the 4×4 matrices representing the quaternions and the 8×8 left and right matrix representations of the octonions, see Tian [244][30].

These are *not* faithful, i.e. $M(x)M(y) \neq M(xy)$ in general, and could not have been, since matrix multiplication is associative while octonion multiplication isn't. These matrices obey

$$\begin{gathered} M(\overline{z})z = (|z|^2, 0, 0, \ldots, 0)^T, \quad M(\overline{z}) = M(z)^T, \\ M(z^{-1}) = M(z)^{-1} = |z|^{-2} M(z)^T, \quad Kz = \overline{z}, \\ M(a)x = ax, \quad M(s + ta) = sI + tM(a) \end{gathered} \tag{65}$$

if s and t are scalar. Indeed

Theorem 12 (M properties). *The properties in EQ 65 continue to hold forever as we continue doubling to reach the "2^n-ons," for all $n \geq 0$.*

Proof: Easy, by induction with the aid of $\overline{(a, b)} = (\overline{a}, -b)$, the properties $X^T Y^T = (YX)^T$ and $X^{-1}Y^{-1} = (YX)^{-1}$ of matrices, the fact that $M^T = M^{-1}$ if M is an orthogonal matrix, and the fact that EQ 65 all are trivially verifiable for the 2^n-ons when $n \leq 3$.

For example, to prove $M(\overline{z}) = M(z)^T$, we have

$$M(a, b)^T = \begin{pmatrix} A^T & KBK \\ -KB^TK & KB^{-1}KAKBK \end{pmatrix} \tag{66}$$

by using $(XY)^T = Y^T X^T$ and $K^T = K$ as necessary (note the upper-right and lower-left entries of the matrix in EQ 57 were swapped *and* transposed in the process of transposing it, which happens here to have the same effect as simply negating them both). Now (since $B^{-1} = B^T$ by orthogonality) this is plainly the same thing as

$$M(\overline{a}, -b) = \begin{pmatrix} A^T & KBK \\ -KB^TK & KB^TKAKB^{-T}K \end{pmatrix}. \tag{67}$$

We have used the inductive assumption to justify replacing the A's in EQ 57 by A^T and the B's of course by $-B$. We

[29] Note: these octonions are is *not* the same basis as the nice basis in §5; see footnote 3.

[30] If $L(x)$ and $R(x)$ are the left and right real matrix representations of an octonion x, then $L(x)^T K = KR(x)$ where $K = \text{diag}(1, -1, -1, -1, -1, -1, -1, -1)$; $\det L(x) = \det R(x) = |x|^8$; $\text{trace} L(x) = 8\,\text{re}\,x$; $L(x)^2 = L(x^2)$; $L(x^{-1}) = L(x)^{-1}$; $L(\overline{x}) = L(x)^T$; $L(x)R(x) = R(x)L(x)$; $L(x)L(y)L(x) = L(xyx)$; $L(xy + yx) = L(x)L(y) + L(y)L(x)$; and $L(xy) = L(x)L(y) + L(x)R(y) - R(y)L(x) = R(x)[L(x)L(y)]R(x)^{-1}$. The eigenvalues of $L(x)$ are $\lambda = (\text{re}\,x) \pm |\,\text{im}\,x|$. In general $L(xy) \neq L(x)L(y)$, $R(xy) \neq R(x)R(y)$, and $L(x) \neq R(x)$, exhibiting the non-associativity and non-commutativity of the octonions.

shall not provide proofs of all the other claims of EQ 65 since they are similar and at least equally easy. Q.E.D.

The 2^{n+1}-ons contain the 2^n-ons as the subalgebra of elements of the form $(a, 0)$.

EQ 65 allows us to rewrite our doubling formula in a matrix-free form[31]resembling the Cayley-Dickson doubling formula (EQ 48). The result is **Our doubling formula**

$$\boxed{(a,b)\,(c,d) \;=\; \left(ac \;-\; \overline{b\overline{d}},\; \overline{\overline{b}\,\overline{c}} \;+\; \overline{\overline{b}\,\overline{\overline{a}\,\overline{\overline{b^{-1}}\,\overline{d}}}}\right)} \qquad (68)$$

where if $b = 0$ then we agree to use

$$(a,b)\,(c,d) \;=\; (ac,\, \overline{a}d) \qquad (69)$$

instead, and as usual conjugation is defined (also recursively) via $\overline{(a,b)} = (\overline{a}, -b)$.

Theorem 13 (Relation to Cayley-Dickson). *Our doubling formula EQ 68 is equivalent to the Cayley-Dickson doubling formula EQ 48 when applied to the cases $2^n \to 2^{n+1}$ for $n \le 2$. Thus EQ 68, starting from the reals, yields the complexes, quaternions, and octonions. However, these formulae are* not *equivalent in the cases $2^n \to 2^{n+1}$ for $n \ge 3$, and hence EQ 68 does* not *yield the sedenions. In the particular case $2^3 \to 2^4$, EQ 68 is equivalent to EQ 70, EQ 72, and EQ 73 below.*

Proof: Simplify EQ 68 by repeated use of $\overline{ty} = \overline{y}\,\overline{t}$ (valid for the 2^n-ons with $n \le 3$) to get (for $2^n \to 2^{n+1}$, $n \le 3$)

$$(a,b)(c,d) \;=\; (ac - d\overline{b},\; cb + [\overline{a} \cdot db^{-1}]b). \qquad (70)$$

Now if we use associativity (valid for the 2^n-ons with $n \le 2$), the result is EQ 48. Because in the octonions $(\overline{a} \cdot db^{-1})b = \overline{a}b^{-1} \cdot bd$ is generally *not* equal to $\overline{a}d$ [an example, in the "nice" octonion basis of §5, is $i_1 i_2^{-1} \cdot i_2 i_3 = -i_4 i_5 = -i_0 \ne i_0 = i_1 i_3$] and hence, in all subsequent 2^n-on algebras, since they contain the octonions as a subalgebra, $xy^{-1} \cdot yz = xz$ also is a non-identity – we have inequivalence when $n \ge 3$. Q.E.D.

Remark. For more relations between our and the Cayley-Dickson formula, see theorem 30.

The octonions obey the variant-Moufang law ([181] EQ $\overline{10}$a p.421; our EQ 16)

$$[\overline{a} \cdot db^{-1}]b = \overline{a}b^{-1} \cdot bd = b^{-1}[b\overline{a} \cdot d], \qquad (71)$$

which allows us to re-express EQ 70 as (for $2^n \to 2^{n+1}$, $n \le 3$)

$$\boxed{(a,b)(c,d) \;=\; (ac - d\overline{b},\; cb + \overline{a}b^{-1} \cdot bd)} \qquad (72)$$

which is **the nicest 16-on definition**, and also as

$$(a,b)(c,d) \;=\; (ac - d\overline{b},\; cb + b^{-1}[b\overline{a} \cdot d]) \qquad (73)$$

when a, b, c, d are octonions. Q.E.D.

We call the new 16-dimensional normed algebra obtained from EQ 72 (or any of its equivalent forms), the *16-ons.*

Incidentally, we could instead start from the complex numbers (but with $\overline{z} = z$) to get the bi-complexes, bi-quaternions, bi-octonions, and bi-16-ons and bi-2^n-ons. Also, in EQ 57 we could have used complex matrices of half the dimensions of our real matrices and replaced the words "orthogonal" by "unitary" and "transpose" (A^T) by "Hermitian conjugate" (A^H) throughout, leading to a 2^{n-1}-complex-dimensional left-representation of the 2^n-ons, as opposed to our usual 2^n-real-dimensional one.

Theorem 14 (Non-distributive). *Our doubling formula (EQ 68) produces* non-*distributive 2^n-ons (and bi-2^n-ons) iff $n \ge 4$.*

Proof: Distributivity for $n \le 3$ follows from the previous theorem. Non-distributivity for $n = 4$ (and hence for all $n \ge 4$ since the 2^4-ons are a subalgebra of the 2^n-ons with $n > 4$) may be verified by direct computation for almost any numerical example. Its genesis is the presence of nonlinear operations such as matrix inversion and matrix multiplication in EQ 57 and hence in EQ 68. Q.E.D.

10 The most important properties of 2^n-ons

Theorem 15 (easy properties). *If a,b,x,y are 2^n-ons, $n \ge 0$, and s and t are scalars (i.e. all coordinates are* 0 *except the real coordinate) then*

unit *A unique 2^n-on 1 exists, with $1x = x1 = x$.*
zero *A unique 2^n-on 0 exists, with $0 + x = x + 0 = x$ and $0x = x0 = 0$.*
additive properties *$x+y = y+x$, $(x+y)+z = x+(y+z)$; $-x$ exists with $x + (-x) = x - x = 0$.*
norm $|x|^2 = x\overline{x} = \overline{x}x$.
norm-multiplicativity $|x|^2|y|^2 = |xy|^2$.
scaling $s \cdot xy = sx \cdot y = xs \cdot y = x \cdot sy = x \cdot ys$.
weak-linearity *$(x + s)y = xy + sy$ and $x(y + s) = xy + xs$.*
right-linearity $x(y + z) = xy + xz$.
inversion *If $x \ne 0$ then a unique x^{-1} exists obeying $x^{-1}x = xx^{-1} = 1$. It is $x^{-1} = \overline{x}|x|^{-2}$.*
left-alternativity $x \cdot xy = x^2y$.
left-cancellation $x \cdot x^{-1}y = y$.
effect on inner products *$\langle xa, b\rangle = \langle a, \overline{x}b\rangle$, $\langle x, y\rangle = \langle \overline{x}, \overline{y}\rangle$, $\langle \overline{x}a, x^{-1}b\rangle = \langle a, b\rangle$, and $\langle xa, xb\rangle = |x|^2\langle a, b\rangle$.*
Conjugate of inverse $\overline{x^{-1}} = (\overline{x})^{-1}$.
Near-anticommutativity of unequal basis elements *$e_k^2 = -1$ and $e_k\overline{e_\ell} = -e_\ell\overline{e_k}$ if $k \ne \ell$. (Note: the case $k, \ell > 0$ shows that unequal pure-imaginary basis elements anticommute.)*
Alternative basis elements *$e_k e_\ell \cdot e_k = e_k \cdot e_\ell e_k$, $e_\ell e_k \cdot e_k = e_\ell \cdot e_k e_k$, and $e_k e_k \cdot e_\ell = e_k \cdot e_k e_\ell$. (However, when $n \ge 4$ the 2^n-ons are* not *flexible i.e. it is not generally true that $xy \cdot x = x \cdot yx$ if x and y are 16-ons that are* not *basis elements. They also are* not *right-alternative.)*

[31]In the second half of the right hand side of EQ 68, note that every possible conjugation that can be performed, is performed, with the conjugation-indicating overline always being drawn over the rightmost product of terms before using that product in a multiplication. To the naive eye, i.e. if this simple governing pattern is unrecognized, EQ 68 seems much more complicated than it is. For naively *simpler*-appearing – but isomorphic – forms of EQ 57 and EQ 68, see EQ 110 and EQ 111.

Proof: These all follow immediately from lemma 11 and/or EQ 65, except for the alternativity of basis elements: The unit corresponds to the identity matrix. It is unique because the assumption that a second identity element $1'$ exists leads to a contradiction by considering $1 \cdot 1'$. The 0 corresponds to the zero matrix and similarly is unique by considering $0+0'$. Left-cancellation arises from the fact that $M(x^{-1})x = 1$ (proven by induction on n, cf. theorem 12) and the associativity of matrix multiplication; left-alternativity and left-cancellation imply one another via scaling, inversion, and weak-linearity. The uniqueness of x^{-1} is due to right-linearity and norm-multiplicativity (if there were two, then their difference Δ would obey $x\Delta = 0$, impossible). The conjugate-of-inverse identity arises from

$$(\overline{x})^{-1} = \frac{x}{|x|^2} = x|x^{-1}|^2 = \overline{x^{-1}}. \tag{74}$$

Finally, let us prove the alternativity of the basis elements. They are flexible because of the flexibility of Cayley-Dickson multiplication combined with theorem 30. They are left-alternative because of the left-alternativity of 2^n-on multiplication. Finally, they are right-alternative because by theorem 30 we know that the basis elements must be left-alternative under Cayley-Dickson multiplication, which implies (because of the symmetry of the definition of Cayley-Dickson multiplication) they also are right-alternative, and finally use theorem 30 again. The $\pm$-signed basis elements thus form an alternative multiplicative subloop with identity 1 and unique two sided inverses (namely $e_k^{-1} = \overline{e_k}$) obeying $a^{-1}b^{-1} = (ba)^{-1}$ (by the near-anticommutativity property). Q.E.D.

Remark. The left-cancellation and inversion properties make it easy to do 2^n-on left-division problems of the form "find x so that $qx = p$." We simply multiply both sides on the left by q^{-1}, getting $x = q^{-1}p$. However, we *cannot* solve right-division problems of the form "find x so that $xq = p$" in this way, because the 16-ons lack right-cancellation. Indeed, it is not immediately apparent that such an x even *exists*. We'll discuss 16-on right-division in §19-24.

Theorem 16 (Quadratic identity). *If x is a 2^n-on (over any field F with $\mathrm{char}F \neq 2$), then $x^2 + |x|^2 = 2x\,\mathrm{re}\,x$.*

Proof: This is just a restatement (via weak-linearity, theorem 15) of $\overline{x}x = |x|^2$, which in turn follows from the matrix picture, cf. theorem 12. (This theorem also holds in Cayley-Dickson algebras, cf. EQ 49.) Q.E.D.

Corollary 17 (Squares of imaginaries). *If x is a 2^n-on with $\mathrm{re}\,x = 0$ ("pure imaginary") then $x^2 = -|x|^2$ is non-positive pure-real.*

Since as soon as one proves some 2^n-on x is pure-imaginary, it has a pure-real square, immediately a large number of consequential identities follow, such as $yx^2 = x^2y$, $(y + x^2)z = yz + x^2z$, $(y+z)x^2 = yx^2 + zx^2$, and $x^2y \cdot z = x^2 \cdot yz$. A typical example, which seems remarkably mysterious if one does not realize that (due to the realness of x^2) it actually is trivial, is:

Corollary 18 (Weakened Jordan identities). *If x and y are 2^n-ons, and $\mathrm{re}\,x = 0$, then $xy \cdot x^2 = x \cdot yx^2$, $x^2 \cdot yx = x^2y \cdot x$, $x^2 \cdot xy = x(x^2y)$, $yx \cdot x^2 = (yx^2)x$. (If $\mathrm{re}\,x \neq 0$, then these, and $xy \cdot x = x \cdot yx$, hold, in general, only when $n \leq 3$. But all these hold in all Cayley-Dickson algebras for all n, x, y, regardless of whether x is pure-imaginary.)*

Theorem 19 (Complex subalgebra). *If x is a 2^n-on – either ours or those of Cayley and Dickson – then the algebra generated by all rational functions (with real coefficients) of x, is isomorphic to $\mathbb{C}$. (This also is true in the Cayley-Dickson 2^n-ons.)*

Proof: The *quadratic identity* $x^2 + |x|^2 = 2x\mathrm{re}x$ (theorem 16) implies that if x is pure-imaginary then $x^2 = -|x|^2$ is negative pure real. *Weak linearity* then implies that $x + s$, where s is pure-real, behaves just like the complex numbers $\mathbb{C}$. Because the Cayley-Dickson 2^n-ons also obey the quadratic identity and weak linearity (indeed: full bilinearity), they also obey the present theorem. Q.E.D.

Power associativity and power distributivity of the 2^n-ons are immediate consequences. We also prove the former directly:

Theorem 20 (Power associativity). *If x is a nonzero 2^n-on (over any field F with $\mathrm{char}F \neq 2$), then (for any integer k) x^k is unambiguous, e.g. $x^2x = xx^2 = x^3$, $x^2x^2 = xx^3 = x^3x$, etc.*

Proof: Define the reals c and s via $c = \mathrm{re}x$ and $s = |\mathrm{im}x|$. Then define c_k and s_k via $c_k + is_k = (c + is)^k$. Then we claim $x^k = c_k + s_k\mathrm{im}x/|x|$. Furthermore we claim that $x^Ax^B = x^{A+B}$ if A, B are non-negative integers. All these claims follow from weak-linearity, real-scaling, and the fact (derivable from the quadratic identity, theorem 16) that $(\mathrm{im}x)^2 = -|x|^2$. Q.E.D.

As a consequence of the above proof, we have

Corollary 21 (Powering preserves im$x$ direction). $\mathrm{im}\,x$ *is not altered (aside from a scaling by some pure-real factor, possibly 0) when x is taken to any integer power (or more generally, if any rational function, with only-real coefficients, of x is taken).*

and

Corollary 22 (Multiplying preserves im$x$ direction). *If two 2^n-ons x, y with the same imaginary parts (up to a proportionality factor): $a\,\mathrm{im}\,x = b\,\mathrm{im}\,y$, $a, b \in \mathbb{R}$, $|a| + |b| \neq 0$ are multiplied, then the result xy also has the same vector of imaginary parts $\mathrm{im}\,(xy)$ (aside from a scaling by another pure-real factor, possibly 0).*

Proof: Follows from corollary 21 by weak-linearity and real-scaling. Q.E.D.

10.1 Niners, Powons, and Twofers (and the reals) – nice subsets of the 2^n-ons

Definition 23 (Niners). A *niner* is a 2^n-on whose first 9 coordinates only (indices 0-8) are permitted to be nonzero (note: these include the octonion subalgebra in coordinate 0-7 and the reals in coordinate 0).

Niners enjoy particularly nice properties. Obviously the sum of two niners is a niner, and (due to $x^{-1} = \overline{x}/|x|^2$) the reciprocal of a niner is a niner. However, the square of a niner is not, in general, a niner.

Some related but less important objects are "powons" and "twofers":

Definition 24 (Powons). A *powon* is a 2^n-on whose nonzero coordinates occur at indices μ such that either $0 \leq \mu \leq 7$ or $\mu = 2^p$ for integer p.

Definition 25 (Twofers). If $n \geq 4$, a *twofer* is a 2^n-on of the form (x, y) where x and y are twofer 2^{n-1}-ons with $ax + by = c$ where a, b, c are reals with $abc \neq 0$. We make the recursion in this definition stop at the octonions by defining every 2^n-on with $n \leq 3$ to be a twofer.

Note that niners⊂powons⊂twofers. The sum of two powons is a powon. The reciprocal of a powon is a powon. However, the square of a powon is not, in general, a powon.

Theorem 26 (Twofer and powon products). *(a) The* Cayley-Dickson product *of two twofers is a twofer.*
(b) The Cayley-Dickson and 2^n-on products are the same thing if
they are used for multiplying xy where y is powon, or
(c) if $n \leq 4$ and they are used for multiplying two twofers.
(d) Any power of a twofer also is a twofer – in particular, its reciprocal and square – indeed, any rational function with real coefficients of a twofer also is a twofer.
(e) However, for each $n \geq 4$, the sum *of two twofers is in general* not *a twofer.*
(f) If x is a powon, then the Cayley-Dickson and 2^n-on products xy agree in their first 17 coordinates (and the same is true of yx due to b).

Proof: By case 4 of theorem 30, Cayley-Dickson and 2^n-on multiplication are the same for the purpose of squaring x or computing $\overline{x}x$.

Now (a) may be proven by induction on n using the Cayley-Dickson doubling formula EQ 48, corollary 22 and the preceding sentence.

(c) arises from octonion diassociativity and EQ 72 – since a 16-on twofer is generated by only a single octonion, multiplying two such 16-ons involves octonion products generated by only two octonions and which therefore fully associate, causing the 16-on multiplication formula EQ 72 to reduce to the Cayley-Dickson formula EQ 48.

(b) Is proven by induction on n using EQ 68 and weak-linearity – since a powon 2^n-on has a powon 2^{n-1}-on as its first half and a real as its second half.

(d) Arises from corollary 22.

(e) Because if $\vec{x}$ and $\vec{y}$ are linearly dependent (i.e. proportional) and $\vec{x}'$ and $\vec{y}'$ are too, then that does not imply that $\vec{x} + \vec{x}'$ and $\vec{y} + \vec{y}'$ are proportional. E.g. in $\mathbb{R}^2$ consider $\vec{x} = (0, 1)$, $\vec{y} = (0, 2)$ $\vec{x}' = (1, 0)$, $\vec{y} = (3, 0)$, and then $\vec{x} + \vec{x}' = (1, 1)$ while $\vec{y} + \vec{y}' = (3, 2)$.

(f) Same proof as (b), only start the induction at the 16-ons instead of the octonions, as is permitted via (c). Q.E.D.

It was recently discovered by Eakin and Sathay that twofers play a very important role in the sedenions. The (unachieved) goal of the original Eakin-Sathay paper [92] was to prove "Yiu's strong non-associativity conjecture" that, if x, y, z are in a Cayley-Dickson 2^n-dimensional linear algebra over any field F with characteristic not 2, then x, y, z associate, in that order, for *all* y, if and only if 1, x, and z are linearly dependent over F. They achieved the proof in a 1989 manuscript [93] which was never published due to a recalcitrant J.Algebra referee. Therefore, the Eakin-Sathay proof was reworked by Khalil & Yiu as §4 of their very useful paper [149] published in an exceedingly obscure journal. As a consequence of the Eakin-Sathay theorem, Khalil & Yiu deduced that the elements of the form (a, b) of the Cayley-Dickson 2^n-ons formed an "alternative subalgebra" if 1, a, and b were linearly dependent vectors over F *and* all lie in the analogous alternative subalgebra of the Cayley-Dickson 2^{n-1}-ons – i.e. (to restate this somewhat more strongly and correctly)

Theorem 27 (Eakin-Sathaye-Khalil-Yiu [149]). *In a 2^n-dimensional Cayley-Dickson algebra over a field F of characteristic not 2, the twofers form an alternative multiplicative*[32] *subloop, (indeed Cayley-Dickson multiplication obeys $xy \cdot x = x \cdot yx$, $xz \cdot z = x \cdot zz$, $zz \cdot x = z \cdot zx$, if z is twofer) and this is the largest-dimensional alternative subloop, with dimension $2n + 2$ if $n \geq 3$.*

Remark. Since Cayley-Dickson and 16-on multiplication are the same, the twofers form an alternative multiplicative subloop and 10-dimensional subset of the *16-ons*.

A 2^n-on analogue of theorem 27 is

Theorem 28 (Powon subspace). *If $n \geq 3$, the powons form a $(n+5)$-dimensional subspace (but not subloop) of the 2^n-ons, such that multiplication of powons is alternative.*

Proof: The dimensionality $n+5$ is since 1 extra dimension is added each doubling. The powons are not a subloop since the square of a powon is generally not a powon for each $n \geq 4$. The fact that multiplication among powons is alternative follows from the fact that Cayley-Dickson doubling yields an alternative multiplication if the original multiplication was associative, and that in turn is due to octonion diassociativity, since the only octonion multiplications arising in a powon multiplication ultimately arise from only *two* octonions. Q.E.D.

We conjecture that the powons are the largest dimensional alternative subspace. Powons also have this property:

Theorem 29 (Powon-distributivity). *If x, y, z are 2^n-ons and x, y are powons, then $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$.*

Proof: Only the first of these (left-linearity) needs to be proven, since the 2^n-ons are right-linear. This may be done by induction on n using EQ 68 and the fact that, in that formula, b is real. Q.E.D.

Many otherwise-mysterious properties of our 2^n-ons, especially niner-related properties and properties of basis elements, can be proved in a unified way once the following 2 theorems are known.

Theorem 30 (Conditions causing Cayley-Dickson and 2^n-ons to be same). *The Cayley-Dickson multiplication of 2^n-vectors xy (EQ 48), and ours (EQ 68) yield the* same *result if either*

1. *x is a niner;*
2. *y is a niner;*
3. *We only examine the first 9 coordinates $(xy)_{0,\ldots,8}$ of the product and ignore the others;*
4. *y (or $\overline{y}$) is a 2^n-onic rational function (with real coefficients) of x;*
5. *x is a basis element, i.e. $x = e_k$ for some k, $0 \leq k < 2^n$. Indeed, more generally, it will suffice if x is any 2^n-on all of whose coordinates are 0, except that nonzeros are allowed anywhere within a block of 8 consecutive coordinates of the form $8k, 8k + 1, 8k + 2, \ldots, 8k + 7$;*

[32] The original cites carelessly incorrectly claimed these are a sub*algebra* or subspace, but those both are false, at least with our definition of "algebra," because the sum of two twofers is not a twofer. They merely form a sub*set* which happens to be a manifold of dimensionality $2n + 2$.

Also, for any 2^n-ons x, y, the first 9 coordinates (indices 0-8) of the Cayley-Dickson product xy agree with the first 9 coordinates of our 2^n-on product xy.

Theorem 31 (Weakened antiautomorphism). *If x and y are 2^n-ons and p is a niner, then $\overline{x}\,\overline{p} = \overline{px}$, $\overline{p}\,\overline{x} = \overline{xp}$ (i.e., "9-antiautomorphism" holds) and*

$$(\overline{x}\,\overline{y})_{0\ldots 8} = (\overline{yx})_{0\ldots 8}, \qquad (75)$$

i.e. the antiautomorphism identity holds in the first 9 coordinates.

Proof sketch (of both theorems simultaneously):

First of all, theorem 31 follows from combining theorem 8 with the first 3 cases of theorem 30; its claims preceding EQ 75 arise directly, while EQ 75 requires also an induction on n. This (essentially) reduces our task to proving theorem 30.

1. If x is a 16-on which happens to be a niner, then its left-representation matrix $M(x)$ is $\begin{pmatrix} A & -I|b| \\ I|b| & A^T \end{pmatrix}$ and this may be seen also to be a valid left-representation for the Cayley-Dickson sedenions. This proves Cayley-Dickson and our multiplications are the same if x is a niner 16-on. Now if x is a 2^n-on whose second half is 0 then then its left-representation matrix $M(x)$ is $\begin{pmatrix} A & 0 \\ 0 & A^T \end{pmatrix}$ which again agrees with the Cayley-Dickson formula. Together, this proves (by induction on n with base case at the 16-ons) that the Cayley-Dickson and our multiplications xy are the same if x is a niner 2^n-on.

2. Now to prove that these two notions of xy are the same if y is a niner 2^n-on, we need to prove that the first 9 *columns* of our left-representation matrix of x agree with the first 9 rows of the $2^n \times 2^n$ matrix representing Cayley-Dickson left-multiplication by x. Similarly to prove that they yield the same first 9 coordinates of xy for *any* 2^n-ons x, y, we need to show instead that the first 9 *rows* are the same. (So these are handled by, essentially, the same proof.) This also may be accomplished by induction on n, using the 16-on 9-coordinate antiautomorphism identity $(\overline{ab})_{0,\ldots,8} = \overline{b}\overline{a}_{0,\ldots,8}$ and the sedenion full-strength antiautomorphism identity $\overline{ab} = \overline{b}\,\overline{a}$ (see theorem 31 and its proof) as the base of the induction.

3. Note that the first half of the right hand side of our 2^n-on multiplication law EQ 68 agrees with the first half of the right hand side of the Cayley-Dickson multiplication law EQ 48, in whatever coordinate subset the antiautomorphism law EQ 75 is valid in. But we've just seen that we may inductively assume that coordinate subset includes $\{0, \ldots, 8\}$. This yields an inductive proof of the fact that $(xy)_{0,\ldots,8}$ is the same for both 2^n-on and Cayley-Dickson multiplication. (Further: The weak-associativity of 2^n-on multiplication – see theorem 35 – in combination with the Cayley-Dickson [EQ 48] and our multiplication laws [EQ 68] may be used to see that the first coordinate of the second half of xy, i.e. coordinate 2^{n-1}, is the same under either Cayley-Dickson or 2^n-on multiplication. For our purposes, though, we only need to prove this when $n = 4$ to get a basis for our induction, and for that we only need the weak-associativity property $\mathrm{re}\,(ab \cdot c) = \mathrm{re}\,(a \cdot bc)$ of the octonions, which could be proven by computer as in §11.)

4. If y is a 2^n-onic rational function of x then the proof is just a consequence of theorem 19.

5. If x has nonzeros only in one of those 8-coordinate-wide blocks, then the two definitions of xy are clearly the same (see EQ 72) if x and y are 16-ons or below. If they are 2^n-ons with $n \geq 5$, we simply proceed by induction on n, building the both matrix left-representations of x and noting that all blocks except one are always 0, and for 16×16 (or smaller) blocks we have equality and the antiautomorphism identity $\overline{vt} = \overline{t}\,\overline{v}$ holds in 8×8 (or smaller) cases. Q.E.D.

Remark. If $y = e_\mu$ is a basis element, then Cayley-Dickson and our multiplications do not in general yield the same results xy if $\mu > 8$ (although the two xy are the same in coordinates 0-8 and μ). Furthermore, the 2^n-on products xe_μ are in general not linear in x except when $0 \leq \mu \leq 8$ (although they are linear if only coordinates 0-8 and μ of the product are examined).

Remark without proof. If y is a powon and we only examine the first 17 coordinates $(xy)_{0,\ldots,16}$ of the product and ignore the others, then Cayley-Dickson and 2^n-on multiplication yield the same result.

The octonions's antiautomorphism identity $\overline{x}\;\overline{y} = \overline{yx}$ (and the related $x^{-1}y^{-1} = (yx)^{-1}$) becomes false in the 16-ons and beyond. But fortunately, as we've already seen (theorem 15) it is valid when $x = \overline{y}$, and theorem 31 and theorem 44 give weakened senses which still hold in all 2^n-ons, and in the 16-ons, respectively.

Define the "bimultiplication" map $(x, y) \to xy \cdot x$ and the "comultiplication" map $(x, y) \to xy \cdot \overline{x}$.

Theorem 32 (Conditions causing CD and our bi(co)multiplication to be same). *Bimultiplication $xy \cdot x$ (and comultiplication $xy \cdot \overline{x}$) of 2^n-vectors x and y yields the same result under either the Cayley-Dickson (EQ 48) and our (EQ 68) multiplication laws, provided either*

1. *x is a niner;*
2. *y is a niner and only the "powon coordinates" 0-7, and coordinates $2^k < 2^n$ of the results are compared, with the others being ignored*[33]*;*
3. *Only the real parts of the results are examined, with the others being ignored.*

Proof: 1. The first claim follows immediately from claims 1 and 2 of theorem 30.

2. Our second claim (in coordinates 0-8) follows from claims 2 and 3 of theorem 30. The claim remains unproven in coordinates 16, 32, etc.

3. Our third claim arises because the real part of $xy \cdot \overline{x}$ is just $|x|^2\,\mathrm{re}\,y$ in both cases. In 2^n-on multiplication this is due to the fact that, due to weak-linearity (theorem 15) and norm-multiplicativity the norms of the real and imaginary parts of y both get multiplied by $|x|^2$ during comultiplication with x. The result for bimultiplication then follows via weak linearity. (In fact, by weak linearity it suffices to prove the claim when x is pure imaginary, in which case both bi- and co-multiplication are the same thing up to an overall sign.)

In Cayley-Dickson multiplication, although we have full bilinearity we do not have norm-multiplicativity so the preceding argument does not work. However, by linearity it will suffice to show that

[33] Actually, we shall only prove this for the "niner coordinates" 0-8.

1. If y is real, then it works (and yes, it does, since reals commute with everything),
2. if y is pure-imaginary then it works, i.e. $\mathrm{re}\, xy\overline{x} = 0$.

So let us now restrict attention to the as-yet-unproven second case. Now by linearity it suffices to prove it when y is in fact a pure-imaginary *basis* element (and as above we may also assume x is pure-imaginary). If x is parallel to y it then obviously works, so by linearity it suffices to prove it when x is orthogonal to y. But in that case by anticommutativity of differing imaginary basis elements (by claim it:basiscdsame of theorem 30 and the claims about basis elements in theorem 15) we get 0. Q.E.D.

Theorem 33 (Linearity properties of bi(co)multiplication). *Let x,y and z be 2^n-ons.*

1. *If y is a niner then $x \to yx \cdot y$ and $x \to yx \cdot \overline{y}$ are linear maps.*
2. *The first 9 coordinates of the output of the maps $x \to yx \cdot y$ and $x \to yx \cdot \overline{y}$ are linear in x.*
3. *If y is niner then $x \to zx \cdot y$ is a linear map.*

Proof: The linearity of the maps $x \to zx$ and (if y is niner) $x \to xy$ are obvious from the definition (EQ 68-69) of 2^n-on multiplication. Claims 1 and 3 follow immediately. Now the linearity of the map $x \to (xy)_{0,\dots,8}$ is obvious from the linearity of 2^n-on multiplication if $n \le 3$ or from claim 3 of theorem 30. Q.E.D.

Remark without proof. If x,y,z are 2^n-ons and y is powon then $x \to (zx \cdot y)_{0,\dots,16}$ is a linear map.

Theorem 34 (Niner properties of 2^n-ons). *If x, y, and z are 2^n-ons, $n \ge 0$, and p and q are 2^n-ons whose only nonzero coordinates are their first 9 (or fewer), i.e. p and q are niners, then*

9-flexibility $xp \cdot x = x \cdot px$, $px \cdot p = p \cdot xp$.

9-similitude unambiguity $xp \cdot x^{-1} = x \cdot px^{-1}$, $px \cdot p^{-1} = p \cdot xp^{-1}$.

9-right-alternativity $xp \cdot p = x \cdot p^2$, $px \cdot x = p \cdot x^2$.

9-right-cancellation $xp^{-1} \cdot p = x$, $px^{-1} \cdot x = p$.

9-effect on inner products $\langle x, yp\rangle = \langle x\overline{p}, y\rangle$, $\langle xp, yp\rangle = |p|^2\langle x, y\rangle$.

9-left-linearity $(x + y)p = xp + yp$, $(p + q)x = px + qx$.

9-Jordan-identity $xp \cdot xx = x(p \cdot xx)$, $py \cdot pp = p(y \cdot pp)$.

9-coordinate-distributivity $([x + y]z)_{0,\dots,8} = (xz + yz)_{0,\dots,8}$.

9-coordinate-Jordan-identity $[xy \cdot xx]_{0,\dots,8} = [x(y \cdot xx)]_{0,\dots,8}$.

9-anticommutativity for orthogonal imaginary 2^n-ons *If $\langle p, x\rangle = \mathrm{re}\, p = \mathrm{re}\, x = 0$ then $px = -xp$.*

9-reflection *If $|a| = 1$ and the geometric reflection operator is defined in EQ 33 then $-(\mathrm{refl}[a](y))_{0,\dots,8} = (a \cdot \overline{y}a)_{0,\dots,8}$, and $-\left(\overline{\mathrm{refl}[a](y)}\right)_{0,\dots,8} = (\overline{a}y \cdot \overline{a})_{0,\dots,8}$, and if either a or y is a niner then $-\mathrm{refl}[a](y) = a \cdot \overline{y}a$ and $-\overline{\mathrm{refl}[a](y)} = \overline{a}y \cdot \overline{a}$.*

Proof: The proof of the octonion, as opposed to niner, versions of the these statements (i.e., if only the first 8 of p and q's coordinates are allowed to be nonzero) all are quite direct. 8-left-linearity arises from the fact it is true if $n \le 3$, and the fact that "only the first 8 coordinates matter" in the sense that $(xp)_{0,\dots,7} = x_{0,\dots,7}p$, $(px)_{0,\dots,7} = px_{0,\dots,7}$. Meanwhile right-linearity is of course valid for 2^n-ons without any 8-restrictions. The other properties now arise from the matrix picture, but regarding every $N \times N$ matrix as an $(N/8)\times(N/8)$ octonion matrix and every N-tuple as an $(N/8)$-tuple of octonions. The fact that all these properties (and distributivity) are true for octonions, then causes them to be true here.

The niner versions are also fairly easy in the *16-ons* ($n \le 4$). When multiplying two 16-ons, at least one of which is a niner, our multiplication formula (EQ 72) becomes equivalent to the (linear, flexible, Jordan) Cayley-Dickson formula (EQ 48) due to octonion diassociativity (and the fact that everything associates with a scalar). 9-left-linearity, 9-Jordan, and 9-flexibility follow. 9-right-alternativity then follows from linearity and left-alternativity and flexibility.

The hardest case is the fully general one where we allow $2^n > 16$. These results all appeared extremely mysterious until theorem 8 was discovered! To see 9-flexibility, combine the flexibility property (cf. footnote 24) of the Cayley-Dickson algebras with the first 3 cases of theorem 8 (for the second 9-flexibility identity, only the first 2 cases of theorem 8 are required). 9-similitude unambiguity, 9-right-alternativity, 9-right-cancellation, then follow. The bilinearity of Cayley-Dickson multiplication, combined with theorem 8, proves 9-left-linearity and 9-coordinate-distributivity. Using the fact that the first 9-effect on inner products identity holds for any p in Cayley-Dickson algebras (due to the fact that $\langle A\vec{x}, \vec{y}\rangle = \langle \vec{x}, A^T\vec{y}\rangle$ for any matrix A) we similarly prove the first 9-effect on inner products identity. The second 9-effect on inner products identity is true because 2^n-on right-multiplication by a *niner* is a *linear* transformation (by 9-left-linearity) and one which by norm-multiplicativity must be a scaled rotation – then this identity merely expresses that fact that spatial rotations preserve angles.

The 9-anticommutativity statement arises from the statement about near-anticommutativity of unequal basis elements in theorem 15: hence if a and b are *orthogonal* and if the multiplication ab is *bilinear*, then a and b must anticommute – and we've seen before (e.g. from 9-left-linearity and right-linearity) that 2^n-on multiplication *is* bilinear if at least one of the multiplicands is niner.[34]

The 9-coordinate Jordan identity arises from the fact that the Cayley-Dickson algebras are Jordan and the first 4 cases of theorem 8, where note that x^2 is the same in either Cayley-Dickson and 2^n-on multiplication due to case 4 of theorem 8. The hardest case is the 9-Jordan identity, which requires, in addition to the reasoning used to obtain the 9-coordinate Jordan identity, also the fact (cf. corollary 21) that x^2 is the *same* as x, except for scaling of its real and imaginary parts by two factors, i.e. is the same as x up to a scaling followed by adding a real number. Hence it suffices (for the purpose of proving the first 9-Jordan identity) if we prove it with x written in place of x^2, and then prove the identity's validity cannot be affected by either scaling and/or adding any real constant to that x^2. But that is obvious from the right-linearity of 2^n-on multiplication.

[34] The further speculation that $ab + ba = 0$ if a, b are 2^n-ons with $\mathrm{re}\, a = \mathrm{re}\, b = \langle a, b\rangle = 0$, while (as we have just proven) true for $n \le 3$, is easily seen by test to be generically false if $n \ge 4$.

To prove 9-reflection: We need only prove one member in each of the two pairs of 9-reflection identities since the other then just arises by using 9-antiautomorphism.

We showed in the proof of theorem 2 that the reflection identities in the Cayley-Dickson algebras hold to precisely the same extent as the left-cancellation identity.

Now let a,b be 2^n-ons with $|a| = 1$ so that $a^{-1} = \overline{a}$. By theorem 30 and right-linearity EQ 34 also is true in 2^n-ons, provided either a or b is a niner, or if we only require equality in the first 9 coordinates. Then by the left-cancellation property of 2^n-ons combined with theorem 32, we get EQ 35, which proves our first reflection identity in the 2^n-ons *provided* a is niner.

But this proof method will not work to prove the Theorem's claims about 9-reflection for *non*-niner a. For that we need some additional tricks:

1. By norm-multiplicativity, pre- and post-multiplying by unit-norm 2^n-ons leaves y's norm unchanged.
2. By theorem 33 all the bi- and comultiplication maps we are speaking of are linear in all the coordinates in which the Theorem claims the reflection identity.
3. Obviously, the reflection identities work (always, in *all* coordinates) in all 5 of the special cases in EQ 37-38. E.g. the two last of these state (cf. theorem 19) that squaring a unit-norm complex number doubles the angle it makes with the real axis, while the second is an analogous statement about cubing.

So we have a linear, norm-preserving map, such that adding a to its input, subtracts a from its output, and such that adding 1 to its input, subtracts a^2 from its output. Such a map must be a reflection with characteristic direction a, *except* possibly composed with a rotation preserving the directions a and 1. By linearity, to prove our claims (i.e. to prove the rotation is merely the identity map) it suffices to prove our claim when y is orthogonal to a and 1. i.e. when $\langle y, a\rangle = \mathrm{re}\, y = 0$. Further, by considering weak-linearity, we may reduce the problem to the case where a also is pure-imaginary wlog. But then by 9-anticommutativity followed by left-cancellation, $-a \cdot y\overline{a} = a \cdot \overline{a}y = y$ is indeed the identity map! Q.E.D.

Remark without proof. If a is a *powon* then these two 17-coordinate reflection identities hold:

$$-\left(\mathrm{refl}[a](y)\right)_{0,\dots,16} = (a \cdot \overline{y}a)_{0,\dots,16}, \tag{76}$$

$$-\left(\overline{\mathrm{refl}[a](y)}\right)_{0,\dots,16} = (\overline{a}y \cdot \overline{a})_{0,\dots,16}. \tag{77}$$

Theorem 35 (Real parts). *If x and y are 2^n-ons, then*
weak-commutativity $\mathrm{re}(xy) = \mathrm{re}(yx)$.
weak-flexibility $\mathrm{re}(x \cdot yx) = \mathrm{re}(xy \cdot x)$
weak-similitude unambiguity $\mathrm{re}(x^{-1} \cdot yx) = \mathrm{re}(x^{-1}y \cdot x)$
weak-right-alternativity $\mathrm{re}(y \cdot xx) = \mathrm{re}(yx \cdot x)$
weak-right-cancellation $\mathrm{re}(yx^{-1} \cdot x) = \mathrm{re}(y \cdot x^{-1}x) = \mathrm{re}(y)$

Proof: The proof of weak-commutativity is $\langle xy, 1\rangle = \langle y, \overline{x}\rangle = \langle \overline{y}, x\rangle = \langle 1, yx\rangle$. The proof of weak-flexibility is $\langle x \cdot yx\rangle = \langle yx, \overline{x}\rangle = \langle xy \cdot x, 1\rangle = \langle x, \overline{xy}\rangle$. The others are proven similarly. Q.E.D.

10.2 Gains rather than losses?

Doubling causes many enjoyable algebraic properties to vanish, and once an identity vanishes, it never re-appears, since each doubled algebra contains the previous one as a subalgebra.

But, occasionally, new good properties can *appear*. For example, the quaternions q enjoy the property that we may express $\overline{q}$ as a quaternionically-linear function of q:

$$\overline{q} = \frac{-1}{2}(q + iqi + jqj + kqk) \tag{78}$$

whereas $\overline{z}$ is *not* expressible as a complex-linear function of z, for complex z, since it is a non-analytic function[35]. Indeed for each $n \geq 0$ except for $n = 1$, in the *Cayley-Dickson* 2^n-ons (which differ from ours when $n \geq 4$) we have

$$\overline{x} \;=\; \frac{-1}{2^n - 2} \sum_{m=0}^{2^n-1} e_m x e_m \tag{79}$$

where the e_m are the basis elements of the algebra ($e_0 = 1$, and $e_m^2 = -1$ for $1 \leq m \leq 2^n - 1$). (Note: we have taken advantage of the flexibility property EQ 9 of the Cayley-Dickson algebras to avoid needing parentheses.) But EQ 79 is not true in our 2^n-ons if $n \geq 3$, and indeed we suspect that the expressibility of $\overline{x}$ as a 2^n-on-linear function of x is irrevocably lost at the 16-ons:

Conjecture 36 (Conjugation as 2^n-onically linear function). *The conjugate $\overline{x}$ of a 2^n-on x is expressible as a formula consisting of multiplications by constant 2^n-ons and 2^n-on additions, iff $n \in \{0, 2, 3\}$. In these 3 cases EQ 79 does the job.*

Another example of an evanescent property-gain is the uniqueness of the octonion "companions" of an 8D rotation, see theorem 3.

Another example: the complex numbers are algebraically closed, whereas the reals are not. However, this property is immediately re-lost at the quaternions, since $(q + iqi + jqj + kqk)q + 1$ has no quaternion zeroes q (since this is just $|q|^2 + 1$; admittedly, this has *bi*quaternion zeros).

