Journal of Pure and Applied Algebra 215 (2011) 2903–2911

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

New solutions to the Hurwitz problem on square identities

Anna Lenzhen [a], Sophie Morier-Genoud [b], Valentin Ovsienko [c,*]

[a] Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

[b] Institut de Mathématiques de Jussieu UMR 7586 Université Pierre et Marie Curie, 4 place Jussieu, case 247, 75252 Paris Cedex 05, France

[c] CNRS, Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne cedex, France

ARTICLE INFO

Article history:
Received 2 September 2010
Received in revised form 11 March 2011
Available online 8 May 2011
Communicated by C. Kassel

MSC: 16W50; 15A66; 11E25; 94B25

ABSTRACT

The Hurwitz problem of composition of quadratic forms, or of "sum of squares identity" is tackled with the help of a particular class of $(\mathbb{Z}/2\mathbb{Z})^n$-graded non-associative algebras generalizing the octonions. This method provides explicit formulas for the classical Hurwitz–Radon identities and leads to new solutions in a neighborhood of the Hurwitz–Radon identities.

1. Introduction

A square identity of size $[r, s, N]$ is an identity

$$(a_1^2 + \cdots + a_r^2)\,(b_1^2 + \cdots + b_s^2) = c_1^2 + \cdots + c_N^2, \tag{1.1}$$

where $a_1, \ldots, a_r$ and $b_1, \ldots, b_s$ are independent indeterminates and each c_i is a bilinear form in $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_s)$ with integer coefficients. The problem to determine all triples of positive integers r, s, N for which there exists a square identity of size $[r, s, N]$ was formulated by Hurwitz [10] and remains widely open. Such triples are called *admissible*. An admissible triple $[r, s, N]$ is *optimal* if r and s cannot be increased and N cannot be decreased. This problem has various applications and interpretations in number theory, linear algebra, geometry and topology, see [21,19] for a complete overview.

The simplest example is called Brahmagupta's two-square identity

$$(a_1^2 + a_2^2)\,(b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2,$$

which can be easily proved algebraically, but can also be understood as equality between the products of the norms of two complex numbers and the norm of their product:

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

The similar equalities in the algebras of quaternions $\mathbb{H}$ and of octonions $\mathbb{O}$ coincide with Euler's four-square identity (1748) and Degen's eight-square identity (1818), respectively. We refer to [7] for the history of these identities and their meaning.

In 1898, Hurwitz proved his celebrated theorem [10] stating that N-square identities exist only for $N = 1, 2, 4$ and 8. Actually, Hurwitz proved a stronger "non-existence" result in the case where c_i are bilinear forms with complex coefficients. In 1918 (published in 1922), Hurwitz [11] generalized his theorem and established the largest integer $r = \rho(N)$ for which

* Corresponding author.
E-mail addresses: anna.lenzhen@univ-rennes1.fr (A. Lenzhen), sophiemg@math.jussieu.fr (S. Morier-Genoud), ovsienko@math.univ-lyon1.fr (V. Ovsienko).

0022-4049/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2011.04.011

there exists a $[r, N, N]$-identity with complex coefficients. In 1922, Radon [18] independently solved a similar problem in the case of real coefficients. The result is the same in both cases: write N in a form $N = 2^n(2k+1)$, then

$$\rho(N) = \begin{cases} 2n+1, & n \equiv 0 \mod 4 \\ 2n, & n \equiv 1, 2 \mod 4 \\ 2n+2, & n \equiv 3 \mod 4. \end{cases}$$

The function ρ is called the *Hurwitz–Radon function* (this function also appears in topology [1] and linear algebra [2]). Note that Hurwitz's constructive proof leads to $[r, N, N]$-identities with integer coefficients. According to [8], this even implies the existence of such identities with coefficients in $\{-1, 0, 1\}$.

A nice feature of the Hurwitz–Radon identities is their relation to Clifford algebras. Every square identity of size $[r+1, N, N]$ defines a representation of the real Clifford algebra $C\ell_{0,r}$ by $N \times N$-real matrices. In this representation the matrices corresponding to the generators of $C\ell_{0,r}$ are orthogonal and skew-symmetric matrices with integer coefficients. Conversely, every such representation of $C\ell_{0,r}$ defines an $[r+1, N, N]$-identity. In his original work [10], Hurwitz implicitly constructed Clifford algebras and their representations. However, this was formulated in an explicit and conceptual way much later (see [21] for more details).

Besides the Hurwitz–Radon formula, a number of solutions to the Hurwitz problem are known. We refer to [3,12,13,15,20,22] for concrete examples of admissible triples $[r, s, N]$ and various methods to prove their optimality. The complete list of the admissible triples with $N \leq 32$ is given in [23].

