Commun. Math. Phys. 306, 83–118 (2011)
Digital Object Identifier (DOI) 10.1007/s00220-011-1279-9

Communications in
**Mathematical
Physics**

A Series of Algebras Generalizing the Octonions and Hurwitz-Radon Identity

Sophie Morier-Genoud[1], **Valentin Ovsienko**[2]

[1] Institut Mathématiques de Jussieu, UMR 7586, Université Pierre et Marie Curie Paris VI, 4 Place Jussieu, Case 247, 75252 Paris Cedex 05, France. E-mail: sophiemg@math.jussieu.fr
[2] CNRS, Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 Boulevard du 11 Novembre 1918, 69622 Villeurbanne Cedex, France. E-mail: ovsienko@math.univ-lyon1.fr

Received: 26 May 2010 / Accepted: 11 February 2011
Published online: 8 June 2011 – © Springer-Verlag 2011

Abstract: We study non-associative twisted group algebras over $(\mathbb{Z}_2)^n$ with cubic twisting functions. We construct a series of algebras that extend the classical algebra of octonions in the same way as the Clifford algebras extend the algebra of quaternions. We study their properties, give several equivalent definitions and prove their uniqueness within some natural assumptions. We then prove a simplicity criterion.

We present two applications of the constructed algebras and the developed technique. The first application is a simple explicit formula for the following famous square identity: $(a_1^2+\cdots+a_N^2)\,(b_1^2+\cdots+b_{\rho(N)}^2) = c_1^2+\cdots+c_N^2$, where c_k are bilinear functions of the a_i and b_j and where $\rho(N)$ is the Hurwitz-Radon function. The second application is the relation to Moufang loops and, in particular, to the code loops. To illustrate this relation, we provide an explicit coordinate formula for the factor set of the Parker loop.

Contents

1. Introduction

The starting idea of this work is the following naive question: *is there a natural way to multiply n-tuples of* 0 *and* 1?

Of course, it is easy to find such algebraic structures. The abelian group $(\mathbb{Z}_2)^n$ provides such a multiplication, but the corresponding group algebra $\mathbb{K}\left[(\mathbb{Z}_2)^n\right]$, over any field of scalars $\mathbb{K}$, is not a simple algebra. A much more interesting algebraic structure on $\mathbb{K}\left[(\mathbb{Z}_2)^n\right]$ is given by the twisted product

$$u_x \cdot u_y = (-1)^{f(x,y)}\, u_{x+y}, \tag{1.1}$$

where $x, y \in (\mathbb{Z}_2)^n$ and f is a two-argument function on $(\mathbb{Z}_2)^n$ with values in $\mathbb{Z}_2 \cong \{0, 1\}$. We use the standard notations u_x for the element of $\mathbb{K}\left[(\mathbb{Z}_2)^n\right]$ corresponding to $x \in (\mathbb{Z}_2)^n$. The only difference between the above product and that of the group algebra $\mathbb{K}\left[(\mathbb{Z}_2)^n\right]$ is the sign. Yet, the structure of the algebra changes completely. Throughout the paper the ground field $\mathbb{K}$ is assumed to be $\mathbb{R}$ or $\mathbb{C}$ (although many results hold for an arbitrary field of characteristic $\neq 2$).

Remarkably enough, the classical Clifford algebras can be obtained as twisted group algebras. The first example is the algebra of quaternions, $\mathbb{H}$. This example was found by many authors but probably first in [23]. The algebra $\mathbb{H}$ is a twisted $(\mathbb{Z}_2)^2$-algebra. More precisely, consider the 4-dimensional vector space over $\mathbb{R}$ spanned by $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$ with the multiplication:

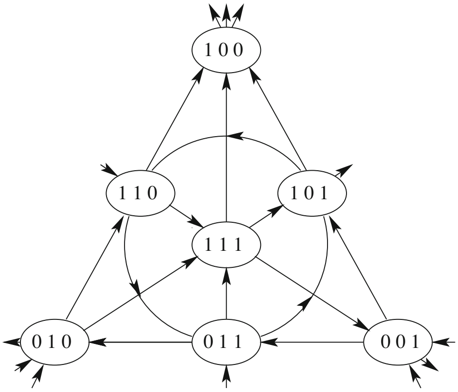

Fig. 1. $(\mathbb{Z}_2)^3$-grading on the octonions

$$u_{(x_1,x_2)} \cdot u_{(y_1,y_2)} = (-1)^{x_1y_1+x_1y_2+x_2y_2}\, u_{(x_1+y_1,\, x_2+y_2)}.$$

It is easy to check that the obtained twisted $(\mathbb{Z}_2)^2$-algebra is, indeed, isomorphic to $\mathbb{H}$, see also [25] for a different grading on the quaternions (over $(\mathbb{Z}_2)^3$).

Along the same lines, a Clifford algebra with n generators, is a $(\mathbb{Z}_2)^n$-graded algebra, see [5]. The (complex) Clifford algebra $C\ell_n$ is isomorphic to the twisted group algebras over $(\mathbb{Z}_2)^n$ with the product

$$u_{(x_1,\ldots,x_n)} \cdot u_{(y_1,\ldots,y_n)} = (-1)^{\sum_{1\leq i\leq j\leq n} x_iy_j}\, u_{(x_1+y_1,\ldots,x_n+y_n)}, \tag{1.2}$$

where $(x_1, \ldots, x_n)$ is an n-tuple of 0 and 1. The above twisting function is bilinear and therefore is a 2-cocycle on $(\mathbb{Z}_2)^n$. The real Clifford algebras $C\ell_{p,q}$ are also twisted group algebras over $(\mathbb{Z}_2)^n$, where $n = p+q$. The twisting function f in the real case contains an extra term $\sum_{1\leq i\leq p} x_iy_i$ corresponding to the signature (see Sect. 3.2).

The algebra of octonions $\mathbb{O}$ can also be viewed as a twisted group algebra [4]. It is isomorphic to $\mathbb{R}\left[(\mathbb{Z}_2)^3\right]$ equipped with the following product:

$$u_{(x_1,x_2,x_3)} \cdot u_{(y_1,y_2,y_3)} = (-1)^{\left(x_1x_2y_3+x_1y_2x_3+y_1x_2x_3+\sum_{1\leq i\leq j\leq 3} x_iy_j\right)}\, u_{(x_1+y_1,\, x_2+y_2,\, x_3+y_3)}.$$

Note that the twisting function in this case is a polynomial of degree 3, and does not define a 2-cocycle. This is equivalent to the fact that the algebra $\mathbb{O}$ is not associative. The multiplication table on $\mathbb{O}$ is usually represented by the Fano plane. The corresponding $(\mathbb{Z}_2)^3$-grading is given in Fig. 1. We also mention that different group gradings on $\mathbb{O}$ were studied in [15], we also refer to [6] for a survey on the octonions and Clifford algebras.

In this paper, we introduce two series of complex algebras, $\mathbb{O}_n$ and $\mathbb{M}_n$, and of real algebras, $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$. The series $\mathbb{O}_n$ and $\mathbb{O}_{p,q}$ generalize the algebra of octonions in a similar way as the Clifford algebras generalize the algebra of quaternions. The situation can be represented by the following diagram:

$$\begin{tikzcd}
& & \vdots & \vdots & & \\
& & C\ell_4 \arrow[u] & \mathbb{O}_5 \arrow[u] & & \\
& & C\ell_3 \arrow[u] & \mathbb{O}_4 \arrow[u] & & \\
\mathbb{R} \arrow[r] & \mathbb{C} \arrow[r] & \mathbb{H} \arrow[r] \arrow[u] & \mathbb{O} \arrow[r] \arrow[u] & \mathbb{S} \arrow[r] & \cdots
\end{tikzcd}$$

where the horizontal line represents the Cayley-Dickson procedure (see, e.g., [6,11]), in particular, $\mathbb{S}$ is the 16-dimensional algebra of sedenions. The algebra $\mathbb{M}_n$ "measures" the difference between $\mathbb{O}_n$ and $C\ell_n$.

The precise definition is as follows. The (complex) algebras $\mathbb{O}_n$ are twisted group algebras $\mathbb{K}\left[(\mathbb{Z}_2)^n\right]$ with the product (1.1), given by the function

$$f_{\mathbb{O}}(x, y) = \sum_{1 \leq i < j < k \leq n} \left(x_i x_j y_k + x_i y_j x_k + y_i x_j x_k\right) + \sum_{1 \leq i \leq j \leq n} x_i y_j, \tag{1.3}$$

for arbitrary n. The algebras $\mathbb{M}_n$ are defined by the twisting function

$$f_{\mathbb{M}}(x, y) = \sum_{1 \leq i < j < k \leq n} \left(x_i x_j y_k + x_i y_j x_k + y_i x_j x_k\right), \tag{1.4}$$

which is just the homogeneous part of degree 3 of the function $f_{\mathbb{O}}$ (i.e., with the quadratic part removed). In the real case, one can again add the signature term $\sum_{1 \leq i \leq p} x_i y_i$, which only changes the square of some generators, and define the algebras $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$.

The function $f_{\mathbb{O}}$ is a straightforward generalization of the twisting function corresponding to the octonions. In particular, the algebra $\mathbb{O}_3$ is just the complexified octonion algebra $\mathbb{O} \otimes \mathbb{C}$. In the real case, $\mathbb{O}_{0,3} \cong \mathbb{O}$, the algebras $\mathbb{O}_{3,0} \cong \mathbb{O}_{2,1} \cong \mathbb{O}_{1,2}$ are isomorphic to another famous algebra called the algebra of split-octonions. The first really interesting new example is the algebra $\mathbb{O}_5$ and its real forms $\mathbb{O}_{p,q}$ with $p + q = 5$.

The algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ are not associative, moreover, they are not alternative. It turns out however, that these algebras have nice properties similar to those of the octonion algebra and of the Clifford algebras at the same time.

As an "abstract algebra", $\mathbb{O}_n$ can be defined in a quite similar way as the Clifford algebras. The algebra $\mathbb{O}_n$ has n generators $u_1, \ldots, u_n$ such that $u_i^2 = -1$ and

$$u_i \cdot u_j = -u_j \cdot u_i, \tag{1.5}$$

respectively, together with the antiassociativity relations

$$u_i \cdot (u_j \cdot u_k) = -(u_i \cdot u_j) \cdot u_k, \tag{1.6}$$

for $i \neq j \neq k$. We will show that *the algebras $\mathbb{O}_n$ are the only algebras with n generators $u_1, \ldots, u_n$ satisfying (1.5) and (1.6) and such that any three monomials u, v, w either associate or antiassociate independently of the order of u, v, w.*

The relations of higher degree are then calculated inductively using the following simple "linearity law". Given three monomials u, v, w, then

$$u \cdot (v \cdot w) = (-1)^{\phi(\deg u, \deg v, \deg w)} (u \cdot v) \cdot w,$$

where ϕ is the trilinear function uniquely defined by the above relations of degree 3, see Sect. 4.4 for the details. For instance, one has $u_i \cdot ((u_j \cdot u_k) \cdot u_\ell) = (u_i \cdot (u_j \cdot u_k)) \cdot u_\ell$, for $i \neq j \neq k \neq \ell$, etc.

The presentation of $\mathbb{M}_n$ is exactly the same as above, except that the generators of $\mathbb{M}_n$ commute. We will prove two classification results characterizing the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ algebras in an axiomatic way.

Our main tool is the notion of *generating function*. This is a function in one argument $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ that encodes the structure of the algebra. Existence of a generating function is a strong condition. This is a way to distinguish the series $\mathbb{O}_n$ and $\mathbb{M}_n$ from the classical Cayley-Dickson algebras.

The main results of the paper contain four theorems and their corollaries.

(1) Theorem 1 states that the generating function determines a (complex) twisted group algebra completely.
(2) Theorem 2 is a general characterization of non-associative twisted group algebras over $(\mathbb{Z}_2)^n$ with a symmetric non-associativity factor, in terms of generating functions.
(3) Theorem 3 answers the question for which n (and p, q) the constructed algebras are simple. The result is quite similar to that for the Clifford algebras, except that the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ degenerate for one value of n over 4 and not 1 over 2 as $C\ell_n$.
(4) Theorem 4 provides explicit formulæ of the Hurwitz-Radon square identities. The algebras $\mathbb{O}_n$ (as well as $\mathbb{M}_n$) are not composition algebras. However, they have natural Euclidean norm $\mathcal{N}$. We obtain a necessary and sufficient condition for elements u and v to satisfy $\mathcal{N}(u \cdot v) = \mathcal{N}(u)\,\mathcal{N}(v)$. Whenever we find two subspaces $V, W \subset \mathbb{O}_n$ consisting of elements satisfying this condition, we obtain a square identity generalizing the famous "octonionic" 8-square identity.

The algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ are closely related to the theory of Moufang loops and, in particular, to code loops, see [14,18,26] and references therein. Indeed, the homogeneous elements $\pm u_x$, where $x \in (\mathbb{Z}_2)^n$ form a Moufang loop of rank 2^{n+1}. As an application, we show in Sect. 9 how the famous Parker loop fits into our framework.

Our main tools include variations on the cohomology of $(\mathbb{Z}_2)^n$ and the linear algebra over $(\mathbb{Z}_2)^n$. A brief account on this subject is presented in Sect. 2.4 and in the Appendix.

2. Twisted Group Algebras over $(\mathbb{Z}_2)^n$

In this section, we give the standard definition of twisted group algebra over the abelian group $(\mathbb{Z}_2)^n$. The twisting function we consider is not necessarily a 2-cocycle. We recall the related notion of graded quasialgebra introduced in [4]. In the end of the section, we give a short account on the cohomology of $(\mathbb{Z}_2)^n$ with coefficients in $\mathbb{Z}_2$.

2.1. Basic definitions. The most general definition is the following. Let $(G, +)$ be an abelian group. A *twisted group algebra* $(\mathbb{K}[G], F)$ is the algebra spanned by the elements u_x for $x \in G$ and equipped with the product

$$u_x \cdot u_y = F(x, y)\, u_{x+y},$$

where $F : G \times G \to \mathbb{K}^*$ is an *arbitrary* two-argument function such that

$$F(0, .) = F(., 0) = 1.$$

The algebra $(\mathbb{K}[G], F)$ is always unital and it is associative if and only if F is a 2-cocycle on G. Twisted group algebras are a classical subject (see, e.g., [7,9] and references therein).

We will be interested in the particular case of twisted algebras over $G = (\mathbb{Z}_2)^n$ and the twisting function F of the form

$$F(x, y) = (-1)^{f(x,y)},$$

with f taking values in $\mathbb{Z}_2 \cong \{0, 1\}$. We will denote by $\left(\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f\right)$ the corresponding twisted group algebra. Let us stress that the function f is not necessarily a 2-cocycle.

