RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 26 = 551 (2022): 65-89
DOI: https://doi.org/10.21857/moxpjh1n5m

MATRIX MORPHOLOGY AND COMPOSITION OF HIGHER DEGREE FORMS WITH APPLICATIONS TO DIOPHANTINE EQUATIONS

Ajai Choudhry

Abstract. In this paper we use matrices to obtain new composition identities $f(x_i)f(y_i) = f(z_i)$, where $f(x_i)$ is an irreducible form, with integer coefficients, of degree n in n variables (n being 3, 4, 6 or 8), and $x_i, y_i,\ i = 1, 2, \ldots, n$, are independent variables while the values of $z_i,\ i = 1, 2, \ldots, n$, are given by bilinear forms in the variables x_i, y_i. When $n = 2, 4$ or 8, we also obtain new composition identities $f(x_i)f(y_i)f(z_i) = f(w_i)$ where, as before, $f(x_i)$ is an irreducible form, with integer coefficients, of degree n in n variables while $x_i, y_i, z_i,\ i = 1, 2, \ldots, n$, are independent variables and the values of $w_i,\ i = 1, 2, \ldots, n$, are given by trilinear forms in the variables x_i, y_i, z_i, and such that the identities cannot be derived from any identities of the type $f(x_i)f(y_i) = f(z_i)$. Further, we describe a method of obtaining both these types of composition identities for forms of higher degrees. We also describe a method of generating infinitely many integer solutions of certain quartic and octic diophantine equations $f(x_1, \ldots, x_n) = 1$ where $f(x_1, \ldots, x_n)$ is a form that admits a composition identity and $n = 4, 6$ or 8.

1. Introduction

Let $f : \mathbb{R}^n \to \mathbb{R}$ be an algebraic form, or simply a form, i.e., a homogeneous polynomial in n variables. A form f is said to be a form admitting composition or a composable form if

$$f(x_1, x_2, \ldots, x_n)f(y_1, y_2, \ldots, y_n) = f(z_1, z_2, \ldots, z_n), \tag{1.1}$$

where each variable $z_i,\ i = 1, 2, \ldots, n$, is a bilinear form in the variables $x_i, y_i,\ i = 1, 2, \ldots, n$, that is,

$$z_i = \phi(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{j=1}^{n}\sum_{k=1}^{n} \lambda_{ijk}x_jy_k,\ \ i = 1, 2, \ldots, n, \tag{1.2}$$

2020 *Mathematics Subject Classification.* 11E76, 11E16, 11C20, 11D25, 11D41.
Key words and phrases. Composition of forms, higher degree forms, threefold composition of forms, unital commutative algebra of matrices, higher degree diophantine equations.

for certain constants λ_{ijk} and for all $x_i, y_i \in \mathbb{R}$.

The subject of higher degree forms that admit composition has been studied by several authors [1, 2, 4–7]. Dickson [1, pp. 222, 224] has given general theorems describing all high degree ternary and quaternary forms admitting composition. While these theorems yield higher degree composable forms with complex coefficients, they are of little help in finding higher degree forms that admit composition and have only integer coefficients. It seems that the existing literature contains only two explicit nontrivial examples of high degree composable forms with integer coefficients, namely the determinant of an $n \times n$ matrix yields a composable form of degree n in n^2 variables, and the norm of an algebraic integer yields a composable form of degree n in n variables.

In this paper we will study forms admitting composition with a view to obtaining infinitely many integer solutions of certain higher degree diophantine equations and accordingly, we will consider only those forms which have integer coefficients, i.e., $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, and such that the constants λ_{ijk} in the relations (1.2) are also all integers. Further, when we refer to a form being irreducible, we mean irreducibility over $\mathbb{Q}$.

We describe a new technique of finding composition identities (1.1) by using matrices. We use this technique to obtain composition identities (1.1) when f is an irreducible form of degree n in n variables and $n = 3$, 4, 6 or 8.

Further, by using the new technique described in this paper, we also obtain forms that satisfy a law of composition that is an extension of the usual composition law defined by (1.1). We say that a form f admits threefold composition if, for all $x_i, y_i, z_i \in \mathbb{R}$,

$$f(x_1, \ldots, x_n) f(y_1, \ldots, y_n) f(z_1, \ldots, z_n) = f(w_1, \ldots, w_n), \tag{1.3}$$

where each $w_i = \phi(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n, z_1, z_2, \ldots, z_n)$ is a trilinear form in the variables x_i, y_i, z_i, and the identity (1.3) cannot be derived from an identity of type (1.1). In fact, the form f need not admit any composition identity of type (1.1) for it to admit a threefold composition identity.

We will show that every binary quadratic form admits threefold composition. We also obtain examples of quaternary quartic forms and octonary octic forms that admit threefold composition. Such threefold composition of forms has not been studied till now and all these results are new.

It would be recalled that, when d is a positive integer which is not a perfect square, the well-known identity for composition of forms, namely

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2,$$

may be applied to generate infinitely many integer solutions of Pell's equation $x^2 - dy^2 = 1$ starting from a single known integer solution. We describe an analogous method for obtaining infinitely many integer solutions of certain quartic and higher degree diophantine equations,

$$f(x_1, x_2, \ldots, x_n) = 1, \tag{1.4}$$

by using the composition identities (1.1) and (1.3). We give several examples to illustrate the method.

In Sect. 2 we discuss how matrices may be used to obtain forms that satisfy composition identities. In Sect. 3 we construct examples of higher degree forms admitting composition and solve certain related diophantine equations. Similarly, in Sect. 4 we construct forms admitting threefold composition and consider related diophantine equations. We conclude the paper with certain remarks and open problems regarding matrix morphology, composition of higher degree forms and related diophantine equations.

2. Matrix morphology, composable forms and diophantine equations

All the matrices considered in this paper are square matrices over the field of real numbers. The determinant of the product of square matrices is equal to the product of their determinants. So, if $A = [x_{ij}]$ and $B = [y_{ij}]$ are two arbitrary $n \times n$ matrices and $C = AB$, then

$$\det A \det B = \det C. \tag{2.1}$$

The identity (2.1) and the fact that the entries of the matrix C are bilinear forms in the entries of the matrices A and B immediately yield the composable form f of degree n in n^2 variables:

$$f : \mathbb{R}^{n^2} \to \mathbb{R}, \quad f(x_{11}, x_{12}, \ldots, x_{nn}) = \det [x_{ij}].$$

The form f is, however, of little interest as the number of variables is too large compared to the degree of the form. In Sect. 2.1 we will show that the identity (2.1) can be used to obtain composable forms of degree n in just n variables for several values of $n \geq 3$.

2.1. *The morphology of matrices.* The set $M_n(\mathbb{R})$ of all real square matrices of order n is a vector space over the field of real numbers with vector addition being the usual matrix addition and scalar multiplication being the usual scalar multiplication of matrices. Since matrix multiplication is distributive, and $(aM_1)(bM_2) = (ab)(M_1M_2)$ when $a, b \in \mathbb{R}$ and $M_1, M_2 \in M_n(\mathbb{R})$, it follows that matrix multiplication is bilinear. Thus, the vector space $M_n(\mathbb{R})$ is equipped with a bilinear product, and hence the set $M_n(\mathbb{R})$ of all $n \times n$ matrices over $\mathbb{R}$ is an algebra over the field $\mathbb{R}$. In fact, $M_n(\mathbb{R})$ is a unital associative algebra since matrix multiplication is associative and there is a neutral element, namely the identity matrix, for the bilinear product (matrix multiplication). Every subalgebra of $M_n(\mathbb{R})$ is closed under the operations of matrix addition, scalar multiplication, and multiplication of matrices. Further, the set of all $n \times n$ matrices whose entries are integers, namely the set $M_n(\mathbb{Z})$, is also closed under addition, scalar multiplication by integers, and multiplication of matrices.

Let $\mathcal{L}$ be a subalgebra of $M_n(\mathbb{R})$ whose dimension is $0 < h < n^2$, $\dim \mathcal{L} = h$, and whose basis is $\{A_1, \ldots, A_h\}$. Every matrix in $\mathcal{L}$ can be written in a unique way as a finite linear combination of elements of the basis, i.e., for each $A \in \mathcal{L}$, there exist unique coefficients $x_1, \ldots, x_h \in \mathbb{R}$ such that

$$A = x_1 A_1 + \cdots x_h A_h.$$

Obviously, each entry of the matrix A is a linear form in the variables $x_1, \ldots, x_h$. Since the coefficients $x_1, \ldots, x_h$ of A are unique, with respect to the basis $\{A_1, \ldots, A_h\}$, each matrix $A \in \mathcal{L}$ can be seen as a function,

$$A : \mathbb{R}^h \to \mathcal{L}, \quad A(x_1, \ldots, x_h) = x_1 A_1 + \cdots x_h A_h. \tag{2.2}$$

Therefore, each matrix in $\mathcal{L}$ can be naturally denoted by $A(x_1, \ldots, x_h)$.

Since the subalgebra $\mathcal{L}$ is closed with respect to matrix multiplication, the product of two arbitrary matrices $A(x_1, \ldots, x_h), A(y_1, \ldots, y_h) \in \mathcal{L}$ may be written as $A(z_1, \ldots, z_h) \in \mathcal{L}$ where the values of $z_i, i = 1, \ldots, h$, are given by bilinear forms in the variables $x_1, \ldots, x_h, y_1, \ldots, y_h$. It follows from the relation $A(x_1, \ldots, x_h)A(y_1, \ldots, y_h) = A(z_1, \ldots, z_h)$ that

$$\det\left(A(x_1, \ldots, x_h)\right) \det\left(A(y_1, \ldots, y_h)\right) = \det\left(A(z_1, \ldots, z_h)\right), \tag{2.3}$$

and hence the form $f : \mathbb{R}^h \to \mathbb{R}$, $f(x_1, \ldots, x_h) = \det\left(A(x_1, \ldots, x_h)\right)$, satisfies the identity,

$$f(x_1, \ldots, x_h) f(y_1, \ldots, y_h) = f(z_1, \ldots, z_h), \tag{2.4}$$

for all $x_i, y_i \in \mathbb{R}$, and is thus a composable form of degree n. If the matrices $A_1, \ldots, A_h$ have integer entries, we get a form $f : \mathbb{Z}^h \to \mathbb{Z}$ with integer coefficients.

We note here that the set

$$\mathcal{L}(\mathbb{Z}) = \{A(x_1, \ldots, x_h) = x_1 A_1 + \cdots x_h A_h : x_i \in \mathbb{Z}, i = 1, \ldots, h\}, \tag{2.5}$$

is also closed under addition, scalar multiplication by integers and multiplication of matrices.

We now give an example of a subalgebra of $M_n(\mathbb{R})$. Let the minimal polynomial of the matrix $M \in M_n(\mathbb{R})$ be $g(x) = a_0 + a_1 x + \cdots + a_h x^h$, $a_h \neq 0$. Obviously, the set $\{I_n, M, M^2, \ldots, M^{h-1}\}$ is linearly independent. Further, $M^h = a_h^{-1}(a_0 I_n + a_1 M + \cdots + a_{h-1} M^{h-1})$ implies that all powers M^k, $k \geq h$, can be written as linear combinations of $I_n, M, \ldots, M^{h-1}$. Hence, $\text{span}\{I_n, M, M^2, \ldots, M^{h-1}\}$, i.e.,

$$\{x_1 I_n + x_2 M + \cdots + x_h M^{h-1} : x_1, \ldots, x_h \in \mathbb{R}\}, \tag{2.6}$$

represents a subalgebra of $M_n(\mathbb{R})$. In fact, this particular subalgebra is also commutative and contains unity (I_n). Thus, it is an example of a unital commutative algebra over $\mathbb{R}$. We could choose the matrix M suitably and try to obtain examples of composable forms but this approach did not yield any interesting results.