In [24,25], Yuzvinsky introduced a new approach to construct square identities, see also [14]. His method is based on *monomial pairings* on the group algebra over $(\mathbb{Z}/2\mathbb{Z})^n$. In particular, the existence of infinite series of identities of size

$$[2n+2, 2^n - \varphi(n), 2^n], \tag{1.2}$$

where the function $\varphi(n)$ is given by the binomial coefficients

$$\varphi(n) = \binom{n}{n/2}, \quad n \equiv 0 \mod 4, \qquad \varphi(n) = 2\binom{n-1}{(n-1)/2}, \quad n \equiv 1 \mod 4,$$

was established. The above values of $[r, s, N]$ are called Yuzvinsky–Lam–Smith formulas (see [21]). Another series of triples:

$$\left[2n, 2^n - 2n, 2^n - 2\right] \tag{1.3}$$

can be found in [6]. To the best of our knowledge, the Hurwitz–Radon formula, the expressions (1.2) and (1.3) as well as their direct consequences, are the only known infinite series of solutions to the Hurwitz problem.

In the present paper, we obtain infinite families of admissible triples $[r, s, N]$ similar to (1.2). Our method is similar to the Yuzvinsky method, but the monomial pairings we consider are different. We use a series of algebras constructed in the recent work [17]. These algebras generalize the classical algebra of octonions and Clifford algebras at the same time. As an application of these algebras, explicit expressions for the Hurwitz–Radon identities were provided in [17]. Here we extend the method to obtain more general identities. As well as (1.2), the triples that we obtain are close to the Hurwitz–Radon triple. Whereas (1.2) is obtained from $[\rho(2^n), 2^n, 2^n]$ by increasing the first entry, $\rho(2^n)$, we will decrease the third entry, 2^n. Let us also mention that our formulas include (1.3) as the simplest case.

Let us also mention that optimality of $[r, s, N]$ is often a difficult problem. For instance, it is not known whether (1.2) is optimal. We show that our formulas generate several optimal (and several best known) values $[r, s, N]$. However, unfortunately we do not have any result on optimality of our formulas.

The paper is organized as follows. In Section 2, we formulate the main results. In Section 3, we introduce the general notion of twisted group algebra over the Abelian group $(\mathbb{Z}/2\mathbb{Z})^n$. In Section 4, we recall the definition of the algebras $\mathbb{O}_n$ and introduce the notion of a Hurwitzian subset of $(\mathbb{Z}/2\mathbb{Z})^n$. Proofs of the main results are given in Section 5.

2. The main results

The first family of admissible triples that we obtain depends on two parameters, ℓ and k.

Theorem 1. (i) *For every n, there exist square identities of size* $[r, s, N]$ *with*

$$\begin{cases} r = 2n, \\ s = 2^n - 2\left(\binom{k-1}{2} + \ell + 1\right)n + 4\binom{k}{3} + 2k\ell, \\ N = 2^n - 2\left(\binom{k-1}{2} + \ell + 1\right), \end{cases} \tag{2.1}$$

for all $1 \leq \ell < k \leq n$.

(ii) *If* $n \equiv 3$ *mod* 4, *then there are also identities of size* $[r+2, s-2, N]$, *where* r, s, N *are as in* (2.1).

For small values of ℓ and k, formula (2.1) gives the following triples:

$$\left[2n,\ 2^n-4n+4,\ 2^n-4\right],\qquad \left[2n,\ 2^n-6n+10,\ 2^n-6\right],\qquad \left[2n,\ 2^n-8n+16,\ 2^n-8\right].$$

We conjecture that the values (2.1) are optimal if n is sufficiently large.

Let us give a few examples of concrete numeric values.

Example 2.1. (a) For $n = 5$, we obtain the following admissible triples: [10, 12, 26], [10, 16, 28]; the latter is optimal (as proved in [23]).

(b) For $n = 6$, we obtain [12, 38, 58], [12, 44, 60] that correspond to the best known values, (cf, [21], pp. 292–293).

(c) For $n = 7$, we obtain the values [14, 88, 120], [14, 96, 122], [14, 104, 124] from (2.1). Furthermore, part (ii) of the theorem leads to [16, 86, 120], [16, 94, 122], [16, 102, 124].

(d) For $n = 8$, we obtain [16, 218, 250], [16, 228, 252].

The second family of identities is parametrized by an integer $k < \frac{n}{2}$. The values of s and N are given in terms of sums of binomial coefficients.

Theorem 2. (i) *If $n \equiv 1$ mod 4, then there exist square identities of size $[r, s, N]$, where*

$$r = 2n,\qquad s = \sum_{0\le i\le k-1} 2\binom{n}{m-i},\qquad N = \sum_{0\le i\le k} 2\binom{n}{m-i}, \tag{2.2}$$

where $m = (n-1)/2$ and $1 \le k \le m$.

