$\mathbb{Z}_2^n$-GRADED QUASIALGEBRAS AND THE HURWITZ PROBLEM ON COMPOSITIONS OF QUADRATIC FORMS

YA-QING HU, HUA-LIN HUANG, AND CHI ZHANG

ABSTRACT. We introduce a series of $\mathbb{Z}_2^n$-graded quasialgebras $\mathbb{P}_n(m)$ which generalizes Clifford algebras, higher octonions, and higher Cayley algebras. The constructed series of algebras and their minor perturbations are applied to contribute explicit solutions to the Hurwitz problem on compositions of quadratic forms. In particular, we provide explicit expressions of the well-known Hurwitz-Radon square identities in a uniform way, recover the Yuzvinsky-Lam-Smith formulas, confirm the third family of admissible triples proposed by Yuzvinsky in 1984, improve the two infinite families of solutions obtained recently by Lenzhen, Morier-Genoud and Ovsienko, and construct several new infinite families of solutions.

CONTENTS

1. INTRODUCTION

As a special class of algebras in braided tensor categories [9], group graded quasialgebras were introduced and investigated in [1] by Albuquerque and Majid. The familiar twisted group algebras may be naturally viewed as group graded quasialgebras and this viewpoint provides a new derivation of some interesting known results and even helps to generalize them; see for instance the subsequent work of Albuquerque and Majid on Clifford algebras [2]. More importantly, this viewpoint allows us to treat some mysterious *nonassociative* algebras exactly as if they were effectively associative with the help of the theory of tensor categories; see for example [10]. As a marvelous example, the octonions were realized as a $\mathbb{Z}_2^3$-graded quasialgebra in [1]. The idea was applied by Morier-Genoud and Ovsienko to introduce an interesting series of algebras generalizing the octonions [11], which

helps to provide new solutions to the Hurwitz problem on compositions of quadratic forms [8].

Recall that the Hurwitz problem on compositions of quadratic forms [5] asks for the description of all triples of positive integers $[r, s, N]$, which are *admissible* in the sense that there exists a sum of squares formula of the type

$$(a_1^2 + a_2^2 + \cdots + a_r^2)(b_1^2 + b_2^2 + \cdots + b_s^2) = c_1^2 + c_2^2 + \cdots + c_N^2,$$

where $a = (a_1, a_2, \ldots, a_r)$ and $b = (b_1, b_2, \ldots, b_s)$ are systems of indeterminates and each c_k is a bilinear form in a and b with coefficients in a field. This century-old problem is centrally located in mathematics and remains widely open; see [13, 14] for a full overview. The admissible triples of the form $[N, N, N]$ were determined by Hurwitz [5] in 1898 and the result is his well-known "1, 2, 4, 8 Theorem". A more general series of admissible triples of the form $[r, N, N]$ was settled independently by Hurwitz [6] in 1918 and by Radon [12] in 1922. The celebrated Hurwitz-Radon Theorem states that $[r, N, N]$ is admissible if and only if $r \leq \rho(N)$, where ρ is the Hurwitz-Radon function defined by $\rho(N) = 8\alpha + 2^\beta$ if $N = 2^{4\alpha+\beta}(2\gamma + 1)$ with $0 \leq \beta \leq 3$. The result of Hurwitz and Radon relies essentially on Clifford algebras; see for instance [3].

Afterwards, many more new solutions to the Hurwitz problem were obtained by various mathematicians; see [14] and the references therein. In particular, Yuzvinsky proposed in the early 1980s three families of admissible triples of the form

$$(1.1) \quad [2n + 2, 2^n - \varphi(n), 2^n] \quad \text{where} \quad \varphi(n) = \begin{cases} \binom{n}{n/2}, & n \equiv 0 \mod 4, \\ 2\binom{n-1}{(n-1)/2}, & n \equiv 1 \mod 4, \\ 4\binom{n-2}{(n-2)/2}, & n \equiv 2 \mod 4. \end{cases}$$

Yuzvinsky's novel idea relies on orthogonal pairings on the group algebra over $\mathbb{Z}_2^n$; see [15, 16]. The proof of Yuzvinsky is very concise and contains a number of errors and gaps. In [7], Lam and Smith have carefully corrected and clarified the proof for the cases in which $n \equiv 0, 1 \mod 4$. Hence these solutions are called the Yuzvinsky-Lam-Smith formulas in literatures. However, the method of Yuzvinsky for the case in which $n \equiv 2 \mod 4$ is shown to be futile in [7] and so the solutions of this case have stayed conjectural.

Remarkably, the four normed division algebras connected to the Hurwitz "1, 2, 4, 8 Theorem", Clifford algebras connected to the Hurwitz-Radon Theorem, and the algebras connected to the Yuzvinsky-Lam-Smith formulas are twisted group algebras over $\mathbb{Z}_2^n$; see [1, 2]. With this insight, Morier-Genoud and Ovsienko recently introduced in [11] their series of algebras $\mathbb{O}_n$ which generalizes the algebra of octonions and Clifford algebras simultaneously and applied them to get explicit expressions of the Hurwitz-Radon square identities with the exception $n \equiv 0 \mod 4$. In their subsequent work [8] with Lenzhen, the algebras $\mathbb{O}_n$ were applied to provide two infinite families of admissible triples which are similar to the Yuzvinsky-Lam-Smith formulas.

Note in hindsight that these algebras useful for the Hurwitz problem are $\mathbb{Z}_2^n$-graded quasialgebras. So it is tempting to try other similar algebras in the problem. In the present paper, we introduce a class of more complicated $\mathbb{Z}_2^n$-graded quasialgebras $\mathbb{P}_n(m)$ ($n \geq m \geq 4$) and apply them to contribute new solutions to the Hurwitz problem. The twisting function of our series of algebras $\mathbb{P}_n(m)$ contains all the terms of $\mathbb{O}_n$ and additional terms of degree ≥ 4. Another feature of our algebras $\mathbb{P}_n(m)$ is that their twisting functions are linear with respect to the second

argument which is crucial in searching for multiplicative pairs. By applying the composition of Euclidean norms on the series of algebras $\mathbb{P}_n(4)$, we provide explicit expressions of the Hurwitz-Radon square identities in a uniform way without the exception $n \equiv 0 \bmod 4$ that occurred in [11]. By choosing suitable multiplicative pairs in some delicate perturbations of $\mathbb{P}_n(4)$, $\mathbb{O}_n$, and $\mathbb{P}_n(n)$, we are able to recover the Yuzvinsky-Lam-Smith formulas in a simpler way and, moreover, confirm Yuzvinsky's third conjectural family of admissible triples. Using a similar idea, we find the duality between the two basic methods of generating new admissible triples by addition and subtraction and improve the Lenzhen-Morier-Genoud-Ovsienko admissible triples. Furthermore, by applying the method of addition on the Yuzvinsky admissible triples, we obtain three new infinite families as well.

Recall that an admissible triple $[r, s, N]$ is said to be *optimal* if there exists no admissible triples of sizes $[r + 1, s, N]$, $[r, s + 1, N]$ or $[r, s, N - 1]$. The admissible triples obtained in this paper recover several well-known optimal triples, such as $[10, 16, 28]$ and $[10, 22, 30]$, and some best known triples, $[10, 16, 28]$, $[10, 22, 30]$, $[12, 44, 60]$, $[12, 38, 58]$, $[12, 32, 52]$ and $[14, 40, 64]$; see [14]. In general, it is very challenging to determine whether a given admissible triple $[r, s, N]$ is optimal when the entries are big. So far, we have not obtained any result about the optimality of our new triples.

An outline of the paper is as follows. Section 2 is devoted to the basic definitions of group graded quasialgebras and multiplicative pairs. Some interesting $\mathbb{Z}_2^n$-graded quasialgebras are recalled and the series of algebras $\mathbb{P}_n(m)$ are introduced. The uniform and explicit expression of the Hurwitz-Radon square identities is then given in Section 3. In Section 4, simpler constructions of Yuzvinsky-Lam-Smith formulas are provided and Yuzvinsky's third family of admissible triples is verified. In Section 5, some improvements of the Lenzhen-Morier-Genoud-Ovsienko formulas are presented. The duality of two basic methods of generating admissible triples is also mentioned in passing. Three new infinite series of admissible triples are shown in Section 6.

Throughout the paper, by $\mathbb{Z}_2$ we mean the cyclic group of order 2 and by $\mathbb{Z}_2^n$ the direct product of n copies of $\mathbb{Z}_2$; we work on the field $\mathbb{R}$ of real numbers for convenience. It is not hard to see that most of our results hold for any field of characteristic not 2.

2. $\mathbb{Z}_2^n$-GRADED QUASIALGEBRAS AND MULTIPLICATIVE PAIRS

In this section, we recall the notion of group graded quasialgebras, some interesting examples of $\mathbb{Z}_2^n$-graded quasialgebras and introduce some new series which will be applied in later sections. For later applications in constructing admissible triples, the notion of multiplicative pairs and the multiplicativity criterion are also recalled.

2.1. **Group graded quasialgebras.** Let G be a finite abelian group with unit e and let ϕ be a normalized 3-cocycle on G with coefficients in $\mathbb{R}^*$. A G-graded quasialgebra is a G-graded $\mathbb{R}$-vector space A, a product map $A \otimes A \to A$ preserving the total degree and associative in the sense that

$$(a \cdot b) \cdot c = \phi(|a|, |b|, |c|)a \cdot (b \cdot c)$$

for all homogeneous $a, b, c \in A$ and a 3-cocycle ϕ. Here and below, $|a|$ denotes the degree of a. A G-graded quasialgebra is called coboundary if ϕ is coboundary. As

pointed out in [1], group graded quasialgebras may be defined in a more general setting. Given G and ϕ as above, if we extend ϕ linearly to $\mathbb{R}G^{\otimes 3}$, then we can regard $(\mathbb{R}G, \phi)$ as a coquasi-Hopf algebra. Let Vec_G^ϕ denote the comodule category of $(\mathbb{R}G, \phi)$ and Vec_G^ϕ has a natural structure of tensor category; see [10]. Then a G-graded quasialgebra is nothing other than an algebra in the tensor category Vec_G^ϕ as defined in [9]. This viewpoint may allow us to apply Drinfeld's useful idea of gauge equivalence; see [4] and [1]. Natural generalization of twisted group algebras provides an interesting class of group graded quasialgebras. Let $F : G \times G \to \mathbb{R}^*$ be a normalized 2-cochain, that is, F obeys $F(x, e) = 1 = F(e, x)$ for all $x \in G$. Denote by ϕ the differential of F, i.e.,

$$\phi(x, y, z) = \frac{F(x, y)F(xy, z)}{F(y, z)F(x, yz)}.$$

Define the (generalized) twisted group algebra $\mathbb{R}_F G$ as follows. It has the same vector space as the usual group algebra $\mathbb{R}G$ but a twisted product by F, namely

$$x \cdot y = F(x, y)xy, \quad \forall x, y \in G.$$

Clearly, $\mathbb{R}_F G$ is an algebra in Vec_G^ϕ, or a G-graded quasialgebra, and it is coboundary since $\phi = \partial F$.