We give below a couple of preliminary lemmas that we will use to construct further examples of subalgebras of $M_n(\mathbb{R})$. In these lemmas and, in fact, throughout this paper, whenever we refer to the span of a set of matrices, $M_1, M_2, \ldots, M_n$, we mean the set of all linear combinations $x_1M_1 + x_2M_2 + \cdots + x_nM_n$ where $x_1, x_2, \ldots, x_n \in \mathbb{R}$.

LEMMA 2.1. *If $\mathcal{V} = \text{span}\{A_1, A_2, \ldots, A_h\}$, where $\{A_1, A_2, \ldots, A_h\}$ is a linearly independent set of matrices in $M_n(\mathbb{R})$, and the matrix product $A_iA_j \in \mathcal{V}$, for all $i, j \in \{1, \ldots, h\}$, then $\mathcal{V}$ is closed under matrix multiplication.*

PROOF. The product of two arbitrary matrices in $\mathcal{V}$ is readily seen to be expressible as a linear combination of the matrix products A_iA_j and hence it is in $\mathcal{V}$. This proves the lemma. □

LEMMA 2.2. *If A_1 and A_2 are two matrices defined by*

$$A_1 = I_2, \quad A_2 = \begin{bmatrix} 0 & 1 \\ -n & m \end{bmatrix}, \tag{2.7}$$

where m, n, are arbitrary integers, then $\mathcal{L} = \text{span}\{A_1, A_2\}$ is a unital commutative subalgebra of $M_2(\mathbb{R})$. Further, for arbitrary parameters $x_1, x_2 \in \mathbb{R}$, if the matrix $A(x_1, x_2)$ is defined by $A(x_1, x_2) = x_1A_1 + x_2A_2$, the form f defined by

$$f : \mathbb{R}^2 \to \mathbb{R}, \;\; f(x_1, x_2) = \det\left(A(x_1, x_2)\right) = x_1^2 + mx_1x_2 + nx_2^2, \tag{2.8}$$

is a composable binary quadratic form that satisfies, for all $x_i, y_i \in \mathbb{R}, i = 1, 2$, the identity,

$$f(x_1, x_2)f(y_1, y_2) = f(z_1, z_2), \tag{2.9}$$

where

$$z_1 = x_1y_1 - nx_2y_2, \quad z_2 = x_1y_2 + x_2y_1 + mx_2y_2. \tag{2.10}$$

PROOF. Clearly $\mathcal{L}$ is a 2-dimensional vector subspace of $M_2(\mathbb{R})$. It is readily seen that $A_2^2 = -nA_1 + mA_2$ and $A_1A_2 = A_2A_1$. It now follows from Lemma 2.1 that $\mathcal{L}$ is closed under matrix multiplication and is hence a unital commutative subalgebra of $M_2(\mathbb{R})$. Further, as discussed in Sect. 2.1, the form f satisfies the identity (2.9). The values of $z_i, i = 1, 2$, stated in (2.10), are readily obtained by direct computation. The identity (2.9) is the well-known identity on composition of binary quadratic forms. □

2.2. *A subalgebra of $M_3(\mathbb{R})$ and a composable cubic form.*

THEOREM 2.3. *If A_1, A_2, A_3 are three matrices defined by*

$$
\begin{aligned}
A_1 &= I_3, \\
A_2 &= \begin{bmatrix} 0 & 1 & 0 \\ -\lambda_3(\lambda_1-\lambda_2-\lambda_3+\lambda_5) & \lambda_1 & \lambda_3 \\ -\lambda_3(\lambda_2-\lambda_4) & \lambda_2 & \lambda_3 \end{bmatrix}, \\
A_3 &= \begin{bmatrix} 0 & 0 & 1 \\ -\lambda_3(\lambda_2-\lambda_4) & \lambda_2 & \lambda_3 \\ -\lambda_1\lambda_4+\lambda_2^2-\lambda_2\lambda_5+\lambda_3\lambda_4 & \lambda_4 & \lambda_5 \end{bmatrix},
\end{aligned} \tag{2.11}
$$

where $\lambda_i, i = 1, \ldots, 5$, are arbitrary integers, then $\mathcal{L} = \operatorname{span}\{A_1 = I_3, A_2, A_3\}$, is a unital commutative subalgebra of $M_3(\mathbb{R})$. Further, for arbitrary parameters $x_1, x_2, x_3 \in \mathbb{R}$, if the matrix $A(x_1, x_2, x_3)$ is defined by

$$
A(x_1, x_2, x_3) = x_1A_1 + x_2A_2 + x_3A_3, \tag{2.12}
$$

the form f, defined by $f : \mathbb{R}^3 \to \mathbb{R}$, $f(x_1, x_2, x_3) = \det(A(x_1, x_2, x_3))$, is a composable ternary cubic form.

PROOF. Clearly, $\mathcal{L}$ is a 3-dimensional vector subspace of $M_3(\mathbb{R})$. It is readily verified that $A_iA_j = A_jA_i$ for $1 \le i < j \le 3$, and further,

$$
\begin{aligned}
A_2^2 &= \lambda_3(-\lambda_1+\lambda_2+\lambda_3-\lambda_5)I_3 + \lambda_1A_2 + \lambda_3A_3 \in \mathcal{L}, \\
A_2A_3 &= (-\lambda_2\lambda_3+\lambda_3\lambda_4)I_3 + \lambda_2A_2 + \lambda_3A_3 \in \mathcal{L}, \\
A_3^2 &= (\lambda_2^2-\lambda_1\lambda_4+\lambda_3\lambda_4-\lambda_2\lambda_5)I_3 + \lambda_4A_2 + \lambda_5A_3 \in \mathcal{L}.
\end{aligned} \tag{2.13}
$$

It now follows from Lemma 2.1 that $\mathcal{L}$ is closed under multiplication of matrices, and is thus a unital commutative subalgebra of $M_3(\mathbb{R})$. It now follows, as before, that $f(x_1, x_2, x_3) = \det(A(x_1, x_2, x_3))$ is a ternary cubic form admitting composition. ∎

The form $f(x_1, x_2, x_3)$, which may be written explicitly as

$$
\begin{aligned}
f(x_1,\, x_2,\, x_3) &= x_1^3 + (\lambda_1+\lambda_3)x_1^2x_2 + (\lambda_2+\lambda_5)x_1^2x_3 \\
&\quad + \lambda_3(2\lambda_1-2\lambda_2-\lambda_3+\lambda_5)x_1x_2^2 + (\lambda_1\lambda_5+2\lambda_2\lambda_3-3\lambda_3\lambda_4)x_1x_2x_3 \\
&\quad + (\lambda_1\lambda_4-\lambda_2^2+2\lambda_2\lambda_5-2\lambda_3\lambda_4)x_1x_3^2 + \lambda_3^2(\lambda_1-2\lambda_2-\lambda_3+\lambda_4+\lambda_5)x_2^3 \\
&\quad - \lambda_3(2\lambda_1\lambda_4-\lambda_1\lambda_5-2\lambda_2^2-\lambda_2\lambda_3+3\lambda_2\lambda_5-\lambda_3\lambda_4+\lambda_3\lambda_5-\lambda_5^2)x_2^2x_3 \\
&\quad + (\lambda_1^2\lambda_4-\lambda_1\lambda_2^2+\lambda_1\lambda_2\lambda_5-3\lambda_1\lambda_3\lambda_4+\lambda_2^2\lambda_3+\lambda_2\lambda_3\lambda_4 \\
&\quad + 2\lambda_3^2\lambda_4-2\lambda_3\lambda_4\lambda_5)x_2x_3^2 + (\lambda_1\lambda_2\lambda_4-\lambda_2^3+\lambda_2^2\lambda_5-2\lambda_2\lambda_3\lambda_4+\lambda_3\lambda_4^2)x_3^3,
\end{aligned} \tag{2.14}
$$

satisfies the composition identity,

$$
f(x_1,\, x_2,\, x_3)f(y_1,\, y_2,\, y_3) = f(z_1,\, z_2,\, z_3), \tag{2.15}
$$

for all $x_i,\ y_i \in \mathbb{R},\ i = 1,\ 2,\ 3$, and the values of $z_i\ i = 1,\ 2,\ 3$, are given by

$$\begin{aligned} z_1 &= x_1y_1 - \lambda_3(\lambda_1 - \lambda_2 - \lambda_3 + \lambda_5)x_2y_2 - \lambda_3(\lambda_2 - \lambda_4)x_2y_3 \\ &\quad - \lambda_3(\lambda_2 - \lambda_4)x_3y_2 + (-\lambda_1\lambda_4 + \lambda_2^2 - \lambda_2\lambda_5 + \lambda_3\lambda_4)x_3y_3, \\ z_2 &= x_1y_2 + x_2y_1 + \lambda_1x_2y_2 + \lambda_2x_2y_3 + \lambda_2x_3y_2 + \lambda_4x_3y_3, \\ z_3 &= x_1y_3 + \lambda_3x_2y_2 + \lambda_3x_2y_3 + x_3y_1 + \lambda_3x_3y_2 + \lambda_5x_3y_3. \end{aligned} \tag{2.16}$$

We note that for various numerical values of the parameters $\lambda_i,\ i = 1, \ldots, 5$, (for instance, when $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (1, 1, 1, 1, 2)$ or $(1, 1, 1, 2, 1)$), the form $f(x_1,\ x_2,\ x_3)$ is irreducible.

2.3. *Subalgebras of $M_{mn}(\mathbb{R})$ where $m \geq 2$ and $n \geq 2$.* We will now construct a unital commutative algebra of matrices of order mn by combining two unital commutative subalgebras of $M_n(\mathbb{R})$ and $M_m(\mathbb{R})$, respectively, by using the right Kronecker product of matrices denoted by $\otimes$. We note that the Kronecker product of two matrices satisfies the associative and distributive laws, and is bilinear. Further, it satisfies the following mixed-product property [3, p. 408]:

"If $A, C \in M_n(\mathbb{R})$ and $B, D \in M_m(\mathbb{R})$, then

$$(A \otimes B)(C \otimes D) = AC \otimes BD." \tag{2.17}$$

THEOREM 2.4. *If $\{A_1 = I_n, A_2, \ldots, A_h\}$ and $\{B_1 = I_m, B_2, \ldots, B_k\}$ are linearly independent sets of matrices in $M_n(\mathbb{Z})$ and $M_m(\mathbb{Z})$, respectively, such that*

$$\begin{aligned} &\mathcal{L}_n = \operatorname{span}\{A_1 = I_n, A_2, \ldots, A_h\}, \\ \text{and} \qquad &\mathcal{L}_m = \operatorname{span}\{B_1 = I_m, B_2, \ldots, B_k\}, \end{aligned} \tag{2.18}$$

are unital commutative subalgebras of $M_n(\mathbb{R})$ and $M_m(\mathbb{R})$, respectively, then

$$\mathcal{L} = \operatorname{span}\{B_i \otimes A_j,\ i = 1, \ldots, k,\ j = 1, \ldots, h\} \tag{2.19}$$

is a unital commutative subalgebra of $M_{mn}(\mathbb{R})$.

PROOF. We first construct a set $\mathcal{S}$ of kh square matrices of order mn given by $\{B_i \otimes A_j,\ i = 1, \ldots, k,\ j = 1, \ldots, h\}$. We note that $B_1 \otimes A_1 = I_m \otimes I_n = I_{mn}$, and hence the neutral element $I_{mn} \in \mathcal{L}$. Further, since $\{A_1, \ldots, A_h\}$ and $\{B_1, \ldots, B_k\}$ are linearly independent sets of matrices, it is readily seen that the set $\mathcal{S}$ consists of kh linearly independent square matrices. It follows that the set $\mathcal{L}$, defined by (2.19) as the span of all the matrices in the set $\mathcal{S}$, is a subspace of the vector space $M_{mn}(\mathbb{R})$ and $\dim \mathcal{L} = kh$.