(ii) *If $n \equiv 3$ mod 4, then there exist square identities of size $[r+2, s, N]$, where r, s and N are as in (2.2).*

Let us give the first and simplest example. In the case $k = 1$, the formula (2.2) reads

$$\left[2n, 2\binom{n}{m}, 2\binom{n+1}{m}\right],\qquad \left[2n+2, 2\binom{n}{m}, 2\binom{n+1}{m}\right],$$

for $n \equiv 1$ mod 4 and $n \equiv 3$ mod 4, respectively.

Example 2.2. We obtain the values [10, 20, 30], [16, 70, 112], [18, 252, 420]. The second one strengthens the known triple [16, 64, 112], see [21], p. 294.

3. Twisted group algebras over $(\mathbb{Z}/2\mathbb{Z})^n$

In this section, we recall the definition of twisted group algebras over the Abelian group $(\mathbb{Z}/2\mathbb{Z})^n$. These algebras include Clifford algebras and the algebra of octonions. We then explain Yuzvinsky's idea [24] of construction of square identities out of a twisted group algebra.

3.1. Definition and examples of twisted group algebras

Consider the group algebra $\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right]$ over the Abelian group $(\mathbb{Z}/2\mathbb{Z})^n$. Denote by u_x the natural basis vectors indexed by elements of the group $x \in (\mathbb{Z}/2\mathbb{Z})^n$. One then has:

$$\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right] = \bigoplus_{x\in(\mathbb{Z}/2\mathbb{Z})^n} \mathbb{R}\,u_x.$$

Given a function $f : (\mathbb{Z}/2\mathbb{Z})^n \times (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$, satisfying $f(x,0) = f(0,x)$ for all $x \in (\mathbb{Z}/2\mathbb{Z})^n$, one defines a twisted product on $\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right]$

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

for all $x, y \in (\mathbb{Z}/2\mathbb{Z})^n$. The defined algebra is called a *twisted group algebra* over $(\mathbb{Z}/2\mathbb{Z})^n$ and denoted by $\left(\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right], f\right)$. The basis vector u_0 is a unit in $\left(\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right], f\right)$.

Example 3.1. Recall that the Clifford algebra $C\ell_{0,n}$ is the associative algebra with n generators $\gamma_1, \ldots, \gamma_n$ and relations

$$\gamma_i^2 = -1,\qquad \gamma_i\gamma_j = -\gamma_j\gamma_i.$$

Write elements of $(\mathbb{Z}/2\mathbb{Z})^n$ in the form $x = (x_1, \ldots, x_n)$, where $x_i = 0, 1$, and choose the function

$$f_{C\ell}(x,y) = \sum_{1\le i\le j\le n} x_i y_j. \tag{3.1}$$

It turns out that the twisted group algebra $\left(\mathbb{R}\left[(\mathbb{Z}/2\mathbb{Z})^n\right], f_{C\ell}\right)$ is isomorphic to the Clifford algebra $C\ell_{0,n}$, see [5] for the details. For instance, if $n = 2$, then this is nothing but the algebra of quaternions $\mathbb{H}$.

The algebra $(\mathbb{R}[(\mathbb{Z}/2\mathbb{Z})^n], f)$ is associative if and only if f is a 2-cocycle on the group $(\mathbb{Z}/2\mathbb{Z})^n$, i.e.,

$$f(y,z)+f(x+y,z)+f(x,y+z)+f(x,y)=0,$$

for all $x, y, z \in (\mathbb{Z}/2\mathbb{Z})^n$. This is obviously the case for the bilinear function (3.1).

The following example realizes the classical non-associative algebra of octonions $\mathbb{O}$ as a twisted group algebra with a cubic twisting function f (that is not a 2-cocycle). This result was found in [4].

Example 3.2. The twisted group algebra $(\mathbb{R}[(\mathbb{Z}/2\mathbb{Z})^3], f)$ defined by the function

$$f(x,y)=x_1x_2y_3+x_1y_2x_3+y_1x_2x_3+\sum_{1\le i\le j\le 3}x_iy_j$$

is isomorphic to the algebra of octonions $\mathbb{O}$.

3.2. Multiplicativity criterion

In this subsection, we explain the Yuzvinsky original idea (see [24] and also [25]).

Let us consider a twisted group algebra $(\mathbb{R}[(\mathbb{Z}/2\mathbb{Z})^n], f)$. We define the Euclidean norm:

$$\mathcal{N}(a)=\sum_{x\in(\mathbb{Z}/2\mathbb{Z})^n}a_x^2, \tag{3.2}$$

for $a=\sum_{x\in(\mathbb{Z}/2\mathbb{Z})^n}a_x u_x$, where $a_x\in\mathbb{R}$.