2.2. Quasialgebra structure. An arbitrary twisted group algebra $\mathcal{A} = \left(\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f\right)$ gives rise to two functions

$$\beta : (\mathbb{Z}_2)^n \times (\mathbb{Z}_2)^n \to \mathbb{Z}_2, \qquad \phi : (\mathbb{Z}_2)^n \times (\mathbb{Z}_2)^n \times (\mathbb{Z}_2)^n \to \mathbb{Z}_2$$

such that

$$u_x \cdot u_y = (-1)^{\beta(x,y)}\, u_y \cdot u_x, \tag{2.1}$$
$$u_x \cdot \left(u_y \cdot u_z\right) = (-1)^{\phi(x,y,z)} \left(u_x \cdot u_y\right) \cdot u_z, \tag{2.2}$$

for any homogeneous elements $u_x, u_y, u_z \in \mathcal{A}$. The function β obviously satisfies the following properties: $\beta(x, y) = \beta(y, x)$ and $\beta(x, x) = 0$. Following [4], we call the structure β, ϕ a *graded quasialgebra*.

The functions β and ϕ can be expressed in terms of the twisting function f:

$$\beta(x, y) = f(x, y) + f(y, x), \tag{2.3}$$
$$\phi(x, y, z) = f(y, z) + f(x + y, z) + f(x, y + z) + f(x, y). \tag{2.4}$$

Note that (2.4) reads

$$\phi = \delta f.$$

In particular, ϕ is a (trivial) 3-cocycle. Conversely, given the functions β and ϕ, to what extent is the corresponding function f uniquely defined? We will give the answer to this question in Sect. 3.3.

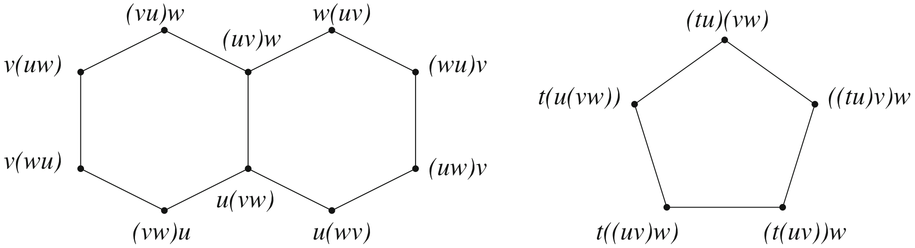

Fig. 2. Two hexagonal and the pentagonal commutative diagrams

Example 2.1. (a) For the Clifford algebra $C\ell_n$ (and for $C\ell_{p,q}$ with $p+q=n$), the function β is bilinear:

$$\beta_{C\ell_n}(x,y)=\sum_{i\neq j} x_i y_j .$$

The function $\phi\equiv 0$ since the twisting function (1.2) is a 2-cocycle; this is of course equivalent to the associativity property. Every simple graded quasialgebra with bilinear β and $\phi\equiv 0$ is a Clifford algebra, see [25].

(b) For the algebra of octonions $\mathbb{O}$, the function β is as follows: $\beta(x,y)=0$ if either $x=0$, or $y=0$, or $x=y$; otherwise, $\beta(x,y)=1$. The function ϕ is the determinant of 3×3 matrices:

$$\phi(x,y,z)=\det|x,y,z|\,,$$

where $x,y,z\in(\mathbb{Z}_2)^3$. This function is symmetric and trilinear.

Remark 2.2. The notion of graded quasialgebra was defined in [5] in a more general situation where G is an arbitrary abelian group and the functions that measure the defect of commutativity and associativity take values in $\mathbb{K}^*$ instead of $\mathbb{Z}_2$. The "restricted version" we consider is very special and this is the reason we can say much more about it. On the other hand, many classical algebras can be treated within our framework.

2.3. The pentagonal and the hexagonal diagrams. Consider any three homogeneous elements, $u,v,w\in\mathcal{A}$. The functions β and ϕ relate the different products, $u(vw)$, $(uv)w$, $(vu)w$, etc. The hexagonal diagrams in Fig. 2 represent different loops in $\mathcal{A}$ that lead to the following identities:

$$\begin{aligned}\phi(x,y,z)+\beta(x,y+z)+\phi(y,z,x)+\beta(z,x)+\phi(y,x,z)+\beta(x,y)&=0,\\ \phi(x,y,z)+\beta(z,y)+\phi(x,z,y)+\beta(z,x)+\phi(z,x,y)+\beta(x+y,z)&=0.\end{aligned}\tag{2.5}$$

Note that these identities can be checked directly from (2.3) and (2.4). In a similar way, the products of any four homogeneous elements t,u,v,w, (see the pentagonal diagrams of Fig. 2) is equivalent to the condition

$$\phi(y,z,t)+\phi(x+y,z,t)+\phi(x,y+z,t)+\phi(x,y,z+t)+\phi(x,y,z)=0,\tag{2.6}$$

which is nothing but the 3-cocycle condition $\delta\phi=0$. We already knew this identity from $\phi=\delta f$.

Let us stress the fact that these two commutative diagrams are tautologically satisfied and give no restriction on f.

2.4. Cohomology $H^*\left((\mathbb{Z}_2)^n\,;\mathbb{Z}_2\right)$. In this section, we recall classical notions and results on the cohomology of $G = (\mathbb{Z}_2)^n$ with coefficients in $\mathbb{Z}_2$.

We consider the space of cochains, $\mathcal{C}^q = \mathcal{C}^q(G;\mathbb{Z}_2)$, consisting of (arbitrary) maps in q arguments $c : G \times \cdots \times G \to \mathbb{Z}_2$. The usual coboundary operator $\delta : \mathcal{C}^q \to \mathcal{C}^{q+1}$ is defined by

$$\delta c(g_1,\ldots,g_{q+1}) = c(g_1,\ldots,g_q) + \sum_{i=1}^{q} c(g_1,\ldots,g_{i-1},g_i+g_{i+1},g_{i+2},\ldots,g_q) + c(g_2,\ldots,g_{q+1}),$$

for all $g_1,\ldots,g_{q+1} \in G$. This operator satisfies $\delta^2 = 0$.

A cochain c is called *q-cocycle* if $\delta q = 0$, and called a *q-coboundary* (or a trivial q-cocycle) if $c = \delta b$, for some cochain $b \in \mathcal{C}^{q-1}$. The space of q^{th} cohomology, $H^q(G;\mathbb{Z}_2)$, is the quotient space of q-cocycles modulo q-coboundaries. We are particularly interested in the case where $q = 1, 2$ or 3.

A fundamental result (cf. [1], p. 66) states that the cohomology ring $H^*(G;\mathbb{Z}_2)$ is isomorphic to the algebra of polynomials in n commuting variables $e_1,\ldots,e_n$:

$$H^*(G;\mathbb{Z}_2) \cong \mathbb{Z}_2[e_1,\ldots,e_n].$$

The basis of $H^q(G;\mathbb{Z}_2)$ is given by the cohomology classes of the following multilinear q-cochains:

$$(x^{(1)},\ldots,x^{(q)}) \mapsto x^{(1)}_{i_1}\cdots x^{(q)}_{i_q}, \qquad i_1 \le \cdots \le i_q, \tag{2.7}$$

where each $x^{(k)} \in (\mathbb{Z}_2)^n$ is an n-tuple of 0 and 1:

$$x^{(k)} = (x^{(k)}_1,\ldots,x^{(k)}_n).$$

The q-cocycle (2.7) is identified with the monomial $e_{i_1}\cdots e_{i_q}$.

Example 2.3. The linear maps $c_i(x) = x_i$, for $i = 1,\ldots,n$ provide a basis of $H^1(G;\mathbb{Z}_2)$ while the bilinear maps

$$c_{ij}(x,y) = x_i\, y_j, \qquad i \le j$$

provide a basis of the second cohomology space $H^2(G;\mathbb{Z}_2)$.

2.5. Polynomials and polynomial maps. The space of all functions on $(\mathbb{Z}_2)^n$ with values in $\mathbb{Z}_2$ is isomorphic to the quotient space

$$\mathbb{Z}_2\,[x_1,\ldots,x_n]\;/\;(x_i^2 - x_i\;:\;i = 1,\ldots,n).$$

A function $P : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ can be expressed as a polynomial in $(x_1,\ldots,x_n)$, but not in a unique way.

Throughout the paper we identify the function P to the polynomial expression in which each monomial is minimally represented (i.e. has the lowest degree possible). So that each function P can be uniquely written in the following form:

$$P = \sum_{k=0}^{n} \sum_{1\le i_1<\cdots<i_k\le n} \lambda_{i_1\ldots i_k}\, x_{i_1}\cdots x_{i_k},$$

where $\lambda_{i_1\ldots i_k} \in \{0,1\}$.

3. The Generating Function

In this section we go further into the general theory of twisted group algebra over $(\mathbb{Z}_2)^n$. We define the notion of generating function. To the best of our knowledge, this notion has never been considered. This notion will be fundamental for us since it allows to distinguish the Clifford algebras, octonions and the two new series we introduce in this paper from other twisted group algebras over $(\mathbb{Z}_2)^n$ (such as Cayley-Dickson algebras). The generating function contains the full information about the algebra, except for the signature.

3.1. Generating functions. The notion of generating function makes sense for any G-graded quasialgebra $\mathcal{A}$, over an arbitrary abelian group G. We are only interested in the case where $\mathcal{A}$ is a twisted group algebra over $(\mathbb{Z}_2)^n$.

Definition 3.1. *Given a G-graded quasialgebra, a function $\alpha : G \to \mathbb{Z}_2$ will be called a* **generating function** *if the binary function β and the ternary function ϕ defined by (2.1) and (2.2) are both determined by α via*

$$\beta(x, y) = \alpha(x + y) + \alpha(x) + \alpha(y), \tag{3.1}$$

$$\begin{aligned}\phi(x, y, z) = {} & \alpha(x + y + z) \\ & + \alpha(x + y) + \alpha(x + z) + \alpha(y + z) \\ & + \alpha(x) + \alpha(y) + \alpha(z).\end{aligned} \tag{3.2}$$

Note that the identity (3.1) implies that α vanishes on the zero element $0 = (0, \dots, 0)$ of $(\mathbb{Z}_2)^n$, because the corresponding element $1 := u_0$ is the unit of $\mathcal{A}$ and therefore commutes with any other element of $\mathcal{A}$.

The identity (3.1) means that β is the differential of α in the usual sense of group cohomology. The second identity (3.2) suggests the operator of "second derivation", δ_2, defined by the right-hand-side, so that the above identities then read:

$$\beta = \delta\alpha, \qquad \phi = \delta_2\alpha.$$

The algebra $\mathcal{A}$ is commutative if and only if $\delta\alpha = 0$; it is associative if and only if $\delta_2\alpha = 0$. The cohomological meaning of the operator δ_2 will be discussed in the Appendix.

Note also that formulæ (3.1) and (3.2) are known in linear algebra and usually called *polarization*. This is the way one obtains a bilinear form from a quadratic one and a trilinear form from a cubic one, respectively.

Example 3.2. (a) The classical algebras of quaternions $\mathbb{H}$ and of octonions $\mathbb{O}$ have generating functions. They are of the form:

$$\alpha(x) = \begin{cases} 1, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

It is amazing that such simple functions contain the full information about the structure of $\mathbb{H}$ and $\mathbb{O}$.

(b) The generating function of $C\ell_n$ is as follows:

$$\alpha_{C\ell}(x) = \sum_{1\leq i\leq j\leq n} x_i x_j. \tag{3.3}$$

Indeed, one checks that the binary function β defined by (3.1) is exactly the skew-symmetrization of the function $f = \sum_{1\leq i\leq j\leq n} x_i y_j$. The function ϕ defined by (3.2) is identically zero, since α is a quadratic polynomial.

The most important feature of the notion of generating function is the following. In the complex case, the generating function contains the full information about the algebra.

Theorem 1. *If $\mathcal{A}$ and $\mathcal{A}'$ are two complex twisted group algebras with the same generating function, then $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic as graded algebras.*

This theorem will be proved in Sect. 3.3.

In the real case, the generating function determines the algebra up to the signature.

3.2. The signature. Consider a twisted group algebra $\mathcal{A} = (\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f)$. We will always use the following set of generators of $\mathcal{A}$:

$$u_i = u_{(0,\ldots,0,1,0,\ldots 0)}, \tag{3.4}$$

where 1 stands at i^{th} position. One has $u_i^2 = \pm 1$, the sign being determined by f. The *signature* is the data of the signs of the squares of the generators u_i.

Definition 3.3. *We say that the twisting functions f and f' differ by a signature if one has*

$$f(x,y) - f'(x,y) = x_{i_1} y_{i_1} + \cdots + x_{i_p} y_{i_p}, \tag{3.5}$$

where $p \leq n$ is an integer.

Note that $f - f'$ as above, is a non-trivial 2-cocycle, for $p \geq 1$. The quasialgebra structures defined by (2.3) and (2.4) are identically the same: $\beta = \beta'$ and $\phi = \phi'$.

The signature represents the main difference between the twisted group algebras over $\mathbb{C}$ and $\mathbb{R}$.

Proposition 3.4. *If $\mathcal{A} = (\mathbb{C}\left[(\mathbb{Z}_2)^n\right], f)$ and $\mathcal{A}' = (\mathbb{C}\left[(\mathbb{Z}_2)^n\right], f')$ are complex twisted group algebras such that f and f' differ by a signature, then $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic as graded algebras.*

Proof. Let us assume $p = 1$ in (3.5), i.e., $f(x,y) - f'(x,y) = x_{i_1} y_{i_1}$, the general case will then follow by induction. Let u_x, resp. u'_x, be the standard basis elements of $\mathcal{A}$, resp. $\mathcal{A}'$. Let us consider the map $\theta : \mathcal{A} \to \mathcal{A}'$ defined by

$$\theta(u_x) = \begin{cases} \sqrt{-1}\, u'_x, & \text{if } x_{i_1} = 1, \\ u'_x, & \text{otherwise.} \end{cases}$$

Note that one can write $\theta(u_x) = \sqrt{-1}^{\,x_{i_1}} u'_x$, for all x. Let us show that θ is a (graded) isomorphism between $\mathcal{A}$ and $\mathcal{A}'$. On the one hand,

$$\theta(u_x \cdot u_y) = (-1)^{f(x,y)}\, \theta(u_{x+y}) = (-1)^{f(x,y)} \sqrt{-1}^{\,(x_{i_1}+y_{i_1})}\, u'_{x+y}.$$

On the other hand,

$$\theta(u_x)\cdot\theta(u_y)=\sqrt{-1}^{\,x_{i_1}}\,u'_x\cdot\sqrt{-1}^{\,y_{i_1}}\,u'_y=\sqrt{-1}^{\,x_{i_1}}\,\sqrt{-1}^{\,y_{i_1}}\,(-1)^{f'(x,y)}\,u'_{x+y}.$$

Using the following (surprising) formula

$$\frac{\sqrt{-1}^{\,x_{i_1}}\sqrt{-1}^{\,y_{i_1}}}{\sqrt{-1}^{\,(x_{i_1}+y_{i_1})}}=(-1)^{x_{i_1}y_{i_1}},\tag{3.6}$$

we obtain $\theta(u_x\cdot u_y)=\theta(u_x)\cdot\theta(u_y)$.