Since $\mathcal{L}_m$ and $\mathcal{L}_n$ are commutative subalgebras of of $M_m(\mathbb{R})$ and $M_n(\mathbb{R})$, respectively, we note that for any $i_1, i_2 \in \{1, \ldots, k\}$ and any $j_1, j_2 \in \{1, \ldots, h\}$, we have $A_{j_1}A_{j_2} = A_{j_2}A_{j_1} \in \mathcal{L}_n$ and $B_{i_1}B_{i_2} = B_{i_2}B_{i_1} \in \mathcal{L}_m$. We may thus write $A_{j_1}A_{j_2} = \sum_{j=1}^{h} s_jA_j,\ s_j \in \mathbb{R}$, and $B_{i_1}B_{i_2} = \sum_{i=1}^{k} r_iB_i,\ r_i \in$

$\mathbb{R}$. It now follows from (2.17) that

$$(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = (B_{i_1}B_{i_2}) \otimes (A_{j_1}A_{j_2}) = (\sum_{i=1}^{k} r_i B_i) \otimes (\sum_{j=1}^{h} s_j A_j).$$

In view of the bilinearity of the Kronecker product, we may now write,

$$(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = \sum_{i=1}^{k}\sum_{j=1}^{h} r_i s_j (B_i \otimes A_j) \in \mathcal{L}. \tag{2.20}$$

It now follows from Lemma 2.1 that the subspace $\mathcal{L}$ is closed under matrix multiplication, and hence $\mathcal{L}$ is a subalgebra of $M_{mn}(\mathbb{R})$. Further, since $A_{j_1}A_{j_2} = A_{j_2}A_{j_1}$ and $B_{i_1}B_{i_2} = B_{i_2}B_{i_1}$, it immediately follows from (2.17) that $(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = (B_{i_2} \otimes A_{j_2})(B_{i_1} \otimes A_{j_1})$. This proves that $\mathcal{L}$ is a unital commutative subalgebra of $M_{mn}(\mathbb{R})$. □

COROLLARY 2.5. *If $\{A_1 = I_n, A_2, \ldots, A_h\}$ is a linearly independent set of matrices in $M_n(\mathbb{Z})$ such that $\mathcal{L}_n = \text{span}\{A_1, A_2, \ldots, A_h\}$ is a unital commutative subalgebra of $M_n(\mathbb{R})$, and the matrix $C(x_1, \ldots, x_{2h})$ is defined by*

$$C(x_i) = \begin{bmatrix} A(x_1, \ldots, x_h) & A(x_{h+1}, \ldots, x_{2h}) \\ -qA(x_{h+1}, \ldots, x_{2h}) & A(x_1, \ldots, x_h) + pA(x_{h+1}, \ldots, x_{2h}) \end{bmatrix}, \tag{2.21}$$

where $A(x_1, \ldots, x_h) = \sum_{j=1}^{h} x_j A_j$ and p, q are arbitrary integers, the form f defined by

$$f : \mathbb{R}^{2h} \to \mathbb{R}, \quad f(x_1, \ldots, x_{2h}) = \det\left(C(x_1, \ldots, x_{2h})\right), \tag{2.22}$$

is a composable form of degree $2n$ in the variables $x_1, x_2, \ldots, x_{2h}$.

PROOF. In view of Lemma 2.2, if p, q, are arbitrary integers, $\text{span}\{B_1 = I_2, B_2 = \begin{bmatrix} 0 & 1 \\ -q & p \end{bmatrix}\}$, is a unital commutative subalgebra of $M_2(\mathbb{R})$. It now follows from Theorem 2.4 that $\mathcal{L} = \text{span}\{B_i \otimes A_j,\ i = 1, 2,\ j = 1, \ldots, h\}$ is a unital commutative subalgebra of $M_{2n}(\mathbb{R})$. An arbitrary matrix $C = C(x_1, x_2, \ldots, x_{2h}) \in \mathcal{L}$ may be written as

$$\begin{aligned} C(x_1, x_2, \ldots, x_{2h}) &= \sum_{j=1}^{h} x_j B_1 \otimes A_j + \sum_{j=1}^{h} x_{h+j} B_2 \otimes A_j \\ &= B_1 \otimes \sum_{j=1}^{h} x_j A_j + B_2 \otimes \sum_{j=1}^{h} x_{h+j} A_j \\ &= B_1 \otimes A(x_1, \ldots, x_h) + B_2 \otimes A(x_{h+1}, \ldots, x_{2h}) \end{aligned} \tag{2.23}$$

which, on using the definition of the Kronecker product, may be written as stated in (2.21). Since $\mathcal{L}$ is closed under multiplication of matrices, it follows, as before, that the form f defined by (2.22) is a composable form of degree $2n$ in the variables $x_1, x_2, \ldots, x_{2h}$. □

2.4. *Composable forms and diophantine equations.* Let $\{A_1 = I_n, A_2, \ldots, A_n\}$ be a linearly independent set of $n \times n$ matrices with integer entries such that

$$\mathcal{L} = \{A(x_1, x_2, \ldots, x_n) = x_1A_1 + x_2A_2 + \cdots + x_nA_n : x_1, \ldots, x_n \in \mathbb{R}\} \tag{2.24}$$

is a unital commutative algebra, that is, a subalgebra of $M_n(\mathbb{R})$, so that the form

$$f(x_1, x_2, \ldots, x_n) = \det(A(x_1, x_2, \ldots, x_n)),$$

is a composable form of degree n in n variables $x_i, i = 1, \ldots, n$.

We also assume that the set of the first rows of the matrices $A_1 = I_n, A_2, \ldots, A_n$ forms the canonical basis for $\mathbb{R}^n$ (that is, the first rows are given by $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$) so that the first row of the matrix $A(x_1, x_2, \ldots, x_n)$ may be written as $(x_1, x_2, \ldots, x_n)$.

Let S denote the set of all integer solutions of the diophantine equation,

$$f(x_1, x_2, \ldots, x_n) = 1, \tag{2.25}$$

that is,

$$S = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : f(x_1, x_2, \ldots, x_n) = 1\}. \tag{2.26}$$

We will show that S is an abelian group under a suitably defined operation of multiplication.

We first note that $f(1, 0, \ldots, 0) = \det(A(1, 0, \ldots, 0)) = \det I_n = 1$. Thus $(1, 0, \ldots, 0) \in S$, and hence the set S is nonempty. Let $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ be two arbitrary elements of S so that $f(x_1, x_2, \ldots, x_n) = 1$ and $f(y_1, y_2, \ldots, y_n) = 1$. As we have already noted, the set $\mathcal{L}(\mathbb{Z})$ is closed under multiplication and accordingly, we define the multiplication operation on elements of S as follows:

$$(x_1, , x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (z_1, z_2, \ldots, z_n), \tag{2.27}$$

where

$$A(x_1, x_2, \ldots, x_n)A(y_1, y_2, \ldots, y_n) = A(z_1, z_2, \ldots, z_n). \tag{2.28}$$

In view of our assumption that the set of the first rows of the matrices $A_1 = I_n, A_2, \ldots, A_n$ forms the canonical basis for $\mathbb{R}^n$, it is sufficient to compute the first row of the matrix product $A(x_1, \ldots, x_n)A(y_1, \ldots, y_n)$ to determine the values of $z_i, i = 1, \ldots, n$.

Since f is a composable form,

$$f(z_1, z_2, \ldots, z_n) = f(x_1, x_2, \ldots, x_n)f(y_1, y_2, \ldots, y_n) = 1,$$

and hence $(z_1, z_2, \ldots, z_n) \in S$. Thus, the set S is closed under the binary operation defined by (2.27). Further, the binary operation defined on the set S is associative (since matrix multiplication is associative) and commutative since matrix multiplication is commutative on the ambient space $\mathcal{L}$). It is also readily seen that $(1, 0, \ldots, 0) \in S$ is a neutral element for our binary operation since $A(1, 0, \ldots, 0) = I_n$.

Finally, we will show that any arbitrary element $(x_1, x_2, \ldots, x_n) \in S$ has its inverse in S. Since $\det(A(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n) = 1$, the matrix $A(x_1, x_2, \ldots, x_n)$ is invertible and in fact, $(A(x_1, x_2, \ldots, x_n))^{-1} \in M_n(\mathbb{Z})$. Further, it follows from the well-known Cayley-Hamilton theorem [3, Theorem 4, p. 252] that there exists a polynomial p such that $(A(x_1, x_2, \ldots, x_n))^{-1} = p(A(x_1, x_2, \ldots, x_n))$ and hence $(A(x_1, x_2, \ldots, x_n))^{-1} \in \mathcal{L}$. Moreover, all the entries of $(A(x_1, x_2, \ldots, x_n))^{-1}$ are integers, and so are the entries of the first row, say $y_1, y_2, \ldots, y_n$. Hence $(A(x_1, x_2, \ldots, x_n))^{-1} = A(y_1, y_2, \ldots, y_n) \in \mathcal{L}(\mathbb{Z})$ where $y_i \in \mathbb{Z}, i = 1, \ldots, n$. It follows that

$$A(x_1, x_2, \ldots, x_n)A(y_1, y_2, \ldots, y_n) = I_n = A(1, 0, \ldots, 0),$$

and hence $f(y_1, y_2, \ldots, y_n) = \det(A(y_1, y_2, \ldots, y_n) = 1$, and further, we have, $(x_1, x_2, \ldots, x_n)\cdot(y_1, y_2, \ldots, y_n) = (1, 0, \ldots, 0)$. This shows that $(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n)^{-1} \in S$.

We have thus proved that the set S of integer solutions of the diophantine equation (2.25) is an abelian group with the binary operation on S defined by (2.27).

3. Higher degree forms admitting composition and related diophantine equations

We will now construct composable forms of degree n in n variables when $n = 4$, 6 and 8 and solve certain related diophantine equations of type (2.25).

3.1. *Quartic forms.* In Sect. 3.1.1 we will obtain a quaternary quartic form admitting composition and in Sect. 3.1.2 we will consider a related quartic diophantine equation.