Similarly, neither the octonions, nor any of the Cayley-Dickson algebras of dimension $2^n \geq 4$, are algebraically closed. This leads to the suspicion that none of the 2^n-ons with $n \geq 4$ are algebraically closed either. True:

Theorem 37 (Algebraic closedness). *The 2^n-ons are algebraically closed precisely when $n = 1$. The bi-2^n-ons are algebraically closed precisely when $n \in \{0, 1\}$.*

Proof: For any quaternion a, $P_a(x) = ax - xa + 1$ has no zeros x (since $\mathrm{re}P_a(x) \equiv 1$ by "weak-commutativity," see theorem 35), not even biquaternionic ones. Now all this remains true if "quaternion" is replaced by "2^n-on for $n \geq 2$" throughout, so the 2^n-ons and bi-2^n-ons are not algebraically closed if $n \geq 2$. Since $x^2 + 1$ has no real zeros the 2^0-ons are not algebraically closed. The bi-2^0-ons and the 2^1-ons both are just $\mathbb{C}$

[35] Incidentally, any of the 4 coordinates inside a quaternion similarly is expressible in terms of the original quaternion via $\mathrm{re}\, q = (q + \overline{q})/2$, and then the coefficient of j inside q is $q_2 = \mathrm{re} -jq$, etc.

and hence are algebraically closed by the usual fundamental theorem of algebra (in $\mathbb{C}$).

This leaves only the bi-complex numbers, i.e. the bi-2-ons; and these obey a fundamental theorem of algebra for any of three reasons: First, Price's book [208] on bicomplex and multicomplex numbers indicates that a degree-D bicomplex polynomial generically has D^2 (not D) bicomplex roots. Second, Segre's algebra isomorphism (our theorem 9) makes the D^2-roots theorem, the fundamental theorem of algebra, and many other claims in Price's book (e.g. generalization of Cauchy integral theorem, fundamental theorem of calculus) immediately obvious. Third, versions of our topological proof of the F.T.O.A. in our theorems 65 and 90 should still work for bicomplex numbers. Q.E.D.

But the reader will be reassured to know that there are some properties that never go away. For example, every complex number is the root of a quadratic equation with real coefficients (and every such quadratic equation is soluble by some complex number). This property also holds in all the Cayley-Dickson algebras [226], and in our 2^n-ons too, see theorem 16.

11 How to make your computer prove identities (especially 2^n-on identities for fixed n). New & old forms of Schwartz-Zippel lemma.

It is possible to verify[36] any set of 16 polynomial (or indeed, rational) identities by computer. One may either use

1. the automatic simplifiers provided with any symbolic algebra system, or
2. the Schwartz-Zippel lemma [229][260][261] to get a "probabilistic proof" with *arbitrarily exponentially small* probability (assuming you have access to a source of truly random bits) of error.

11.1 The original Schwartz-Zippel method

The Schwartz-Zippel method allows one to "prove" any multivariate polynomial (or indeed rational – or indeed algebraic [261] with a few more bells and whistles added) identity that holds over the reals, by essentially, just trying it on random numbers. This is a proof in the sense that if the random numbers don't work, the identity is false. If they do work (for certain kinds of rational or integer random number generators, which are easily constructed – integers random uniform in an interval of width $300DV$ work, where D is the degree and V is the number of variables) this means either the identity was true, or it was false and you got unlucky, *but* such bad luck can be proved to happen $< 1\%$ of the time (this is the Schwartz-Zippel "lemma"). So by repeated experiments with independent random numbers each time, one may shrink the incorrectness probability to arbitrarily high powers of 0.01.

For example, to prove the identity

$$(x+3)^4 = x^4 + 12x^3 + 54x^2 + 27(4x+3), \tag{80}$$

Schwartz and Zippel might try it for random integer x with $0 \le x \le 400$. Because a degree-4 polynomial has at most 4 roots of this form, if this identity had been false, each such test would have detected that falsity with probability $> 99\%$. Similarly, to gain 99% confidence in the correctness of

$$(x + y^2 + 1)^2 = 2(xy^2 + x + y^2) + x^2 + y^4 + 1, \tag{81}$$

Schwartz and Zippel might try it for random pair (x, y) of integers with $0 \le x, y \le 1000$. In all of these examples, a full expansion into monomials followed by a lexicographic sorting of those monomials by degree-type would also have proven the identity. But the brute force expansion technique can be very laborious. For example an $N \times N$ determinant, fully expanded, is $N!$ monomials. All the computer time so far expended by humanity would not suffice for the brute force verification of the fact that 30×30 determinants are multiplicative. However, simply trying it on $2 \cdot 30^2$ random integers each of absolute value$\le 10^7$ could be accomplished in milliseconds.

Indeed, there is reason to suspect[37] that *no nonrandom* polynomial-time algorithm for verifying general polynomial identities *exists*, in which case the randomized Schwartz-Zippel verifier reigns supreme.

11.2 The domain of applicability of Schwartz-Zippel

The Schwartz-Zippel method, as just formulated, only applies to proving identities holding over the real (or complex) numbers, i.e., identities which are consequences solely of the properties of *commutative fields*:

Theorem 38. *Any multivariate rational identity (with algebraic numbers as coefficients) that is unfalsifiable over $\mathbb{R}$, in fact is unfalsifiable over any commutative field.*

Proof: Let us initially assume that all coefficients are restricted to be integers. Any such rational identity over the real numbers may be proven (or disproven) by carrying out various "algebraic simplification steps" (depending for their validity only on the associative, commutative, and distributive laws, i.e. the field properties, or the reals) to reduce both sides of the identity to a canonical form (i.e. to ratios of polynomials, then to polynomials whose monomial terms are sorted into lexicographic order, then to $0 = 0$, or in the case of a disproof, to $0 = 1$) at which point its validity (or lack thereof) becomes obvious. Since these steps depend only on field properties, we see that any rational identity (having only integers as coefficients) valid over the reals is necessarily valid in *any* field in which it is well-defined. So this kind of identity

[36] See the book "$A = B$" [194] for further information about proving identities by computer, although the identities discussed there are mainly of a different and more sophisticated character than the ones we shall discuss here, so that our discussions are complementary.

[37] That is because [146] the existence of such an verifier would yield proofs of lower bounds in complexity theory. Therefore either no such derandomization exists, or it will be very difficult to find.

in the reals, necessarily is unfalsifiable over any commutative field[38].

Furthermore, if the coefficients are real algebraic numbers (canonically described by their minimal polynomials) all of this also goes through in any field in which those algebraic numbers exist. Q.E.D.

11.3 Extension to handle *not*-necessarily-commutative fields

As an important extension, we now point out that the Schwartz-Zippel method may be extended to handle polynomial identities which are consequences purely of the properties of *not*-necessarily-commutative fields[39].

Theorem 39 (Extension of Schwartz-Zippel to non-commutative identities). *To gain $> 99\%$ confidence in the correctness of a polynomial identity of degree D among V not-necessarily-commuting (but associative and distributive) variables, it suffices to try it on random $N \times N$ integer matrices, for any N with $2N > D$, with the integers x selected uniformly at random such that $|x| \le 300N^2VD$.*

Proof: To make this go through, we need two things. First, we need an analogue of the Schwartz-Zippel lemma about counting zeros of polynomials. Second, we need a theorem that $N \times N$ matrices of order N do *not* obey any "extraneous" identities, i.e. beyond those implied by associativity and distributivity, i.e. by the properties of any not-necessarily-commutative field.

These two needs are satisfied: The Amitsur-Levitski theorem [16][222] states that the minimal degree of an "extraneous" polynomial identity satisfied by $N \times N$ matrices is $2N$. The required analogue of the Schwartz-Zippel lemma then is trivial since we can rely on the *original* versions of that lemma (based on N^2V real numbers – the entries of our matrices) only. Q.E.D.

11.4 Extension to allow differential operators

As a second important extension, we now consider the problem of automatically proving identities such as

$$\frac{\partial^2}{\partial x \partial y}(x^2 F + xy) = 1 + 2x\frac{\partial}{\partial y}F + x^2\frac{\partial^2}{\partial y \partial x}F \qquad (82)$$

where $F = F(x, y)$ is an arbitrary sufficiently-differentiable function of x, y. (By "sufficiently-differentiable" we mean, having enough derivatives so that both sides of the identity are defined.)

Definition 40 (Differential-polynomial). A "differential-polynomial" is an expression involving a finite number of variables $x_1, x_2, \ldots, x_v$ and unspecified functions $F_1, F_2, \ldots, F_v$ of them, combined via $+$, $-$, $\cdot$, and partial derivatives.

Again, it is possible to accomplish this by brute force expansion of both sides into monomials in partial derivatives of F. But again, that can be exponentially laborious and there is a far simpler and quicker randomized way.

Theorem 41 (Extension of Schwartz-Zippel to differential-polynomial identities). *Any fixed-order differential-polynomial identity may be verified (with confidence$>$ 99%) by a randomized polynomial-time algorithm.*

Proof: Both sides of the identity are polynomials in the variables *and* in the partial derivatives of all the unspecified functions. Then our identity is valid iff it then holds as a polynomial identity. Nowadays well known techniques of "algorithmic differentiation" [27][118] allow one to evaluate any fixed-order partial derivative of a function in at most constant factor more arithmetic operations than any desired algorithm uses to compute the function itself (and this is also true if one counts the non-arithmetic bookkeeping operations as well). Using those techniques we simply evaluate both sides of our identity employing random numbers in place of the variables $x_1, x_2, \ldots, x_v$, the unspecified functions $F_1, F_2, \ldots, F_v$, and their partial derivatives. The only (minor) difficulty is making sure that the "random" numbers are compatible, i.e. that all equalities of mixed partials such as $F_{xy} = F_{yx}$ are obeyed. (The point is there are fewer degrees of freedom, i.e. fewer "variables," than one might naively have supposed.) But since we are assuming the maximum order of any partial-differential is *fixed*, this could be assured by simply building a polynomial-sized table of all required partial derivatives of all functions ahead of time. Q.E.D.

11.5 Remarks on practical experience with computer proofs

Unfortunately, the symbolic algebra system `MAPLE` appears to have been implemented extremely inefficiently, and thus in some cases exhausts all available memory (300 megabytes!) before it can prove moderately complicated 16-on identities[40]. Meanwhile the Schwartz-Zippel method is far faster and consumes negligible memory. Also, despite the fact that it only yields a "probabilistic proof," we tend to think that proof is, in practice, more reliable than `MAPLE`'s "genuine" proof, due to the comparative simplicity of the computer program. Because of the directness and reliability of such computer proofs we shall not provide explicit manual proofs of many of the 2^n-on ($n \le 6$) identities in this monograph, unless said proofs are particularly simple, logically central, or illuminating.

[38] Warning. Some simplification steps may involve multiplying both sides by an quantity which could, in some fields, be identically 0. E.g. $3 = 0$ in GF_3. These steps are irreversible and hence in such fields the final $0 = 0$ would not back-imply the original identity. However, this can only arise in cases where the original "identity" EQ 41 involved division by 0, in which case the problem would not be that EQ 41 is invalid; it would be that it was not defined. I.e., we would still have a never-false identity.

[39] J.H.Conway and D.Smith ([68], sec. 7.4) conjectured that the free Moufang loop with n generators is generated by n generic octonions. If so, one presumably could automatically prove or disprove, by similar techniques, any identity following from the defining properties of a Moufang loop.

[40] It may help to start the 16-on-defining recursion EQ 72 at the complex numbers – dimension 2 – instead of the reals at dimension 1, thus halving the number of and size of the identities `MAPLE` must tackle. It definitely helps to stay with the bilinear Cayley-Dickson formula (EQ 48) for as long as possible before switching to the nonlinear formula (EQ 72), so that `MAPLE` needs to rediscover their initial equivalence (i.e. our theorem 13) as few times as possible.

12 The 16-ons

In this section, we focus on the 16-ons as opposed to the 2^n-ons generally, and work from the 16-on-specific multiplication-defining formulae EQ 70 and EQ 72. In some cases we re-prove general 2^n-on theorems in our specific case $n = 4$.

Theorem 42 (Block structure of 16-on multiplication). *If x is a 16-on and y is an octonion, then multiplying xy or yx has the same effect as regarding x as a 2-tuple of octonions and performing separate octonion multiplications to each element of the tuple. (See the two formulae in the proof.)*

Proof: The nonlinear term in the multiplication formula EQ 68 vanishes since the second half of y is 0 or since we need to use the EQ 69 instead. Namely:

$$(a, b)(c, 0) = (ac, \overline{\overline{b}\,\overline{c}}) \tag{83}$$

which is just (ac, cb) if b, c are octonion; and

$$(a, 0)(c, d) = (ac, \overline{a}d). \tag{84}$$

Q.E.D.

Unfortunately, the 16-ons are *nondistributive* since their multiplication operation is given by a non-bilinear rational formula. But fortunately

Theorem 43 (Weakened distributivity laws). *If x, y, z are 16-ons, then $z(x + y) = zx + zy$ ("right-linearity"). In general, left-linearity $(x + y)z = xz + yz$ does not hold in the 16-ons, but it does hold ("conditional left-linearity") in certain circumstances:*

weak linearity *If either x or y (or both) are scalar 16-ons, then $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$.*

niner distributivity *If z is a niner, or if both x and y are niners [i.e. if $x = (a, s)$, $y = (b, t)$ where s and t are real], or if $x = (s, a)$ and $y = (t, b)$ where s and t are real ["reverse niners*"], then $(x + y)z = xz + yz$.*

octonion distributivity *If x and y are either*

1. *Both octonions, or*
2. *Both orthogonal to the octonion subalgebra*, or*
3. *One is octonion and the other is orthogonal to the octonions*,*

then $(x + y)z = xz + yz$.

9-coordinate distributivity *The first 9 coordinates (indices 0-8) of $(x+y)z$ are equal to the first 9 coordinates of $xz + yz$, i.e. $([x + y]z)_{0,...,8} = (xz + yz)_{0,...,8}$.*

power-distributivity *If x is 16-on and s, t are real, $(sx^k + tx^\ell)x^m = sx^{k+m} + tx^{\ell+m} = x^m(sx^k + tx^\ell)$; If x, y are 16-ons and s, t are real, $(sx^k + tx^\ell)y = sx^k y + tx^\ell y$.*

Also, all of the non-asterisked(*) statements above hold for all 2^n-ons, not just 16-ons.

Proof: For power-distributivity, see theorem 19 or the proof of lemma 52. For everything else, the proof is direct from EQ 72: Right linearity is obvious from EQ 72 and the linearity of the octonion-multiplications inside it. The proofs of conditional left-linearity depend on the fact that, under the conditions stated, (EQ 72) becomes equivalent to the bilinear equation (EQ 48). Depending on which condition, this equivalence may be either seen directly, or is due to the diassociativity of the octonions (e.g. any 3 octonions associate if at least one of them is a scalar octonion).

Finally, the fact that the non-asterisked statements hold for general 2^n-ons, not just 16-ons, follows directly from theorem 34 (to prove our theorem's final claim, about power-distributivity, note also corollary 21). Q.E.D.

A 16-on property failure that makes division-like problems even more painful is the fact that the octonions's antiautomorphism identity $\overline{x}\,\overline{y} = \overline{yx}$ (and the related $x^{-1}y^{-1} = (yx)^{-1}$) becomes *false* in the 16-ons. But fortunately, as we've already seen (theorem 15) these identities are valid when $x = \overline{y}$. Also fortunately,

Theorem 44 (Weakened antiautomorphism in 16-ons). *If t and y are 16-ons, then*

$$(\overline{t}\,\overline{y})_{0...8} = (\overline{yt})_{0...8}, \tag{85}$$

i.e. the antiautomorphism identity holds in the first 9 coordinates. Also, if $t = (a, b)$ and $y = (c, d)$ and b associates with a, d (in particular: if t, or y, is a niner, or if $t_{0,...,7} = 0$), then $\overline{t}\overline{y} = \overline{yt}$.
(See also theorem 31.)

Proof: As our starting point we use theorem 8, showing $\overline{t}\overline{y} = \overline{yt}$ is true in the *Cayley-Dickson* 2^n-ons. Compare EQ 48 with EQ 72 to realize that the 16-ons are the same as the sedenions except for the replacement of $\overline{a}d$ by $\overline{a}b^{-1} \cdot bd$ in the last 8 coordinates. If b associates with a and d then (by the Moufang-Artin diassociativity theorem for octonions) these two terms are the same and we get full-power antiautomorphism for 16-ons also. Otherwise, we claim that, for octonion a, b, d, the identity

$$\mathrm{re}(\overline{a}b^{-1} \cdot bd) = \mathrm{re}(\overline{a}d) \tag{86}$$

holds. Proof:

$$\langle \overline{a}b^{-1} \cdot bd, 1\rangle = |b|^{-2}\langle bd, ba\rangle = \langle d, a\rangle = \langle \overline{a}d, 1\rangle. \tag{87}$$

Therefore, the first of the 8 suspect coordinates is ok. Q.E.D.

Theorem 45 (Quadraticity). *Any 16-on x obeys EQ 49.*

Proof: Consider the fact (see the proof of the next theorem) that the 16-on multiplication formula, when being used to compute powers of x, is *equivalent* to the unmodified Cayley-Dickson formula. Since all the Cayley-Dickson algebras are quadratic [226], the 16-ons are also. Q.E.D.

Theorem 46 (Power associativity). *The 16-ons are power-associative, i.e. if x is a 16-on then x^n is unambiguous (doesn't care how $xxx \ldots x$ is parenthesized) for any integer n.*

Proof: Follows from the diassociativity of the octonions. Let $x = (a, b)$ be a 16-on regarded as an ordered pair of octonions. Then everything inside $(a, b)^n$ is a rational function of only *two* octonions a and b. So diassociativity allows us to reparenthesize every term in the final expression for $(a, b)^n$ in any way we please, just as though the components a and b had been quaternions instead of octonions. (This also means that our 16-on multiplication formula in this case always acts the same as the *un*modified Cayley-Dickson formula.) Thus the (known) fact that the octonions (pairs of quaternions) are power-associative is equivalent to the fact we are trying to prove that the 16-ons (pairs of octonions) are, and to the (also known [226]) fact that the sedenions are. Q.E.D.

Remark. For yet more proofs of power associativity for 16-ons (besides theorem 19), see the proof of lemma 52 and claim 9 in the proof of theorem 60.

13 What about the impossibility theorems?

Theorems showing the "impossibility" of 16-ons with a multiplicative norm, or of 16-ons that form a division algebra, and theorems showing the uniqueness of the reals, complexes, quaternions, and octonions, have, so far, come from two kinds of arguments: algebraic and topological arguments.

13.1 Algebraic arguments

All previous algebraic impossibility arguments known to us depended heavily on the distributive property of multiplication, and in some cases on its associative, commutative, or alternative properties. The 16-ons, since they are *non*distributive (and non- all the others), evade all these impossibility theorems.

However, we've seen in theorems 43 and 35 that the 16-ons obey weakened – but still quite strong – distributivity and alternativity properties. We shall show in §15 that these algebraic properties *characterize* the 16-ons, i.e. they are the unique 16-real-dimensional and 2-octonion-dimensional rational algebraic structure satisfying them. As a side effect of this demonstration, we shall see how to *extend* previous algebraic impossibility theorems to make them show that the reals, complexes, quaternions, octonions, *and* 16-ons are the only algebraic structures satisfying certain properties.

13.2 Topological arguments

The topological arguments have depended [124][94] on such theorems as the following:

1. Let svf(n) be the maximum number of smooth vector fields that can exist on, and be tangent to, the sphere $S^{n-1} = \{\vec{x} \,|\, \vec{x} \in \mathbb{R}^n, |\vec{x}| = 1\}$, such that all n of the vectors are everywhere mutually orthogonal. (So obviously svf$(n) \le n-1$.) Adams [2] showed
$$\text{svf}(n) = 8\alpha + 2^\beta - 1 \tag{88}$$
if $n = u2^{4\alpha+\beta}$, where α, β, u are integers with $0 \le \alpha$, $0 \le \beta \le 3$, u odd. (All of these are achieved by bilinear constructions.) Thus the naive upper bound $n-1$ is tight exactly when $n \in \{1, 2, 4, 8\}$.
2. Hopf [130] showed that if there exists a continuous mapping $S^{n-1} \times S^{n-1} \to S^{n-1}$ obeying $f(-a, b) = f(a, -b) = -f(a, b)$, then n is a power of 2; Adams [1][4][96][98] used "secondary cohomology theory" to show that if there exists a continuous mapping $S^{n-1} \times S^{n-1} \to S^{n-1}$ with a 2-sided identity e, i.e. such that $f(e, b) = b$, $f(a, e) = a$, then $n \in \{1, 2, 4, 8\}$.

These topological arguments break down for the 16-ons, because the 16-on multiplication formula (EQ 72) is *not* an everywhere-smooth map from $\mathbb{R}^{16} \times \mathbb{R}^{16}$ to $\mathbb{R}^{16}$, and (if restricted to the unit-norm case) it is *not* an everywhere-smooth map from $S^{15} \times S^{15}$ to S^{15}. Instead the 16-on multiplication $(a, b)(c, d)$ where a, b, c, d are octonions, is *dis*continuous at $b = 0$, yielding different results if b approaches 0 in different directions. If, however, $b \ne 0$, then the 16-on multiplication map (EQ 72) *is* smooth.

So there is an 8-dimensional subspace, call it $\mathbb{R}^8$, such that the 16-on multiplication map is smooth exactly on $(\mathbb{R}^{16} - \mathbb{R}^8) \times \mathbb{R}^{16} \to \mathbb{R}^{16}$. If we restrict to the unit norm case, it is smooth exactly on $(S^{15} - S^7) \times S^{15} \to S^{15}$.

We will now construct counterexamples to illustrate how these topological arguments can completely lose their force in the presence of various kinds of discontinuities[41].

First, let us discuss a case in which the discontinuity is apparently the mildest possible kind, namely it occurs only at a single point, rather than a subspace.

Theorem 47 (Vector fields on sphere minus 1 point). *For each $n \ge 1$, there exist $n-1$ mutually orthonormal smooth vector fields on S^{n-1}, all tangent to S^{n-1},* except *that these fields have a single non-continuous point. (We can also get n such fields by adjoining the radially-outward unit vector in $\mathbb{R}^n$; this extra field is not tangent to, but rather orthogonal to, S^{n-1}.)*

Proof: Consider the "square grid" yielding $n-1$ mutually orthonormal constant vector fields in $\mathbb{R}^{n-1}$. Now apply stereographic projection to map $\mathbb{R}^{n-1} \to S^{n-1}$. The stereographic projection map is a spherical inversion map in a $\mathbb{R}^n$ containing both the $\mathbb{R}^{n-1}$ and the S^{n-1}, and hence (by Liouville's theorem [166]) is conformal, i.e. preserves angles. Hence, the vector fields are mapped to mutually orthonormal vector fields on S^{n-1}, except at the single "North pole" point which corresponds to ∞ in $\mathbb{R}^{n-1}$ (and at this point we assign an arbitrary set of mutually orthonormal vectors). Q.E.D.

Theorem 48 (Multiplication-like maps I). *If $n \ge 2$, there is a "multiplication" map $a \circ b = c$, where $a, b, c \in S^{n-1}$, with the two sided identity element $e = (1, 0, 0, \ldots, 0, 0)$, which is smooth everywhere on $S^{n-1} \times S^{n-1}$ except at a single point p on one of the S^{n-1}'s, i.e. it is smooth exactly on $(S^{n-1} - p) \times S^{n-1}$. This map, if a is fixed but b is variable, is 1-to-1.*

Proof: Create n mutually orthonormal n-vector fields on $S^{n-1} \subset \mathbb{R}^n$ as in the preceding theorem. Actually, it is best to view this as a $n \times n$ *matrix*-valued field $M(x)$, $x \in S^{n-1}$. Then $M(x)$ is smooth at all $x \in S^{n-1}$ except for the single point $x = p$, and $M(x)$ has orthonormal rows and columns: $M(x)^T M(x) = M(x) M(x)^T = I_{n\times n}$. The first column of $M(x)$ is always x itself (the radially-outward-pointing unit vector), and without loss of generality (by postmultiplication of $M(x)$ by some constant $n \times n$ orthogonal matrix Q, namely $Q = M(e)^{-1}$) we may assume that $M(e) = I_{n\times n}$. Then let

[41] But see §22 for ways to keep topology alive even when there are (certain kinds of) discontinuities. Specifically see our notion of "generalized smoothness."

the "multiplication" operation $c = a \circ b$ be the matrix-vector multiplication $c = M(a)b$. Q.E.D.

The domain of definition of this multiplication map may, of course, be readily extended to $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ by simply using

$$c = |b|(\frac{a}{|a|} \circ \frac{b}{|b|})|a| \, ; \tag{89}$$

it is then smooth everywhere except when a is a non-negative real multiple of p, and it causes the Euclidean norm to be multiplicative. The map admittedly does not exhibit many of the properties commonly associated with "multiplication" – e.g. it lacks commutativity, associativity, and distributivity, and it is non-rational – but it does retain the following: there is a unique 0 and a unique two sided identity 1; and the map is right-linear.

Another property that this map $c(a, b)$ lacks is commutativity with unary negation, i.e., it does not satisfy

$$c(-a, b) = c(a, -b) = -c(a, b). \tag{90}$$

It is possible to redefine our counterexample so that it *does* obey (EQ 90) – provided we now accept more than 1 bad point. It suffices to make our matrix-field $M(x)$ obey $M(-x) = -M(x)$.

The proof is the same, except that instead of basing everything on the "stereographic projection" bijective map $\mathbb{R}^{n-1} \leftrightarrow S^{n-1}$, we instead employ Mercator's "cylindrical conformal projection" bijective map $C^{r-1,s} \leftrightarrow S^{n-1}$, where $r \geq 1$ and $s \geq 1$ are integers with $r + s = n$, and

$$C^{r-1,s} = \{(\vec{x}, \vec{y}) \,|\, \vec{x} \in \mathbb{R}^r, \, |\vec{x}| = 1, \, \vec{y} \in \mathbb{R}^s\} \tag{91}$$

is the surface of an infinitely long n-dimensional cylinder of unit radius inside $\mathbb{R}^n$, having r "radial" directions and s "axial" directions. To be precise, if $(\vec{z}, \vec{\ell})$ is on S^{n-1}, where $|\vec{\ell}|^2 + |\vec{z}|^2 = 1$, then

$$\vec{x} = \frac{\vec{z}}{|\vec{z}|} \quad \text{and} \quad \vec{y} = \mathrm{gd}^{-1}(|\vec{\ell}|)\frac{\vec{\ell}}{|\vec{\ell}|}. \tag{92}$$

Here gd is the "Gudermannian" function [254], defined by

$$\mathrm{gd}(Y) = \arctan(\sinh(Y)) = 2\arctan(\tanh(\frac{Y}{2})). \tag{93}$$

$$\mathrm{gd}^{-1}(L) = \ln(\tan(L)+\sec(L)) = \ln\tan(\frac{\pi}{4}+\frac{L}{2}) = \frac{1}{2}\ln\frac{1+\sin Y}{1-\sin Y}$$

$$\frac{\mathrm{d}}{\mathrm{d}x}\mathrm{gd}(x) = \mathrm{sech}(x), \quad \frac{\mathrm{d}}{\mathrm{d}x}\mathrm{gd}^{-1}(x) = \sec(x).$$

There is now an s-dimensional subspace of $\mathbb{R}^n$, which, wherever it intersects S^{n-1}, leads to a bad point, i.e. a point where the vector fields are discontinuous. There is thus an S^{s-1} of bad points on our S^{n-1}. If $r = n - 1$ and $s = 1$ that means there are two bad points on S^{n-1}, the "North pole" and the "South pole" which correspond to the two ends of the cylinder at $t = \pm\infty$; for general r and s the bad points correspond to the S^{s-1} of infinitely distant parts of the cylinder.

The role of the square grid, giving $n - 1$ orthonormal vector fields in flat space $\mathbb{R}^{n-1}$, is now taken over by the square grid "wrapped" around the cylinder, giving $n - 1$ orthonormal vector fields on C^{n-1}, *except* that we agree to make the s axially-pointing vectors *discontinuously reverse their direction* when $\vec{y} = \vec{0}$. I.e. these s fields go "bad" on an r-dimensional subspace of R^n, which, where it intersects $C^{r-1,s}$, forms an S^{r-1}. In that case, the matrix-field $M(x)$ we get on $x \in S^{n-1}$ indeed obeys $M(-x) = -M(x)$, but s of its columns discontinuously reverse sign on a bad S^{r-1}, and all n columns of $M(x)$ are discontinuous on a bad S^{s-1} (which corresponds to the subspace of $\mathbb{R}^n$ orthogonally complementary to the subspace containing the bad S^{r-1}).

We conclude:

Theorem 49 (Multiplication-like maps II). *Let $r \geq 1$ and $s \geq 1$ be integers with $r+s = n$. Then there is a "multiplication" map $a \circ b = c$, where $a, b, c \in S^{n-1}$, with the two sided identity element $e = (1, 0, 0, \ldots, 0, 0)$, which is smooth everywhere on $S^{n-1} \times S^{n-1}$ except when a lies on an S^{r-1} or on the orthogonally-complementary (and hence disjoint) S^{s-1}, i.e. it is smooth exactly on $(S^{n-1} - [S^{r-1} \cup S^{s-1}]) \times S^{n-1}$, where*

$$S^{r-1} \cup S^{s-1} = \{(\vec{x}, \vec{y}) \,|\, \vec{x} \in \mathbb{R}^r, \, \vec{y} \in \mathbb{R}^s, \text{ such that } |\vec{x}|^2 + |\vec{y}|^2 = 1 \text{ and } |\vec{x}| = 1 \text{ or } |\vec{y}| = 1\}. \tag{94}$$

The first r (of the n total) coordinates of c, however, are smooth except when a lies on the S^{s-1}. This map, if a is fixed but b is variable, is 1-to-1. It obeys $(-a) \circ b = a \circ (-b) = -(a \circ b)$.

Summary: Although it may be possible in the future to get topology-based impossibility statements about "multiplication" in $\mathbb{R}^n$ where the multiplication map is allowed to have certain kinds of discontinuities, the topological theorems available today seem not powerful enough to do that. Theorems 48 and 49 suggest investigating the limits on any such result, which all would be a future line of topological investigation; see open problem #3 in §30.

For comparison, here are the relevant topological properties of the 16-ons. (A goal for future topologists should be to try to prove these properties best possible, and prove the impossibility of dimensions$\neq 2^n$.)

Theorem 50 (Topological properties of 16-ons). *Let x be a unit-norm 16-on, also regarded as a unit-vector in $\mathbb{R}^{16}$, i.e. as a point on S^{15}. Let e_1, e_2,..., e_{15} denote the (mutually orthonormal) imaginary unit 16-ons. Then the 15 vector fields xe_1, xe_2,..., xe_{15} are mutually orthonormal for all $|x| = 1$, and all are tangent to the S^{15}, i.e. orthogonal to x itself. The first 8 of these fields are smooth for all $x \in S^{15}$. The last 7 are smooth for all $x = (a, b)$ where a and b are octonions with $b \neq 0$, i.e. smooth for $x \in S^{15} - S^7$. Also, the first 9 coordinates (among the 16 total) of all 15 of these vector fields, are smooth for all $x \in S^{15}$. All of these fields $v_k(x)$ obey $v_k(-x) = -v_k(x)$.*

Proof: Right-linearity and norm-multiplicativity cause the orthonormality of 1, e_1, e_2,..., e_{15} to remain unaffected by left-multiplication by x. (Also, this follows from the orthogonal nature of the $M(x)$ matrix in EQ 57.) If $x = (a, b)$, the term $ab^{-1} \cdot bd$ in the 16-on-multiplication formula (EQ 72) leads to the discontinuities when $b = 0$, but these discontinuities can only affect the last 8 coordinates of our output vector fields – indeed only the last 7 due to EQ 86 – and if $k \leq 7$ then $d = 0$ and if $k = 8$ then $d = 1$, in either case causing $ab^{-1} \cdot bd = ad$ (by octonion diassociativity), which is smooth. Q.E.D.

14 Impossibility of "better" 16-ons

In this section we shall exhibit various ways in which attempts to make "better" 16-ons are doomed to failure. We need some ground rules about what "16-ons" are, so throughout *this* section we adopt the following

Assumptions: Let "16-ons" mean an arbitrary 16 dimensional nnacd-algebra over $\mathbb{R}$,

1. having a conjugation operation $x \to \overline{x}$ that is linear ($\overline{a+b} = \overline{a} + \overline{b}$), self-inverse ($\overline{\overline{x}} = x$), and norm-preserving ($|\overline{x}|^2 = |x|^2$), such that $x\overline{x} = \overline{x}x$ is pure-real, and such that $\overline{s} = s$ if s is real;
2. whose multiplication operation both is right-linear $[x(y+z) = xy + xz]$, and causes the Euclidean norm to be multiplicative ($|a|^2|b|^2 = |ab|^2$), and obeys $hs = sh$ if h is a 16-on and s is a real.

Let us first discuss these assumptions, their immediate consequences, and possible replacement assumption-sets.

Lemma 51 (16-on norm). *In 16-ons satisfying the above assumptions,* $x\overline{x} = |x|^2$.

Proof: By realness, $x\overline{x} = \pm|x|^2$ and since $s\overline{s} = s^2 > 0$ if s is real, the sign must be $+$, and cannot ever change to $-$, because $x \to \overline{x}$, being linear, is a smooth function, and so is $x \to |x|^2$, since it is the Euclidean norm, and both are nonzero everywhere where $x \neq 0$. Q.E.D.

Hence there is automatically a 2-sided inverse $x^{-1} = \overline{x}(x\overline{x})^{-1}$ and a 2-sided identity 1. In the other direction, the existence of a 2-sided inverse (combined with norm-multiplicativity and real-commutation) implies the existence of a self-inverse conjugation operation $\overline{x} = x^{-1}|x|^2$, albeit perhaps not a linear one.

Lemma 52 (Weak linearity). *In the above assumption list, we can* drop *the first set of assumptions, about the existence and properties of a conjugation operation $x \to \overline{x}$, and instead merely assume our 16-ons have an identity* 1 *and obey weak-linearity, and that if i is a pure-imaginary 16-on (i.e. $\langle i, 1\rangle = 0$) then i^2 is some real-linear combination of* 1 *and* i.

Proof: Define the real part of a 16-on via $\operatorname{re} x = \langle x, 1\rangle$, then *define* $\overline{x} = 2\operatorname{re}(x) - x$, and $\operatorname{im} x = x - \operatorname{re} x$, and then $|x|^2 = |\overline{x}|^2$, $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{s} = s$ for s real, $\overline{\overline{x}} = x$, $\operatorname{re} x = \operatorname{re} \overline{x}$, and $|x|^2 = (\operatorname{re} x)^2 + |\operatorname{im} x|^2$ follow. Then $x\overline{x} = (\operatorname{re} x)^2 - (\operatorname{im} x)^2 = \overline{x}x$ follows from weak-linearity and real-commutativity. Then the realness of $x\overline{x}$ would be implied by the realness of squares i^2 of pure-imaginary 16-ons i. But the 2-dimensional nnacd-algebra of quantities $a + bi$, where a and b are real, is necessarily distributive (implied by 2-dimensionality, weak-linearity, and real-commutativity), with identity, and norm-multiplicative, and hence by Hurwitz's theorem [134][135][147][227][94], is necessarily isomorphic to the complex numbers $\mathbb{C}$. Therefore i^2 is indeed real (and non-positive), and, furthermore, weak-linear 16-ons are necessarily power-associative and power-distributive. Q.E.D.

Lemma 53 (Another assumption set). *If in a nnacd-algebra*

1. $x\overline{x} = \overline{x}x = \langle x, x\rangle$ *(norm)*
2. $\langle yx, z\rangle = \langle x, \overline{y}z\rangle$ *(right-linearity)*
3. $\overline{y} \cdot yx = \overline{y}y \cdot x$ *(left-cancellation)*
4. $sh = hs$ *if s is real (real-commutativity)*

then the norm-multiplicativity law $\langle x, x\rangle\langle y, y\rangle = \langle xy, xy\rangle$ holds.

Proof: This lemma is proposition 1 page 8 of the book [189] by S.Okubo. Let $z = yx$. Then $\langle yx, yx\rangle = \langle yx, z\rangle = \langle x, \overline{y}z\rangle$ by #2. And $\overline{y}z = \overline{y} \cdot yx = \langle y, y\rangle x$ by #3. So $\langle yx, yx\rangle = \langle x, \langle y, y\rangle x\rangle = \langle y, y\rangle\langle x, x\rangle$. Q.E.D.

Second, let us discuss impossibility results about 16-ons satisfying the above assumptions.

Theorem 54 (Distributivity impossible). *Distributive 16-ons are impossible.*

Proof: Hurwitz's theorem [134] of 1898 says that a distributive algebra with identity and causing the Euclidean norm to be multiplicative, must be the reals, complexes, quaternions, or octonions. (Proofs of Hurwitz's theorem may be found in [227], chapter 17 of [147], [94], and see claim 10 in our proof of theorem 60.) Even without any assumption that an identity 1 exists, Hurwitz showed the dimension must be $1, 2, 4, 8$. Q.E.D.

Theorem 55 (Antiautomorphism impossible). *16-ons obeying the antiautomorphism identity $\overline{a}\overline{b} = \overline{ba}$ are impossible. Equivalently, unit-norm 16-ons cannot satisfy $a^{-1}b^{-1} = (ba)^{-1}$.*

Proof: By right-linearity and linearity of the $x \to \overline{x}$ operation, $\overline{a}\overline{b}$ is linear in b. Similarly $\overline{ba}$ is linear in a. Therefore antiautomorphism would imply that ab is linear in both a and b, i.e. that multiplication is distributive. But this contradicts the previous theorem. Q.E.D.

Theorem 56 (LR-alternativity impossible). *16-ons can exist obeying either the left-alternative $x \cdot xy = xx \cdot y$ or right-alternative $yx \cdot x = y \cdot xx$ law, but in 16-ons whose generic multiplicative structure is that of a loop (in the sense of the remark after theorem 71) it is impossible to satisfy both.*

Proof: Obviously, having 1-sided alternativity and a 1-sided cancellation law both are possible, since the 16-ons we've already constructed do the job. The only difficulty is to show that both alternativity laws cannot hold simultaneously.

Any two of the laws $x \cdot xy = xx \cdot y$, $yx \cdot x = y \cdot xx$ and $x^{-1}y^{-1} = (yx)^{-1}$ implies the third in a loop. Here is the proof of that (supplied by Orin Chein): Left alternativity and $(xy)^{-1} = y^{-1}x^{-1}$ imply $[xx \cdot y]^{-1} = [x \cdot xy]^{-1}$, so $y^{-1}[x^{-1}x^{-1}] = [y^{-1}x^{-1}]x^{-1}$. Putting $w = x^{-1}$ and $z = y^{-1}$, we get $z \cdot ww = zw \cdot w$ (right alternativity). Similarly we can go in the other direction. Finally, it is well known ([47], ch. VII) that left and right alternativity imply full-alternativity, i.e. that we have a Moufang loop, and that in Moufang loops we have $x^{-1}y^{-1} = (yx)^{-1}$. (End of Chein's proof.)

But $x^{-1}y^{-1} = (yx)^{-1}$ contradicts the previous theorem. Q.E.D.

Theorem 57 (Cancellation impossible). *16-ons can exist obeying either the left-cancellation $x \cdot x^{-1}y = xx^{-1} \cdot y = y$ or right-cancellation $yx \cdot x^{-1} = y \cdot xx^{-1} = y$ law, but it is impossible to satisfy both.*

Proof: They exist, since our 16-ons do the job. The only difficulty is to show that both cancellation laws cannot hold simultaneously.

As Moufang ([181] p.418; also see our footnote 16) pointed out in her original paper about alternativity, the left and right cancellation laws taken together (plus the assumption that every nonzero element has a 2-sided inverse) imply that ab^{-1} and ba^{-1} are inverses. But that contradicts theorem 55. Q.E.D.

Remark. If we also assume weak-linearity and that $\overline{x} - x$ is pure-real, the left-alternative law and left-cancellation law imply each other, and the right-alternative law and right-cancellation law imply each other.

In that case, theorems 56 and 57 show that fully-alternative 16-ons are impossible – but now without any assumption of loop-ness, but instead as a consequence of weak-linearity.

Theorem 58 (Moufang-ness). *It is impossible for 16-ons whose generic multiplicative structure is that of a loop (in the sense of the remark after theorem 72) to obey any Moufang identity (EQ 11).*

Proof: Any Moufang identity is known ([47], ch. VII; [177]) to imply all the others in a loop. These in turn (by taking one of the variables to be 1) imply antiautomorphism, which, theorem 55 showed, is impossible. Q.E.D.

Theorem 59 (Few coordinates). *16-ons which are ordered pairs of octonions, and whose multiplication operation is expressed in terms of octonionic rational operations and conjugation, cannot obey the distributive identity, the antiautomorphism identity, both the left and right alternativity identities, or a Moufang identity in more than 1 octonionic and 1 real coordinate (9 coordinates total). Indeed, none of these identities can even be obeyed in coordinates* 0, 8, *a, and b alone (4 coordinates total) for any fixed* a, b *with* $1 \le a < 8 < b \le 15$.

Proof: The G_2 automorphism group of the octonions (see §28) causes all 7 imaginary coordinates of an octonion to be equivalent. Thus by applying an appropriate automorphism of the octonions we would see that validity of an identity in coordinate 0 and a would imply validity in coordinates 0 and a' for any a' with $1 \le a' \le 7$. So just obeying any one of these identities in the 4 coordinates mentioned would imply it must be obeyed in all 16 coordinates, which according to the previous theorems is impossible. Q.E.D.

15 Characterization of 16-ons as uniquely optimally distributive

Assumptions. Throughout *this* section, "16-on" means a 16-dimensional nnacd-algebra over the reals which is

1. weak-linear [$a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ if at least one of a, b, or c is pure-real],
2. real-commutative [$hr = rh$ if r is pure-real],
3. right-linear [$a(b+c) = ab+ac$]
4. with unit (1),
5. whose multiplication has left-cancellation ($a \cdot a^{-1}b = b$)
6. and causes the Euclidean norm to be multiplicative ($|ab|^2 = |a|^2|b|^2$).

We've already seen in §14 that such 16-ons *cannot* have right-cancellation, be antiautomorphic, or be left-linear – even in coordinates $1, 8, a, b$ only. But we would like for them to be *as nearly* linear as possible.

In the below, we shall number 16-on coordinates from 0 to 15, with the octonion subalgebra being in coordinates 0-7. We now exhibit a precise sense in which *our* 16-ons are the uniquely "most linear possible" 16-ons.

Theorem 60 (Uniqueness and optimality of our 16-ons). *Let H be a nnacd 16-on algebra (obeying the Assumptions above) such that H contains the octonions as an 8-dimensional subalgebra, and H's multiplication operation is (regarding each 16-on as an ordered pair of octonions) expressible as two octonionic rational functions of the 4 involved octonions and their conjugates. Let H obey the following partial-distributivity properties:*

niner distributivity *If z is a niner, or if both x and y are niners, then* $(x+y)z = xz + yz$

octonion distributivity *If x and y are either*

1. *Both octonions, or*
2. *Both orthogonal to the octonion subalgebra, or*
3. *One is octonion and the other is orthogonal to the octonions,*

then $(x+y)z = xz + yz$.

9-coordinate distributivity *The first 9 coordinates (indices 0-8) of* $(x+y)z$ *are equal to the first 9 coordinates of* $xz + yz$.

Then: There is, up to isomorphism, a unique 16-on algebra, namely ours (i.e. whose multiplication is given by EQ 72).

Remark. Our assumption that H contains an octonion subalgebra in its first 8 coordinates could be *replaced* by, e.g., the weaker assumption that those coordinates contain *some* subalgebra. This algebra necessarily must be fully distributive and left-alternative, and it is known [259][12] that any such algebra which is simple (in particular, which is a division algebra or normed algebra) must be the octonions.

Corollary 61 (Extension to arbitrary fields of characteristic not 2). *Theorem 60 actually holds not only for 16-on nnacd-algebras over the reals, but in fact, over any field* F *with* $\mathrm{char} F \ne 2$.

Proof (of the theorem and corollary). The proof will consist of a numbered sequence of 16 claims, each a consequence of our assumptions and of previous claims. The reader can first verify that it works over $\mathbb{R}$, and then go over it again checking that all steps work over any field F with $\mathrm{char} F \ne 2$. We have put the special mark ♣ in certain places to indicate "here is an occasion where characteristic$\ne$ 2 matters."

1. Let $\langle x, y\rangle = \langle y, x\rangle$ denote the (Euclidean 16D) inner product of x and y; this could be defined in terms of the Euclidean norm $|x|^2 = \langle x, x\rangle$ by $2\langle x, y\rangle = |x+y|^2 - |x|^2 - |y|^2$. There is then a notion of the "real part" of a 16-on: $\mathrm{re}\, x = \langle x, 1\rangle$ and its "conjugate" $\overline{x} = 2\,\mathrm{re}\, x - x$ ♣. Two 16-ons x, y are "orthogonal" if $\langle x, y\rangle = 0$.