2.2. Examples of $\mathbb{Z}_2^n$-graded quasialgebras.
Remarkably enough, many interesting algebras, such as the normed division algebras and Clifford algebras, turn out to be coboundary $\mathbb{Z}_2^n$-graded quasialgebras. Now we recall some examples from [1, 2, 11]. In the following, we write elements of the group $\mathbb{Z}_2^n$ in the form $x = (x_1, \ldots, x_n)$ with $x_i \in \{0, 1\}$ and its multiplication by $+$ and we present the vector space $\mathbb{R}\mathbb{Z}_2^n$ by $\bigoplus_{x \in \mathbb{Z}_2^n} \mathbb{R}u_x$. Define functions $f_m : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$ for all $1 \le m \le n$ by

$$f_1 = \sum_i x_i y_i, \quad f_2 = \sum_{i<j} x_i y_j, \quad f_3 = \sum_{\substack{\text{distinct } i,j,k \\ i<j}} x_i x_j y_k,$$

(2.1)
$$f_4 = \sum_{\substack{\text{distinct } i,j,k,l \\ i<j<k}} x_i x_j x_k y_l, \quad \ldots,$$

$$f_m = \sum_{\substack{\text{distinct } i_1,i_2,\ldots,i_{m-1},l \\ i_1<\cdots<i_{m-1}}} x_{i_1} x_{i_2} \cdots x_{i_{m-1}} y_l, \quad \ldots.$$

Example 2.1. Let $F_{Cl} : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{R}^*$ be a function defined by

(2.2)
$$F_{Cl}(x, y) = (-1)^{f_1(x,y)+f_2(x,y)}.$$

Then the associated twisted group algebra $\mathbb{R}_{F_{Cl}}\mathbb{Z}_2^n$ is the well-known real Clifford algebra $Cl_{0,n}$; see [2] for details. This recovers the algebra of complex numbers $\mathbb{C}$ when $n = 1$ and the algebra of quaternions $\mathbb{H}$ when $n = 2$. Note that $Cl_{0,n}$ is associative in the usual sense since the function F_{Cl} is a 2-cocycle.

Example 2.2. Assume $n \ge 3$. Define the function $F_{\mathbb{O}} : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{R}^*$ by

(2.3)
$$F_{\mathbb{O}}(x, y) = (-1)^{f_1(x,y)+f_2(x,y)+f_3(x,y)}.$$

Then the twisted group algebra $\mathbb{R}_{F_{\mathbb{O}}}\mathbb{Z}_2^n$ is the algebra of higher octonions $\mathbb{O}_n$ introduced in [11] by generalizing the realization of octonions via quasialgebra (i.e., the

case of $n = 3$) given in [1]. Clearly, the series of algebras $\mathbb{O}_n$ are nonassociative in the usual sense as the function $F_\mathbb{O}$ is not a 2-cocycle.

2.3. The series of algebras $\mathbb{P}_n(m)$.
Now assume $n \geq m \geq 4$. Define

$$(2.4) \quad f_{\mathbb{P}(m)}(x,y) = \sum_{i=1}^{3} f_i(x,y) + f_m(x,y) \quad \text{and} \quad F_{\mathbb{P}(m)}(x,y) = (-1)^{f_{\mathbb{P}(m)}(x,y)}.$$

Let $\mathbb{P}_n(m)$ denote the corresponding twisted group algebra $\mathbb{R}_{F_{\mathbb{P}(m)}} \mathbb{Z}_2^n$ and we get a series of nonassociative algebras $\{\mathbb{P}_n(m)\}_{n \geq 4}$.

It was shown in [1] that Cayley-Dickson algebras are all coboundary $\mathbb{Z}_2^n$-graded quasialgebras. Recall that, starting from $\mathbb{R}$, the Cayley-Dickson construction produces the algebra $\mathbb{C}$ of complex numbers, the algebra $\mathbb{H}$ of quaternions, and the algebra $\mathbb{O}$ of octonions consecutively. The immediate follower of the octonions $\mathbb{O}$ is the algebra $\mathbb{S}$ of sedenions. It can be realized as the twisted group algebra $\mathbb{R}_{F_\mathbb{S}} \mathbb{Z}_2^4$ with

$$F_\mathbb{S}(x,y) = F_{\mathbb{P}(4)}(x,y)(-1)^{\sum_{\substack{\text{distinct } i,j,k,4 \\ j<k}} x_i y_j y_k x_4}.$$

Therefore, the series of algebras $\mathbb{P}_n(4)$ may be regarded as a partial generalization of the algebra $\mathbb{S}$ of sedenions. Similarly, $\mathbb{P}_n(m)$ are partial generalizations of the higher Cayley algebras [1].

2.4. Multiplicative pairs and multiplicativity criterion.
In this subsection we recall some key notions that appeared in the novel method of Yuzvinsky [15, 16]; see also [7, 8]. Consider the twisted group algebra $\mathbb{R}_F \mathbb{Z}_2^n$. For every $a = \sum_{x \in \mathbb{Z}_2^n} a_x u_x \in \mathbb{R}_F \mathbb{Z}_2^n$, we define its Euclidean norm by

$$(2.5) \quad \mathcal{N}(a) = \sum_{x \in \mathbb{Z}_2^n} a_x^2.$$

With this square norm, it is well-known that "the law of moduli"

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

of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ provides exactly the "1,2,4,8"-square identities. The idea of Yuzvinsky is that in order to obtain (more general) square identities it suffices to find a pair of subsets A, B of $\mathbb{Z}_2^n$ such that

$$(2.6) \quad \mathcal{N}(a)\mathcal{N}(b) = \mathcal{N}(a \cdot b), \quad \forall a \in \text{Span}_\mathbb{R}(u_x, \ x \in A), \ b \in \text{Span}_\mathbb{R}(u_y, \ y \in B).$$

If this is the case, we say that (A, B) is a *multiplicative pair,* or an *orthogonal pairing.* Given such a pair (A, B), one may induce from it an admissible triple $[r, s, N] = [\text{card}(A), \text{card}(B), \text{card}(A + B)]$ and the explicit square identity is

$$(2.7) \quad \left(\sum_{x \in A} a_x^2 \right) \left(\sum_{y \in B} b_y^2 \right) = \sum_{z \in A+B} c_z^2,$$

where $A + B$ is the sumset $\{a + b \mid a \in A, b \in B\}$ and

$$c_z = \sum_{\substack{z = x+y \\ (x,y) \in A \times B}} F(x,y) a_x b_y = \sum_{(x,x+z) \in A \times B} F(x, x+z) a_x b_{x+z}.$$

In the rest of the paper *we always assume that the twisting function F is of the form $F(x,y) = (-1)^{f(x,y)}$, where f maps $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ to $\mathbb{Z}_2$.* When there is no risk of confusion, the map f is also called the twisting function of the associated

twisted group algebra. This restriction on F allows us to formulate a criterion of the multiplicativity of a pair of subsets of $\mathbb{Z}_2^n$. The following proposition is well-known; see for example [8]. We include it here for completeness.

Proposition 2.3. (A, B) *forms a multiplicative pair if and only if for all $z \in A + B$ and for all $x \neq t$ such that $x + z, \ t + z \in B$, the following equation holds:*

$$(2.8) \qquad f(x, x + z) + f(x, t + z) + f(t, x + z) + f(t, t + z) = 1.$$

Proof. Let $a = \sum_{x \in A} a_x u_x$ and $b = \sum_{y \in B} b_y u_y$. Then the product of their Euclidean norms is obviously

$$\mathcal{N}(a)\,\mathcal{N}(b) = \sum_{(x,y) \in A \times B} a_x^2\, b_y^2 = \sum_{z \in A+B} \ \sum_{(x, x+z) \in A \times B} a_x^2 b_{x+z}^2.$$

On the other hand,

$$\begin{aligned}
\mathcal{N}(a \cdot b) &= \sum_{z \in A+B} \left(\sum_{(x, x+z) \in A \times B} (-1)^{f(x, x+z)} a_x b_{x+z} \right)^2 \\
&= \sum_{z \in A+B} \ \sum_{\substack{(x, x+z) \in A \times B \\ (t, t+z) \in A \times B}} (-1)^{f(x, x+z) + f(t, t+z)} a_x a_t b_{x+z} b_{t+z}.
\end{aligned}$$

Hence condition (2.6) is fulfilled if and only if for all $z \in A + B$ and for all $x \neq t$ such that $x + z, \ t + z \in B$, the coefficients of $a_x\, a_t\, b_{x+z}\, b_{t+z}$ and $a_x\, a_t\, b_{t+z}\, b_{x+z}$ are exactly opposite, i.e., equation (2.8) holds. $\qquad\square$

This proposition has several equivalent forms, and later on we will need the following one.

Corollary 2.4. (A, B) *forms a multiplicative pair if and only if for all $x \neq t \in A$ and for all $y \in B$ such that $x + t + y \in B$, the following equation holds:*

$$(2.9) \qquad f(x, y) + f(t, y) + f(x, x + t + y) + f(t, x + t + y) = 1.$$

For later applications, we also need the following simple fact in which further restriction is put on the twisting function f.

Corollary 2.5. *Suppose that $F(x, y) = (-1)^{f(x,y)}$, where $f(x, y)$ is linear in its second argument, then equation (2.8) becomes*

$$(2.10) \qquad f(x, x + t) + f(t, x + t) = 1, \quad \forall x \neq t \in A.$$

In the rest of the paper, our main mission is to search for multiplicative pairs in suitable $\mathbb{Z}_2^n$-graded quasialgebras $\mathbb{A}$. According to the previous discussion, we shall frequently encounter the following function

$$(2.11) \qquad c_{\mathbb{A}}(x, t) \triangleq f_{\mathbb{A}}(x, x + t) + f_{\mathbb{A}}(t, x + t), \quad \forall x, t \in \mathbb{Z}_2^n,$$

and we call it the *test function* of multiplicativity.

3. The Hurwitz-Radon square identities revisited

The aim of this section is to give explicit formulas of the Hurwitz-Radon triples $[\rho(2^n), 2^n, 2^n]$. Recall that this was partially achieved by Morier-Genoud and Ovsienko in [11] with help of the higher octonions $\mathbb{O}_n$ only with the exception $n \equiv 0 \bmod 4$. It turns out that by applying the series of algebras $\mathbb{P}_n(4)$ instead of $\mathbb{O}_n$, we are able to rule out the exception and come up with the square identities in a uniform manner. The crux is to construct the so-called Hurwitzian sets. Our method of construction in this section is combinatorial and seems of independent interest.