To understand (3.6), beware that the power $x_{i_1}+y_{i_1}$ in the denominator is taken modulo 2. □

In the real case, the algebras $\mathcal{A}$ and $\mathcal{A}'$ can be non-isomorphic but can also be isomorphic. We will encounter throughout this paper the algebras for which either situation occurs.

3.3. Isomorphic twisted algebras. Let us stress that all the isomorphisms between the twisted group algebras we consider in this section preserve the grading. Such isomorphisms are called *graded isomorphisms*.

It is natural to ask under what condition two functions f and f' define isomorphic algebras. Unfortunately, we do not know the complete answer to this question and give here two conditions which are sufficient but certainly not necessary.

Lemma 3.5. *If $f-f'=\delta b$ is a coboundary, i.e., $b:(\mathbb{Z}_2)^n\to\mathbb{Z}_2$ is a function such that*

$$f(x,y)-f'(x,y)=b(x+y)+b(x)+b(y),$$

then the corresponding twisted algebras are isomorphic.

Proof. The isomorphism is given by the map $u_x\mapsto(-1)^{b(x)}\,u_x$, for all $x\in(\mathbb{Z}_2)^n$. □

Lemma 3.6. *Given a group automorphism $T:(\mathbb{Z}_2)^n\to(\mathbb{Z}_2)^n$, the functions f and*

$$f'(x,y)=f(T(x),T(y))$$

define isomorphic twisted group algebras.

Proof. The isomorphism is given by the map $u_x\mapsto u_{T^{-1}(x)}$, for all $x\in(\mathbb{Z}_2)^n$. □

Note that the automorphisms of $(\mathbb{Z}_2)^n$ are just arbitrary linear transformations.

We are ready to answer the question formulated in the end of Sect. 2.2.

Proposition 3.7. *Given two twisted algebras $\mathcal{A}=(\mathbb{K}\left[(\mathbb{Z}_2)^n\right],f)$ and $\mathcal{A}'=(\mathbb{K}\left[(\mathbb{Z}_2)^n\right],f')$, the corresponding quasialgebra structures coincide, i.e., $\beta'=\beta$ and $\phi'=\phi$, if and only if*

$$f(x,y)-f'(x,y)=\delta b(x,y)+\sum_{1\leq i\leq n}\lambda_i\,x_iy_i,$$

where $b:(Z_2)^n\to\mathbb{Z}_2$ is an arbitrary function, and λ_i are coefficients in $\mathbb{Z}_2$. In particular, if $\mathbb{K}=\mathbb{C}$, then $\mathcal{A}\cong\mathcal{A}'$.

Proof. If the quasialgebras structures coincide, then $\phi' = \phi$ implies $\delta f' = \delta f$, so that $f - f'$ is a 2-cocycle. We use the information about the second cohomology space $H^2((\mathbb{Z}_2)^n; \mathbb{Z}_2)$ (see Sect. 2.4). Up to a 2-coboundary, every non-trivial 2-cocycle is a linear combination of the following bilinear maps: $(x, y) \mapsto x_i y_i$, for some i and $(x, y) \mapsto x_k y_\ell$, for some $k < \ell$. One deduces that $f - f'$ is of the form

$$f(x, y) - f'(x, y) = \delta b(x, y) + \sum_{1 \leq i \leq n} \lambda_i \, x_i y_i + \sum_{k<\ell} \mu_{k\ell} \, x_k y_\ell.$$

Since $\beta' = \beta$, one observes that $f - f'$ is symmetric, so that the last summand vanishes, while the second summand is nothing but the signature. The isomorphism in the complex case then follows from Proposition 3.4 and Lemma 3.5.

Conversely, if f and f' are related by the above expression, then the quasialgebra structures obviously coincide. □

Now, we can deduce Theorem 1 as a corollary of Proposition 3.7. Indeed, if $\mathcal{A}$ and $\mathcal{A}'$ have the same generating function α, then the quasialgebra structures of $\mathcal{A}$ and $\mathcal{A}'$ are the same.

3.4. Involutions. Let us mention one more property of generating functions.

Recall that an *involution* on an algebra $\mathcal{A}$ is a linear map $a \mapsto \bar{a}$ from $\mathcal{A}$ to $\mathcal{A}$ such that $\overline{ab} = \bar{b}\,\bar{a}$ and $\bar{1} = 1$, i.e., an involution is an anti-automorphism. Every generating function defines a graded involution of the following particular form:

$$\overline{u_x} = (-1)^{\alpha(x)} \, u_x. \tag{3.7}$$

Proposition 3.8. *If α is a generating function, then the linear map defined by formula (3.7) is an involution.*

Proof. Using (2.1) and (3.1), one has

$$\overline{u_x u_y} = (-1)^{\alpha(x+y)} \, u_x u_y = (-1)^{\alpha(x+y)+\beta(x,y)} \, u_y \, u_x = (-1)^{\alpha(x)+\alpha(y)} \, u_y \, u_x = \overline{u_y} \, \overline{u_x}.$$

Hence the result. □

In particular, the generating functions of $\mathbb{H}$ and $\mathbb{O}$, see Example 3.2, correspond to the canonical involutions, i.e., to the conjugation.

4. The Series $\mathbb{O}_n$ and $\mathbb{M}_n$: Characterization

In this section, we formulate our first main result. Theorem 2 concerns the general properties of twisted $(\mathbb{Z}_2)^n$-algebras with $\phi = \delta f$ symmetric. This result distinguishes a class of algebras of which our algebras of $\mathbb{O}$- and $\mathbb{M}$-series are the principal representatives. We will also present several different ways to define the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$, as well as of $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$.

4.1. Symmetric quasialgebras. An arbitrary twisted group algebra leads to a quasialgebra structure. One needs to assume some additional conditions on the "twisting" function f in order to obtain an interesting class of algebras.

We will be interested in the case where the function $\phi = \delta f$, see formula (2.4), is symmetric:

$$\phi(x, y, z) = \phi(y, x, z) = \phi(x, z, y). \tag{4.1}$$

This condition seems to be very natural: it means that if three elements, u_x, u_y and u_z form a antiassociative triplet, i.e., one has $u_x \cdot (u_y \cdot u_z) = -(u_x \cdot u_y) \cdot u_z$, then this property is independent of the ordering of the elements in the triplet.

An immediate consequence of the identity (2.5) is that, if ϕ is symmetric, then it is completely determined by β:

$$\begin{aligned}\phi(x, y, z) &= \beta(x + y,\ z) + \beta(x, z) + \beta(y, z)\\ &= \beta(x,\ y + z) + \beta(x, y) + \beta(x, z),\end{aligned} \tag{4.2}$$

as the "defect of linearity" in each argument.

The following statement is our main result about the general structure of a twisted group algebra $\mathcal{A} = (\mathbb{K}[(\mathbb{Z}_2)^n], f)$. We formulate this result in a slightly more general context of $(\mathbb{Z}_2)^n$-graded quasialgebra.

Theorem 2. *Given a $(\mathbb{Z}_2)^n$-graded quasialgebra $\mathcal{A}$, the following conditions are equivalent.*

(i) *The function ϕ is symmetric.*
(ii) *The algebra $\mathcal{A}$ has a generating function.*

This theorem will be proved in Sect. 6.1.

It is now natural to ask under what condition a function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is a generating function for some twisted group algebra. The following statement provides a necessary and sufficient condition.

Proposition 4.1. *Given a function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$, there exists a twisted group algebra $\mathcal{A}$ such that α is a generating function of $\mathcal{A}$, if and only if α is a polynomial of degree ≤ 3.*

This proposition will be proved in Sect. 6.2. Furthermore, we will show in Sect. 6.3 that the generating function can be chosen in a canonical way.

Theorem 2 has a number of consequences. In particular, it implies two more important properties of ϕ. The function ϕ is called *trilinear* if it satisfies

$$\phi(x + y, z, t) = \phi(x, z, t) + \phi(y, z, t), \tag{4.3}$$

and similarly in each argument. The function ϕ is *alternate* if it satisfies

$$\phi(x, x, y) = \phi(x, y, x) = \phi(y, x, x) = 0, \tag{4.4}$$

for all $x, y \in (\mathbb{Z}_2)^n$.

Let us stress that an algebra satisfying (4.4) is *graded-alternative* i.e.,

$$u_x \cdot (u_x \cdot u_y) = u_x^2 \cdot u_y \qquad (u_y \cdot u_x) \cdot u_x = u_y \cdot u_x^2,$$

for all homogeneous elements u_x and u_y. This does not imply that the algebra is alternative. Let us mention that alternative graded quasialgebras were classified in [3].

The following result is a consequence of Theorem 2 and Proposition 4.1.

Corollary 4.2. *If the function ϕ is symmetric, then ϕ is trilinear and alternate.*

This corollary will be proved in Sect. 6.2.

Our next goal is to study two series of algebras with symmetric function $\phi = \delta f$. Let us notice that the Cayley-Dickson algebras are not of this type, cf. [4].

4.2. The generating functions of the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$. We already defined the complex algebras $\mathbb{O}_n$ and $\mathbb{M}_n$, with $n \geq 3$ and the real algebra $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$, see the Introduction, formulæ (1.3) and (1.4).

Let us now calculate the associated function $\phi = \delta f$ which is exactly the same for $f = f_{\mathbb{O}}$ or $f_{\mathbb{M}}$. One obtains

$$\phi(x, y, z) = \sum_{i \neq j \neq k} x_i y_j z_k.$$

This function is symmetric in x, y, z and Theorem 2 implies that the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ have generating functions. The explicit formulæ are as follows:

$$\alpha_{\mathbb{O}}(x) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i < j \leq n} x_i x_j + \sum_{1 \leq i \leq n} x_i, \tag{4.5}$$

and

$$\alpha_{\mathbb{M}}(x) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i \leq n} x_i. \tag{4.6}$$

Note that the generating functions $\alpha_{\mathbb{O}}$ and $\alpha_{\mathbb{M}}$ are $\mathfrak{S}_n$*-invariant* with respect to the natural action of the group of permutations $\mathfrak{S}_n$ on $(\mathbb{Z}_2)^n$.

Thanks to the $\mathfrak{S}_n$-invariance, we can give a very simple description of the above functions. Denote by $|x|$ the *weight* of $x \in (\mathbb{Z}_2)^n$ (i.e., the number of 1 entries in x written as an n-tuple of 0 and 1). The above generating functions, together with that of the Clifford algebras depend only on $|x|$ and are 4-periodic:

$\lvert x \rvert$	1	2	3	4	5	6	7	8	$\cdots$
$\alpha_{C\ell}$	1	1	0	0	1	1	0	0	$\cdots$
$\alpha_{\mathbb{O}}$	1	1	1	0	1	1	1	0	$\cdots$
$\alpha_{\mathbb{M}}$	1	0	0	0	1	0	0	0	$\cdots$

(4.7)

This table is the most simple way to use the generating function in any calculation. One can deduce the explicit formulæ (3.3), (4.5) and (4.6) directly from Table (4.7).

4.3. Characterization of the algebras of the $\mathbb{O}$- and $\mathbb{M}$-series. Let us formulate two uniqueness results that allow us to give axiomatic definitions of the introduced algebras.

Recall that the group of permutations $\mathfrak{S}_n$ acts on $(\mathbb{Z}_2)^n$ in a natural way. We will characterize the algebras of the $\mathbb{O}$- and $\mathbb{M}$-series in terms of $\mathfrak{S}_n$-invariance. We observe that, in spite of the fact that the functions $f_{\mathbb{O}}$ and $f_{\mathbb{M}}$ are not $\mathfrak{S}_n$-invariant, the corresponding algebras are. However, we believe that $\mathfrak{S}_n$-invariance is a technical assumption and can be relaxed, see the Appendix for a discussion.

The first uniqueness result is formulated directly in terms of the twisting function f. We study the unital twisted algebras $\mathcal{A} = (\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f)$ satisfying the following conditions:

(1) The function f is a polynomial of degree 3.
(2) The algebra $\mathcal{A}$ is graded-alternative, see (4.4).
(3) The set of relations between the generators (3.4) of $\mathcal{A}$ is invariant with respect to the action of the group of permutations $\mathfrak{S}_n$.

Since we will use the relations of degree 2 or 3, the condition (3) means that we assume that the generators either all pairwise commute or all pairwise anticommute and that one has either

$$u_i \cdot (u_j \cdot u_k) = (u_i \cdot u_j) \cdot u_k, \qquad \text{for all} \qquad i \neq j \neq k,$$

or

$$u_i \cdot (u_j \cdot u_k) = -(u_i \cdot u_j) \cdot u_k, \qquad \text{for all} \qquad i \neq j \neq k.$$

Proposition 4.3. *The algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ are the only twisted $(\mathbb{Z}_2)^n$-algebras satisfying the above three conditions.*

Proof. Since the algebra $\mathcal{A}$ is unital, we have $f(0,.) = f(.,0) = 0$. This implies that f contains no constant term and no terms depending only on x (or only on y) variables. The most general twisting function f of degree 3 is of the form

$$\begin{aligned} f(x,y) = \sum_{i<j<k} \Big(& \lambda^1_{ijk}\, x_i x_j y_k + \lambda^2_{ijk}\, x_i y_j x_k + \lambda^3_{ijk}\, y_i x_j x_k \\ & + \mu^1_{ijk}\, y_i y_j x_k + \mu^2_{ijk}\, y_i x_j y_k + \mu^3_{ijk}\, x_i y_j y_k \Big) \\ + \sum_{i,j} & \nu_{ij}\, x_i y_j, \end{aligned}$$

where $\lambda^e_{ijk}, \mu^e_{ijk}$ and ν^e_{ij} are arbitrary coefficients 0 or 1. Indeed, the expression of f cannot contain the monomials $x_i x_j y_j$ and $x_i y_i y_j$ because of the condition (2).

By Lemma 3.5, adding a coboundary to f gives an isomorphic algebra (as $(\mathbb{Z}_2)^n$-graded algebras). We may assume that for any $i < j < k$, the coefficient $\mu^1_{ijk} = 0$ (otherwise, we add the coboundary of $b(x) = x_i x_j x_k$).

We now compute $\phi = \delta f$ and obtain:

$$\begin{aligned} \phi(x,y,z) = \sum_{i<j<k} \Big(& (\lambda^1_{ijk} + \mu^3_{ijk})\, x_i y_j z_k + (\lambda^2_{ijk} + \mu^3_{ijk})\, x_i z_j y_k + (\lambda^1_{ijk} + \mu^2_{ijk})\, y_i x_j z_k \\ & + \lambda^2_{ijk}\, y_i z_j x_k + (\lambda^3_{ijk} + \mu^2_{ijk})\, z_i x_j y_k + \lambda^3_{ijk}\, x_i y_j z_k \Big). \end{aligned}$$

We can assume that

$$u_i \cdot (u_j \cdot u_k) = -(u_i \cdot u_j) \cdot u_k, \qquad i \neq j \neq k.$$

Indeed, if $u_i \cdot (u_j \cdot u_k) = (u_i \cdot u_j) \cdot u_k$ for some values of i, j, k such that $i \neq j \neq k$, then (3) implies the same associativity relation for all i, j, k. Since ϕ is trilinear, this means that $\mathcal{A}$ is associative, so that $\phi = 0$. This can only happen if $\lambda^e_{ijk} = \mu^e_{ijk} = 0$ for all i, j, k, so that $\deg f = 2$.