2. Norm-multiplicativity implies $\langle ab, ab\rangle = \langle a, a\rangle\langle b, b\rangle$ and then right-linearity (consider $b \to b + d$) implies

$$\langle ab, ad\rangle = \langle a, a\rangle\langle b, d\rangle = |a|^2\langle b, d\rangle. \tag{95}$$

If the 16-ons were fully-distributive, then we could also similarly left-linearize to deduce

$$\langle ab, cd\rangle + \langle ad, cb\rangle = 2\langle a, c\rangle\langle b, d\rangle. \quad \clubsuit \tag{96}$$

It is still legitimate to deduce EQ 96 (thanks to our weakened distributivity assumptions) if either (i) either a or c (or both) are pure-real; (ii) both a and c are niners; (iii) both b and d are niners.

3. $x\overline{x} = \overline{x}x = |x|^2$ =non-negative pure-real is forced by weak-linearity and real-commutativity, see lemmas 51 and 52.

Hence $x^{-1} = \overline{x}|x|^{-2}$; also the quadratic identity EQ 49 follows automatically as in theorem 16.

[Side remark: Left-cancellation would follow automatically, *without* need to assume it, if we had full distributivity. Proof ([147], [227] p.74) involves use of left-linearity $(b+c)a = ba+ca$ to assume wlog that b is pure-imaginary, use of $(x+y)^2 = xx + yy + 2xy$ if x is pure-real (from weak-linearity), use of bilinearity of inner product, and definition of $|b|^2 = \langle b, b\rangle$ and use of EQ 96.]

4. From 3, left-cancellation, and weak-linearity we deduce left-alternativity: $a \cdot ab = a^2b$. Left-cancellation also gives us (by scaling by $|b|^2$) $\overline{b} \cdot ba = |b|^2a$. [Side remark: if H were fully distributive we could by a mirror argument to the above deduce right-cancellation and right-alternativity, and hence full-alternativity.]

5. The 16-on identity

$$\overline{y} \cdot xa + \overline{x} \cdot ya = 2\langle x, y\rangle a = y \cdot \overline{x}a + \overline{y} \cdot xa \quad \clubsuit \tag{97}$$

must hold *if* at least one of $\{x, y\}$ is pure real, or if both x and y are niners, or if x is octonion and y is orthogonal to the octonions, or if both x and y are orthogonal to the octonions. This follows from (and implies) $\overline{b} \cdot ba = b \cdot \overline{b}a = |b|^2a$ (left-alternativity) by linearizing b (take $b = x + y$) using our weakened linearity and distributivity assumptions.

6. Let e be a niner, orthogonal to 1, with $|e|^2 = 1$. Then $\overline{e} = -e$ follows from orthogonality to 1, hence by claim 3 we have $e^2 = -1$. Now let U be a subalgebra of dimension≤ 8 and let e be orthogonal to every element in U ("orthogonal to U" for short). [We shall most commonly have in mind that U is the 8D octonion subalgebra in coordinates 0-7, in which case e has a 1 in coordinate 8 and a 0 in every other coordinate.] Then: Ue and U are orthogonal (follows from EQ 95 with b octonion and $d = e$). Hence the representation of any 16-on in the form $u_1 + u_2e$, $u_1, u_2 \in U$, is unique. Also, eU and U are orthogonal due to legitimate (covered under either case ii or iii) use of EQ 96 with a and $b = d$ octonion and $c = e$. Hence the representation of any 16-on in the form $u_1 + eu_2$, $u_1, u_2 \in U$, also is unique.

7. The following 4 "eye-shift"[42] identities must hold in our 16-ons if $a, b \in U$:

$$eb = \overline{b}e, \quad b \cdot ea = e \cdot \overline{b}a, \quad eb \cdot a = e \cdot ab, \quad eb \cdot ea = -a\overline{b}. \tag{98}$$

These arise from claim 5 and our weakened-linearity assumptions. To get the first just take $y = \overline{b}$, $x = e$, and $a = 1$ in EQ 97 (and use the fact that $\langle e, b\rangle = 0$ since e is orthogonal to the octonions).

[42] See footnote 22 for why we use this terminology.

The second just comes directly from putting $y = e$ in EQ 97, which is legal since e is a niner. The third arises as follows. In EQ 97 put $a = 1$ and $y = \overline{ev} = -ev$; this last equality arises from the fact that (if v is octonion) ev is perpendicular to the octonions and hence to 1. This is legal since y is orthogonal to the octonions and x is octonion. So we have $ev \cdot x + \overline{x} \cdot ev = 0$. Now use the second identity in EQ 98 to change the second term to $e \cdot xv$, and change the names of the variables.

To get the fourth, put $x = e$ and $y = -eb$ in EQ 97 (legal since both are orthogonal to the octonions) to get $eb \cdot ea - \overline{e}(eb \cdot a) = -2\langle e, eb\rangle a = -2a\langle 1, b\rangle\langle e, e\rangle = -2a\langle 1, b\rangle$. Now use $-\overline{e} = e$ and the third identity of EQ 98 to reduce the second term on the left to $+e(eb \cdot a) = e(e \cdot ab)$ and now use left-alternativity to reduce it to $-ab$. So $eb \cdot ea - ab = -2a\langle 1, b\rangle$, which we may rewrite as $eb \cdot ea = ab - 2a\langle 1, b\rangle = a(b - 2\,\mathrm{re}\,b) = -a\overline{b}$ (where we have used right-linearity). ♣

The use of EQ 98 is that it allows re-expressing 2^n-ons with "eyes left" (cf. footnote 22).

[Side note: We shall not use this, but it should also be possible to derive the following

$$ae \cdot b = a\overline{b} \cdot e, \quad a \cdot be = ba \cdot e, \quad ae \cdot be = -\overline{b}a, \tag{99}$$

which are convenient for re-expressing 2^n-ons with "eyes right." These are definitely true if a, b are octonions, as has been confirmed by computer proof (cf. §11).]

8. Now assume that $U + eU$ is also a subalgebra of H, closed under multiplication. This is justified if either

1. $U + eU$ is distributive.
2. $\dim(H) = 2\dim(U)$ in which case $U + eU = H$ (sum of two disjoint vector spaces) is the whole algebra (this holds if U is the octonions and H the 16-ons).
3. $\dim(U) = 1$, i.e. U is isomorphic to the reals, in which case weak-linearity is the same thing as distributivity for $U + eU$ and case 1 applies.

9. Side remark: 8.3 will allow us to conclude the algebra generated by 1 and any pure-imaginary 16-on must be isomorphic to the complex numbers, so our 16-ons must automatically be power-associative and power-distributive.

10. Side remark: If H were fully distributive (and if we drop the demand that it be 16-dimensional) we could use case 8.1 and apply EQ 98 to all 4 terms in the full expansion, via distributivity, of $(a + be)(c + de)$, to conclude that the multiplication in $U + Ue$ must be defined in terms of the multiplication in U via the linear Cayley-Dickson doubling formula EQ 48. This would prove H is the reals, complexes, quaternions, or octonions *only* (since doubling further yields the sedenions which are not a normed algebra) which was, essentially, Hurwitz's theorem (and constitutes a proof of that theorem). This also proves that fully distributive 16-ons are *impossible*, motivating our present theorem's weaker assumptions of "9-coordinate distributivity," etc.

11. But we only have right-linearity, so we only get a weaker result:

$$(a + eb)(c + ed) = (a + eb)c + (a + eb) \cdot ed. \tag{100}$$

12. Now using our assumption of left-linearity $[(x+y)z = xz + yz]$ *if* z is niner (here $z = c$), and also using EQ 98, we can simplify further to get

$$= ac + eb \cdot c + (a + eb) \cdot ed \quad (101)$$

$$= ac + e \cdot cb + (a + eb) \cdot ed. \quad (102)$$

Note: it would not be legal to continue by trying to shift the e in the last term leftward by use of EQ 98, because $\overline{a+eb}$ is not an octonion, i.e. not in U. However, if $a = 0$ the last term simplifies to $-d\overline{b}$, while if $b = 0$ it simplifies to $e \cdot \overline{a}d$. Note the agreement of all of these with the 4 terms in the Cayley-Dickson formula EQ 48.

13. This tells us that our 16-on-multiplication formula must agree with the Cayley-Dickson sedenion formula (EQ 48) if either $a = 0$ or $b = 0$, and indeed (by weak-linearity and niner-distributivity) merely if any of $\{a, b, d\}$ are real.

14. So at this point, we've reached the following conclusions. Our assumptions force us to have a rationally-modified Cayley-Dickson formula, such that the modifications have no effect if any of $\{a, b, d\}$ are real, and such that only the 2 terms in EQ 48 not involving c, are modified, and those modifications must not introduce any involvement of c.

But now consider 9-coordinate distributivity. This forces the first 9 coordinates of the product 16-on to be determined by a truly-bilinear formula, and (by considering $a = 0$ and employing EQ 98; cf. claim 13) that formula must be in agreement with the Cayley-Dickson formula EQ 48. So, our 16-on-multiplication formula *must* be

$$(a,b)(c,d) \;=\; (ac - d\overline{b},\; cb + \text{modification}(\overline{a}d)). \quad (103)$$

The modification is permitted to involve b, but not c (due to right-linearity), and must have no effect if any of $\{a, b, d\}$ are pure-real octonions, and it must always have the same real-part as $\overline{a}d$ (by 9-coordinate distributivity; this is the 9th coordinate). It must be a purely-linear function of d (by right-linearity).

15. Now consider the requirement that the Euclidean norm be multiplicative:

$$|(a,b)|^2 |(c,d)|^2 = |(a,b)(c,d)|^2. \quad (104)$$

The left-hand side of this is

$$(|a|^2 + |b|^2)(|c|^2 + |d|^2) = |a|^2|c|^2 + |b|^2|d|^2 + |b|^2|c|^2 + |a|^2|d|^2. \quad (105)$$

The right-hand side, writing $M = \text{modification}(\overline{a}d)$, is

$$|ac|^2 + |d\overline{b}|^2 - 2\langle ac, d\overline{b}\rangle + |cb|^2 + |M|^2 + 2\langle cb, M\rangle \quad (106)$$

which is

$$|a|^2|c|^2 + |b|^2|d|^2 + |b|^2|c|^2 + |M|^2 - 2\langle c, \overline{a} \cdot d\overline{b}\rangle + 2\langle cb, M\rangle. \quad (107)$$

(We have used the octonion properties that $\langle xy, z\rangle = \langle x, z\overline{y}\rangle$, $|\overline{x}|^2 = |x|^2$.) Hence, for EQ 104 to hold we need that $|a|^2|d|^2 = |M|^2 + 2\langle cb, M\rangle - 2\langle c, \overline{a} \cdot d\overline{b}\rangle$ or equivalently that $|a|^2|d|^2 = |M|^2 + 2\langle cb, M\rangle - 2\langle cb, (\overline{a} \cdot d\overline{b})\overline{b^{-1}}\rangle$. The obvious solution is to choose

$$M = (\overline{a} \cdot d\overline{b})\overline{b^{-1}} = (\overline{a} \cdot db^{-1})b = \overline{a}b^{-1} \cdot bd = b^{-1}(b\overline{a} \cdot d) \quad (108)$$

with $|M|^2 = |ad|^2$. (We've used the Moufang-like law EQ 16 here to get several equivalent formulas for M.) We now claim that this obvious solution is the *only* solution. This is since any other solution M' would have to be $M' = M + f(a, b, d)$, and, no matter what $f \neq 0$ you choose, an adversary can then obtain a contradiction by choosing c to defeat that f, i.e. to cause $|f|^2 + 2\langle f, M\rangle + 2\langle cb, f\rangle \neq 0$.

16. So, in conclusion, the only possible 16-on-multiplication formula consistent with our assumptions (and it *is* consistent with them, as we've seen in the rest of this monograph) is

$$(a,b)(c,d) \;=\; (ac - d\overline{b},\; cb + \overline{a}b^{-1} \cdot bd). \quad (109)$$

This is exactly our EQ 72. Q.E.D.

16 Uniquely optimal 2^n-ons, and the simplest formula for them

It is possible to simplify our 2^n-on multiplication/doubling formulae EQ 57 and EQ 68 by applying the algebra isomorphism $(x, y)_{\text{new}} = (x, \overline{y})_{\text{old}}$. Then they respectively become

$$\begin{pmatrix} A & -KB^T \\ BK & BKA^TKB^{-1} \end{pmatrix} \quad (110)$$

and[43]

$$(a,b)(c,d) = (ac - \overline{\overline{b}d}, b\overline{c} + b\overline{\overline{a}\,\overline{b^{-1}d}}). \quad (111)$$

Again in the special case where B is non-invertible or $b = 0$, then use

$$\begin{pmatrix} A & -KB^T \\ BK & KA^TK \end{pmatrix}, \qquad (ac, \overline{\overline{a}\,\overline{d}}) \quad (112)$$

respectively. These appear to be the **simplest possible formulae for our 2^n-ons**. One precise quantifiaction of "simplest" is this:

Lemma 62 (Simplest I). *Among all 16 possible isomorphic versions of our 2^n-on doubling formula EQ 111 gotten by agreeing to conjugate and/or negate either (or both, or neither) 2^{n-1}-on half of our 2^n-ons, the one with the fewest number of conjugation bars and the fewest minus signs is EQ 111.*

Proof: Exhaustive examination. Q.E.D.

But: although EQ 111 seems "simplest" in the sense that the fewest possible conjugation-bars are involved, for other reasons I have preferred the "more complicated" EQ 68 throughout this monograph. See §32.1 for discussion.

For the purpose of defining *16-ons*, as opposed to general 2^n-ons, there are many more possible equivalent (up to algebra isomorphisms) ways to rewrite EQ 111. The 4-term product may be rewritten in any of 3 equivalent ways by using the Moufang identity, e.g. see EQ 108. Then one may apply the antiautomorphism identity $\overline{ty} = \overline{y}\,\overline{t}$ (or not) to every octonion-multiplication. Since there are 6 such multiplications in the formula, that is $3 \times 2^6 = 192$ possible variations. Finally, as in lemma 62, each of these 192 may be rewritten in any of 16 possible ways by agreeing to one of 16 possible algebra isomorphisms involving conjugating and/or negating each octonion half of each 16-on.

[43] The same formula is given in §6.11 of J.H.Conway and D.Smith's book [67] (I suggested it to them after they consulted me about the best such formula) although they mistakenly omitted the acknowledgment of that formula to me!

Lemma 63 (Simplest II). *Among the* $192 \times 16 = 3072$ *definitions of 16-ons from octonions described above (all equivalent), there is one which (i) has the fewest possible conjugation bars, (ii) has the fewest possible minus signs, (iii) bears the greatest resemblance (in the sense it exactly agrees with 3 of the 4 terms in, and the 4th term most resembles) to the Cayley-Dickson doubling formula EQ 48: namely, EQ 72.*
Proof: Exhaustive examination. Q.E.D.

All of these $192 \times 16 = 3072$ formulas are *equivalent* for the purpose of generating 16-ons from octonions. *However*, if these formulae are reused to generate 2^n-ons for $n \geq 5$, then each of the 192 isomorphism-equivalence classes among these 3072 formulae generally will *not* be equivalent[44] since the Moufang and antiautomorphism laws are *not* valid (and cannot be valid, see theorems 55 and 58) for 16-ons and their successors.

Theorem 64 (Uniqueness of our 2^n-ons). *Of the 192 equivalence classes among the 3072 (at the* $2^3 \to 2^4$ *doubling) possible ways, described above, to rewrite our (unique optimally distributive) 16-on multiplication formula (EQ 111),* exactly one, *namely the 16 isomorphs of EQ 111, continues on to generate* 2^n*-ons for each* $n \geq 4$*, each having multiplicative Euclidean norm. And of these 16, lemma 62 has shown a sense in which EQ 111 is simplest.*
Remark. More detail: Exactly *two* yield 32-ons for which the Euclidean norm is multiplicative, namely EQ 111 and

$$(a,b)(c,d) = (ac - \overline{d}b, b\overline{c} + b\overline{\overline{a} \cdot \overline{d}\,\overline{b^{-1}}}). \tag{113}$$

But EQ 113 produces 32-ons which are not left-alternative and not right-linear, and if it is re-iterated to produce 64-ons, they do not have multiplicative Euclidean norm. Meanwhile, EQ 111 (since it is equivalent to using EQ 110 in the matrix picture of lemma 11) keeps on yielding 2^n-ons, each having multiplicative Euclidean norm, left-alternativity, and right-linearity, forever.

Proof: Computer verification (see §11). This is not merely a probabilistic[45] proof, but a real one, since the computer here is only used to find *counterexamples* to norm-multiplicativity (and that is done with exact arithmetic). The only positive statements we need to prove, namely that EQ 113 and 111 lead to 32-ons with multiplicative norm, may be established manually. For EQ 113, after taking the norm, expanding out both sides, and canceling equal terms, it comes down to showing that

$$\langle ac, \overline{d}b \rangle = \langle b\overline{c}, b\overline{\overline{a} \cdot \overline{d}\,\overline{b^{-1}}} \rangle; \tag{114}$$

which may be done by repeatedly simplifying the right hand side with the aid of theorem 15:

$$= \langle \overline{b} \cdot b\overline{c}, \overline{\overline{a} \cdot \overline{d}\,\overline{b^{-1}}} \rangle \tag{115}$$

$$= \langle \overline{c}, \overline{\overline{a} \cdot \overline{d}\,\overline{b^{-1}}} \rangle \, |b|^2 \tag{116}$$

$$= \langle c, \overline{a} \cdot \overline{d}\,\overline{b^{-1}} \rangle \, |b|^2 \tag{117}$$

$$= \langle ac, \overline{a^{-1}}(\overline{a} \cdot \overline{d}\,\overline{b^{-1}}) \rangle \, |b|^2 \tag{118}$$

$$= \langle ac, \overline{a}^{-1}(\overline{a} \cdot \overline{d}\,\overline{b^{-1}}) \rangle \, |b|^2 \tag{119}$$

$$= \langle ac, \overline{d}\,\overline{b^{-1}} \rangle \, |b|^2 \tag{120}$$

$$= \langle ac, \overline{d}b \rangle. \tag{121}$$

(This in fact shows that any number of doublings using EQ 111, followed by *one* use of EQ 113, yields 2^n-ons with multiplicative norm.) The proof of norm-multiplicativity for EQ 111 is almost exactly parallel (and since we already know EQ 111 is valid, it is omitted). Q.E.D.

Theorem 64 must not be taken too seriously, because there are not merely 192, but in fact ∞ ways to rewrite EQ 72 that are equivalent at the $2^3 \to 2^4$ doubling but inequivalent at higher doublings. Namely, one may use the distributive law (which is valid for octonions but not 16-ons) to rewrite any product xy in it as, e.g., $fy + gy$ where $f + g = x$. Furthermore, one could use the alternative law (also valid for octonions but not 16-ons) to rewrite any xy as $(xy \cdot f)f^{-1}$. We suspect that few or none of these will yield anything interesting that keeps working forever – because they generally stop $x = 1$ from being the identity, and/or destroy niner-distributivity – but we have not proven it, and besides, even if we did prove it, there might be other, undreamt of, kinds of formulae and there might be interesting 2^n-ons which arise in some *other* way than by merely repeating the same kind of doubling formula as was used last time. So it remains possible that, for all sufficiently large n, our prescription for generating 2^n-ons is not the uniquely best one (whatever "uniquely best" might mean).

Indeed, even our 16-on-uniqueness theorem 60 must not be taken too seriously – although it must be taken a good deal more seriously than theorem 64. It shows our 16-ons are uniquely best, but other people might prefer other notions of "best" than the one (based on maximizing partial distributivity properties) we have chosen. See §27 for a comparative survey of 16-on formulas discovered by us or by other people (this survey is necessarily incomplete, since there undoubtably are other, as-yet-unknown, formulas). We will say, though, that "good" 16-on formulas seem rare. During this research I produced over 100 kinds of formulas yielding 16-ons with multiplicative Euclidean norm, but almost none of them have pleasant algebraic properties.

17 Fundamental theorem of algebra for octonions and below

The "fundamental theorem of algebra" states that every univariate polynomial over $\mathbb{C}$ has a root. (A stronger version: every degree-D such polynomial has exactly D roots, if we count multiple roots multiply.)

We (§10) have already seen examples of quaternionic and octonionic polynomials without roots, so this theorem fails to generalize. However, if we restrict the allowed class of polynomials, there *are* valid quaternionic and octonionic fundamental theorems of algebra. Such a theorem was first found by S.Eilenberg and I.Niven [100] in 1944, and our purpose in this section is to produce a considerable strengthening of it[46],

[44] Conceivably, by some coincidence, some of them are still equivalent.
[45] We do not intend by this to disparage probabilistic proofs.
[46] Incidentally, we'll also strengthen the usual fundamental theorem of algebra – over the complex numbers! (See theorem 66.) It seems unlikely that *that* is new, but we have not made any effort to find out.

suitable for later use in proving that division in our 16-ons (or with many alternate definitions of 16-ons) works.

We need to know the definition and basic properties of L.E.J. Brouwer's "topological degree" (a notion apparently tracing back to L.Kronecker in some form). The following list has been extracted from books [6][17][40][72][87][120][124][133][178][239] on algebraic topology.

Topological degree: definition and simplest consequences. Let f be a smooth map from S^n to S^n. More generally degree(f) may be defined for a differentiable map f between two smooth n-dimensional closed oriented manifolds. Degree(f) is an integer. Degree is invariant under homotopies. Degree of the constant mapping (all the manifold is mapped to a single point) or homotopes of it, is 0 by definition. If the map happens to be piecewise linear on simplices, for some triangulation of the two manifolds, and maps simplices to simplices, then, for some simplex S on the target manifold (it does not matter which one)

$$\text{degree}(f) = \qquad (122)$$
$$(\#\text{simplices mapped orientation-preservingly to } S)$$
$$-(\#\text{simplices mapped orientation-reversingly to } S).$$

Also, for any generic point y on the target manifold, it does not matter which,

$$\text{degree}(f) = \sum_{\text{preimages } x \text{ of } y} \text{sign}\left[\text{JacobianDeterminant}(f)_x\right]. \qquad (123)$$

Brouwer-Hopf mapping theorem: Two differentiable selfmaps of S^n are homotopic iff their degrees agree. If f extends to a continuous map from the *ball* B^{n+1} to S^n, then degree(f) = 0. The identity map $f(x) = x$ has degree(f) = 1. The map from x to its reflection in some hyperplane through 0, has degree= −1. For maps from S^1 to S^1, "degree" coincides with "winding number." Behavior under composition: Degree($f(g())$) = degree(f)degree(g). Brouwer's fixpoint theorem: every continuous map $B^n \to B^n$ has a fixpoint. Theorem on the degree of the antipodal map: For the antipodal map $f(x) = -x$ on S^n, $n > 0$, degree(f) = $(-1)^{n+1}$. Theorem: If degree(f) $\neq (-1)^{n+1}$, then f (mapping $S^n \to S^n$) has a fixpoint. Antipode Theorem: If degree(f) $\neq 1$ (note 1 is the degree of the identity map), then f (mapping $S^n \to S^n$) maps x to its antipode $-x$, for some x. Corollary: Any differentiable map f from S^{2k} to S^{2k} either has a fixpoint or maps some point to its antipode. Corollary ("hair combing theorem"): S^n has a smooth tangent vector field iff n is odd. Theorem: If f is a homotopy equivalence then degree(f) = ±1. Borsuk's oddity theorem: If $f(-z) = -f(z)$ then degree(f) is odd, and if $f(-z) = f(z)$ then degree(f) is even.

Example applications: 1. if a,b are fixed nonzero octonions with $|ab| = 1$, and $|x| = 1$, then the map $x \to ax^{-1} \cdot xb$ is a map from S^7 to S^7. It is homotopic to the map $x \to 1$. (To see that, consider slowly distorting (a, b) from $(1, 1)$ to (a, b).) Hence it has degree= 0. Hence, this map has both a fixpoint ($x \to x$) and a point x that is mapped to $-x$. (It seems much more difficult to prove these without help from topology.)

If in this example we were to make a, b and x be 16-ons rather than octonins, then this argument would apparently no longer be valid because this map is not longer smooth on the 15-sphere $|x| = 1$. However, that will be rectified in §22 where we will show how to extend Brouwer-degree theory to "generalized-smooth" maps (with a generalized notion of "homotopy"). This map *is* generalized-smooth, so our reasoning here really is valid even for 16-ons.

2. The octonion map $x \to axb$ (for all x including ∞) is homotopic to the identity map and has degree 1; hence it need not have a fixpoint. The map $x \to a_0 x a_1 x a_2 x a_3 x \cdots a_{m-1} x a_m$ is homotopic to $x \to x^m$, is an m-to-1 map, and has Brouwer-degree m. If some of the x's here are replaced by $\overline{x}$ or x^{-1}, e.g. say there are A x's and B $\overline{x}$'s where $A + B = m$, then this map is homotopic to x^{A-B} and has degree= $A - B$.

Theorem 65 (Fundamental theorem of algebra, plain version). *Let $n \le 3$. Any univariate 2^n-onic polynomial $P(x)$ having a unique monomial of highest-degree $n > 0$, has at least 1 root.*

Proof sketch: This theorem was shown by Eilenberg and Niven [100] in 1944, and we imitate their proof[47]. For simplicity of exposition we shall take $n = 3$ (octonions) in this proof but the argument works for any $n \le 3$. Our polynomial $P(x)$ constitutes a smooth selfmap of $\mathbb{R}^8 \cup \infty$, which is S^8 topologically, due to stereographic projection. Now this map has Brouwer "topological degree" the same as the polynomial degree. This is (1) due to writing explicit easy homotopies in which all the coefficients of the non-dominant terms shrink to 0; and (2) They also need to see that x^n has Brouwer-degree n, for which they (a) rely on a lemma due to Niven and Brand [186] that the equation $i = x^n$ has exactly n roots x (namely, just the complex roots)[48] in the quaternions – and this then plainly is also true in the octonions since any 2 octonions (here x,i) generate a quaternion subalgebra, and (b) They explicitly compute the Jacobian determinant of the map x^n at the roots x of $x^n = i$, then use the definition of topological degree as a sum of Jacobian determinant signs (here all the signs are identical).

With the topological degree now known, it then follows immediately from general theorems of topology that $P(x) = y$ has a solution x for any y. Q.E.D.

We now make several extensions of the Eilenberg-Niven theorem and proof. For some of them we shall need the notion of the *local* topological degree of $f(x)$ at x. Namely, consider a small sphere (of radius r) centered at x: the local topological degree of f at x is then the topological degree of $x + r[f(y) - x]/|f(y) - x|$ for y on that sphere, in the limit (if one exists) $r \to 0$.

Theorem 66 (Extended Fundamental theorem of algebra). *Let $n = 1$, 2, or 3.*

1. *Any univariate 2^nonic polynomial $P(x)$ having a unique monomial of highest-degree $n > 0$, has at least n roots, if roots are counted according to "multiplicity," i.e. local topological*

[47] Eilenberg and Niven actually stated and proved their theorem for quaternions, but noted at the end of their paper that their argument also works for both octonions and complex numbers.

[48] Indeed [186], there are exactly $r \ge 2$ quaternion solutions x to $x^r = q$, where q is any non-real quaternion (or if $r = 2$ and $q > 0$ is real). There are an infinite number of solutions if $q \neq 0$ is real (with $q < 0$ if $r = 2$). If $q = 0$ the unique solution is $x = 0$.

degree. (For generic polynomials, all roots are of degree 1*, so generically there genuinely are* $\geq n$ *roots.)*

2. *Let* $P(x, \overline{x})$ *be a bivariate* 2^n*-onic polynomial with a unique asymptotically dominant term, when* $|x| \to \infty$*, containing* A x*'s and* B $\overline{x}$*'s. Then it has at least* $|A - B|$ *roots* x*.*

3. *In 1 and 2, the uniqueness of the asymptotically dominant monomial is not necessary – all that is really necessary is that the summed equi-dominant monomials (call that* $h(x)$*), is a function of* x *such that* $\lim_{r\to\infty} \min_{x,\,|x|^2=r} |h(x)| = \infty$*. (This ensures continuity on* S^{2^n} *at* ∞ *in* $\mathbb{R}^{2^n}$*.)*

4. *Suppose the topological degree* $|A - B|$ *of* $P(x, \overline{x})$ *is* odd*. Then not only must a root* x *of* P *exist, but in fact a root of "odd local degree" must exist.*

Proof: (1) The topological degree is n implies that $P(x) = y$ has (for generic y) at least n roots x, due to the definition of topological degree as a sum of Jacobian determinant signs. The contribution of generic points in the neighborhood of x to the sign-sum is the local degree of x, and these contributions have to add up to n.

(2) and (3) are similar but the topological degree is $|A - B|$. This also, incidentally, extends the usual (i.e. for complex numbers) fundamental theorem of algebra.

(4) Follows by consideration of the definition of topological degree in terms of signed simplex counting or sum of signs of Jacobian. If x is a root of locally-even degree, then the contribution of $x+\epsilon$, for all sufficiently small-norm generic ϵ, to the sign-sum will be even. Hence, since the total sign sum (which is equal to the topological degree) must be generically odd, it is impossible for all the roots x to be locally-even. Q.E.D.

18 Analysis of some quaternion and octonion equations

Theorem 67 (Quaternionic similitude). *The quaternion equation*

$$x^{-1}tx = b \tag{124}$$

implies $|t| = |b|$ *and* $\operatorname{re} t = \operatorname{re} b$*. These conditions are sufficient for a solution* x *to exist.*

Proof: Barth Pollak [207] considered the quaternion equation $\overline{x}tx = b$ over an arbitrary base field with characteristic$\neq 2$. This is merely the extremely special case of his results that arises by taking $\mathbb{R}$ as the base field.

But it also follows much more simply and directly: With the aid of the understanding of rotations in §4, we see that $t \to x^{-1}tx$ is the identity map on reals and maps pure-imaginary quaternions (regarded as 3-vectors) to arbitrarily rotated versions of themselves. The theorem then follows, and with the additional realization that there are a 1-parameter infinity of norm-1 solutions x if there are any. Q.E.D.

Theorem 68 (A quadratic which generically has exactly 2 roots). *The following kind of quadratic function (where all letters are quaternions and* $ab \neq 0$*):*

$$F(x) = xaxb + xc + dxb + f. \tag{125}$$

has either 1*,* 2*, or* ∞ *roots* x *such that* $F(x) = 0$*. Generically (over the choice of* a, b, c, d, f*) it has exactly 2 roots.*

Proof: If we are interested in the roots of $F(x)$, then it makes no difference to left-multiply and right-multiply $F(x)$ by nonzero constants. Choose 1 and b^{-1} as those constants to see that wlog we may consider only $F(x)$ of the form

$$F(x) = xax + xc' + dx + f'. \tag{126}$$

We may now omit the primes (thus renaming the constants), and from now on we shall perform such renamings of constants without comment. Now we may make a linear change of variables from x to y where $x = pyq$. This does not change the number of roots if $pq \neq 0$. Choose p and q so $qap = 1$ to see that wlog (after re-simplifying by an overall right- and left-multiplication of $F(x)$ by p^{-1} and q^{-1}) we may consider only $F(x)$ of the form

$$F(x) = xx + xb + dx + f. \tag{127}$$

Now change variables via $x = y - d$ to see that wlog we may consider only $F(y)$ of the form

$$F(y) = yy + yc + f. \tag{128}$$

Finally, change variables via $y = z - \operatorname{re}(c)/2$ to see (here we use the fact that reals commute with quaternions) that wlog we need consider only $F(z)$ of the form

$$F(z) = zz + z(c - \operatorname{re} c) + f. \tag{129}$$

which is a quadratic(z) with all coefficients to the right of their powers of z, and with the coefficient of the linear term being pure-imaginary. Theorem 2 of [185] shows that quadratics of the form in EQ 129 have either 1,2 or ∞ roots, with 2 occurring generically – namely: ∞ roots occur iff $c = 0$, and f is real, and $f > 0$. Otherwise: a single root occurs iff $(|c - \operatorname{re} c|^2 + 2\operatorname{re} f)^2 - 4|f|^2 = \overline{f}(c - \operatorname{re} c) - (c - \operatorname{re} c)f = 0$. Q.E.D.

Remark. In particular, if $f = 0$ then EQ 129 cannot have ∞ roots, and its roots are 0 and $c - \operatorname{re} c$.

By the same argument, $F(x)$ is a 2-to-1 map, generically, almost everywhere, of the quaternionic space.

Corollary 69. *The quadratic in EQ 129 still is a 2-to-1 map, generically, almost everywhere, over the* octonions*.*

Proof: The constant term is irrelevant for this kind of consideration, so we may as well consider the map $z \to zz + kz$, and that, since it involves only 2 variables z and k, by diassociativity is living entirely within the quaternion subalgebra generated by z and k, and within said subalgebra must be, generically, 2-to-1. Q.E.D.

Remark. A fully general quaternion (or octonion) univariate quadratic can (if there are enough terms) be a fully general set of 4 (respectively 8) simultaneous quadratic equations over the reals. Hence it is very hard to solve and no "fundamental theorem of algebra" can be hoped for. The following comparatively nice quaternion quadratic

$$q^2 + q(2i + 5j + 7k) - (11 + 17i + 19j + 23k) = 0 \tag{130}$$

has a root $q \approx -3.61 - 2.70i - 4.54j - 7.30k$, all of whose coefficients are expressible as rational functions of the real root Z of $4Z^6 + 112Z^4 - 516Z^2 - 21025$. This cubic in Z^2

has Galois group S_3 and hence the algebraic degree 3 of this q, is irreducible. Thus, quaternionic quadratics of the form (EQ 130) are not soluble by any finite process involving real rational operations and square-rootings only.

Remark. Solving the octonion linear equation $b \cdot ax + bx \cdot a = 0$ for x is discussed in lemma 3.4.2 of [149]. Some other quaternion and octonion equations are discussed in [68].

19 What is a "division algebra" and are the 2^n-ons one?

One (boring) **definition** of "division algebra" is "an algebra in which $xy = 0$ implies $x = 0$ or $y = 0$." By that definition, all of our 2^n-ons are nnacd "division algebras" simply because of the multiplicativity of Euclidean norm.

A **stronger definition** of "division algebra" is "an algebra in which, given b and given $a \neq 0$,

1. there exists z so that $az = b$, and
2. there exists q so that $qa = b$."

Finally, a **still stronger definition** would require, not only that the solutions z and q of these two division problems must exist, but that, furthermore, they must be *unique*.

The first of these division problems, for our 2^n-ons, trivially does have a unique solution z: in the matrix picture of lemma 11 we have the 8×8 linear system $M(a)z = b$, with solution $z = M(a)^{-1}b = |a|^{-2}M(a)^T b$ since $M(a)$ is scaled-orthogonal (and hence, always invertible). An equivalent result follows from the left-cancellation law: $z = |a|^{-2}\overline{a}b = a^{-1}b$.

The second division problem, however, is not so trivial because there is no right-cancellation law in the 16-ons, and, to get a solution q, we need to solve a *non*linear system – so it is not even clear a solution must exist and, even if it does, it is not clear how to find it.

20 Existence and uniqueness of solutions to 16-on division problems

Theorem 70 (16-on division). *There exists a unique solution $x = (a, b)$ to any generic 16-on division problem.*

Proof: We've already discussed the easy (linear system) case (left division) in §19. The remaining hard (nonlinear system; right division) 16-on division problem is this. We wish to solve

$$(a, b)(c, d) \;=\; (ac - d\overline{b},\, cb + [\overline{a} \cdot db^{-1}]b) \;=\; (X, Y) \qquad (131)$$

(in which all letters are octonions) for the 16-on (a, b).

We may, and will, assume throughout that $b \neq 0$ and $d \neq 0$, since if $b = 0$ or $d = 0$, then the 16-on-multiplication formula becomes equivalent to the linear Cayley-Dickson formula (EQ 48) so division may be accomplished by solving a linear system. (Indeed, the $d = 0$ case is just two independent octonion division problems – trivial – see footnote 49.) Since (by norm-multiplicativity) this linear system is orthogonal, it always has a unique solution.

We shall also assume throughout that $c \neq 0$ since if $c = 0$ the division problem also may be solved directly (by solving for $\overline{b}$ in terms of X and then solving for $\overline{a}$) and plainly has a unique solution. (And this solution exists if $d \neq 0$ and $b \neq 0$.)

We first solve the left coordinate for a (using the fact that the octonions obey right-cancellation):

$$ac - d\overline{b} = X \quad \Longrightarrow \quad a = (X + d\overline{b})c^{-1} \qquad (132)$$

Next we substitute this value into the right coordinate's equation (and use anti-automorphism EQ 15):

$$cb + [\overline{c}^{\,-1}(\overline{X} + b\overline{d}) \cdot db^{-1}]b = Y \qquad (133)$$

which we successively simplify by: right-multiply by b^{-1}:

$$c + \overline{c}^{\,-1}(\overline{X} + b\overline{d}) \cdot db^{-1} = Yb^{-1} \qquad (134)$$

right multiply by bd^{-1}:

$$c \cdot bd^{-1} + \overline{c}^{\,-1}(\overline{X} + b\overline{d}) = Yb^{-1} \cdot bd^{-1} \qquad (135)$$

apply the Moufang-like identity ([181] EQ 10a p.420=our EQ 16) to the right side:

$$c \cdot bd^{-1} + \overline{c}^{\,-1}(\overline{X} + b\overline{d}) = b^{-1}(bY.d^{-1}) \qquad (136)$$

left-multiply by b and use left-cancellation:

$$b(c \cdot bd^{-1}) + b \cdot \overline{c}^{\,-1}(\overline{X} + b\overline{d}) = bY \cdot d^{-1} \qquad (137)$$

multiply by the scalar $|c|^2|d|^2$:

$$|c|^2 b(c \cdot b\overline{d}) + |d|^2 b \cdot c(\overline{X} + b\overline{d}) = |c|^2 bY \cdot \overline{d} \qquad (138)$$

use commutativity of addition and distributivity to rearrange terms:

$$(|c|^2 + |d|^2)b(c \cdot b\overline{d}) = |c|^2 bY \cdot \overline{d} - |d|^2 b \cdot c\overline{X} \qquad (139)$$

and use commutativity of multiplication by pure-real quantities to rearrange terms:

$$b(c \cdot b\overline{d})(|c|^2 + |d|^2) = bY \cdot \overline{d}|c|^2 - b \cdot c\overline{X}|d|^2 \qquad (140)$$

reducing the problem to solving a quadratic equation for b. It is now tempting to just left-multiply by b^{-1} to "get rid of common left-factors of b" and reduce to a linear equation – except that due to non-associativity, getting rid of the b in the first term on the right would be illegal! (It *would* be legal if we were dealing with octonions=quaternion-pairs instead of 16-ons=octonion-pairs, in which case we would end up with a closed form for b equivalent to the usual octonion-division formula.) Nevertheless, this quadratic clearly has a root $b = 0$, which for our purposes is *spurious* since if $b = 0$ we should have started with the Cayley-Dickson multiplication formula EQ 48 instead of ours, and anyway would already be done. We are interested in the *nonzero* roots of this quadratic. We know, by our fundamental theorem of algebra (theorem 66), that it generically has at least one nonzero root. Therefore, a non-spurious solution to the 16-on division problem generically *exists*. Q.E.D.

Theorem 71 (Uniqueness via miracle). *In theorem 70, there is a finite algorithm (there are rational closed forms) to compute the 16 coefficients of the quotient 16-on, and (generically) that quotient is unique.*

Proof: We begin by applying the left-Moufang identity ([181] EQ 10 p.419; our EQ 11) to the left side of EQ 140, getting

$$(bc \cdot b)\overline{d}(|c|^2 + |d|^2) = bY \cdot \overline{d}|c|^2 - b \cdot c\overline{X}|d|^2. \quad (141)$$

We then right-multiply by $(\overline{d})^{-1}$ (and use cancellation), getting

$$(bcb)(|c|^2 + |d|^2) = bY|c|^2 - (b \cdot c\overline{X})d. \quad (142)$$

We now left-multiply by b^{-1}, and use the flexible law EQ 9, the cancellation law, and the Moufang-like law EQ 16, to get

$$(|c|^2 + |d|^2)cb = Y|c|^2 - (c\overline{X} \cdot db^{-1})b. \quad (143)$$

Now right-multiplying by b^{-1} and using the cancellation law (remember, cancellation works on *both* sides in the octonions) yields

$$c = \frac{Y|c|^2 b^{-1} - c\overline{X} \cdot db^{-1}}{|c|^2 + |d|^2}. \quad (144)$$

But this is plainly a *linear* equation for b^{-1}, which

1. may be solved by 8-dimensional Gaussian elimination,
2. generically has a *unique* solution.

Miraculously, our nonlinear system really was a linear one in many layers of disguise! Q.E.D.

Theorem 72 (Exceptional cases). *In nongeneric division problems (and assuming $d \neq 0$ so that we do not merely have*[49] *two octonion division problems), uniqueness and existence could be avoided in EQ 131 only in cases where $b = 0$ or when EQ 144 is a singular linear system. Then these things could happen:*

1. *Both a pure-octonion quotient [(a, b) with $b = 0$] exists,* and *a non-octonion 16-on quotient exists.*
2. *There is a solution only in a limiting sense as $b \to 0$ along some smooth curve, but there is no solution with $b = 0$. (In this case, a solution will only "exist" if infinitesimal quantities are adjoined to the underlying real numbers; in that case it will be unique.)*
3. *A continuum infinity of solutions (a, b) could exist.*

Proof: Simply re-read the proofs of the preceding two theorems, asking at each stage what nongeneric event could happen to invalidate its logical function. The possibilities listed in the present theorem cover them.

Here are examples of these nonexistence or nonuniqueness phenomena:

1. Let $X = ac$ and $Y = \overline{a}d$ so that (see EQ 69) our division problem $(a, b)(c, d) = (X, Y)$ has solution $b = 0$. Then the equation for b^{-1} is $(|c|^2 + |d|^2)c = |c|^2\overline{a}d \cdot b^{-1} - c\overline{ac} \cdot db^{-1}$, which simplifies to

$$(1 + |\frac{d}{c}|^2)c = \overline{a}d \cdot b^{-1} - \overline{a} \cdot db^{-1}. \quad (145)$$

The right hand side of EQ 145 is a linear transformation of (the octonion regarded as an 8D vector) b^{-1} which has a very considerable (i.e. 4D) nullspace, namely, *every* b^{-1} in the quaternion subalgebra generated by $\overline{a}$ and d. Nevertheless, clearly by choosing b to be orthogonal to this subalgebra and then letting b determine c via EQ 145, we can create examples of 16-on division problems with at least two solutions, one with $b = 0$ and one with $b \neq 0$.

2. If we pick c and d then simply choose X and Y so that $Y|c|^2 b^{-1} - c\overline{X} \cdot db^{-1}$ is a non-invertible linear function of b^{-1} (i.e., as before, with a nontrivial nullspace), then in general EQ 144 is only going to have infinite "solutions" b^{-1}, leading to infinitesimal but nonzero b and then via EQ 132 to finite a. On the other hand if the left hand side of EQ 144 happens to be in the range of that non-invertible linear function, then in general there will be a continuum infinity family of solutions b^{-1}.

3. Here is an explicit counterexample: $(a, b)(c, d) = (a', b')(c, d) = (X, Y)$:

$$\begin{aligned} (a, b) &= (0,0,1,0,0,0,0,0, \quad 0,0,0,0,1,0,0,0) \neq \\ (a', b') &= (0,0,0,0,0,0,0,0, \quad 0,0,0,1,1,0,0,0), \\ (c, d) &= (1,0,0,0,0,0,0,0, \quad 0,1,0,0,0,0,0,0), \\ (X, Y) &= (0,0,1,0,0,-1,0,0, \quad 0,0,0,1,1,0,0,0). \end{aligned} \quad (146)$$

Q.E.D.

Remark: Loops via dense countable subsets of $\mathbb{R}$. The nonzero 16-ons do not *quite* form a multiplicative loop, due to the exceptional nongeneric cases in the preceding theorem. However, if instead of working over $\mathbb{R}^{16}$ we instead operate in a countable dense subset of $\mathbb{R}^{16}$ closed under 16-on-rational operations (including conjugation) and containing only 16-vectors whose 15D imaginary parts are[50] *generic*, then we have a genuine loop, (and a genuine nnacd division algebra) since all the nongeneric cases that could cause trouble, are impossible.

These also automatically yield a dense set of *unit-norm* 16-ons (consider expressions such as $x^2/\overline{x}x$), which also form a genuine multiplicative (sub)loop.