3.1. **The Hurwitzian sets.** Thanks to subsection 2.4, in order to obtain the Hurwitz-Radon square identities it suffices to construct multiplicative pairs of form $(H, \mathbb{Z}_2^n)$ with card$H = \rho(2^n)$ in the algebra $\mathbb{P}_n(4)$. We will call H a *Hurwitzian set* in the algebra $\mathbb{P}_n(4)$, or simply an H-set, if $(H, \mathbb{Z}_2^n)$ satisfies this condition. According to Corollary 2.5, an H-set is a subset H of $\mathbb{Z}_2^n$ such that

$$c_{\mathbb{P}(4)}(x, t) = f_{\mathbb{P}(4)}(x, x + t) + f_{\mathbb{P}(4)}(t, x + t) = 1, \quad \forall x \neq t \in H.$$

Given $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, set $o(x) = 1 + \sum_{i=1}^n x_i 2^{n-i}$. Define an order on $\mathbb{Z}_2^n$ by

$$x > y \Leftrightarrow o(x) > o(y).$$

It is obvious that this order is nothing other than the lexicographic order and $o(x)$ indicates the exact position of x in $\mathbb{Z}_2^n$. With this order, all values of $c_{\mathbb{P}(4)}(x, t)$ will form a 2^n-by-2^n symmetric matrix and all H-sets are characterized as subsets of $\mathbb{Z}_2^n$ such that the corresponding principal submatrices of size $\rho(2^n)$ have zeros in the diagonal and all ones off-diagonal. Therefore, searching for H-sets is equivalent to searching for such principal submatrices.

By the definitions of $f_{\mathbb{P}(4)}$ and $f_{\mathbb{O}}$, we have

$$c_{\mathbb{P}(4)}(x, t) = [f_{\mathbb{O}}(x, x + t) + f_{\mathbb{O}}(t, x + t)] + [f_4(x, x + t) + f_4(t, x + t)].$$

Let $\beta_4(x, t) = f_4(x, x + t) + f_4(t, x + t)$. Note that

$$f_4(x, x) = \sum_{\substack{\text{distinct } i,j,k,l \\ i<j<k}} x_i x_j x_k x_l = 4 \sum_{i<j<k<l} x_i x_j x_k x_l = 0.$$

Hence, $\beta_4(x, t) = f_4(x, t) + f_4(t, x)$. On the other hand, it was observed in [11] that

$$f_{\mathbb{O}}(x, x + t) + f_{\mathbb{O}}(t, x + t) = f_{\mathbb{O}}(x + t, x + t).$$

Let $\alpha_{\mathbb{O}}(x) = f_{\mathbb{O}}(x, x)$. We remark that $\alpha_{\mathbb{O}}(x)$ is called a generating function in [11]. 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 explicit formula of $\alpha_{\mathbb{O}}(x)$ is as follows:

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

$$= \binom{|x|}{3} + \binom{|x|}{2} + \binom{|x|}{1}.$$

Therefore $\alpha_{\mathbb{O}}(x)$ depends only on $|x|$ and can be easily proved to be 4-periodic:

(3.1)

$|x|$	1	2	3	4	5	6	7	8	$\cdots$
$\alpha_{\mathbb{O}}$	1	1	1	0	1	1	1	0	$\cdots$

3.2. **Explicit expressions of the Hurwitz-Radon square identities.** Now we are ready to present our H-set. To determine an H-set $H = \{\mathbf{h}\}$ in $\mathbb{Z}_2^n$, it suffices to determine the subset $o(H) = \{o(\mathbf{h})\}$ in $\{1, 2, 3, \ldots, 2^n\}$. We observe an interesting method to find the latter by the following function.

Definition 3.1. Define the function $H : \mathbb{N} \to \mathbb{N}$, called H-function in the following, by:

$$(3.2) \quad \begin{array}{c|c|c|c|c|c|c|c|c|c} n & 1 \leq n \leq 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & n \geq 17 \\ \hline H(n) & n-1 & 16 & 32 & 56 & 64 & 88 & 104 & 112 & 2^4 H(n-8) \end{array}$$

Now let $H \subset \mathbb{Z}_2^n$ be the subset such that $o(H) = \{H(i) + 1 \mid i = 1, \ldots, \rho(2^n)\}$. More precisely, $H = \{\mathbf{h}_i \mid o(\mathbf{h}_i) = H(i) + 1, \ 1 \leq i \leq \rho(2^n)\}$. Recall that an arbitrary $\mathbf{h} \in \mathbb{Z}_2^n$ is obtained by the 2-adic digital expression of $o(\mathbf{h}) - 1$. It turns out that such a set H is an H-set.

Before stating the main theorem, we include the following example of H-sets to offer some flavor to the reader and also for later applications.

TABLE 1. $n = 7$ and $\rho(2^7) = 16$

$\mathbf{h}_1 = (0,0,0,0,0,0,0)$	$H(1)=0$	$\mathbf{h}_9 = (0,0,0,1,0,0,0)$	$H(9) = 8$
$\mathbf{h}_2 = (0,0,0,0,0,0,1)$	$H(2)=1$	$\mathbf{h}_{10} = (0,0,1,0,0,0,0)$	$H(10)= 16$
$\mathbf{h}_3 = (0,0,0,0,0,1,0)$	$H(3)=2$	$\mathbf{h}_{11} = (0,1,0,0,0,0,0)$	$H(11)= 32$
$\mathbf{h}_4 = (0,0,0,0,0,1,1)$	$H(4)=3$	$\mathbf{h}_{12} = (0,1,1,1,0,0,0)$	$H(12)= 56$
$\mathbf{h}_5 = (0,0,0,0,1,0,0)$	$H(5)=4$	$\mathbf{h}_{13} = (1,0,0,0,0,0,0)$	$H(13)= 64$
$\mathbf{h}_6 = (0,0,0,0,1,0,1)$	$H(6)=5$	$\mathbf{h}_{14} = (1,0,1,1,0,0,0)$	$H(14)= 88$
$\mathbf{h}_7 = (0,0,0,0,1,1,0)$	$H(7)=6$	$\mathbf{h}_{15} = (1,1,0,1,0,0,0)$	$H(15)=104$
$\mathbf{h}_8 = (0,0,0,0,1,1,1)$	$H(8)=7$	$\mathbf{h}_{16} = (1,1,1,0,0,0,0)$	$H(16)=112$

Theorem 1. *Let n be a positive integer, $N = 2^n$ and $r = \rho(N)$. Then the set $H = \{\mathbf{h_i}\}_{i=1}^r \subset \mathbb{Z}_2^n$ as defined above is a Hurwitzian set in $\mathbb{P}_n(4)$.*

Proof. First, we observe from Table 1 that the weight $|\mathbf{h}_i|$ of each $\mathbf{h}_i$ is at most 3 for all $1 \leq i \leq 16$. For any $i \geq 17$ there exists a unique integer k such that $9 \leq i - 8k \leq 16$. Then by the definition of the H-function and the construction of H, it is not hard to see that $|\mathbf{h}_i| = |\mathbf{h}_{i-8k}|$. Therefore, $|\mathbf{h}| \in \{0, 1, 2, 3\}$, $\forall \mathbf{h} \in H$. It follows that $|x + y| \in \{1, 2, 3, 4, 5, 6\}$ for all $x \neq y \in H$.

Next note that, for our purpose it is enough to verify that for all $x \neq y \in H$,

$$c_{\mathbb{P}(4)}(x, y) = \alpha_{\mathbb{O}}(x+y) + \beta_4(x, y) = \alpha_{\mathbb{O}}(x+y) + \sum_{\substack{\text{distinct } i,j,k,l \\ i<j<k}} (x_i x_j x_k y_l + y_i y_j y_k x_l) = 1.$$

In the following we carry out the verification case by case according to $|x + y|$.

(1) $|x + y| = 1$. In this case, according to the symmetry of $c_{\mathbb{P}(4)}(x, y)$ we may assume without loss of generality that $0 = x_{i_1} \neq y_{i_1} = 1$ and $x_j = y_j$, $\forall j \neq i_1$. Moreover, there exist at most two other indices i_2 and i_3 such that

$x_{i_2} = x_{i_3} = 1 = y_{i_2} = y_{i_3}$ as $|x|, |y| \in \{0, 1, 2, 3\}$. Then we have the following table which includes all the indices i such that x_i or y_i is 1:

	i_1	i_2	i_3
x	0	a_1	a_2
y	1	a_1	a_2

Note that in the above table a_1 or a_2 may be 0. Now by direct computation, we have $\alpha_{\mathbb{O}}(x + y) = 1$ by (3.1) and $\beta_4(x, y) = 0$ due to the fact that $|x| \leq 2$, $|y| \leq 3$ and $x_i = 0$ if $i \notin \{i_2, i_3\}$.

(2) $|x + y| = 2$. By a similar analysis, we have the tables of information for x and y:

	i_1	i_2	i_3
x	0	0	a_1
y	1	1	a_1

or

	i_1	i_2	i_3	i_4
x	0	1	a_1	a_2
y	1	0	a_1	a_2

It is not hard to see that $\alpha_{\mathbb{O}}(x + y) = 1$ and $\beta_4(x, y) = 0$.

(3) $|x + y| = 3$. As before, the tables of information for x and y are as follows:

	i_1	i_2	i_3
x	0	0	0
y	1	1	1

or

	i_1	i_2	i_3	i_4
x	0	0	1	a_1
y	1	1	0	a_1

In the first case, it is obvious that $\alpha_{\mathbb{O}}(x + y) = 1$ and $\beta_4(x, y) = 0$. For the second, when $a_1 = 0$, again one has $\alpha_{\mathbb{O}}(x + y) = 1$ and $\beta_4(x, y) = 0$. If a_1 were 1, then $|x| = 2$ and $x \in \{\mathbf{h}_4, \mathbf{h}_6, \mathbf{h}_7\}$ as we can read from Table 1 and deduce from Definition 3.1 of the H-function $H(n)$ that $|\mathbf{h}_i| \in \{1, 3\}$ when $i \geq 9$. However, in this case we cannot find a $y \in H$ such that it matches the second table.

(4) $|x + y| = 4$. Similar to case (3). The tables of information for x and y are as follows:

	i_1	i_2	i_3	i_4
x	0	1	1	1
y	1	0	0	0

or

	i_1	i_2	i_3	i_4	i_5
x	0	0	1	1	a_1
y	1	1	0	0	a_1

In the first case, it is obvious that $\alpha_{\mathbb{O}}(x+y) = 0$ and $\beta_4(x, y) = y_{i_1} x_{i_2} x_{i_3} x_{i_4} = 1$. For the second case if a_1 were 0, then $|x| = |y| = 2$ and $x, y \in \{\mathbf{h}_4, \mathbf{h}_6, \mathbf{h}_7\}$, so one has $|x+y| = 2$, which contradicts our assumption; if a_1 were 1, then $x, y \in \{\mathbf{h} \in H \mid |\mathbf{h}| = 3\}$. However, by Table 1 and Definition 3.1, one sees the fact that $|x + y| \in \{2, 6\}$, which is also a contradiction.

(5) $|x + y| = 5$. The table of information for x and y is of the form:

	i_1	i_2	i_3	i_4	i_5
x	0	0	1	1	1
y	1	1	0	0	0

Hence in this case one has $\alpha_{\mathbb{O}}(x+y) = 1$ and $\beta_4(x, y) = (y_{i_1} + y_{i_2})x_{i_3} x_{i_4} x_{i_5} = 0$.