In other words, we obtain a system of equations $\phi(x_i, y_j, z_k) = 1$ for all i, j, k. This system has a unique solution $\lambda^1_{ijk} = \lambda^2_{ijk} = \lambda^3_{ijk} = 1$ and $\mu^2_{ijk} = \mu^3_{ijk} = 0$.

Finally, if all of the generators commute, we obtain $\nu_{ij} = \nu_{ji}$, so that $\nu_{ij} = 0$ up to a coboundary, so that $f = f_{\mathbb{M}}$. If all of the generators anticommute, again up to a coboundary, we obtain $\nu_{ij} = 1$, if and only if $i < j$, so that $f = f_{\mathbb{O}}$. □

The second uniqueness result is formulated in terms of the generating function.

Proposition 4.4. *The algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ and the algebras $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$ with $p+q=n$, are the only non-associative twisted $(\mathbb{Z}_2)^n$-algebras over the field of scalars $\mathbb{C}$ or $\mathbb{R}$ that admit an $\mathfrak{S}_n$-invariant generating function.*

Proof. By Proposition 4.1, we know that the generating function is a polynomial of degree ≤ 3. Every $\mathfrak{S}_n$-invariant polynomial $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ of degree ≤ 3 is a linear combination

$$\alpha = \lambda_3\alpha_3 + \lambda_2\alpha_2 + \lambda_1\alpha_1 + \lambda_0\alpha_0$$

of the following four functions:

$$\alpha_3(x) = \sum_{1\leq i<j<k\leq n} x_i x_j x_k, \qquad \alpha_2(x) = \sum_{1\leq i<j\leq n} x_i x_j, \qquad \alpha_1(x) = \sum_{1\leq i\leq n} x_i, \qquad \alpha_0(x)=1.$$

Since $\alpha(0) = 0$, cf. Sect. 3.1, one obtains $\lambda_0 = 0$. The function α_1 does not contribute to the quasialgebra structure $\beta = \delta\alpha$ and $\phi = \delta_2\alpha$, so that λ_1 can be chosen arbitrary. Finally, $\lambda_3 \neq 0$ since otherwise $\phi = 0$ and the corresponding algebra is associative. We obtain the functions $\alpha_{\mathbb{O}} = \alpha_3 + \alpha_2 + \alpha_1$ and $\alpha_{\mathbb{M}} = \alpha_3 + \alpha_1$ as the only possible $\mathfrak{S}_n$-invariant generating functions that define non-associative algebras. □

Note that relaxing the non-associativity condition $\phi \not\equiv 0$, will also recover the Clifford algebras $C\ell_n$ and $C\ell_{p,q}$ and the group algebra itself.

4.4. Generators and relations. Let us now give another definition of the complex algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ and of the real algebras $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$. We use a purely algebraic approach and present our algebras in terms of generators and relations.

Consider the generators (3.4). The generators of $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$ square to ±1. More precisely,

$$u_i^2 = \begin{cases} 1, & i \leq p \\ -1, & \text{otherwise,} \end{cases} \tag{4.8}$$

where $1 = u_{(0,\ldots,0)}$ is the unit. For the complex algebras $\mathbb{O}_n$ and $\mathbb{M}_n$, one can set $u_i^2 = 1$ for all i.

The rest of the relations is independent of the signature. The main difference between the series $\mathbb{O}$ and $\mathbb{M}$ is that the generators *anticommute* in the $\mathbb{O}$-case and *commute* in the $\mathbb{M}$-case:

$$u_i \cdot u_j = -u_j \cdot u_i \quad \text{in} \quad \mathbb{O}_n,\ \mathbb{O}_{p,q}, \qquad u_i \cdot u_j = u_j \cdot u_i \quad \text{in} \quad \mathbb{M}_n,\ \mathbb{M}_{p,q}. \tag{4.9}$$

The third-order relations are determined by the function ϕ and therefore these relations are the same for both series:

$$u_i \cdot (u_i \cdot u_j) = u_i^2 \cdot u_j, \tag{4.10}$$

$$u_i \cdot (u_j \cdot u_k) = -(u_i \cdot u_j) \cdot u_k, \tag{4.11}$$

where $i \neq j \neq k$ in the second relation. Note that the antiassociativity relation in (4.11) is the reason why the algebras from the $\mathbb{M}$ series generated by commuting elements, can, nevertheless, be simple.

Recall that a Clifford algebra is an algebra with n anticommuting generators satisfying the relations (4.8) and the identity of associativity. We will now give a very similar definition of the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ (as well as $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$). The associativity is replaced by the identity of quasialgebra.

Define a family of algebras $\mathcal{A}$ with n generators $u_1, \ldots, u_n$. Consider the monoid X_n of non-associative monomials in u_i and define a function $\phi : X_n \times X_n \times X_n \to \mathbb{Z}_2$ satisfying the following two properties:

(1) $\phi(u_i, u_j, u_k) = \begin{cases} 1, & \text{if } i \neq j \neq k, \\ 0, & \text{otherwise.} \end{cases}$

(2) $\phi(u \cdot u', v, w) = \phi(u, v, w) + \phi(u', v, w)$, and similar in each variable.

Such function exists and is unique. Moreover, ϕ is symmetric.

Define an algebra $\mathcal{A}^{\mathbb{C}}$ or $\mathcal{A}^{\mathbb{R}}$ (complex or real), generated by $u_1, \ldots, u_n$ that satisfies the relations (4.8) together with one of the following two relations. All the generators either anticommute: $u_i \cdot u_j = -u_j \cdot u_i$, where $i \neq j$, or commute: $u_i \cdot u_j = u_j \cdot u_i$, where $i \neq j$.

We will also assume the identity

$$u \cdot (v \cdot w) = (-1)^{\phi(u,v,w)} \, (u \cdot v) \cdot w,$$

for all monomials u, v, w.

Proposition 4.5. *If the generators anticommute, then $\mathcal{A}^{\mathbb{C}} \cong \mathbb{O}_n$ and $\mathcal{A}^{\mathbb{R}} \cong \mathbb{O}_{p,q}$. If the generators commute, then $\mathcal{A}^{\mathbb{C}} \cong \mathbb{M}_n$ and $\mathcal{A}^{\mathbb{R}} \cong \mathbb{M}_{p,q}$.*

Proof. By definition of $\mathcal{A} = \mathcal{A}^{\mathbb{C}}$ (resp. $\mathcal{A}^{\mathbb{R}}$), the elements

$$u_{i_1 \ldots i_k} = u_{i_1} \cdot (u_{i_2} \cdot (\cdots (u_{i_{k-1}} \cdot u_{i_k}) \cdots),$$

where $i_1 < i_2 < \cdots < i_k$, form a basis of $\mathcal{A}$. Therefore, $\dim \mathcal{A} = 2^n$. The linear map sending the generators of $\mathcal{A}$ to the generators (3.4) of $\mathbb{O}_n$ or $\mathbb{M}_n$ ($\mathbb{O}_{p,q}$ or $\mathbb{M}_{p,q}$, respectively) is a homomorphism, since the function ϕ corresponding to these algebras is symmetric and trilinear. It sends the above basis of $\mathcal{A}$ to that of $\mathbb{O}_n$ or $\mathbb{M}_n$ ($\mathbb{O}_{p,q}$ or $\mathbb{M}_{p,q}$, respectively). □

5. The Series $\mathbb{O}_n$ and $\mathbb{M}_n$: Properties

In this section, we study properties of the algebras of the series $\mathbb{O}$ and $\mathbb{M}$. The main result is Theorem 3 providing a criterion of simplicity. We describe the first algebras of the series and give the list of isomorphisms in lower dimensions. We also define a non-oriented graph encoding the structure of the algebra. Finally, we formulate open problems.

5.1. Criterion of simplicity. The most important property of the defined algebras that we study is the simplicity. Let us stress that we understand simplicity in the usual sense: an algebra is called *simple* if it contains no proper ideal. Note that in the case of commutative associative algebras, simplicity and division are equivalent notions, in our situation, the notion of simplicity is much weaker.

Remark 5.1. This notion should not be confounded with the notion of graded-simple algebra. The latter notion is much weaker and means that the algebra contains no graded ideal; however, this notion is rather a property of the grading and not of the algebra itself.

The following statement is the second main result of this paper. We will treat the complex and the real cases independently.

Theorem 3. (i) *The algebra* $\mathbb{O}_n$ (*resp.* $\mathbb{M}_n$) *is simple if and only if* $n \neq 4m$ (*resp.* $n \neq 4m+2$). *One also has*

$$\mathbb{O}_{4m} \cong \mathbb{O}_{4m-1} \oplus \mathbb{O}_{4m-1}, \qquad \mathbb{M}_{4m+2} \cong \mathbb{M}_{4m+1} \oplus \mathbb{M}_{4m+1}.$$

(ii) *The algebra* $\mathbb{O}_{p,q}$ *is simple if and only if one of the following conditions is satisfied*
(1) $p+q \neq 4m$,
(2) $p+q = 4m$ *and* p, q *are odd.*

(iii) *The algebra* $\mathbb{M}_{p,q}$ *is simple if and only if one of the following conditions is satisfied*
(1) $p+q \neq 4m+2$,
(2) $p+q = 4m+2$ *and* p, q *are odd.*

This theorem will be proved in Sect. 7.

The arguments developed in the proof of Theorem 3 allow us to link the complex and the real algebras in the particular cases below. Let us use the notation $\mathbb{O}_n^{\mathbb{R}}$ and $\mathbb{M}_n^{\mathbb{R}}$ when we consider the algebras $\mathbb{O}_n$ and $\mathbb{M}_n$ as 2^{n+1}-dimensional real algebras. We have the following statement.

Corollary 5.2. (i) *If* $p+q = 4m$ *and* p, q *are odd, then* $\mathbb{O}_{p,q} \cong \mathbb{O}_{p+q-1}^{\mathbb{R}}$.
(ii) *If* $p+q = 4m+2$ *and* p, q *are odd, then* $\mathbb{M}_{p,q} \cong \mathbb{M}_{p+q-1}^{\mathbb{R}}$.

This statement is proved in Sect. 7.4.

Remark 5.3. To explain the meaning of the above statement, we notice that, in the case where the complex algebras split into a direct sum, the real algebras can still be simple. In this case, all the simple real algebras are isomorphic to the complex algebra with $n-1$ generators. In particular, all the algebras $\mathbb{O}_{p,q}$ and $\mathbb{O}_{p',q'}$ with $p+q = p'+q' = 4m$ and p and p' odd are isomorphic to each other (and similarly for the $\mathbb{M}$-series). A very similar property holds for the Clifford algebras.

Theorem 3 immediately implies the following.

Corollary 5.4. *The algebras* $\mathbb{O}_n$ *and* $\mathbb{M}_n$ *with even* n *are not isomorphic.*

This implies, in particular, that the real algebras $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p',q'}$ with $p+q=p'+q'=2m$ are not isomorphic.

5.2. The first algebras of the series. Let us consider the first examples of the introduced algebras. It is natural to ask if some of the introduced algebras can be isomorphic to the other ones.

Proposition 5.5. (i) *For* $n = 3$, *one has:*

$$\mathbb{O}_{3,0} \cong \mathbb{O}_{2,1} \cong \mathbb{O}_{1,2} \ncong \mathbb{O}_{0,3}.$$

The first three algebras are isomorphic to the algebra of split-octonions, while $\mathbb{O}_{0,3} \cong \mathbb{O}$.

(ii) *For $n = 4$, one has:*

$$\mathbb{O}_{4,0} \cong \mathbb{O}_{2,2} \cong \mathbb{O}_{3,0} \oplus \mathbb{O}_{3,0}\,, \qquad \mathbb{O}_{0,4} \cong \mathbb{O}_{0,3} \oplus \mathbb{O}_{0,3}.$$

In particular, $\mathbb{O}_{4,0}$ and $\mathbb{O}_{2,2}$ are not isomorphic to $\mathbb{O}_{0,4}$.

Proof. The above isomorphisms are a combination of the general isomorphisms of type (a) and (b), see Sect. 3.3. The involved automorphisms of $(\mathbb{Z}_2)^3$ and $(\mathbb{Z}_2)^4$ are

$$\begin{array}{ll} x'_1 = x_1, & x'_1 = x_1, \\ x'_2 = x_1 + x_2, & x'_2 = x_1 + x_2, \\ x'_3 = x_1 + x_2 + x_3, & x'_3 = x_1 + x_2 + x_3, \\ & x'_4 = x_1 + x_2 + x_3 + x_4. \end{array}$$

Then, the twisting functions of the above isomorphic algebras coincide modulo coboundary. □

Let us notice that the very first algebras of the $\mathbb{O}$-series are all obtained as a combination of the algebras of octonions and split-octonions. In this sense, we do not obtain new algebras among them.

In the $\mathbb{M}$-case, we have the following isomorphism.

Proposition 5.6. *One has*

$$\mathbb{M}_{1,2} \cong \mathbb{M}_{0,3}.$$

Proof. This isomorphism can be obtained by the following automorphism of $(\mathbb{Z}_2)^3$.

$$x'_1 = x_1 + x_2 + x_3, \quad x'_2 = x_2, \quad x'_3 = x_3.$$

This algebra is not isomorphic to $\mathbb{O}_{0,3}$ or $\mathbb{O}_{3,0}$. □

The next algebras, $\mathbb{O}_5$ and $\mathbb{M}_5$, as well as all of the real algebras $\mathbb{O}_{p,q}$ and $\mathbb{M}_{p,q}$ with $p + q = 5$, are not combinations of the classical algebras. Since these algebras are simple, they are not direct sums of lower-dimensional algebras. The next statement shows that these algebras are not tensor products of classical algebras. Note that the only "candidate" for an isomorphism of this kind is the tensor product of the octonion algebra and the algebra of complex (2×2)-matrices.

Proposition 5.7. *Neither of the algebras $\mathbb{O}_5$ and $\mathbb{M}_5$ is isomorphic to the tensor product of the octonion algebra $\mathbb{O}$ and the algebra $\mathbb{C}[2]$ of complex (2×2)-matrices:*

$$\mathbb{O}_5 \not\cong \mathbb{O} \otimes \mathbb{C}[2], \qquad \mathbb{M}_5 \not\cong \mathbb{O} \otimes \mathbb{C}[2].$$

Proof. Let us consider the element $u = u_{(1,1,1,1,0)}$ in $\mathbb{O}_5$ and the element $u = u_{(1,1,0,0,0)}$ in $\mathbb{M}_5$. Each of these elements has a very big centralizer Z_u of $\dim Z_u = 24$. Indeed, the above element of $\mathbb{O}_5$ commutes with itself and with any homogeneous element u_x of the weight $|x| = 0, 1, 3, 5$ as well as 6 elements such that $|x| = 2$. The centralizer Z_u is the vector space spanned by these 24 homogeneous elements, and similarly in the $\mathbb{M}_5$ case. We will show that the algebra $\mathbb{O} \otimes \mathbb{C}[2]$ does not contain such an element.

