

AN OCTONION ALGEBRA ORIGINATING IN COMBINATORICS

DRAGOMIR Ž. ĐOKOVIĆ AND KAIMING ZHAO

(Communicated by Birge Huisgen-Zimmermann)

ABSTRACT. C.H. Yang discovered a polynomial version of the classical Lagrange identity expressing the product of two sums of four squares as another sum of four squares. He used it to give short proofs of some important theorems on composition of δ -codes (now known as T -sequences). We investigate the possible new versions of his polynomial Lagrange identity. Our main result shows that all such identities are equivalent to each other.

1. INTRODUCTION

C.H. Yang [7, 8, 9] discovered a polynomial version (see below) of the classical Lagrange identity on the product of two sums of four squares. He used his identity to give short and elegant proofs of some important theorems [9] in combinatorics of binary and ternary sequences. These results provide new methods for the construction of several classes of combinatorial objects such as T -sequences, orthogonal designs, and Hadamard matrices [5, 9]. Our motivation and the main goal was to investigate the possible new versions of the polynomial Lagrange identity. However, our main result shows that all such identities are equivalent to each other (for the precise statement, see Theorem 4.1).

Let $A = \mathbf{Z}[z, z^{-1}]$ be the Laurent polynomial ring over the integers \mathbf{Z} . For any $f = f(z) = \sum_k a_k z^k \in A$, $a_k \in \mathbf{Z}$, we define its *conjugate* as $f^* = f(z^{-1})$. We also say that a_0 is the *constant term* of f and write $\text{CT}(f) = a_0$. Note that $\text{CT}(ff^*) = \sum_k a_k^2$. Let A_0 be the fixed subring of A under the conjugation, i.e., $A_0 = \{f \in A \mid f = f^*\}$. It is easy to see that $A_0 = \mathbf{Z}[z + z^{-1}]$. We embed the polynomial ring $\mathbf{Z}[t]$ into A by sending $t \rightarrow z + z^{-1}$ and view A as a $\mathbf{Z}[t]$ -algebra. It is easy to check that $A = A_0 \oplus A_0 z$. Thus A is a free $\mathbf{Z}[t]$ -module of rank 2.

We are mainly interested in the free A -module $E = A^4$. When viewed as a $\mathbf{Z}[t]$ -module it is again free but now its rank is 8. For any $x = (x_0, x_1, x_2, x_3) \in E$ we define its *norm* as $N(x) = \sum_k x_k x_k^*$. Thus $N : E \rightarrow A_0$ is a quadratic form on the A_0 -module E .

Received by the editors May 12, 2009 and, in revised form, September 21, 2009 and February 13, 2010.

2010 *Mathematics Subject Classification*. Primary 17A75, 05B20, 05B30.

Key words and phrases. Laurent polynomial ring, polynomial Lagrange identity, octonion algebra, composition algebra.

The first author was supported by an NSERC Discovery Grant.

The second author was supported by the NSERC and the NSF of China (Grant 10871192).

©2010 American Mathematical Society
Reverts to public domain 28 years from publication

Now we state the Lagrange identity for Laurent polynomials (modified Theorem 1 in [9]). Let $x = (x_k)$, $y = (y_k) \in E$ and define $(p, q, r, s) \in E$ by *Yang's formulae*:

$$\begin{aligned} p &= x_0y_0 - x_1y_1^* - x_2y_2^* - x_3y_3^*, \\ q &= x_0y_1 + x_1y_0^* + x_2y_3^* - x_3y_2^*, \\ r &= x_0y_2 - x_1y_3^* + x_2y_0^* + x_3y_1^*, \\ s &= x_0y_3 + x_1y_2^* - x_2y_1^* + x_3y_0^*. \end{aligned}$$

We can use these formulae to define an A_0 -bilinear multiplication “ \circ ” on E by $x \circ y = (p, q, r, s)$. It is straightforward to verify that the Lagrange identity $N(x \circ y) = N(x)N(y)$ is indeed valid.