3.1.1. *A composable quartic form.*

Theorem 3.1. *If $C_i, i = 1, \ldots, 4$, are four 4×4 matrices defined by*

$$C_1 = I_4, \qquad C_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -n & m & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -n & m \end{bmatrix},$$
$$C_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -q & 0 & p & 0 \\ 0 & -q & 0 & p \end{bmatrix}, \qquad C_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -n & m \\ 0 & -q & 0 & p \\ qn & -qm & -pn & pm \end{bmatrix}, \tag{3.1}$$

where m, n, p and q are arbitrary integers, then $\mathcal{L} = \operatorname{span}\{C_1, C_2, C_3, C_4\}$ is a unital commutative subalgebra of $M_4(\mathbb{R})$. Further, for arbitrary parameters $x_i \in \mathbb{R}, i = 1, \ldots, 4$, if the matrix C is defined by

$$C(x_1, x_2, x_3, x_4) = x_1C_1 + x_2C_2 + x_3C_3 + x_4C_4, \tag{3.2}$$

the form f, defined by

$$f : \mathbb{R}^4 \to \mathbb{R},\ f(x_1, x_2, x_3, x_4) = \det(C(x_1, x_2, x_3, x_4)), \tag{3.3}$$

is a composable quaternary quartic form that satisfies the identity

$$f(x_1, x_2, x_3, x_4) f(y_1, y_2, y_3, y_4) = f(z_1, z_2, z_3, z_4), \tag{3.4}$$

where the values of $z_i, i = 1, \ldots, 4$, are given in terms of arbitrary parameters $x_i, y_i, i = 1, \ldots, 4$, by

$$\begin{aligned}
z_1 &= x_1y_1 - nx_2y_2 - qx_3y_3 + qnx_4y_4,\\
z_2 &= x_1y_2 + x_2y_1 + mx_2y_2 - qx_3y_4 - qx_4y_3 - mqx_4y_4,\\
z_3 &= x_1y_3 - nx_2y_4 + x_3y_1 + px_3y_3 - nx_4y_2 - npx_4y_4,\\
z_4 &= x_1y_4 + x_2(y_3 + my_4) + x_3(y_2 + py_4) + x_4(y_1 + my_2 + py_3 + mpy_4).
\end{aligned}$$

Proof. In view of Lemma 2.2, if the matrices A_1, A_2 are defined by (2.7) and matrices B_1, B_2 are defined by $B_1 = I_2, B_2 = \begin{bmatrix} 0 & 1 \\ -q & p \end{bmatrix}$, where p, q are arbitrary integers, both $\text{span}\{A_1, A_2\}$ and $\text{span}\{B_1, B_2\}$ are unital commutative subalgebras of $M_2(\mathbb{R})$. We note that

$$C_1 = B_1 \otimes A_1, \quad C_2 = B_1 \otimes A_2, \quad C_3 = B_2 \otimes A_1, \quad C_4 = B_2 \otimes A_2,$$

and it now follows from Theorem 2.4 that $\mathcal{L} = \text{span}\{C_1, C_2, C_3, C_4\}$ is a unital commutative subalgebra of $M_4(\mathbb{R})$, and hence the form f defined by (3.3) is a composable form which satisfies the identity (3.4). We note that the form $f(x_1, x_2, x_3, x_4)$ is irreducible for various values of the parameters m, n, p and q (for instance, when $(m, n, p, q) = (1, 2, 1, 1)$ or $(1, 3, 1, 1)$). The values of z_i in the identity (3.4) are readily obtained by direct computation. □

3.1.2. *A related quartic diophantine equation.* We will now consider the diophantine equation,

$$f(x_1, x_2, x_3, x_4) = 1, \tag{3.5}$$

where $f(x_1, x_2, x_3, x_4)$ is the quartic form defined by (3.3). We note that the conditions mentioned in Sect. 2.4 are satisfied. Thus, the integer solutions of Eq. (3.5) form a group and we can combine two integer solutions of Eq. (3.5) using the binary operation (2.27) and obtain a new solution of Eq. (3.5).

We will now consider a special case of Eq. (3.5) when $m = 5$, $n = -23$, $p = 2$, $q = -7$, that is, the equation,

$$\begin{aligned}(3.6)\quad & x_1^4 + 10x_1^3x_2 + 4x_1^3x_3 + 10x_1^3x_4 - 21x_1^2x_2^2 + 30x_1^2x_2x_3 - 42x_1^2x_2x_4 \\ & - 10x_1^2x_3^2 - 50x_1^2x_3x_4 - 589x_1^2x_4^2 - 230x_1x_2^3 - 42x_1x_2^2x_3 - 690x_1x_2^2x_4 \\ & - 50x_1x_2x_3^2 + 1388x_1x_2x_3x_4 + 1150x_1x_2x_4^2 - 28x_1x_3^3 - 210x_1x_3^2x_4 \\ & + 294x_1x_3x_4^2 + 1610x_1x_4^3 + 529x_2^4 - 230x_2^3x_3 + 2116x_2^3x_4 - 589x_2^2x_3^2 \\ & + 1150x_2^2x_3x_4 - 5290x_2^2x_4^2 - 70x_2x_3^3 + 294x_2x_3^2x_4 + 4830x_2x_3x_4^2 \\ & - 14812x_2x_4^3 + 49x_3^4 + 490x_3^3x_4 - 1029x_3^2x_4^2 - 11270x_3x_4^3 + 25921x_4^4 = 1.\end{aligned}$$

It is readily verified that Eq. (3.6) is irreducible, and (6, 2, 3, 1) is a numerical solution of Eq. (3.6). If $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is an arbitrary integer solution of Eq. (3.6) such that $\alpha_i > 0$ for each i, on combining (6, 2, 3, 1) with the solution $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ using the binary operation (2.27), we obtain a new solution of Eq. (3.6), and we may now combine (6, 2, 3, 1) with the new solution just obtained to obtain yet another solution, and in fact, by repeated application of this process, we can obtain an infinite sequence of solutions in positive integers of Eq. (3.6). If we denote the nth solution of the sequence by $(\alpha_1^{(n)}, \alpha_2^{(n)}, \alpha_3^{(n)}, \alpha_4^{(n)})$, the $(n+1)$th solution is given by the following linear recursive relations:

$$\begin{aligned}\alpha_1^{(n+1)} &= 6\alpha_1^{(n)} + 46\alpha_2^{(n)} + 21\alpha_3^{(n)} + 161\alpha_4^{(n)}, \\ \alpha_2^{(n+1)} &= 2\alpha_1^{(n)} + 16\alpha_2^{(n)} + 7\alpha_3^{(n)} + 56\alpha_4^{(n)}, \\ \alpha_3^{(n+1)} &= 3\alpha_1^{(n)} + 23\alpha_2^{(n)} + 12\alpha_3^{(n)} + 92\alpha_4^{(n)}, \\ \alpha_4^{(n+1)} &= \alpha_1^{(n)} + 8\alpha_2^{(n)} + 4\alpha_3^{(n)} + 32\alpha_4^{(n)}.\end{aligned}$$

If we take (6, 2, 3, 1) as the initial solution of the sequence, the next three solutions of Eq. (3.6) obtained by the above process are (352, 121, 192, 66), (22336, 7680, 12215, 4200), and (1420011, 488257, 776628, 267036).

3.2. *Sextic forms.* In Sect. 3.2.1 we obtain two senary sextic forms admitting composition and in Sect. 3.2.2 we consider related diophantine equations.

3.2.1. *Composable sextic forms.*

THEOREM 3.2. *If $A(x_1, x_2, x_3) = x_1A_1 + x_2A_2 + x_3A_3$ where A_1, A_2, A_3 are the three matrices defined by* (2.11)*, and the matrix $C(x_1, x_2, \ldots, x_6)$ is defined by*

$$(3.7)\quad C(x_1, \ldots, x_6) = \begin{bmatrix} A(x_1, x_2, x_3) & A(x_4, x_5, x_6) \\ -qA(x_4, x_5, x_6) & A(x_1, x_2, x_3) + pA(x_4, x_5, x_6) \end{bmatrix},$$

where p and q are arbitrary integers, the form f, defined by

$$(3.8)\qquad f : \mathbb{R}^6 \to \mathbb{R},\ f(x_1, x_2, \ldots, x_6) = \det(C(x_1, x_2, \ldots, x_6)),$$

is a composable senary sextic form.

PROOF. In view of Theorem 2.3, when the matrices A_1, A_2, A_3 are defined by (2.11), $\text{span}\{A_1, A_2, A_3\}$ is a unital commutative subalgebra of $M_3(\mathbb{R})$, and it immediately follows from Corollary 2.5 that the form f defined by (3.8) is a senary sextic composable form. It has been verified, using the software MAPLE, that the sextic form $f(x_1, \ldots, x_6)$ is irreducible for various numerical values of the parameters λ_i, p and q. We do not give the sextic form $f(x_1, \ldots, x_6)$ explicitly as it is too cumbersome to write. According to MAPLE, there are 11926 terms in the expansion of $f(x_1, \ldots, x_6)$. □

As in the case of Eq. (3.5), it is readily established that the integer solutions of the sextic equation $f(x_1, \ldots, x_6) = 1$ form an abelian group.

We note that if $A_i, i = 1, 2, 3$, are any three matrices $\in M_3(\mathbb{R})$ such that $\text{span}\{A_1, A_2, A_3\}$ is a unital commutative subalgebra of $M_3(\mathbb{R})$, Theorem 3.2 is still valid since exactly the same proof remains applicable. In the following lemma we obtain three such matrices and we use them in the next theorem to obtain a second example of a senary sextic form admitting composition.

LEMMA 3.3. *If A_1, A_2, A_3 are three matrices defined by*

$$A_1 = I_3, \quad A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \tag{3.9}$$

then $\mathcal{L} = \text{span}\{A_1 = I_3, A_2, A_3\}$ is a unital commutative subalgebra of $M_3(\mathbb{R})$.

PROOF. Clearly, $\mathcal{L}$ is a 3-dimensional vector subspace of $M_3(\mathbb{R})$. Since the matrices A_1, A_2, A_3 satisfy the relations $A_2A_3 = A_3A_2 = I_3$, $A_2^2 = A_3$, $A_3^2 = A_2$, it follows from Lemma 2.1 that $\mathcal{L}$ is closed under multiplication of matrices, and it is thus a unital commutative subalgebra of $M_3(\mathbb{R})$. □

THEOREM 3.4. *If the matrix $C(x_1, x_2, \ldots, x_6)$ is defined by*

$$C(x_1, \ldots, x_6) = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_1 & x_2 & x_6 & x_4 & x_5 \\ x_2 & x_3 & x_1 & x_5 & x_6 & x_4 \\ qx_4 & qx_5 & qx_6 & x_1 & x_2 & x_3 \\ qx_6 & qx_4 & qx_5 & x_3 & x_1 & x_2 \\ qx_5 & qx_6 & qx_4 & x_2 & x_3 & x_1 \end{bmatrix}, \tag{3.10}$$

where q is an arbitrary integer, the form f, defined by

$$f : \mathbb{R}^6 \to \mathbb{R}, \; f(x_1, x_2, \ldots, x_6) = \det(C(x_1, x_2, \ldots, x_6)), \tag{3.11}$$

is a composable senary sextic form which satisfies the identity

$$f(x_1, x_2, \ldots, x_6)f(y_1, y_2, \ldots, y_6) = f(z_1, z_2, \ldots, z_6), \tag{3.12}$$

where the values of z_i, $i = 1, \ldots, 6$, *are given by*

$$
\begin{aligned}
z_1 &= x_1y_1 + x_2y_3 + x_3y_2 + qx_4y_4 + qx_5y_6 + qx_6y_5,\\
z_2 &= x_1y_2 + x_2y_1 + x_3y_3 + qx_4y_5 + qx_5y_4 + qx_6y_6,\\
z_3 &= x_1y_3 + x_2y_2 + x_3y_1 + qx_4y_6 + qx_5y_5 + qx_6y_4,\\
z_4 &= x_1y_4 + x_2y_6 + x_3y_5 + x_4y_1 + x_5y_3 + x_6y_2,\\
z_5 &= x_1y_5 + x_2y_4 + x_3y_6 + x_4y_2 + x_5y_1 + x_6y_3,\\
z_6 &= x_1y_6 + x_2y_5 + x_3y_4 + x_4y_3 + x_5y_2 + x_6y_1.
\end{aligned} \tag{3.13}
$$

PROOF. In view of Lemma 3.3, we may apply Theorem 3.2 with the matrices A_1, A_2, A_3 defined by (3.9). In the matrix $C(x_1, \ldots, x_6)$ defined by (3.7), we take $p = 0$ and replace q by $-q$, and thus obtain the matrix $C(x_1, \ldots, x_6)$ defined by (3.10). It now immediately follows that the form f defined by (3.11) is a composable senary sextic form that satisfies the identity (3.12) in which the values of $z_i, i = 1, \ldots, 6$, obtained by direct computation, are given by (3.13). □