Assume, *ad absurdum*, that an element $u \in \mathbb{O} \otimes \mathbb{C}[2]$ has a centralizer of dimension ≥ 24. Consider the subspace $\mathbb{O} \otimes 1 \oplus 1 \otimes \mathbb{C}[2]$ of the algebra $\mathbb{O} \otimes \mathbb{C}[2]$. It is

12-dimensional, so that its intersection with Z_u is of dimension at least 4. It follows that Z_u contains at least two independent elements of the form

$$z_1 = e_1 \otimes 1 + 1 \otimes m_1, \qquad z_2 = e_2 \otimes 1 + 1 \otimes m_2,$$

where e_1 and e_2 are pure imaginary octonions and m_1 and m_2 are traceless matrices.

Without loss of generality, we can assume that one of the following holds:

(1) the generic case: e_1, e_2 and m_1, m_2 are linearly independent and pairwise anticommute,
(2) $e_2 = 0$ and m_1, m_2 are linearly independent and anticommute,
(3) $m_2 = 0$ and e_1, e_2 are linearly independent and anticommute.

We will give the details of the proof in the case (1). Let us write

$$u = u_0 \otimes 1 + u_1 \otimes m_1 + u_2 \otimes m_2 + u_{12} \otimes m_1 m_2,$$

where $u_0, u_1, u_2, u_{12} \in \mathbb{O}$.

Lemma 5.8. *The element u is a linear combination of the following two elements:*

$$1 \otimes 1, \qquad e_1 \otimes m_1 + e_2 \otimes m_2 - e_1 e_2 \otimes m_1 m_2.$$

Proof. Denote by [,] the usual commutator, one has

$$\begin{aligned}[u, z_1] &= [u_0, e_1] \otimes 1 + [u_1, e_1] \otimes m_1 + ([u_2, e_1] - 2u_{12}) \otimes m_2 \\ &\quad + ([u_{12}, e_1] - 2u_2) \otimes m_1 m_2, \\ [u, z_2] &= [u_0, e_2] \otimes 1 + [u_2, e_2] \otimes m_2 \\ &\quad + ([u_1, e_2] + 2u_{12}) \otimes m_1 + ([u_{12}, e_2] + 2u_1) \otimes m_1 m_2.\end{aligned}$$

One obtains $[u_0, e_1] = [u_0, e_2] = 0$, so that u_0 is proportional to 1. Furthermore, one also obtains $[u_1, e_1] = 0$ and $[u_2, e_2] = 0$ that implies

$$u_1 = \lambda_1 \, e_1 + \mu_1 \, 1, \qquad u_2 = \lambda_2 \, e_2 + \mu_2 \, 1.$$

The equations $[u_2, e_1] - 2u_{12} = 0$ and $[u_1, e_2] + 2u_{12}$ give

$$u_{12} = \lambda_2 \, e_2 e_1 \qquad \text{and} \qquad u_{12} = -\lambda_1 \, e_1 e_2,$$

hence $\lambda_1 = \lambda_2$, since e_1 and e_2 anticommute by assumption. Finally, the equations $[u_{12}, e_1] - 2u_2 = 0$ and $[u_{12}, e_2] + 2u_1 = 0$ lead to $\mu_1 = \mu_2 = 0$.

Hence the lemma. □

In the case (1), one obtains a contradiction because of the following statement.

Lemma 5.9. *One has* $\dim Z_u \leq 22$.

Proof. Lemma 5.8 implies that the element u belongs to a subalgebra

$$\mathbb{C}[4] = \mathbb{C}[2] \otimes \mathbb{C}[2] \subset \mathbb{O} \otimes \mathbb{C}[2].$$

We use the well-known classical fact that, for an arbitrary element $u \in \mathbb{C}[4]$, the dimension of the centralizer inside $\mathbb{C}[4]$:

$$\{X \in \mathbb{C}[4] \mid [X, u] = 0\}$$

is at most 10 (i.e., the codimension is ≤ 6). Furthermore, the 4-dimensional space of the elements $e_3 \otimes 1$, where $e_3 \in \mathbb{O}$ anticommutes with e_1, e_2 is transversal to Z_u.

It follows that the codimension of Z_u is at least 10. Hence the lemma. □

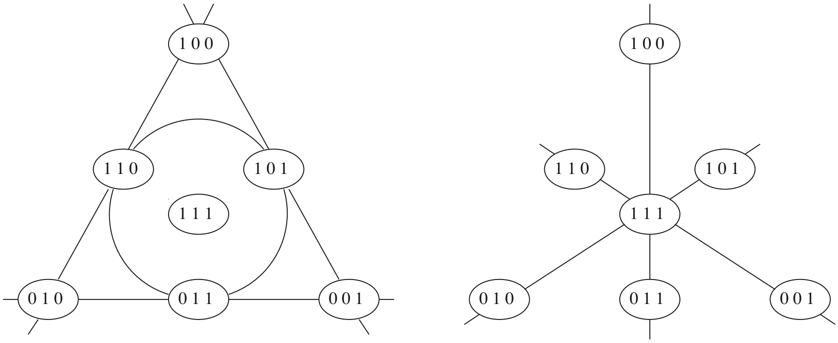

Fig. 3. The algebras $C\ell_3$ and $\mathbb{M}_3$

Cases (2) and (3) are less involved. In Case (2), u is proportional to $e_1 \otimes 1$ and one checks that $Z_u = e_1 \otimes \mathbb{C}[2] \oplus 1 \otimes \mathbb{C}[2]$ is of dimension 8. In Case (3), u is proportional to $1 \otimes m_1$ so that $Z_u = \mathbb{O} \otimes 1 \oplus \mathbb{O} \otimes m_1$ is of dimension 16. In each case, we obtain a contradiction. □

5.3. The commutation graph. We associate a non-oriented graph, that we call the commutation graph, to every twisted group algebra in the following way. The vertices of the graph are the elements of $(\mathbb{Z}_2)^n$. The (non-oriented) edges $x - y$ join the elements x and y such that u_x and u_y anticommute.

Proposition 5.10. *Given a complex algebra* $(\mathbb{C}[(\mathbb{Z}_2)^n], f)$ *with symmetric function* $\phi = \delta f$, *the commutation graph completely determines the structure of* $\mathcal{A}$.

Proof. In the case where ϕ is symmetric, formula (4.2) and Proposition 3.7 imply that the graph determines the structure of the algebra $\mathcal{A}$, up to signature. □

This means two complex algebras, $\mathcal{A}$ and $\mathcal{A}'$, corresponding to the same commutation graph are isomorphic. Conversely, two algebras, $\mathcal{A}$ and $\mathcal{A}'$ with different commutation graphs, are not isomorphic as $(\mathbb{Z}_2)^n$-graded algebras. However, we do not know if there might exist an isomorphism that does not preserve the grading.

Example 5.11. The algebra $\mathbb{M}_3$ is the first non-trivial algebra of the series $\mathbb{M}_n$. The corresponding commutation graph is presented in Fig. 3, together with the graph of the Clifford algebra $C\ell_3$.

The algebra $C\ell_3$ is not simple: $C\ell_3 = \mathbb{C}[2] \oplus \mathbb{C}[2]$. It contains a central element $u_{(1,1,1)}$ corresponding to a "singleton" in Fig. 3.

Remark 5.12. (a) The defined planar graph is *dual trivalent*, that is, every edge represented by a projective line or a circle, see Fig. 3, contains exactly 3 elements. Indeed, any three homogeneous elements u_x, u_y and u_{x+y} either commute or anticommute with each other. This follows from the tri-linearity of ϕ.

(b) We also notice that the superposition of the graphs of $C\ell_n$ and $\mathbb{M}_n$ is precisely the graph of the algebra $\mathbb{O}_n$. We thus obtain the following "formula": $C\ell + \mathbb{M} = \mathbb{O}$.

Example 5.13. The commutation graph of the algebra $\mathbb{M}_4$ is presented in Fig. 4.

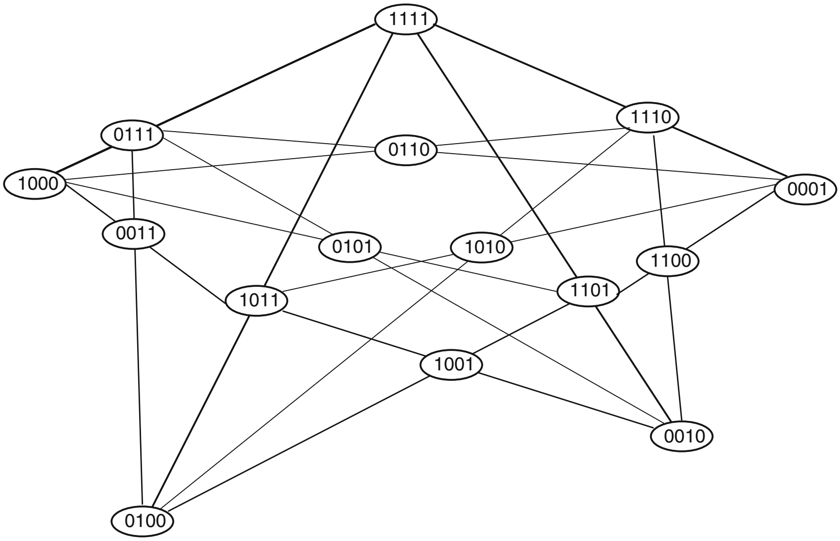

Fig. 4. The commutation graph of $\mathbb{M}_4$

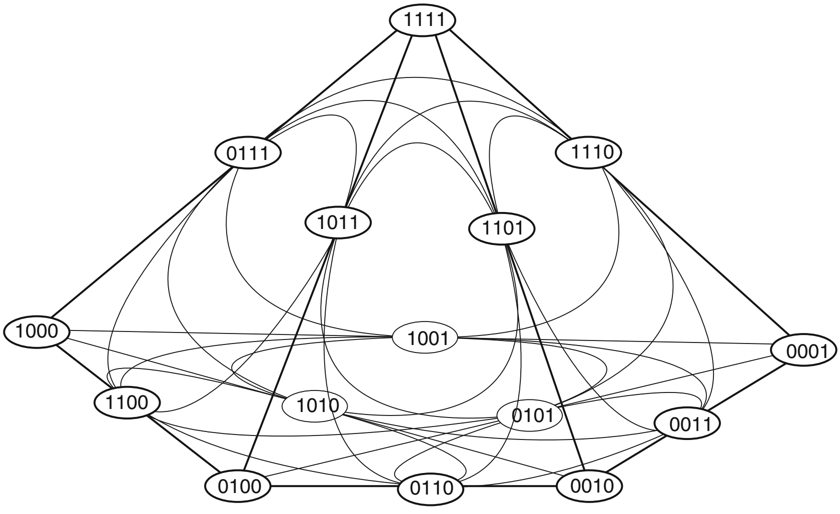

Fig. 5. The commutation graph of $C\ell_4$

The commutation graph of the Clifford algebra $C\ell_4$ is is presented in Fig. 5. Note that both algebras, $\mathbb{M}_4$ and $C\ell_4$ are simple. The superposition of the graphs of $\mathbb{M}_4$ and $C\ell_4$ cancels all the edges from $(1, 1, 1, 1)$. Therefore, the element $(1, 1, 1, 1)$ is a singleton in the graph of the algebra $\mathbb{O}_4$. This corresponds to the fact that $u_{(1,1,1,1)}$ in $\mathbb{O}_4$ is central, in particular, $\mathbb{O}_4$ is not simple.

The planar graph provides a nice way to visualize the algebra $(\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f)$.

6. Generating Functions: Existence and Uniqueness

In this section we prove Theorem 2 and its corollaries. Our main tool is the notion of generating function. We show that the structure of all the algebras we consider in this paper is determined (up to signature) by a single function of one argument $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$. This of course simplifies the understanding of these algebras.

6.1. Existence of a generating function. Given a $(\mathbb{Z}_2)^n$-graded quasialgebra, let us prove that there exists a generating function α if and only if the ternary map ϕ is symmetric.

The condition that ϕ is symmetric is of course necessary for existence of α, cf. formula (3.2), let us prove that this condition is, indeed, sufficient.

Lemma 6.1. *If ϕ is symmetric, then β is a 2-cocycle: $\delta\beta = 0$.*

Proof. If ϕ is symmetric then the identity (4.2) is satisfied. In particular, the sum of the two expressions of ϕ gives:

$$\beta(x+y,\ z) + \beta(x,\ y+z) + \beta(x,y) + \beta(y,z) = 0,$$

which is nothing but the 2-cocycle condition $\delta\beta = 0$. □

Using the information about the second cohomology space $H^2((\mathbb{Z}_2)^n; \mathbb{Z}_2)$, as in the proof of Proposition 3.7, we deduce that β is of the form

$$\beta(x,y) = \delta\alpha(x,y) + \sum_{i \in I} x_i y_i + \sum_{(k,\ell) \in J} x_k y_\ell,$$

where $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is an arbitrary function and where I is a subset of $\{1, \ldots, n\}$ and J is a subset of $\{(k,\ell) \mid k < \ell\}$. Indeed, the second and the third terms are the most general non-trivial 2-cocycles on $(\mathbb{Z}_2)^n$ with coefficients in $\mathbb{Z}_2$.

Furthermore, the function β satisfies two properties: it is symmetric and $\beta(x,x) = 0$. The second property implies that β does not contain the terms $x_i y_i$. The symmetry of β means that whenever there is a term $x_k y_\ell$, there is $x_\ell y_k$, as well. But, $x_k y_\ell + x_\ell y_k$ is a coboundary of $x_k x_\ell$. We proved that $\beta = \delta\alpha$, which is equivalent to the identity (3.1).

Finally, using the equality (4.2), we also obtain the identity (3.2).

Theorem 2 is proved.

6.2. Generating functions are cubic. In this section, we prove Proposition 4.1. We show that a function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is a generating function of a $(\mathbb{Z}_2)^n$-graded quasialgebra if and only if α is a polynomial of degree ≤ 3.

The next statement is an application of the pentagonal diagram in Fig. 2.

Lemma 6.2. *A generating function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ satisfies the equation $\delta_3\alpha = 0$, where the map δ_3 is defined by*

$$\begin{aligned}\delta_3\alpha\,(x,y,z,t) := {} & \alpha(x+y+z+t) \\ & +\alpha(x+y+z) + \alpha(x+y+t) + \alpha(x+z+t) + \alpha(y+z+t) \\ & +\alpha(x+y)+\alpha(x+z)+\alpha(x+t)+\alpha(y+z)+\alpha(y+t)+\alpha(z+t) \\ & +\alpha(x) + \alpha(y) + \alpha(z) + \alpha(t). \end{aligned} \tag{6.1}$$

Proof. This follows immediately from the fact that ϕ is a 3-cocycle: substitute (3.2) to the equation $\delta\phi = 0$ to obtain $\delta_3\alpha = 0$. □

The following statement characterizes polynomials of degree ≤ 3.

Lemma 6.3. *A function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is a polynomial of degree ≤ 3 if and only if $\delta_3\alpha = 0$.*

Proof. This is elementary, see also [14,30]. □

Proposition 4.1 is proved.