Remark: true continuum loop. It is also possible to get a true loop *without* resorting to any subset of $\mathbb{R}$, *provided* we change the 16-on multiplication law slightly (and hence this may come at the cost of sacrificing some desirable properties, although only on a measure-0 subset). Let (a, b) and (c, d) be unit-norm 16-ons regarded as octonion pairs. We use the usual 16-on multiplication formula for multiplying $(a, b)(c, d)$ except on the measure-0 set of (a, b), (c, d) that cause the map on (a, b) to be ($\geq$ 2)-to-1. On this set, we replace the multiplication law with some other multiplication table which *is* a true loop. By the usual nonconstructive arguments of G.Cantor [74], such replacements exist. Of course, this recipe has not been uniquely specified! It is highly unclear what the

[49] EQ 131 with $d = 0$ is just $(a, b)(c, d) = (ac, cb) = (X, Y)$, with solution $a = Xc^{-1}$, $b = c^{-1}Y$. Except when $c = d = 0$, this solution exists; and whenever it exists it is unique.

[50] An explicit set of 150 generic reals may be constructed with the **Lindemann-Weierstrass theorem** ([22] p.6, [29]) that $\exp(a_j)$ are algebraically independent if the a_j are algebraic numbers which are linearly independent over the rationals. E.g., use $\exp\sqrt{p_j}$ for $j = 1, 2, \ldots, 150$ where p_j is the jth prime. If we use these to construct 10 generic pure-imaginary 16-ons, then adjoin all 16-ons constructible from these via rational 16-on operations and 16-on conjugation, then we get a genuine nnacd division algebra (since every element is sufficiently generic; any 16-on lying on the discontinuity would imply the existence of 8 algebraic equations, not satisfied identically by all reals, but satisfied by our 150 generic reals, a contradiction) and, if we only look at the multiplicative structure, a genuine multiplicative loop. 1 and 0 are generated automatically from x/x and $x - x$.

"best" loopifying recipe is, from among the many possibilities of this kind.

21 The beginnings of 2^n-onic (and bi-2^n-onic) analysis; Trotter formula; Newton method; division and root-finding algorithms

21.1 Power series and Trotter formula

The fact that the 2^n-ons obey weak-linearity, power-distributivity[51], and power-associativity (equivalently, that any 2^n-on x generates a subalgebra of the 2^n-ons isomorphic to the complex numbers $\mathbb{C}$) means that formal power series

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots, \tag{147}$$

whose coefficients a_k are *real* (or in the case of bi-2^n-ons, *complex*) and formal rational operations with them, are unambiguous. Thus, if for some reason one wanted to define $\ln(1+x)$ for 2^n-ons x, one could use

$$\ln(1+x) \;=\; x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots, \quad |x| < 1, \tag{148}$$

and similarly

$$\sqrt{1+x} \;=\; 1 + \frac{x}{2} - \frac{1\cdot x^2}{2^2 2!} + \frac{1\cdot 3x^3}{2^3 3!} - \frac{1\cdot 3\cdot 5x^4}{2^4 4!} + \ldots, \quad |x| < 1, \tag{149}$$

$$\exp(x) \;=\; 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots \tag{150}$$

$$\sin(x) \;=\; x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots \tag{151}$$

et cetera. For 2^n-ons q

$$\exp(q) = (\cos|\operatorname{im} q| + (\operatorname{im} q)\sin|\operatorname{im} q|)\exp\operatorname{re} q\,; \tag{152}$$

this is also true for *bi*2^n-ons provided it is interpreted correctly (all quantities in it are now complex, including $|\operatorname{im} q|$ and $\operatorname{re} q$).

These functions then will obey all the usual 1-variable identities, e.g. $\exp(x)^k = \exp(kx)$, $\ln(x^k) = k\ln x$, $(\sqrt{x})^2 = x$, $\sin(x)^2 + \cos(x)^2 = 1$, et cetera. However, the quaternions onward in general will *not* obey (≥ 2)-variable identities (whose validity tends to depend on distributivity, associativity, and/or commutativity) such as $(x+y)^2 = x^2 + 2xy + y^2$, $e^x e^y = e^{x+y}$, $\sin(x+y) = \sin x\cos y + \sin y \cos x$, etc. Nevertheless,

Theorem 73 (Trotter's product limit formula in 16-ons).

$$e^{x+y} \;=\; \lim_{n\to\infty}(e^{x/n}e^{y/n})^n \;=\; \lim_{n\to\infty}(1 + \frac{x+y}{n})^n \tag{153}$$

is valid in the 16-ons.

Proof: This is because

$$e^{x/n}e^{y/n} \;=\; 1 + \frac{x+y}{n} + O(\frac{x^2}{n^2}) + O(\frac{y^2}{n^2}) + O(\frac{xy}{n^2}) + O(\frac{yx}{n^2}) \tag{154}$$

despite the presence of non-commutativity and non-associativity *and* non-distributivity. The key is that weak-linearity and norm-multiplicativity still are valid. These cause the bounds represented in EQ 154 by the big-O's; and all these terms are too small to alter the value of the limit. Here are the details. We have

$$(1 + \frac{x}{n} + \frac{x^2}{2n^2} + \ldots)(1 + \frac{y}{n} + \frac{y^2}{2n^2} + \ldots) = \tag{155}$$

$$= (\frac{x}{n} + \frac{x^2}{2n^2} + \ldots)(1 + \frac{y}{n} + \frac{y^2}{2n^2} + \ldots) + (1 + \frac{y}{n} + \frac{y^2}{2n^2} + \ldots) \tag{156}$$

by weak-linearity, which is

$$= 1 + \frac{x}{n} + \frac{y}{n} + \frac{y^2}{2n^2} + \frac{x^2}{2n^2} + (x + \frac{x^2}{2n} + \ldots)\frac{y}{n^2} + O(n^{-3}) \tag{157}$$

by right-linearity. *If* x and y are 16-ons, then $(x + \frac{x^2}{2n} + \ldots)y$ is, for large n, a small, i.e. $O(n^{-1})$, perturbation of xy, because if x is on the discontinuity (i.e. in the octonion subalgebra) then so is x^2, $x + x^2$, etc., so that everything acts continuous since the octonions are continuous; while if x is off the discontinuity, immediately everything is continuous. *However* if x and y are 32-ons this perturbation is *not* necessarily small, because now x can be on a discontinuity but *not* in a subalgebra (consider zeroing just coordinates 24-31 [or 8-15] of x), in which case x^2 can be *off* the discontinuity.

So in the 16-on case we have reached agreement with EQ 154. We now argue that the O terms in EQ 154 are too small to affect the value of the limit in EQ 153. If x and y are fixed, then all the derivatives of the 2^k-on multiplication map $(1+x/n)(1+y/n)$, with respect to both x and y, are bounded, for all sufficiently large n, by some constant divided by n. (If x is on the discontinuity, we only speak of derivatives in directions that remain on it.) Perhaps this is (depending on x and y) a large bounding constant, but that does not matter. As $n \to \infty$, the n^{-2}-factor decrease is enough (now for the same reasons as in the standard analysis of Trotter's formula in the linear associative case) to overwhelm any perturbing effect caused by the O-terms and the nth powering in EQ 153. Q.E.D.

16-on numerical example. Let x and y be the following two 16-ons:

$$x = (2,5,5,6,2,7,2,-6,\;\; 4,4,9,-4,1,6,-2,-5) \tag{158}$$

$$y = (2,9,4,4,8,-4,-7,3,\;\; 2,-8,2,2,-6,-4,-9,6) \tag{159}$$

Then e^{x+y} (to accuracy ± 0.05, computed via the 500-term Maclaurin series and Horner's rule) is

$$(-36.2,-19.7,-12.6,-14.0,-14.0,-4.2,7.0,4.2,\\ -8.4,5.6,-15.4,2.8,7.0,-2.8,15.4,-1.4) \tag{160}$$

At this accuracy, the Trotter approximation $[\exp(x/16384)\exp(y/16384)]^{16384}$ is exactly the same.

There are many other such reassuring 16-on examples, including ones in which x lies on the discontinuity.

[51] See theorem 19 or claim 9 of the proof of theorem 60.

However, corresponding numerical tests in the *32-ons* indicate that the Trotter product formula is *false*. [The limit appears to exist, but it is not equal to $\exp(x+y)$.]

32-on numerical counterexample #1. Let x and y be the following two 32-ons:

$$x = (2, 2, 5, -5, 6, -4, 1, 5, 4, -2, -2, -8, 0, -1, 1, 4, \\ 9, 6, 0, -9, 9, 2, 9, -2, 8, 6, 5, 3, 0, 1, 5, -7) \quad (161)$$

$$y = (2, 6, -7, -5, 8, -3, 3, 5, 0, -7, 9, -2, 2, -3, 3, -9, \\ -2, 5, -8, -4, -4, 1, -1, 3, 5, -3, 7, -5, -8, -8, -4, 5) \quad (162)$$

Then (to accuracy ± 0.05)

$$e^{x+y} = (-38.6, -3.4, 0.8, \ldots, -4.8, 7.2, -1.2) \quad (163)$$

(Only the first and last 3 coordinates are given.) To the same accuracy, the Trotter approximations are given in figure 21.1.

n	$[\exp(x/n)\exp(y/n)]^n$
4	$(24.8, -7.5, -2.5, \ldots, 10.5, 5.3, 4.0)$
32	$(12.0, 7.9, 4.5, \ldots, -10.1, -3.8, -6.5)$
256	$(-13.0, -10.1, 1.7, \ldots, 9.2, -0.7, 3.1)$
2048	$(-10.8, -10.1, 2.4, \ldots, 8.9, -1.2, 2.6)$
16384	$(-10.7, -10.1, 2.5, \ldots, 8.9, -1.3, 2.5)$

Figure 21.1. Trotter approximations to e^{x+y}, for x and y in EQ 161 and 162, to accuracy ± 0.05. (All exp's computed via 500-term Maclaurin series and Horner's rule.) They appear to be converging – but not to e^{x+y} in EQ 163!

32-on numerical counterexample #2. Let x and y be the following two 32-ons:

$$x = (2, 7, 9, 7, -5, -7, 1, 0, 7, 8, 0, -7, 3, 2, 5, -7, \\ 5, 9, -3, -9, 4, -7, -9, -6, 0, 0, 0, 0, 0, 0, 0, 0) \quad (164)$$

$$y = (2, 7, -3, -4, 7, 1, 6, 7, 0, 8, 4, -1, 0, 1, 8, -8, \\ 9, 5, 6, 1, -6, -4, 3, 8, -8, 2, 9, 0, 3, -4, -6, -1) \quad (165)$$

Then (to accuracy ± 0.05)

$$e^{x+y} = (89.7, -353.1, 12.9, \ldots, -97.7, -34.9, -209.3) \quad (166)$$

To the same accuracy, the Trotter approximations are given in figure 21.2.

n	$[\exp(x/n)\exp(y/n)]^n$
4	$(54.1, -1.6, 1.6, \ldots, -0.1, 0.5, 0.6)$
32	$(-41.7, -9.3, 4.1, \ldots, 5.7, -0.7, -6.7)$
256	$(34.6, 13.3, 4.6, \ldots, -3.6, -4.8, -0.9)$
2048	$(32.7, 13.6, 5.7, \ldots, -3.9, -5.8, -1.0)$
16384	$(32.7, 13.6, 5.8, \ldots, -3.9, -5.8, -1.0)$

Figure 21.2. Trotter approximations to e^{x+y}, for x and y in EQ 164 and 165, to accuracy ± 0.05. (All exp's computed via 500-term Maclaurin series and Horner's rule.) They appear to be converging – but not to e^{x+y} in EQ 166!

21.2 Newton's method, linear approximations, and root-finding algorithms

If we broaden our permitted kinds of power series to permit fully-general monomials, e.g.,

$$a + (bx + xc + d \cdot ex + f \cdot xg + \ldots) + \ldots \quad (167)$$

then *all* functions of 2^n real variables, locally multivariate-polynomial near 0, become possible, so that 2^n-ons no longer play any particular role.

Despite the lack of 2^n-onic differentiability of general power series, it sometimes is still possible to *use* derivatives in some of their classic applications. Specifically, consider "Newton's method" $x \leftarrow x - F(x)/F'(x)$ of finding real roots x of equations $F(x) = 0$. For simplicity let us consider only the case where F is a polynomial (a sum of fully general monomials(x) as in EQ 167). If we have an initial guess g for a root, we may change variables to h where $x = g + h$, and rewrite the polynomial as a sum of monomials in h. In the octonions and below (which are distributive) this rewriting is straightforward. In the 16-ons and beyond (nondistributive) it is not, and, to make matters worse, the sum in general becomes infinite (nonpolynomial power series). We may then suppose that g is close to the desired root r, hence $|h|^2$ is small, and hence (by norm-multiplicativity) all quadratic and higher-degree terms are small. So we neglect them, i.e., replace $F(g + h)$ by its linear approximation $\widetilde{F}(g+h)$ at g. By then solving the linear system $\widetilde{F}(g + h) = 0$ for h, we get a new guess at the root $g_{\text{new}} = g + h$, which hopefully is better (and if g were initially close enough to a [generic] root, it definitely will be better), and we may continue on. Although this method is valid in the 2^n-ons even when $n \geq 4$, it is then most convenient to view F as really being a rational function mapping 2^{n-3}-tuples of octonions to 2^{n-3}-tuples of octonions so that we may write $\widetilde{F}(g + h)$ comparatively easily – we are really then doing the (2^{n-3})-dimensional Newton method over the octonions.

Observe that a linear octonionic function such as $F(x) = a \cdot xb + cx \cdot d + e \cdot fx + g$ does *not* have any octonionic "slope." It nevertheless is a linear function, and it in general has a root x, which we can find. The "slope," or "derivative," or "Jacobian matrix" of this function does exist, but *only* in the wider world of 8×8 real matrices, and *not* inside the octonions proper. However, notice that there are *efficiency advantages* to remaining inside the octonions rather than going out into this wider matrix world. E.g., representing an 8×8 matrix would require 64 numbers, But the present linear function is represented via 6 octonions, requiring only 48 numbers, or actually only 45 if we realize three of these octonions are unit-norm wlog.

Hopefully the above concrete example clarifies the point that Newton's method, and local linear approximations, still exist in the octonions even though "derivatives" do not.

It is now possible to turn our nonconstructive proofs of 2^n-on fundamental theorems of algebra (§17 and 23) into algorithms for rootfinding. The algorithm is:

1. Take advantage of the supposition that there is an asymptotically dominant monomial, to generate an upper bound on $|x|^2$, for any root x of our polynomial.
2. We now have restricted x to lie inside a ball, i.e. a compact set S.

3. Repeatedly try random initial guesses within S for Newton's method. We will eventually be assured of success (i.e. an initial guess leading to obviously-quadratic convergence) since these initial guesses will (with probability 1) eventually cover S arbitrarily densely, and hence, with probability 1, will eventually generate an initial guess in each obvious-quadratic-convergence region[52].

It is also possible to convert this into a fully deterministic algorithm by either using explicitly specified coverings of S by tiny equal balls to generate initial guesses, or by regarding the whole problem as a set of rational nonlinear equations in real 2^n-dimensional space, and using nowadays-standard results [52][215] that solving such systems is an algorithmic task.

21.3 Fueterian 2^n-onic analysis

During the years 1928-1949 Rudolf Fueter (1880-1950) and his students developed a theory of quaternionic analysis paralleling (to the extent that that is possible) complex analysis. (Actually [136][138][139] much of this had been anticipated by C.Lanczos in his 1919 PhD thesis [164], and A.C.Dixon [83] in 1904, but that was not realized by Fueter.) There are excellent reviews of this in English by Deavours [75] and Sudbery [242]. There is a difficult-to-obtain book about it by Fueter & Bareiss [111]. A bibliography of work prior to about 1945 is in [122]. Later, extensions of Fueterian analysis to the octonions and sedenions were made by Dentoni & Sce [78] and the father-daughter team of K. & M. Imaeda (in papers [136][137][138][139] which also are difficult to obtain).

We shall show that essentially all of this may be generalized to hold in the 2^n-ons for every n, and we also shall extend previous results even for fixed n.

A goodly part of it has nothing particularly to do with the 2^n-ons and works for $(1+s)$-vectors for arbitrary odd s.

Fact: The discussions of Cayley-Dickson and our 2^n-ons are to a great extent the same discussion, because, e.g., by theorems 30 and 19, functions of a *single* sedenion variable are the same thing as the corresponding functions of a 16-on variable (for rational functions with real coefficients, at least, or any norm-convergent power series with real coefficients).

Continuity: For the same reason, we do not need to worry about the discontinuity of 2^n-on multiplication if $n \geq 4$, because, when we are dealing with polynomial functions (with real coefficients, or even with 2^n-on coefficients, so long as they are on the left) of a *single* 2^n-on variable, everything is continuous.

Liouville's theorem on multidimensional conformal maps [166] might seem to show that any attempt to generalize complex analysis to dimensions≥ 3 is impossible or uninteresting. Fueter's goal was to try to preserve desirable analyticity-like properties as much as one can in the quaternions. The key idea for evading Liouville's theorem is to start from *Morera's theorem* in complex analysis [214], which states that a function $f(z)$ mapping $\mathbb{C} \to \mathbb{C}$ is "analytic" in a domain D iff $\int_C f(z)\mathrm{d}z = 0$ for every closed contour $C \subset D$. Inspired by this, Fueter defined a quaternionic function $F(q)$ of a quaternion q to be *left-regular* in a domain D if $\int_{\partial\sigma}(\mathrm{d}Q)F(q) = 0$ for every closed hypersurface $\partial\sigma$ in D ($\mathrm{d}Q$ is the unit outward normal to $\partial\sigma$). Similarly it is *right-regular* if $\int_{\partial\sigma} F(q)(\mathrm{d}Q) = 0$ (order matters!).

The differential version of this integral statement (generalized to complexes, octonions, sedenions, etc. by letting $n \geq 1$ in the below) is

Definition 74 (Left-regularity). $F(q)$ is *left-regular at q* if

$$DF(q) \stackrel{\text{def}}{=} \sum_{\mu=0}^{2^n-1} e_\mu \cdot \frac{\partial F(q)}{\partial x_\mu} = 0 \tag{168}$$

where $q = \sum_{\mu=0}^{2^n-1} e_\mu x_\mu$, the x_μ are reals, $F(q)$ and its partial derivative are regarded as 2^n-vectors, the $\cdot$ means a 2^n-onic multiplication, and the e_μ are the orthonormal basis elements. Similarly $F(q)$ is *right-regular at q* if

$$F(q)D \stackrel{\text{def}}{=} \sum_{\mu=0}^{2^n-1} \frac{\partial F(q)}{\partial x_\mu} e_\mu = 0. \tag{169}$$

We just call F *regular* (or *two sided-regular*) if F is both left and right regular. These conditions are analogous to the Cauchy-Riemann equations. In fact if $n = 1$ they *are* the Cauchy-Riemann equations, causing regularity to be the same thing as analyticity.

The *Cauchy-Riemann equations* say that a function $f(z) = a(x,y) + ib(x,y)$ where a and b are real and $z = x + iy$ where x and y are real, is analytic iff

$$\frac{\partial a}{\partial x} = \frac{\partial b}{\partial y}; \quad \frac{\partial b}{\partial x} = -\frac{\partial a}{\partial y}. \tag{170}$$

These also imply

$$\frac{\partial^2 a}{\partial x^2} + \frac{\partial^2 a}{\partial y^2} = \frac{\partial^2 b}{\partial x^2} + \frac{\partial^2 b}{\partial y^2} = 0. \tag{171}$$

We also define $\overline{D}$ by

$$\overline{D}F(q) \stackrel{\text{def}}{=} \sum_{\mu=0}^{2^n-1} \overline{e_\mu} \frac{\partial F(q)}{\partial x_\mu}; \tag{172}$$

$$F(q)\overline{D} \stackrel{\text{def}}{=} \sum_{\mu=0}^{2^n-1} \frac{\partial F(q)}{\partial x_\mu} \overline{e_\mu}. \tag{173}$$

Lemma 75 (Linearity). *Any linear combination, with real (or more generally niner) coefficients, of left-regular functions also is left-regular.*

[52] To show fully rigorously that this really is an algorithm for finding all solutions to 2^n-onic polynomials with *integer* coefficents, we also need explicit upper bounds on the number of such solutions, and explicit lower bounds on the distance between any two unequal solutions and the distance between any solution and the discontinuity (if it does not lie exactly on the discontinuity), and on the radius of balls which fit inside each obvious-quadratic-convergence region; the latter may be gotten from bounds on the norm of the Hessian of the 2^n-on multiplication map provided we are at least some nonzero distance from the discontinuity. These can be used to become sure we have found all solutions so that we may terminate the algorithm. Such explicit bounds are available from general results [187] about algebraic numbers of bounded degree [253], and the fact that the discriminant of a polynomial with integer coefficients is an integer (expressible as a certain determinant [252]).

Remark. The lemma is also true with "right" or "two sided" written in place of "left." The coefficients are allowed to be arbitrary constant Cayley-Dicksons if we are working in Cayley-Dickson algebras rather than the 2^n-ons. That is due, essentially, to the full bilinearity of Cayley-Dickson algebras combined with EQ 50.

Lemma 76 (Laplacian in terms of D).

$$D\overline{D} = \overline{D}D = \nabla^2 \stackrel{\text{def}}{=} \sum_{\mu=0}^{2^n-1} \frac{\partial^2}{\partial x_\mu^2}. \tag{174}$$

Proof:

$$D\overline{D} = \sum_{\mu=0}^{2^n-1}\sum_{\nu=0}^{2^n-1} e_\mu \overline{e_\nu} \frac{\partial^2}{\partial x_\mu x_\nu} = \sum_{\mu=0}^{2^n-1} \frac{\partial^2}{\partial x_\mu^2} \tag{175}$$

because $e_\mu\overline{e_\nu} + e_\nu\overline{e_\mu} = 0$ if $\mu \neq \nu$ (and $e_\mu\overline{e_\mu} = \overline{e_\mu}e_\mu = 1$) by the anticommutativity-like property of basis elements in theorem 15. Q.E.D.

Corollary 77 (Regular$\Longrightarrow$Harmonic). *Each component of a left-regular or right-regular $F(q)$ satisfies Laplace's equation $\nabla^2 F = 0$ in $\mathbb{R}^4$, or more generally in $\mathbb{R}^{(2^n)}$ for each $n \geq 2$.*

Corollary 78. *Any regular 2^n-onic function of bounded norm throughout $\mathbb{R}^{(2^n)}$ is a constant.*

Corollary 79. *The only 2^n-onic functions regular in both x and $\overline{x}$ are constants.*

Sad fact (Hamilton, 1860 or before): For any $n > 1$, $F(q) = q^2$ is *neither* left nor right regular, and its components do *not* satisfy Laplace's equation $\nabla^2 F = 0$.

Definition 80. A norm-convergent quaternion (or 2^n-on) power series with 2^n-on coefficients on the left only (or just real coefficients)

$$\sum_{k\geq 0} c_k (x-a)^k \tag{176}$$

is called a *regular power series.*

Due to Hamilton's sad fact, regular power series are in general *not* regular 2^n-onic functions. Furthermore, although such power series have formal "derivatives" and integrals, via

$$\frac{\mathrm{d}}{\mathrm{d}x} x^n \quad \text{“=”} \quad n x^{n-1}, \quad n \neq 0, \tag{177}$$

those have a certain lack of validity or of interest in the sense that, e.g.,

$$\lim_{h\to 0} h^{-1}[(x+h)^n - x^n] \neq n x^{n-1} \tag{178}$$

in general in the quaternions and beyond. Indeed, such limits in general do not even exist (different values are approached as $h \to 0$ from different directions): Sudbery ([242] theorem 1) showed that $\lim_{h\to 0} h^{-1}[f(q+h) - f(q)]$ generally exists for quaternion$\to$quaternion functions f iff $f(q) = a + qb$.

Happy Fact: The saving grace is that such quaternionic power series F *do* satisfy the *bi*harmonic equation $\nabla^2\nabla^2 F = 0$ in $\mathbb{R}^4$. More generally, in $\mathbb{R}^{2^n}$ they satisfy $\nabla^{2^n} F = 0$. This all has nothing to do with 2^n-ons but follows merely from

Theorem 81 (k-iterated Laplacians). *Let $k \geq 1$ be an integer. Let $F(x+iy)$ be a function meromorphic at 0. The following $2k$ functions of $x, y_1, y_2, \ldots, y_{2k-1}$*

$$F_0 \stackrel{\text{def}}{=} \operatorname{re} F(x+iy), \quad F_m \stackrel{\text{def}}{=} \frac{y_m}{y} \operatorname{im} F(x+iy). \tag{179}$$

(where $m = 1, 2, \ldots, 2k-1$ and $y \stackrel{\text{def}}{=} \sqrt{y_1^2 + y_2^2 + \ldots y_{2k-1}^2}$ satisfy $(\nabla^2)^k F_0 = 0$ and $(\nabla^2)^k F_m = 0$.

Remark. This definition of F_0,..., F_{2k-1} is an attempt to generalize the notion of an "analytic function" in 2 real dimensions to $2k$ dimensions for each $k \geq 1$, and the theorem generalizes the fact that the real and imaginary parts of an analytic function are harmonic.

Proof: For any particular integer k one may directly verify the differential-polynomial identities $(\nabla^2)^k F_j = 0$ (using the fact that it works for $k = 1$, by the Cauchy-Riemann equations). Indeed, `MAPLE`'s automated simplifier does the proof automatically. However, when k is somewhere between 10 and 20 `MAPLE`'s proofs start to take an unacceptably large amount of time.

We also remark that if $F(z) = z^p$ for any particular integer p, these are simply *polynomial* identities, which makes them easier to verify. The same idea for *general* p in the neighborhood of $z = 1$ is the approach of §11.4.

So far, all attempts to extend this to arbitrarily large k by devising some kind of inductive or combinatorial argument, have foundered on the shoals of immense symbolic complexity. But the following rather unconventional attack succeeded.

First, it is obvious that the theorem works if $F(z) = a + bz$ is either constant or linear, since then $\nabla^2 F = 0$. A less obvious, but still true, *claim* is that the theorem works if $F(z) = z^{-1}$: From the formula for the laplacian (where $r = |\vec{x}|$ in s-dimensional space)

$$\nabla^2(r^p \vec{x}) = (p+s)p \cdot r^{p-2}\vec{x}, \tag{180}$$

and using the fact that $z^{-1} = \overline{z}/|z|^2$ we have $\nabla^2(z^{-1}) = -2(s-2)\cdot z^{-1}/|z|^2$. Continuing onward iterating the application of the laplacian k times in all where $s = 2k$ we get a factor of

$$(-2)(s-2)\cdot(-4)(s-4)\cdot\ldots(2-s)(2)\cdot(-s)(0) = 0, \tag{181}$$

proving the *claim.*

Now any generic reciprocated polynomial of degree m may be written as a *partial fraction expansion* [214][255]

$$\frac{a_1}{z-b_1} + \frac{a_2}{z-b_2} + \cdots + \frac{a_m}{z-b_m}. \tag{182}$$

(By "generic" we here mean "having no repeated roots.") Therefore any function $F(z)$ analytic at zero may be approximated arbitrarily closely throughout any sufficiently small fixed neighborhood of $z = 0$ by expressions of form EQ 182. By linearity and invariance of the laplacian under z-translation we know our theorem works for all such partial fraction expansions. Therefore, it works to arbitrarily good approximation locally for generic analytic functions and hence must be a valid identity. Q.E.D.

This allows us to convert any analytic function $f(z) = a(x,y) + ib(x,y)$ where a and b are real and $z = x+iy$ where x

and y are real, to a quaternion→quaternion, or more generally to a 2^n-on→ 2^n-on function, via the formal process described by

$$F(q) = \left(a(w, |\vec{v}|), \frac{\vec{v}}{|\vec{v}|} b(w, |\vec{v}|) \right) \quad (183)$$

where $q = (w, \vec{v})$ is a quaternion (or 2^n-on) regarded as having real part $w = q_0$ and $2^n - 1$ imaginary parts $\vec{v} = (q_1, q_2, q_3, \ldots, q_{2^n-1})$ with $|\vec{v}| = \sqrt{\sum_{k=1}^{2^n-1} q_k^2}$. Note that this process converts $f(z) = z^k$ to $F(q) = q^k$ (as may be seen from the proof of theorem 20) and hence all regular power series have this form.

Theorem 82 (Generalized analytic functions). *Let $n \le 7$. Let F be a 2^n-on→ 2^n-on function constructed from any analytic function $a + ib$ as in EQ 183; this includes all norm-convergent regular power series EQ 176. Then $(\nabla^2)^{(2^{n-1}-1)} F$ is two sided regular so that every component of $(\nabla^2)^{2^{n-1}} F$ is 0.*

Proof sketch: Essentially the same proof works as for theorem 81. Q.E.D.

Remark. This generalizes theorems of previous authors to all n: For $n = 1$ this is the Cauchy-Riemann equations, for $n = 2$ this was Fueter's quaternion theorem (theorem 4.1 of [75]),..., and for $n = 4$ Imaeda & Imaeda ([136] p.86) claimed left-regularity.

In appropriate units, the Maxwell equations[53] of electromagnetism are

$$-(\frac{\partial}{\partial t} + I\vec{\nabla})(\vec{E} + I\vec{B}) = \vec{J} + I\rho \quad (184)$$

where $I = \sqrt{-1} \ne i, j, k$, and by 3-vectors such as $\vec{E}$ we mean $E_1 i + E_2 j + E_3 k$, and $\vec{E}$ is the electric field, $\vec{B}$ is the magnetic field, ρ is the charge density, and $\vec{J}$ is the current density. This may be verified directly from EQ 4 by comparison with the usual form

$$\vec{\nabla} \cdot \vec{B} = 0, \quad \vec{\nabla} \times \vec{E} + \frac{\partial}{\partial t}\vec{B} = \vec{0}, \quad (185)$$

$$\vec{\nabla} \cdot \vec{E} = \rho, \quad \vec{\nabla} \times \vec{B} - \frac{\partial}{\partial t}\vec{E} = \vec{J} \quad (186)$$

of Maxwell's equations. Note that the operator $\frac{\partial}{\partial t} + I\vec{\nabla}$ is a square root of the wave operator $\frac{\partial^2}{\partial t^2} - \frac{\partial^2}{\partial x^2} - \frac{\partial^2}{\partial y^2} - \frac{\partial^2}{\partial z^2}$ so that, in a sense, Maxwell's vacuum equations are a square root of the wave equation. If $\rho = 0$, $\vec{J} = \vec{0}$, we get the *vacuum Maxwell equations* in the form $(\partial_t + I\vec{\nabla})F = 0$ where $F = E + IB$ is biquaternion-valued. If we regard t as imaginary, e.g. $It = \ell$ with ℓ real, then this is $(\partial_\ell + \vec{\nabla})F = 0$ which is, in fact, the same as the *left-regularity condition* $DF = 0$. This is additional evidence for the "naturalness" of our quaternionic-analyticity concepts.

Remarks: some other regular functions

1. The 2^n-on function $x \to x^{1-2^n}$ has harmonic gradient in 2^n-dimensional space (since it is, essentially, the "electric field of a point charge") and hence automatically its laplacian is two sided regular.
2. Linear functions automatically are harmonic and hence regular: this includes $x \to ax + xb + c$ in the octonions and below ($0 \le n \le 3$) and $x \to ax + b$ for all $n \ge 0$.

There is now an analogue of Cauchy's theorem from complex analysis [214], expressing $F(a)$ as an integral over a hypersurface containing a.

Theorem 83 (Generalized Cauchy theorem). [54] *Let S be a $(2^n - 1)$-dimensional topological sphere hypersurface in 2^n-space. Let $F(x)$ be a 2^n-on→ 2^n-on function expressible as a power-series (EQ 176) everywhere inside S. Let $\bigcirc_k = k\pi^{k/2}/(k/2)!$ be the surface area of a unit sphere in $\mathbb{R}^k$. Then*

$$-(2^n - 2)!!^2 \bigcirc_{2^n} \cdot F(a) = \int_S (\nabla^2)^{2^{n-1}-1} [F(x)(x-a)^{-1}] \mathrm{d}x. \quad (187)$$

Here $\mathrm{d}x$ is the outward-pointing 2^n-on infinitesimal element of surface area and $t!!$ denotes the product of all the numbers from 1 to t having the same parity as t – except that the term $-(2^n - 2)!!^2$ in EQ 187 is to be replaced with $+1$ when $n = 1$.

Proof: All the terms c_k for $k \ge 1$ in the power series EQ 176 lead to regular functions after taking the iterated laplacian, and hence to zero after integration. Hence only the wanted c_0 term remains alive since the function we get after laplacianizing, since it is nonregular at $x = a$, upon integration need not yield 0. However it is regular within S but outside a small sphere centered at $x = a$ hence the integral does not change if we alter the shape of S. So the integral must yield $c_0 = F(a)$ up to some proportionality factor. That proportionality factor may be worked out by considering the case where S is the unit-radius sphere. We get a factor $\bigcirc_{2^n}$ from the surface area of the sphere. From the formula for the laplacian (where $r = |\vec{x}|$ in s-dimensional space)

$$\nabla^2(r^p \vec{x}) = (p + s)pr^{p-2}\vec{x}, \quad (188)$$

and using the fact that $x^{-1} = \overline{x}/|x|^2$ we have $\nabla^2(x^{-1}) = -2(2^n - 2)x^{-1}/|x|^2$. Continuing onward with more laplacians we get a factor of

$$(-2)(2^n - 2)(-4)(2^n - 4) \ldots (2 - 2^n)(2) = -(2^n - 2)!!^2. \quad (189)$$

There is no minus sign in the complex number case $n = 1$ because there are no terms in the above product; but if $n \ge 2$ we get one because there are an odd number of terms in the product, each with a minus sign. Q.E.D.

22 Topology in the presence of discontinuities

The insight of this section is that much of Brouwer topological-degree theory (reviewed in §17) may be generalized to hold for maps from S^n to S^n having certain kinds of *discontinuities*. Although this apparently is a new contribution to topology, it is surprisingly easy. Also, it is an important contribution, because rational maps are important. Rational maps (of course) in general are discontinuous, but nevertheless generalized-smoothness is fairly common for them.

[53] Maxwell's equations were stated incorrectly by Deavours [75] p.1008.

[54] We are emulating the proof of this theorem given by Deavours [75] in the case $n = 2$; but Deavours' proof contains errors, the most obvious of which is that the minus sign in the EQ above EQ 16 on p.1004 is obviously bogus.

In particular, for each $n \geq 4$, 2^n-on right-multiplication maps for unit-norm 2^n-ons are in general smooth *but* with discontinuities. All the jumps (in any and all coordinates) in those discontinuities are *bounded*, as one may see by considering the norm-multiplicativity and subadditivity properties of the 2^{n-1}-ons and 2^n-ons. This is one way in which these discontinuities are "not very severe." But a much more interesting way is the fact (lemma 87) that 16-on multiplication maps are "generalized smooth."

To maximize convenience, in the discussion below we shall only consider and allow, maps f from S^n to S^n whose domain and range are the *whole* of S^n (except perhaps for subsets of measure 0 and dimension$< n$). (Our notions are readily generalized to other kinds of maps with only bounded-size jumps.) We shall only allow $f(x)$ to be discontinuous when $x \in D$ where $D \subset S^n$, measure$(D) = 0$; for $x \notin D$ we shall require $f(x)$ to be *smooth*.

Definition 84. We call such a map $f : S^n \to S^n$ "generalized-smooth" if

dim(discontinuity)≤A: The dimension of the support set D of the discontinuity is $\leq A$;

#jumping coordinates≤B: At most B of the coordinates of $f(x)$ [regarding $f(x)$ as being an n-vector of coordinates on the image S^n] jump at the discontinuity (the remaining ones are continuous) for some finite atlas of local coordinate patches of the image S^n;

A,B conditions: $B \geq 2$ and $A + B < n$.

Non-examples. The vector fields on S^n constructed in theorems 48 and 49 are *not* generalized-smooth. Also, for each $n \geq 2$ the algebra of $n \times n$ real matrices involves discontinuous maps $Y \to XY^{-1}$ and $X \to X^{-1}Y$ from $\mathbb{R}^{n\times n}$to $\mathbb{R}^{n\times n}$ which do *not* satisfy the dimension-sum conditions of generalized-smoothness. These non-examples indicate that nnacd-algebras featuring generalized-smoothness are not terribly easy to get.

A *homotopy* used to mean the process of continuously distorting the smooth map $f(x)$ to become the parameterized family of smooth maps $f_t(x)$ for $x \in S^n$ and $t \in [0, 1]$, where $f_t(x)$ was required to be smooth in both t and x, and $f_0(x) = f(x)$. Then $f_0(x)$ and $f_1(x)$ were said to be "homotopically equivalent."

Definition 85. A *generalized-homotopy* shall mean the process of distorting the generalized-smooth map $f(x) = f_0(x)$ to become the parameterized family of generalized-smooth maps $f_t(x)$, where, for each $x \in S^n$ and $t \in [0, 1]$, for all sufficiently small $|\Delta t|$ there exist ϵ and δ, depending continuously on Δt and with $\epsilon = \delta = 0$ when $\Delta t = 0$, such that

$$f_{t+\Delta t}(x) = f_t(x + \epsilon) + \delta. \tag{190}$$

We shall only consider homotopies f_t (and maps f) with the property that f_t, for each $t \in [0, 1]$, never maps a measure$= 0$ set to a measure> 0 set.

The *topological degree* of a generalized-smooth map $f(x)$ shall mean

$$\text{degree}(f) = \frac{\int_{S^n} \det \text{Jacobian} f(x)\, dx}{\text{measure of the image } S^n}. \tag{191}$$

For smooth maps whose range is the whole of S^n, this definition of topological degree agrees with Brouwer's from §17. The following is the central lemma of our theory.

Lemma 86 (Smoothing). *Let D_r denote the subset of S^n with distance $\leq r$ from the support-set $D = D_0$ of the discontinuities in generalized-smooth map f mapping S^n to S^n. Then if the discontinuities in f are smoothed out by a minimum-energy interpolation, within D_r, of the data at the boundary of the set D_r, to get a now-continuous map $\widetilde{f}$, then*

$$\lim_{r\to 0+} \text{degree}(\widetilde{f}) = \text{degree}(f). \tag{192}$$

Proof: Here by "energy" we mean the average Frobenius norm of $\widetilde{f}$'s Jacobian determinant, but the precise definition does not matter much; many alternative notions could be substituted. The integral in EQ 191 will be perturbed, if f is replaced by $\widetilde{f}$, by an amount which goes to 0 as $r \to 0^+$. This is due to dimensional analysis using the fact that D has (by assumption) dimension$\leq A$, and the fact that (by assumption) $\leq B$ of the coordinates of $f(x)$ jump at the discontinuity, where $A + B < n$ and $B \geq 2$. The measure of D_r is thus proportional to r^{n-A} and the Jacobian determinant is at most proportional (by Hadamard's determinant bound, using the fact that $\leq B$ rows of the Jacobian have lengths of order $1/r$, the others have lengths of order 1; note that the compactness of S^n is used here) to r^{-B}, and so the integral of the latter over D_r has magnitude bounded by $r^{n-A-B} \to 0$. Q.E.D.

Remark. The "true meaning" of generalized smoothness is perhaps best understood via measure theory: $f(x)$ and $\widetilde{f}(x)$ differ on a set of x's of *measure*$\to 0$ as $r \to 0^+$, and the image-multisets of f and of $\widetilde{f}$ differ on a subset of the image S^n having *measure*$\to 0$ as $r \to 0^+$. Note that in 1D, a function with a jump-discontinuity makes a jump of (i.e. "misses") nonzero measure. The significance of generalized smoothness is that it is possible for *high*-dimensional map to have jump discontinuities which only "miss" *zero* measure. Such discontinuities are much milder. In fact to anybody who can only see nonzero-measure sets, it is as though these discontinuities did not exist.

We now claim that, for generalized-smooth maps f, the following usual properties of degree still hold: degree is an integer, it is invariant under (our class of) homotopies, the degree of the identity map is 1, and for a full-measure set of points $y = f(x)$ on the image S^n have $\geq$ degree(f) preimages x.

23 Existence of solutions to generic 2^n-on division problems & 2^n-onic fundamental theorem of algebra, if $n \leq 4$

The way to achieve salvation while avoiding enormous symbolic-algebra complexity, is, as usual in this monograph, to call upon topology. But for 2^n-ons with $n \geq 4$, at first it appears that this avenue is closed to us because topology is about continua, whereas the 2^n-on right-multiplication map is discontinuous.

This avenue in fact *is* closed to us, but not in the 16-on case, because we may apply the preceding section's theory of Brouwer-degree of *dis*continuous maps.

Lemma 87 (Generalized smoothness for $n \le 4$). *2^n-on right multiplication maps $x \to xy$ are always "generalized-smooth" in the sense of §22 iff $n \le 4$.*

Proof: For 16-ons $x = (a, b)$ (with a, b octonion) we have discontinuities when and only when $b = 0$, and we only have discontinuities in the second half of the coordinates of the product 2^n-on (and only in the 7 imaginary coordinates in that half; the real coordinate is continuous by EQ 86, i.e. the first 9 coordinates of the product of two 16-ons are continuous by claim 3 of theorem 30). For octonions and below, multiplication maps are smooth everywhere. All this is enough to assure generalized smoothness.

But for 32-ons, the support set of the discontinuity is all x such that $x_{8,\dots,15} = 0$ *or* $x_{24,\dots,31} = 0$. Furthermore, by work of Adams (see our EQ 88) at most 9 mutually linearly independent smooth tangent-vector fields can exist on S^{31}. Furthermore it is easy to see that at least 14 (of the 32) coordinates jump everywhere on our discontinuity. All this is more than enough to assure that the right multiplication map for the 32-ons is *not* generalized-smooth. Q.E.D.

Theorem 88 (Degree of right-multiplication maps). *If $n \le 4$, then 2^n-on right-multiplication maps $x \to xy$, for unit-norm x, y, have degree$= 1$.*

Proof: Because the identity map has degree$= 1$, and we may homotope that map $x \to x1$ to the right-multiplication map $x \to xy$. (Note: the map and its Jacobian matrix both are smooth functions of y, indeed are *linear* in y, although discontinuous in x. Thus smooth alterations of y are homotopies in §22's generalized sense of the word.) This map is also "generalized-smooth" in the sense of §22 since generalized-smoothness is preserved under our class of homotopies. Q.E.D.

Corollary 89 (division). *If $n \le 4$, generic 2^n-on division problems have at least one solution.*
More generally, we may extend our fundamental theorem of algebra (§17) to the 2^n-ons for $n \le 4$:

Theorem 90 (FTOA for 2^n-ons). *Let $n \le 4$. Consider a generic 2^n-onic polynomial $P(x, \overline{x})$, where x is a 2^n-on, and where $P(x, \overline{x})$ has (if expanded into monomials, and see the remark below) a unique asymptotically dominant (as $|x|^2 \to \infty$) monomial containing A x's and B $\overline{x}$'s, $A \ne B$. Then P has a root, i.e. x exists with $P(x, \overline{x}) = 0$.*

Proof: We can homotope (in the sense of §22) this dominant monomial to $x^A \overline{x}^B$ while making all the subdominant monomials vanish. (Note that by power-associativity, real-commutativity, and weak-linearity, any 2^n-onic product of x's and $\overline{x}$'s with A of the former and B of the latter, is the same thing as $x^A \overline{x}^B$.) Then P has Brouwer-degree $A - B$. (To see that $x^A \overline{x}^B$ has Brouwer-degree $A - B$, realize it is norm-preserving map and it lives in a subalgebra of the 2^n-ons isomorphic to the complex numbers, by, e.g. theorems 19 or the proof of lemma 52.) Hence it generically has at least $|A - B|$ roots. Q.E.D.

Remark on "expansion into monomials": For 16-onic polynomials, due to non-distributivity the whole notion of a "monomial" is of doubtful value – since the obvious "expansion" of a general polynomial into monomials, is in general not valid. Hence we are best off defining a "polynomial" of x not as a "sum of monomials" but rather as "any function of x obtained from x and 16-on constants by using addition and multiplication only." (If all the constant coefficients introduced during this process are octonionic, then the distributive law is valid, thanks to the weakened distributivity properties of 2^n-ons, and hence the obvious expansion into monomials is valid.) Nevertheless, thanks to norm multiplicativity and subadditivity we still can think of there as being a "dominant monomial" as $|x| \to \infty$ despite the inexactness of distributivity and hence of the monomial expansion. The theorem is applicable with this interpretation of "dominant monomial," i.e. its domain of validity is much larger than might naively have been thought.

Remark. The *extension* (theorem 66) of the octonion FTOA also goes through for 2^n-ons, $n \le 4$.

The lack of generalized-smoothness for the 2^n-on multiplication maps when $n \ge 5$, and the presence of miracles in some of our proofs with $n = 4$, suggest that perhaps these 2^n-ons do *not* have solutions to generic division problems (and hence do *not* obey a fundamental theorem of algebra), and that these solutions are *not* generically unique. Both of these suspicions, we shall soon see (albeit with some aid from computers), are true.