We note that the senary form defined by (3.11) has two irreducible factors given by

$$f(x_1, x_2, \ldots, x_6) = f_1(x_1, x_2, \ldots, x_6) f_2(x_1, x_2, \ldots, x_6), \tag{3.14}$$

where

$$f_1(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 + x_2 + x_3)^2 - q(x_4 + x_5 + x_6)^2, \tag{3.15}$$

$$
\begin{aligned}
f_2(x_1, x_2, x_3, x_4, x_5, x_6) &= x_1^4 - (2x_2 + 2x_3)x_1^3 + (3x_2^2 + 3x_3^2 - 2qx_4^2\\
&\quad + 2qx_4x_5 + 2qx_4x_6 + qx_5^2 - 4qx_5x_6 + qx_6^2)x_1^2 + (-2x_2^3 + 2qx_2x_4^2 - 8qx_2x_4x_5\\
&\quad + 4qx_2x_4x_6 + 2qx_2x_5^2 + 4qx_2x_5x_6 - 4qx_2x_6^2 - 2x_3^3 + 2qx_3x_4^2 + 4qx_3x_4x_5\\
&\quad - 8qx_3x_4x_6 - 4qx_3x_5^2 + 4qx_3x_5x_6 + 2qx_3x_6^2)x_1 + x_2^4 - 2x_2^3x_3 + 3x_2^2x_3^2 + qx_2^2x_4^2\\
&\quad + 2qx_2^2x_4x_5 - 4qx_2^2x_4x_6 - 2qx_2^2x_5^2 + 2qx_2^2x_5x_6 + qx_2^2x_6^2 - 2x_2x_3^3 - 4qx_2x_3x_4^2\\
&\quad + 4qx_2x_3x_4x_5 + 4qx_2x_3x_4x_6 + 2qx_2x_3x_5^2 - 8qx_2x_3x_5x_6 + 2qx_2x_3x_6^2 + x_3^4 + qx_3^2x_4^2\\
&\quad - 4qx_3^2x_4x_5 + 2qx_3^2x_4x_6 + qx_3^2x_5^2 + 2qx_3^2x_5x_6 - 2qx_3^2x_6^2 + q^2x_4^4 - 2q^2x_4^3x_5\\
&\quad - 2q^2x_4^3x_6 + 3q^2x_4^2x_5^2 + 3q^2x_4^2x_6^2 - 2q^2x_4x_5^3 - 2q^2x_4x_6^3 + q^2x_5^4 - 2q^2x_5^3x_6\\
&\quad + 3q^2x_5^2x_6^2 - 2q^2x_5x_6^3 + q^2x_6^4,
\end{aligned} \tag{3.16}
$$

and, in accordance with a theorem of Dickson [1, p. 219, Theorem 3], we now get the simultaneous composition identities,

$$
\begin{aligned}
f_1(x_1, x_2, \ldots, x_6) f_1(y_1, y_2, \ldots, y_6) &= f_1(z_1, z_2, \ldots, z_6),\\
f_2(x_1, x_2, \ldots, x_6) f_2(y_1, y_2, \ldots, y_6) &= f_2(z_1, z_2, \ldots, z_6),
\end{aligned} \tag{3.17}
$$

where x_i, y_i, $i = 1, 2, \ldots, 6$, are arbitrary while the values of z_i, $i = 1, 2, \ldots, 6$, are given by (3.13).

3.2.2. *A related pair of simultaneous diophantine equations.* We will now consider a pair of simultaneous diophantine equations related to the forms $f_1(x_1, \ldots, x_6)$ and $f_2(x_1, \ldots, x_6)$ defined by (3.15) and (3.16), respectively, in the special case when $q = 3$. We note that the form $f_1(x_1, \ldots, x_6)$ has just two independent variables and accordingly, we make a suitable linear transformation after which we can rewrite the formulae (3.17) for simultaneous composition of forms as follows:

$$f_1(u_i)f_1(v_i) = f_1(w_i), \quad f_2(u_i)f_2(v_i) = f_2(w_i), \tag{3.18}$$

where $f_1(u_i) = u_1^2 - 3u_2^2$, and

$$\begin{aligned} f_2(u_i) = {} & u_1^4 - 6u_1^3u_3 - 6u_1^3u_6 + 3u_1^2u_2^2 - 18u_1^2u_2u_5 + 15u_1^2u_3^2 + 24u_1^2u_3u_6 \\ & - 9u_1^2u_4^2 + 18u_1^2u_4u_5 + 18u_1^2u_5^2 + 15u_1^2u_6^2 - 18u_1u_2^2u_6 - 36u_1u_2u_3u_4 \\ & + 36u_1u_2u_3u_5 + 36u_1u_2u_4u_6 + 72u_1u_2u_5u_6 - 18u_1u_3^3 - 36u_1u_3^2u_6 + 54u_1u_3u_4^2 \\ & - 54u_1u_3u_5^2 - 36u_1u_3u_6^2 - 108u_1u_4u_5u_6 - 54u_1u_5^2u_6 - 18u_1u_6^3 + 9u_2^4 - 54u_2^3u_4 - 54u_2^3u_5 \\ & - 9u_2^2u_3^2 + 18u_2^2u_3u_6 + 135u_2^2u_4^2 + 216u_2^2u_4u_5 + 135u_2^2u_5^2 + 18u_2^2u_6^2 + 54u_2u_3^2u_4 \\ & - 108u_2u_3u_5u_6 - 162u_2u_4^3 - 324u_2u_4^2u_5 - 324u_2u_4u_5^2 - 54u_2u_4u_6^2 - 162u_2u_5^3 \\ & - 54u_2u_5u_6^2 + 9u_3^4 + 18u_3^3u_6 - 54u_3^2u_4^2 - 54u_3^2u_4u_5 + 27u_3^2u_5^2 + 27u_3^2u_6^2 \\ & - 54u_3u_4^2u_6 + 108u_3u_4u_5u_6 + 108u_3u_5^2u_6 + 18u_3u_6^3 + 81u_4^4 + 162u_4^3u_5 + 243u_4^2u_5^2 \\ & + 27u_4^2u_6^2 + 162u_4u_5^3 + 108u_4u_5u_6^2 + 81u_5^4 + 27u_5^2u_6^2 + 9u_6^4, \end{aligned} \tag{3.19}$$

and the values of w_i, $i = 1, 2, \ldots, 6$, in the simultaneous composition formulae (3.18) are given by

$$\begin{aligned} w_1 &= u_1v_1 + 3u_2v_2, \\ w_2 &= u_1v_2 + u_2v_1, \\ w_3 &= u_1v_3 + 3u_2v_4 + u_3v_1 - 2u_3v_3 - u_3v_6 + 3u_4v_2 \\ &\quad - 6u_4v_4 - 3u_4v_5 - 3u_5v_4 + 3u_5v_5 - u_6v_3 + u_6v_6, \\ w_4 &= u_1v_4 + u_2v_6 - u_3v_4 + u_3v_5 + u_4v_1 - u_4v_3 - 2u_4v_6 + u_5v_3 \\ &\quad - u_5v_6 + u_6v_2 - 2u_6v_4 - u_6v_5, \\ w_5 &= u_1v_5 + u_2v_3 + u_3v_2 - u_3v_4 - 2u_3v_5 - u_4v_3 \\ &\quad + u_4v_6 + u_5v_1 - 2u_5v_3 - u_5v_6 + u_6v_4 - u_6v_5, \\ w_6 &= u_1v_6 + 3u_2v_2 - 3u_2v_4 - 3u_2v_5 + u_3v_3 - u_3v_6 - 3u_4v_2 + 3u_4v_4 \\ &\quad + 6u_4v_5 - 3u_5v_2 + 6u_5v_4 + 3u_5v_5 + u_6v_1 - u_6v_3 - 2u_6v_6. \end{aligned} \tag{3.20}$$

We will now consider the simultaneous diophantine equations,

$$f_1(u_i) = 1, \quad f_2(u_i) = 1. \tag{3.21}$$

It is readily verified that $f_2(u_i) = 1$ is an irreducible equation, and a numerical solution of the simultaneous equations (3.21) is given by

$$(u_1, u_2, u_3, u_4, u_5, u_6) = (2, 1, 3, -1, 3, -4). \tag{3.22}$$

By applying the composition identities (3.18), we can combine any integer solution $u_i = \alpha_i,\ i = 1, 2, \ldots, 6$, of the simultaneous diophantine equations (3.21) with the known solution (3.22) to obtain a new solution, and as in the case of Eq. (3.6), by repeatedly combining each successive solution with the known solution (3.22), we get an infinite sequence of solutions in integers of the simultaneous equations (3.21). If we denote the nth solution of the sequence by $(\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_6^{(n)})$, the $(n+1)$th solution is given by the following linear recursive relations:

$$
\begin{aligned}
\alpha_1^{(n+1)} &= 2\alpha_1^{(n)} + 3\alpha_2^{(n)},\\
\alpha_2^{(n+1)} &= \alpha_1^{(n)} + 2\alpha_2^{(n)},\\
\alpha_3^{(n+1)} &= 3\alpha_1^{(n)} - 3\alpha_2^{(n)} + 12\alpha_5^{(n)} - 7\alpha_6^{(n)},\\
\alpha_4^{(n+1)} &= -\alpha_1^{(n)} - 4\alpha_2^{(n)} + 4\alpha_3^{(n)} + 7\alpha_4^{(n)} + 7\alpha_5^{(n)},\\
\alpha_5^{(n+1)} &= 3\alpha_1^{(n)} + 3\alpha_2^{(n)} - 4\alpha_3^{(n)} - 7\alpha_4^{(n)} - 4\alpha_6^{(n)},\\
\alpha_6^{(n+1)} &= -4\alpha_1^{(n)} - 3\alpha_2^{(n)} + 7\alpha_3^{(n)} + 12\alpha_4^{(n)} + 7\alpha_6^{(n)}.
\end{aligned}
\tag{3.23}
$$

If we take $(2, 1, 3, -1,\ 3, -4)$ as the initial solution of the sequence, the next three solutions of the infinite sequence of integer solutions of Eqs. (3.21) are given by (7, 4, 67, 20, 20, −30), (26, 15, 459, 525, −255, 459), and (97, 56, −6240, 3640, −7224, 12577).

3.3. *Octic forms.* We will now construct an octonary octic form admitting composition and consider a related octic diophantine equation.

3.3.1. *A composable octic form.*

THEOREM 3.5. *If the matrix $P(x_1, x_2, \ldots, x_8)$ is defined by*

$$
P(x_1, x_2, \ldots, x_8) = \begin{bmatrix} C(x_1, \ldots, x_4) & C(x_5, \ldots, x_8) \\ -sC(x_5, \ldots, x_8) & C(x_1, \ldots, x_4) + rA(x_5, \ldots, x_8) \end{bmatrix}.
$$

where $C(x_1, x_2, x_3, x_4)$ is defined by (3.2) *and r, s are arbitrary integers, the form f, defined by*

$$
f : \mathbb{R}^8 \to \mathbb{R},\ f(x_1, x_2, \ldots, x_8) = \det(P(x_1, x_2, \ldots, x_8)),
\tag{3.24}
$$

is a composable octonary octic form.