Let us now prove Corollary 4.2. If the map ϕ is symmetric, then Theorem 2 implies the existence of the generating function α. The map ϕ is then given by (3.2). One checks by an elementary calculation that

$$\phi(x+y,z,t) + \phi(x,z,t) + \phi(y,z,t) = \delta_3\alpha(x,y,z,t).$$

By Lemma 6.2, one has $\delta_3\alpha = 0$. It follows that ϕ is trilinear.

Furthermore, from (4.2), we deduce that ϕ is alternate.

Corollary 4.2 is proved.

6.3. Uniqueness of the generating function. Let us show that there is a canonical way to choose a generating function.

Lemma 6.4. (i) *Given a $(\mathbb{Z}_2)^n$-graded quasialgebra $\mathcal{A}$ with a generating function, one can choose the generating function in such a way that it satisfies*

$$\begin{cases} \alpha(0) = 0, \\ \alpha(x) = 1, \quad |x| = 1. \end{cases} \tag{6.2}$$

(ii) *There exists a unique generating function of $\mathcal{A}$ satisfying (6.2).*

Proof. Part (i). Every generating function α vanishes on the zero element $0 = (0, \ldots, 0)$, cf. Sect. 3.1. Furthermore, a generating function corresponding to a given algebra $\mathcal{A}$, is defined up to a 1-cocycle on $(\mathbb{Z}_2)^n$. Indeed, the functions $\beta = \delta\alpha$ and $\phi = \delta_2\alpha$ that define the quasialgebra structure do not change if one adds a 1-cocycle to α. Since every 1-cocycle is a linear function, we obtain

$$\alpha(x) \sim \alpha(x) + \sum_{1 \leq i \leq n} \lambda_i \, x_i .$$

One therefore can normalize α in such a way that $\alpha(x) = 1$ for all x such that $|x| = 1$.

Part (ii). The generating function normalized in this way is unique. Indeed, any other function, say α', satisfying (6.2) differs from α by a polynomial of degree ≥ 2, so that $\alpha - \alpha'$ cannot be a 1-cocycle. Therefore, $\beta' \neq \beta$ which means the quasialgebra structure is different. □

We will assume the normalization (6.2) in the sequel, whenever we speak of *the* generating function corresponding to a given algebra.

Let us now consider an algebra $\mathcal{A}$ with n generators $u_1, \ldots, u_n$. The group of permutations $\mathfrak{S}_n$ acts on $\mathcal{A}$ by permuting the generators.

Corollary 6.5. *If the group of permutations $\mathfrak{S}_n$ acts on $\mathcal{A}$ by automorphisms, then the corresponding generating function α is $\mathfrak{S}_n$-invariant.*

Proof. Let α be a generating function. Since the algebra $\mathcal{A}$ is stable with respect to the $\mathfrak{S}_n$-action, the function $\alpha \circ \sigma$ is again a generating function. If, moreover, α satisfies (6.2), then $\alpha \circ \sigma$ also satisfies this condition. The uniqueness Lemma 6.4 implies that $\alpha \circ \sigma = \alpha$. □

Note that the converse statement holds in the complex case, but fails in the real case.

6.4. From the generating function to the twisting function. Given an arbitrary polynomial map $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ of $\deg \alpha \leq 3$ such that $\alpha(0) = 0$, there is a simple way to associate a twisting function f such that $(\mathbb{K}[(\mathbb{Z}_2)^n], f)$ admits α as a generating function.

Proposition 6.6. *There exists a twisting function f satisfying the property*

$$f(x, x) = \alpha(x). \tag{6.3}$$

Proof. Let us give an explicit formula for a twisting function f. The procedure is linear, we associate to every monomial in α a function in two variables via the following rule:

$$\begin{aligned} x_i x_j x_k &\longmapsto x_i x_j y_k + x_i y_j x_k + y_i x_j x_k, \\ x_i x_j &\longmapsto x_i y_j, \\ x_i &\longmapsto x_i y_i, \end{aligned} \tag{6.4}$$

where $i < j < k$. □

7. Proof of the Simplicity Criterion

In this section, we prove Theorem 3. We use the notation $\mathcal{A}$ to refer to any of the algebras $\mathbb{O}_n, \mathbb{O}_{p,q}$ and $\mathbb{M}_n, \mathbb{M}_{p,q}$.

7.1. The idea of the proof. Our proof of simplicity of a twisted group algebra $\mathcal{A}$ will be based on the following lemma.

Lemma 7.1. *If for every homogeneous element u_x in $\mathcal{A}$ there exists an element u_y in $\mathcal{A}$ such that u_x and u_y anticommute, then $\mathcal{A}$ is simple.*

Proof. Let us suppose that there exists a nonzero proper two-sided ideal $\mathcal{I}$ in $\mathcal{A}$. Every element u in $\mathcal{I}$ is a linear combination of some homogeneous elements of $\mathcal{A}$. We write

$$u = \lambda_1 \, u_{x_1} + \cdots + \lambda_k \, u_{x_k}.$$

Among all the elements of $\mathcal{I}$ we choose an element such that the number k of homogeneous components is the smallest possible. We can assume that $k \geq 2$, otherwise u is homogeneous and therefore u^2 is non-zero and proportional to 1, so that $\mathcal{I} = \mathcal{A}$. In addition, up to multiplication by u_{x_1} and scalar normalization we can assume that

$$u = 1 + \lambda_2 \, u_{x_2} + \cdots + \lambda_k \, u_{x_k}.$$

If there exists an element $u_y \in \mathcal{A}$ anticommuting with u_{x_2} then one obtains that $u \cdot u_y - u_y \cdot u$ is a nonzero element in $\mathcal{I}$ with a shorter decomposition into homogeneous components. This is a contradiction with the choice of u. Therefore, $\mathcal{A}$ has no proper ideal. □

We now need to study central elements in $\mathcal{A}$, i.e., the elements commuting with every element of $\mathcal{A}$.

7.2. Central elements. In this section we study the *commutative center* $\mathcal{Z}(\mathcal{A})$ of $\mathcal{A}$, i.e.,

$$\mathcal{Z}(\mathcal{A}) = \{w \in \mathcal{A} |\ w \cdot a = a \cdot w,\ \text{ for all } a \in \mathcal{A}\}.$$

Note that, in the case where $\mathcal{A}$ admits a generating function, formula (4.2) implies that the commutative center is contained in the associative nucleus of $\mathcal{A}$, so that the commutative center coincides with the usual notion of center, see [31], p. 136 for more details.

The unit 1 of $\mathcal{A}$ is obviously an element of the center. We say that $\mathcal{A}$ has a trivial center if $\mathcal{Z}(\mathcal{A}) = \mathbb{K}\,1$.

Consider the following particular element:

$$z = (1, \dots, 1)$$

in $(\mathbb{Z}_2)^n$, with all the components equal to 1, and the associated homogeneous element u_z in $\mathcal{A}$.

Lemma 7.2. *The element u_z in $\mathcal{A}$ is central if and only if*

(1) *$n = 4m$ in the cases $\mathcal{A} = \mathbb{O}_n, \mathbb{O}_{p,q}$;*
(2) *$n = 4m + 2$ in the cases $\mathcal{A} = \mathbb{M}_n, \mathbb{M}_{p,q}$.*

Proof. The element u_z in $\mathcal{A}$ is central if and only if for all $y \in (\mathbb{Z}_2)^n$ one has $\beta(y, z) = 0$. We use the generating function α. Recall that $\beta(y, z) = \alpha(y + z) + \alpha(y) + \alpha(z)$. The value $\alpha(x)$ depends only on the weight $|x|$, see Table (4.7). For every y in $\mathbb{Z}_2^n$, one has

$$|z + y| = |z| - |y|.$$

Case (1). According to Table (4.7), one has $\alpha(x) = 0$ if and only if $|x|$ is a multiple of 4.

Assume $n = 4m$. One gets $\alpha(z) = 0$ and for every y one has $\alpha(y) = 0$ if and only if $\alpha(y+z) = 0$. So, in that case, one always has $\alpha(y) = \alpha(y+z)$ and therefore $\beta(y, z) = 0$.

Assume $n = 4m + r$, $r = 1, 2$ or 3. We can always choose an element y such that $|y| = |r - 2| + 1$. We get

$$\alpha(z) = \alpha(y) = \alpha(y + z) = 1.$$

Hence, $\beta(y, z) = 1$. This implies that u_z is not central.

Case (2). According to Table (4.7), one has $\alpha(x) = 0$ if and only if $|x|$ is not equal to 1 mod 4.

Assume $n = 4m + 2$. One gets $\alpha(z) = 0$ and for every y one has $|y| = 1 \mod 4$ if and only if $|y + z| = 1 \mod 4$. So, in that case, one always has $\alpha(y) = \alpha(y + z)$ and therefore $\beta(y, z) = 0$.

Assume $n = 4m + r$, $r = 0, 1$ or 3. We choose the element $y = (1, 0, \dots, 0)$, if $r = 0, 3$, or $y = (1, 1, 0, \dots, 0)$, if $r = 1$. We easily compute $\beta(y, z) = 1$. This implies that u_z is not central. □

Let us consider the case where u_z is not central.

Lemma 7.3. *If u_z is not central, then $\mathcal{A}$ has a trivial center.*

Proof. It suffices to prove that for every homogeneous element u_x in $\mathcal{A}$, that is not proportional to 1, there exists an element u_y in $\mathcal{A}$, such that u_x and u_y anticommute. Indeed, if u is central, then each homogeneous component of u is central.

Let us fix $x \in (\mathbb{Z}_2)^n$ and the corresponding homogeneous element $u_x \in \mathcal{A}$, such that x is neither 0, nor z. We want to find an element $y \in (\mathbb{Z}_2)^n$ such that $\beta(x, y) = 1$ or equivalently u_x anticommutes with u_y. Using the invariance of the functions α and β under permutations of the coordinates, we can assume that x is of the form

$$x = (1, \dots, 1, 0, \dots, 0),$$

where first $|x|$ entries are equal to 1 and the last entries are equal to 0. We assume $0 < |x| < n$, so that, x starts with 1 and ends by 0.

Case $\mathcal{A} = \mathbb{O}_n$ or $\mathbb{O}_{p,q}$. If $|x| \neq 4\ell$, then we use exactly the same arguments as in the proof of Lemma 7.2 in order to find a suitable y (one can also take one of the elements $y = (1, 0, \dots, 0)$ or $y = (0, \dots, 0, 1)$). Assume $|x| = 4\ell$. Consider the element

$$y = (0, 1, \dots, 1, 0, \dots, 0),$$

with $|y| = |x|$. One has $\alpha(x) = \alpha(y) = 0$ and $\alpha(x+y) = 1$. So we also have $\beta(x, y) = 1$ and deduce u_x anticommutes with u_y.

Case $\mathcal{A} = \mathbb{M}_n$ or $\mathbb{M}_{p,q}$. Similarly to the proof of Lemma 7.2, if $k \neq 4\ell + 2$ then we can find a y such that u_y anticommutes with u_x. If $k = 4\ell + 2$ then $\alpha(x) = 0$. The element $y = (0, \dots, 0, 1)$ satisfies $\alpha(y) = 1$ and $\alpha(x + y) = 0$. □

Consider now the case where u_z is a central element. There are two different possibilities: ${u_z}^2 = 1$, or ${u_z}^2 = -1$.

Lemma 7.4. *If $u_z \in \mathcal{A}$ is a central element and if ${u_z}^2 = 1$, then the algebra splits into a direct sum of two subalgebras:*

$$\mathcal{A} = \mathcal{A}^+ \oplus \mathcal{A}^-,$$

where $\mathcal{A}^+ := \mathcal{A} \cdot (1 + u_z)$ and $\mathcal{A}^- := \mathcal{A} \cdot (1 - u_z)$.

Proof. Using ${u_z}^2 = 1$, one immediately obtains

$$\begin{aligned} (1 \pm u_z)^2 &= 2\,(1 \pm u_z), \\ (1 + u_z) \cdot (1 - u_z) &= 0. \end{aligned} \tag{7.1}$$

In addition, using the expression of ϕ in terms of β given in (4.2) and the fact that $\beta(\cdot, z) = 0$, one deduces that $\phi(\cdot, \cdot, z) = 0$ and thus $a \cdot (b \cdot u_z) = (a \cdot b) \cdot u_z$ for all $a, b \in \mathcal{A}$. It follows that

$$(a \cdot (1 \pm u_z)) \cdot (b \cdot (1 \pm u_z)) = (a \cdot b) \cdot ((1 \pm u_z) \cdot (1 \pm u_z)) \tag{7.2}$$

for all $a, b \in \mathcal{A}$. This expression, together with the above computations (7.1), shows that $\mathcal{A}^+$ and $\mathcal{A}^-$ are, indeed, two subalgebras of $\mathcal{A}$ and that they satisfy $\mathcal{A}^+ \cdot \mathcal{A}^- = \mathcal{A}^- \cdot \mathcal{A}^+ = 0$. Moreover, for any $a \in \mathcal{A}$, one can write

$$a = \frac{1}{2}\, a \cdot (1 + u_z) + \frac{1}{2}\, a \cdot (1 - u_z).$$

This implies the direct sum decomposition $\mathcal{A} = \mathcal{A}^+ \oplus \mathcal{A}^-$. □

Notice that the elements $\frac{1}{2}\,(1 + u_z)$ and $\frac{1}{2}\,(1 - u_z)$ are the units of $\mathcal{A}^+$ and $\mathcal{A}^-$, respectively.

7.3. Proof of Theorem 3, part (i). If $n \neq 4m$, then by Lemma 7.1 and Lemma 7.3 we immediately deduce that $\mathbb{O}_n$ is simple.

If $n = 4m$, then u_z is central and, in the complex case, one has $u_z^2 = 1$. By Lemma 7.2 and Lemma 7.4, we immediately deduce that $\mathbb{O}_n$ is not simple and one has

$$\mathbb{O}_{4m} = \mathbb{O}_{4m} \cdot (1 + u_z) \oplus \mathbb{O}_{4m} \cdot (1 - u_z),$$

where $z = (1, \ldots, 1) \in (\mathbb{Z}_2)^n$. It remains to show that the algebras $\mathbb{O}_{4m-1}$ and $\mathbb{O}_{4m} \cdot (1 \pm u_z)$ are isomorphic. Indeed, using the computations (7.1) and (7.2), one checks that the map

$$u_x \longmapsto \frac{1}{2}\, u_{(x,0)} \cdot (1 \pm u_z),$$

where $x \in (\mathbb{Z}_2)^{n-1}$, is the required isomorphism.

The proof in the case of $\mathbb{M}_n$ is completely similar.

7.4. Proof of Theorem 3, part (ii). The algebras $\mathbb{O}_{p,q}$ with $p+q \neq 4m$ and the algebras $\mathbb{M}_{p,q}$ with $p+q \neq 4m+2$ are simple because their complexifications are.