We shall see in the next section that (E, \circ) is in fact an octonion algebra over $\mathbf{Z}[t]$. In Section 3 we give an explicit description of the orthogonal group $O(N)$ of the pair (E, N) ; see Theorem 3.4. In Section 4, we show that all A_0 -bilinear multiplications on E satisfying the Lagrange identity are equivalent, in the sense defined there, to the above multiplication “ \circ ”.

Our main result can probably be generalized by replacing \mathbf{Z} with a more general commutative ring. We decided not to pursue this here in order to preserve the essentially combinatorial flavor of the original problem.

We are grateful to the referee for correcting a couple of errors in the original proof of Lemma 4.3, for giving the stronger result in Theorem 4.3, and for other detailed comments and suggestions. Actually most of the proofs have been improved by the referee.

2. YANG FORMULAE DEFINE AN OCTONION ALGEBRA

We make $A = \mathbf{Z}[z, z^{-1}]$ into a $\mathbf{Z}[t]$ -algebra via the homomorphism $\mathbf{Z}[t] \rightarrow A$ sending $t \rightarrow z + z^{-1}$. We shall often identify $\mathbf{Z}[t]$ with its image A_0 under this homomorphism. According to the definition in [1, Chapter III, §2], A is a quadratic $\mathbf{Z}[t]$ -algebra. By using the basis $\{1, z\}$, we see that its type is $(-1, t)$. Indeed we have $z^2 = -1 + tz$. Moreover, $(A, *)$ is an example of a Cayley algebra (see [1]).

Let $H = A \times A$, a free A -module of rank 2. We shall also view it as a free $\mathbf{Z}[t]$ -module of rank 4 with basis $(1, 0)$, $(z, 0)$, $(0, 1)$, $(0, z)$. We make H into an associative noncommutative algebra by using the Cayley–Dickson process; i.e., we define the multiplication in H by

$$(a, b)(c, d) = (ac - d^*b, bc^* + da), \quad a, b, c, d \in A.$$

The involution “ $*$ ” on A extends to an involutory anti-automorphism of H by setting

$$(a, b)^* = (a^*, -b), \quad a, b \in A.$$

Thus H is an example of a quaternion algebra over $\mathbf{Z}[t]$; see [1], No. 5, Example 2. As such, it has type $(-1, t, -1)$.

Let $E = H \times H$, a free A -module of rank 4. We shall also view it as a free $\mathbf{Z}[t]$ -module of rank 8 with basis

$$\begin{aligned} e_0 &= (1, 0, 0, 0), & e'_0 &= ze_0 = (z, 0, 0, 0), \\ e_1 &= (0, 1, 0, 0), & e'_1 &= ze_1 = (0, z, 0, 0), \\ e_2 &= (0, 0, 1, 0), & e'_2 &= ze_2 = (0, 0, z, 0), \\ e_3 &= (0, 0, 0, 1), & e'_3 &= ze_3 = (0, 0, 0, z). \end{aligned}$$

We make E into a nonassociative algebra by using the Cayley–Dickson process once more. Thus, we define the multiplication in E by

$$(u, v)(x, y) = (ux - y^*v, vx^* + yu), \quad u, v, x, y \in H.$$

The involution “ $*$ ” on H extends to one on E by setting

$$(u, v)^* = (u^*, -v), \quad u, v \in H.$$

Thus E is an example of an octonion algebra over $\mathbf{Z}[t]$; see [1, Chapter III, Appendix]. By using the above basis, we find that the type of this octonion algebra is $(-1, t, -1, -1)$.

Let us write the above octonion multiplication in terms of the A -basis $\{e_0, e_1, e_2, e_3\}$. For $x = (x_0, x_1, x_2, x_3)$ and $y = (y_0, y_1, y_2, y_3)$, we find that

$$\begin{aligned} xy &= (x_0y_0 - x_1y_1^* - x_2y_2^* - x_3y_3^*, \\ &\quad x_0y_1 + x_1y_0^* + x_2^*y_3 - x_3y_2^*, \\ &\quad x_0y_2 - x_1^*y_3 + x_2y_0^* + x_3y_1^*, \\ &\quad x_0^*y_3 + x_1y_2 - x_2y_1 + x_3y_0). \end{aligned}$$

Hence, the map sending $(x_0, x_1, x_2, x_3) \rightarrow (x_0, x_1, x_2, x_3^*)$ is an isomorphism of this octonion algebra with the algebra (E, \circ) defined by the Yang formulae.