(6) $|x + y| = 6$. The table of information for x and y must be as follows:

	i_1	i_2	i_3	i_4	i_5	i_6
x	0	0	0	1	1	1
y	1	1	1	0	0	0

Again, by direct calculation one has $\alpha_{\mathbb{O}}(x+y) = 1$ and $\beta_4(x, y) = 3+3 = 0$.

In summary, $c_{\mathbb{P}(4)}(x, y) = 1$, $\forall x \neq y \in H$ always holds. The proof is complete. $\square$

Corollary 3.2. *Keep all the assumptions of Theorem* 1. *Then we have the following explicit expressions of the Hurwitz-Radon square identities:*

$$\left(\sum_{x \in H} a_x^2\right)\left(\sum_{y \in \mathbb{Z}_2^n} b_y^2\right) = \sum_{z \in \mathbb{Z}_2^n} c_z^2,$$

where

$$c_z = \sum_{x \in H} (-1)^{f_{\mathbb{P}(4)}(x, x+z)} a_x b_{x+z}.$$

4. The Yuzvinsky admissible triples

In this section, by using various types of $\mathbb{Z}_2^n$-graded quasialgebras, we recover the *Yuzvinsky-Lam-Smith formulas* in a simpler way, and moreover we confirm the third family of admissible triples

$$\left[2n + 2, 2^n - 4\binom{n-2}{\frac{n-2}{2}}, 2^n\right], \quad n \geq 4 \text{ and } n \equiv 2 \mod 4,$$

foreseen by Yuzvinsky in 1984. Throughout this section, n is always assumed to be ≥ 4 (in order to make sure that $2n + 2 < 2^n$).

4.1. **Basic ideas.** The three families of admissible triples proposed in [16] by Yuzvinsky are in the neighbourhood of the Hurwitz-Radon triples. They can be constructed via the latter by adding 1 or 2 to the first component and subtracting the second accordingly. Thus, to obtain such kind of triples via multiplicative pairs, we should expand the Hurwitzian sets and detect their companions with the help of the test functions in suitable $\mathbb{Z}_2^n$-graded quasialgebras.

The procedure we adopt goes as follows. Take some $\mathbb{Z}_2^n$-graded quasialgebra $\mathbb{A}$ with twisting function f in which Hurwitzian sets are known to exist, for example $\mathbb{O}_n$ and $\mathbb{P}_n(4)$, and choose a Hurwitzian set H. Then add one or two appropriate elements to H, say $H \cup \{z_1\}$ or $H \cup \{z_1, z_2\}$, and detect its companion set B. This relies essentially on the test function. In order to make the cardinality $\text{card}B$ relatively big and keep the computation under control, we shall make a delicate manipulation on the twisting function. More precisely, we perturb the twisting function f to f' such that $f'|_{H \times \mathbb{Z}_2^n} = f$. Denote $\delta_i(y) = f'(z_i, y) + f(z_i, y)$, $\forall y \in \mathbb{Z}_2^n$ for $i = 1, 2$, and call them the *perturbation functions*. The crux of our method lies in adding to H and detecting B by the symmetry in $\mathbb{Z}_2^n$, and furthermore in manipulating the twisting functions and choosing the added elements in a consistent way.

4.2. **Another Hurwitzian set in $\mathbb{P}_n(4)$.** For our purpose in this section and the next, we need another Hurwitzian set in $\mathbb{P}_n(4)$ which is different from the one given in Section 3.

To describe the elements in $\mathbb{Z}_2^n$, in the rest of the paper we use the following notation:

$$
\begin{array}{rcl}
e_0 & \triangleq & (0, 0, \ldots, 0), \\
\overline{e_0} & \triangleq & (1, 1, \ldots, 1), \\
e_i & \triangleq & (0, \ldots, 0, 1, 0, \ldots, 0), \text{ where 1 only occurs at the } i\text{th position}, \\
\overline{e_i} & \triangleq & \overline{e_0} + e_i = (1, \ldots, 1, 0, 1, \ldots, 1), \text{ where 0 only occurs at the } i\text{th position}
\end{array}
$$

for all $1 \le i \le n$. For any $B \subseteq \mathbb{Z}_2^n$, let $\overline{B} = \overline{e_0} + B = \{\overline{e_0} + y \mid y \in B\}$. We then introduce the following subset H of $\mathbb{Z}_2^n$:

$$(4.1) \qquad H = \begin{cases} \{e_0, e_i, \overline{e_i} \mid 1 \le i \le n\}, & \text{for } n \equiv 0 \mod 4, \\ \{e_1 + e_i, e_i \mid 1 \le i \le n\}, & \text{for } n \equiv 1 \mod 4, \\ \{e_1 + e_i, e_i \mid 1 \le i \le n\}, & \text{for } n \equiv 2 \mod 4, \\ \{e_0, \overline{e_0}, e_i, \overline{e_i} \mid 1 \le i \le n\}, & \text{for } n \equiv 3 \mod 4. \end{cases}$$

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

Theorem 2. *H is a Hurwitzian set in $\mathbb{P}_n(4)$.*

Proof. Similarly to Theorem 1, we need to calculate the test function $c_{\mathbb{P}_n(4)}(x, y) = \alpha_{\mathbb{O}}(x + y) + \beta_4(x, y)$ and verify that $\alpha_{\mathbb{O}}(x + y)$ and $\beta_4(x, y)$ always have different values for any two distinct elements $x, y \in H$. If (x, y) is one of

$$(e_0, \overline{e_0}), \ (e_0, e_i), \ (e_0, \overline{e_i}), \ (e_i, e_j), \ (e_i, e_1 + e_j), \ (e_1 + e_i, e_1 + e_j), \quad 1 \le i, j \le n,$$

then it is obvious that $\beta_4(x, y) = 0$ and $\alpha_{\mathbb{O}}(x + y) = 1$. Now the following direct case by case calculations will complete the proof:

$$c_{\mathbb{P}_n(4)}(e_i, \overline{e_i}) = \alpha_{\mathbb{O}}(\overline{e_0}) + \binom{n-1}{3} = 1, \qquad \text{while } n \equiv 0, 3 \mod 4,$$

$$c_{\mathbb{P}_n(4)}(e_i, \overline{e_j}) = \alpha_{\mathbb{O}}(\overline{e_0} + e_i + e_j) + \binom{n-2}{3} = 1, \qquad \text{while } n \equiv 0, 3 \mod 4,$$

$$c_{\mathbb{P}_n(4)}(e_i, \overline{e_0}) = \alpha_{\mathbb{O}}(\overline{e_0} + e_i) + \binom{n-1}{3} = 1, \qquad \text{while } n \equiv 0, 3 \mod 4,$$

$$c_{\mathbb{P}_n(4)}(\overline{e_0}, \overline{e_j}) = \alpha_{\mathbb{O}}(e_j) + n\binom{n-1}{3} + (n-1)\binom{n-2}{3} = 1,$$
$$\text{while } n \equiv 3 \mod 4,$$

$$c_{\mathbb{P}_n(4)}(\overline{e_i}, \overline{e_j}) = \alpha_{\mathbb{O}}(e_i + e_j) + 2\binom{n-1}{3} + 2(n-2)\binom{n-2}{3} = 1,$$
$$\text{while } n \equiv 0, 3 \mod 4.$$

$\square$

Now we are ready to construct the three families of Yuzvinsky admissible triples. The construction is split into three cases according to the residue of n modulo 4.

4.3. **The case in which** $n \equiv 0 \mod 4$. In this case, let $f = f_{\mathbb{P}(4)}$ and $H = \{e_0, e_i, \overline{e_i} \mid 1 \le i \le n\}$. We need to add an element z to H and perturb the twisting function f to f' by δ. According to Corollary 2.4, one easily obtains the following lemma.

Lemma 4.1. *$(H \cup \{z\}, B)$ forms a multiplicative pair with respect to f' if and only if for all $h \in H$ and for all $y \in B$ such that $h + z + y \in B$, the equation*

$$f'(z, y) + f'(z, h + z + y) = f(h, h + z) + 1$$

or, equivalently,

$$(4.2) \qquad \delta(y) + \delta(h + z + y) = f(h, h + z) + f(z, h + z) + 1,$$

holds.

We observe that if we choose $z = \overline{e_0}$, then $H \cup \{z\}$ has a nice symmetry and the equation (4.2) is easier to handle. In this situation, one has

Lemma 4.2. $(H \cup \{\overline{e_0}\}, B)$ *is a multiplicative pair if and only if for all* $i = 1, \ldots, n$ *the following equations hold:*

$$(4.3) \qquad \delta(y) + \delta(\overline{y}) = 1, \ \text{whenever } y, \overline{y} \in B,$$

$$(4.4) \qquad \delta(y) + \delta(e_i + \overline{y}) = 1, \ \text{whenever } y, e_i + \overline{y} \in B,$$

$$(4.5) \qquad \delta(y) + \delta(e_i + y) = 0, \ \text{whenever } y, e_i + y \in B.$$

Proof. Let h take turns to be e_0, e_i, and $\overline{e_i}$. Direct calculations of the right-hand side of equation (4.2) yield the above equations. $\qquad \square$

Next we shall choose a suitable companion set B for $H \cup \{\overline{e_0}\}$ and a proper perturbation function δ. By (4.3), we should assume that B is symmetric with respect to $\overline{e_0}$, i.e., there exists a subset $B_1 \subset B$ such that $B = B_1 \uplus \overline{e_0} + B_1$. Here and below, $\uplus$ stands for disjoint union. By the symmetry of $\mathbb{Z}_2^n$ with respect to the weight of its elements, we may further assume that B_1 is a subset of $\{y \in \mathbb{Z}_2^n \mid |y| \leq \frac{n}{2}\}$. Accordingly, $\overline{e_0} + B_1$ is a subset of $\{y \in \mathbb{Z}_2^n \mid |y| \geq \frac{n}{2}\}$. In addition, note that equations (4.4) and (4.5) are symmetric in view of (4.3), so we only need to solve the three equations for $y \in B_1$.

After these preparations, we are now able to state the first Yuzvinsky-Lam-Smith formula.

Theorem 3. *There exists a series of admissible triples of sizes*

$$\left[2n + 2, 2^n - \binom{n}{n/2}, 2^n \right], \qquad \text{for } n \geq 4 \text{ and } n \equiv 0 \mod 4.$$

Proof. Let $B_1 = \{y \in \mathbb{Z}_2^n \mid |y| < n/2\}$ and let

$$\delta(y) = \begin{cases} 1, & \text{if } |y| \geq n/2 + 1, \\ 0, & \text{otherwise.} \end{cases}$$

Then $B = \{y \in \mathbb{Z}_2^n \mid |y| \neq n/2\}$, $H \cup \{\overline{e_0}\} + B = \mathbb{Z}_2^n$ and $\text{card} B = 2^n - \binom{n}{n/2}$. For any $y \in B_1$, we have $|y| \leq n/2 - 1$, $|\overline{y}| \geq n/2 + 1$, and thus $\delta(y) = 0$, $\delta(\overline{y}) = 1$. Also, $|e_i + \overline{y}| > n/2$ when $e_i + \overline{y} \in B$ and $|e_i + y| < n/2$ when $e_i + y \in B$ hold for any $i = 1, \ldots, n$. Clearly, for all $y \in B_1$ we have $\delta(e_i + \overline{y}) = 1$, $\delta(e_i + y) = 0$. Now the theorem follows by Lemma 4.2 and equation (2.7). $\qquad \square$

4.4. The case in which $n \equiv 1 \mod 4$. The method is similar to the previous case. In this case, $\rho(2^n) = 2n$ and we need to add two elements into the chosen H-set. We observe that there is a symmetric H-set $H = \{e_i, \overline{e_i}, 1 \leq i \leq n\}$ in the higher octonions $\mathbb{O}_n$; see [11]. It is tempting to expand H by $\{e_0, \overline{e_0}\}$ according to the obvious symmetry.