PROOF. When the matrices $C_i, i = 1, \ldots, 4$, are defined by (3.1), we have already proved in Theorem 3.1 that $\mathcal{L} = \operatorname{span}\{C_1, C_2, C_3, C_4\}$ is a unital commutative subalgebra of $M_4(\mathbb{R})$. We now apply Corollary 2.5 where we replace p, q by r, s, respectively, and immediately obtain the composable form f defined by (3.24). It has been verified using MAPLE that the octic form $f(x_1, x_2, \ldots, x_8)$ is irreducible for various numerical values of the parameters m, n, p, q, r, s. ∎

3.3.2. *A related octic diophantine equation.* We will now consider the diophantine equation

$$f(x_1, x_2, \ldots, x_8) = 1, \tag{3.25}$$

where $f(x_1, x_2, \ldots, x_8)$ is the octic form defined by (3.24). As in Sect. 3.1.2, the integer solutions of the octic diophantine equation (3.25) form an abelian group, and we can combine two integer solutions of Eq. (3.25) using the binary operation (2.27) for the group of integer solutions of Eq. (3.25).

We will now consider Eq. (3.25) when $(m, n, p, q, r, s) = (0, -5, 0, -3, 0, -14)$. This is an irreducible equation and it is readily verified that a numerical solution of this equation is given by

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (4, 2, 2, 1, 14, 7, 8, 4). \tag{3.26}$$

If $(\alpha_1, \alpha_2, \ldots, \alpha_8)$ is an arbitrary integer solution of our numerical octic equation such that $\alpha_i > 0$ for each i, we may use the binary operation (2.27), and the solutions (3.26) and $(\alpha_1, \alpha_2, \ldots, \alpha_8)$, to obtain a new solution, and as before, by repeatedly combining each successive solution with the known solution (3.26), we get an infinite sequence of solutions in positive integers of our octic equation. If we denote the nth solution of the sequence by $(\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_8^{(n)})$, the $(n+1)$th solution may be written in terms of the nth solution as follows:

$$\begin{aligned}
&\big(4\alpha_1^{(n)} + 10\alpha_2^{(n)} + 6\alpha_3^{(n)} + 15\alpha_4^{(n)} + 196\alpha_5^{(n)} + 490\alpha_6^{(n)} + 336\alpha_7^{(n)} + 840\alpha_8^{(n)},\\
&2\alpha_1^{(n)} + 4\alpha_2^{(n)} + 3\alpha_3^{(n)} + 6\alpha_4^{(n)} + 98\alpha_5^{(n)} + 196\alpha_6^{(n)} + 168\alpha_7^{(n)} + 336\alpha_8^{(n)},\\
&2\alpha_1^{(n)} + 5\alpha_2^{(n)} + 4\alpha_3^{(n)} + 10\alpha_4^{(n)} + 112\alpha_5^{(n)} + 280\alpha_6^{(n)} + 196\alpha_7^{(n)} + 490\alpha_8^{(n)},\\
&\alpha_1^{(n)} + 2\alpha_2^{(n)} + 2\alpha_3^{(n)} + 4\alpha_4^{(n)} + 56\alpha_5^{(n)} + 112\alpha_6^{(n)} + 98\alpha_7^{(n)} + 196\alpha_8^{(n)},\\
&14\alpha_1^{(n)} + 35\alpha_2^{(n)} + 24\alpha_3^{(n)} + 60\alpha_4^{(n)} + 4\alpha_5^{(n)} + 10\alpha_6^{(n)} + 6\alpha_7^{(n)} + 15\alpha_8^{(n)},\\
&7\alpha_1^{(n)} + 14\alpha_2^{(n)} + 12\alpha_3^{(n)} + 24\alpha_4^{(n)} + 2\alpha_5^{(n)} + 4\alpha_6^{(n)} + 3\alpha_7^{(n)} + 6\alpha_8^{(n)},\\
&8\alpha_1^{(n)} + 20\alpha_2^{(n)} + 14\alpha_3^{(n)} + 35\alpha_4^{(n)} + 2\alpha_5^{(n)} + 5\alpha_6^{(n)} + 4\alpha_7^{(n)} + 10\alpha_8^{(n)},\\
&4\alpha_1^{(n)} + 8\alpha_2^{(n)} + 7\alpha_3^{(n)} + 14\alpha_4^{(n)} + \alpha_5^{(n)} + 2\alpha_6^{(n)} + 2\alpha_7^{(n)} + 4\alpha_8^{(n)}\big).
\end{aligned}$$

If we take $(4, 2, 2, 1, 14, 7, 8, 4)$ as the initial solution of the sequence, the next three solutions of our octic equation are as follows:

(12285, 5460, 7092, 3152, 468, 208, 270, 120),
(578740, 258910, 334134, 149481, 729790, 326485, 421344, 188496),
(612075793, 273723336, 353382120, 158034240, 45691800, 20433600, 26380172, 11797344).

4. Threefold composition of forms and related diophantine equations

We will now consider forms that admit threefold composition and solve related diophantine equations.

4.1. *Quadratic forms.*

Theorem 4.1. *For arbitrary integers a, b, c, the binary quadratic form $Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ admits the threefold composition identity,*

$$Q(x_1, x_2)Q(y_1, y_2)Q(z_1, z_2) = Q(u_1, u_2) = Q(v_1, v_2) = Q(w_1, w_2), \tag{4.1}$$

for all $x_i, y_i, z_i \in \mathbb{R}, i = 1, 2$, and, if we write,

$$\phi_1(x_1, x_2, y_1, y_2, z_1, z_2) = ax_1y_1z_1 + bx_1y_2z_1 + cx_1y_2z_2 - cx_2y_1z_2 + cx_2y_2z_1,$$
$$\phi_2(x_1, x_2, y_1, y_2, z_1, z_2) = ax_1y_1z_2 - ax_1y_2z_1 + ax_2y_1z_1 + bx_2y_1z_2 + cx_2y_2z_2,$$

the values of u_i, v_i, w_i are given by,

$$u_1 = \phi_1(x_1, x_2, y_1, y_2, z_1, z_2), \qquad u_2 = \phi_2(x_1, x_2, y_1, y_2, z_1, z_2), \tag{4.2}$$

$$v_1 = \phi_1(y_1, y_2, z_1, z_2, x_1, x_2), \qquad v_2 = \phi_2(y_1, y_2, z_1, z_2, x_1, x_2), \tag{4.3}$$

$$w_1 = \phi_1(z_1, z_2, x_1, x_2, y_1, y_2), \qquad w_2 = \phi_2(z_1, z_2, x_1, x_2, y_1, y_2). \tag{4.4}$$

Proof. Let M_1 and M_2 be two matrices defined by

$$M_1 = \begin{bmatrix} t & 0 \\ b & -t \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 \\ c & 0 \end{bmatrix}, \quad t, b, c \in \mathbb{Z},\ t \neq 0. \tag{4.5}$$

Clearly $\mathcal{M} = \text{span}\{M_1, M_2\}$ is a 2-dimensional vector space which is not closed under multiplication of matrices since it is readily seen that $M_1^2 \notin \mathcal{M}$. An arbitrary matrix in $\mathcal{M}$ may be written as $M(x_1, x_2) = x_1M_1 + x_2M_2$ where $x_1, x_2 \in \mathbb{R}$. It is readily verified that

$$M(x_1, x_2)M(y_1, y_2)M(z_1, z_2) = M(u_1, u_2), \tag{4.6}$$

where u_1 and u_2 are trilinear forms in the variables x_i, y_i, z_i defined by

$$\begin{aligned} u_1 &= t^2x_1y_1z_1 + bx_1y_2z_1 + cx_1y_2z_2 - cx_2y_1z_2 + cx_2y_2z_1, \\ u_2 &= t^2x_1y_1z_2 - t^2x_1y_2z_1 + t^2x_2y_1z_1 + bx_2y_1z_2 + cx_2y_2z_2. \end{aligned} \tag{4.7}$$

It follows from (4.6) that the product $M(x_1, x_2)M(y_1, y_2)M(z_1, z_2) \in \mathcal{M}$. Taking determinants on both sides of (4.6), and replacing t^2 by a, we get the threefold composition identity,

$$Q(x_1, x_2)Q(y_1, y_2)Q(z_1, z_2) = Q(u_1, u_2). \tag{4.8}$$

We note that on permuting the three pairs of variables (x_1, x_2), (y_1, y_2), (z_1, z_2) in the identity (4.8), while the left-hand side of the identity remains unchanged, the values of u_1, u_2 get changed either to v_1, v_2, or to w_1, w_2, whose values are given by (4.3) and (4.4), respectively. We thus get the complete identity (4.1).

In the form $Q(x_1, x_2)$, we may choose the integers a, b and c such that $Q(x_1, x_2)$ is a negative definite form. The product $Q(x_1,\, x_2)Q(y_1,\, y_2)$ is thus necessarily positive, and hence cannot be expressed by the form $Q(z_1,\, z_2)$. Thus there cannot exist an identity $Q(x_1,\, x_2)Q(y_1,\, y_2) = Q(z_1,\, z_2)$ for arbitrary a, b, c, and hence the form $Q(x_1, x_2)$ indeed admits threefold composition. □

It follows from the identity (4.1) that a solution of the diophantine chain,

$$Q(u_1,\, u_2) = Q(v_1,\, v_2) = Q(w_1,\, w_2), \tag{4.9}$$

is given in terms of arbitrary parameters x_i, y_i, z_i by (4.2), (4.3) and (4.4).

4.2. *Higher degree forms admitting threefold composition.* We will now give a theorem, analogous to Theorem 2.4, for constructing forms that admit threefold composition. If $\mathcal{S}$ is a set of matrices, we will denote the span of $\mathcal{S}$ by $[\mathcal{S}]$.

THEOREM 4.2. *If $\mathcal{S}_1 = \{A_1, A_2, \ldots, A_h\}$ and $\mathcal{S}_2 = \{B_1, B_2, \ldots, B_k\}$ are linearly independent sets of matrices in $M_n(\mathbb{Z})$ and $M_m(\mathbb{Z})$, respectively, such that for any three, not necessarily distinct, matrices in $\mathcal{S}_i$, their product is in $[\mathcal{S}_i]$, both for $i = 1$ and $i = 2$, and either $[\mathcal{S}_1]$ or $[\mathcal{S}_2]$ is not closed under multiplication of matrices, then*

$$\mathcal{V} = \operatorname{span}\{B_i \otimes A_j,\ i = 1, \ldots, k,\ j = 1, \ldots, h\}, \tag{4.10}$$

is a vector subspace of $M_{mn}(\mathbb{R})$ such that for any three arbitrary matrices in $\mathcal{V}$, their product is also in $\mathcal{V}$. Further, for arbitrary parameters $x_{ij} \in \mathbb{R}, i = 1, \ldots, k,\ j = 1, \ldots, h$, if the matrix $C = C(x_{ij})$ is defined by

$$C(x_{ij}) = \sum_{i=1}^{k} \sum_{j=1}^{h} x_{ij}(B_i \otimes A_j), \tag{4.11}$$

the form f, of degree mn in the variables $x_{ij}, i = 1, \ldots, k,\ j = 1, \ldots, h$, defined by

$$f : \mathbb{R}^{kh} \to \mathbb{R},\ f(x_{11}, x_{12}, \ldots, x_{kh}) = \det\left(C(x_{11}, x_{12}, \ldots, x_{kh})\right), \tag{4.12}$$

satisfies a threefold composition identity.

PROOF. As in the proof of Theorem 2.4, we first construct the set $\mathcal{S} = \{B_i \otimes A_j, i = 1, \ldots, k, j = 1, \ldots, h\}$ of kh linearly independent square matrices of order mn so that $\mathcal{V}$ is a vector subspace of $M_{mn}(\mathbb{R})$ and $\dim \mathcal{V} = kh$.

For any $i_1, i_2, i_3 \in \{1, \ldots, k\}$ and $j_1, j_2, j_3 \in \{1, \ldots, h\}$, our assumption implies that $A_{j_1}A_{j_2}A_{j_3} \in [\mathcal{S}_1]$ and $B_{i_1}B_{i_2}B_{i_3} \in [\mathcal{S}_2]$. We may thus write $A_{j_1}A_{j_2}A_{j_3} = \sum_{j=1}^{h} s_j A_j,\ s_j \in \mathbb{R}$, and $B_{i_1}B_{i_2}B_{i_3} = \sum_{i=1}^{k} r_i B_i,\ r_i \in \mathbb{R}$.