24 Nonuniqueness and nonexistence of solutions to generic 2^n-on division problems if $n \ge 5$; and the Jacobian of the mul map

Consider the $2^n \times 2^n$ Jacobian determinant $J(y)$ of the right-multiplication map $x \to xy$ for unit-norm 2^n-ons x, regarded as real 2^n-vectors.

The *left*-multiplication map $x \to yx$ is in comparison trivial, since it is just a linear map, i.e. a matrix-vector multiplication. The matrix was given in EQ 57 (or in simpler but isomorphic form in EQ 110). This matrix, of course, is the Jacobian. Call it $L(y)$. Because $L(y)$ is always an orthogonal matrix (when $|y| = 1$) with determinant $+1$ (lemma 11), this map is everywhere smooth, orientation-preserving, and 1-to-1 on the sphere of unit-norm 2^n-ons, for every $n > 0$.

But the right-multiplication map is *non*linear when $n \ge 4$ and hence is not so easily treated. Letting $x = (a, b)$ and $y = (c, d)$ be 2^n-ons regarded as ordered pairs of 2^{n-1}-ons, we see from EQ 68 that its Jacobian may be recursively constructed from the L and J matrices of a, b, c, d and the conjugation-inducing matrix $K = \mathrm{diag}(+1, -1, -1, \dots, -1)$: $J(y) =$

$$\begin{pmatrix} J(c) & -KJ(\overline{d}) \\ KL(\overline{b})KJ(\overline{\overline{\overline{b^{-1}}\,\overline{d}}})K & \begin{matrix} KJ(\overline{c})K + KJ(\overline{\overline{a}\,\overline{\overline{\overline{b^{-1}}\,\overline{d}}}})K \\ +KL(b^{-1})KL(\overline{a})KJ(\overline{d}) \end{matrix} \end{pmatrix}. \tag{193}$$

Table 24.1 gives the results of a Monte-Carlo empirical study of the behavior of $D = \det J$ when performing 20000 multiplications of random unit-norm 2^n-ons.

2^n	D	avg(D)	avg($\|D\|$)	%negative
1	always ± 1	0	1	50
2,4,8	always 1	1	1	0
16	$\in [2\times 10^{-5}, 154]$	≈ 1.02	≈ 1.02	0
32	$\in [-348, 714]$	≈ 0.50	≈ 0.65	25.3
64	$\in [-2340, 1839]$	≈ -0.17	≈ 4.46	48.1

Figure 24.1. Experimental study of the determinant D of the $2^n \times 2^n$ Jacobian matrix J of the right-multiplication map when multiplying unit-norm 2^n-ons. For each $n \in \{0,1,2,3,4,5,6\}$ we tried 20000 random pairs of unit-norm 2^n-ons. The numerical ranges given are delineated by the minimum and maximum determinant value (among the 20000) ever seen. All the bounds on the ranges whose absolute values are greater than 10, would increase unboundedly if an infinite number of samples had been taken, since it is easy to see that as $b \to 0$ with $x = (a, b)$, we have $|\det J(y)| \to \infty$.

This data is consistent with the hypothesis that 2^4-on multiplication (from either the left or the right) is a 1-to-1 orientation-preserving mapping on the unit-norm 2^4-ons (except perhaps on subsets of measure 0 where the map is discontinuous) and that 2^4-on division problems generically have a unique solution. Also, it is compatible with the hypothesis that the average value of $\det J$ is 1, for random unit-norm 2^4-ons.

And indeed results earlier in this monograph *prove* all these hypotheses about 16-ons. Also, all the patterns in the empirical data about 2^n-ons for $n \le 3$ has also been proven (comparatively trivially).

For 2^n-ons with $n \ge 5$, though, matters are different. For 32-ons, the average value of $\det J$ is apparently about 1/2, and, apparently, about 1/4 of the product 32-ons arising when multiplying random unit-norm 32-ons, have $\det J < 0$ (with average≈ -0.34), and about 3/4 of them have $\det J > 0$ (with average$\approx +0.74$). I.e., 32-on multiplication is sometimes a many-to-1 map and sometimes (about 1/4 of the time) is orientation-reversing.

Theorem 91 (Non-uniqueness for 32-on division). *Generic 32-on division problems do* not *have unique solutions; indeed a nonzero constant fraction of the 32-on division problems corresponding to products of random unit-norm 32-ons, have nonunique answers.*

Proof: This is a fully rigorous conclusion of the computer study in table 24.1 since all we need to establish it is the presence of *some* nonzero-measure neighborhood of one of our generic sample points, throughout which $\det J < 0$. Q.E.D.

(This of course also proves that the fundamental theorem of algebra fails at the 32-ons.)

Conjecture 92 (Non-uniqueness for 2^n-on division). *The above non-uniqueness statement also holds for the 2^n-ons, for each $n \ge 5$.*

Non-proofs: The Monte-Carlo computer experiments in table 24.1 are convincing evidence, but not a proof, of this for the 64-ons.

Because the 2^n-ons for each $n \ge 5$ include the 32-ons as a subalgebra, it might seem that by considering some sufficiently tiny, but nonzero-measure, neighborhood of one of our 32-on sample points at which there is nonuniqueness – our conclusion about 2^n-ons would immediately follow. However, that argument so far has been defeated by the obstacle that the 32-on subalgebra is the locus of the *discontinuity* in the 64-on multiplication map. Thus any argument about the many-to-1 character of a 32-on multiplication map might not necessarily carry over to generic 64-ons.

Theorem 93 (Finiteness of the nonuniqueness). *The cardinality of the non-uniqueness of solutions to generic 2^n-on division problems is* finite. *Also, for any 2^n-on division problem (or more general problem involving solving any fixed system of rational equations), if it has a finite number of solutions, that number is bounded by some explicitly writable function of n only.*

Proof: Consequence of general results [253] about systems of polynomial equations. Q.E.D.

Claim 94 (Nonexistence for division). *There do not always exist solutions to generic 32-on division problems.*

Computer demonstration: This is not a proof and could could conceivably (though it is unlikely) be incorrect. The key observation from the computer Monte-Carlo study in table 24.1 is that the average Jacobian determinant (and indeed, also the average *absolute value* of that determinant) is *less* than 1. This is not a rigorous demonstration, since it depends on a Monte Carlo numerical integration, i.e. depends on statistics and also on assumptions about the random number generator – but it nevertheless is highly convincing. Consequently it is impossible for the entirety of S^{31} to be covered by products xy if y is any fixed 32-on such that the averaged-over-x value of $|J(y)|$ is at or below the average-over-y. Hence there must be a nonzero-measure set of 32-on division problems with no solution.

Presumably generic 64-on, 128-on, etc. division problems also do not necessarily have solutions.

Remarks re rigor. It is in principle possible (although we have not done it) to make our nonrigorous computer demonstration of the lack of generic existence of solutions to division problems in the 32-ons rigorous – in several ways. (But all of these ways would depend on even heavier use of computers.) One could replace the Monte Carlo numerical integration with another numerical integration having rigorous error bounds. Alternatively, one could resort to (known) algorithms [52][215] (or our own suggestions in §21.2) for deciding whether solutions of any finite system of real polynomial equations exist. Such an algorithm could be applied to some appropriately chosen 32-on division problem, and would, by running to completion, prove nonexistence. (Unfortunately, present algorithms and computer hardware seem insufficiently powerful to do this in any reasonable amount of time.)

Despite theorems 91-94, $J(y)$ still obeys some nice properties in the 2^n-ons. It is actually somewhat more convenient to work with $\widetilde{J} = \left(\begin{smallmatrix} K & 0 \\ 0 & K \end{smallmatrix}\right) J \left(\begin{smallmatrix} K & 0 \\ 0 & K \end{smallmatrix}\right)$, where as usual $K = \operatorname{diag}(+1, -1, -1, \ldots, -1)$, which of course has the same determinant (and spectrum) as J. By the block triangularization identity

$$\det \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \det \begin{pmatrix} A & B \\ 0 & D - CA^{-1}B \end{pmatrix} = \det(A)\det(D - CA^{-1}B) \tag{194}$$

we have

$$\det J(y) = \det \widetilde{J} = \det \begin{pmatrix} KJ(c)K & -J(\overline{d})K \\ L(\overline{b})KJ(\overline{\overline{b^{-1}}\,\overline{d}}) & \begin{matrix} J(\overline{\overline{a}\,\overline{\overline{b^{-1}}\,\overline{d}}})+ \\ L(b^{-1})KL(\overline{a})KJ(\overline{d})K \end{matrix} \end{pmatrix}$$
$$= \det J(c) \det[J(\overline{c}) + J(\overline{\overline{a}\,\overline{\overline{b^{-1}}\,\overline{d}}}) + L(b^{-1})KL(\overline{a})KJ(\overline{d})K + L(\overline{b})KJ(\overline{\overline{b^{-1}}\,\overline{d}})KJ(c)^{-1}KJ(\overline{d})K] \quad (195)$$

Theorem 95 (Nice properties of right-mul map Jacobian). *Let $J(y)$ be the Jacobian matrix of the map $x \to xy$ wher x and y are 2^k-ons. Then*

1. *$J(ys) = sJ(y)$ for real s,*
2. *$\det J(y) = \det J(-y)$ if $n > 0$ so that 2^n is even.*
3. *$\det J(y) = \det J(\overline{y})$ if $n \geq 0$.*

Proof: $J(ys) = sJ(y)$ for real s is immediate from the scaling property in theorem 15. Using $s = -1$ leads to the next claim. The final claim now follows from the preceding claims combined with the identity EQ 195. Q.E.D.

25 Survey of identities satisfied and unsatisfied by 2^n-ons

We have already covered a large number of the most important 2^k-on identities in §6, 10, 15, 21.1, and 12. We shall not repeat them here, and shall instead concentrate on new ones[55].

Since we shall be stating a very large number of identities, we first shall define some *abbreviated notation* and conventions: The Jordan and Lie products are, respectively,

$$x \circ y \stackrel{\text{def}}{=} \frac{xy + yx}{2}, \quad [x, y] \stackrel{\text{def}}{=} xy - yx \quad (196)$$

and the "associator" is

$$(x, y, z) \stackrel{\text{def}}{=} xy \cdot z - x \cdot yz. \quad (197)$$

25.1 Miscellaneous identities

The identity

$$a \circ b + \langle a, b \rangle = b \operatorname{re} a + a \operatorname{re} b, \quad (198)$$

and equivalently EQ 34 , holds in all Cayley-Dickson algebras (it is an immediate consequence of considering $x = a + b$ in the quadratic identity of theorem 16). But in our 2^n-ons it holds only in coordinates 0-8 or if either a or b is a niner (as an immediate consequence of theorem 30).

The reader may enjoy the exercise of proving from EQ 49 and theorem 8 that

$$\operatorname{re}(ab) = \langle a, \overline{b} \rangle = \langle \overline{a}, b \rangle \quad (199)$$

holds in Cayley-Dickson algebras. The same law also holds in the 2^n-ons as a consequence of the analogous starting points.

Adem's identity [5] states that

$$x(y, z, w) + (x, y, z)w + (x, yz, w) = (xy, z, w) + (x, y, zw) \quad (200)$$

holds in all Cayley-Dickson algebras. However, in our 2^n-ons it holds only in the first 9 coordinates (indices 0-8).

Lemma 1.4.5 of [149] states that in the Cayley-Dickson 2^n-ons with $n \geq 4$, left-alternativity $(u, u, w) = 0$ holds for *all* u iff $w = (a, b)$ with $a, b \in \mathbb{R}$. [Of course, the same statement is true about right-alternativity $(w, u, u) = 0$.] In contrast, in our 2^n-ons, left-alternativity is always true and we know from theorem 34 that right-alternativity $(w, u, u) = 0$ holds whenever either u or w is a niner, i.e. for a far larger set of w.

These 3 identities (invented in a different context by Razmyslov [213] and Hentzel and Peresi [126] and [125] respectively)

$$[a, [a, b]^2] = 0 \quad (201)$$

and

$$[c^2, (b, a, c)] = [c, (b, a, c^2)] \quad (202)$$

$$(a^2, a, b) = (a, a^2, b) \quad (203)$$

hold for all 2^k-ons a, b, c for all $k \geq 0$, but $(b, a^2, a) = (b, a, a^2)$ only holds in the first $\min\{9, 2^k\}$ coordinates, with the others ignored, i.e.

$$(b, a^2, a)_{0,\ldots,8} = (b, a, a^2)_{0,\ldots,8}. \quad (204)$$

The following are true for 2^k-ons x, y – *but* in the first $\min\{2^k, 9\}$ coordinates only – for all $k \geq 1$:

$$\overline{a \cdot ba} = \overline{a} \cdot \overline{b}\overline{a}, \quad (205)$$

$$(a, b, c) + (\overline{a}, b, c) = 0. \quad (206)$$

The following is true for 2^k-ons with $k \leq 3$, and in the real coordinate alone (with the other coordinates ignored) it is true for all $k \geq 4$:

$$\overline{y}(x \cdot y\overline{x}) = (\overline{y} \cdot xy)\overline{x}. \quad (207)$$

The middle Moufang identity $(xy \cdot z)x = x(yz \cdot x)$, the left Bol identity $(x \cdot yx)z = x(y \cdot xz)$ and its variant $(x \cdot y\overline{x})z = x(y \cdot \overline{x}z)$ all hold for 2^k-ons x, y, z if $k \leq 3$; but if $k \geq 4$ they each only hold in the real coordinate *alone*, with the others ignored. (Consequently, certain squares, e.g. $[(xy \cdot a)x - x(ya \cdot x)]^2$, are always pure-real for 2^k-ons x, y, a for all $k \geq 0$; cf. corollary 17.)

The *Jordan identities*

$$xx \cdot yx = (xx \cdot y)x, \quad xy \cdot xx = x(y \cdot xx) \quad (208)$$

hold for 2^k-ons x, y with $k \leq 3$, and, in the real coordinate alone (with the other coordinates ignored) they are true for all $k \geq 4$. (They are also, trivially, true for all k if x is pure-imaginary, see corollary 18.)

[55] Also: There are an enormous number of identities valid in the quaternions or octonions, but *not* in any higher 2^k-ons. To conserve space, we have avoided trying to list all of these. See [136] appendix, [5] [12] [16] [21] [41] [42] [47] [49] [64] [68] [89] [94] [109] [110] [125] [126] [143] [169] [184] [209] [220] [222] [213] [233] [257] [259] [258] for ideas.

The *triple product identity*

$$y \cdot xy + yx \cdot y = 4\langle \overline{x}, y\rangle y - 2|y|^2 \overline{x} \tag{209}$$

holds for 2^k-ons x, y for each $k \le 3$, and is true in the real coordinate only with the other coordinates ignored, for each $k \ge 4$. Thus

$$\left(y \cdot xy + yx \cdot y - 4\langle \overline{x}, y\rangle y + 2|y|^2 \overline{x}\right)^2 \tag{210}$$

is pure-real in the 2^k-ons for all $k \ge 0$ by corollary 17.

The Amitsur-Levitzki identity ([16] theorems 1 and 3; [222])

$$\sum_{\sigma \in S_m} (-1)^\sigma x_{\sigma(1)}(x_{\sigma(2)}(x_{\sigma(3)}(\dots x_{\sigma(m)})\dots))) = 0 \tag{211}$$

(the left hand side is "an $m \times m$ determinant with m identical rows;" the sum has $m!$ terms) holds in the 2^n-ons, $n \ge 1$, if $m = 2^n$.

Proof: EQ 211 holds in the $(m/2) \times (m/2)$ matrices [16][222], and the parenthesizations are such that, due to the left-representations of the 2^n-ons as $2^{n-1} \times 2^{n-1}$ complex matrices (see remarks before theorem 14), it must hold in the 2^n-ons. Q.E.D.

EQ 211 with $m = 4$ and EQ 201 together were proved [89] to generate every polynomial identity obeyed by the quaternions (and biquaternions, i.e. 2×2 matrices over $\mathbb{C}$).

$[a, b] \circ [c, d]$ is pure real for octonion a,b,c,d, and hence

$$[[a, b] \circ [c, d], e] = 0 \tag{212}$$

for octonion a,b,c,d,e. Racine [209] proved that EQ 212 and the "big Racine identity"

$$P(a, b, c, x^2) = P(a, b, c, x) \circ x \tag{213}$$

where

$$P(a, b, c, x) \stackrel{\text{def}}{=} \tag{214}$$

$$x \circ (a \circ (b \circ c)) + x \circ (b \circ (c \circ a)) + x \circ (c \circ (a \circ b))$$
$$-x \circ (c \circ (b \circ a)) - x \circ (a \circ (c \circ b)) - x \circ (b \circ (a \circ c)) \tag{215}$$

together with the alternative laws generate every polynomial identity of degree≤ 5 obeyed by the octonions. However, all of these fail in the 16-ons (but work [126] in every Cayley-Dickson 2^n-dimensional algebra for all n).

There are many identities that hold in every left-alternative ring, but which fail in the 16-ons. Among these are Mikheev's $(w, x, x)^4 = 0$ and the various possibilities offered by Chuvakov [64]. Similarly there are many identities that hold in every quadratic algebra, but fail in the 16-ons. Among these are Hentzel and Peresi's $[(a, b, a), a] = 0$ [126] and the big Racine identity (EQ 213). (Of course the 16-ons are not a ring and not a [linear] algebra, since nondistributive, explaining how these conflicts are possible.) Hentzel and Peresi's ([126], eq. 11)

$$a(a, b, b) + b(b, a, a) + a \circ (b, a, b) + b \circ (a, b, a) = (a, b, ab) + (b, a, ba) \tag{216}$$

is obeyed in the octonions, but in the 2^k-ons with $k \ge 4$, is obeyed in the real coordinate only.

25.2 Generalizations of "vector product"

Definition 96. (Eckmann [95][97][98]): A "vector product" of r vectors in $\mathbb{R}^n$ is a function, mapping $(\mathbb{R}^n)^r \to \mathbb{R}^n$, obeying the following two properties[56]:

orthogonality:

$$\langle \text{vp}(\vec{x}_1, \vec{x}_2, \vec{x}_3, \dots, \vec{x}_r), \vec{x}_j\rangle = 0 \quad \text{for each } j = 1, 2, 3, \dots, r \tag{217}$$

length=area relation:

$$|\text{vp}(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_r)|^2 = \det \begin{pmatrix} \langle \vec{x}_1, \vec{x}_1\rangle & \langle \vec{x}_1, \vec{x}_2\rangle & \dots & \langle \vec{x}_1, \vec{x}_r\rangle \\ \langle \vec{x}_2, \vec{x}_1\rangle & \langle \vec{x}_2, \vec{x}_2\rangle & \dots & \langle \vec{x}_2, \vec{x}_r\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \vec{x}_r, \vec{x}_1\rangle & \langle \vec{x}_r, \vec{x}_2\rangle & \dots & \langle \vec{x}_r, \vec{x}_r\rangle \end{pmatrix} \tag{218}$$

Eckmann proved that r-*multilinear* vector products exist precisely for the following (r, n): $(1, 2k)$ with $k \ge 1$, $(n-1, n)$ with $n \ge 3$, $(2, 7)$, and $(3, 8)$. Then, by using topological results of Adams, he proved that this is still the full list even if we relax the requirement of multilinearity to now merely requiring *continuity*.

Examples of multilinear vector product functions that accomplish this are as follows [46][265].

r = 1, n = 2k: replace every pair of consecutive coordinates (x, y) by $(-y, x)$. [One could also use $(y, -x)$, so there are two choices per pair; also the pairs need not be consecutive elements. Taking these possibilities into account, we conclude that there are at least $(2k)!/k!$ different answers to this question.]

r = n − 1: Make an $n \times n$ matrix out of our $n - 1$ vectors (each n-dimensional) plus one extra row. Use the cofactors (arising when expanding the determinant of the matrix) of the elements of the extra row, as the n coordinates of the vector product. Note: when $r = 2$, $n = 3$ this is the usual 3D vector cross product, which also arises by regarding the two 3-vectors as pure-imaginary quaternions, multiplying them, and discarding the real part of the result.

r = 2, n = 7: Regard the two 7-vectors as pure-imaginary octonions, multiply them, and discard the real coordinate of the result.

r = 3, n = 8: Regard the three 8-vectors as octonions a, b, c. There are two inequivalent such vector products:

$$\text{vp}_1(a, b, c) = -a \cdot \overline{b}c + \langle a, b\rangle c + \langle b, c\rangle a - \langle c, a\rangle b, \tag{219}$$

$$\text{vp}_2(a, b, c) = -a\overline{b} \cdot c + \langle a, b\rangle c + \langle b, c\rangle a - \langle c, a\rangle b \tag{220}$$

which differ by $(a, \overline{b}, c)$.

We now point out that if the demand of multilinearity is dropped and replaced by merely demanding that the vector product function be *rational*, then we can get *additional* vector product functions at (r, n) previously deemed impossible:

[56] This generalizes the definition for $r = 2$ given in theorem 4 item 4.

Theorem 97 (Vector product). *Let a and b be (2^k-1)-vectors, regarded as 2^k-ons with real coordinate 0, i.e. pure-imaginary 2^k-ons. Then the following function:*

$$a \times b \stackrel{\text{def}}{=} ab - \text{re}(ab) \tag{221}$$

(i.e. ab with the real part discarded) is a vector product (with $r=2$ and $n=2^k-1$) for every $k \geq 2$. But rational $(2,n)$ vector products are impossible unless n is of the form $n=2^k-1$, so our construction achieves every achievable n.

Proof: The first orthogonality statement $\langle a\times b, a\rangle = 0$ (for pure-imaginary a, b) arises from, e.g. $\langle ab+s, a\rangle = \langle ab, a\rangle = \langle b, \overline{a}a\rangle = \langle b, |a|^2\rangle = 0$ where s is any real. The second orthogonality statement $\langle a\times b, b\rangle = 0$ arises from $\langle ab+s, b\rangle = \langle b, \overline{a}b\rangle = \langle 1, \overline{b}\cdot\overline{a}b\rangle = \langle 1, b\cdot ab\rangle$ (if s is any real and a,b are pure-imaginary) and now use weak-flexibility (theorem 35) to see that the real part of $b\cdot ab$ is the same as the real part of $ba\cdot b$. But $\langle ba\cdot b, 1\rangle = \langle \overline{ba}, b\rangle = -\langle ba, b\rangle = -\langle a, \overline{b}b\rangle = -\langle a, |b|^2\rangle = 0$. Finally, the fact that $|a\times b|^2 = |a|^2|b|^2 - \langle a,b\rangle^2$ for pure-imaginary a, b is just a restatement of $|ab|^2 = |a|^2|b|^2$ with the aid of weak-linearity.

Finally, we must prove the impossibility statement for $n \neq 2^k-1$. Realize that by using EQ 4 "backwards" we may use the n-dimensional vector product to define an $(n+1)$-dimensional product. It can be directly seen that this product causes the Euclidean norm to be multiplicative, if the length=area and orthogonality properties of the vector product hold. But since rational algebra multiplications causing the Euclidean norm to be multiplicative happen *only* in power-of-2 dimensions (Pfister; see our theorem 4 item 6) a rational vector product can exist only in 2^k-1 dimensions. Q.E.D.

The $(r=2, n=15)$ vector product is a rational and generalized-smooth function (or more precisely it is 15 different rational functions), but it is not linear and not continuous. The $(2,31)$, $(2,63)$, $(2,127)$, etc., vector products are rational, but are not "generalized smooth" (defined in §22).

Is there a $(3,2^k)$ vector product, generalizing the known cases $k=2$ and $k=3$? Apparently not. If one tries to use EQ 219 and EQ 220 for *16-on* a,b,c, then indeed

$$\langle \text{vp}_1(a,b,c),\, a\rangle = 0 \quad\text{and}\quad \langle \text{vp}_2(a,b,c),\, c\rangle = 0 \tag{222}$$

hold (as may be proven by computer; and in fact these continue to hold in the 2^k-ons for all $k\geq 2$), but

$$\langle \text{vp}_1(a,b,c),\, b\rangle,\ \ \langle \text{vp}_1(a,b,c),\, c\rangle,\ \ \langle \text{vp}_2(a,b,c),\, a\rangle,\ \ \langle \text{vp}_2(a,b,c),\, b\rangle \tag{223}$$

are, in general, nonzero. Also, EQ 218 then holds only when $k\in\{2,3\}$.

25.3 Vector products as Lie (Malcev, etc.) algebras

A *Lie algebra* is a linear algebra with an *anticommutative* multiplication $(xy+yx=0)$, obeying the 3rd degree *Jacobi identity*

$$xy\cdot z + zx\cdot y + yz\cdot x \;=\; 0. \tag{224}$$

One natural way in which Lie algebras A^- arise is by using the "Lie product" $[x,y] \stackrel{\text{def}}{=} xy - yx$, instead of the usual product, in an *associative* algebra A. This is obvious once one realizes that the left hand side of the Jacobi identity based on Lie products may be rewritten as a sum of associators:

$$\begin{aligned}[[x,y],z] + [[z,x],y] + [[y,z],x] = \\ (x,y,z)+(z,x,y)+(y,z,x) \\ -(x,z,y)-(z,y,x)-(y,x,z).\end{aligned} \tag{225}$$

In particular, if we use the pure-imaginary quaternions as A we get as A^- the 3-dimensional Lie algebra of vector cross products in this way. (Also, if we multiply two pure-imaginary quaternions using the usual quaternion product, *and* zero the real part of the result, this is the same thing, except for an overall factor of 2, which does not affect the validity of EQ 224.)

The octonions, however, are non-associative. The algebra of "7-dimensional vector cross products," i.e. of pure-imaginary octonions under the Lie-octonion multiplication, is *not* Lie, i.e. does not obey the Jacobi identity. However, if A is an *alternative* algebra, then A^- is (although not Lie unless A is associative) still a *Malcev* algebra [182], i.e. it has an anticommutative multiplication obeying the 4th degree *Malcev identity*

$$xy\cdot xz = (xy\cdot z)x + (yz\cdot x)x + (zx\cdot x)y. \tag{226}$$

(Every Lie algebra is Malcev, but the reverse is not the case.) Thus the pure-imaginary octonions under Lie multiplication (or under ordinary octonion multiplication with zeroing of the real part of the result, which is the same thing except for an overall factor of 2) form a 7D Malcev algebra. This, in fact, is known to be the *only* simple Malcev algebra that is not a Lie algebra [182].

In a linear algebra, equivalent forms of the Malcev identity include the more-symmetrical looking *4*-variable Sagle's identity [223][224]

$$(xy\cdot z)t+(tx\cdot y)z+(zt\cdot x)y+(yz\cdot t)x = xz\cdot yt = zx\cdot ty = yt\cdot zx = ty\cdot xz \tag{227}$$

its mirror

$$t(z\cdot yx) + x(t\cdot zy) + y(x\cdot tz) + z(y\cdot xt) = ty\cdot zx, \tag{228}$$

and

$$J(x,y,xz) = J(x,y,z)x, \quad J(zx,y,x) = xJ(z,y,x) \tag{229}$$

where $J(x,y,z)$ is the left hand side of EQ 224.

It is unknown what the 16-on generalization of the Malcev identity should be (if there is one).

25.4 Vector products – other properties

Everyone knows that the usual 3D vector products obey lots of identities – but how many of them are satisfied by our new, higher-dimensional vector products? For brevity, let us write $a\times b$ for the vector product of (2^k-1)-vectors a and b, instead of writing $ab - \text{re}(ab)$ where a and b are pure-imaginary 2^k-ons.

Vasilovskii [245] pointed out that all polynomial identities of the 3D vector product $\times$ follow from this single 4-variable master identity:

$$((y\times z)\times(t\times x))\times x + ((y\times x)\times(z\times x))\times t = 0. \tag{230}$$

But EQ 230 fails in ≥ 7 dimensions.

Anticommutativity

$$a \times b + b \times a = 0 \quad (231)$$

holds in the pure-imaginary 2^k-ons for $k \leq 3$, but in general *fails* if $k \geq 4$. (When $k = 4$, EQ 231 holds in the first 8 imaginary coordinates, but fails in the last 7.) The discarding of the real part destroys associativity, even for the 3D vector product:

$$i \times (j \times j) = i \times 0 = 0 \neq -i = k \times j = (i \times j) \times j. \quad (232)$$

Of course, right-linearity

$$a \times (b + c) = a \times b + a \times c \quad (233)$$

holds eternally, but left-linearity

$$(b + c) \times a = b \times a + c \times a, \quad (234)$$

while valid if $k \leq 3$, in general *fails* if $k \geq 4$. (When $k = 4$, EQ 234 holds in the first 8 imaginary coordinates, but fails in the last 7. This partial success is a consequence of 9-coordinate distributivity, see theorem 34.) For *scalar* s,

$$(sa) \times b = s(a \times b) = a \times (bs) = a \times (sb) = (a \times b)s. \quad (235)$$

Also

$$a \times a = 0 \quad (236)$$

holds for pure-imaginary 2^k-ons a, for each $k \geq 2$ (as a consequence, essentially, of the fact that a^2 is pure-real if a is pure-imaginary, which follows in turn from corollary 17). Although

$$a \times (a \times b) = \langle a, b\rangle a - |a|^2 b \quad (237)$$

holds in the pure-imaginary 2^k-ons for each $k \geq 2$,

$$(b \times a) \times a = \langle a, b\rangle a - |a|^2 b \quad (238)$$

holds, in general, when $k \in \{2, 3\}$ only.

The cyclic interchange rule for inner products

$$\langle c, a \times b\rangle = \langle a, b \times c\rangle = \langle b, c \times a\rangle \quad (239)$$

holds in the pure-imaginary 2^k-ons for $k \leq 3$ but in general *fails* if $k \geq 4$. Both Lagrange's identity

$$\langle a \times b, c \times d\rangle = \langle a, c\rangle\langle b, d\rangle - \langle a, d\rangle\langle b, c\rangle \quad (240)$$

and Grassman's identities

$$a \times (b \times c) = \langle a, c\rangle b - \langle a, b\rangle c, \quad (241)$$
$$(a \times b) \times c = \langle c, a\rangle b - \langle c, b\rangle a \quad (242)$$

hold in the quaternions but (in general) *fail* in the 2^k-ons for each $k \geq 3$.

The following special cases of Grassman's identities

$$a \times (b \times a) = |a|^2 b - \langle a, b\rangle a, \quad (243)$$
$$(a \times b) \times a = |a|^2 b - \langle a, b\rangle a \quad (244)$$

hold in the pure-imaginary 2^k-ons for $k \leq 3$ only. However, EQ 244 holds for *all* k, *if* we only pay attention to the first $\min\{2^k, 9\}$ coordinates on both sides.

26 Relevant results from elementary abstract algebra

This section will begin by reviewing the (mostly standard) definitions of loops, groups, nnac-rings, etc. Then we construct, for the first time, a large taxonomy of known loop types. For us, this taxonomy serves the useful role of providing a classification and road map to a large number of 2^n-on identities and non-identities, allowing us to see how the 2^n-ons fit in to the larger picture of all loops and all abstract algebraic systems. But the loops taxonomy should be of more general interest.

Then we discuss, albeit in much less detail, what the analogous taxonomy would be for quasigroups and nnac-rings, and we conclude by introducing a new abstract algebraic entity we call "abstract 2^n-ons."

26.1 Quick review of elementary algebra definitions

A *magma* is a set S of elements together with a binary operation (usually called "multiplication" and denoted by juxtaposition and/or $\cdot$) on those elements, such that $a, b \in S$ implies $ab \in S$.

A *quasigroup* is a magma such that $a, b \in S$ implies the existence of unique x, y so that $ax = b$, $ya = b$, i.e. in which left- and right-division are possible.

A *loop* is a quasigroup containing an *identity element* 1 such that $x \in S$ implies $1x = x1 = x$. (Note. If the operation is called $+$ instead of $\cdot$, i.e. we are speaking of an additive loop, then the identity element is called 0 instead of 1.)

A *group* is a loop obeying the associative law that $x, y, z \in S$ implies $xy \cdot z = x \cdot yz$. The easiest theorem in group theory is

Theorem 98 (Inverses in groups). *Each element x of a group has a unique 2-sided inverse x^{-1} such that $x^{-1}x = xx^{-1} = 1$. Indeed, in an associative magma with a left-identity 1 with $1x = x$ we have that $x^{-1}x = 1$ implies $xx^{-1} = 1$.*

Proof: By associativity $(x^{-1})^{-1} \cdot x^{-1}y = y$. Write xy in place of y to see $(x^{-1})^{-1}(x^{-1} \cdot xy) = xy$. Hence $(x^{-1})^{-1}(x^{-1}x \cdot y) = (x^{-1})^{-1}y = xy$. Write x^{-1} in place of y to see $1 = (x^{-1})^{-1}x^{-1} = xx^{-1}$. Q.E.D.

(Note. In additive groups the inverse of x is denoted $-x$ rather than x^{-1}. McCune [177] pointed out that a minimal set of group axioms is $1x = x$, $x^{-1}x = 1$, and $xy \cdot z = x \cdot yz$.)

A *semigroup* is an associative magma.

An *abelian group* is a group obeying the commutative law that $x, y \in S$ implies $xy = yx$.

A *nnac-ring* is a multiplicative magma equipped with a second binary operation $+$ with respect to which it simultaneously is an additive abelian group, and such that these operations obey the distributive laws $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

A *ring* is a nnac-ring with an associative multiplication.

Rings and nnac-rings are *unital* if they have a multiplicative identity 1 so that $1x = x1 = x$.

A nnac-ring S has *characteristic 2* if $x + x = 0$ holds for all $x \in S$. Otherwise it has characteristic not 2. (More generally if k is the least positive integer so that multiplying a ring-element by k always yields 0, then the ring has "characteristic k.")

A *nnc-field* is a ring whose nonzero elements form a multiplicative group.

A *field* is a nnc-field with commutative multiplication.

26.2 A taxonomy of loops

There are at least 50 species of finite loops interesting enough to have been christened and to have had theorems proven about them. These species and results have gradually accumulated scattered throughout the literature, resulting in a confusing mare's nest of relationships among them. The purpose of this section is to notice that a vast number of loop definitions can be summarized in a table (figure 26.1), and then an even vaster number of results about finite loops can be summarized in a single diagram (figure 26.3). Although the task of completely elucidating this diagram remains incomplete, it nevertheless is very useful.

Most of the attention of loop theorists has focused on the question of what properties we can require loops to obey, which make them "closer to being a group." The question then how many theorems from group theory will then hold (perhaps in some altered form) in that kind of loop. For example, since the Moufang law is a weakening of the associative law, so we might expect Moufang loops to have some group-like properties.

Building diagram 26.3 felt rather like Linnaeus classifying life-forms into phylla and species. Although at first I felt that drawing the diagram was merely a mechanical task of summarizing known results, and therefore could not possibly lead to anything new, that impression was incorrect, for two reasons:

1. Because the mare's nest is so complex, at least one important mistake had escaped previous notice[57].
2. The taxonomy-diagram enables one rapidly to get a sense of where a species of loops fits into the whole picture. That in turn focuses attention on the right questions needed to fill in the "missing links" in the diagram – and then some of those questions may be answered easily.

We begin with figure 26.1, tabulating the definitions of over 40 different kinds of loops got by adjoining an extra requirement (tabulated) to the defining axioms of a loop. To read it, one needs a little more **loop notation:**

Left-division: $a\backslash b$ is the unique solution to $ax = b$. Similarly for right-division: b/a is the unique solution to $xa = b$. These have precedence the same as $\cdot$ but lower than juxtaposition, e.g. $a\backslash bc = a\backslash(bc)$. Left-inverse: $x^L \stackrel{\text{def}}{=} x\backslash 1$; right-inverse: $x^R \stackrel{\text{def}}{=} 1/x$; we agree that when the superscript is an R or L it does *not* connote exponentiation.

The *multiplication group* of a loop L is the group generated by all the permutations of L's elements of the form $x \to xy$ and $x \to yx$ for $y \in L$. The *inner mappings* are the subgroup of the multiplication group which preserve 1.

Two loops with the same set of elements are *isotopes* of each other if multiplication in one loop, denotes $*$, is defined by $x * y = x/b \cdot a\backslash y$ for some fixed loop elements a, b. Two loops are *isomorphic* if there is some bijective function f mapping elements of the first loop to elements of the second such that $f(x) \cdot f(y) = f(x \cdot y)$.

[57] According to Math'l Reviews 96k:20153, Solarin & Chibova [238] proved that C-loops are conjugacy-closed. We give a 10-element counterexample in figure 26.2.2d.

#	L	Q	2^n-ons	type of loop	defining identity
1	•	•	$n \le 2$, $8_{\mathbb{R}}$	Group (assoc.)	$x \cdot yz = xy \cdot z$
2	•	•	$n \le 3$, $\mathbb{R}$, $i_{\text{if } k \text{ even}}$	Pflugfelder M_k-loop [201]	$xy \cdot zx^k = (x \cdot yz)x^k$ for fixed integer $k \ge 1$
3			no n	tag-loop [90]	Transitive automorphism group
4	•	?		Bruck-loop [19]	R-Bol $\wedge$ AI
5	•	•	$8i$, $8_{\mathbb{R}}$	Fenyves "Extra loop" [104][105]	$x(y \cdot zx) = (xy \cdot z)x$
6	•	•	$n = 0$	Alternative A-loop [151]	diassociative $\wedge$ A-loop
7	•	•	$8i$, $8_{\mathbb{R}}$	PA-CC	Power-assoc $\wedge$ conju.closed
8	•	?	$n \le 2$, $\mathbb{R}$, $i_{n \le 3}$	Wilson [256]	$x \cdot (xy)^{-1} = xz \cdot (x \cdot yz)^{-1}$ where $xx^{-1} = 1$
9	•	•	$8i$, $8_{\mathbb{R}}$	conjugacy-closed (CC) [116][150][161]	L-conju.closed $\wedge$ R-conju.closed
10			$n \le 2$	G-loop [115]	isomorphic to all its isotopes
11	•	•	$n \le 3$	Moufang [181][180]	$xy \cdot zx = (x \cdot yz)x$
12			$8i$, $8_{\mathbb{R}}$	Central loop ("C-loop") [104][105][204]	$x(y \cdot yz) = (xy \cdot y)z$
13		•	see table 26.2	RIF-loop [152]	inverse-property $\wedge$ inner mappings preserve
			$n \le 3$		inverses; equivalently $xy \cdot (z \cdot xy) = (x \cdot yz)x \cdot y$
14			$n \le 3$	ARIF [152]	W1 $\wedge$ W2 $\wedge$ flexible
15			$n \le 3$	W1 [152]	$zx \cdot (yxy) = z(xyx) \cdot y$
16			$n \le 3$	W2 [152]	$(yxy) \cdot xz = y \cdot (xyx)z$
17		•	$n \le 3$	diassociative [180][47]	subloop generated by x, y is group
18	?		$n \le 3$	Left-Bol [47]	$x(y \cdot xz) = (x \cdot yx)z$
19	?		$n \le 3$	Right-Bol [47]	$x(yz \cdot y) = (xy \cdot z)y$
20		•	i, $8_{\mathbb{R}}$	LC-loop [104][105][204]	$xx \cdot yz = (x \cdot xy)z$
21		•	$8i$, $8_{\mathbb{R}}$	RC-loop [104][105][204]	$x(yz \cdot z) = xy \cdot zz$
22			$n = 0$	A-loop [50]	inner mappings are automorphisms
23		•	$n \le 3$, $\mathbb{R}$	IP-alternative	Inverse-property $\wedge$ alternative
24			•	power-associative [102]	powers of x form multiplicative group
25			$n \le 3$, $\mathbb{R}$	alternative [47]	LR-alternative$\cap$flexible
26		•	$n \le 3$, $\mathbb{R}$	Inverse-property (IP) [47]	LIP $\wedge$ RIP
27			$n \le 3$, $\mathbb{R}$	flexible [47]	$x \cdot yx = xy \cdot x$
28			$n \le 3$, $\mathbb{R}$	LR-alternative (LRalt)	L-alternative $\wedge$ R-alternative
29			•	L-alternative (Lalt)	$x \cdot xy = xx \cdot y$
30			$n \le 3$, $\mathbb{R}$	R-alternative (Ralt)	$x \cdot yy = xy \cdot y$
31			i, $8_{\mathbb{R}}$	nuclear-square (NS) [104][105][204]	L-nuclear-sq.$\wedge$M-nuclear-sq.$\wedge$R-nuclear-sq.;
					equivalently all orderings of x, y, z^2 associate
32			i, $8_{\mathbb{R}}$	L-nuclear-sq. (LN)	$xx \cdot yz = (xx \cdot y)z$
33		•	i, $8_{\mathbb{R}}$	M-nuclear-sq. (MN)	$x(yy \cdot z) = (x \cdot yy)z$
34			i, $8_{\mathbb{R}}$	R-nuclear-sq. (RN)	$x(y \cdot zz) = xy \cdot zz$
35			•	L4-power-assoc. (L4PA)	$x \cdot (x \cdot xx) = xx \cdot xx$
36			•	3-power-assoc. (3PA)	$x \cdot xx = xx \cdot x$
37			•	L-Inverse-property (LIP)	$x^{-1} \cdot xy = y$
38			$n \le 3$, $\mathbb{R}$	R-Inverse-property (RIP)	$yx \cdot x^{-1} = y$
39		?	$n \le 3$; see tab. 26.2	Weak-Inverse-property (WIP) [190]	$x^{-1} = y(xy)^{-1}$
40	?		$8i$, $8_{\mathbb{R}}$	R-conjugacy-closed (RCC)	$z \cdot yx = (zy/z) \cdot zx$
41	?		$8i$, $8_{\mathbb{R}}$	L-conjugacy-closed (LCC)	$xy \cdot z = xz \cdot (z \backslash yz)$
42			$n \le 3$, 9	Antiautomorphic (aa)	$(xy)^{-1} = y^{-1}x^{-1}$
43		?	$\mathbb{R}$	Automorphic Inverse (AI)	$(xy)^{-1} = x^{-1}y^{-1}$
44			•	Has 2-sided inverses (2SI)	$\forall x \exists x^{-1}$: $x^{-1}x = xx^{-1} = 1$
45			no n	Steiner	$xy = yx \ \wedge \ x \cdot xy = y$
46			$n \le 1$, $\mathbb{R}$	Abelian	$xy = yx$
47	•	•	no n	Binary group	$xy = yx \wedge xx = 1 \wedge x \cdot yz = xy \cdot z$

Figure 26.1. 47 named kinds of loops.

How to read figure 26.1. Any group automatically simultaneously is all the kinds of loops above the line. The "L" column includes a mark "•" if this kind of loop obeys the Lagrange property, no mark if it disobeys it, and The "Q" column is marked "•" iff this kind of *quasigroup* is necessarily a loop [162][205]. Statements involving x^{-1} should be read as "for all x there exists a function of x called x^{-1} such that...". Unless otherwise stated, all identities mentioned are true in the 2^n-ons if $n \le 2$. The "2^n-on" column includes

- • if the defining identity holds for all 2^n-ons; i if it holds for all pure-imaginary 2^n-ons,
- $\mathbb{R}$ if it holds for all 2^n-ons in the real coordinate only; $i_{\mathbb{R}}$ if it holds for pure-imaginary 2^n-ons in the real coordinate only,

9 if it holds for all 2^n-ons in coordinates $0, \ldots, 8$,
$8_{\mathbb{R}}$ if it holds for octonions in the real coordinate only; $8i_{\mathbb{R}}$ if it holds for pure-imaginary octonions in the real coord. only,
$8i$ if it holds for pure-imaginary octonions, and
A condition on n: if true for 2^n-ons obeying that condition.

For each $n \geq 0$, the 2^n-on *basis* elements form a 2^n-element Steiner loop if their signs are ignored.

#	2^n-ons	type of loop & defining identity
0	•	$t \cdot x\overline{t} = \overline{t \cdot \overline{x}\overline{t}}$
1	$n \leq 3$	$xy(z \cdot xy) = (x \cdot yz)x \cdot y$
2	i, 9, $n \leq 3$	$(b \cdot ac)d = \overline{(b \cdot \overline{a}c)d}$ where $d = \overline{bc}$
3	•	$d(b \cdot ac) = \overline{d(b \cdot \overline{a}c)}$ where $d = \overline{bc}$
4	*, $n \leq 3$	$(ab \cdot c)d = \overline{(\overline{a}b \cdot c)d}$ where $d = \overline{bc}$
5	•	$d(c \cdot ba) = \overline{d(c \cdot b\overline{a})}$ where $d = \overline{cb}$
5	$n \leq 3$, 9	LWIP: $x^L = (yx)^L y$
6	$n \leq 3$, $\mathbb{R}$	RWIP: $y(xy)^R = x^R$

Figure 26.2. RIF-like (above line) and WIP (below line) properties of the 2^n-ons. The meanings of the codes in the 2^n-on column are the same as in figure 26.1. (*) The identity in line 4 is valid for *pure-imaginary* 2^n-ons for all n, provided the real coordinate is ignored (i.e. if the "=" is interpreted as "the imaginary coordinates are equal").