For brevity, denote $f_{\mathbb{O}}$ by f and perturb it by δ_1 and δ_2 as follows:

$$f'(x, y) = \begin{cases} f(x, y) + \delta_1(y), & \text{if } x = e_0, \\ f(x, y) + \delta_2(y), & \text{if } x = \overline{e_0}, \\ f(x, y), & \text{otherwise.} \end{cases}$$

Similarly, we have the following lemma for the companion set B of $H \cup \{e_0, \overline{e_0}\}$.

Lemma 4.3. $(H \cup \{e_0, \overline{e_0}\}, B)$ *forms a multiplicative pair with respect to f' if and only if the following equations hold:*

$$f'(e_0, y) + f'(e_0, y+h) = f(h,h) + 1, \quad \forall h \in H, \text{ whenever } y, y+h \in B,$$

$$f'(\overline{e_0}, y) + f'(\overline{e_0}, h+\overline{y}) = f(h,\overline{h}) + 1, \quad \forall h \in H, \text{ whenever } y, h+\overline{y} \in B,$$

$$f'(e_0, y) + f'(e_0, \overline{y}) + f'(\overline{e_0}, y) + f'(\overline{e_0}, \overline{y}) = 1, \quad \text{whenever } y, \overline{y} \in B,$$

or, equivalently,

(4.6)
$$\delta_1(y) + \delta_1(y+h) = f(h,h) + 1, \quad \forall h \in H, \text{ whenever } y, y+h \in B,$$

(4.7)
$$\delta_2(y) + \delta_2(h+\overline{y}) = f(h,\overline{h}) + f(\overline{e_0},\overline{h}) + 1, \quad \forall h \in H, \text{ whenever } y, h+\overline{y} \in B,$$

(4.8)
$$\delta_1(y) + \delta_1(\overline{y}) + \delta_2(y) + \delta_2(\overline{y}) = 0, \quad \text{whenever } y, \overline{y} \in B.$$

Now if we set $\delta = \delta_1 = \delta_2$, then equation (4.8) holds automatically. In this situation, the previous lemma is reduced to:

Lemma 4.4. $(H \cup \{e_0, \overline{e_0}\}, B)$ *is a multiplicative pair if and only if for all $i = 1, \ldots, n$ the following equations hold:*

(4.9)
$$\delta(y) + \delta(y+e_i) = 0, \quad \text{whenever } y, y+e_i \in B.$$

(4.10)
$$\delta(y) + \delta(y+\overline{e_i}) = 1, \quad \text{whenever } y, y+\overline{e_i} \in B.$$

Proof. By direct calculations. $\qquad\square$

Now we put some assumptions on B again due to the obvious symmetry of $\mathbb{Z}_2^n$. Let $B = B_1 \uplus \overline{e_0} + B_1$ in which B_1 is a subset of $\{y \in \mathbb{Z}_2^n \mid |y| \geq \frac{n+1}{2}\}$. Meanwhile, $\overline{e_0} + B_1$ is a subset of $\{y \in \mathbb{Z}_2^n \mid |y| \leq \frac{n-1}{2}\}$. It follows that for any $y \in B$, $e_i + y \in B$ if and only if $\overline{e_i + y} \in B$. Thus equation (4.10) can be replaced by

(4.11)
$$\delta(e_i + y) + \delta(\overline{e_i + y}) = 1, \quad \text{whenever } y, e_i + y, \overline{e_i + y} \in B.$$

Again, we assume the symmetric condition $\delta(y) + \delta(\overline{y}) = 1$, $\forall y \in B$ on the perturbation function. Then equation (4.11) will hold automatically.

The following is the second Yuzvinsky-Lam-Smith formula.

Theorem 4. *There exists a series of admissible triples of sizes*

$$\left[2n+2, 2^n - 2\binom{n-1}{\frac{n-1}{2}}, 2^n \right], \quad \text{for } n \geq 4 \text{ and } n \equiv 1 \mod 4.$$

Proof. For any $y = (y_1, \ldots, y_n) \in \mathbb{Z}_2^n$, define

$$\delta(y) = \begin{cases} 1, & \text{if } |y| \geq \frac{n+1}{2} + 1, \\ 1, & \text{if } |y| = \frac{n+1}{2} \text{ and } y_1 = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Let

$$B_1 = \{y \in \mathbb{Z}_2^n \mid |y| \geq \frac{n+1}{2} + 1\} \uplus \{y \in \mathbb{Z}_2^n \mid |y| = \frac{n+1}{2} \text{ and } y_1 = 0\}.$$

Then we have $\overline{e_0} + B_1 = \{y \in \mathbb{Z}_2^n \mid |y| \leq \frac{n-1}{2} - 1\} \uplus \{y \in \mathbb{Z}_2^n \mid |y| = \frac{n-1}{2} \text{ and } y_1 = 1\}$ and $\delta(B_1) = 1$. It is not hard to see that

$$\text{card} B = 2^n - 2 \binom{n-1}{\frac{n-1}{2}} \text{ and } H \cup \{e_0, \overline{e_0}\} + B = \mathbb{Z}_2^n.$$

To prove the theorem, it is enough to verify that $(H \cup \{e_0, \overline{e_0}\}, B)$ makes a multiplicative pair. According to the previous arguments, it remains to verify equation (4.9) for all $y \in B_1$ by symmetry.

We claim that for all $y \in B_1$ if $e_i + y \in B$, then $e_i + y \in B_1$. With this, it is clear that equation (4.9) holds for all $y \in B_1$ and the theorem follows.

The claim is confirmed in two cases according to the weight of y. First, if $|y| \geq \frac{n+1}{2} + 1$, then $|e_i + y| \geq \frac{n+1}{2}$. Certainly, if $e_i + y \in B$, then $e_i + y \in B_1$. Next, if $|y| = \frac{n+1}{2}$ and $y_1 = 0$, then $|e_i + y|$ is either $\frac{n+1}{2} + 1$ or $\frac{n-1}{2}$. If $|e_i + y| = \frac{n+1}{2} + 1$, then $e_i + y \in B$ implies $e_i + y \in B_1$. If $|e_i + y|$ were $\frac{n-1}{2}$, then $y_i = 1$. Therefore, if $e_i + y \in B$, then $e_i + y \in \overline{e_0} + B_1$ by the definition of B. More precisely, $e_i + y \in \{x \in \mathbb{Z}_2^n \mid |x| = \frac{n-1}{2} \text{ and } x_1 = 1\}$, and thus $(e_i + y)_1 = 1$. But this means that $i = 1$ since $y_1 = 0$ by assumption, which contradicts with the condition $y_i = y_1 = 1$ imposed earlier on y. $\qquad\square$

4.5. The case in which $n \equiv 2 \bmod 4$.
The idea is similar, only in this case more complicated $\mathbb{Z}_2^n$-graded quasialgebras and more delicate perturbation functions get involved. We shall consider the algebra $\mathbb{P}_n(n)$ and its H-set $H = \{e_i, e_i + e_n \mid 1 \leq i \leq n\}$. The verification that H is indeed an H-set is fairly easy and thus omitted. Note that $\rho(2^n) = 2n$ and we need to add two elements into the chosen H-set. We intend to expand H to $H \cup \{\overline{e_0}, \overline{e_n}\}$ according to the apparent symmetry of H with respect to e_n. Let $f = f_{\mathbb{P}(n)}$ and perturb it by δ_1, δ_2 and δ_3 in the following way:

$$f'(x,y) = \begin{cases} f(x,y) + \delta_1(y), & \text{if } x = \overline{e_0}, \\ f(x,y) + \delta_2(y), & \text{if } x = \overline{e_n}, \\ f(x,y) + \delta_3(y), & \text{if } x = e_0, \\ f(x,y), & \text{otherwise.} \end{cases}$$

Similarly, by routine calculations we have the following.

Lemma 4.5. $(H \cup \{\overline{e_0}, \overline{e_n}\}, B)$ *forms a multiplicative pair with respect to f' if and only if for $\forall h \in H \setminus \{e_0\}$ the following equations hold:*

$f'(\overline{e_0}, y) + f'(\overline{e_0}, y + \overline{h}) = f(h, \overline{h}) + 1$, *whenever $y, y + \overline{h} \in B$,*

$f'(\overline{e_n}, y) + f'(\overline{e_n}, y + \overline{h + e_n}) = f(h, h + \overline{e_n}) + 1$, *whenever $y, y + \overline{h + e_n} \in B$,*

$f'(e_0, y) + f'(e_0, y + h) = f(h, h) + 1$, *whenever $y, y + h \in B$,*

$f'(e_0, y) + f'(e_0, \overline{y}) + f'(\overline{e_0}, y) + f'(\overline{e_0}, \overline{y}) = 1$, *whenever $y, \overline{y} \in B$,*

$f'(e_0, y) + f'(e_0, y + \overline{e_n}) + f'(\overline{e_n}, y) + f'(\overline{e_n}, y + \overline{e_n}) = 1$, *whenever $y, y + \overline{e_n} \in B$,*

$f'(\overline{e_0}, y) + f'(\overline{e_0}, e_n + y) + f'(\overline{e_n}, y) + f'(\overline{e_n}, e_n + y) = 1$, *whenever $y, e_n + y \in B$,*

or, equivalently,

(4.12)
$$\delta_1(y) + \delta_1(y + \overline{h}) = f(\overline{e_0}, h) + f(h, \overline{e_0}) + 1, \quad \text{whenever } y, y + \overline{h} \in B,$$

(4.13)
$$\delta_2(y) + \delta_2(y + \overline{h} + e_n) = f(\overline{e_n}, h) + f(h, \overline{e_n}) + 1, \quad \text{whenever } y, y + \overline{h + e_n} \in B,$$

(4.14)
$$\delta_3(y) + \delta_3(y + h) = f(h, h) + 1, \quad \text{whenever } y, y + h \in B,$$

(4.15)
$$\delta_3(y) + \delta_3(\overline{y}) + \delta_1(y) + \delta_1(\overline{y}) = 0, \quad \text{whenever } y, \overline{y} \in B,$$

(4.16)
$$\delta_3(y) + \delta_3(y + \overline{e_n}) + \delta_2(y) + \delta_2(y + \overline{e_n}) = 0, \quad \text{whenever } y, y + \overline{e_n} \in B,$$

(4.17)
$$\delta_1(y) + \delta_1(e_n + y) + \delta_2(y) + \delta_2(e_n + y) = 0, \quad \text{whenever } y, y + e_n \in B.$$

Again, if we set $\delta = \delta_1 = \delta_2 = \delta_3$, then equations (4.15), (4.16), and (4.17) hold automatically. With this reduction, one has the following.