3. ORTHOGONAL GROUP

It is obvious that $U_1 = \{x \in A \mid xx^* = 1\}$ is the group of invertible elements of A . It consists of the elements $\pm z^k, k \in \mathbf{Z}$. In our proofs below we shall often use the following obvious fact: The subset U_1 generates A as an additive group.

The ring homomorphisms $\varphi : A \rightarrow \mathbf{C}$ are parametrized by nonzero complex numbers w . By definition, the homomorphism φ_w corresponding to w sends the indeterminate z to w . The homomorphism φ_w is compatible with the involutions (conjugation on A and complex conjugation on \mathbf{C}); i.e., $\varphi_w(x^*) = \overline{\varphi_w(x)}$ for all $x \in A$ if and only if $|w| = 1$.

The following lemma will be used in the next section.

Lemma 3.1. *If $m \in \mathbf{Z}$ is not a square, then the equation $xx^* = m$ has no solution in A .*

Proof. Assume that $ff^* = m$ for some $f \in A$. By applying the homomorphism φ_1 we obtain $f(1)f^*(1) = m$. As $f^*(1) = f(1) \in \mathbf{Z}$, we have a contradiction. \square

We also remark that, for $x \in A$, $\text{CT}(xx^*) = 0$ implies $x = 0$, and $\text{CT}(xx^*) = 1$ implies $xx^* = 1$.

Denote the general linear group of the A_0 -module E by $\text{GL}(A_0, E)$. We introduce the orthogonal groups

$$\begin{aligned} \text{O}(N) &= \{\varphi \in \text{GL}(A_0, E) \mid N(\varphi(u)) = N(u), \forall u \in E\}, \\ \text{O}_4(\mathbf{Z}) &= \{\varphi \in \text{GL}_4(\mathbf{Z}) \mid N(\varphi(u)) = N(u), \forall u \in \mathbf{Z}^4\}, \end{aligned}$$

where \mathbf{Z}^4 is considered as an additive subgroup of $E = A^4$.

Let $Q : E \times E \rightarrow A_0$ be the polar form of N , i.e.,

$$\begin{aligned} Q(x, y) &= N(x + y) - N(x) - N(y) \\ &= \sum_{k=0}^3 (x_k^*y_k + x_ky_k^*). \end{aligned}$$

Note that Q is a symmetric A_0 -bilinear $O(N)$ -invariant form and that Q is nondegenerate; i.e., its kernel is 0.

Let us begin with a useful remark.

Remark 3.2. An A_0 -linear map $\varphi : E \rightarrow E$ preserving N is automatically bijective, and so $\varphi \in O(N)$. Indeed, as Q is nondegenerate, the injectivity is obvious. If S is the matrix of Q with respect to some A_0 -basis of E , then $\det(\varphi)^2 \det(S) = \det(S) \neq 0$, forcing $\det(\varphi) = \pm 1$, and φ is bijective.

The following result is crucial to this paper.

Theorem 3.3. (a) *The group $O_4(\mathbf{Z})$ consists of entry permutations on \mathbf{Z}^4 with arbitrary sign changes.*

(b) *The set $U'_1 = \{x \in A \mid xx^* = -(z - z^{-1})^2\}$ is equal to $(z - z^{-1})U_1$.*

(c) *The unit sphere $U_4 = \{x \in E \mid N(x) = 1\}$ is equal to $\bigcup_{k=0}^3 U_1 e_k$.*

(d) *The sphere $U'_4 = \{x \in E \mid N(x) = -(z - z^{-1})^2\}$ is equal to $(z - z^{-1})U_4$.*

Proof. (a) Fix $\alpha \in O_4(\mathbf{Z})$. Let $\alpha(e_i) = \sum_j a_{ij} e_j$, where $a_{ij} \in \mathbf{Z}$. From $1 = N(\alpha(e_i)) = \sum_j a_{ij}^2$, we see that, for each i , exactly one of a_{ij} is ± 1 and the other ones vanish. The rest follows easily.