If now u_z is central, then the property $u_z^2 = 1$ or -1 becomes crucial. Using the expressions for $f_{\mathbb{O}}$ or $f_{\mathbb{M}}$, one computes

$$\begin{aligned} f_{\mathbb{O}_{p,q}}(z, z) &= \sum_{i<j<k} z_i z_j z_k \;\; + \sum_{i \leq j} z_i z_j + \sum_{1 \leq i \leq p} z_i \\ &= \frac{n(n-1)(n-2)}{6} + \frac{n(n+1)}{2} + p \\ &= p, \quad \mod 2. \end{aligned}$$

And similarly, one obtains $f_{\mathbb{M}_{p,q}}(z, z) = p$. It follows that $u_z^2 = (-1)^p$.

If p is even, then Lemma 7.2 just applied guarantees that $\mathcal{A}$ is not simple.

Finally, if u_z is central and p is odd, then $u_z^2 = -1$.

Lemma 7.5. *If u_z is central and p is odd, then*

$$\mathbb{O}_{p,q} \cong \mathbb{O}_{p,q-1} \otimes \mathbb{C}, \qquad \mathbb{M}_{p,q} \cong \mathbb{M}_{p,q-1} \otimes \mathbb{C}.$$

Proof. We construct an explicit isomorphism from $\mathbb{O}_{p,q-1} \otimes \mathbb{C}$ to $\mathbb{O}_{p,q}$ as follows:

$$\begin{aligned} u_x \otimes 1 &\longmapsto u_{(x,0)}, \\ u_x \otimes \sqrt{-1} &\longmapsto u_{(x,0)} \cdot u_z\,, \end{aligned}$$

for all $x \in (\mathbb{Z}_2)^{n-1}$. We check that the above map is indeed an isomorphism of algebras by noticing that $f_{\mathbb{O}_{p,q}}((x, 0), (y, 0)) = f_{\mathbb{O}_{p,q-1}}(x, y)$. □

Let us show that Lemma 7.5 implies that the (real) algebras $\mathbb{O}_{p,q}$ with $p+q = 4m$ and p odd and the algebras $\mathbb{M}_{p,q}$ with $p+q = 4m+2$ and p odd are simple. Indeed,

$$\mathbb{O}_{p,q-1} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{O}_{p+q-1},$$

viewed as a real algebra. We then use the following well-known fact. A simple unital complex algebra viewed as a real algebra remains simple.

The proof of Theorem 3 is complete.

Lemma 7.5 also implies Corollary 5.2.

8. Hurwitz-Radon Square Identities

In this section, we use the algebras $\mathbb{O}_n$ (and, in the real case, $\mathbb{O}_{0,n}$) to give explicit formulæ for solutions of a classical problem of products of squares. Recall that the octonion algebra is related to the 8-square identity. In an arbitrary commutative ring, the product $(a_1^2 + \cdots + a_8^2)\,(b_1^2 + \cdots + b_8^2)$ is again a sum of 8 squares $c_1^2 + \cdots + c_8^2$, where c_k are explicitly given by bilinear forms in a_i and b_j with coefficients ±1, see, e.g., [11]. This identity is equivalent to the fact that $\mathbb{O}$ is a composition algebra, that is, for any $a, b \in \mathbb{O}$, the norm of the product is equal to the product of the norms:

$$\mathcal{N}(a \cdot b) = \mathcal{N}(a)\,\mathcal{N}(b). \tag{8.1}$$

Hurwitz proved that there is no similar N-square identity for $N > 8$, as there is no composition algebra in higher dimensions.

The celebrated Hurwitz-Radon Theorem [19,27] establishes the maximal number r, as a function of N, such that there exists an identity

$$\left(a_1^2 + \cdots + a_N^2\right)\left(b_1^2 + \cdots + b_r^2\right) = \left(c_1^2 + \cdots + c_N^2\right), \tag{8.2}$$

where c_k are bilinear forms in a_i and b_j. The theorem states that $r = \rho(N)$ is the maximal number, where $\rho(N)$ is the Hurwitz-Radon function defined as follows. Write N in the form $N = 2^{4m+\ell}\,N'$, where N' is odd and $\ell = 0, 1, 2$ or 3, then

$$\rho(N) := 8m + 2^{\ell}.$$

It was proved by Gabel [16] that the bilinear forms c_k can be chosen with coefficients ±1. Note that the only interesting case is $N = 2^n$ since the general case is an immediate corollary of this particular one. We refer to [28,29] for the history, results and references.

In this section, we give explicit formulæ for the solution to the Hurwitz-Radon equation, see also [22] for further development within this framework.

8.1. The explicit solution. We give an explicit solution for Hurwitz-Radon equation (8.2) for any $N = 2^n$ with n not a multiple of 4.

We label the a-variables and the c-variables by elements of $(\mathbb{Z}_2)^n$. In order to describe the labeling of the b-variables, we consider the following particular elements of $(\mathbb{Z}_2)^n$:

$$\begin{aligned}
e_0 &:= (0, 0, \ldots, 0),\\
\overline{e_0} &:= (1, 1, \ldots, 1),\\
e_i &:= (0, \ldots, 0, 1, 0, \ldots, 0),\ \text{where 1 occurs at the } i^{\text{th}} \text{ position},\\
\overline{e_i} &:= (1, \ldots, 1, 0, 1, \ldots, 1),\ \text{where 0 occurs at the } i^{\text{th}} \text{ position},
\end{aligned}$$

for all $1 \leq i \leq n$ and $1 < j \leq n$. We then introduce the following subset H_n of $(\mathbb{Z}_2)^n$:

$$\begin{aligned}
H_n &= \{e_i, \overline{e_i},\ 1 \leq i \leq n\}, \quad \text{for } n = 1 \mod 4,\\
H_n &= \{e_i, e_1 + e_j,\ 0 \leq i \leq n,\ 1 < j \leq n\}, \quad \text{for } n = 2 \mod 4,\\
H_n &= \{e_i, \overline{e_i},\ 0 \leq i \leq n\}, \quad \text{for } n = 3 \mod 4.
\end{aligned} \tag{8.3}$$

In each case, the subset H_n contains exactly $\rho(2^n)$ elements.

We write the Hurwitz-Radon identity in the form

$$\left(\sum_{x \in (\mathbb{Z}_2)^n} a_x^2\right)\left(\sum_{x \in H_n} b_x^2\right) = \sum_{x \in (\mathbb{Z}_2)^n} c_x^2.$$

We will establish the following.

Theorem 4. *The bilinear forms*

$$c_x = \sum_{y \in H_n} (-1)^{f_{\mathbb{O}}(x+y,y)} \, a_{x+y} b_y, \tag{8.4}$$

where $f_{\mathbb{O}}$ is the twisting function of the algebra $\mathbb{O}_n$ defined in (1.3)*, are a solution to the Hurwitz-Radon identity.*

In order to prove Theorem 4 we will need to define the natural norm on $\mathbb{O}_n$.

8.2. The Euclidean norm. Assume that a twisted group algebra $\mathcal{A} = (\mathbb{K}[(\mathbb{Z}_2)^n], f)$ is equipped with a generating function α. Assume furthermore that the twisting function satisfies $f(x,x) = \alpha(x)$, as in (6.3).

The involution on $\mathcal{A}$ is defined for every $a = \sum_{x \in (\mathbb{Z}_2)^n} a_x \, u_x$, where $a_x \in \mathbb{C}$ (or in $\mathbb{R}$) are scalar coefficients and u_x are the basis elements, by the formula

$$\bar{a} = \sum_{x \in (\mathbb{Z}_2)^n} (-1)^{\alpha(x)} \, a_x \, u_x .$$

We then define the following norm of an element $a \in \mathcal{A}$:

$$\mathcal{N}(a) := (a \cdot \bar{a})_0 \, .$$

Proposition 8.1. *The above norm is nothing but the Euclidean norm in the standard basis:*

$$\mathcal{N}(a) = \sum_{x \in (\mathbb{Z}_2)^n} a_x^2. \tag{8.5}$$

Proof. One has

$$\mathcal{N}(a) = \sum (-1)^{\alpha(x)} \, a_x^2 \, u_x \cdot u_x = \sum (-1)^{\alpha(x)+f(x,x)} \, a_x^2.$$

The result then follows from the assumption $f(x,x) = \alpha(x)$. □

The following statement is a general criterion for $a, b \in \mathcal{A}$ to satisfy the composition equation (8.1). This criterion will be crucial for us to establish the square identities.

Proposition 8.2. *Elements $a, b \in \mathcal{A}$ satisfy (8.1), if and only if for all $x, y, z, t \in (\mathbb{Z}_2)^2$ such that*

$$x + y + z + t = 0, \qquad (x,y) \neq (z,t), \qquad a_x \, b_y \, a_z \, b_t \neq 0,$$

one has $\alpha(x+z) = \alpha(y+t) = 1$.

Proof. Calculating the left-hand-side of (8.1), we obtain

$$\mathcal{N}(a \cdot b) = \sum_{x+y+z+t=0} (-1)^{f(x,y)+f(z,t)} \, a_x \, b_y \, a_z \, b_t .$$

According to (8.5), the product of the norm in the right-hand-side is:

$$\mathcal{N}(a) \, \mathcal{N}(b) = \sum_{x,y} a_x^2 \, b_y^2.$$

It follows that the condition (8.1) is satisfied if and only if

$$f(x,y)+f(z,t)+f(x,t)+f(z,y)=1,$$

whenever $(x,y)\neq(z,t)$ and $a_x\,b_y\,a_z\,b_t\neq 0$.

Taking into account the linearity of the function (6.4) and substituting $t=x+y+z$, one finally gets (after cancellation):

$$f(z,x)+f(x,z)+f(x,x)+f(z,z)=1.$$

In terms of the function α this is exactly the condition $\alpha(x+z)=1$. Hence the result. □

8.3. Proof of Theorem 4. Let us apply Proposition 8.2 to the case of the algebra $\mathbb{O}_n$.

Given the variables $(a_x)_{x\in(\mathbb{Z}_2)^n}$ and $(b_x)_{x\in H_n}$, where H_n is the subset defined in (8.3), form the following vectors in $\mathbb{O}_n$:

$$a=\sum_{x\in(\mathbb{Z}_2)^n}a_x\,u_x,\qquad b=\sum_{y\in H_n}b_y\,u_y.$$

Taking two distinct elements $y,t\in H_n$ one always has $\alpha_{\mathbb{O}}(y+t)=1$. Therefore, from Proposition 8.2 one deduces that $\mathcal{N}(a)\mathcal{N}(b)=\mathcal{N}(a\cdot b)$. Writing this equality in terms of coordinates of the three elements a, b and $c=a\cdot b$, one obtains the result.

Theorem 4 is proved.

Let us give one more classical identity that can be realized in the algebra $\mathbb{O}_n$.

Example 8.3. The most obvious choice of two elements $a,b\in\mathbb{O}_n$ that satisfy the condition (8.1) is: $a=a_0\,u_0+\sum a_i\,u_i$ and $b=b_0\,u_0+\sum b_i\,u_i$. One immediately obtains in this case the following elementary but elegant identity:

$$(a_0^2+\cdots+a_n^2)\,(b_0^2+\cdots+b_n^2)=(a_0\,b_0+\cdots+a_n\,b_n)^2+\sum_{0\le i<j\le n}(a_i\,b_j-b_j\,a_i)^2,$$

for an arbitrary n, known as the Lagrange identity.

9. Relation to Code Loops

The constructions of the algebras that we use in this work are closely related to some constructions in the theory of Moufang Loops. In particular, they lead to examples of Code Loops [18]. In this section, we apply our approach in order to obtain an explicit construction of the famous Parker Loop.

The loop of the basis elements. The structure of loop is a nonassociative version of a group (see, e.g., [17]).

Proposition 9.1. *The basis elements together with their opposites, $\{\pm u_x, x\in(\mathbb{Z}_2)^n\}$, in a twisted algebra $(\mathbb{K}\left[(\mathbb{Z}_2)^n\right], f)$, form a loop with respect to the multiplication rule. Moreover, this loop is a Moufang loop whenever $\phi=\delta f$ is symmetric.*

Proof. The fact that the elements $\pm u_x$ form a loop is evident. If the function $\phi = \delta f$ is symmetric, then this loop satisfies the Moufang identity:

$$u \cdot (v \cdot (u \cdot w)) = ((u \cdot v) \cdot u) \cdot w$$

for all u, v, w. Indeed, the symmetry of ϕ implies that ϕ is also trilinear and alternate, see Corollary 4.2. □

Let us mention that the Moufang loops associated with the octonions and split-octonions are important classical objects invented by Coxeter [12].

Code loops. The notion of code loops has been introduced by Griess, [18]. We recall the construction and main results. A doubly even binary code is a subspace V in $(\mathbb{Z}_2)^n$ such that any vectors in V has weight a multiple of 4. It was shown that there exists a function f from $V \times V$ to $\mathbb{Z}_2$, called a *factor set* in [18], satisfying

(1) $f(x, x) = \frac{1}{4}|x|$,
(2) $f(x, y) + f(y, x) = \frac{1}{2}|x \cap y|$,
(3) $\delta f(x, y, z) = |x \cap y \cap z|$,

where $|x \cap y|$ (resp. $|x \cap y \cap z|$) is the number of nonzero coordinates in both x and y (resp. all of x, y, z). The associated code loop $\mathcal{L}(V)$ is the set $\{\pm u_x, x \in V\}$ together with the multiplication law

$$u_x \cdot u_y = (-1)^{f(x,y)}\, u_{x+y}.$$

The most important example of code loop is the Parker loop that plays an important rôle in the theory of sporadic finite simple groups. The Parker loop is the code loop obtained from the Golay code. This code can be described as the 12-dimensional subspace of $(\mathbb{Z}_2)^{24}$ given as the span of the rows of the following matrix, see [10]:

$$G = \begin{pmatrix}
1 & & & & & & & & & & & & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
& 1 & & & & & & & & & & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
& & 1 & & & & & & & & & & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
& & & 1 & & & & & & & & & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
& & & & 1 & & & & & & & & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
& & & & & 1 & & & & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
& & & & & & 1 & & & & & & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
& & & & & & & 1 & & & & & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
& & & & & & & & 1 & & & & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
& & & & & & & & & 1 & & & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
& & & & & & & & & & 1 & & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
& & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

An explicit formula for the Parker loop. Let us now give the generating function of the Parker loop. We identify the Golay code with the space $(\mathbb{Z}_2)^{12}$, in such a way that the i^{th} row of the matrix G, denoted ℓ_i, is identified with the i^{th} standard basic vector $e_i = (0, \dots, 0, 1, 0 \dots, 0)$ of $(\mathbb{Z}_2)^{12}$. As previously, we write $u_i = u_{e_i} = u_{\ell_i}$ the corresponding vector in the Parker loop. The coordinates of an element $x \in (\mathbb{Z}_2)^{12}$ are denoted by $(x_1, \dots, x_{11}, x_{12})$.

Proposition 9.2. *The Parker loop is given by the following generating function α from $(\mathbb{Z}_2)^{12}$ to $\mathbb{Z}_2$:*

$$\alpha_G(x) = \sum_{1 \leq i \leq 11} x_i x_{i+1}\,(x_{i+5} + x_{i+8} + x_{i+9}) + x_i x_{i+2}\,(x_{i+6} + x_{i+8}) + x_{12} \left(\sum_{1 \leq i \leq 11} x_i + \sum_{1 \leq i < j \leq 11} x_i x_j \right), \tag{9.1}$$

where the indices of x_{i+k} are understood modulo 11.