Recall that a composition algebra is a normed algebra such that, for any two elements a and b,

$$\mathcal{N}(a)\,\mathcal{N}(b)=\mathcal{N}(a\cdot b). \tag{3.3}$$

It is well-known (and follows for instance from Hurwitz's theorem) that there are no composition algebras of dimension greater than 8. Therefore, if $n\ge 4$, then the condition (3.3) cannot be satisfied for arbitrary elements a and b of the twisted group algebra $(\mathbb{R}[(\mathbb{Z}/2\mathbb{Z})^n], f)$. In order to find square identities, we will look for subsets A, B of $(\mathbb{Z}/2\mathbb{Z})^n$, such that the condition (3.3) is satisfied for

$$a\in \mathrm{Span}_{\mathbb{R}}(u_x, x\in A),\qquad b\in \mathrm{Span}_{\mathbb{R}}(u_x, x\in B).$$

Definition 3.3. Given two subsets $A, B\subset(\mathbb{Z}/2\mathbb{Z})^n$, we say that (A, B) is a *multiplicative pair* if the condition (3.3) holds for any two elements of the form

$$a=\sum_{x\in A}a_xu_x,\qquad b=\sum_{y\in B}b_yu_y.$$

Note that this definition depends on the twisting function f. Moreover, existence of multiplicative pairs is an important property of f.

Recall that the *sumset*, $A+B$, of subsets A and B in $(\mathbb{Z}/2\mathbb{Z})^n$ is the set formed by pairwise sums of the elements of A and B, i.e.

$$A+B=\{a+b\mid a\in A, b\in B\}.$$

Proposition 3.4. *If (A, B) is a multiplicative pair, then there exists a square identity of size*

$$[r,s,N]=[\mathrm{card}(A),\mathrm{card}(B),\mathrm{card}(A+B)],$$

which can be written explicitly as

$$\left(\sum_{x\in A}a_x^2\right)\left(\sum_{y\in B}b_y^2\right)=\left(\sum_{z\in A+B}c_z^2\right)$$

where

$$c_z=\sum_{\substack{(x,y)\in A\times B\\ x+y=z}}(-1)^{f(x,y)}a_x\,b_y.$$

Proof. This is an immediate consequence of the property (3.3). □

The following important statement is proved in [24]. It provides a criterion for subsets A and B to be a multiplicative pair and, therefore, it also proves the existence of corresponding square identities. The proof is elementary and we give it here for the sake of completeness.

Proposition 3.5. *Let A and B be two subsets of $(\mathbb{Z}/2\mathbb{Z})^n$. The following two conditions are equivalent*

(i) *The pair (A, B) is multiplicative.*

(ii) *For all $x\ne z\in A$ and $y\ne t\in B$ such that $x+y+z+t=0$, one has*

$$f(x,y)+f(z,t)+f(x,t)+f(z,y)=1. \tag{3.4}$$

Proof. The product of the Euclidean norms is obviously $\mathcal{N}(a)\,\mathcal{N}(b) = \sum_{x,y} a_x^2\, b_y^2$. On the other hand, one obtains:

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

It follows that the condition (3.3) is satisfied if and only if the terms $a_x\, b_y\, a_z\, b_t$ and $a_x\, b_t\, a_z\, b_y$ cancel whenever $(x, y) \neq (z, t)$ and $a_x\, b_y\, a_z\, b_t \neq 0$, in other words, the corresponding signs are opposite. Hence the result. □

Our next goal is to find a twisted group algebra $(\mathbb{R}\,[(\mathbb{Z}/2\mathbb{Z})^n]\,, f)$ that admits multiplicative pairs of large cardinality.

4. The algebras $\mathbb{O}_n$

In this section, we apply the results of Section 3 to a particular series of twisted group algebras.

4.1. Definitions

We recall the definition and the main properties of the algebras $\mathbb{O}_n$ generalizing the algebra of octonions. This section presents a brief account, the details can be found in [17].

Definition 4.1. The algebra $\mathbb{O}_n$ is the twisted group algebra defined by the function

$$f_{\mathbb{O}}(x, y) = \sum_{1\le i<j<k\le n} \left(x_i x_j y_k + x_i y_j x_k + y_i x_j x_k\right) + \sum_{1\le i\le j\le n} x_i y_j, \tag{4.1}$$

for all $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, elements of $(\mathbb{Z}/2\mathbb{Z})^n$.

Note that $\mathbb{O}_3$ is exactly the algebra of octonions $\mathbb{O}$, cf. Example 3.2.

The main property of the algebra $\mathbb{O}_n$ is that its structure is determined (up to isomorphism) by a single function in one variable

$$\alpha : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$$

that we call the *generating function*.

Definition 4.2. Given a twisted group algebra $(\mathbb{R}\,[(\mathbb{Z}/2\mathbb{Z})^n]\,, f)$, we say that this algebra has a generating function if there exists a function $\alpha : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ such that

(i) For all $x, y \in (\mathbb{Z}/2\mathbb{Z})^n$, the following equation is satisfied:

$$f(x, y) + f(y, x) = \alpha(x + y) + \alpha(x) + \alpha(y),$$

(ii) For all $x, y, z \in (\mathbb{Z}/2\mathbb{Z})^n$,

$$\begin{aligned} &f(y, z) + f(x + y, z) + f(x, y + z) + f(x, y)\\ &\quad = \alpha(x + y + z) + \alpha(x + y) + \alpha(x + z) + \alpha(y + z) + \alpha(x) + \alpha(y) + \alpha(z). \end{aligned}$$

Remark 4.3. The above conditions (i) and (ii) have cohomological meaning. In particular the expression on the right-hand side of (i) and the left-hand side of (ii) are the differentials $\delta\alpha$ and δf, respectively. The idea of existence of a generating function goes back to Eilenberg and MacLane (see [16]); this idea is also crucial for the theory of error-correcting codes and code loops (see [9]).