Hence, in view of (2.17), we have,

$$\begin{aligned}(B_{i_1}\otimes A_{j_1})(B_{i_2}\otimes A_{j_2})(B_{i_3}\otimes A_{j_3}) &= ((B_{i_1}B_{i_2})\otimes(A_{j_1}A_{j_2}))(B_{i_3}\otimes A_{j_3}),\\ &= (B_{i_1}B_{i_2}B_{i_3})\otimes(A_{j_1}A_{j_2}A_{j_3})\\ &= (\sum_{i=1}^{k} r_iB_i)\otimes(\sum_{j=1}^{h} s_jA_j)\\ &= \sum_{i=1}^{k}\sum_{j=1}^{h} r_is_j(B_i\otimes A_j)\in\mathcal{V}.\end{aligned}$$

It now follows by a straightforward extension of the argument given in Lemma 2.1 that for any three arbitrary matrices in $\mathcal{V}$, their product is also in $\mathcal{V}$.

An arbitrary matrix $C=C(x_{ij})\in\mathcal{V}$ may be written as stated in (4.11). Since for any three arbitrary matrices $C(x_{ij}), C(y_{ij}), C(z_{ij})\in\mathcal{V}$, their product is also in $\mathcal{V}$, we may write this product as $C(w_{ij}), w_{ij}\in\mathbb{R}, i=1,\dots,k,\ j=1,\dots,h$, that is, $C(x_{ij})C(y_{ij})C(z_{ij})=C(w_{ij})$, and, on taking determinants, we get, $\det(C(x_{ij}))\det(C(y_{ij}))\det(C(z_{ij}))=\det(C(w_{ij}))$, which gives the threefold composition identity satisfied by the form f defined by (4.12). The values of w_{ij} are given by trilinear forms in the variables x_{ij}, y_{ij} and z_{ij}.

Finally, we note that if both $[\mathcal{S}_1]$ and $[\mathcal{S}_2]$ are closed under matrix multiplication, then the form f will satisfy the usual composition identity (1.1), which may be used twice to yield the composition identity (1.3), hence the stipulation imposed in the theorem. □

4.3. *Quartic forms and a related quartic diophantine equation.*

THEOREM 4.3. *The quartic form* $f(x_1,\dots,x_4)$ *defined by*

$$\begin{aligned}(4.13)\quad f(x_1,\dots,x_4) &= s^4t^4x_1^4+2s^2t^4mx_1^3x_2+2s^4t^2px_1^3x_3+s^2t^2mpx_1^3x_4\\ &+(m^2+2s^2n)t^4x_1^2x_2^2+3s^2t^2mpx_1^2x_2x_3+(m^2+2s^2n)t^2px_1^2x_2x_4\\ &+(p^2+2t^2q)s^4x_1^2x_3^2+(p^2+2t^2q)s^2mx_1^2x_3x_4+(s^2np^2+t^2m^2q-2s^2t^2nq)x_1^2x_4^2\\ &+2t^4mnx_1x_2^3+(m^2+2s^2n)t^2px_1x_2^2x_3+3t^2mnpx_1x_2^2x_4+(p^2+2t^2q)s^2mx_1x_2x_3^2\\ &+(m^2p^2+8s^2t^2nq)x_1x_2x_3x_4+(p^2+2t^2q)mnx_1x_2x_4^2+2s^4pqx_1x_3^3\\ &+3s^2mpqx_1x_3^2x_4+(m^2+2s^2n)pqx_1x_3x_4^2+mnpqx_1x_4^3+t^4n^2x_2^4+t^2mnpx_2^3x_3\\ &+2t^2n^2px_2^3x_4+(s^2np^2+t^2m^2q-2s^2t^2nq)x_2^2x_3^2+(p^2+2t^2q)mnx_2^2x_3x_4\\ &+(p^2+2t^2q)n^2x_2^2x_4^2+s^2mpqx_2x_3^3+(m^2+2s^2n)pqx_2x_3^2x_4+3mnpqx_2x_3x_4^2\\ &+2n^2pqx_2x_4^3+s^4q^2x_3^4+2s^2mq^2x_3^3x_4+(m^2+2s^2n)q^2x_3^2x_4^2+2mnq^2x_3x_4^3+n^2q^2x_4^4,\end{aligned}$$

where $s\neq0$, $t\neq0$ *and* $m,n,p,q,s,t\in\mathbb{Z}$, *admits threefold composition, and for all* $x_i, y_i, z_i\in\mathbb{R}$, $i=1,\dots,4$, *it satisfies the identity,*

$$(4.14)\qquad f(x_1,\dots,x_4)f(y_1,\dots,y_4)f(z_1,\dots,z_4)=f(w_1,\dots,w_4),$$

where the values of $w_i,\ i = 1, \ldots, 4,$ *are given by*

$$
\begin{aligned}
w_1 &= s^2t^2x_1y_1z_1 + mt^2x_1y_2z_1 + nt^2x_1y_2z_2 - nt^2x_2y_1z_2 \\
&\quad + \cdots + nqx_4y_1z_4 - nqx_4y_2z_3 - nqx_4y_3z_2 + nqx_4y_4z_1, \\
w_2 &= s^2t^2x_1y_1z_2 - s^2t^2x_1y_2z_1 + s^2t^2x_2y_1z_1 + mt^2x_2y_1z_2 \\
&\quad + \cdots + npx_2y_4z_2 + nqx_2y_4z_4 - nqx_4y_2z_4 + nqx_4y_4z_2, \\
w_3 &= s^2t^2x_1y_1z_3 - s^2t^2x_1y_3z_1 + s^2t^2x_3y_1z_1 + mt^2x_1y_2z_3 \\
&\quad + \cdots + npx_4y_2z_3 + nqx_3y_4z_4 - nqx_4y_3z_4 + nqx_4y_4z_3, \\
w_4 &= s^2t^2x_1y_1z_4 - s^2t^2x_1y_2z_3 - s^2t^2x_1y_3z_2 + s^2t^2x_1y_4z_1 \\
&\quad + \cdots + mpx_4y_1z_4 + mqx_4y_3z_4 + npx_4y_2z_4 + nqx_4y_4z_4.
\end{aligned} \tag{4.15}
$$

PROOF. In the matrices M_1, M_2 defined by (4.5), we first replace the parameters t, b, c by s, m, n, respectively, to get the matrices A_1, A_2, and we then replace the parameters b, c in the matrices M_1, M_2 by p, q, respectively, to get the matrices B_1 and B_2. The matrices A_1, A_2, B_1, B_2 may be written as

$$
A_1 = \begin{bmatrix} s & 0 \\ m & -s \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ n & 0 \end{bmatrix}, B_1 = \begin{bmatrix} t & 0 \\ p & -t \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0 & 1 \\ q & 0 \end{bmatrix}, \tag{4.16}
$$

where $s \neq 0$, $t \neq 0$ and $m, n, p, q, s, t \in \mathbb{Z}$. We note that the matrices $\{A_1, A_2\}$ and $\{B_1, B_2\}$ satisfy the conditions of Theorem 4.2. A straightforward application of Theorem 4.2 now gives the form $f(x_1, \ldots, x_4)$ which satisfies the threefold composition identity (4.14). It has been verified using MAPLE that the quartic form $f(x_1, \ldots, x_4)$ is irreducible for various numerical values of the parameters m, n, p, q, s and t. The values of $w_i,\ i = 1, \ldots, 4$, given by (4.15) are obtained by direct computation.

We will now show that the form $f(x_1, \ldots, x_4)$ defined by (4.13) does not satisfy any composition identity of type (1.1). If such an identity exists, it would be valid for all values of the integer parameters m, n, p, q, s, t. We now choose $(m, n, p, q, s, t) = (0, 1, 0, 2, 0, 0)$ when (1.1) reduces to $(4x_4^4)(4y_4^4) = 4z_4^4$ which is false since the value of z_4 must be given by a bilinear form with integer coefficients. Thus the form $f(x_1, \ldots, x_4)$ does not satisfy any identity of type (1.1) and is indeed a form admitting threefold composition. □

We will now consider the quartic diophantine equation $f(x_1, \ldots, x_4) = 1$ when $(m, n, p, q, s, t) = (-1, -4, 1, -1, 1, 1)$, that is, the equation,

$$
\begin{aligned}
& x_1^4 - 2x_1^3x_2 + 2x_1^3x_3 - x_1^3x_4 - 7x_1^2x_2^2 - 3x_1^2x_2x_3 - 7x_1^2x_2x_4 - x_1^2x_3^2 + x_1^2x_3x_4 \\
& - 13x_1^2x_4^2 + 8x_1x_2^3 - 7x_1x_2^2x_3 + 12x_1x_2^2x_4 + x_1x_2x_3^2 + 33x_1x_2x_3x_4 - 4x_1x_2x_4^2 \\
& - 2x_1x_3^3 + 3x_1x_3^2x_4 + 7x_1x_3x_4^2 - 4x_1x_4^3 + 16x_2^4 + 4x_2^3x_3 + 32x_2^3x_4 - 13x_2^2x_3^2 \\
& - 4x_2^2x_3x_4 - 16x_2^2x_4^2 + x_2x_3^3 + 7x_2x_3^2x_4 - 12x_2x_3x_4^2 - 32x_2x_4^3 + x_3^4 - 2x_3^3x_4 \\
& - 7x_3^2x_4^2 + 8x_3x_4^3 + 16x_4^4 = 1.
\end{aligned} \tag{4.17}
$$

It is readily verified that (4.17) is an irreducible equation, and two numerical solutions of Eq. (4.17) are (1, 0, 0, 0), and (21, 8, 33, 13).

If $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is any integer solution of Eq. (4.17) such that $\alpha_i > 0$ for each i, in the identity (4.14) we take, $(x_1, x_2, x_3, x_4) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $(y_1, y_2, y_3, y_4) = (1, 0, 0, 0)$, $(z_1, z_2, z_3, z_4) = (21, 8, 33, 13)$, and, on using the relations (4.15), we obtain a new solution of Eq. (4.17). As before, we combine the solution just obtained with the solutions $(y_1, y_2, y_3, y_4) = (1, 0, 0, 0)$ and $(z_1, z_2, z_3, z_4) = (21, 8, 33, 13)$ to obtain yet another solution of Eq. (4.17), and by repeatedly applying this process, we get an infinite sequence of solutions in positive integers of Eq. (4.17). If we denote the nth solution of the sequence by $(\alpha_1^{(n)}, \alpha_2^{(n)}, \alpha_3^{(n)}, \alpha_4^{(n)})$, the $(n+1)$th solution is given by the following linear recursive relations:

$$\begin{aligned}
\alpha_1^{(n+1)} &= 21\alpha_1^{(n)} + 32\alpha_2^{(n)} + 33\alpha_3^{(n)} + 52\alpha_4^{(n)},\\
\alpha_2^{(n+1)} &= 8\alpha_1^{(n)} + 13\alpha_2^{(n)} + 13\alpha_3^{(n)} + 20\alpha_4^{(n)},\\
\alpha_3^{(n+1)} &= 33\alpha_1^{(n)} + 52\alpha_2^{(n)} + 54\alpha_3^{(n)} + 84\alpha_4^{(n)},\\
\alpha_4^{(n+1)} &= 13\alpha_1^{(n)} + 20\alpha_2^{(n)} + 21\alpha_3^{(n)} + 33\alpha_4^{(n)}.
\end{aligned}$$

If we take (21, 8, 33, 13) as the initial solution of the sequence, the next three solutions of Eq. (4.17) obtained by the above process are as follows:

$$(2462, 961, 3983, 1555), \quad (294753, 115068, 476920, 186184),$$
$$(35291917, 13777548, 57103521, 22292541).$$

4.4. *Octic forms and a related octic diophantine equation.* We will now obtain an octic form that admits threefold composition by applying Theorem 4.2 to the linearly independent sets of matrices $\{M_1, M_2\}$ and $\{C_i, i = 1, \ldots, 4\}$ where the matrices M_i and C_i are defined by (4.5) and (3.1), respectively. Denoting the 8 matrices $C_i \otimes M_j, i = 1, \ldots, 4, j = 1, 2$, by $P_i, i = 1, \ldots, 8$, we write $\mathcal{V} = \text{span}\{P_1, \ldots, P_8\}$. Any arbitrary matrix $P = P(x_1, \ldots, x_8) \in \mathcal{V}$ may now be written as $P = \sum_{i=1}^{8} x_i P_i$ where $x_i \in \mathbb{R}, i = 1, \ldots, 8$. It follows from Theorem 4.2 that the form f defined by $f : \mathbb{R}^8 \to \mathbb{R}$, $f(x_1, \ldots, x_8) = \det(P(x_1, \ldots, x_8))$ admits a threefold composition identity.