Proof. The ternary function

$$\phi(x, y, z) = \delta f(x, y, z) = |x \cap y \cap z|$$

is obviously symmetric in x, y, z. Theorem 2 then implies the existence of a generating function α_G. By Proposition 4.1 we know that α_G is a polynomial of degree ≤ 3. Moreover, linear terms in α_G do not contribute in the quasialgebra structure (i.e do not contribute in the expression of β and ϕ, see (3.1)). To determine the quadratic and cubic terms, we use the following equivalences:

$$\begin{aligned} &\alpha_G \text{ contains the term } x_i x_j,\, i \neq j \iff u_i, u_j \text{ anti-commute,} \\ &\alpha_G \text{ contains the term } x_i x_j x_k,\, i \neq j \neq k \iff u_i, u_j, u_k \text{ anti-associate.} \end{aligned}$$

For instance, the construction of the Parker loop gives that u_i and u_j commute for all $1 \leq i, j \leq 11$, since $|\ell_i \cap \ell_j| = 8$, for $1 \leq i, j \leq 11$. Thus, α_G does not contain any of the quadratic terms $x_i x_j$, $1 \leq i \neq j \leq 11$. But, u_{12} anti-commutes with u_i, $i \leq 11$, since $|\ell_{12} \cap \ell_i| = 6, i \leq 11$. So that the terms $x_{12} x_i$, $i \leq 11$, do appear in the expression of α_G. Similarly, one has to determine which one of the triples u_i, u_j, u_k anti-associate to determine the cubic terms in α_G. This yields to the expression (9.1) □

The explicit formula for the factor set f in coordinates on $(\mathbb{Z}_2)^{12}$ is immediately obtained by (6.4). Note that the signature in this case is $(11, 1)$, so that we have to add $x_{12} y_{12}$ to (6.4).

Remark 9.3. The difference between the loops generated by the basis elements of $\mathbb{O}_n$ and $\mathbb{M}_n$ and the Parker loop is that the function (9.1) is not $\mathfrak{S}_n$-invariant. Our classification results cannot be applied in this case.

We hope that the notion of generating function can be a useful tool for study of code loops.

Acknowledgements. This work was completed at the Mathematisches Forschungsinstitut Oberwolfach (MFO). The first author has benefited from the award of a *Leibniz Fellowship*, the second author is also grateful to MFO for hospitality. We are pleased to thank Christian Duval, Alexey Lebedev, Dimitry Leites, John McKay and Sergei Tabachnikov for their interest and helpful comments. We are also grateful to anonymous referees for a number of useful comments.

10. Appendix: Linear Algebra and Differential Calculus over $\mathbb{Z}_2$

The purpose of this Appendix is to relate the algebraic problems we study to the general framework of linear algebra over $\mathbb{Z}_2$ which is a classical domain.

Automorphisms of $(\mathbb{Z}_2)^n$ *and linear equivalence.* All the algebraic structures on $(\mathbb{Z}_2)^n$ we consider are invariant with respect to the action of the group automorphisms

$$\mathrm{Aut}((\mathbb{Z}_2)^n) \cong \mathrm{GL}(n, \mathbb{Z}_2).$$

For instance, the generating function $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$, as well as β and ϕ, are considered up to the $\mathrm{Aut}((\mathbb{Z}_2)^n)$-equivalence (called "congruence" in the classic literature [2]).

Quadratic forms. The interest to describe an algebra in terms of a generating function can be illustrated in the case of the Clifford algebras.

There are exactly two non-equivalent non-degenerate quadratic forms on $(\mathbb{Z}_2)^{2m}$ with coefficients in $\mathbb{Z}_2$ (see [2,13] for the details):

$$\alpha(x) = x_1 x_{m+1} + \cdots + x_m x_{2m} + \lambda\,(x_m^2 + x_{2m}^2), \qquad (10.1)$$

where $\lambda = 0$ or 1. Note that sometimes the case $\lambda = 1$ is not considered (see [20], p.xix) since the extra term is actually linear, for $x_i^2 = x_i$. The corresponding polar bilinear form $\beta = \delta\alpha$ and the trilinear form $\phi = \delta_2\alpha$ do not depend on λ. The corresponding twisted group algebra is isomorphic to the Clifford algebra $C\ell_n$.

The normal form (10.1) is written in the standard Darboux basis; this formula has several algebraic corollaries. For instance, we immediately obtain the well-known factorization of the complex Clifford algebras:

$$C\ell_{2m} \cong C\ell_2^{\otimes m} \cong \mathbb{C}[2^m],$$

where $\mathbb{C}[2^m]$ are $(2^m \times 2^m)$-matrices. Indeed, the function (10.1), with $\lambda = 0$, is nothing but the sum of m generating functions of $C\ell_2$. The other classical symmetry and periodicity theorems for the Clifford algebras can also be deduced in this way.

Let us mention that bilinear forms over $\mathbb{Z}_2$ is still an interesting subject [21].

Cubic polynomials. In this paper, we were led to consider polynomials $\alpha : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ of degree 3:

$$\alpha(x) = \sum_{i<j<k} \alpha^3_{ijk}\, x_i x_j x_k + \sum_{i<j} \alpha^2_{ij}\, x_i x_j,$$

where α^3_{ijk} and α^2_{ij} are arbitrary coefficients (equal to 1 or 0). It turns out that it is far of being obvious to understand what α is "non-degenerate" means.

To every polynomial α, we associate a binary function $\beta = \delta\alpha$ and a trilinear form $\phi = \delta_2\alpha$, see formula (3.2), which is of course just the polarization (or linearization) of α. The form ϕ is alternate: $\phi(x, x, .) = \phi(x, ., x) = \phi(., x, x) = 0$ and depends only on the homogeneous part of degree 3 of α, i.e., only on α^3_{ijk}. There are three different ways to understand the notion of non-degeneracy.

(1) The most naive way: α (and ϕ) is non-degenerate if for all linearly independent $x, y \in (\mathbb{Z}_2)^n$, the linear function $\phi(x, y, .) \not\equiv 0$. One can show that, with this definition, *there are no non-degenerate cubic forms on* $(\mathbb{Z}_2)^n$ *for* $n \geq 3$. This is of course not the way we proceed.

(2) The second way to understand non-degeneracy is as follows. The trilinear map ϕ itself defines an n-dimensional algebra. Indeed, identifying $(\mathbb{Z}_2)^n$ with its dual space, the trilinear function ϕ defines a product $(x, y) \mapsto \phi(x, y, .)$. One can say that ϕ (and α) is non-degenerate if this algebra is simple. This second way is much more interesting and is related to many different subjects. For instance, classification of simple Lie (super)algebras over $\mathbb{Z}_2$ is still an open problem, see [8] and references therein. This definition also depends only on the homogeneous part of degree 3 of α.

(3) We understand non-degeneracy yet in a different way. We say that α is non-degenerate if for all linearly independent x, y there exists z such that

$$\beta(x, z) \neq 0, \qquad \beta(y, z) = 0,$$

where $\beta = \delta\alpha$. This is equivalent to the fact that the algebra with the generated function α is simple, cf. Sect. 7.

We believe that every non-degenerate (in the above sense) polynomial of degree 3 on $(\mathbb{Z}_2)^n$ is equivalent to one of the two forms (4.5) and (4.6). Note that a positive answer would imply the uniqueness results of Sect. 4.3 without the $\mathfrak{S}_n$-invariance assumption.

Higher differentials. Cohomology of abelian groups with coefficients in $\mathbb{Z}_2$ is a well-known and quite elementary theory explained in many textbooks. Yet, it can offer some surprises.

Throughout this work, we encountered and extensively used the linear operators δ_k, for $k = 1, 2, 3$, cf. (3.2) and (6.1), that associate a k-cochain on $(\mathbb{Z}_2)^n$ to a function. These operators were defined in [30], and used in the Moufang loops theory, [18,14,26]. Operations of this type are called *natural* or *invariant* since they commute with the action of $\mathrm{Aut}((\mathbb{Z}_2)^n)$. The operator δ_k fits the usual understanding of "higher derivation" since the condition $\delta_k\alpha = 0$ is equivalent to the fact that α is a polynomial of degree $\leq k$.

The cohomological meaning of δ_k is as follows. In the case of an abelian group G, the cochain complex with coefficients in $\mathbb{Z}_2$ has a richer structure. There exist k natural operators acting from $C^k(G; \mathbb{Z}_2)$ to $C^{k+1}(G; \mathbb{Z}_2)$:

$$\begin{tikzcd}
C^1(G;\mathbb{Z}_2) \arrow[r, "\delta"] & C^2(G;\mathbb{Z}_2) \arrow[r, shift left, "\delta_{1,0}"] \arrow[r, shift right, "\delta_{0,1}"] & C^3(G;\mathbb{Z}_2) \arrow[r, shift left=2, "\delta_{1,0,0}"] \arrow[r, "\delta_{0,1,0}"] \arrow[r, shift right=2, "\delta_{0,0,1}"] & \cdots
\end{tikzcd}$$

where $\delta_{0,\ldots,1,\ldots,0}$ is a "partial differential", i.e., the differential with respect to one variable. For instance, if $\beta \in C^2(G; \mathbb{Z}_2)$ is a function in two variables, then

$$\delta_{1,0}\beta(x, y, z) = \beta(x + y, z) + \beta(x, z) + \beta(y, z).$$

In this formula z is understood as a parameter and one can write $\delta_{1,0}\beta(x, y, z) = \delta\gamma(x, y)$, where $\gamma = \beta(., z)$. At each order one has

$$\delta = \delta_{1,0,\ldots,0} + \delta_{0,1,\ldots0} + \cdots + \delta_{0,\ldots,0,1}.$$

If $\alpha \in C^1(G; \mathbb{Z}_2)$, then an *arbitrary* sequence of the partial derivatives gives the same result: $\delta_k\alpha$, for example one has

$$\delta_2\alpha = \delta_{1,0} \circ \delta\alpha = \delta_{0,1} \circ \delta\alpha, \qquad \delta_3\alpha = \delta_{1,0,0} \circ \delta_{1,0} \circ \delta\alpha = \cdots = \delta_{0,0,1} \circ \delta_{0,1} \circ \delta\alpha,$$

etc. The first of the above equations corresponds to the formula (4.2) since $\beta = \delta\alpha$.

References

1. Adem, A., Milgram, R.: *Cohomology of finite groups*. Fundamental Principles of Math. Sci. **309**, Berlin: Springer-Verlag, 2004
2. Albert, A.A.: Symmetric and alternate matrices in an arbitrary field. I. Trans. Amer. Math. Soc. **43**, 386–436 (1938)
3. Albuquerque, H., Elduque, A., Pérez-Izquierdo, J.M.: Alternative quasialgebras. Bull. Austral. Math. Soc. **63**, 257–268 (2001)
4. Albuquerque, H., Majid, S.: Quasialgebra structure of the octonions. J. Algebra **220**, 188–224 (1999)
5. Albuquerque, H., Majid, S.: Clifford algebras obtained by twisting of group algebras. J. Pure Appl. Algebra **171**, 133–148 (2002)
6. Baez, J.: The octonions. Bull. Amer. Math. Soc. (N.S.) **39**, 145–205 (2002)
7. Berkovich, Ya.G., Zhmud', E.M.: *Characters of finite groups, Part 1*. Translations of Mathematical Monographs **172**. Providence, RI: Amer. Math. Soc., 1998
8. Bouarroudj, S., Grozman, P., Leites, D.: *Classification of finite dimensional modular Lie superalgebras with indecomposable Cartan matrix*. SIGMA **5**, 060 (2009), 63pp
9. Conlon, S.B.: Twisted group algebras and their representations. J. Austr. Math. Soc. **4**, 152–173 (1964)
10. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups. Third edition. New York: Springer-Verlag, 1999
11. Conway, J.H., Smith, D.A.: On quaternions and octonions: their geometry, arithmetic, and symmetry. Natick, MA: A K Peters, Ltd., 2003
12. Coxeter, H.S.M.: Integral Cayley numbers. Duke Math. J. **13**, 561–578 (1946)
13. Dieudonné, J.: La géométrie des groupes classiques. Seconde édition, Berlin-Gottingen-Heidelberg: Springer-Verlag, 1963
14. Drápal, A., Vojtechovský, P.: Symmetric multilinear forms and polarization of polynomials. Linear Algebra Appl. **431**(5-7), 998–1012 (2009)
15. Elduque, A.: Gradings on octonions. J. Alg. **207**, 342–354 (1998)
16. Gabel, M.R.: Generic orthogonal stably free projectives. J. Algebra **29**, 477–488 (1974)
17. Goodaire, E., Jespers, E., Polcino, M.: *Alternative loop rings*. Amsterdam: North-Holland Publ., 1996
18. Griess, R.L. Jr.: Code Loops. J. Alg. **100**, 224–234 (1986)
19. Hurwitz, A.: Uber die Komposition der quadratischen Formen. Math. Ann. **88**, 1–25 (1923)
20. Knus, M.-A., Merkurjev, A., Rost, M., Tignol, J.-P.: The book of involutions. AMS Colloquium Publ. **44**, Providence, RI: Amer. Math. Soc., 1998
21. Lebedev, A.: *Non-degenerate bilinear forms in characteristic 2, related contact forms, simple Lie algebras and superalgebras*. http://arXiv.org/abs/0601536v2 [math.Ac], 2006
22. Lenzhen, A., Morier-Genoud, S., Ovsienko, V.: New solutions to the Hurwitz problem on square identities. J. Pure Appl. Alg. (2011). doi:10.1016/j.jpaa.2011.04.011
23. Lychagin, V.: Colour calculus and colour quantizations. Acta Appl. Math. **41**, 193–226 (1995)
24. Morier-Genoud, S., Ovsienko, V.: Well, Papa, can you multiply triplets? Math. Intell. **31**, 1–2 (2009)
25. Morier-Genoud, S., Ovsienko, V.: Simple graded commutative algebras. J. Alg. **323**, 1649–1664 (2010)
26. Nagy, G., Vojtechovský, P.: The Moufang loops of order 64 and 81. J. Symb. Comp. **42**, 871–883 (2007)
27. Radon, J.: Lineare scharen orthogonale Matrizen Abh. Math. Sem. Univ. Hamburg **1**, 1–14 (1922)
28. Rajwade, A.R.: Squares. London Mathematical Society Lecture Note Series, **171**. Cambridge: Cambridge Univ. Press, 1993
29. Shapiro, D.: Compositions of quadratic forms. Berlin: Walter de Gruyter & Co., 2000
30. Ward, H.: Combinatorial polarization. Discrete Math. **26**(2), 185–197 (1979)
31. Zhevlakov, K.A., Slin'ko, A.M., Shestakov, I.P., Shirshov, A.I.: *Rings that are nearly associative*. Pure and Appl. Math. **104**, New York-London: Academic Press, Inc., 1982

Communicated by Y. Kawahigashi