(b) By applying the homomorphisms $\varphi_{\pm 1}$ to $xx^* = -(z - z^{-1})^2$, we conclude that x is divisible by $z - 1$ and $z + 1$, and so we have $x = (z - z^{-1})y$ for some $y \in A$. As $xx^* = -(z - z^{-1})^2 yy^*$, we deduce that $yy^* = 1$, i.e., $y \in U_1$.

(c) Suppose $x = (x_0, x_1, x_2, x_3) \in U_4$. Then $\sum_{k=0}^3 x_k x_k^* = 1$. By comparing the constant terms, we conclude that exactly one of the x_k belongs to U_1 while the others vanish.

(d) Suppose $x = (x_k) \in U'_4$. Then $\sum_k x_k x_k^* = 2 - z^2 - z^{-2}$. Hence $\sum_k \text{CT}(x_k x_k^*) = 2$, which by the above remark implies that exactly one of the x_k s is nonzero. This nonzero component belongs to $(z - z^{-1})U_1$ by (b). \square

Note that $O_4(\mathbf{Z}) = E_{16}\Sigma_4$ is the semidirect product of the elementary abelian group E_{16} of order 16 which acts on \mathbf{Z}^4 by multiplying the coordinates with ± 1 and the symmetric group Σ_4 of degree 4 which permutes the coordinates.

For $u = (u_0, u_1, u_2, u_3) \in U_1^4$ we define $\sigma_u \in O(N)$ by $\sigma_u(x) = (u_k x_k)$, where $x = (x_k) \in E$. Then

$$(3.1) \quad T = \{\sigma_u \mid u \in U_1^4\}$$

is an abelian subgroup of $O(N)$.

Any $\alpha \in O_4(\mathbf{Z})$ extends uniquely to an A -linear element of $O(N)$, still denoted by α . Thus we consider $O_4(\mathbf{Z})$ as a subgroup of $O(N)$. Define $\tau_0 \in O(N)$ by $\tau_0(x_0, x_1, x_2, x_3) = (x_0^*, x_1, x_2, x_3)$, and define similarly τ_k for $k = 1, 2, 3$. Let Γ denote the group of order 16 generated by the τ_k s. The group $O(N)$ admits the following factorization.

Theorem 3.4. $O(N) = T\Sigma_4\Gamma$.

Proof. Let $\varphi \in O(N)$. Since $\varphi(U_4) = U_4$, for any index i there exist $u_i \in U_1$ and an index i' such that $\varphi(e_i) = u_i e_{i'}$. Since the form Q is φ -invariant, the map $i \rightarrow i'$ must be a permutation of $\{0, 1, 2, 3\}$.

For any $a \in A$ we have $a + a^* \in A_0$ and so

$$\varphi((a + a^*)e_i) = (a + a^*)u_i e_{i'}.$$

Now let $a \in U_1$, $a \neq \pm 1$. Then each of the terms $\varphi(ae_i)$, $\varphi(a^*e_i)$, $au_i e_{i'}$ and $a^*u_i e_{i'}$ belongs to U_4 , and the sum of the first two terms is not 0. It follows that $\varphi(ae_i)$ is equal to $au_i e_{i'}$ or $a^*u_i e_{i'}$.

Assume that there exist $a, b \in U_1$ different from ± 1 such that $\varphi(ae_i) = au_i e_{i'}$ while $\varphi(be_i) = b^*u_i e_{i'}$. Then $\varphi((a + b)e_i) = (a + b^*)u_i e_{i'}$, and by taking the norms we obtain the contradiction $(a - a^*)(b - b^*) = 0$. Consequently, one of the two identities, $\varphi(ae_i) = au_i e_{i'}$ or $\varphi(ae_i) = a^*u_i e_{i'}$, must hold for all $a \in A$. Equivalently, there exists $\varepsilon_i \in \{0, 1\}$ such that $\varphi\tau_i^{\varepsilon_i}(ae_i) = au_i e_{i'}$ for all $a \in A$. Let

$$u = (u_i) \in U_1^4 \quad \text{and} \quad \tau = \prod_{i=0}^3 \tau_i^{\varepsilon_i} \in \Gamma.$$