One can immediately check the following statement.

Proposition 4.4 (*[17]*)**.** (i) *The function*

$$\alpha_{\mathbb{O}}(x) := f_{\mathbb{O}}(x, x),$$

for $x \in (\mathbb{Z}/2\mathbb{Z})^n$, is a generating function for the algebra $\mathbb{O}_n$.

(ii) *For $f = f_{\mathbb{O}}$ and $x + y + z + t = 0$, one has*

$$f_{\mathbb{O}}(x, y) + f_{\mathbb{O}}(z, t) + f_{\mathbb{O}}(x, t) + f_{\mathbb{O}}(z, y) = \alpha_{\mathbb{O}}(x + z). \tag{4.2}$$

(iii) *The function $\alpha_{\mathbb{O}}(x)$ depends only on the weight of the element x, i.e., on the integer*

$$|x| = \sum_{1\le i\le n} x_i.$$

Note that equation (4.2) is equivalent to (3.4).

The algebra $\mathbb{O}_n$ is the unique twisted group algebra over $(\mathbb{Z}/2\mathbb{Z})^n$ that admits a generating function $\alpha_{\mathbb{O}}$ which is invariant under the action of the group of permutations $\mathfrak{S}_n$ on $(\mathbb{Z}/2\mathbb{Z})^n$, i.e., the action permuting the coordinates of x.

By (iii) of Proposition 4.4, the value $\alpha_{\mathbb{O}}(x)$ only depends on the weight $|x|$. It turns out that $\alpha_{\mathbb{O}}$ is 4-periodic.

$$\alpha_{\mathbb{O}}(x) = \begin{cases} 0, & \text{if } |x| \equiv 0 \bmod 4,\\ 1, & \text{otherwise.} \end{cases}$$

4.2. The Hurwitzian sets

We use the function $\alpha_{\mathbb{O}}$ to give a combinatorial characterization of multiplicative pairs for the algebra $\mathbb{O}_n$.

Lemma 4.5. *A pair (A, B) of subsets of $(\mathbb{Z}/2\mathbb{Z})^n$ is a multiplicative pair if and only if the following condition is satisfied. If*

$$w \in (A + A) \cap (B + B)$$

and $w \neq 0$, then $|w| \not\equiv 0 \pmod 4$.

Proof. The condition $0 \neq w \in (A + A)$ means $w = x + z$ for some elements $x, z \in A$ such that $x \neq z$. Similarly, $w = y + t$, where $y, t \in B$. By (3.4) and (4.2), multiplicativity of a pair (A, B) is equivalent to

$$\alpha_{\mathbb{O}}(x + z) = \alpha_{\mathbb{O}}(y + t) = 1, \tag{4.3}$$

for all $x, z \in A$ and $y, t \in B$ such that $x + z = y + t$. Since $\alpha_{\mathbb{O}}$ is 0 only for elements of weight multiple of 4, the lemma now follows. □

Definition 4.6. A subset $H \subset (\mathbb{Z}/2\mathbb{Z})^n$ is called a *Hurwitzian set* if H forms a multiplicative pair with $(\mathbb{Z}/2\mathbb{Z})^n$, and $\mathrm{card}(H)$ is the greatest possible with this condition.

Let us fix the following notation for some particular elements of $(\mathbb{Z}/2\mathbb{Z})^n$:

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

The following table provides a possible choice of Hurwitzian sets and the size of the identities obtained by applying Proposition 3.4, depending on the class of n mod 4.

	Hurwitzian set	Size of identity
$n \equiv 0 \bmod 4$	$H = \{e_i, e_1 + e_i\}$	$[2n, 2^n, 2^n]$
$n \equiv 1 \bmod 4$	$H = \{e_i, \overline{e_i}\}$	$[2n, 2^n, 2^n]$
$n \equiv 2 \bmod 4$	$H = \{e_i, e_1 + e_i\}$	$[2n, 2^n, 2^n]$
$n \equiv 3 \bmod 4$	$H = \{e_0, \overline{e_0}, e_i, \overline{e_i}\}$	$[2n + 2, 2^n, 2^n]$

(4.4)

where $1 \leq i \leq n$. Indeed, it is easy to check that $|x + z|$ is never a multiple of 4, when $x, z \in H$. Therefore the condition (4.3) is always satisfied.