Lemma 4.6. $(H \cup \{\overline{e_0}, \overline{e_n}\}, B)$ *is a multiplicative pair if and only if the following equations hold:*

(4.18) $\qquad \delta(y) + \delta(y + \overline{e_i}) = 1, \quad \forall i \neq n, \text{ whenever } y, y + \overline{e_i} \in B,$

(4.19) $\qquad \delta(y) + \delta(y + \overline{e_i} + e_n) = 1, \quad \forall i \neq n, \text{ whenever } y, e_n + y + \overline{e_i} \in B,$

(4.20) $\qquad \delta(y) + \delta(y + e_i) = 0, \quad \forall i \neq n, \text{ whenever } y, y + e_i \in B,$

(4.21) $\qquad \delta(y) + \delta(y + e_i + e_n) = 0, \quad \forall i \neq n, \text{ whenever } y, e_n + y + e_i \in B,$

(4.22) $\qquad \delta(y) + \delta(y + \overline{e_n}) = 1, \quad \text{whenever } y, y + \overline{e_n} \in B,$

(4.23) $\qquad \delta(y) + \delta(y + \overline{e_n} + e_n) = 1, \quad \text{whenever } y, e_n + y + \overline{e_n} \in B,$

(4.24) $\qquad \delta(y) + \delta(y + e_n) = 0, \quad \text{whenever } y, e_n + y \in B.$

Proof. In equations (4.12)–(4.14) let h take turns to be e_n, e_i, and $e_i + e_n$, $i \neq n$, and carry out direct calculations. $\qquad \square$

We proceed to decide B in light of the preceding lemma and simultaneously by taking advantage of the obvious symmetry of $\mathbb{Z}_2^n$ as before. Assume $B = B_0 \uplus e_n + B_0$ in which B_0 is a subset of $\{y \in \mathbb{Z}_2^n \mid y_n = 0\}$. Assume also that for all $y \in \mathbb{Z}_2^n$, the equation $\delta(y) + \delta(y + e_n) = 0$ holds. Together with the symmetry of B, equations (4.18)–(4.24) are further reduced to:

(4.25) $\quad \delta(y) + \delta(y + e_i) = 0, \quad \forall i \neq n, \text{ whenever } y \in B_0, y + e_i \in B_0,$

(4.26) $\quad \delta(y) + \delta(y + e_i + \overline{e_n}) = 1, \quad \forall i \neq n, \text{ whenever } y \in B_0, y + e_i + \overline{e_n} \in B_0,$

(4.27) $\quad \delta(y) + \delta(y + \overline{e_n}) = 1, \quad \text{whenever } y \in B_0, y + \overline{e_n} \in B_0.$

Theorem 5. *There exists a series of admissible triples of sizes*

$$\left[2n + 2, 2^n - 4\binom{n-2}{\frac{n-2}{2}}, 2^n \right], \quad \text{for } n \geq 4 \text{ and } n \equiv 2 \mod 4.$$

Proof. We identify $\mathbb{Z}_2^{n-1}$ with $\{y \in \mathbb{Z}_2^n \mid y_n = 0\}$ by sending vector $y \in \mathbb{Z}_2^{n-1}$ to vector $(y, 0) \in \mathbb{Z}_2^n$. Thus, $\overline{e_n}$ functions exactly as $\overline{e_0}$ in $\mathbb{Z}_2^{n-1}$. From this point

of view, equations (4.25)–(4.27) are essentially identical to equations (4.9)–(4.11). Hence we can choose δ and B in a similar manner. More precisely, let

$$B_0 = B_1' \uplus \overline{e_n} + B_1',$$

where $B_1' = \{(y, 0) \mid y \in B_1\}$ and

$$B_1 = \{y \in \mathbb{Z}_2^{n-1} \mid |y| \geq \frac{n}{2} + 1\} \uplus \{y \in \mathbb{Z}_2^{n-1} \mid |y| = \frac{n}{2} \text{ and } y_1 = 0\}.$$

Let

$$\delta(y) = \begin{cases} 1, & \text{if } y \in B_1' \uplus e_n + B_1', \\ 0, & \text{otherwise.} \end{cases}$$

Hence $B = B_1' \uplus \{\overline{e_n} + B_1'\} \uplus \{e_n + B_1'\} \uplus \{\overline{e_0} + B_1'\}$, and by simple counting

$$\mathrm{card}B = 2^n - 4\binom{n-2}{\frac{n-2}{2}}.$$

Now with the easy fact $H \cup \{\overline{e_0}, \overline{e_n}\} + B = \mathbb{Z}_2^n$ the theorem follows. $\square$

5. Improvement of the Lenzhen-Morier-Genoud-Ovsienko formulas

In principle, given any admissible triple $[r, s, N]$, one can also construct new triples from it by decreasing the second and the third entries while preserving the first. Similar to the method of Yuzvinsky, the construction relies on an explicit realization of the known triple by multiplicative pairs. Morier-Genoud and Ovsienko constructed the Hurwitzian sets in their higher octonions $\mathbb{O}_n$ with the exception $n \equiv 0 \bmod 4$ in [11], and this enabled them to apply this idea on the Hurwitz-Radon triple $[\rho(2^n), 2^n, 2^n]$ to provide two infinite families of admissible triples in their joint work [8] with Lenzhen.

Note that in our series of algebras $\mathbb{P}_n(m)$ the Hurwitzian sets (of cardinality $\rho(2^n)$) can be constructed for all n. Hence we are able to increase the first entry of the Lenzhen-Morier-Genoud-Ovsienko triples in the case of $n \equiv 0 \bmod 4$. In addition, we observe that there is a flaw in their construction and by a proper remedy we can strengthen their admissible triples in some cases.

5.1. The idea of constructing new triples.
To begin with, we give more details on the idea of constructing new triples from the known ones. Suppose that (A, B) is a multiplicative pair in a suitable $\mathbb{Z}_2^n$-graded quasialgebra. Obviously, if $A_1 \subseteq A$ and $B_1 \subseteq B$, then (A_1, B_1) is a multiplicative pair as well and it results in a new triple $[\mathrm{card}(A_1), \mathrm{card}(B_1), \mathrm{card}(A_1 + B_1)]$ by Corollary 2.4.

There are two basic methods of constructing new triples in which the first entries are preserved. One is called *the method of addition*. Let $\{B_i\}$ be the set of all subsets of B. Then we get a series of new triples $[\mathrm{card}(A), \mathrm{card}(B_i), \mathrm{card}(A + B_i)]$. The subtlety is that one may move a step forward. Namely, by noticing that there might exist extra elements $y \in B \setminus B_i$ such that $A + \{y\} \subseteq A + B_i$ and if this is the case, we can expand B_i by $\{y\}$ and get better triples. Dually, the other is *the method of subtraction*. Let $C = A + B$ and let $\{C_i\}$ be the set of all subsets of C. For each C_i, one has the new triple $[\mathrm{card}(A), \mathrm{card}(B \setminus (A + C_i)), \mathrm{card}(A + \{B \setminus (A + C_i)\})]$. The reason why the last entry is not $\mathrm{card}(C \setminus C_i)$ is that the removal of $A + C_i$ from B may lead to the removal of some extra elements in $C \setminus C_i$. So one should use $\mathrm{card}(A + \{B \setminus (A + C_i)\})$ instead of $\mathrm{card}(C \setminus C_i)$ to get the more accurate formula.

In the following we give a description of the condition about whether the subtlety may happen in the multiplicative pair $(H, \mathbb{Z}_2^n)$.

Proposition 5.1. *Let H be a Hurwitzian set and let $B' \subseteq \mathbb{Z}_2^n$. Then $H + \{\mathbb{Z}_2^n \setminus (H + B')\} = \mathbb{Z}_2^n \setminus B'$ if and only if for all $z \in \mathbb{Z}_2^n \setminus B'$, $H + z \nsubseteq H + B'$,*

Proof. Clearly, the relation $H + \{\mathbb{Z}_2^n \setminus (H + B')\} \subsetneq \mathbb{Z}_2^n \setminus B'$ holds if and only if there exists an element $z \in \mathbb{Z}_2^n \setminus B'$, such that for all $y \in \mathbb{Z}_2^n \setminus (H + B')$, $z \notin H + y$ or, equivalently, $y \notin H + z$. Hence one has $H + z \subseteq H + B'$. This completes the proof. $\qquad\square$

Remark 5.2. There is a dual version for the method of addition. In addition, if the condition of the proposition holds, then the third entry of the triple $[\mathrm{card}(H), 2^n - \mathrm{card}(H + B'), 2^n - \mathrm{card}(B')]$ will not decrease by removing extra elements in $\mathbb{Z}_2^n \setminus B'$, and in the meantime, the second entry of the triple $[\mathrm{card}(H), \mathrm{card}(B'), \mathrm{card}(H + B')]$ will not increase by adding extra elements to B'.

Example 5.3. From subsection 4.2, one has $H = \{e_0, e_i, \overline{e_i} \mid 1 \le i \le 4\}$ is an H-set in case $n = 4$ and $H + \mathbb{Z}_2^4 = \mathbb{Z}_2^4$. Using the method of subtraction, to remove $B' = \{e_0, e_1\}$ from the second $\mathbb{Z}_2^4$, one has to remove $H + B'$ from the first $\mathbb{Z}_2^4$. However, in this situation one easily derives that $H + B' = \mathbb{Z}_2^4$. Therefore, one has such an unusual formula:

$$H + \{\mathbb{Z}_2^4 \setminus (H + B')\} = H + \varnothing = \varnothing =\subsetneq \mathbb{Z}_2^4 \setminus B'.$$

Dually, after using the method of addition to get $[\mathrm{card}(H), \mathrm{card}(B'), \mathrm{card}(\mathbb{Z}_2^4)]$ one needs to move forward by expanding B' to Z_2^4 in order to get a better triple $[\mathrm{card}(H), \mathrm{card}(\mathbb{Z}_2^4), \mathrm{card}(\mathbb{Z}_2^4)]$. This example explains the subtlety in both the method of subtraction and the method of addition.

5.2. **Strengthening the Lenzhen-Morier-Genoud-Ovsienko formulas.** Take H to be the Hurwitzian set defined in (4.1) and let B be a subset of $\mathbb{Z}_2^n$. Expand B to the utmost B' such that $H + B = H + B'$ and obtain triples $[\mathrm{card}(H), \mathrm{card}(B'), \mathrm{card}(H + B')]$ and $[\mathrm{card}(H), 2^n - \mathrm{card}(H + B'), 2^n - \mathrm{card}(B')]$ by Proposition 5.1.