The composite $\beta = \sigma_u^{-1}\varphi\tau$ is A -linear, and we have $\sigma_u^{-1}\varphi\tau(e_i) = e_{i'}$ for all i . Hence, $\varphi = \sigma_u\beta\tau$ with $\sigma_u \in T$, $\beta \in \Sigma_4$ and $\tau \in \Gamma$. □

4. COMPOSITION ALGEBRA STRUCTURES ON E

In this section we determine all A_0 -bilinear multiplications “ \cdot ” on E which satisfy the (polynomial) Lagrange identity

$$(4.1) \quad N(x \cdot y) = N(x)N(y).$$

Since E is a free A_0 -module of rank 8 and the form Q is nondegenerate, such an algebra (E, \cdot) will be a composition algebra in the sense of the definition in [3, p. 305] provided that it has an identity element.

We say that two A_0 -bilinear multiplications \star and \diamond are *equivalent* if there exist $\sigma_1, \sigma_2, \tau \in O(N)$ such that $x \diamond y = \tau(\sigma_1(x) \star \sigma_2(y))$ for all $x, y \in E$.

The following theorem is our main result.

Theorem 4.1. *Any A_0 -bilinear multiplication “ \cdot ” on E satisfying the Lagrange identity (4.1) is equivalent to the multiplication “ \circ ” defined by Yang’s formulae.*

Proof. We shall reduce the proof to the special case where e_0 is the identity element of the A_0 -algebra (E, \cdot) . Then the assertion of the theorem follows from the next theorem.

Define A_0 -linear maps $L, R : E \rightarrow E$ by $L(u) = e_0 \cdot u$ and $R(u) = u \cdot e_0$. The Lagrange identity implies that L and R preserve N . By Remark 3.2, $L, R \in O(N)$.

Next we use a well known argument due to, at least, Kaplansky [2]. We have $N(R^{-1}(x) \cdot L^{-1}(y)) = N(x)N(y)$ for $x, y \in E$. With $x \star y = R^{-1}(x) \cdot L^{-1}(y)$, we have

$$\begin{aligned} (e_0 \cdot e_0) \star x &= R^{-1}(e_0 \cdot e_0) \cdot L^{-1}(x) = e_0 \cdot L^{-1}(x) = x, \\ x \star (e_0 \cdot e_0) &= R^{-1}(x) \cdot L^{-1}(e_0 \cdot e_0) = R^{-1}(x) \cdot e_0 = x. \end{aligned}$$

Thus $e_0 \cdot e_0$ is the identity element of the algebra (E, \star) . As $e_0 \cdot e_0 \in U_4$, we have $e_0 \cdot e_0 = ae_i$ for some $a \in U_1$ and some index i . Hence, there exists $\sigma \in O(N)$ such that $\sigma(e_0) = e_0 \cdot e_0$. If $x \diamond y = \sigma^{-1}(\sigma(x) \star \sigma(y))$, then e_0 is the identity element of the algebra (A, \diamond) . □

We assume now that e_0 is the identity element of (E, \cdot) . Consequently, this is a composition algebra in which the alternative laws

$$(4.2) \quad x \cdot (x \cdot y) = (x \cdot x) \cdot y, \quad (x \cdot y) \cdot y = x \cdot (y \cdot y)$$

are valid [3, p. 306]. The reader should consult this book for additional properties of composition algebras. We state only a few properties that we need.

Define the A_0 -linear map *trace* $T : E \rightarrow A_0$ by $T(x) = Q(e_0, x)$. Then for any $x \in E$ we have $x \cdot x - T(x)x + N(x)e_0 = 0$. Linearizing gives

$$(4.3) \quad x \cdot y + y \cdot x = T(x)y + T(y)x - Q(x, y)e_0, \forall x, y \in E.$$

Clearly $Ae_0 \perp A^3$ with respect to Q , where $A^3 = Ae_1 + Ae_2 + Ae_3$.