Remark 4.7. For $n = 1, 2$ or 3 mod 4, the triples in the table are the optimal triples given by Hurwitz–Radon theorem. When $n \equiv 0$ mod 4, we do not achieve the optimal $[2n + 1, 2^n, 2^n]$. This is related to the fact that for $n \equiv 0$ mod 4, the algebra $\mathbb{O}_n$ is not simple.

5. Generalized Hurwitz–Radon identities

In this section, we prove Theorems 1 and 2. The proofs are based on Proposition 3.4. The idea is to start with a multiplicative pair (H, B), where $B = (\mathbb{Z}/2\mathbb{Z})^n$, and reduce the size of $H + B$ by removing elements from B. We first give some examples.

5.1. The simplest examples

Let H be a Hurwitzian set as in table (4.4).

(1) For $B = (\mathbb{Z}/2\mathbb{Z})^n \setminus H$, the sumsets are as follows:

$$H + B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \{e_0, e_1\}, \qquad H + B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \{e_0, \bar{e}_0\},$$

for $n \equiv 0, 2$ mod 4 and $n \equiv 1, 3$ mod 4, respectively. This leads to the formula (1.3). Furthermore, in the case $n \equiv 3$ mod 4, one obtains an identity of size

$$[2n + 2, 2^n - 2n - 2, 2^n - 2].$$

(2) Assume n is odd and let

$$B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \{x, |x| = 1, 3, n - 3, n - 1\}.$$

The sumset is then of the form:

$$H + B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \{x, |x| = 0, 2, n - 2, n\}.$$

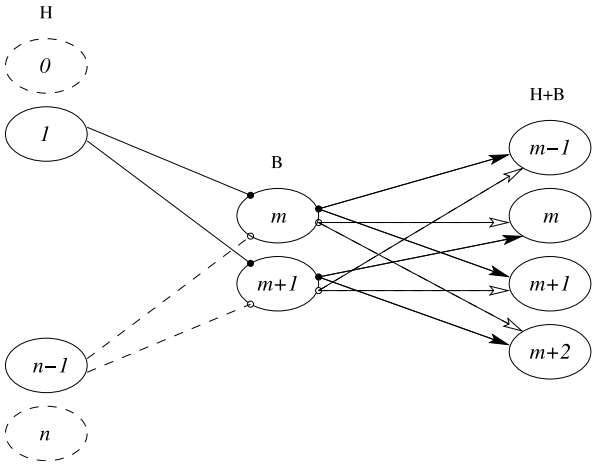

Fig. 1. Sumset $H + B$ for $n = 2m + 1$ and B consisting of elements of weight m and $m + 1$.

This leads to identities of size

$$\left[2n, 2^n - 2\left(n + \binom{n}{3}\right), 2^n - 2\binom{n}{2} - 2\right],$$

which corresponds to the second "border case" in Theorem 1, namely to formula (2.1) with $(\ell, k) = (n - 1, n)$.

(3) Again, let n be odd and write $n = 2m+1$. Set $B = \{x, |x| = m, m + 1\}$. Then $H+B = \{x, |x| = m-1, m, m+1, m+2\}$, see Fig. 1. This leads to identities of size

$$\left[2n, 2\binom{n}{m}, 2\binom{n+1}{m}\right], \qquad \left[2n+2, 2\binom{n}{m}, 2\binom{n+1}{m}\right],$$

if $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$, respectively. This is Theorem 2, in the particular case $k = 1$.

5.2. Proof of Theorem 1

In Section 5.1, part (2), we removed all the elements of weight 2 and $(n-2)$. We will now remove them one after another.

Consider first the case when n is odd.

Set $e_{ij} := e_i + e_j$ and $\overline{e_{ij}} := \overline{e_0} + e_{ij}$. In order to eliminate two elements e_{ij} and $\overline{e_{ij}}$ from $H + B$, we have to remove from B the following set:

$$H \cup \left\{H + e_{ij}\right\} \cup \left\{H + \overline{e_{ij}}\right\}.$$

Notice however, that $\left\{H + e_{ij}\right\}$ and $\left\{H + \overline{e_{ij}}\right\}$ coincide and their intersection with H is $\{e_i, e_j, \overline{e_i}, \overline{e_j}\}$. Thus the cardinality of the removed set is $4n - 4$.

Finally, we fix (ℓ, k) with $\ell < k$ and let B be the following set

$$B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \left(H \cup \bigcup_{(i,j) \prec (\ell,k)} \left\{H + e_{ij}\right\}\right),$$

where $\prec$ is the lexicographical order. It can be easily proved by induction that the removed set is of cardinality

$$\left((k-1)(k-2) + 2\ell + 2\right)n - \frac{2}{3}(k-2)(k-1)k + 2\,k\ell.$$

The corresponding sumset is then of the form

$$H + B = (\mathbb{Z}/2\mathbb{Z})^n \setminus \{e_0, \overline{e_0}, e_{ij}\,\overline{e_{ij}}, (i,j) \prec (\ell,k)\}.$$

Its cardinality is

$$\operatorname{card}(H + B) = 2^n - (k-1)(k-2) - 2\,\ell - 2.$$

We now apply Proposition 3.4 to obtain identities (2.1) for an odd n.