Remarks on the loop definitions in figure 26.1: McCune [177] pointed out that a minimal set of axioms for a Moufang loop is $1x = x$, $x^{-1}x = 1$, and $(xy \cdot z)y = x(y \cdot zy)$. One may substitute $(xy \cdot x)z = x(y \cdot xz)$ but not $(x \cdot yz)x = xy \cdot zx$ for the lattermost of these. In a loop, any of the 4 Moufang equalities EQ 11 implies the other three ([47] lemma 3.1 p115; [200] ch. IV). Wilson [256] showed that M_3 loops were the same thing as Moufang Wilson loops while Chein and Robinson [63] showed these were the same as Fenyves' "extra" loops. Wilson loops are conjugacy-closed [116], and indeed showed the M_3 loops are the same thing as the flexible CC loops while the Wilson loops are the CC loops obeying the "right weak inverse property" (RWIP) that $y(xy)^R = x^R$.

The M_k loops are members of an even larger class of loops gotten by regarding x^k, *not* as the kth power map, but rather as an *arbitrary* map among loop elements. Pflugfelder [201] and Chein and Robinson [63] proved that (with this wider interpretation applied to x^k and x^g)

1. A loop obeying the M_k-loop defining identity
2. A Moufang loop such that x^g always is "nuclear," i.e. associates with everything in the loop (where $x \cdot x^g = x^k$)

were the same thing. In particular M_1 and Moufang loops are the same thing, and M_2 loops are the same thing as groups. As another application, the power-map M_a loops automatically are also M_b if $a - 1$ divides $b - 1$.

Outside of the loops literature, LIP is more commonly called "left cancellation" and RIP "right cancellation." Any two among {LIP, RIP, antiautomorphism} implies the third and implies the inverse-property [47]. (However, no one among these three implies any other, due to counterexamples of cardinality≤ 6.)

RWIP, the right weak inverse property, is $y(xy)^R = x^R$, and LWIP, the left weak inverse property, is $x^L = (yx)^L y$. Osborn [190] showed that RWIP and LWIP imply each other; therefore they are more commonly simply called WIP, for *weak inverse property.* WIP and antiautomorphism together are equivalent to the full inverse property IP.

Any two among {AI, Abelian, antiautomorphism} implies the third. Any conjugacy-closed loop obeying $xx = 1$ is an Abelian group (corr. 3.24 of [150]).

The presence of antiautomorphism in a loop causes the Left and Right versions of any property to imply its mirror, e.g. L-Bol$\Longleftrightarrow_{\text{antiaut}}$R-Bol$\Longleftrightarrow_{\text{antiaut}}$Moufang, antiaut$\Longrightarrow$2-sided inverses, etc. For example, for a complete proof that L-alternative$\Longrightarrow_{\text{antiaut}}$R-alternative see the proof of theorem 56.

The definitions of W1 and W2 given in figure 26.1 really only are unambiguous as stated if flexibility is *assumed.* (Or, they could be disambiguated by agreeing on any particular parenthesizations for the 3-term products. If W1 is assumed to hold for *both* possible parenthesizations of its righthand side [or its lefthand side], then flexibility happens automatically.) Then W1$\wedge$flexible$\Longrightarrow$inverse-property [152]. By mirror symmetry, W2$\wedge$flexible$\Longrightarrow$inverse-property also. (This is one of many instances where deductions may be made using mirror symmetry.)

Figure 26.3 gives a large set of inclusion and equivalence relations amongst these classes of loops. These relations were either extracted from the literature [204][217] [152] [104][105][115][116] [150] [151][200][47] [161] or proved (or disproved) ourselves. McCune's automated deduction engines `Otter` [176] and `Mace2` [175] were very helpful for constructing such proofs or counterexamples. For example:

Theorem 99 (Proved by `Otter` in 10 milliseconds). *A loop which is both right-alternative and flexible is automatically L4-power-associative.*

As another example, the question arises whether a flexible left-alternative left-cancellative loop could avoid being antiautomorphic, right-alternative, right-cancellative, or weak-inverse. The answer "yes" was proven by `Mace2` in a fraction of a second. Specifically, given the following *hypotheses*:

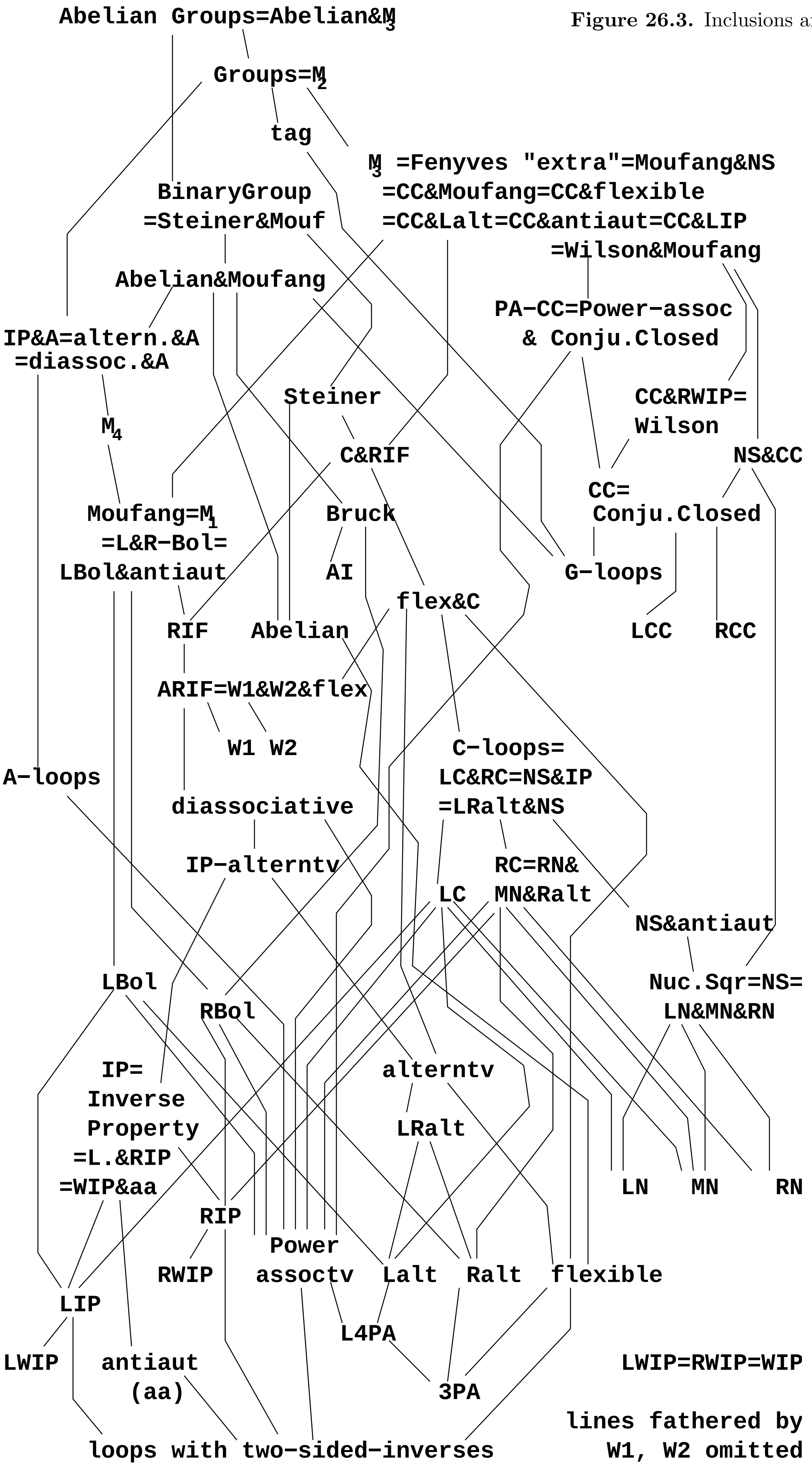
$$xy = xz \implies y = z, \quad yx = zx \implies y = z, \tag{245}$$
$$\forall xy \exists z(zx = y), \quad \forall xy \exists z(xz = y),$$
$$1x = x1 = x, \quad x^{-1}x = xx^{-1} = 1, \quad (x^{-1})^{-1} = x,$$
$$xy \cdot x = x \cdot yx, \quad xx \cdot y = x \cdot xy, \quad x^{-1} \cdot xy = y$$

`Mace2` found the 6-element loop in table 26.2.2f.

Unfortunately, for hard problems, there is no limit to the amount of computer time `Otter` and `Mace` require[58].

[58]The speed, reliability, and deductive power of `Otter` and `Mace2` are definitely superhuman on *some* problems, but on other problems their speed and power are definitely subhuman. `Otter` often is strong in loop theory but seems extremely weak on nnac-ring theory.

Figure 26.3. Inclusions among about 50 classes of loops.



	False implication	size	disproof
1	Flexible∧C-loops⟹RIF	24	table 1 of [152]
2	ARIF⟹C∨RIF	?	section 4 of [152]
3	C⟹flexible	12	table 2 of [152]
4	tag⟹group		[90]
5	Inverse property⟹3-power-associative	8	mace
6	Extra⟹group	16	example 1 of [204]
7	Moufang⟹LN∨MN∨RN	?	Example 2 in [204]
8	3PA⟹power-associativity	6	Example 3.1 of [204]
9	NS∧2-sided inverses⟹antiautomorphic∨LIP	5	mace
10	Antiautomorphism⟹3-power-associativity	6	mace
11	Flexibility⟹Antiautomorphism	6	mace
12	Power-assoctv∧Conju.-closed∧NS⟹diassociative	16	table 2 of [151]
13	LN⟹3-power-associative∨MN.	6	Example 7 of [204]
14	MN⟹3-power-associative	6	Example 8 of [204]
15	RN∧LN⟹MN	8	mace
16	LC⟹RN∨Ralt	12	ex. 5 of [204]
17	MN∧LN⟹RN	≥ 8	since would imply RC and C
18	RIF∧flexible∧C⟹Moufang∨Steiner		[152]
19	RIF⟹C		[152]
20	Steiner∧C∧RIF⟹Moufang	10	table 1 of [105]
21	L-alternative∧R-alternative∧C-loop∧2-sided-inverse ⟹Moufang∨antiautomorphic∨flexible∨left-Bol	12	Table 2 of [152] = example 3 in [204]
22	A-loops⟹Moufang; Moufang⟹A-loops		[151][50]
23	Diassociative⟹ARIF∨L-Bol	27	Theorem 5.2 in [123], see caption
24	Flexible∧L-alternative∧2-sided-inverses∧$(xx = 1)$ ⟹R-alternative∨WIP∨antiaut	6	mace
25	Flexible⟹L4-power-associative	6	mace
26	L-Bol⟹flexible∨Ralt	8	Example 4 of [204]
27	A-loop⟹inverse property		[50]
28	R-alternative⟹L4-power-associative	6	mace
29	Inverse-property⟹L-alternative∨R-alternative	7	mace
30	2-sided inverses⟹Inverse-property	5	Example 3.2 of [204]
31	Conjugacy-closed⟹power-associative	6	Table 1 of [161]
32	$(xx = 1)$∧nuclear-square∧L-alternative∧LC ⟹RC-loop∨antiaut	6	mace
33	L-Bol⟹antiautomorphic∨R-Bol	8	example 4 in [204]
34	$(xx = 1)$∧NS∧antiaut⟹LIP∨WIP∨RC∨C-loop	6	mace
35	Abelian∧Moufang⟹group		ch. 8 of [47]
36	LC⟹C∨L-Bol	6	table 2 of [105]
37	Moufang⟹ M_k for some $k > 2$		counterexamples in [57][58]
38	power-assoc∧alternative∧IP⟹ $(ab \cdot b)b = a(b \cdot bb)$	18	[203]
39	L-Bol∧G-loop⟹Moufang	≤ 50	[218][212]
40	C⟹Conjugacy-closed	10	mace
41	$(xx = 1)$∧nuclear-square∧antiaut⟹C∨LIP∨WIP	6	mace
42	$(xx = 1)$∧RC⟹C∨LIP∨antiaut	6	mace
43	conjugacy-closed⟹antiaut∨LIP∨2-sided inverses	6	mace
44	WIP⟹2-sided inverses	6	mace
45	2-sided inverses⟹WIP	6	mace
46	nuclear-square⟹2-sided inverses	6	mace
47	conjugacy-closed⟹WIP	9	mace
48	WIP⟹2SI	6	mace
49	G⟹{2SI or any other equational property}		[161]
50	W1∧flexibility⟹LBol∨RBol		since ARIF does not imply Moufang=LBol∧RBol
51	NS∧conju.closed⟹2SI∨3PA∨LIP	6	mace
52	NS∧conju.closed⟹WIP	16	example 2.20 in [150]
53	Alternative∧Abelian⟹ $(ab \cdot b)b = a(b \cdot bb)$∨WIP∨antiaut∨AI∨power-assoc.	21	[203]
54	Automorphic-inverse⟹2-sided inverse	5	mace
55	A-loop∧Abelian∧$(xx = 1)$ ⟹alternative		[50] p.322
56	A-loop with all isotopes also A-loops⟹alternative	8	[50] p.321
57	flexible∧Lalt∧antiaut⟹Ralt.	6	mace

Figure 26.4. Non-implications in loops, including size of smallest known counterexample loop if the disproof is by explicit counterexample. (For new counterexamples of size≥ 7, see figure 26.2.2.) ∨=or, ∧=and.

Remarks on non-implications in figure 26.4.
Theorem 5.2 in [123] constructed a non-group diassociative loop of the same cardinality as any of a large class of groups, in particular of order p^3 for each odd prime p. Chein [57] showed that Moufang loops of order p, p^2, p^3, or pq are groups if p and q are prime, so these cannot be Moufang. (See also [58][62].) They also cannot be ARIF because any odd-cardinality ARIF loop is Moufang [152]. The smallest such counterexample has cardinality 27.

Kunen [161] showed any equation valid in all G-loops is valid in all loops.

Figure 26.4 mentions many counterexamples found by `Mace`. We shall feel free not to state counterexample loops with ≤ 6 elements since `Mace` will find them in under a minute. We give larger counterexamples in figure 26.2.2.

a	0	1	2	3	4	5	6	7
0	3	0	1	2	5	7	4	6
1	0	1	2	3	4	5	6	7
2	6	2	5	0	1	4	7	3
3	4	3	7	1	0	6	5	2
4	1	4	3	7	6	2	0	5
5	2	5	0	6	7	1	3	4
6	7	6	4	5	2	3	1	0
7	5	7	6	4	3	0	2	1

b	0	1	2	3	4	5	6	7
0	5	0	3	2	1	4	7	6
1	0	1	2	3	4	5	6	7
2	3	2	1	0	6	7	4	5
3	7	3	0	1	2	6	5	4
4	1	4	6	7	5	0	2	3
5	4	5	7	6	0	1	3	2
6	2	6	4	5	7	3	1	0
7	6	7	5	4	3	2	0	1

c	0	1	2	3	4	5	6
0	4	0	3	5	1	6	2
1	0	1	2	3	4	5	6
2	6	2	5	0	3	1	4
3	2	3	4	6	5	0	1
4	1	4	6	2	0	3	5
5	3	5	1	4	6	2	0
6	5	6	0	1	2	4	3

d	0	1	2	3	4	5	6	7	8	9
0	1	0	4	5	2	3	7	6	9	8
1	0	1	2	3	4	5	6	7	8	9
2	4	2	1	6	0	8	3	9	5	7
3	5	3	6	1	9	0	2	8	7	4
4	2	4	0	9	1	7	8	5	6	3
5	3	5	8	0	7	1	9	4	2	6
6	7	6	3	2	8	9	1	0	4	5
7	6	7	9	8	5	4	0	1	3	2
8	9	8	5	7	6	2	4	3	1	0
9	8	9	7	4	3	6	5	2	0	1

e	0	1	2	3	4	5	6	7	8
0	8	0	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6	7	8
2	4	2	0	7	5	3	1	8	6
3	2	3	4	5	6	7	8	0	1
4	3	4	5	6	7	8	0	1	2
5	7	5	3	1	8	6	4	2	0
6	5	6	7	8	0	1	2	3	4
7	6	7	8	0	1	2	3	4	5
8	1	8	6	4	2	0	7	5	3

f	0	1	2	3	4	5
0	1	0	3	2	5	4
1	0	1	2	3	4	5
2	4	2	1	5	0	3
3	5	3	4	1	2	0
4	3	4	5	0	1	2
5	2	5	0	4	3	1

Figure 26.5. Counterexample loops found by `Mace`.
a: 8-element loop which is LN and RN but not MN (N=nuclear-square).
b: 8-element loop which is RBol but neither LBol, Moufang, nor antiaut.
c: 7-element loop with inverse property which is not right-alternative.
d: 10-element loop which is C but not RCC.
e: 9-element loop which is CC but not WIP.
f: 6-element loop satisfying the hypotheses in EQ 245 as well as $x^2 = 1$. In this loop $x^{-1}y^{-1} = (yx)^{-1}$, $xy \cdot y = x \cdot yy$, $xy \cdot y^{-1} = x$, and $x^{-1} = y(xy)^{-1}$ (and the right-Bol and all Moufang identities) all are, in general, untrue. For example $0 = 0^{-1} \neq 2(0 \cdot 2)^{-1} = 2 \cdot 3^{-1} = 2 \cdot 3 = 5$.

The taxonomy in figure 26.3 attempts to include *all* possible inclusions and intends that every inclusion is *strict*. That goal is largely achieved, but cannot be completely achieved until several open problems are resolved. The precise degree to which we have achieved success is described by the non-implications in figure 26.4. The main ways in which we have failed will be flagged as open questions in the ensuing text.

26.2.1 Power associativity

We almost completely understand which loop types in figure 26.3 are power-associative:

Theorem 100 (Power-associative loops). *PA-CC-loops, A-loops, L-Bol and R-Bol loops, and LC and RC-loops (and all their "ancestors" in figure 26.3) are power-associative; however all the other kinds of loops there in general are not* – except *that it is presently unknown what the status of W1, W2, and IP-alternative loops are.*

Proof: The power-associativity of A-loops was shown by Bruck and Paige [50], of Bol loops by D.A.Robinson [217], and LC and RC-loops by F.Fenyves [105]. Fenyves and Robinson employed the same methodology which was (in the LC case) to prove $x^{m+1}y = x{\cdot}x^m y = x^m{\cdot}xy$ and thence $x^{m+n}y = x^n{\cdot}x^m y$ on the way to proving full power associativity. All the required disproofs of power associativity arise from small counterexample loops, all easily found, mentioned in figure 26.4 which do not even obey either 2SI, 3PA, or L4PA (or its mirror). The sole exception, which was much harder, was Phillips' [203] discovery of a 21-element commutative alternative loop which disobeys antiaut, AI, WIP, and power-associativity.

However, this proof method fails to tell us whether W1 (perhaps with flexibility also) implies power-associativity.[59] I do not even know whether LRalt loops necessarily have 2-sided inverses[60] or are flexible, nor whether IP-alternativity implies $(a \cdot aaa)aa = a(aaa \cdot aa)$. (J.D.Phillips [203] found a 18-element loop showing that IP-alternativity does not imply $(ab \cdot b)b = a(b \cdot bb)$.) Q.E.D.

identity	name	mirror	with 3PA implies
$x(x \cdot xx) = xx \cdot xx$	L4PA	R	P
$(xx \cdot x)x = xx \cdot xx$	R4PA	L	Q
$x(xx \cdot x) = xx \cdot xx$	Q4PA	P	R
$(x \cdot xx)x = xx \cdot xx$	P4PA	Q	L
$x(x \cdot xx) = (xx \cdot x)x$	S4PA	self	T,U,V
$x(xx \cdot x) = (x \cdot xx)x$	T4PA	self	S,U,V
$x(xx \cdot x) = (xx \cdot x)x$	U4PA	V	S,T,V
$(x \cdot xx)x = x(x \cdot xx)$	V4PA	U	S,T,U
$xx \cdot x = x \cdot xx$	3PA	self	none

Figure 26.6. The 8 inequivalent kinds of 4-term power associativity, and the 3-power-associativity identity 3PA. In loops, none of these imply any other. But in combination with 3PA, some of these *do* imply others (listed). The W1 identity $zx \cdot (y \cdot xy) = z(x \cdot yx) \cdot y$ implies all of them, as does LR-alternativity, but the inverse property does not imply any of these. (All of these implications and non-implications are proven in seconds by `Otter` and `Mace`.)

Similarly figure 26.3 includes a complete understanding of which loop types are necessarily groups[61], or are diassociative, conjugacy-closed, 3PA, and L4PA. The only loop type in figure 26.3 whose status vis-a-vis 2-sided inverses is unknown, is LRalt.

26.2.2 Antiautomorphism, WIP, LIP

Theorem 101 (WIP loops). *The only loops in figure 26.3 which are WIP, LIP, or antiautomorphic are the direct and indirect ancestors of the nodes whose labels include LWIP or RWIP; LIP; or antiaut, respectively,* except *that it is presently unknown what the status of alternative and LRalt loops are.*

Proof: Again the disproofs are in table 26.4 and the proofs are well known; all disproofs arise from small counterexample loops except for Phillips' 21-element loop and the one in figure e. Q.E.D.

26.2.3 Lagrange property and simple Bol loops

A finite loop has the *weak Lagrange property* if the cardinality of each subloop divides the cardinality of the whole loop. It has the *strong Lagrange property* if every subloop obeys the weak Lagrange property.

Let $P \subset L$ be a subloop of L. If $x \in L$ then $xP \stackrel{\text{def}}{=} \{xy : y \in P\}$ is a *left coset* of P and right cosets Px are defined similarly. Unlike in group theory, cosets can have nonempty intersection. P is a *normal* subloop of L if

$$xP = Px, \quad (xP)y = x(Py), \quad x(yP) = (xy)P. \qquad (246)$$

(Normal subloops *do* have disjoint cosets, cf. p.92 of [47].) A loop is *simple* if it has no nontrivial normal subloops.

"The two biggest problems in loop theory" have been claimed [59] to be

1. The Lagrange property for finite Moufang loops.
2. The existence of finite simple non-Moufang Bol loops.

Status. The Moufang-Lagrange problem has just recently been solved by A.Grishkov and A.Zavrnitsine [119]: Moufang loops obey the strong Lagrange property[62]. Furthermore there are rumors that the second problem is also nearing solution. Specifically, E.K.Loginov, of Ivanovo State Energy University (Russia) claims [167] to have a proof that all finite simple left-Bol loops (with a finite number of possible exceptions, arising when the left-multiplication group of the Bol loop is sporadic simple) are Moufang. If so, and assuming none of the possible exceptions actually happen, it would follow from theorem 104 that Bol loops must obey the strong Lagrange property.

It was previously known that groups, conjugacy-closed-loops ([150] corollary of theorem 3.1), A-loops with the inverse property [59], Moufang loops of odd cardinality [112] or cardinality< 16320 [59], left-Bol loops of odd cardinality [108], and M_k-loops with $k = 2^r+1$ or k even [56] all obey the strong Lagrange property. If loop L has a normal subloop N such that both N and L/N have the weak Lagrange property, then so does L (this is lemma V.2.1 of [47]; it also holds if "weak" is changed to "strong"). Moufang loops (and not merely groups) are known to obey the Jordan-Hölder theorem of having a "composition series" of normal subloops unique up to isomorphism [47].

On the other hand, a 5-element loop exists with 2-element subgroups, and the 10-element Steiner loop in table 1 of Fenyves [105] has subloops of cardinality 4.

Here is a powerful general way to construct loops disobeying the Lagrange property: Start with a "block design," i.e. a system of "points" and "blocks" (point subsets) such that *every pair of points is in exactly one block*. We can turn this into a loop by demanding that the points forming each block be the non-1 elements of a subloop. Because each pair of points is in exacly one block, this (and the requirement that $1x = x1 = x$) completely defines the loop's multiplication table. The cardinality of this loop is 1 plus the number of points, and the subloop sizes are 1 plus the block sizes. In particular, if q is any prime power, it is known that a "projective plane of order q" exists, which is a system of $q^2 + q + 1$ points in which all

[59] `Otter` proved that the form $zx \cdot (y \cdot xy) = z(x \cdot yx) \cdot y$ of W1 implies R-alternativity, 2-sided inverses, 3PA, all the 4-variable 4-power-associativity identities in figure 26.6, and several other kinds of partial power associativity. LR-alternativity implies all these things, *except* perhaps 2-sided inverses, too.

[60] Exhaustive computer searches by J.D.Phillips [203] indicate that any LR-alternative loop without 2-sided inverses must have at least 33 elements.

[61] The ones which say "group"!

[62] Despite obeying the Lagrange theorem neither CC nor Moufang loops are not *too* group-like; e.g. Paige's 120-element simple Moufang loop has no elements x with $x^5 = 1$, and Table 1 of [161] gives a 6-element CC loop with no subgroups of size 2, showing that both CC and Moufang loops can disobey the Sylow theorem.

the blocks (called "lines") have cardinality $q+1$, every pair of points is in exactly one line, and every pair of lines intersects at exactly one point. This will yield a loop disobeying the weak Lagrange property for any prime power q such that $q+2$ does not divide q^2+q+2, i.e. *every* prime power $q \geq 3$. The first example is $q=3$ since 5 does not divide 14. In this way we may create a non-Lagrange loop with any equational property we desire, provided that property is satisfiable by loops of cardinality $q+2$ with q a prime power, and provided that property's defining identities involve at most *two* variables. (E.g. commutative, diassociative.) Also we have

Theorem 102 (Some non-Lagrange loops). *Abelian and non-Abelian loops with transitive automorphism groups exist which disobey the Lagrange property.*

Proof: From the unique projective plane of order 3 (13 points and 13 lines, each line consisting of 4 points), which has a symmetry group of order 5616 which includes the cyclic group of order 13 (and therefore is transitive, i.e. includes symmetries mapping any point to any other) we get by the construction above a 14-element tag-loop with subloops of size 5. Namely: The lines $\{s, s+1, s+4, s+6\}_{s=0,\dots,12}$ mod 13 are chosen to be the non-identity elements of identical subloops. Now, if we so desire, we may further choose the subloops to be identical Abelian size-5 groups. In that case our size-14 counterexample loop is an Abelian loop. Q.E.D.

Combining all these results and counterexamples almost completely settles the question of which loops in figure 26.3 obey the Lagrange property and which don't; specifically it justifies the "L" column in figure 26.1. Only these open cases remain:

1. Bol (and Bruck) loops (which Loginov's proof, if correct, would nearly settle);
2. A-loops (Note: theorem 2.2 of [50] goes in the right direction toward proving A-loops obey the Lagrange property...);
3. LCC loops. (I have done an exhaustive computer search among LCC loops of cardinality $n \leq 12$; none have subloops of cardinality 2 or 3 unless these divide n.)

All simple Moufang loops have been classified [192][165][88][183]; the only ones other than the simple groups [65] are the "Paige loops," which are the unit-norm octonions over finite fields with octonions of opposite overall sign identified.

Chein et al. [59] proved that if finite Moufang loops have the weak Lagrange property, then they have the strong one, and then further reduced the Moufang-loop Lagrange problem to proving the weak Lagrange property for Paige loops. Now Paige loops have a tremendous amount of structure, and not just loop structure but in fact algebraic structure. That is why Grishkov and Zavarnitsine [119] were able to settle the Moufang-Lagrange problem, and also why I was able to show the following weaker, but simpler, and more intuitive, result.

Theorem 103 (Lagrange property for (≤ 2)-generated subloops of Paige loops). *Any subloop of a Paige loop that is generated by 2 or fewer elements, has cardinality dividing the cardinality of the full loop.*

Proof: It is known that the subgroups generated by a single element inside a diassociative loop must have cardinality dividing the cardinality of the full loop ([47] theorem V.1.2); therefore Paige loops *do* obey the weak lagrange property insofar as their subloops (which automatically are sub*groups*) generated by *one* element are concerned.

We now claim this is also true of the subloops (which also automatically are sub*groups*) generated by *two* elements. That is because two octonions generate (both additively and multiplicatively) a quaternion subalgebra of the octonion algebra. Therefore if we restrict ourselves to multiplicative generation, we must get a multiplicative subgroup of a quaternion subgroup of the unit-norm octonions. (Optionally with overall $\pm$ sign modded out in both cases, and this "sub"group of the quaternions is permitted to be all of them.)

Now the full group of unit-norm quaternions necessarily has cardinality dividing the cardinality of the unit-norm octonions, because the right-cosets $(q,0)(a,b)$ of the quaternions $(q,0)$ are the octonions $(qa, \overline{q}b)$, and all these cosets all are *disjoint* or *identical* by considering the fact that a canonical representative $(1, \overline{a^{-1}}b)$ of the coset is got by choosing $q=a^{-1}$ (or if $a=0$ then choose $q=b^{-1}$). [More precisely one may postulate $(qa, \overline{q}b) = (rc, \overline{r}d)$ and left-multiply both sides by an appropriate quaternion to cause $(1,B)=(1,D)$ and then conclude either the 2 cosets are identical or reach a contradiction.] Further, plainly these cosets tile the full set of octonions.

In the reasoning above we have focused on the quaternion subalgebra in the first 4 coordinates of the octonions, but the same reasoning is valid for any other quaternion subalgebra, just the coordinate-based notation is no longer applicable. Namely, instead of regarding an octonion as an ordered pair of quaternions (a,b), regard it as $a+ib$ where i is *any* pure-imaginary unit-norm octonion orthogonal to the quaternion subalgebra a and b live in. Such an i always exists, even in the octonions over a finite field, because we may use the "7D vector product" (or 8D product of three 8-vectors; see §25.2) to construct it.

Now by the Lagrange theorem in *groups*, any subgroup of the full quaternion subgroup then must divide the full cardinality of the unit-norm octonions.

(An alternative line of reasoning would be to actually compute the cardinalities of quaternion algebras over a finite field.) Q.E.D.

With theorem 103 known, it now suffices, to prove the Lagrange property for Moufang loops, merely to prove it insofar as Paige loop subloops requiring ≥ 3 generators are concerned. I believe that the complicated Grishkov-Zavarnitsine proof (although they did not look at it that way) really just did exactly that. It depended upon relationships between subloops of Paige loops and subgroups of certain certain "groups with triality." Probably if their proof (and the previous results about simple groups it depended on) were all combined and then streamlined, then everything would be a consequence of properties of the octonion algebra.

Re the simple Bol loops question: since simple Moufang loops are classified, the open question is whether there are any simple Bol loops *besides* them. A relation between the two problems:

Theorem 104 (Chein et al. [59]). *If all Moufang loops obey the Lagrange property but some Bol loop violates the weak Lagrange property, then there exists a finite simple non-Moufang Bol loop. Conversely: If no finite simple non-Moufang Bol loops exist, it then follows that Bol loops obey the strong Lagrange property. (This theorem is also true with the word "Bruck" substituted for every occurrence of the word "Bol.")*

26.3 Some kinds of quasigroups

Phillips and Vojtechovsky [205] classified all the kinds of quasigroups defined by one identity of "Bol-Moufang type," i.e. which asserts the equality of two 4-term products of the same 3 variables in the same order, but parenthesized differently. Our figure 26.6 does the same if there is only 1 variable, but the 2-variable cases remain unclassified. (They [204] also did the same classification for loops; all of their types were mentioned in figure 26.1.) Figure 26.7 lists the Phillips-Vojtechovsky quasigroup identities not already present in figure 26.1.

#	2^n-ons	type of quasigroup	defining identity
1	$8_\mathbb{R}$, i	LC2	$x(x \cdot yz) = (x \cdot xy)z$
2	$8_\mathbb{R}$, i	LC3	$x(x \cdot yz) = (xx \cdot y)z$
3	$8_\mathbb{R}$, i	LC4	$x(y \cdot yz) = (x \cdot yy)z$
4	$8_\mathbb{R}$	RC2	$x(yz \cdot z) = (xy \cdot z)z$
5	$8_\mathbb{R}$, $i\mathbb{R}$	RC3	$x(y \cdot zz) = (xy \cdot z)z$
6	$8_\mathbb{R}$	RC4	$x(yy \cdot z) = (xy \cdot y)z$
7	$8_\mathbb{R}$	LG1	$x(y \cdot zz) = (x \cdot yz)z$
8	$8_\mathbb{R}$	LG2	$xy \cdot zz = (x \cdot yz)z$
9	$8_\mathbb{R}$	LG3	$x(y \cdot zy) = (x \cdot yz)y$
10	$8_\mathbb{R}$	RG1	$x(xy \cdot z) = (xx \cdot y)z$
11	•	RG2	$x(x \cdot yz) = xx \cdot yz$
12	$8_\mathbb{R}$	RG3	$x(yx \cdot z) = (xy \cdot x)z$

Figure 26.7. Kinds of quasigroups named by Phillips and Vojtechovsky [205] and the behavior of their defining identities in the 2^n-ons (same conventions as in figure 26.1).

26.4 Results about nnac-rings

The same figure 26.1 may instead be viewed as defining (but now in combination with the nnac-ring axioms rather than the loop axioms) various kinds of nnac-rings. (For properties of x^{-1}, we agree to assume $x \neq 0$.) One might then hope for a considerable analogy between the properties of the thus-defined loops and the corresponding nnac-rings, especially if we agree to consider only *unital* nnac-rings (which makes their multiplication more loop-like).

But this hope is only partially satisfied. Facts about loops need not hold in nnac-rings or vice versa, because the multiplicative nnac-ring axioms are neither a subset nor a superset of the loop axioms, even if we further assume the ring is unital. However, the nonzero elements of any unital nnac-ring with left- and right-*cancellation*, i.e. the loop "inverse-property," necessarily form a multiplicative loop and hence all results about IP-loops will also hold for such nnac-rings. Examples:

1. A brilliantly simple argument of Evans and Neumann (p.349 of [102]) showed that in a loop there is no finite set of equations equivalent to power-associativity. In contrast, Albert [11] showed that a nnac-ring with characteristic$\notin \{2,3,5\}$ is power-associative iff $x \cdot xx = xx \cdot x$ and $xx \cdot xx = x \cdot (x \cdot xx)$, i.e. iff 3PA and L4PA hold. In loops, right-alternativity does not imply power-associativity, indeed does not even imply L4PA. However, in rings with characteristic$\neq 2$, right-alternativity *does* imply both power-associativity and the right Moufang identity $(xy \cdot z)y = x(yz \cdot y)$, see chapter 16 of [259].
2. Right-Bol loops are power-associative [217]. However, nnac-rings which are simultaneously left-Bol, right-Bol, and obey a middle Moufang identity need not even be 3-power-associative – figure 26.8 gives a 4-element counterexample. But *unital* right-Bol nnac-rings are power-associative.

```
+ | 0 1 2 3    * | 0 1 2 3
--+--------    --+--------
0 | 0 1 2 3    0 | 0 0 0 0
1 | 1 0 3 2    1 | 0 2 2 0
2 | 2 3 0 1    2 | 0 0 0 0
3 | 3 2 1 0    3 | 0 2 2 0
```

Figure 26.8. Non-unital 4-element nnac ring with characteristic 4 which obeys the left-Bol, right-Bol, right-alternative, and middle-Moufang identities but is neither left-alternative ($0 = 0 \cdot 2 = 11 \cdot 2 \neq 1 \cdot 12 = 1 \cdot 2 = 2$), nor 3-power-associative ($0 = 11 \cdot 1 \neq 1 \cdot 11 = 2$).

3. It is an open question whether there is a finite equational basis for loop diassociativity, and while Moufang$\Longrightarrow$diassociativity, the reverse implication is false due to a 10-element counterexample ([105] table 1). In contrast, in nnac-rings, any two among {L-alternative, R-alternative, Flexible} suffice to imply the third and then all Moufang identities and diassociativity; then the latter implies alternativity back again ([227] p.30, [259] p.35).
4. Diassociative loops automatically have the inverse property. However, diassociative nnac-rings, even if unital and even if some finite set of characteristics are forbidden, do not necessarily even *have* multiplicative inverses for all nonzero elements. For example, construct the octonions over the ring of integers modulo n, where n is a *composite* number. These octonions will in general feature zero-divisors.
5. Just as in a loop, the presence of antiautomorphism in a nnac-ring causes the Left and Right versions of any property to imply the other, e.g. L-alternative$\Longleftrightarrow$R-alternative.
6. Although the loops with "nuclear square" properties form their own phylum in figure 26.3, the situation is precisely the opposite for nnac-rings with nuclear-square properties; see theorem 105.

Theorem 105 (Nuclear square nnac-rings are associative). *A unital nnac-ring containing $\frac{1}{2}$ obeying any of the 3 nuclear-square identities (LN, MN, or RN in figure 26.1) is automatically associative.*

Proof: If x^2 and y^2 associate with any other two elements (on either the left, right, or middle), then by distributivity so do $x^2 \pm y^2$. Now note that if $y = x - 1$ then y and x commute so that $x^2 - y^2 = (x-y)(x+y) = x + y = 2x - 1$. Since $2x - 1$ associates with everything else, if the the ring contains $\frac{1}{2}$ this means *everything* associates. Q.E.D.

26.5 Abstract 2^n-ons

We define a new abstract algebraic entity, *abstract 2^n-ons*, by the following axioms designed to encapsulate the key algebraic properties of 2^n-ons independently of any particular construction. There are the following abstract operations: $x+y$, $xy = x \cdot y$, and $\overline{x}$, and there is an abstract notion of being "real." In terms of these we shall also define x^{-1}, $x-y$, $-x$, $|x|^2$, and $2\,\mathrm{re}\,x$, and the special symbols 0, 1, and 2.

1. **Additive axioms:** $(x+y)+z = x+(y+z)$, $x+y = y+x$.
2. **Multiplicative axioms:** $x(-y) = (-x)y = -(xy)$, $(-x)(-y) = xy$, $x(y+z) = xy + xz$, $xx \cdot y = x \cdot xy$.
3. **Axioms about 0:** $x+0 = x$, $x+(-x) = 0$, $-(-x) = x$, $0x = x0 = 0$.
4. **Axioms about 1:** $1x = x1 = x$, $2 \overset{\text{def}}{=} 1+1$.
5. **Axioms about reciprocals:** x^{-1} exists if $x \neq 0$, in which case $x^{-1}x = xx^{-1} = 1$.
6. **Axioms about conjugation:** $\overline{\overline{x}} = x$, $\overline{x \pm y} = \overline{x} \pm \overline{y}$; $|x|^2 \overset{\text{def}}{=} \overline{x}x = x\overline{x}$, $|xy|^2 = |x|^2|y|^2$, $2\,\mathrm{re}\,x \overset{\text{def}}{=} x + \overline{x}$.
7. **Axioms about "reals":** 0, 1, $|x|^2$, and $2\,\mathrm{re}\,x$ all are real. If r and s are real then so are rs, $r \pm s$, $\overline{r}$, and r^{-1}. If r is real then $rx = xr$, $r \cdot xy = rx \cdot y$, $x \cdot ry = xr \cdot y$, $x \cdot yr = xy \cdot r$, $(x+r)y = xy + ry$, and $\mathrm{re}\,r = r$, $|r|^2 = rr$.

One could also add some axioms about characteristic, such as $2 \neq 0$ (characteristic$\neq 2$). (Certainly some of the above axioms are redundant; I have made no effort to obtain a minimal set of axioms.)

There are several reasons one might be interested in studying abstract 2^n-ons.

1. It is interesting to determine which axiom subsets imply which properties.
2. Instead of starting the 2^n-on doubling construction from a *field* such as $\mathbb{R}$ or GF_3, it is possible to start it off from any kind of abstract 2^n-ons. The doubled 2^n-ons will then obey the same properties. The resulting extra freedom might enable new combinatorial constructions, etc.

Example. Abstract 2^n-ons obey the quadratic identity $x^2 - 2\mathrm{re}(x)x + |x|^2 = 0$ and are power-associative. That is because the proofs of these things we have already given already are (or may easily be rephrased to be) suitably abstract.

Theorem 106 (Finite abstract 2^n-ons). *The only finite abstract 2^n-ons with cardinality≤ 11 are finite fields, even if we we omit all the abstract 2^n-on axioms after axiom set 5 about reciprocals.*

Proof: Exhaustive computer search. Q.E.D.

Example. One may ask such questions as: "is it possible for *flexible* abstract 2^n-ons (i.e. obeying $xy \cdot x = x \cdot yx$) to exist which are not *right-alternative* (i.e. do not obey $xy \cdot y = x \cdot yy$)?" I do not know, but an exhaustive computer enumeration of for small finite sets 2^n-ons shows that this is impossible if there are ≤ 11 elements. On the other hand, this *is* possible with a set of size 8 if we omit all the axioms after *and including* axiom set 5 about reciprocals.

Example. Suppose you wanted to use abstract 2^n-ons to find interesting point sets in 24-dimensions, such as (perhaps) the Leech lattice [67]. Simply write down an interesting finite (or countably infinite) set of 3-vectors and define a "multiplication," "addition," and "conjugation" law for them. If the laws you define satisfy the abstract 2^n-on axioms, then upon doubling 3 times using EQ 68, you will get a finite (or infinite) set of 24-vectors which are abstract 2^n-ons.

27 Comparison with other or previous attempts to create 16-ons

In this section we shall discuss other attempts to build 16-ons from octonions. Some of these attempts are important mathematically, while others are important historically.

During the course of this research, we found over 100 different ways to create 16-ons with multiplicative norm from pairs of octonions. However, since almost all of them have completely unattractive algebraic properties, we'll make no attempt to describe them.

There are 8 particularly mathematically natural ways to try to get 16-ons by modifying the Cayley-Dickson doubling formula EQ 48 for $(a,b)(c,d)$ in such a way as to cause the Euclidean norm to be multiplicative. We call these the 8 *pre-eminent* formulae. They are given in figure 27.1, together with some of their properties.

$8 \to 16$ doubling formula	alternativity?	linearity?	antiaut?	Jordan?	orthogL?
$(ac - d\overline{b},\ cb + \overline{a}b^{-1} \cdot bd)$	left, right(0), flex(0)	right, weak, left(0-8)	0-8	1-8	yes
$(ac - d\overline{b},\ cd^{-1} \cdot db + \overline{a}d)$	right, left(0), flex(0)	left, weak, right(0-8)	0-8	1-8	yes
$(ac - d\overline{b},\ cb + \overline{a}c \cdot c^{-1}d)$	right(0)	left, right(0-8)	0-8	1-8	no
$(ac - d\overline{b},\ ca^{-1} \cdot ab + \overline{a}d)$	left(0)	right, left(0-8)	0-8	1-8	no
$(ac - da \cdot a^{-1}\overline{b},\ cb + \overline{a}d)$	left(0)	right, left(0, 8-15)	0, 8-15	8-15	no
$(ac - dc^{-1} \cdot c\overline{b},\ cb + \overline{a}d)$	right(0)	left, right(0, 8-15)	0, 8-15	8-15	no
$(ab \cdot b^{-1}c - d\overline{b},\ cb + \overline{a}d)$	left, right(0), flex(0)	right, left(0,8-15), weak	0, 8-15	8-15	yes
$(ad \cdot d^{-1}c - d\overline{b},\ cb + \overline{a}d)$	right, left(0), flex(0)	left, right(0,8-15), weak	0, 8-15	8-15	yes

Figure 27.1. The 8 pre-eminent 16-on multiplication formulas, for multiplying $(a,b)(c,d)$ where (a,b) and (c,d) are 16-ons, regarded as octonion 2-tuples. The one in the top line of the table is the one we have preferred in this monograph.

Coordinates numbered 0-15: 0-7 are the octonion subalgebra; 0 is the real coordinate.

(0-8) means "in coords 0,1,2,...8 only," and *(0,8-15)* means "in coordinates 0, 8, 9, 10,..., 15 only."
Left-alternative law is $xx \cdot y = x \cdot xy$. *Right-alternative* law is $y \cdot xx = yx \cdot x$. *Flexible* law is $xy \cdot x = x \cdot yx$.

Left-linear law is $(x+y)z = xz + yz$. *Right-linear law* is $z(x+y) = zx + zy$.
Weak left-linear law is $(x \pm 1)z = xz \pm z$. *Weak right-linear* law is $z(x \pm 1) = zx \pm z$.
Weak-linear means both weak-left and weak-right linear.
Antiaut law is $\overline{a}\overline{b} = \overline{ba}$. *Jordan (1-8)* means that coordinates 1-8 of $(x \circ y) \circ x^2 - x \circ (y \circ x^2)$ are 0, where $x \circ y \stackrel{\text{def}}{=} xy - yx$.
OrthogL means that $\langle x, xy - yx \rangle = 0$.