Recall that we have extended the conjugation $*$ from A to E in Section 2. Moreover, note that

$$(ae_0 + v)^* = a^*e_0 - v, \quad a \in A, v \in A^3.$$

It is easy to verify that

$$(4.4) \quad Q(x, z \cdot y^*) = Q(x \cdot y, z) = Q(y, x^* \cdot z), \forall x, y, z \in E.$$

The fact that in the next theorem one can assert that the two algebras are actually isomorphic is due to the referee.

Theorem 4.2. *Every A_0 -algebra (E, \cdot) satisfying the Lagrange identity (4.1) and having e_0 as the identity element is isomorphic to the Yang algebra (E, \circ) .*

We shall break the proof into several lemmas.

Lemma 4.3. *By replacing “ \cdot ” with an isomorphic multiplication, we may also assume that*

$$(4.5) \quad (ae_0) \cdot y = ay$$

for all $a \in A$ and $y \in E$.

Proof. Let us fix an index i and $b \in U_1$. Then the right multiplication by be_i belongs to $O(N)$, and Theorem 3.4 yields an index j as well as $u_j \in U_1$ such that $(ae_0) \cdot (be_i) = u_jae_j$ for all $a \in A$ or $(ae_0) \cdot (be_i) = u_ja^*e_j$ for all $a \in A$. Specializing a to 1 implies that $j = i$ and $u_j = b$; hence $(ae_0) \cdot (be_i) = abe_i$ for all $a \in A$ or $(ae_0) \cdot (be_i) = a^*be_i$ for all $a \in A$.

Assume that $(ae_0) \cdot (b_1e_i) = ab_1e_i$ holds for all $a \in U_1$ and $(ae_0) \cdot (b_2e_i) = a^*b_2e_i$ holds for all $a \in U_1$, for some units b_1, b_2 different from ± 1 . Then $(ae_0) \cdot ((b_1 + b_2)e_i) = (ab_1 + a^*b_2)e_i$ holds for all $a \in U_1$. By taking norms on both sides, we obtain that

$$(1 - a^2)b_1b_2^* + (1 - (a^*)^2)b_1^*b_2 = 0$$

for all $a \in U_1$. This is clearly a contradiction.

Since U_1 generates A as an abelian group, we conclude that either $(ae_0) \cdot (be_i) = abe_i$ for all $a, b \in A$ or $(ae_0) \cdot (be_i) = a^*be_i$ for all $a, b \in A$. In particular, $(ae_0) \cdot (be_i)$ is A -linear in b .

If $(ae_0) \cdot (be_0) = a^*be_0$ for all $a, b \in A$, then setting $b = 1$ gives the contradiction: $ae_0 = a^*e_0$ for all $a \in A$. Thus we have $(ae_0) \cdot (be_0) = abe_0$ for all $a, b \in A$. For $i \neq 0$, there is an $\varepsilon_i \in \{0, 1\}$ such that $\tau_i^{\varepsilon_i}(\tau_i^{\varepsilon_i}(ae_0) \cdot \tau_i^{\varepsilon_i}(be_i)) = abe_i$ for all $a, b \in A$.

If τ is the product of the $\tau_i^{\varepsilon_i}$ with $i \neq 0$, then $\tau^2 = 1$ and the multiplication “ \star ” defined by $x \star y = \tau(\tau(x) \cdot \tau(y))$ satisfies all the requirements.

Moreover, the map $\tau : (E, \star) \rightarrow (E, \cdot)$ is an isomorphism of unital A_0 -algebras. □

We assume from now on that the identity (4.5) holds. This property will be shared by the modified multiplication, which will be introduced in Lemma 4.6.