In the case n is even, the proof is similar, with e_1 playing the role of $\overline{e_0}$.

Theorem 1 is proved.

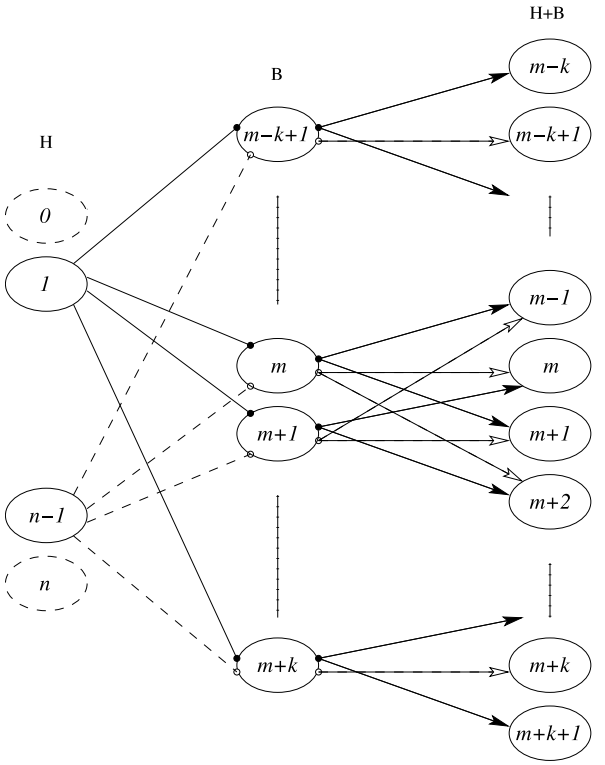

Fig. 2. Sumset $H + B$ for $n = 2m + 1$ and B consisting of elements of weight between $(m - k + 1)$ and $(m + k)$.

5.3. Proof of Theorem 2

We write $n = 2m + 1$. Fix k such that $0 \leq k \leq m$ and set

$$B = \{x, |x| = m - k, m - k + 1, \ldots, m, m + 1, \ldots, m + k + 1\}.$$

The sumset is as follows (see Fig. 2)

$$H + B = \{x, |x| = m - k - 1, m - k, \ldots, m + k + 1, m + k + 2\}.$$

By Proposition 3.4, this leads to the formulas of Theorem 2.

Theorem 2 is proved.

5.4. The twisting function $f_{\mathbb{O}}$ and representations of the Clifford algebras

Let us finally mention that the twisting function $f_{\mathbb{O}}$ that defines the algebras $\mathbb{O}_n$ allows one to construct representations of the Clifford algebras $C\ell_{0,r}$ explicitly.

For $x \in (\mathbb{Z}/2\mathbb{Z})^n$, we define a $(2^n \times 2^n)$-matrix G_x whose coefficients are indexed by elements $(y, t) \in (\mathbb{Z}/2\mathbb{Z})^n \times (\mathbb{Z}/2\mathbb{Z})^n$ and are given by

$$G_x(y, t) = \begin{cases} (-1)^{f_{\mathbb{O}}(y+t,y)}, & \text{if } y + t = x, \\ 0, & \text{otherwise.} \end{cases}$$

Note that for $x = (0, \ldots, 0)$ one obtains $G_0 = \mathrm{Id}$.

The matrices G_x satisfy the following properties.

(i) $G_x^2 = (-1)^{f_{\mathbb{O}}(x,x)}\,\mathrm{Id}$, $G_x^T = G_x^{-1} = (-1)^{f_{\mathbb{O}}(x,x)}\,G_x$.
(ii) $G_x G_{x'} = -G_{x'} G_x$ if and only if $f_{\mathbb{O}}(x, x') + f_{\mathbb{O}}(x', x) = 1$.

This leads to representations of Clifford algebras in $\mathbb{R}[2^n]$. Indeed, if A is a subset of r elements of $(\mathbb{Z}/2\mathbb{Z})^n$ such that $f_{\mathbb{O}}(x, x) = 1$ and $f_{\mathbb{O}}(x, x') + f_{\mathbb{O}}(x', x) = 1$, for all $x, x' \in A$, then the matrices G_x, $x \in A$, represent the real Clifford algebra $C\ell_{0,r}$ in the algebra $\mathbb{R}[2^n]$.

Example 5.1. We describe explicitly the irreducible representations of some of the simple real Clifford algebras. We give a possible choice of sets A. The condition on the set A can be expressed using the generating function $\alpha_{\mathbb{O}}$. We use the notation of Section 4.2.