For convenience, let $e_{ij} \triangleq e_i + e_j$ and $\overline{e_{ij}} \triangleq \overline{e_0} + e_{ij}$ and define $\Gamma(l, k)$ with $1 \le l < k \le n$ as

$$\Gamma(l, k) = \{e_{ij} \in \mathbb{Z}_2^n \mid 1 \le i < j < k\} \cup \{e_{ik} \in \mathbb{Z}_2^n \mid 1 \le i \le l\}.$$

We will construct subsets B_{lk} and B'_{lk} via $\Gamma(l, k)$ and get the following triples:

Theorem 6. *Let $n > 4$ and $1 \le l < k \le n$.*

(1) *If $n \ge 5$ and $n = 1, 2 \bmod 4$, then there exist square identities of sizes $[r, s, N]$ with*

(5.1)
$$\begin{cases} r &= \rho(2^n), \\ s &= 2\left(\binom{k-1}{2} + l + 1\right), \\ N &= 2\left(\binom{k-1}{2} + l + 1\right)n - 4\binom{k}{3} - 2kl, \end{cases}$$

while $k \le n - 2$;
if $k = n - 1$ and $l \le n - 3$, there are square identities of sizes $[r, s + 2l, N]$;
if $k = n - 1$ and $l = n - 2$, there are square identities of sizes $[r, s + 2l + 2, N]$;
if $k = n$, there are square identities of sizes $[r, s + 2(n - 1 - l), N]$.

(2) *If $n \geq 8$ and $n = 0, 3 \bmod 4$, then there exist square identities of sizes $[r, s, N]$ with*

(5.2)
$$
\begin{cases}
r &= \rho(2^n), \\
s &= 2\left(\binom{k-1}{2} + l + 1\right), \\
N &= 2\left(\binom{k-1}{2} + l + 1\right)(n+1) - 4\binom{k}{3} - 2kl,
\end{cases}
$$

while $k \leq n - 1$;
if $k = n$ and $l \leq n - 2$, there are square identities of sizes $[r, s + 2l, N]$;
if $k = n$ and $l = n - 1$, there are square identities of sizes $[r, s + 2l + 2, N]$.

Proof. In this proof, we always assume $i < j$ in the notation of e_{ij}.

(1) *Cases in which $n \equiv 1, 2 \bmod 4$.* Recall that $H = \{e_m, e_1 + e_m \mid 1 \leq m \leq n\}$ is an H-set. Let $B_{lk} = \{e_0, e_1, e_{ij}, e_1 + e_{ij} \mid e_{ij} \in \Gamma(l, k)\}$ whose cardinality is

$$
\mathrm{card}(B_{lk}) = 2 + 2\binom{k-1}{2} + 2l.
$$

The summation of H and any element e_{ij} of $\Gamma(l, k)$ is

$$
H + e_{ij} = \{e_i, e_j, e_{ij} + e_m, e_1 + e_i, e_1 + e_j, e_1 + e_{ij} + e_m \mid i \neq m \neq j\},
$$

which is identical to $H + \{e_1 + e_{ij}\}$ as H is symmetric with respect to e_1. Hence the corresponding sumset is then of the form

$$
H + B_{lk} = H \cup \bigcup_{e_{ij} \in \Gamma(l,k)} \{H + e_{ij}\}.
$$

Therefore its cardinality is

$$
\mathrm{card}(H + B_{lk}) = 2n + 2\left(\sum_{1 \leq i < j \leq k-1} (n-j) + l(n-k)\right)
$$
$$
= 2\left(\binom{k-1}{2} + l + 1\right)n - 4\binom{k}{3} - 2kl.
$$

Further, we expand B_{lk} to its utmost B'_{lk} by adding elements in $\mathbb{Z}_2^n \setminus B_{lk}$ by enumeration. Suppose e_x is an element not in B_{lk}.

(a) If $|e_x| \geq 5$, then $e_x + e_0$ is not in $H + B_{lk}$. Hence no elements of this form can be added into B'_{lk}.

(b) If $e_x = e_{i_1} + e_{i_2} + e_{i_3} + e_{i_4}$ with $i_1 < i_2 < i_3 < i_4$, then there exists an element $e_{i_5} \in H$ where $i_5 \notin \{i_1, i_2, i_3, i_4\}$, such that $e_x + e_{i_5} \notin H + B_{lk}$. Therefore B'_{lk} contains no elements of this form.

(c) If $e_x = e_{i_1} + e_{i_2} + e_{i_3}$ with $1 < i_1 < i_2 < i_3$, then there exists an element $e_{i_4} \in H$ where $i_4 \notin \{1, i_1, i_2, i_3\}$, such that $e_x + e_{i_4} \notin H + B_{lk}$. Hence e_x cannot be added into B'_{lk}. If $e_x = e_1 + e_{i_1 i_2}$ where $e_{i_1 i_2} \notin \Gamma(l, k)$ and $1 < i_1 < i_2$, then we have $e_x + H = e_{i_1 i_2} + H$. The next case is similar to this, so we discuss them together in the following.

(d) If $e_x = e_{i_1 i_2}$ with $e_{i_1 i_2} \notin \Gamma(l, k)$, then whether e_x satisfies the condition of Proposition 5.1 depends on the parameters l and k. Now, as mentioned above, we only need to check whether $e_{i_1 i_2} + e_m \in H + B_{lk}$. Since $e_{i_1 i_2} + e_m$ can only appear in $H + \{e_{i_1 m}\}$ or $H + \{e_{i_2 m}\}$, it suffices to check whether $e_{i_1 m}$ or $e_{i_2 m}$ belongs to $\Gamma(l, k)$ for all $m \neq i_1, i_2$. If

so, then e_x and $e_1 + e_x$ can be added into B'_{lk}. In the following we separate the discussions into several cases:

(i) $k \le n - 2$.
- (A) If $i_1 < i_2 \le n - 1$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n$.
- (B) If $i_1 < n - 1$ and $i_2 = n$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n - 1$.
- (C) If $i_1 = n - 1$ and $i_2 = n$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n - 2$.

Hence in this case, no elements can be added into B'_{lk}.

(ii) $k = n - 1$ and $l \le n - 3$.
- (A) If $i_1 \le l$ and $i_2 = n$, then $e_{i_1 m} \in \Gamma(l, k)$ holds for all $m \ne i_1, i_2$, so these $2l$ elements of the form $e_{i_1 i_2}$ and $e_1 + e_{i_1 i_2}$ can be added into B'_{lk}.
- (B) If $l < i_1 < n - 1$ and $i_2 = n$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n - 1$.
- (C) If $i_1 = n - 1$ and $i_2 = n$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n - 2$.
- (D) If $l < i_1 < i_2 = n - 1$, then $e_{i_1 m}$, $e_{i_2 m} \notin \Gamma(l, k)$ when $m = n$.

(iii) $k = n - 1$ and $l = n - 2$.
- (A) If $i_1 \le l$ and $i_2 = n$, then $e_{i_1 m} \in \Gamma(l, k)$ holds for all $m \ne i_1, i_2$, so these $2l$ elements of the form $e_{i_1 i_2}$ and $e_1 + e_{i_1 i_2}$ can be added.
- (B) If $i_1 = n - 1$ and $i_2 = n$, then $e_{i_1 m}$ is always in $\Gamma(l, k)$ for all $m \ne i_1, i_2$, so these 2 elements $e_{i_1 i_2}$ and $e_1 + e_{i_1 i_2}$ can be added.

(iv) $k = n$.
If $l < i_1 < i_2 = n$, then $e_{i_1 m} \in \Gamma(l, k)$ holds for all $m \ne i_1, i_2$, so these $2(n - 1 - l)$ elements of the form $e_{i_1 i_2}$ and $e_1 + e_{i_1 i_2}$ can be added.

(e) If $e_x = e_{i_1} \notin B_{lk}$, then $H + e_{i_1}$ is exactly $H + e_{1 i_1}$. This has already been discussed in the above case.

(2) The proof for the cases in which $n \equiv 0, 3 \mod 4$ is similar to the above cases except that $\overline{e_0}$ plays the role of e_1. $\qquad\square$

From the proof of the above theorem, one can easily conclude that B'_{lk} is the utmost subset that can be expanded from B_{lk}. Hence by Proposition 5.1 and Remark 5.2, one has the following.

Corollary 5.4. *Let $[r, s', N]$ be the admissible triples obtained in Theorem 6. Then there exists a series of admissible triples of the form $[r, 2^n - N, 2^n - s']$.*

Example 5.5. Theorem 6 generates several best known admissible triples (see [14]):

n	(l, k)	triple	method
5	$(2, 4)$	$[10, 16, 28]$	addition
5	$(3, 4)$	$[10, 22, 30]$	addition
6	$(1, 2)$	$[12, 44, 60]$	subtraction
6	$(1, 3)$	$[12, 38, 58]$	subtraction
6	$(4, 5)$	$[12, 32, 52]$	addition

Remark 5.6. The admissible triples obtained here strengthen the Lenzhen-Morier-Genoud-Ovsienko formulas in the following aspects: First, since our twisting function is a bit more complex than theirs, we are able to avoid the exception of finding Hurwitzian sets when $n \equiv 0 \mod 4$ and optimise the corresponding triples; Second, by observing the subtlety of the method of subtraction in constructing new triples, the Lenzhen-Morier-Genoud-Ovsienko formulas can be improved in several cases, especially when k is close to n the third entries of their triples can be decreased; Third, using the same method of constructing the second families of the Lenzhen-Morier-Genoud-Ovsienko triples [8, Theorem 2], we can also provide similar families of triples for $n \equiv 0, 2 \mod 4$.

Furthermore, by observing the symmetry of the Hurwitzian set in the case $n \geq 8$ and $n = 0 \mod 4$, we are able to expand the corresponding multiplicative pairs and improve the triples.

Proposition 5.7. *If $n \geq 8$ and $n = 0 \mod 4$, then there exist square identities of sizes $[r, s, N]$ with*

$$(5.3) \qquad \begin{cases} r & = & \rho(2^n) + 1, \\ s & = & 2\left(\binom{k-1}{2} + l + 1\right), \\ N & = & 2\left(\binom{k-1}{2} + l + 1\right)(n+1) - 4\binom{k}{3} - 2kl, \end{cases}$$

while $k \leq n - 1$;
if $k = n$ and $l \leq n - 2$, there are square identities of sizes $[r, s + 2l, N]$;
if $k = n$ and $l = n - 1$, there are square identities of sizes $[r, s + 2l + 2, N]$.