Lemma 4.4. *For $a \in A$ and $x \in Ae_1 + Ae_2 + Ae_3$, we have $x \cdot (ae_0) = a^*x$.*

Proof. Recall that $Ae_1 + Ae_2 + Ae_3$ is the kernel of the trace T and is perpendicular to Ae_0 relative to Q . By using (4.3), we obtain that

$$\begin{aligned} x \cdot (ae_0) &= x \cdot (ae_0) + (ae_0) \cdot x - (ae_0) \cdot x \\ &= T(ae_0)x + T(x)ae_0 - Q(x, ae_0)e_0 - ax \\ &= (a + a^* - a)x = a^*x. \end{aligned} \quad \square$$

Lemma 4.5. *For $a, b \in A$ and $i \neq 0$ we have $(ae_i) \cdot (be_i) = -ab^*e_0$.*

Proof. Since N is anisotropic, it suffices to show that $N((ae_i) \cdot (be_i) + ab^*e_0) = 0$. Expanding the LHS and applying (4.4) gives

$$\begin{aligned} N((ae_i) \cdot (be_i) + ab^*e_0) &= 2N(a)N(b) + Q((ae_i) \cdot (be_i), ab^*e_0) \\ &= 2N(a)N(b) + Q(ae_i, (ab^*e_0) \cdot (be_i)^*) \\ &= 2N(a)N(b) - Q(ae_i, (ab^*e_0) \cdot (be_i)) \\ &= 2N(a)N(b) - N(b)Q(ae_i, ae_i) \\ &= 2N(a)N(b) - 2N(a)N(b) = 0. \end{aligned} \quad \square$$

Lemma 4.6. *By replacing “ \cdot ” with an isomorphic multiplication, we may assume that*

$$(4.6) \quad e_i \cdot e_j = e_k = -e_j \cdot e_i$$

for any cyclic permutation (i, j, k) of $(1, 2, 3)$.

Proof. Let (i, j, k) be a cyclic permutation of $(1, 2, 3)$. Since $(e_0 + e_i) \cdot (e_0 + e_j) = e_0 + e_i + e_j + e_i \cdot e_j$ and $N(e_0 + e_j) = N(e_0 + e_i) = 2$, we have $N(e_0 + e_i + e_j + e_i \cdot e_j) = 4$. As $e_i \cdot e_j \in U_4$, Lemma 3.1 implies that $e_i \cdot e_j \in U_1e_k$. A similar argument shows that $e_j \cdot e_i \in U_1e_k$.

In particular we have $e_1 \cdot e_2 = ue_3$ for some $u \in U_1$. The multiplication “ \star ” defined by $x \star y = \sigma_a^{-1}(\sigma_a(x) \cdot \sigma_a(y))$, where $a = (1, 1, 1, u)$, has the previously stated property and sends $(e_1, e_2) \rightarrow e_3$. By replacing “ \cdot ” with this new multiplication, we may assume that $e_1 \cdot e_2 = e_3$.

Since $(e_i + e_j) \cdot (e_i + e_j) = e_i \cdot e_j + e_j \cdot e_i - 2e_0$, we have $N(e_i \cdot e_j + e_j \cdot e_i - 2e_0) = 4$. Since $e_i \cdot e_j + e_j \cdot e_i \in Ae_k$, it follows that this sum is 0, i.e., $e_j \cdot e_i = -e_i \cdot e_j$. In particular, we have $e_2 \cdot e_1 = -e_3$. Thus the assertion of the lemma is valid if $(i, j, k) = (1, 2, 3)$.

The remaining equalities (4.6) follow easily by using the alternative laws (4.2). For instance, we have $e_1 \cdot e_3 = e_1 \cdot (e_1 \cdot e_2) = (e_1 \cdot e_1) \cdot e_2 = (-e_0) \cdot e_2 = -e_2$.

To finish the proof, we point out that the map $\sigma_a : (E, \star) \rightarrow (E, \cdot)$ is an isomorphism of unital A_0 -algebras. □

In view of the last lemma, we may assume now (and we do) that the identities (4.6) are valid for any cyclic permutation (i, j, k) of $(1, 2, 3)$.

Lemma 4.7. *For any cyclic permutation (i, j, k) of $(1, 2, 3)$ we have*

$$(4.7) \quad (ae_i) \cdot (be_j) = a^*b^*e_k = -(be_j) \cdot (ae_i)$$

for all $a, b \in A$. Consequently, the multiplications “ \cdot ” and “ \circ ” coincide.