- If $n \equiv 3 \bmod 4$, an irreducible representation of $C\ell_{0,2n} = \mathbb{R}[2^n]$ is given by

  $G_x, x \in \{e_i, \overline{e_i}, 1 \leq i \leq n\}$.

- If $n \equiv 1, 3 \bmod 4$, an irreducible real representation of $C\ell_{0,2n-1} = \mathbb{C}[2^{n-1}]$ is given by

  $G_x, x \in \{e_i, e_1 + e_j, 1 \leq i \leq n, 1 < j \leq n\}$.

- If $n \equiv 2, 3 \bmod 4$, an irreducible real representation of $C\ell_{0,2n-2} = \mathbb{H}[2^{n-2}]$ is given by

  $G_x, x \in \{e_i, e_1 + e_j, 1 \leq i \leq n, 1 < j < n\}$.

Acknowledgements

The second author has benefited from the award of a *Leibniz Fellowship* at the Mathematisches Forschungsinstitut Oberwolfach (MFO). The third author is also grateful to MFO for hospitality. We would like to thank C. Duval for helpful comments. We are also deeply grateful to the anonymous referee for a number of helpful remarks and suggestions.

References

[1] J.F. Adams, Vector fields on spheres, Ann. of Math. 75 (2) (1962) 603–632.
[2] J.F. Adams, P.D. Lax, R.S Phillips, On matrices whose real linear combinations are non-singular, Proc. Amer. Math. Soc. 16 (1965) 318–322.
[3] J. Adem, Construction of some normed maps, Bol. Soc. Mat. Mexicana 20 (2) (1975) 59–75.
[4] H. Albuquerque, S. Majid, Quasialgebra structure of the octonions, J. Algebra 220 (1999) 188–224.
[5] H. Albuquerque, S. Majid, Clifford algebras obtained by twisting of group algebras, J. Pure Appl. Algebra 171 (2002) 133–148.
[6] N. Anghel, Clifford matrices and a problem of Hurwitz, Linear Multilinear Algebra 47 (2) (2000) 105–117.
[7] J.H. Conway, D.A. Smith, On Quaternions and Octonions: their Geometry, Arithmetic, and Symmetry, A K Peters, Ltd., Natick, MA, 2003.
[8] M.R. Gabel, Generic orthogonal stably free projectives, J. Algebra 29 (1974) 477–488.
[9] R.L. Griess Jr., Code Loops, J. Algebra 100 (1986) 224–234.
[10] A. Hurwitz, Uber die Komposition der quadratischen Formen von beliebig vielen Variablen, Nahr. Ges. Wiss. Göttingen (1898) 309–316.
[11] A. Hurwitz, Uber die Komposition der quadratischen Formen, Math. Ann. 88 (1922) 1–25.
[12] K.Y. Lam, Topological methods for studying the composition of quadratic forms, Canadian Math. Soc. Conf. Proc. 4 (1984) 173–192.
[13] K.Y. Lam, Some new results on composition of quadratic forms, Invent. Math. 79 (1985) 467–474.
[14] T.Y. Lam, T.L. Smith, On Yuzvinsky's monomial pairings, Quart. J. Math. Oxford Ser. 44 (2) (1993) 215–237.
[15] K.Y. Lam, P.Y.H. Yiu, Sums of squares formulae near the Hurwitz–Radon range, in: Contemp. Math., vol. 58, Amer. Math. Soc., Providence, RI, 1987, II.
[16] S. MacLane, Cohomology theory of Abelian groups, in: Proc. Intern. Congress of Math., Cambridge, Mass., vol. 2, 1950, pp. 8–14.
[17] S. Morier-Genoud, V. Ovsienko, A series of algebras generalizing the octonions and Hurwitz–Radon identity, Comm. Math. Phys. (in press) Available from: arXiv:1003.0429.
[18] J. Radon, Lineare scharen orthogonale Matrizen, Abh. Math. Sem. Univ. Hamburg 1 (1922) 1–14.
[19] A.R. Rajwade, Squares. London Mathematical Society Lecture Note Series, vol. 171. Cambridge.
[20] A. Sánchez-Flores, A method to generate upper bounds for the sums of squares formulae problem, Bol. Soc. Mat. Mexicana 2 (3) (1996) 79–92.
[21] D. Shapiro, Compositions of Quadratic Forms, Walter de Gruyter Co., Berlin, 2000.
[22] P.Y.H. Yiu, Some upper bounds for composition numbers, Bol. Soc. Mat. Mexicana 2 (3) (1996) no. 2, 65–77.
[23] P.Y.H. Yiu, Composition of sums of squares with integer coefficients, in: Deformations of Mathematical Structures, II, Kluwer Acad. Publ, Dordrecht, 1994, pp. 7–100.
[24] S. Yuzvinsky, Orthogonal pairings of Euclidean spaces, Michigan Math. J. 28 (1981) 131–145.
[25] S. Yuzvinsky, A series of monomial pairings, Linear Multilinear Algebra 15 (1984) 109–119.