Proof. In fact, notice that in this case we expand the Hurwitzian set H by $\overline{e_0}$ to H', thus obtain a more symmetric multiplicative pair (H', B), which yields the first family of the Yuzvinsky-Lam-Smith formulas. By applying the method of addition on this pair and expanding the subset $B_{lk} = \{e_0, \overline{e_0}, e_{ij}, \overline{e_0} + e_{ij} \mid e_{ij} \in \Gamma(l,k)\}$ to B'_{lk} in the same manner, one obtains the desired result. The reason why this procedure works is that B'_{lk} contains elements whose weights are either ≤ 2 or $\geq n - 2$, i.e., B'_{lk} does not intersect with $\mathbb{Z}_2^n \setminus B$. $\qquad\square$

5.3. **The cases in which $n = 4$ and $n = 7$.** Notice that in Theorem 6, we exclude the cases in which $n = 4$ and 7. The reason is that the general argument therein breaks down into these two specific cases. Nevertheless, with care we can find suitable multiplicative pairs and realize the associated triples. For the sake of completeness, we list below the results while omitting further details:

(1) If $n = 4$, then we have the admissible triples $[9, s, 8 + s]$ for $s = 1, 2, \ldots, 7$. These are very well-known triples; see [14].
(2) If $n = 7$, then the formulas in Theorem 6 are still correct for $k \leq 5$ and for $l = 1$, $k = 6$. As for the others, we list them in the following table:

(l,k)	addition	subtraction	(l,k)	addition	subtraction
$(2,6)$	$[16, 30, 104]$	$[16, 24, 98]$	$(3,6)$	$[16, 40, 108]$	$[16, 20, 88]$
$(4,6)$	$[16, 54, 112]$	$[16, 16, 74]$	$(5,6)$	$[16, 72, 116]$	$[16, 12, 56]$
$(1,7)$	$[16, 76, 118]$	$[16, 10, 52]$	$(2,7)$	$[16, 82, 120]$	$[16, 8, 46]$
$(3,7)$	$[16, 90, 122]$	$[16, 6, 38]$	$(4,7)$	$[16, 100, 124]$	$[16, 4, 28]$
$(5,7)$	$[16, 112, 126]$	$[16, 2, 16]$	$(6,7)$	$[16, 128, 128]$	$[16, 0, 0]$

6. Some new families of admissible triples

In this section, we apply the method of addition on the Yuzvinsky formulas and obtain some new families of admissible triples:

Theorem 7. *Let $n \geq 4$.*

(1) *If $n \equiv 0$ mod 4, then there exists a series of admissible triples of sizes:*

$$\left[2n + 2, 2\sum_{i=0}^{k} \binom{n}{i}, 2\sum_{i=0}^{k+1} \binom{n}{i}\right], \quad k = 0, \ldots, \frac{n}{2} - 2.$$

(2) *If $n \equiv 1$ mod 4, then there exists a series of admissible triples of sizes:*

$$\left[2n + 2, 2\sum_{i=0}^{k} \binom{n}{i}, 2\sum_{i=0}^{k+1} \binom{n}{i}\right], \quad k = 0, \ldots, \frac{n-1}{2} - 2.$$

(3) *If $n \equiv 2$ mod 4, then there exists a series of admissible triples of sizes:*

$$\left[2n + 2, 4\sum_{i=0}^{k} \binom{n-1}{i}, 4\sum_{i=0}^{k+1} \binom{n-1}{i}\right], \quad k = 0, \ldots, \frac{n-2}{2} - 2.$$

Proof. Denote by (H', B) the multiplicative pairs corresponding to the Yuzvinsky admissible triples in each case. We prove the theorem case by case according to the residue of n modulo 4.

(1) $n \equiv 0 \mod 4$. Recall from subsection 4.3 that

$$H' = \{e_i, \overline{e_i} \mid 0 \leq i \leq n\} \text{ and } B = \{y \in \mathbb{Z}_2^n \mid |y| \neq n/2\}.$$

Let $B_k = \{y \in \mathbb{Z}_2^n \mid |y| \leq k \text{ or } |y| \geq n - k\}$, $k = 0, \ldots, n/2 - 2$. Then one has $B_k \subseteq B$ and $\text{card}(B_k) = 2\sum_{i=0}^{k} \binom{n}{i}$. By the symmetry of H' and B_k, it is not hard to see that

$$H' + B_k = B_{k+1} = \{y \in \mathbb{Z}_2^n \mid |y| \leq k + 1 \text{ or } |y| \geq n - k - 1\}.$$

Moreover, for any $y \in B \setminus B_k$, one has $H' + y \not\subseteq B_{k+1}$.

(2) $n \equiv 1 \mod 4$. Recall from subsection 4.4 that $H' = \{e_i, \overline{e_i} \mid 0 \leq i \leq n\}$ and

$$B = \mathbb{Z}_2^n \setminus \left\{ \{y \in \mathbb{Z}_2^n \mid |y| = \frac{n+1}{2} \text{ and } y_1 = 1\} \right.$$
$$\left. \uplus \{y \in \mathbb{Z}_2^n \mid |y| = \frac{n-1}{2} \text{ and } y_1 = 0\}\right\}.$$

Let $B_k = \{y \in \mathbb{Z}_2^n \mid |y| \leq k \text{ or } |y| \geq n - k\}$, $k = 0, \ldots, (n-1)/2 - 2$. Then by a similar manner, one obtains the desired result.

(3) $n \equiv 2 \mod 4$. Recall from subsection 4.5 that

$$H' = \{e_i, e_i + e_n, \overline{e_0}, \overline{e_n} \mid 1 \leq i \leq n\},$$
$$B = B_1' \uplus \{\overline{e_n} + B_1'\} \uplus \{e_n + B_1'\} \uplus \{\overline{e_0} + B_1'\},$$

where $B_1' = \{(y, 0) \mid y \in B_1\}$, and

$$B_1 = \{y \in \mathbb{Z}_2^{n-1} \mid |y| \geq \frac{n}{2} + 1\} \uplus \{y \in \mathbb{Z}_2^{n-1} \mid |y| = \frac{n}{2} \text{ and } y_1 = 0\}.$$

For $k = 0, \ldots, (n-2)/2 - 2$, let

$$B_k = B'_{1k} \uplus \{\overline{e_n} + B'_{1k}\} \uplus \{e_n + B'_{1k}\} \uplus \{\overline{e_0} + B'_{1k}\},$$

where $B'_{1k} = \{(y, 0) \mid y \in B_{1k}\}$ and $B_{1k} = \{y \in \mathbb{Z}_2^{n-1} \mid |y| \leq k \text{ or } |y| \geq n-1-k\}$. It is obvious that $B_k \subseteq B$ and $\operatorname{card}(B_k) = 4 \sum_{i=0}^{k} \binom{n-1}{i}$. Similarly, by the symmetry of H' and B_k, one has $H' + B_k = B_{k+1}$. Moreover, if $y \in B \setminus B_k$, then $H' + y \nsubseteq B_{k+1}$, which means that B_k cannot be expanded in this situation.

$\square$

Remark 6.1. Note that if increasing k by 1 at the "border" of each case in the above theorem, then one will recover the Yuzvinsky admissible triples by expanding B_k to B. Take $k = 1$ in the first two series of admissible triples, then the resulting square identities improve the well-known Lagrange identity. More preciously, our third entries are nearly half of that of the latter. In general, our new triples look very similar to those of [8, Theorem 2] as the idea of construction is nearly the same. The only difference is that our starting point is the Yuzvinsky triples instead of the Hurwitz-Radon triples in *loc. cit.*

References

[1] Helena Albuquerque and Shahn Majid, *Quasialgebra structure of the octonions*, J. Algebra **220** (1999), no. 1, 188–224, DOI 10.1006/jabr.1998.7850. MR1713433

[2] Helena Albuquerque and Shahn Majid, *Clifford algebras obtained by twisting of group algebras*, J. Pure Appl. Algebra **171** (2002), no. 2-3, 133–148, DOI 10.1016/S0022-4049(01)00124-4. MR1904473

[3] M. F. Atiyah, R. Bott, and A. Shapiro, *Clifford modules*, Topology **3** (1964), no. suppl. 1, 3–38. MR0167985

[4] V. G. Drinfel'd, *Quasi-Hopf algebras* (Russian), Algebra i Analiz **1** (1989), no. 6, 114–148; English transl., Leningrad Math. J. **1** (1990), no. 6, 1419–1457. MR1047964

[5] A. Hurwitz, *Uber die Komposition der quadratischen Formen von beliebig vielen Variablen*, Nahr. Ges. Wiss. Göttingen, 1898, pp. 309–316.

[6] A. Hurwitz, *Über die Komposition der quadratischen Formen* (German), Math. Ann. **88** (1922), no. 1-2, 1–25, DOI 10.1007/BF01448439. MR1512117

[7] T. Y. Lam and Tara L. Smith, *On Yuzvinsky's monomial pairings*, Quart. J. Math. Oxford Ser. (2) **44** (1993), no. 174, 215–237, DOI 10.1093/qmath/44.2.215. MR1222375

[8] Anna Lenzhen, Sophie Morier-Genoud, and Valentin Ovsienko, *New solutions to the Hurwitz problem on square identities*, J. Pure Appl. Algebra **215** (2011), no. 12, 2903–2911, DOI 10.1016/j.jpaa.2011.04.011. MR2811573

[9] Shahn Majid, *Algebras and Hopf algebras in braided categories*, Advances in Hopf algebras (Chicago, IL, 1992), Lecture Notes in Pure and Appl. Math., vol. 158, Dekker, New York, 1994, pp. 55–105. MR1289422

[10] Shahn Majid, *Foundations of quantum group theory*, Cambridge University Press, Cambridge, 1995. MR1381692

[11] Sophie Morier-Genoud and Valentin Ovsienko, *A series of algebras generalizing the octonions and Hurwitz-Radon identity*, Comm. Math. Phys. **306** (2011), no. 1, 83–118, DOI 10.1007/s00220-011-1279-9. MR2819420

[12] J. Radon, *Lineare scharen orthogonaler matrizen* (German), Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 1–14, DOI 10.1007/BF02940576. MR3069384

[13] A. R. Rajwade, *Squares*, London Mathematical Society Lecture Note Series, vol. 171, Cambridge University Press, Cambridge, 1993. MR1253071

[14] Daniel B. Shapiro, *Compositions of quadratic forms*, de Gruyter Expositions in Mathematics, vol. 33, Walter de Gruyter & Co., Berlin, 2000. MR1786291

[15] Sergey Yuzvinsky, *Orthogonal pairings of Euclidean spaces*, Michigan Math. J. **28** (1981), no. 2, 131–145. MR616264

[16] Sergey Yuzvinsky, *A series of monomial pairings*, Linear and Multilinear Algebra **15** (1984), no. 2, 109–119, DOI 10.1080/03081088408817582. MR740665

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405 – AND – SCHOOL OF MATHEMATICS, SHANDONG UNIVERSITY, JINAN 250100, PEOPLE'S REPUBLIC OF CHINA
  E-mail address: `yaqhu@indiana.edu`
  E-mail address: `yachinghu@mail.sdu.edu.cn`

SCHOOL OF MATHEMATICAL SCIENCES, HUAQIAO UNIVERSITY, QUANZHOU 362021, PEOPLE'S REPUBLIC OF CHINA – AND – SCHOOL OF MATHEMATICS, SHANDONG UNIVERSITY, JINAN 250100, PEOPLE'S REPUBLIC OF CHINA
  E-mail address: `hualin.huang@hqu.edu.cn`
  E-mail address: `hualin@sdu.edu.cn`

SCHOOL OF MATHEMATICS, SHANDONG UNIVERSITY, JINAN 250100, PEOPLE'S REPUBLIC OF CHINA
  E-mail address: `chizhang@mail.sdu.edu.cn`