All 8 of the pre-eminent formulas will, starting with the reals, generate the complex numbers, quaternions, and octonions. At the next doubling they yield 16-ons with multiplicative norm – and since these formulas resemble one another, one is led to the question of whether they are, algebraically, actually the same. They're not:

Theorem 107 (Differentness). *The table (figure 27.1) has grouped the 8 pre-eminent formulas into 4 pairs. Each member of the pair is the "opposite algebra" to the other member of that pair, i.e. the two 16-on algebras they yield are anti-isomorphic, i.e. left-multiplication in one corresponds to right-multiplication in the other. But no member of any pair yields 16-ons which are algebraically the "same" (in any common sense) as any member of any other pair.*

Proof: The oppositeness claims are confirmable tediously but straightforwardly (e.g. by computer as in §11, or by converting one formula into the other with the aid of octonion "eye-shift" identities EQ 98).

Now note that coordinates 0-7 are algebraically *special* since they correspond to the octonion subalgebra (and discontinuity locus). Multiplying two 16-ons whose nonzero coordinates lie in 0-7 and 0-7 (or in 8-15 and 8-15) yields another 16-on whose nonzero coordinates are in 0-7; Multiplying two 16-ons whose nonzero coordinates are in 0-7 and 8-15 yields one whose nonzero coordinates are in 8-15.

With this in mind, it now is clear by inspecting the properties listed in the table that any two 16-on formulae from different pairs, are genuinely different. Q.E.D.

At the next doubling, none of these formulas, as written, yield 32-ons with multiplicative norm, although as we've seen in §9 it is possible to rewrite some of them in a way which is, at the 16-ons, equivalent, which *does* keep going forever yielding 2^k-ons with multiplicative norm.

Now these 4, genuinely different, pre-eminent algebra & opposite pairs correspond (in the case of 16-ons) to the 4 obvious variants of the block-matrix formula EQ 57.

Our 8 pre-eminent formulas actually are merely special cases of these 4 parameterized *families* of formulas:

$$(a,b)(c,d) = (ac - d\overline{b},\ cb + \overline{a}[sb^{-1} + tc] \cdot [sb^{-1} + tc]^{-1} d) \quad (247)$$

$$(a,b)(c,d) = (ac - d\overline{b},\ c[sd + ta]^{-1} \cdot [sd + ta]^{-1} b + \overline{a}d) \quad (248)$$

$$(a,b)(c,d) = (ac - d[sa + tc^{-1}] \cdot [sa + tc^{-1}]^{-1} \overline{b},\ cb + \overline{a}d) \quad (249)$$

$$(a,b)(c,d) = (a[sb + td] \cdot [sb + td]^{-1} c - d\overline{b},\ cb + \overline{a}d) \quad (250)$$

all of which yield 16-ons with multiplicative Euclidean norm for *any* real parameters s, t (not both 0). Note, s and t are allowed to depend upon a, b, c, d; it is not necessary that they be constants. But generic members of these families are less attractive than the 8 (nongeneric) pre-eminent formulas because, e.g., none of them are even 1-sided linear.

A particularly amusing formula (also leading to 16-ons, but not 32-ons, with multiplicative Euclidean norm) is

$$(a,b)(c,d) = (a[d\overline{b}d] \cdot [d\overline{b}d]^{-1} c - d \cdot \overline{b},\ c \cdot b + \overline{a} \cdot d) \quad (251)$$

which really is merely an instance of EQ 250 due to the octonion triple product identity EQ 209 and octonion flexibility EQ 9.

J.D.H. Smith [235] suggested the following formula for 16-on multiplication:

$$(a,b)(c,d) = (ab \cdot cb^{-1} - b \cdot \overline{d},\ b\overline{c} + db^{-1} \cdot ab). \quad (252)$$

But the resulting 16-ons have little virtue. They are right-linear. But they are neither left nor weak linear, nor quadratic, nor power-associative, nor left nor right alternative. They do not yield a 15D vector product. They do not obey the Jordan identity, nor any variant of the Bol or Moufang identities I know of, in even a single coordinate. This doubling formula, if applied to the quaternions, does not yield the octonions. According to J.D.H.Smith [235], the great advantage of these 16-ons is that division problems generically have unique solutions. However (1) we've seen that our 16-ons also have the quotient-existence property (and our proof techniques are also applicable to numerous other possible 16-on-formulae) and (2) division problems in J.D.H.Smith's 16-ons do not *always* have a unique solution, as one may demonstrate by constructing a counterexample $(a,b)(c,d) = (a',b')(c,d) = (X,Y)$:

$$\begin{aligned}
(a,b) &= (0,0,0,0,0,0,1,0, \quad 0,0,0,0,0,0,1,0) \neq \\
(a',b') &= (0,0,0,0,0,0,0,0, \quad 0,0,0,0,0,1,1,0), \\
(c,d) &= (0,1,0,0,0,0,0,0, \quad 0,0,1,0,0,0,0,0), \\
(X,Y) &= (0,0,0,0,1,0,0,-1, \quad 0,0,0,0,1,0,0,1).
\end{aligned} \quad (253)$$

Pfister [199][211] constructed rational sum-of-squares formulae (EQ 41) for each power of 2. Although Pfister did not look at it this way, his construction may be regarded as yielding nnacd-algebras, with multiplicative Euclidean norm, of each dimension 2^k, $k \geq 0$. Indeed the resulting constructions can be written in such a way that they resemble our EQ 57. However, not surprisingly (because Pfister apparently was completely unconcerned with the algebraic properties of these constructions) the algebras that result are ugly – indeed, Pfister's construction does not even yield the complex numbers starting from the real numbers.

Zassenhaus and Eichhorn [257], building on Olga Taussky [243], found a rational 16-square identity (EQ 41). This also may be regarded as corresponding to a non-distributive 16-on algebra with multiplicative Euclidean norm.

Their approach is based on defining the "determinant" of a 2×2 matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, whose entries are octonions, to be

$$\det_{\text{ZE}} M = ad - ac \cdot a^{-1} b. \quad (254)$$

This definition has the advantage that

$$(\det_{\rm ZE} M)\overline{\det_{\rm ZE} M} \;=\; \det_{\rm ZE}(MM^H) \qquad (255)$$

(Zassenhaus and Eichhorn note as an aside, following Taussky, that $\overline{\det_{\rm ZE} M} \neq \det_{\rm ZE}(M^H)$ in general. Also, EQ 255 does *not* hold for *16-on* a, b, c, d.) Upon rearranging terms, EQ 254 becomes the 16-square identity

$$(|a|^2+|b|^2)(|c|^2+|d|^2) = |a\overline{c}+b\overline{d}|^2+|ad-(ac)(a^{-1}b)|^2. \quad (256)$$

The corresponding nnacd 16-on algebra then arises from the doubling formula

$$(a,b)(c,d) \;=\; (a\overline{c}+b\overline{d},\; ad-ac\cdot a^{-1}b) \qquad (257)$$

applied to the octonions. (This formula does not yield the octonions starting from the quaternions.) The properties of these 16-ons are unappealing compared to our EQ 72: They are neither left nor right alternative, nor flexible (none of these even in any one coordinate with the others ignored). They are not even power-associative, e.g. $aa^2 \neq a^2a$ in general. They obey neither weak-linearity nor the quadratic identity. They still are right-linear, are left-linear if only the first 8 coordinates of the answer are considered (as opposed to our 9), and obey real-part antiautomorphism $\mathrm{re}(\overline{ab}) = \mathrm{re}(\overline{b}\overline{a})$. But there is at least one way in which they are *superior* to our 16-ons: they obey the Jordan identity

$$(x \circ y) \circ x^2 - x \circ (y \circ x^2) \qquad (258)$$

in coordinates 1-15 (i.e. all imaginary coordinates), as opposed to our coordinates 0-8 only.

The most attractive octonion-to-16on doubling formula that we know of (besides ours) is the following interesting (new) formula

$$(a,b)(c,d) \;=\; (ad^{-1}\cdot dc - \overline{b}d,\; dc\cdot d^{-1}b + \overline{d}a). \qquad (259)$$

It is somewhat less attractive than ours (EQ 111). E.g. it does *not* yield the octonions if applied to quaternions. EQ 259, applied to the octonions, yields quadratic, right-alternative, left-linear (left-alternative and flexible and right-linear in the real coordinate only; meanwhile our 16-ons obey left-linearity in coordinates 0-8), weak-linear, power-associative, power-distributive 16-ons. They obey antiautomorphism $\overline{ab} = \overline{b}\overline{a}$ and the Jordan identity

$$(x \circ y) \circ x^2 - x \circ (y \circ x^2) \qquad (260)$$

both in the real coordinate only (as opposed to our 16-ons – coordinates 0-8).

But when it comes to Bol and Moufang identities (and variants thereof) EQ 259 seems superior to our EQ 72:

The 16-ons of EQ 259 obey the variant right-Bol identity $z(xy \cdot \overline{x}) = (zx \cdot y)\overline{x}$. In contrast, our 16-ons (EQ 72) don't obey any Bol identities (nor any variants arising from conjugating one of the repeated variables) except that they obey the left-Bol identity in the real coordinate only, i.e. $\mathrm{re}([x \cdot yx]z) = \mathrm{re}(x[y \cdot xz])$ (while the 16-ons of EQ 259 do not).

Both kinds (EQ 259 and EQ 72) of 16-ons obey the middle Moufang identity (cf. EQ 11) in the real coordinate only. Both kinds obey the fundamental vector product identities EQ 39 and EQ 40 (for the vector product EQ 221) but the 16-ons of EQ 259 are superior in the sense that their vector product obeys

$$(b \times a) \times a = \langle a, b\rangle a - |a|^2 b \qquad (261)$$

whereas ours doesn't.

The 16-ons of EQ 259 obey this variant-Moufang identity

$$xy \cdot z = xz \cdot [z^{-1}y \cdot z] \qquad (262)$$

but our 16-ons (EQ 72) don't, although ours do obey

$$\mathrm{re}(xy \cdot z) = \mathrm{re}([z \cdot yz^{-1}] \cdot zx) \qquad (263)$$

while the 16-ons of EQ 259 don't.

28 Automorphism groups of 2^n-ons

The *automorphism group* of an algebra A is the set of transformations $x \to T(x)$ such that

multiplicative automorphism: $xy = z$ $(x, y, z \in A)$ implies $T(x)T(y) = (Tz)$.

additive automorphism: $x + y = z$ $(x, y, z \in A)$ implies $T(x) + T(y) = T(z)$.

Linearity. Any automorphism T obeying the additive aut property must be *linear*. (Hence, it must also be *continuous*.)

Unsuccessful search for nonlinear 16-on automorphisms. It remains conceivable that there could be some nonlinear automorphism of the multiplicative structure *alone* of an nnacd-algebra (ignoring addition). A theorem proved[63]in the early 20th century by H.Brandt claims that

$$x \to \overline{c}xc \qquad (264)$$

is an automorphism of the octonions x iff $c^6 = 1$. But computer experiments indicate that, in the *16-ons* (where this map is, in general, nonlinear), these are *not* automorphisms for the multiplicative structure, if c is any 16-on obeying $c^3 = 1$ with exactly 2 nonzero coordinates.

Manogue and Schray ([169] eq. 33) further noted that if $c^3 = 1$ then $2c = 1 + b\sqrt{3}$ for some pure-imaginary octonion b with $|b|^2 = 1$, and then all identities arising from the automorphism EQ 264 are resolvable into *two* identities, one of which is the coefficient of $\sqrt{3}$, while the other is the rest. (None of them seem to generalize to 16-ons.)

Theorem 108 (Norms, conjugates, inverses). *Any automorphism T of the 2^n-ons, $n \geq 1$, maps $1 \to 1$, $0 \to 0$, the reals to themselves ($T(x) = x$ if $x \in \mathbb{R}$), $\overline{x} \to \overline{T(x)}$, $x^{-1} \to T(x)^{-1}$, and $|T(x)|^2 = |x|^2$.*

[63] This is theorem 2.2.1 of [149]. It was rediscovered by Max Zorn [264], J.H.Conway and D.Smith (theorem in §8.7 of [68]), and Manogue and Schray ([169] eq. 29 & 31).

Proof: The unique multiplicative identity 1 and the unique additive identity 0 must be mapped to themselves. Then the integers and rationals must also be self-mapped, and by continuity, the reals also. (Also, the fact, from theorem 5, that the reals are the algebraically special "center" of the 2^n-ons, forces them to be self-mapped.) Since there are no automorphisms of the reals, any real x must literally be mapped to x. Now since $x\overline{x} = \overline{x}x = |x|^2$ is real, and $\overline{x}$ is, up to real-proportionality, the unique 2^n-on which, when multiplied by x, yields a real, we see that $\overline{x}$ must be mapped to $k_x\overline{T(x)}$ for some real k_x. Now since the only linear transformations of multidimensional space which act as scalings along rays from $\vec{0}$, *are* scalings, k_x must be independent of x, i.e. we shall simply write "k." But considering $\overline{\overline{x}} = x$, we see that $k^2 = 1$ so that $k = \pm 1$. But $k = -1$ is impossible because the positive reals are mapped to the positive reals, so $k = 1$. The remaining claims should now be obvious. Q.E.D.

Corollary 109 (Inner product, Euclidean metric). *Any automorphism T of the 2^n-ons, $n \geq 1$, preserves Euclidean inner product: $\langle T(x), T(y)\rangle = \langle x, y\rangle$. Hence (considering linearity) it must be an orthogonal linear transformation, preserving $\vec{0}$ and the Euclidean metric.*

Proof: Follows from $2\langle x, y\rangle = |x + y|^2 - |x|^2 - |y|^2$. Q.E.D.

Reals, complex numbers, and quaternions. There are no automorphisms of the real numbers. The automorphism group of the complex numbers just consists of the identity and complex conjugation, and is abstractly $\mathbb{Z}_2$. The automorphism group of the quaternions is[64] abstractly SO(3). SO(3) consists of the maps $x \to qx\overline{q}$, where q is a quaternion of unit norm (3 degrees of freedom). It includes the map $a + bi + cj + dk \to a + bi - cj - dk$. (The map $x \to \overline{x}$ is *not* included, but is an *anti*automorphism, so that is ok.)

Octonions. The automorphism group of the octonions is[65] abstractly the 14-dimensional exceptional Lie group G_2. It was stated incorrectly by Gürsey & Tze [121] that G_2 consisted of the maps $x \to \overline{(ab)}[b(ax\overline{a})\overline{b}](ab)$ for unit norm octonions a, b ($14 = 7 + 7$ degrees of freedom). Unfortunately these maps are almost never automorphisms (nor are any of the two other, supposedly equivalent, maps given by [121]), as one concludes immediately by numerical test. Manogue & Schray [169] claim that G_2 consists of the maps

$$T_G(x): \quad x \to (d\ell) \cdot (c\ell)(d \cdot cx) \tag{265}$$

where c, d and ℓ are octonions with $|c|^2 = |d|^2 = |\ell|^2 = 1$, $\mathrm{re}\, c = \mathrm{re}\, d = \mathrm{re}\, \ell = 0$, and $\langle \ell, c\rangle = \langle \ell, d\rangle = \langle \ell, cd\rangle = \langle c, d\rangle = 0$ ($8 \times 3 - 10 = 14$ degrees of freedom). This, in contrast, passes numerical sanity checking.

Conway and Smith ([68] appendix to ch.6) note that the octonion automorphisms that take a particular quaternion subalgebra to itself form an $SO(4)$ and map the quaternion 2-tuple (x, y) to $(\overline{a}xa, \overline{a}yb)$ where a, b are quaternions (wlog of unit norm) describing the automorphism.

See [68][21][94][227][141][264] for more discussion of the real, complex, quaternion, and octonion automorphism groups; we regard that all as known, hence we have contented ourselves above with statements of the results only, without giving their proofs.

28.1 Rotations

This leads to the following descriptions of 7D and 8D rotations in terms of octonions, as promised in footnote 10. We use the facts that

$$T_{7/G}(x) \stackrel{\text{def}}{=} Lx\overline{L} \tag{266}$$

where $|L| = 1$, performs a rotation in 7-space that lies in $\mathrm{SO}(7)/G_2$, and

$$T_{8/7}(x) \stackrel{\text{def}}{=} RxR \tag{267}$$

with $|R| = 1$, performs a rotation in 8-space that lies in SO(8)/SO(7). Thus a 21-degree-of-freedom parameterization of SO(7), the 7D rotations, is

$$x \to T_{7/G}(T_G(x)) \tag{268}$$

and a 28-degree-of-freedom parameterization of SO(8), the 8D rotations, is

$$x \to T_{8/7}(T_{7/G}(T_G(x))). \tag{269}$$

28.2 16-on automorphisms

Theorem 110 (16-on automorphisms). *The full set of automorphisms of 16-ons (x, y) (regarded as octonion pairs) are generated by $(x, y) \to (g(x), g(y))$, where $g \in G_2$ is an octonion automorphism, and $(x, y) \to (x, -y)$. The automorphism group is abstractly $G_2 \times \mathbb{Z}_2$.*

Proof: Regard a 16-on as an ordered pair (x, y) of octonions.

The 16-ons $(x, 0)$ form the octonion subalgebra and also are the locus of the discontinuity in the right-multiplication map, hence are algebraically special, hence 16-ons of this form must be mapped, by any automorphism, only to 16-ons of this *same* form.

Plainly, any automorphism of the octonions $x \to T(x)$, $y \to T(y)$, yields *an* automorphism of the 16-ons (x, y), since the 16-on multiplication formula is defined by octonionic formulae. Thus the group of 16-on automorphisms contains G_2 as a subgroup. Our plan to determine the automorphism group A of the 16-ons will be to mod out the G_2 inside it, i.e., we consider the elements $T \in A$ which *fix* x, i.e. which map $T(x, y) = (x, f(y))$.

The 16-on equation $(a, b)(c, 0) = (ac, cb)$ [special case of our EQ 72] is mapped by such an automorphism to $(a, f(b))(c, 0) = (ac, cf(b)) = (ac, f(cb))$. Therefore, any such automorphism must obey $cf(b) = f(cb)$ for all octonions a, b, c. The only way in which this is possible is that $f(b) = \lambda b$ for some *scalar* λ, since[66] the only linear transformations of $\mathbb{R}^8$ which commute with every octonion left-multiplication are scalings. It is a simple matter to verify from EQ 72 that $\lambda = \pm 1$ are exactly the allowed values of this scaling parameter. Q.E.D.

[64] This is discussed in §2.1 of [149].

[65] This is discussed in §2.3 of [149].

[66] Octonion left-multiplications generate $SO(8)$. So any element of $SO(8)$ commuting with all octonion left-multiplications would necessarily commute with everything in $SO(8)$, and it should be obvious that only $\pm$ the identity matrix can do that.

28.3 2^n-on automorphisms

Theorem 111 (2^n-on automorphisms). *Let $n \geq 4$. The full set of automorphisms of 2^n-ons (x, y) (regarded as pairs of 2^{n-1}-ons) are generated by $(x, y) \to (g(x), g(y))$, where g is is a 2^{n-1}-on automorphism, and $(x, y) \to (x, -y)$. The automorphism group (if $n \geq 3$) is abstractly $G_2 \times (\mathbb{Z}_2)^{n-3}$.*

Proof: We have already established this for $n \leq 4$ so from now on assume $n \geq 5$. The key to the proof is to establish that the 2^{n-1}-on subalgebra S consisting of the first half of the coordinates is algebraically "special." At first this is not obvious because there are other "decoy" 2^{n-1}-on subalgebras, e.g. consider only allowing the first and third 2^{n-2}-wide blocks of coordinates to be nonzero.

But S has the following unique property among 2^{n-1}-dimensional nnacd subalgebras: elements $s \in S$ (plus you may add to s an arbitrary real multiple of a certain algebra element i which is orthogonal to everything in S) have the property that the left-multiplication map $x \to sx$ for generic x in the full 2^n-on algebra, is a rational function of degree smaller than every competitor.

Observe that "degree" is a algebraically visible notion, due to metrical behavior on the unit sphere (since by corollary 109 this metric is automorphism-invariant).

With this hurdle surpassed, we may now simply follow the proof of the preceding 16-on theorem, changing "16" to "2^n," "octonion" to "2^{n-1}-on," and "G_2" to "the 2^{n-1}-on aut group," everywhere. This establishes the induction step in an induction on n in which the base cases $n = 3$ and $n = 4$ were already known. Q.E.D.

Remark. Eakin and Sathay [92] found the automorphism groups of all the Cayley-Dickson 2^n-dimensional linear algebras, and claim the answer *also* is $G_2 \times (\mathbb{Z}_2)^{n-3}$. Their proof also depended on finding a (different) reason the 2^{n-1}-dimensional subalgebra in the first 2^{n-1} coordinates was "special." Their reason was, essentially ([92], lemma 1.2) that if y is a Cayley-Dickson 2^n-on such that x, x, y associate (in every order) for *all* x, then y is of the form $a + ib$ where $a, b \in \mathbb{R}$ and $i = e_{2^{n-1}}$. However, this claim is *not* true in our *non*linear 2^n-ons. All y of this form indeed work – but also, by theorem 34, all "niners" y work. I.e., 9-alternativity is violated in the linear Cayley-Dickson 2^n-ons if $n \geq 4$, but is satisfied in our nonlinear 2^n-ons; this is one (surprising) way in which our nonlinear 2^n-ons are nicer than the linear ones.

Remark. Our proofs about automorphism groups still go through over any base field F with char$F \neq 2$, instead of $\mathbb{R}$. The result is that the automorphism group of the 2^n-ons over F is $G_2(F) \times (\mathbb{Z}_2)^{n-3}$ for each $n \geq 3$, if $G_2(F)$ is the automorphism group of the octonions over F.

29 Multiplicative complexity

What is the minimum number of multiplications (and/or divisions) needed to accomplish such bilinear tasks as multiplying two octonions (or other "ons")?[67] The naive method for multiplying two Cayley-Dickson 2^n-dimensional numbers requires 4^n multiplications. However, it is possible to use much fewer. The simplest example is this. The naive method for multiplying two complex numbers $P = (a + ib)(c + id)$ requires 4 multiplications and 2 additive operations. But we may instead employ only 3 multiplications and 3 additive operations via $X = (a + b)(c + d)$, $Y = ac$, and $Z = bd$, and then $P = (Y - Z, X - Y - Z)$.

I undertook a computer search for bilinear algorithms with small numbers of multiplications. The results of that search are in table 29.1. (We shall not describe the search methods here, reserving that, and a deeper look at the search results, for a later publication. The theory of bilinear multiplicative complexity is discussed in [51].)

I believe that the cases with $\text{cost}_2 < 10^{-9}$ correspond to exact formulas. Thus, there apparently is a way to multiply octonions that employs only 24 real bilinear multiplications (improving over the old record 30; there is a lower bound of 15). The 8-mul and 3-mul exact algorithms for quaternion and complex multiplication were already known – and known to be minimal (even if non-bilinear algorithms are allowed) [106][86][85][76][33][132] – they here have been rediscovered by computer.[68]

#muls	cost_2	cost_2
	complex	bi-complex
2	1.0	1.7×10^{-30}
3	0.0	1.1×10^{-18}
4	0.0	4.5×10^{-19}
	quaternion	bi-quaternion
5		4.00004
6	2.867	2.0
7	1.934	3.2×10^{-18}
8	2.4×10^{-18}	9.5×10^{-18}
9	4.0×10^{-18}	
	octonion	bi-octonion
15		8.798
16		6.46
17		1.845
18		0.412
19		0.115
20	3.366	0.038
21	1.0605	0.0063
22	0.00014	0.002
23	8.7×10^{-5}	
24	2.2×10^{-10}	

Figure 29.1. Results of computer search for bilinear formulae for multiplying complex numbers, quaternions, and octonions using few bilinear scalar multiplications. ("Cost_2" is 0 if exact formula; positive if inexact formula; computer search attempts to minimize this but often cannot be completely successful due to limitations of floating point arithmetic.) In the "bi" cases the "scalars" are complex numbers.

What is perhaps more interesting is the computer's apparent discovery of a 22-mul "ϵ-algorithm" for multiplying octonions

[67] The justification for only considering multiplications is supposed to be that they are much more expensive than either additions or scalings by constant factors. This is maximally true if the coefficients are not reals but rather large *matrices*.

[68] At least 8 multiplications and/or divisions are required to reciprocate a quaternion, and at least 11 are required to perform a quaternionic division [33].

to accuracy $O(\epsilon)$. That is: the constant coefficients in the algorithm depend rationally on ϵ. (Multiplication by a constant does not count as a "true bilinear multiplication." By choosing ϵ to be, say, 2^{-100}, we can get high accuracy.)

Such ϵ-algorithms first arose during investigations of the bilinear multiplicative complexity of matrix multiplication. The naive method for multiplying a 2×2 matrix by a 2×3 matrix requires $2{\cdot}2{\cdot}3 = 12$ multiplications. Hopcroft et al. [127][128]) found a way to do it with only 11 multiplications. Alekseyev [13] claimed to have shown 11 to be minimum possible. (There are errors in his proof, although his result is probably correct.) However, Bini et al. [32] found a 10-multiplication ϵ-formula, illustrating the fact that ϵ-algorithms can have fewer multiplications than any exact algorithm. This leads [51] to an algorithm for (exactly) multiplying $N \times N$ matrices, $N \to \infty$, in $O(N^{2.77989})$ (exact) arithmetic operations, improving over both the naive $O(N^3)$ method and Strassen's $O(N^{2.80735})$ method. The present record is $N^{\epsilon+2.375477\ldots}$ by Coppersmith and Winograd [69] and employs not only ϵ-algorithms, but many other ideas due to many authors.

The fact that bicomplexes may be multiplied in only 2 complex multiplications (known to be minimal) is due to their algebra isomorphism to $\mathbb{C} \oplus \mathbb{C}$ discovered by C.Segre [230] in 1892 (see our theorem 9), and here rediscovered by the computer. This is the simplest example I know of where, by allowing *complex* constant coefficients in a bilinear algorithm, the mul count may be decreased below what is possible if only real coefficients are permitted.

The fact that biquaternions may be multiplied in only 7 complex multiplications (which is known to be minimal) is due to their algebra isomorphism (known to C.F.Gauss) to $\mathbb{C}^{2\times 2}$, combined with Strassen's 7-mul formula [240] for multiplying 2×2 matrices, both of which are rediscovered here by computer. The situation with bi-octonions remains unclear.

Theorem 112 (Both way Cayley-Dickson product). *There is a bilinear algorithm for computing* both AB and BA *simultaneously, where A and B are two N-dimensional Cayley-Dickson numbers, in* $\binom{N+1}{2}$ *bilinear multiplications.*
Remark. This improves over the naive N^2 by a factor approaching 2 as $N \to \infty$.

Proof: Here is the algorithm:

1. Find all $A_i \cdot B_i$ products (N in all).
2. Find all $(A_0+A_i)\cdot(B_0+B_i)$ products for $i = 1, \ldots, N-1$, i.e. $N-1$ in all.
3. Find all $(A_i - A_j) \cdot (B_i + B_j)$ products for $1 \le i < j \le N-1$, i.e. $(N-1)(N-2)/2$ in all.
4. Finally, we *claim* it suffices to take linear combinations (with constant coefficients) of the preceding results. The total number of bilinear multiplications required is $N + N - 1(N-1)(N-2)/2 = \binom{N+1}{2}$.

The final *claim* is justified because this corresponds to De Groote's 10-mul method [76] for quaternions in the case $N = 4 = 2^2$ and to Karatsuba's complex-number-multiplication method if $N = 2 = 2^1$, and we may now just consider all the quaternion subalgebras inside Cayley-Dicksons if $N = 2^n > 4$. This algorithm actually works in any linear algebra whose multiplication table is defined by quaternion (or complex) subalgebra multiplication tables with 1 common identity element. Q.E.D.

30 Open problems

1. Top open problems about the loop taxonomy in §26.2 include:

1. Is there a finite equational basis for diassociativity? Probably the answer is "no" since there is none for power-associativity [102]. (One might also ask: is there a finite equational basis for diassociativity within *power-associative* loops?)
2. Are IP-alternative loops necessarily power-associative?
3. Is every M_4 loop an A-loop?
4. Does LR-alternativity imply 2-sided inverses?

Perhaps related, and perhaps not: Are flexible 16-ons (i.e obeying $x \cdot yx = xy \cdot x$) impossible? (See also [28] and our §26.5 re this.)

2. (a) Is the multiplicative loop of unit-norm 16-ons (over $\mathbb{R}$) "simple?" Paige [192] and Liebeck [165] showed that the octonions over finite fields were the only simple *finite* Moufang loops, aside from the (already-classified) finite simple groups. (b) If the 16-ons are taken over finite fields, instead of over $\mathbb{R}$, what happens? Does it lead to any interesting discrete structures (such as the Hamming codes and the 240 root vectors of E_8, which arise [67] from the unit-norm octonions)? Are there interesting derived algebras?

3. Can it be shown, on topological grounds, that nnacd division algebras over $\mathbb{R}$, whose generic division problems have *unique* solutions, can only exist in dimensions 1,2,4,8,16 – even if a *dis*continuous multiplication map (*but* with only certain mild kinds of discontinuities, e.g. "generalized smoothness" in the sense of §22) is permitted? **Conjecture:** generalized-smooth maps $S^n \times S^n \to S^n$ exist only if $n \in \{1, 3, 7, 15\}$. **Conjecture:** If there are n tangent vector fields, all mutually orthonormal, on S^n, and these fields are "generalized smooth," then $n \in \{1, 3, 7, 15\}$. **Conjecture:** If there is a generalized-smooth "vector-product" operation on pairs of n-vectors, then $n \in \{1, 3, 7, 15\}$. **Conjecture:** If there is a nnacd-algebra in $\mathbb{R}^n$, with 2-sided identity, with right-linear multiplication, and such that the Euclidean norm is multiplicative, and in which generic division problems have a unique solution, then $n \in \{1, 2, 4, 8, 16\}$.

4. Do the 16-ons have applications in theoretical physics? J.C.Maxwell's [171] initial derivation of his equations for electromagnetism clearly was inspired by the quaternions. Recently, quaternions have been usefully employed in celestial mechanics, e.g. solar system simulations [247][248][249][250][251]. They have also been used in fluid mechanics [221]. C.Lanczos, in his PhD thesis [164] of 1919, claimed that the Maxwell vacuum equations are precisely the conditions – analogous to the Cauchy-Riemann equations for complex functions – for the "analyticity"[69] of a biquaternion-

[69] See §21.3. Much later, Lanczos's characterization of Maxwell's equations was rediscovered by Imaeda [137] by using Fueter's theory. Neither Fueter's group, nor Imaeda, were aware of Lanczos's earlier work. Lanczos also discovered the quaternion generalization of the Cauchy integral theorem (which involves a 3-dimensional integral) well before these authors.

valued function in 4-space. Daboul & Delbourgo [73] discovered an interesting new representation of octonions, and then used it to show[70] that P.A.M.Dirac's equation for the wavefunction of an electron has a very nice octonionic reformulation – indeed apparently nicer than Dirac's own formulation involving certain 4×4 matrices. (These, of course, are two of the most important equations in physics. But see also [193].) Proca's equation for spin-1 particle ("Maxwell's equations with a massive photon" [237]) also can be reformulated quaternionically, and we've seen earlier how Lorentz transformations may be nicely represented biquaternionically. So far, physicists have not made any great use of these observations. Baez ([21], page 147) claimed that $\mathrm{SL}(2, D)$ is algebraically isomorphic to the Lorentz group $\mathrm{SO}(d+1, 1)$ for the d-dimensional ($d \in \{1, 2, 4, 8\}$) division algebras D with identity over $\mathbb{R}$.

More recently there has been interest in, and success at, reformulating 10-dimensional string theory and supersymmetry theory octonionically, and in trying to develop octonion-based Grand Unified Theories. Numerous papers on this will be retrieved in any computerized literature search, but we are incompetent to comment about them. The validity of the Trotter product formula (EQ 153) – which is the basis of quantum mechanics – in the 16-ons, also suggests the possibility of applications to physics.

5. Might it be possible to (a) Reach a complete understanding of every possible rational "doubling formula" that leads to a multiplication which preserves Euclidean norm; (b) show that if such a 2^n-dimensional multiplication exists, it must arise via n successive such doublings; (c) understand in what ways our doubling formula is the "best" among these?

6. Improve our 16-on uniqueness theorem 60 so that no assumption that the 16-ons have an 8D subalgebra, is needed anymore. Decide what (if anything) the next (i.e. 15D) identity should be, corresponding to the Jacobi identity and Malcev identities for the 3D and 7D vector products arising from the pure-imaginary quaternions and octonions respectively.

7. Classify the "homogeneous" (in the sense of [84]) *nnacd*-algebras. I conjecture there are none with dimension> 8.

8. For what percentage of unit-norm y is the 2^n-on right-multiplication map $x \to xy$ two-to-one, one-to-one, etc.?

9. Find some version of the following **conjecture** that is true, and prove it: The 2^n-ons are the only normed left-alternative right-linear weak-linear power-associative nnacd-algebras whose multiplication law is defined by rational functions, such that they contain a 4D associative[71] division subalgebra H, and such that the flexible, alternative, and distributive laws each are obeyed provided at least one of their variables lies in H.

10. Find the multiplicative complexity of 2^n-on multiplication.

11. What cardinalities are possible for finite abstract 2^n-ons, as defined in §26.5? Are the cardinalities that arise by just applying our doubling construction starting from some finite field, the only possibilities?

31 Historical notes

Some of the following information about the little-known early mathematicians Olinde Rodrigues [188] and Thomas P. Kirkman [31] (and the latter's famous "schoolgirls problem" – which as we now see is related to the sedenions) seems to be unavailable in the usual sources about the history of mathematics.

31.1 Rodrigues: mathematician and social reformer

Benjamin Rodrigues was born 6 Oct 1795 and died 17 Dec 1851, both in France. He used "Olinde" in preference to his given first name. Apparently nobody knows what he looked like. His father was an accountant/banker of Spanish descent. Rodrigues acquired a doctorate at the newly founded University of Paris in 1815. He was influenced by Gaspard Monge (1746-1818) and taught by M.Dinet. R. did not enter the Ecole Polytechnique despite taking their admission exam twice (came top). There have been claims R. was barred from admission because of being Jewish, but those claims seem contradicted by evidence. Nevertheless, anti-Semitism after the restoration in 1816 seems to have been sufficiently strong (and R. found this obvious) to block him from pursuing an academic career. R's thesis contained the (now well known, but at that time ignored and forgotten) "Rodrigues formula" for Legendre polynomials. At about the same time he found a theorem associated with his name about curvature of surfaces in differential geometry.

Rodrigues later became a wealthy Parisian banker, the director of the Caisse Hypothécaire bank, and an investor in early railroads. In his spare time he published pamphlets on social reform, politics, and banking, including arguing against racism and sexism. Rodrigues is best known as a patron and/or disciple of the philosopher and pre-socialist economist Claude Henri de Rouvroy, the Comte de Saint-Simon (1760-1825). Apparently Rodrigues and Saint-Simon only first met in May 1823, when R. was 26. This was only two years before the latter's death on 19 May 1825. Rodrigues became, by some accounts, S-S's chief assistant, and the formation of the sect of Saint-Simonians was largely due to his exertions. Rodrigues' brother Eugene apparently also was an excellent student at the Univ. of Paris and a follower of Saint-Simon, but he died at the age of 23 from a heart problem.

Saint-Simon had initially been a rich nobleman (his family claimed a line of ancestors tracing back to Charlemagne; S-S. once organized the first company to build the Panama Canal, but that project was overtaken by the French Revolution and failed). But he later became penniless. S-S. wrote prolifically about such topics as the future of industrialization, the utopian reorganization of society, emancipating women, new improved kind of Christianity, etc. Some have considered Saint-Simon, for his advocacy of studying history and religion via quasi-scientific methods, to be the founder of sociology and perhaps of theology. He is credited with inspiring Marx and Engels and of being the inventor of the Panama

[70] The key problem overcome by Dirac was to find the "square root" a certain differential operator. The point is that such operator square roots can be easy to create if we allow ourselves to use octonions.

[71] Perhaps "4D associative" must be replaced by "8D alternative."

Canal concept. But some have dismissed him as unorganized and incoherent.

After Saint-Simon's death, his followers diverged in different directions, some advocating "free love," others forming a quasi-religious cult. Rodrigues became infuriated with the directions leading Saint-Simonians S-A. Bazard and especially P. d'Enfantin were taking, and in February 1832 split away from them, declaring himself to be the one true representative of Saint-Simon. Rodrigues published Saint-Simon's *Oeuvres* in 1832 and succeeded him as head of the French Socialist party (or what later became that party). Also, soon after S-S's death, R. founded the journal *Le Producteur*.

Rodrigrues' 1840 paper [J.de Math. Pures et Appliquees 5 (1840) 380-440] on rotations, discussed in [15][117], may be thought of as a discovery – predating Hamilton's – of the quaternions. (Still earlier, C.F.Gauss had also made unpublished remarks about 2×2 complex matrices and Euler's 4-square formula [published by Euler in 1754 and expressing the multiplicativity of the quaternion norm], which also may be thought of as a pre-Hamilton discovery of the quaternions. Hamilton published incorrect versions of Rodrigues' rotation formula. But, to paraphrase a remark by John Tukey regarding his [re]discovery of the FFT: when Hamilton discovered the quaternions, they stayed discovered.) In combinatorial works which also were forgotten and ignored until long afterwards, Rodrigues discovered [J.de Math. P.&A. 4 (1839) 236-240] that the number of permutations of $\{1, 2, 3, ..., n\}$ having I inversions was the coefficient of t^I in $(1+t)(1+t+t^2)(1+t+t^2+t^3)\dots(1+t+t^2+...+t^{n-1})$, and found a formula (derived recursively) for the number of ways to triangulate an n-gon.

A conference on Rodrigues' life and works took place on 1 Dec 2001 at Imperial College, London [188]. On 17 July 1898, the *Olinde Rodrigues*, 3098 tons, was captured by US forces in the cruiser *New Orleans* off Cuba when it attempted to run the US blockade of that island [72].

31.2 Kirkman: sedenion-schoolgirl connection?

The triples in EQ 55 are a solution to the Reverend Th.P.Kirkman's famous "15 schoolgirls problem" from combinatorics [153][156][157], indeed, it is [170] the most symmetric possible STS(15), with 8!/2 symmetries (or 168 symmetries for either of its two resolutions into a KTS(15), which number also is maximal).

Could Kirkman (1806-1895) – who was a graduate of Trinity College, Dublin (same location as Hamilton), was a friend of Hamilton's, and was interested in quaternions, and who created the schoolgirls problem only 4 years after Hamilton and Graves discovered their algebras – have known about the sedenions, and indeed might his invention of the schoolgirls problem have been inspired by sedenionic questions? The answer appears to be: Kirkman knew of the connection between sedenions and the schoolgirls problem and worked on both during the same 3-year-wide span. However, Kirkman's papers contain errors which prevented him from actually discovering the sedenions.

Here is a deeper look. In 1846, Kirkman invented [31][153] what now are mis-named "Steiner triple systems" (STSs), indeed completely settling their existence question years before Steiner even posed it. An STS(n) is a set of triples of n things such that each pair of things is contained in exactly 1 triple; Kirkman showed an STS(n) exists iff $n \bmod 6 \in \{1, 3\}$. He later posed and solved [156][157] the "schoolgirls problem" of finding a "resolvable" STS(15), i.e. a KTS(15), where a KTS(n) means an STS(n), which may be partitioned into "parallel classes" of $n/3$ mutually-disjoint triples each. J.J.Sylvester then asked whether, further, the set of all $\binom{15}{3}$ triples could be partitioned into 13 disjoint KTS(15)'s. Kirkman claimed incorrectly [156] to have solved Sylvester's problem, but in fact his KTS(15)'s overlap. The first genuine Sylvester solutions were found by R.H.F.Denniston over 120 years later [77]. Kirkman in 1848 [154][156] wrote papers concerning the possible existence of "pluquaternions," i.e. a 16-dimensional (or more generally N-dimensional) algebra with multiplicative Euclidean norm. Kirkman (spurred by a "pregnant hint" from Cayley) claimed to give a combinatorial test of existence for such N-ons for any particular even N, and this test was, essentially, the existence question for an STS($N-1$) but with certain sign/chirality/consistency conditions imposed on each triple. He further claimed to have carried out this test in the case $N = 16$, finding as the result that 16-dimensional pluquaternions, and bilinear sum-of-16-squares identities, could not exist. While this conclusion of impossibility was correct, as was proved by A.Hurwitz nearly 50 years later, Kirkman's reasoning wasn't. He seems not to have understood how to manipulate nonassociative quantities. Indeed, by means of some bogus reasoning Kirkman deduced that the sedenions exhibit an internal contradiction of the form $i = -i$, and, not to be deterred, proposed introducing "bisignal imaginaries" for which this would not be a contradiction, but merely a new law. This is quite insane. However, this can be somewhat salvaged if we recognize (and this is not at all what Kirkman had in mind) that $1 = -1$ over any field F with char$F = 2$. I.e.:

Theorem 113. *For any N with N mod $6 \in \{2, 4\}$, there is an N-dimensional commutative (but in general non-associative) algebra over* GF_2*, such that the sum of squares (which is just the parity of the number of 1-bits) is multiplicative.*

Proof: Define $N-1$ different $\sqrt{-1}$ symbols, and define their multiplication by requiring that each triple from a STS($N-1$) on the symbols, acts like quaternions (i, j, k). The norm will be multiplicative because all the "unwanted cross terms" will be multiples of 2, i.e. 0; i.e. because $(ax+by)^2 = (ax)^2+(by)^2$ in characteristic-2 fields. Since the quaternions *mod 2* are commutative, so are these. Indeed these N-ons are alternative, i.e. diassociative, but for all sufficiently large N one can easily construct example STSs yielding non-associativity. Q.E.D.

On the other hand, Kirkman's actual constructions of Steiner systems and of sum-of-squares identities, presumably were correct (and all were rediscovered by later authors). For example, Kirkman found that any product of two sums of $8k$ squares may always be expressed as a sum of $8k^2$ squares

[72] The former name of this ship was *Franconia*, built 1872. It was purchased from Hamburg America Line and scrapped in 1908. This may be the only ship named after a mathematician.

of bilinear functions, so that, in particular, from the case $k = 2$ we have that $(\sum_{16} x_j^2)(\sum_{16} y_j^2) = (\sum_{32} z_j^2)$ where the z_j are bilinear functions of the x_k and y_ℓ. Kirkman credits this particular ($k = 2$; 16,16,32) special case to a communication from "professor J.R.Young."[73] Also, Kirkman showed any product of sums of $(6k + 2b + 8)n$ squares where $k \geq 0$ and $b \in \{0, 1\}$, may be expressed as a sum of $[9k^2 + 3(2b+5)k + (b+7)b+8]n^2$ squares. In particular, take $n = 1, k = 0, b = 1$ to get: $(\sum_{10} x_j^2)(\sum_{10} y_j^2) = (\sum_{16} z_j^2)$. These (16,16,32) and (10,10,16) identities were rediscovered much later, and still later were proved, via topology [2][211], to be best possible. (See also [163][234][5].)

32 Conway's role in all this

John H. Conway[74], after hearing lectures by A.Pfister in about 1969, invented EQ 72 and realized it would yield 16-ons with multiplicative Euclidean norm. He did not publicize this. In 2002, Conway was writing a book [68] on Octonions with Derek Smith[75]and was attempting to un-bury his old 16-on ideas, and happened to mention EQ 72 to me. After then discovering its generalization to any n and the 16-on division-existence and uniqueness theorems, I proposed to Conway that we write a joint paper on 2^n-ons. But, due to other responsibilities, Conway ultimately was only able to do a small fraction of the work on this paper, and hence eventually proposed that he no longer be listed as an "author," and instead merely be given a hefty "acknowledgment." Conway has been very helpful to me throughout. He also was mostly responsible for the simplified equation 111 and theorem 110, and partially responsible for the notions of the 8 "pre-eminent" formulas in §27 as well as spotting several important errors in early drafts.

32.1 Conway's ideas about notation and simplicity

Conway emphasized to me the importance of presenting the *simplest possible* form of the key doubling formula which defines the 2^n-ons, and he wanted to devise the simplest possible notations for dealing with them, and also to prove that our definition of 2^n-ons was the "best" possible one. Let me discuss some of his and my thoughts on that.

First, it is not clear what "best" (or "simplest") should mean. Our lemmas 62 and 63 and theorems 60 and 64 (see also §14) gave senses on which our 16-ons are uniquely best, and weaker senses in which our 2^n-ons for all n are uniquely best. But neither Conway nor I are fully satisfied with this, and indeed I found different 16-ons (EQ 259) which in some ways seem "superior."

Conway was unhappy about the large number of "bars" in my defining formula EQ 68 for the 2^n-ons[76]. Therefore Conway devised the simplified but isomorphic formula EQ 111, which my lemma 62 shows is indeed the simplest possible way to rewrite EQ 68.