Proof. In view of (4.3), it suffices to prove the first equality. We first treat the case $a = 1$. By applying the linearized left alternative law, we find that

$$\begin{aligned} e_i \cdot (be_j) &= e_i \cdot ((be_0) \cdot e_j) \\ &= (e_i \cdot (be_0) + (be_0) \cdot e_i) \cdot e_j - (be_0) \cdot (e_i \cdot e_j) \\ &= (b + b^*)e_k - be_k = b^*e_k. \end{aligned}$$

For arbitrary a , by using this special case, the linearized right alternative law and Lemma 4.4, we obtain that

$$\begin{aligned} (ae_i) \cdot (be_j) &= (e_i \cdot (a^*e_0)) \cdot (be_j) \\ &= e_i \cdot ((a^*e_0) \cdot (be_j) + (be_j) \cdot (a^*e_0)) - (e_i \cdot (be_j)) \cdot (a^*e_0) \\ &= e_i \cdot ((a + a^*)be_j) - (b^*e_k) \cdot (a^*e_0) \\ &= ((a + a^*)b^* - ab^*)e_k = a^*b^*e_k. \quad \square \end{aligned}$$

This concludes the proof of Theorem 4.2 and also of Theorem 4.1.

The referee supplied an alternative proof of Theorem 4.2. His proof proceeds first by changing scalars from the base ring $\mathbf{Z}[t]$ to its quotient field $\mathbf{Q}(t)$, and then applying a theorem of Thakur [6] (see also [4, Chapter VIII, Exercise 6]) which establishes a connection between octonion algebras and ternary Hermitian forms. In the case of a Yang algebra, let us write $E = Ae_0 \oplus A^3$, where A^3 is the column A -space. Extending the conjugation of A componentwise to A^3 , we have a Hermitian form $h : A^3 \times A^3 \rightarrow A$ given by $h(v, w) = v^t w^*$. With this notation, the Yang multiplication is given by

$$(ae_0 \oplus v) \circ (be_0 \oplus w) = (ab - h(v, w))e_0 \oplus (aw + b^*v + v^* \times w^*),$$

where $a, b \in A$ and $v, w \in A^3$. The sign \times stands for the ordinary cross product in 3-space.

REFERENCES

- [1] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Hermann, Paris, 1970. MR0274237 (43:2)
- [2] I. Kaplansky, Infinite-dimensional quadratic forms admitting composition, *Proc. Amer. Math. Soc.* **4** (1953), 956–960. MR0059895 (15:596g)
- [3] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der mathematischen Wissenschaften 294, Springer-Verlag, 1991. MR1096299 (92i:11039)
- [4] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc. Colloq. Publ. 44, Amer. Math. Soc., Providence, RI, 1998. MR1632779 (2000a:16031)
- [5] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in *Contemporary Design Theory: A Collection of Surveys*, Eds. J.H. Dinitz and D.R. Stinson, J. Wiley, New York, 1992, pp. 431–560. MR1178508
- [6] M. L. Thakur, Cayley algebra bundles on \mathbf{A}_K^2 revisited, *Comm. Algebra* **23** (1995), no. 13, 5119–5130. MR1356125 (97a:17006)
- [7] C. H. Yang, Lagrange identity for polynomials and δ -codes of lengths $7t$ and $13t$, *Proc. Amer. Math. Soc.* **88** (1983), 746–750. MR702312 (85f:05034)

- [8] C. H. Yang, A composition theorem for δ -codes, Proc. Amer. Math. Soc. **89** (1983), 375–378. MR712655 (85i:94025)
- [9] C. H. Yang, On composition of four-symbol δ -codes and Hadamard matrices, Proc. Amer. Math. Soc. **107** (1989), 763–776. MR979054 (90e:94043)

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, N2L 3G1, CANADA

E-mail address: `djokovic@uwaterloo.ca`

DEPARTMENT OF MATHEMATICS, WILFRID LAURIER UNIVERSITY, WATERLOO, ONTARIO, N2L 3C5, CANADA –AND– INSTITUTE OF MATHEMATICS, ACADEMY OF MATHEMATICS AND SYSTEM SCIENCES, CHINESE ACADEMY OF SCIENCES, BEIJING 100190, PEOPLE'S REPUBLIC OF CHINA

E-mail address: `kzhao@wlu.ca`