Since the entries of the matrices M_i and C_i are in terms of arbitrary parameters b, c, t, m, n, p, and q, the coefficients in the form f are polynomials in these parameters. As the matrices P_i, the form f and the related composition formula are too cumbersome to write, we do not give them explicitly. We have, however, verified, using MAPLE that the form f is irreducible for various numerical values of the parameters b, c, t, m, n, p, and q. Further, it has been verified, as in the case of the quartic form (4.13), that the form $f(x_1, \ldots, x_8)$ does not satisfy any composition identity of the type (1.1) and it is indeed a form that admits threefold composition.

We now consider the octic diophantine equation $f(x_1, \ldots, x_8) = 1$ when $(b, c, t, m, n, p, q) = (0, -14, 1, 3, -1, 0, -3)$, so that the matrix $P(x_1, \ldots, x_8)$ may be written as,

$$P = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ 3x_1 - x_2 & -x_1 & 3x_3 - x_4 & -x_3 & 3x_5 - x_6 & -x_5 & 3x_7 - x_8 & -x_7 \\ 3x_3 & 3x_4 & x_1 & x_2 & 3x_7 & 3x_8 & x_5 & x_6 \\ 9x_3 - 3x_4 & -3x_3 & 3x_1 - x_2 & -x_1 & 9x_7 - 3x_8 & -3x_7 & 3x_5 - x_6 & -x_5 \\ 14x_5 & 14x_6 & 14x_7 & 14x_8 & x_1 & x_2 & x_3 & x_4 \\ 42x_5 - 14x_6 & -14x_5 & 42x_7 - 14x_8 & -14x_7 & 3x_1 - x_2 & -x_1 & 3x_3 - x_4 & -x_3 \\ 42x_7 & 42x_8 & 14x_5 & 14x_6 & 3x_3 & 3x_4 & x_1 & x_2 \\ 126x_7 - 42x_8 & -42x_7 & 42x_5 - 14x_6 & -14x_5 & 9x_3 - 3x_4 & -3x_3 & 3x_1 - x_2 & -x_1 \end{bmatrix},$$

and now the octic equation is given by

$$\det P = 1. \tag{4.18}$$

It is readily verified that (4.18) is an irreducible equation. We will show that Eq. (4.18) has infinitely many solutions in positive integers.

We note that two numerical solutions of Eq. (4.18) are $(1, 0, 0, 0, 0, 0, 0, 0)$ and $(2, 6, 1, 3, 7, 21, 4, 12)$. If $(\alpha_1, \ldots, \alpha_8)$ is an arbitrary solution of Eq. (4.18) such that $\alpha_i > 0$ for each i, we may use the threefold composition identity satisfied by the form f to combine the three solutions $(\alpha_1, \ldots, \alpha_8)$, $(1, 0, 0, 0, 0, 0, 0, 0)$ and $(2, 6, 1, 3, 7, 21, 4, 12)$, taken in that order, and get a new solution, and by repeatedly applying this process, we get an infinite sequence of solutions in positive integers of Eq. (4.18). As before, following our earlier notation, the $(n+1)$th solution of the sequence may be written in terms of the nth solution $(\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_8^{(n)})$ as follows:

$$\begin{aligned}
&\big(2\alpha_1^{(n)} + 6\alpha_2^{(n)} + 3\alpha_3^{(n)} + 9\alpha_4^{(n)} + 98\alpha_5^{(n)} + 294\alpha_6^{(n)} + 168\alpha_7^{(n)} + 504\alpha_8^{(n)},\\
&6\alpha_1^{(n)} + 20\alpha_2^{(n)} + 9\alpha_3^{(n)} + 30\alpha_4^{(n)} + 294\alpha_5^{(n)} + 980\alpha_6^{(n)} + 504\alpha_7^{(n)} + 1680\alpha_8^{(n)},\\
&\alpha_1^{(n)} + 3\alpha_2^{(n)} + 2\alpha_3^{(n)} + 6\alpha_4^{(n)} + 56\alpha_5^{(n)} + 168\alpha_6^{(n)} + 98\alpha_7^{(n)} + 294\alpha_8^{(n)},\\
&3\alpha_1^{(n)} + 10\alpha_2^{(n)} + 6\alpha_3^{(n)} + 20\alpha_4^{(n)} + 168\alpha_5^{(n)} + 560\alpha_6^{(n)} + 294\alpha_7^{(n)} + 980\alpha_8^{(n)},\\
&7\alpha_1^{(n)} + 21\alpha_2^{(n)} + 12\alpha_3^{(n)} + 36\alpha_4^{(n)} + 2\alpha_5^{(n)} + 6\alpha_6^{(n)} + 3\alpha_7^{(n)} + 9\alpha_8^{(n)},\\
&21\alpha_1^{(n)} + 70\alpha_2^{(n)} + 36\alpha_3^{(n)} + 120\alpha_4^{(n)} + 6\alpha_5^{(n)} + 20\alpha_6^{(n)} + 9\alpha_7^{(n)} + 30\alpha_8^{(n)},\\
&4\alpha_1^{(n)} + 12\alpha_2^{(n)} + 7\alpha_3^{(n)} + 21\alpha_4^{(n)} + \alpha_5^{(n)} + 3\alpha_6^{(n)} + 2\alpha_7^{(n)} + 6\alpha_8^{(n)},\\
&12\alpha_1^{(n)} + 40\alpha_2^{(n)} + 21\alpha_3^{(n)} + 70\alpha_4^{(n)} + 3\alpha_5^{(n)} + 10\alpha_6^{(n)} + 6\alpha_7^{(n)} + 20\alpha_8^{(n)}\big).
\end{aligned}$$

If we take $(2, 6, 1, 3, 7, 21, 4, 12)$ as the initial solution of the sequence, the next three solutions of Eq. (4.18) obtained by the above process are as follows:

(13650, 45045, 7880, 26004, 520, 1716, 300, 990),
(1660070, 5482800, 958437, 3165480, 2093345, 6913800, 1208592, 3991680),
(4520236757, 14929326951, 2609759880, 8619450840,
337438200, 1114482600, 194820028, 643446804).

5. Concluding remarks

The composable forms constructed in Sections 3 and 4 above are illustrative examples, and many more forms admitting composition may be obtained in a similar manner. In fact, the general methods given in this paper may be used to construct forms of arbitrarily high degree admitting the composition identity (1.1) or the threefold composition identity (1.3).

It would also be of interest to explore the existence of forms that admit m-fold composition where $m > 3$, that is, we seek forms which satisfy a composition identity,

$$f(x_{11},\dots,x_{1n})f(x_{21},\dots,x_{2n})\cdots f(x_{k1},\dots,x_{kn}) = f(w_1,\dots,w_n), \tag{5.1}$$

where $k = m$ and the identity (5.1) cannot be derived from a similar identity with $k < m$.

The examples of diophantine equations given in Sections 3 and 4 are also only illustrative in nature. It would be of interest to construct diophantine equations $f(x_i) = 1$ with infinitely many solutions in positive integers when $f(x_i)$ is a form of degree n in n variables and $n > 8$.

Acknowledgements.

I am extremely grateful to the referee for his very insightful report and valuable guidance that has led to elegant proofs of the results obtained in the paper. I also wish to thank the Harish-Chandra Research Institute, Prayagraj for providing me with all necessary facilities that have helped me to pursue my research work in mathematics.

References

[1] L. E. Dickson, *Homogeneous polynomials with a multiplication theorem*, in Comptes Rendus du Congrès International des Mathématiciens, Strasbourg, 1920, ed. H. Villat, Toulouse (1921), pp. 215–230.

[2] O. C. Hazlett, *Homogeneous polynomials with a multiplication theorem*, Trans. Amer. Math. Soc. **31** (1929), 223–232.

[3] P. Lancaster and M. Tismenetsky, The Theory of Matrices, Second Edition, Academic Press, San Diego, 1985.

[4] C. C. MacDuffee, *On the composition of algebraic forms of higher degree*, Bull. Amer. Math. Soc. **51** (1945), 198–211.

[5] S. Pumplün, *Forms of higher degree permitting composition*, Beitr. Algebra Geom. **52** (2011), 265–284.

[6] R. D. Schafer, *On forms of degree n permitting composition*, J. Math. Mech. **12** (1963), 777–792.

[7] R. D. Schafer, *Forms permitting composition*, Advances in Math. **4** (1970), 111–148.

Morfologija matrica i kompozicija formi višeg stupnja s primjenama na diofantske jednadžbe

Ajai Choudhry

SAŽETAK. U ovom članku koristimo matrice za dobivanje novih kompozicijskih identiteta $f(x_i)f(y_i) = f(z_i)$, gdje je $f(x_i)$ ireducibilna forma s cjelobrojnim koeficijentima stupnja n u n varijabli (n je 3, 4, 6 ili 8), x_i, y_i, $i = 1, 2, \ldots, n$ su nezavisne varijable, dok su vrijednosti od z_i, $i = 1, 2, \ldots, n$ dane bilinearnim formama u varijablama x_i, y_i. Za $n = 2$, 4 ili 8, također dobivamo nove kompozicijske identitete $f(x_i)f(y_i)f(z_i) = f(w_i)$ gdje je, kao prije, $f(x_i)$ ireducibilna forma s cjelobrojnim koeficijentima stupnja n u n varijabli, dok su x_i, y_i, z_i, $i = 1, 2, \ldots, n$ nezavisne varijable i vrijednosti od w_i, $i = 1, 2, \ldots, n$ su dane trilinearnim formama u varijablama x_i, y_i, z_i, takve da se ovi identiteti ne mogu izvesti iz identiteta oblika $f(x_i)f(y_i) = f(z_i)$. Nadalje, opisujemo metodu dobivanja obje ove vrste kompozicijskih identiteta za forme viših stupnjeva. Također opisujemo metodu generiranja beskonačno mnogo cjelobrojnih rješenja određenih kvartičnih i oktičnih diofantskih jednadžbi $f(x_1, \ldots, x_n) = 1$, gdje je $f(x_1, \ldots, x_n)$ forma koja dozvoljava kompozicijski identitet i $n = 4$, 6 ili 8.

Ajai Choudhry
13/4 A Clay Square, Lucknow - 226001, India
E-mail: ajaic203@yahoo.com

Received: 12.5.2021.
Revised: 14.10.2021.; 16.11.2021.
Accepted: 14.12.2021.