But EQ 111 has some annoying features, such as the fact that "left multiplication by i" does not do the "expected thing $(0, 1)(c, d) = (-d, c)$" [although this *is* obeyed by EQ 68] but instead causes $(0, 1)(c, d) = (-\overline{d}, \overline{c})$. Thus, annoyingly, the 2^n-ons of EQ 111 obey *neither* the "eyes-left $(a, b) = a + ib$" nor "eyes-right $(a, b) = a + bi$" conventions, despite the fact that they are isomorphic to the "eyes-left" 2^n-ons of EQ 68. Unhappiness reigned.

Conway then came to believe that the following was the Path Of Righteousness. Define not one, but *two*, (related) vector-vector multiplication operations among 2^n-ons a, b, denoted

$$c = a\{b\} \quad \text{and} \quad c' = \{a\}b \tag{270}$$

The first of these is the usual 2^n-on multiplication $c = ab$ of EQ 68. The second is $c' = \overline{\overline{a}\overline{b}}$. I.e.,

$$\{a\}b \overset{\text{def}}{=} \overline{\overline{a}\{\overline{b}\}}. \tag{271}$$

(In the 2^n-ons with $n \leq 3$, these two kinds of multiplication are identical due to theorem 8.) The $\{\}$'s surround the multiplicand in which the multiplication is *linear*[77].

We hypothesize that the $\overline{\overline{a}\overline{b}}$ operation will arise frequently, as will long sequences of repeated left-multiplications or repeated right-multiplications. Conway's notation is well suited to handling these events. For example, Conway would rewrite our 2^n-on defining formula EQ 68 as

$$\boxed{(a, b)\{(c, d)\} = \big(a\{c\} - \{d\}\overline{b},\ \{c\}b + \{\overline{a}\{\{d\}b^{-1}\}\}b\big),} \tag{272}$$

[where in the special case $b = 0$ then use

$$(a, b)\{(c, d)\} = (a\{c\} - \{d\}\overline{b},\ \{c\}b + \overline{a}\{d\}) \tag{273}$$

instead of EQ 272, and as usual $\overline{(a, b)} \overset{\text{def}}{=} (\overline{a}, -b)$] which has only two bars, and also strikingly resembles the original linear Cayley-Dickson formula EQ 48, making it easy to remember. Because this is so nice, Conway then dropped his objections to EQ 68 and abandoned his favortism of EQ 111, provided EQ 68 is rewritten as EQ 272.

I have chosen to stay with conventional algebra notation in this monograph, but Conway's notation may prove superior in the long run.

[73]Dickson [79] cites papers by Young in Trans. Royal Irish Acad. 21, II (1848) 311-338; Proc. Royal Irish Acad. 4 (1847) 19-20, 50; Philosophical Magaz. (3) 34 (1849) 114.

[74]Conway: Math. Dept., Princeton University, Fine Hall, Washington Road, Princeton NJ 08544-1000.

[75]**Note on Smiths.** Derek Smith (coauthor with J.H.Conway of book [68] on octonions), J.D.H.Smith (loop theorist and former student of Conway's), Tara L. Smith (coauthor with Paul Yiu of papers about Octonions, Cayley-Dickson algebras, and Hurwitz's sum of squares problem), Frank D. "Tony" Smith (author of extensive strange web pages about octonions and physics), and Warren D. Smith are, as far as we know, all unrelated.

[76]But I personally rather like them because, essentially, the most bars that can be used, are used, and always in a right-to-left manner, which makes the formula easy to remember – also the matrix formulation in EQ 57 has a pleasing "symmetry" about it.

[77]It seems best to emphasize linearity, rather than nonlinearity, since in long products, if $n \geq 4$, there will be exactly one linear multiplicand, in general.

33 Acknowledgments, apologia, and computer code

33.1 Acknowledgments

Daniel B. Shapiro[78], author of [231], also helped me by contributing about 4 pages of comments on an earlier draft, including pointing out several important papers I had not known about, pointing out the current formulation of theorem 4 item 6, and spotting one of the same errors detected by Conway. Derek Smith also helped me.

33.2 Two missing topics

Despite its length, in some ways the present work remains incomplete. The two most significant omissions (which I had originally intended to include) are:

1. A section on how to define "determinants" of matrices of 2^n-ons,
2. Studies of 2^n-ons over finite or discrete fields and rings rather than the reals; the question of whether interesting new combinatorial configurations can be obtained in that way; and the examination of subalgebras of the 2^n-ons.

These perhaps will be addressed in future works.

33.3 Computer code

During this research I wrote a useful collection of computer routines, in the computer language "C," [158] for experimenting with 2^n-ons and their variants. It is available electronically (as is this monograph itself) from `http://math.temple.edu/~wds/homepage/works.html`.

References

[1] J.F.Adams: On the non-existence of elements of Hopf invariant one, Annals of Math. 72 (1960) 20-104.

[2] J.F.Adams: Vector fields on spheres, Annals of Math. 75 (1962) 603-632.

[3] J.P.May: Memorial address and reminiscences about J. Frank Adams: The Mathematical Intelligencer 12,1 (1990) 40-48.

[4] J.F.Adams & M.F.Atiyah: K-theory and the Hopf invariant, Quart. J. Math. Oxford (2) 17 (1966) 31-38.

[5] José Adem: Construction of some normed maps, Boletin de la Sociedad Matematica Mexicana 20,1 (Abril 1975) 59-75.

[6] Max K. Agoston: Algebraic topology, a first course, Marcel Dekker Inc. 1976.

[7] M.Ajtai, J.Komlos, E.Szemeredi: Sorting in $c \log n$ parallel steps, Combinatorica 3,1 (1983) 1-19.

[8] N.I. Akhiezer & I.M. Glazman: Theory of linear operators in Hilbert space, Dover 1993.

[9] A.A.Albert: Quadratic forms permitting composition, Annals of Math. (2) 43 (1942) 161-177; MR 3,261.

[10] A.A.Albert: Absolute valued real algebras, Annals of Math. 48, 2 (1947) 495-501.

[11] A.A.Albert: Power-associative rings, Trans. Amer. Math. Soc. 64 (1948) 552-593.

[12] A.A.Albert: On the right-alternative algebras, Annals of Math. (ser. 2) 50 (1949) 381-328; The structure of right-alternative algebras, 51 (1954) 408-417.

[13] V.B.Alekseyev: On the complexity of some algorithms of matrix multiplication, J.Algorithms 6 (1985) 71-85.

[14] S.C.Althoen et al.: Rotational Scaled Quaternion Division Algebras, J. Algebra 146,1 (1992) 124-143.

[15] Simon L. Altmann: Hamilton, Rodrigues, and the Quaternion Scandal, Mathematics Magazine 62 (1989) 291-308.

[16] A.S.Amitsur & J.Levitski: Minimal identities for algebras, Trans. Amer. Math. Soc. 105 (1962) 202-221.

[17] M.A.Armstrong: Basic Topology, Springer 1983.

[18] Emil Artin: Geometric algebra, Wiley Interscience 1957, reprinted 1988.

[19] M.Aschbacher, M.Kinyon, J.D.Phillips: Finite Bruck loops, `Math.GR/0401193`.

[20] Helmer Aslaksen: Quaternionic determinants, Mathematical Intelligencer 18,3 (1996) 57-65.

[21] John C. Baez: The Octonions, Bull. Amer. Math. Soc. 39 (2002) 145-205.

[22] A.Baker: Transcendental Number Theory, Cambridge Univ. Press 1975.

[23] A.Barlotti & K.Strambach: The geometry of binary systems, Advances in Math. 49,1 (1983) 1-105.

[24] A. Barvinok: Computing mixed discriminants, mixed volumes, and permanents, Discrete & Computational Geometry 18 (1997) 205-237.

[25] A. Barvinok: Polynomial time algorithms to approximate permanents and mixed discriminants to within a simply exponential factor, Random Structures & Algorithms 14 (1999) 29-61.

[26] Alexander Barvinok: New permanent estimators via noncommutative determinants, 2000.

[27] W.Baur & V.Strassen: The complexity of partial derivatives, Theoretical Computer Sci. 22 (1983) 317-330.

[28] G.M.Benkart, D.J. Britten, J.M. Osborn: Real flexible division algebras, Canadian J. Math. 34,3 (1982) 550-588.

[29] F.Beukers, J.P.Bézivin, P.Roba: An alternative proof of the Lindemann-Weierstrass theorem, Amer. Math. Monthly 97,3 (1990) 193-197.

[30] F. Bien: Construction of telephone networks by group representations, Notice AMS 36,1 (1989) 5-22.

[31] N.L.Biggs: T.P.Kirkman, mathematician, Bull. London Math'l Soc. 13 (1981) 97-120.

[32] D.Bini, M.Capovani, F.Romani, G.Lotti: $O(n^{2.7799})$ complexity for approximate matrix multiplication, Information Proc. Lett. 8,5 (1979) 234-235.

[33] Markus Bläser, Peter Kirrinnis, Daniel Lauer: On the multiplicative complexity of the inversion and division of Hamiltonian quaternions, Foundations of Computable Mathematics 2,2 (2002) 191-199.

[34] F. van der Blij: History of the octaves, Simon Stevin, Wisen Natuurkundig Tijdschrift 34, III (Feb 1961) 106-125; MR 24#A149.

[78] Shapiro: Dept. Math., Ohio State University, 231 W 18th Avenue Columbus, OH 43210 USA.

[35] B.Bojarski, T.Iwaniec: Another approach to the Liouville theorem, Math. Nachrichten 107 (1982) 253-262;

[36] G.Bol: Gewebe und Gruppen, Math. Annalen 114 (1937) 414-431.

[37] Raoul Bott and John Milnor: On the parallelizability of the spheres, Bull. Amer. Math. Soc. 64 (1958) 87-89.

[38] H.Brandt: Idealtheorie in Quaternionalgebren, Mathematische Annalen 99 (1928) 1-29.

[39] H.Brandt: Zur Zahlentheorie der Quaternionen, J.Buch deutsch. Math V. 53 (1943) 23-57.

[40] Glen E. Bredon: Algebraic topology, Springer (GTM #139) 1993.

[41] Murray Bremner: On algebras obtained from the Cayley-Dickson process, Commun. Algebra 29,8 (2001) 3523-3534.

[42] Murray Bremner & Irvin Hentzel: Identities for algebras obtained from the Cayley-Dickson process, Commun. Algebra 29,8 (2001) 3523-3534.

[43] L.E.J.Brouwer: Beweis der Invarianz der Dimensionzahl, Math.Annalen 70 (1911) 161-165.

[44] L.E.J.Brouwer: Über Abbildungen von Mannigfaltigkeiten, Math.Annalen 71 (1912) 97-115.

[45] Robert B. Brown: On generalized Cayley-Dickson algebras, Pacific J. Math. 20 (1967) 415-422.

[46] Robert B. Brown & Alfred Gray: Vector cross products, Commentarii Mathematici Helvetici 42 (1967) 222-236.

[47] Richard Hubert Bruck: A survey of binary systems, Springer-Verlag 1958, third corrected printing 1971 (Ergebnisse der Math. #20).

[48] R.H.Bruck: Loops with transitive automorphism groups, Pacific J. Math. 1 (1951) 481-483.

[49] R.H. Bruck & Erwin Kleinfeld: The structure of alternative division rings, Proc. Amer. Math. Soc. 2 (1951) 878-896.

[50] R.H. Bruck & L.J. Paige: Loops whose inner mappings are automorphisms, Annals of Math. 63,2 (1956) 308-323.

[51] P.Bürgisser, M.Clausen, M.A.Shokrollahi (with T.Lickteig): Algebraic complexity theory, Springer (GMW #315) 1997.

[52] John Canny: Improved algorithms for sign-determination and existential quantifier elimination, Computer Journal 36,5 (1993) 409-418.

[53] E.Cartan, J.A.Schouten: On Riemannian geometries admitting an absolute parallelism, Koninklijke Akademie van Wetenschappen te Amsterdam, Proc. Sec. Sciences 29 (1926) 933-946.

[54] J.W.S. Cassels, W.J. Ellison, A. Pfister: On sums of squares and on elliptic curves over function fields, J. Number Theory 3 (1971) 125-149.

[55] Arthur Cayley: On Jacobi's elliptic functions in reply to the Rev. B. Bronwin; and on quaternions, Philos. Magazine 26 (1845) 208-211.

[56] O.Chein: Lagrange's theorem for M_k loops, Arch. Math. Basel 24 (1973) 121-122.

[57] O.Chein: Moufang loops of small order I, Trans.Amer.Math.Soc. 188 (1974) 31-51.

[58] O.Chein: Moufang loops of small order, Memoirs AMS 13 (1978) #197.

[59] O. Chein, M.K. Kinyon, A. Rajah, P. Vojtechovsky: Loops and the Lagrange Property, Results Math. 43, 1-2 (2003) 74-78.

[60] O.Chein & H.O.Pflugfelder: On maps $x \to x^n$ and the isotopy-isomorphy property of Moufang loops, Aequationes Math. 6 (1971) 157-161.

[61] O.Chein, H.O.Pflugfelder, J.D.H.Smith: Quasigroups and loops, theory and applications, Heldermann Verlag 1990.

[62] O.Chein & A.Rajah: Feasible orders of nonassociative Moufang loops, Comment.Math.Univ.Carolin. 41,2 (2000) 237-244.

[63] O.Chein & D.A.Robinson: An 'extra' identity for characterizing Moufang loops, Proc.Amer.Math.Soc. 33,1 (1972) 29-32.

[64] V.P.Chuvakov: Prime, right-alternative, almost-alternative rings, Algebra & Logic 25 (1986) 380-387

[65] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson: ATLAS of finite groups, Clarendon Press Oxford 1985.

[66] J.H.Conway: On numbers and games, Academic Press 1976.

[67] J.H.Conway & N.J.A.Sloane: Sphere packings, lattices, and groups, (Third edition) Springer-Verlag 1998.

[68] J.H.Conway & Derek Smith: On quaternions and octonions, A.K.Peters, Jan. 2003.

[69] D.Coppersmith & S.Winograd: Matrix multiplication via arithmetic progressions, J.Symbolic Comput. 9,3 (1990) 251-280. Abbreviated version in ACM Sympos. Theor. Computer Sci. 19 (1987) 1-6.

[70] H.S.M.Coxeter: Quaternions and Rotations, Amer. Math. Monthly 53 (1946) 136-146 & postscript 588.

[71] H.S.M.Coxeter: Integral Cayley numbers, Duke Math. J. 13 (1946) 561-578.

[72] Jane Cronin: Fixed points and topological degree in nonlinear analysis, American Mathematical Society, Providence, R.I. 1964

[73] J.Daboul & R.Delbourgo: Matrix representations of octonions, and generalizations, J.Math'l Physics 20,1 (1984) 1-10.

[74] J.W.Dauben: Georg Cantor: His Mathematics and Philosophy of the Infinite, Princeton University Press 1990.

[75] C.A.Deavours: The Quaternion Calculus, Amer. Math. Monthly 80,9 (1973) 995-1008.

[76] Hans F. de Groote: On the complexity of quaternion multiplication, Information Processing Letters 3,6 (July 1975) 177-179.

[77] R.H.F. Denniston: Some packings with Steiner triple systems, Discrete Math. 9 (1974) 213-227; Sylvester's problem of the 15 schoolgirls, 229-233.

[78] P.Dentoni and M.Sce: Funzioni regolari nell'algebra di Cayley, Rendiconti Seminario Matematico Universita Padova 50 (1973) 251-267.

[79] L.E.Dickson: On quaternions and their generalization and the history of the eight square theorem, Annals of Math 20,3 (1919) 155-171 and 297.

[80] L.E.Dickson: A new simple theory of the hypercomplex integers, Journal de Math. Pures et Appliquées (1923) 281-326

[81] Leonard Eugene Dickson: Algebras and their arithmetics, Univ. Chicago Press 1923.

[82] Jean Dieudonné: Les déterminants sur un corps non-commutatif, Bull. Soc. Math. France 71 (1943) 27-45.

[83] A.C.Dixon: On the Newtonian potential, The Quarterly journal of pure and applied mathematics 35 (1903-1904) 283-296.

[84] D. Z. Djoković: Real homogeneous algebras, Proc. Amer. Math. Soc. 41 (1973) 457-462.

[85] D.P.Dobkin: On the complexity of a class of arithmetic computations, PhD thesis, Harvard 1973.

[86] D.P. Dobkin & J. Van Leeuwen: The complexity of vector products, Info. Proc. Lett. 4,6 (1976) 149-154.

[87] Albrecht Dold: Lectures on algebraic topology, Springer (GMW #200) 2nd ed. 1980.

[88] Stepthen Doro: Simple Moufang loops, Math'l. Proc. Cambridge Philos. Soc. 83 (1978) 377-392.

[89] V.S. Drensky: A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0, Algebra & Logic 20 (1981) 188-194.

[90] Arthur A. Drisko: Loops with transitive automorphisms, J.Algebra 184,1 (1996) 213-229.

[91] F.J.Dyson: Quaternion determinants, Helvetica Physica Acta 45 (1972) 289-302.

[92] Paul Eakin & Avinash Sathay: On automorphisms and derivations of Cayley-Dickson algebras, J.Algebra 129 (1990) 263-278.

[93] Paul Eakin & Avinash Sathay: Yiu's conjecture on the Cayley-Dickson algebras, unpublished manuscript (1989) Dept. of Math. Univ. of Kentucky, Lexington KY 40506.

[94] H-D. Ebbinghaus & 7 others: Numbers, Springer-Verlag 1991.

[95] B.Eckmann: Stetige Lösungen linearer Gleichungssysteme, Comment. Math. Helvetica 15 (1942/3) 318-339; there is also an addendum by G.W.Whitehead: Note on cross sections in Stiefel manifolds, Comment. Math. Helv. 37 (1963) 239-240.

[96] Beno Eckmann: Cohomologie et classès caractéristiques, Cours CIME 1966.

[97] Beno Eckmann: Continuous solutions of linear equations, Expositiones Mathematicae 9 (1991) 351-365.

[98] Beno Eckmann: Topology, Algebra, Analysis – Relations and missing links, Notices AMS 46,5 (May 1999) 520-527.

[99] I.A.Eganova & M.I.Shirikov: Orthomatrices and octonions, Reports Math'l Physics 20,1 (1984) 1-10.

[100] S.Eilenberg & I.Niven: The "fundamental theorem of algebra" for quaternions, Bull. Amer. Math. Soc. 50 (1944) 246-248.

[101] A.Elduque: Third power associative composition algebras, Manuscripta Math. 84,1 (1994) 73-87.

[102] Trevor Evans & B.H. Neumann: On varieties of groupoids and loops, J.London Math'l. Soc. 28 (1953) 342-350.

[103] John A. Ewell: On sums of sixteen squares, Rocky Mountain Math. J. 17,2 (1987) 295-299.

[104] Ference Fenyves: Extra loops I: Publicationes Mathematicae Debrecen 15 (1968) 235-238.

[105] Ference Fenyves: Extra loops II: Publicationes Mathematicae Debrecen 16 (1969) 187-192.

[106] Charles M. Fiduccia: On the Algebraic Complexity of Matrix Multiplication, Ph.D. thesis, Engineering dept. Brown University, June 1973.

[107] V.T. Fillipov: On the varieties of Mal'tcev algebras, Algebra & Logic 20 (1981) 200-210.

[108] T.Foguel, M.K.Kinyon, J.D.Phillips: On twisted subgroups and Bol loops of odd order, submitted Rocky Mountain Math. J.

[109] Hans Freudenthal: Zur ebenen Oktavengeometrie, Proc. Konink. Nederl. Akad. Wetensch. A56 (1953) 195-200 = Indag. Math. 15 (1953) 195-200.

[110] Hans Freudenthal: Oktaven, Ausnahmegruppen, und Oktavengeometrie, Geometriae Dedicata 19 (1985) 1-63.

[111] R.Fueter & E.Bareiss: Functions of a hyper complex variable, v+318 pages. Manuscipt reproduced by Argonne National Labs with permission of Univ. of Zurich Switzerland, 1948/49. Lectures by Rudolf Fueter, written and supplemented by Erwin Bareiss, approved by Fueter, typed by Wilfred Bauert. [I have never seen this. Probably some versions of it are available in Argonne and Zurich libraries.] I have also seen cited "Funktionentheorie im Hyperkomplexen," 318 pages, Mathematisches Institut der Universität Zürich 1949, which is probably a German version of the same thing. Quaternionic analysis papers by Fueter (all in German) include: Comment.Math.Helv. 4 (1932) 9-20, 6 (1933/4) 199-222, 7 (1934-5) 307-330, 8 (1935-6) 371-378, 9 (1936) 320-334; Elemente der Math. III 5 (1948) 89-94; and Über Vierfachperiodische Funktionen, Monatschefte Math. und Phys. 48 (1939) 161-169.

[112] G.Glauberman: On loops of odd order I: J.Algebra 1 (1964) 374-396; II: J.Algebra 8 (1968) 393-414.

[113] G. Golub & C. Van Loan: Matrix computations, Jonhns Hopkins Univ. Press.

[114] E.G. Goodaire, E. Jespers, C. Polcino Milies: Alternative loop rings, Elsevier 1996. QA252.GE5 QA174.2.G66

[115] E.G.Goodaire & D.A. Robinson: A class of loops isomorphic to all loop isotopes, Canad. J. Math. 34,3 (1982) 662-672.

[116] E.G.Goodaire & D.A. Robinson: Some special conjugacy-closed loops, Canad. Math. Bull. 33,1 (1990) 73-78.

[117] J. J. Gray, Olinde Rodrigues' paper of 1840 on transformation groups, Arch. Hist. Exact Sci. 21,4 (1979/80) 375-385.

[118] A.Griewank & J.F.Corliss (eds.): Automatic differentiation of algorithms, Theory Implementation and Applications, SIAM 1991.

[119] Alexander N. Grishkov & Andrei V. Zavarnitsine: Lagrange's Theorem for Moufang loops, Math'l. Proc. Cambridge Philos. Soc., accepted, 2004.

[120] V.Guillemin & A. Pollack: Differential topology, Prentice-Hall 1974.

[121] Feza Gürsey & Chia-Hsiung Tze: On the role of division, Jordan, and related algebras in particle physics, World Scientific 1996.

[122] H.Haefeli: Hyperkomplexe Differentiale, Comment. Math. Helvetica 7 (1935) 307-330.

[123] Joan Hart & Kenneth Kunen: Single axioms for odd exponent groups, J.Automated Reasoning 14 (1995) 383-412.

[124] Allen Hatcher: Algebraic Topology, Planned 3-volume work; vol 1 has been published by Cambridge University Press; vol 2 is partially done and is available from `http://www.math.cornell.edu/~hatcher/`.

[125] I.R.Hentzel & L.Peresi: Identities of Cayley-Dickson algebras, J.Algebra 188,1 (1997) 292-309.

[126] I.R.Hentzel & L.Peresi: Degree 3, 4, and 5 identities of quadratic algebras, J.Algebra 206 (1998) 1-16.

[127] J.E.Hopcroft & L.R.Kerr: On the number of multiplications necessary for matrix multiplication, SIAM J Appl Math 20,1 (1971) 30-36.

[128] J.E.Hopcroft & J.Musinski: Duality applied to the complexity of matrix multiplication and other bilinear forms, SIAM J Comput 2,3 (1973) 159-173.

[129] H.Hopf: Über die Abbildungen von Sphären auf Sphären niedrigere Dimension, Fundamenta Mathematicae 25 (1935) 427-440.

[130] Heinz Hopf: Ein topologisches Beitrag zur reellen Algebra, Commentarii Mathematici Helvetici 13 (1940/41) 219-239

[131] Roger A. Horn & Charles A. Johnson: Matrix analysis, Cambridge University Press 1985.

[132] Thomas D. Howell & Jean-Claude Lafon: The complexity of the quaternion product, Cornell dept. computer science TR 75-245 (June 1975); available online at `http://home.pipeline.com/~hbaker/quaternion/cornellcstr75-245.dvi.gz`.

[133] Sze-Tsen Hu: Homotopy theory, Academic Press 1959.

[134] Adolf Hurwitz: Über die Komposition der quadratischen Formen von beliebig vielen Variabeln, Nachrichten von den Königlichen Gesellschaft der Wissenschaften in Göttingen, Math.-Phys. Klasse (1898) 309-316 [Math. Werke II, 565-571].

[135] Adolf Hurwitz: Über die Komposition der quadratischen Formen, Mathematische Annalen 88 (1923) 1-25 (published posthumously).

[136] K. Imaeda & M.Imaeda: Sedenions, algebra and analysis, Appl. Math. & Computation 115,2-3 (2000) 77-88.

[137] K. Imaeda: A new form of classical electrodynamics, Il Nuovo Cimento 32,1 (1976) 138-162.

[138] K.Imaeda & M.Imaeda: The theory of functions of an octonion variable, The Bulletin of the Okayama Univ.of Science 19A (1984) 93-; 20A (1985) 133-. (I have been unable to obtain a copy of this.)

[139] K.Imaeda, H.Tachibana, M.Imaeda, S.Ohta: Solutions of the octonionic wave equation and the theory of functions of an octonion variable, Il Nuovo Cimento 100B,1 (1987) 53-71.

[140] T.Iwaniec, G.Martin: The Liouville theorem, pp.339-361 in *Analysis and Topology*, World Scientific 1998.

[141] N.Jacobson: Composition algebras and their automorphisms, Rendiconti del circolo matematico di Palermo, ser 2, vol 7 (1958) 55-80.

[142] N.Jacobson: Basic Algebra (2 vols), Freeman 1985.

[143] N.Jacobson: Structure and representations of Jordan algebras, American Mathematical Society (Colloquium pub #39) 1968.

[144] N.Jacobson: Lie algebras, Dover 1979.

[145] D.Joyner, R.Kreminski, J.Turisco: Applied abstract algebra, Johns Hopkins Univ. Press 2003.

[146] Valentine Kabanets & Russell Impagliazzo: Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds, Technical Report TR02-055, Electronic Colloquium on Computational Complexity. and ACM Sympos. Theoretical Computer Sci. 35 (2003) 355-364.

[147] I.L. Kantor & A.S. Solodovnikov: Hypercomplex numbers, An elementary introduction to algebras, Springer-Verlag 1989.

[148] Irving Kaplansky: Infinite-dimensional quadratic forms admitting composition, Proc. Amer. Math. Soc. 4 (1954) 956-960.

[149] Sailah H. Khalil & Paul Yiu: The Cayley-Dickson algebras, a theorem of Hurwitz, and quaternions, Bulletin de la société des sciences et des lettres de Łódź, vol. XLVII [Série: Recherches sur les Déformations, vol. XXIV] (1997) 117-169 (entire issue). References Y1, Y2, and SY are missing from this paper.

[150] M.K.Kinyon, K.Kunen, J.D.Phillips: Diassociativity in conjugacy-closed loops, Communications in Algebra 32 (2004) 767-787.

[151] M.K.Kinyon, K.Kunen, J.D.Phillips: Every diassociative A-loop is Moufang, Proc. Amer. Math. Soc. 130 (2002) 619-624.

[152] M.K.Kinyon, K.Kunen, J.D.Phillips: A generalization of Moufang and Steiner loops,Algebra Universalis 48,1 (2002) 81-101.

[153] Thomas P. Kirkman: On a problem in combinations, Cambridge & Dublin Math'l Journal 2 (1847) 191-204.

[154] Thomas P. Kirkman: On pluquaternions and the homoid products of sums of n squares, The London, Edinburgh & Dublin PHILOSOPHICAL MAGAZINE and JOURNAL OF SCIENCE, 3rd ser. 33 (July-Dec 1848) 447-459 & 494-509.

[155] Th.P. Kirkman: On bisignal univalent imaginaries, Philosophical Magazine (ser. 3) 37 (1850) 292-301.

[156] Th.P.Kirkman: On the triads made with fifteen things, Philos. Mag. (ser. 3) 37 (1985) 169-171.

[157] Th.P. Kirkman: On the problem of the fifteen young ladies, Philosophical Magazine (ser. 4) 23 (1862) 199-204.

[158] B.W.Kernighan & D.M.Ritchie: The C programming language, 2nd edition – ANSI C, Prentice Hall 1988.

[159] K.Kunen: Alternative loop rings, Commun. Algebra 26 (1998) 557-564.

[160] K.Kunen: Moufang quasigroups, J.Algebra 183 (1996) 231-234.

[161] Kenneth Kunen: The structure of conjugacy-closed loops, Trans. Amer. Math. Soc. 352 (2000) 2889-2991.

[162] K.Kunen: Quasigroups, loops, and associative laws, J Algebra 185 (1996) 194-204.

[163] Kee Yuen Lam & Paul Yiu: Beyond the impossibility fo a 16-square identity, pp. 137-163 in *Five decades as a mathematician and educator*, World Scientific 1995, MR 97g:11040.

[164] C.Lanczos: PhD dissertation "The functional theoretical relationships of the Maxwell Aether equations," University of Szeged, Budapest, Hungary 1919. Reprinted (in handwritten German, author name written as "Kornel Laewy (Lánczos)") pages A1-A82 volume VI of "C.Lanczos, collected published papers with commentaries," North Carolina State Univ. 1998. See also commentaries pages 2-15 to 2-23 and xl-xli in volume I.

[165] Martin W. Liebeck: The classification of simple Moufang loops, Math. Proc. Cambridge Philos. Soc. 102,1 (1987) 33-47.

[166] J.Liouville's theorem that the conformal maps in dimension≥ 3 are precisely the compositions of spherical inversions $\vec{x} \to \vec{x}/|\vec{x}|^2$, translations, scalings, and orthogonal linear transformations, was apparently first published as appendix 6, pp. 609-616, in the 5th edition of G.Monge's book *Application de l'analyse á la gèomètrie*, Bachelier 1850. Liouville, who was the editor of this book, inserted this as one of 7 added notes at the end. Liouville also described his result, but without proof, in a 1-page note "Théorème sur l'equation $\mathrm{d}x^2 + \mathrm{d}y^2 + \mathrm{d}z^2 = \lambda(\mathrm{d}\alpha^2 + d\beta^2 + d\gamma^2)$," J. Math. Pures et Appl. 15 (1850) 103. Modern re-treatments: P.Hartman: On isometries and a theorem of Liouville, Mathematische Zeitschrift 69 (1958) 202-210; R.Nevanlinna: pp. 3-9 in his book *Analytic functions*, Princeton University Press 1960; M.Berger, section 9.5.4 in his book *Geometry I*, Springer 1987. Strengthenings of this theorem, which now only assume that the map has a derivative in a local Sobolev-norm sense (and that this Jacobian must be a scaled orthogonal matrix when it exists), include [216][35][140].

[167] Eugene K. Loginov: Simple Bol loops, submitted Math'l Proc. Cambridge Philos. Soc. 2003.

[168] E.K.Loginov: Analytic loops and gauge fields, Nuclear Physics B 606 (2001) 636-646.

[169] Corinne A. Manogue & Jörg Schray: Finite Lorentz transformations, automorphisms, and division algebras, J.Math'l.Phys. 34 (1993) 3746-3767.

[170] R.A.Mathon, K.T.Phelps, A. Rosa: Small Steiner triple systems and their properties, Ars Combinatorica 15 (1983) 3-110.

[171] James Clerk Maxwell: Treatise on Electricity and Magnetism (1873), available as Dover reprint.

[172] K. McCrimmon: Generically algebraic algebras, Trans. AMS 127 (1967) 527-551.

[173] K. McCrimmon: Norms and noncommutative Jordan algebras, Pacific J. Math. 15,3 (1965) 925-956.

[174] W.McCune: Son of Bird Brain (automated deduction system) http://www-unix.mcs.anl.gov/AR/sobb/.

[175] William W. McCune: Mace 2.0 reference manual and guide, cs.SC/0106042

[176] William W. McCune: Otter 3.3 reference manual, cs.SC/0310056

[177] W.W. McCune & R.Padmanhabhan: Automated deduction in equational logic and cubic curves, Springer 1996 (LNCS#1095).

[178] J.W.Milnor: Topology from the differentiable viewpoint, Univ. Virginia Press, Charlottesville VA 1965.

[179] P.J.Morandi: Lie algebras, composition algebras, and the existences of vector cross products on finite dimensional vector spaces, Exposition Math. 17,1 (1999) 63-73.

[180] R.Moufang: Die Desarguesschen Sätze vom Rang 10, Mathematische Annalen 108 (1933) 296-310.

[181] Ruth Moufang: Zur struktur von Alternativkörpern, Math. Annalen 110 (1934/5) 416-430.

[182] Hyo Chul Myung: Malcev admissible algebras, Birkhauser Boston 1986 (Progress in Math. #64).

[183] G.P.Nagy & P.Vojtechovsky: Octonions and simple Moufang Loops, Quasigroups & related systems 10 (2003) 65-94.

[184] José I. Nieto: Normed right alternative algebras over the reals, Canadian J. Math. 24,6 (1972) 1183-1186.

[185] Ivan Niven: Equations in Quaternions, Amer. Math. Monthly 48 (1941) 654-661.

[186] Ivan Niven: The roots of a quaternion, Amer. Math. Monthly 49 (1942) 386-388; Addendum by Louis Brand: 519-520.

[187] A.M.Odlyzko: Lower bounds for discriminants of number fields, Acta Arithmetica 29,3 (1976) 275-297.

[188] *Olinde Rodrigues and His Circle: Mathematics and Social Utopia*, Proceedings of conference (London, Dec. 2001), editor Eduardo Ortiz (e.ortiz@ic.ac.uk). Not yet published.

[189] Susumu Okubo: Introduction to Octonion and other nonassociative algebras in physics, Cambridge Univ. Press 1995 (Montroll memorial lectures #2).

[190] J.Marshall Osborn: Loops with the weak inverse property, Pacific J. Math. 10 (1960) 295-304.

[191] J.Marshall Osborn: Quadratic division algebras, Trans.Amer.Math.Soc. 105 (1962) 202-221.

[192] Lowell J. Paige: A class of simple Moufang loops, Proc. Amer. Math. Soc. 7,3 (1956) 471-482.

[193] R.Penney: Octonions and the Dirac equation, Amer. J. Phys. 36 (1968) 871-873; Octonions and isospin, Nuovo Cimento B 3 (1971) 95-113.

[194] Marko Petkovsek, Herb Wilf, and Doron Zeilberger: $A = B$, A.K. Peters 1996.

[195] A.Pfister: Zur Darstellung von -1 als Summe von Quadraten in einem Körper, J. London Math. Soc. 40 (1965) 159-165.

[196] A.Pfister: Quadratische Formen in beliebigen Körper, Inventiones Math. 1 (1966) 116-132.

[197] A.Pfister: Zur Darstellung definiter Funktionen als Summe von Quadraten, Inventiones Math. 4 (1967) 229-237.

[198] A. Pfister: Hilbert's 17th Problem and related problems in definite forms, pp. 483-490 in volume 2 of *Mathematical Developments Arising from Hilbert Problems*, AMS Proc. Sympos. Pure Math. 28 (1976).

[199] Albrecht Pfister: Quadratic Forms with Applications to Algebraic Geometry and Topology, (London Math. Soc. Lecture Notes #217) Cambridge Univ. Press 1995.

[200] Hala Orlik-Pflugfelder: Quasigroups and loops, introduction, Heldermann Verlag (Berlin) 1990; sigma series in pure math. #7.

[201] Hala Orlik-Pflugfelder: A special class of Moufang loops, Proc.Amer.Math.Soc. 26 (1970) 583-586.

[202] A.Philips, R.Lubotsky, P. Sarnak: Ramanujan graphs, Combinatorica 8,3 (1988) 261-277.

[203] Private communication from J.D.Phillips, Wabash University math dept.

[204] J.D.Phillips & Petr Vojtechovsky: The varieties of loops of Bol-Moufang type: submitted Algebra Universalis.

[205] J.D.Phillips & Petr Vojtechovsky: The varieties of quasigroups of Bol-Moufang type: an equational reasoning approach, submitted J.Algebra.

[206] R.S. Pierce: Associative algebras, Springer (GTM #88) 1982.

[207] Barth Pollak: The equation $\bar{t}at = b$ in a quaternion algebra, Duke Math. J. 27 (1960) 261-271.

[208] G. Baley Price: An Introduction to Multicomplex Spaces and Functions, Marcel-Dekker, New York, 1991.

[209] Michel L. Racine: Minimal identities of octonion algebras, J.Algebra 115 (1988) 251-260.

[210] J.Radon: Lineare Scharen orthogonaler Matrizen, Abhandlung. Math. Sem. Universität Hamburg 1 (1922) 1-14.

[211] A.R.Rajwade: Squares, Cambridge Univ. Press (London Math. Soc. Lecture Notes #171) 1993.

[212] V.S.Ramamurthi & B.L.Sharma: A class of non-Moufang Bol loops isomorphic to all their loop isotopes, Aeq. Math. 29,2-3 (1985) 132-134.

[213] Yu.P.Razmyslov: The existence of a finite basis for the identities of the matrix algebra of order two over a field of characteristic zero, Algebra & Logic 12 (1973) 47-63.

[214] R.Remmart: Theory of Complex Functions, Springer-Verlag 1991.

[215] J. Renegar: On the computational complexity and geometry of the first order theory of the reals, J. Symbolic Comput. 13,3 (1992) 255-352.

[216] Ju. G. Resetnjak: Liouville's conformal mapping theorem under minimal regularity hypotheses, Sibersk Mat. Z. 8 (1967) 835-840; MR36#1630. Stability estimates in the class W_p^1 in Liouville's conformal mapping theorem for a closed domain, Sibersk Mat. Z. 17,6 (1976) 1382-1394, 1439; English translation in Siberian Math. J. 17,6 (1976/7) 1009-1018. Resetnjak also has papers indicating that n-dimensional mappings ($n \geq 3$) that are *close* to conformal (in certain normed senses) must be close to being Mobius transformations, e.g. see Siberian Math.J. 11 (1970) 833-846 and 17,4 (1976) 673-674.

[217] D.A.Robinson: Bol loops, Trans.Amer.Math.Society 123 (1966) 341-354.

[218] D.A.Robinson: A Bol group isomorphic to all loop isotopes, Proc. Amer. Math. Soc. 19 (1968) 671-672.

[219] Olinde Rodrigrues: Des lois géométriques qui régissent les déplacemaents d'un système solide dans l'espace, et la variation des coordonees proventant de ses déplacements considérés indépendamment des causes qui peuvent les produire, J.de Math. Pures et Appliquees 5 (1840) 380-440.

[220] R.É. Roomel'di: Solvability of $(-1,1)$ nil rings, Algebra & Logic 25 (1986) 380-387.

[221] A.Rose: On the use of a complex (quaternion) velocity potential in three dimensions, Comment. Math. Helvet. 24 (1950) 135-148.

[222] S.Rosset: A new proof of the Amitsur-Levitski identity, Israel J. Math. 23,2 (1976) 187-188.

[223] A. A. Sagle: Mal'cev algebras, Trans. Amer. Math. Soc. 101 (1961) 426-458.

[224] Arthur A. Sagle: Simple Mal'cev algebras over fields of characteristic 0, Pacific J. Math. 12,3 (1962) 1057-1078.

[225] R.D. Schafer: An introduction to nonassociative algebras, Academic Press 1966; reprinted by Dover.

[226] R.D. Schafer: On the algebras formed by the Cayley-Dickson process, Amer. J. Math. 76 (1954) 435-446.

[227] R.D. Schafer: On forms of degree n permitting composition, J.Math. Mech. 12 (1963) 777-792.

[228] R.D. Schafer: Forms permitting composition, Adv. Math. 4 (1970) 127-148.

[229] J.T.Schwartz: Fast probabilistic algorithms for verification of polynomial identities, J. ACM 27,4 (1980) 701-717.

[230] Corrado Segre: La Rappresentazioni Reali delle Forme Complesse e Gli Enti Iperalgebrici, Math. Annalen 40 (1892) 413-467.

[231] D.B.Shapiro: Compositions of quadratic forms, W. de Gruyter Verlag 2000.

[232] D.B.Shapiro: Products of Sums and Squares, Exposit. Math. 2 (1984) 235-261.

[233] L.A.Skornjakov: Alternative rings, Rendiconti L. Mat. e Appl. (5) 24 (1965) 360-372???

[234] Tara L. Smith & Paul Yiu: Constructions of sums of squares formulae integer coefficients, Boletin de la Sociedad Matematica Mexicana (2) 37, 1-2 (1992) 479-495.

[235] Jonathan D.H.Smith: A left-loop on the 15-sphere, J.Algebra 176 (1995) 128-138.

[236] Warren D. Smith: New theorems in vector calculus, `http://math.temple.edu/~wds/homepage/works.html`.

[237] Warren D. Smith: Reasons the photon is massless, `http://math.temple.edu/~wds/homepage/works.html`.

[238] A.R.T. Solarin & V.O. Chibova: A note on G-loops, Zb.Rad. (Kragujevac) 17 (1995) 17-26; MR 96k:20153. Contains incorrect result.

[239] E.Spanier: Algebraic topology, Springer 1966.

[240] Volker Strassen: Gaussian elimination is not optimal, Numerische Mathematik 13,4 (1969) 354-356.

[241] Eduard Study: Theorie der linearen Gleichungen, Acta Math. 42 (1920) 1-61.

[242] A.Sudbery: Quaternionic Analysis, Math'l Proc. Cambridge Philosophical Soc. 85,2 (1979) 199-225.

[243] Olga Taussky: A determinantal identity for quaternions and a new eight square identity, J. of Math'l Analysis & Applics. 15 (1966) 162-164.

[244] Yongge Tian: Matrix representations of octonions and their applications, Adv. Applied Clifford Algebras 10,1 (2000) 67-91. [Unfortunately mispaginated and truncated.]

[245] S.Yu.Vasilovskii: A basis of the identities of the simple three dimensional Lie algebra over an infinite field, Algebra & Logic 28 (1989) 355-368.

[246] Jan Vrbik: Dirac equation and Clifford algebra, J. Math'l. Phys. 35,5 (1994) 2309-2314.

[247] Jan Vrbik: Celestial mechanics via quaternions, Canad. J. Phys. 72 (1994) 141-146.

[248] Jan Vrbik: Perturbed Kepler problem in quaternionic form, J.Phys. A 28 (1995) 193-198.

[249] Jan Vrbik: Simple simulation of solar system, Astrophysics & Space Science 266,4 (1999) 557-567.

[250] Jan Vrbik: Iterative solution to perturbed Kepler problem via Kustaanheimo-Stiefel equation, Celestial Mechanics & Dynamical Astronomy 71 (1999) 273-287.

[251] Jan Vrbik: New methods of celestial mechanics, 2000 book manuscript `http://spartan.ac.brocku.ca/~jvrbik/RESEARCH`.

[252] B.L.van der Waerden: Algebra (2 vols) [older editions had been titled "Modern Algebra"] Springer 1991.

[253] Hugh E. Warren: Partitions by algebraic varieties, Bulletin of the Amer. Math'l. Soc. 73 (1967) 192-194.

[254] E.Weisstein: The Guddermannian (article in his online encyclopedia of mathematics) `http://mathworld.wolfram.com/GudermannianFunction.html`.

[255] E.T. Whittaker, G.N. Watson: A course of modern analysis, Cambridge Univ. Press (one recent edition is 1986).

[256] Eric L. Wilson: A class of loops with the isotopy-isomorphy property, Canad. J. Math. 18 (1966) 589-592.

[257] Hans Zassenhaus & Wolfgang Eichhorn: Herleitung von Acht- und Sechzehn-Quadrate-Identitäten mit Hilfe von Eigenschaften der verallgemeinerten Quaternionen und der Cayley-Dicksonschen Zahlen, Archiv der Mathematik 17 (1966) 492-496.

[258] Fuzhen Zhang: Quaternions and Matrices of Quaternions, Linear Algebra & its Applications 251, 1-3 (1997) 21-57.

[259] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov, A.I. Shirshov: Rings that are nearly associative, Academic Press 1982.

[260] R.Zippel: Probabilistic algorithms for sparse polynomials, EUROSAM '79, Springer (Lecture Notes in CS#72) 216-226;

[261] R.Zippel: Zero testing of algebraic functions, Info. Proc. Lett. 61,2 (1997) 63-67.

[262] Max Zorn: Theorie der Alternativen Ringe, Abh. Math. Seminar Hamburg 8 (1930) 123-147.

[263] Max Zorn: Alternativkörper und quadratische Systeme, Abh. Math. Seminar Hamburg 9 (1933) 395-402.

[264] M. Zorn: The automorphisms of Cayley's non-associative algebra, Proc. Nat'l Acad. Sci. USA 21 (1935) 355-358.

[265] P.Zvengrowski: A 3-fold vector product in $\mathbb{R}^8$, Comm. Math. Helv. 40 (1965/6) 149-152.