Enumerative Combinatorics and Applications

ecajournal.haifa.ac.il

ECA **1:3** (2021) Article #S2R18

Semi-Invariants of Binary Forms and Symmetrized Graph-Monomials

Shashikant Mulay

Department of Mathematics, University of Tennessee, Knoxville, TN 37996 U.S.A.
Email: smulay@utk.edu

Received: November 10, 2020, **Accepted**: March 10, 2021, **Published**: March 26, 2021

Abstract: This article provides a method for constructing invariants and semi-invariants of a binary N-ic form over a field k characteristics 0 or $p > N$. A practical and broadly applicable sufficient condition for ensuring non-triviality of the symmetrization of a graph-monomial is established. This allows the construction of infinite families of invariants (especially, skew-invariants) and families of k-linearly independent semi-invariants. These constructions are very useful in the quantum physics of Fermions. Additionally, they permit us to establish a new polynomial-type lower bound on the coefficient of q^w in $(1-q)\binom{N+d}{d}_q$ for all sufficiently large integers d and $w \le Nd/2$.

Keywords: Semi-invariants of binary forms; Symmetrized graph-monomials
2020 Mathematics Subject Classification: 05E05, 13A50

1. Introduction

Fix an integer $N \ge 2$. Let k be a field of characteristic either 0 or strictly greater than N. Let X, Y, t, $z_1, \ldots, z_N$ be indeterminates. Let $E_1(t), \ldots, E_N(t)$ and $f(X+t)$ be the polynomials defined by

$$f(X+t) \;:=\; \prod_{i=1}^{N}(X + z_i + t) \;=:\; X^N + \sum_{i=1}^{N} E_i(t)X^{N-i}.$$

For $1 \le i \le N$, let $e_i := E_i(0)$. Then, $f(X) = X^N + e_1X^{N-1} + \cdots + e_N$. A polynomial $P(e_1, \ldots, e_N) \in k[e_1, \ldots, e_N]$ is said to be *translation invariant* provided $P(E_1(t), \ldots, E_N(t)) = P(e_1, \ldots, e_N)$. It is a (well known) simple exercise to verify that the subring $k[y_1, \ldots, y_{N-1}]$ of $k[e_1, \ldots, e_N]$, where $y_i := E_i(-e_1/N)$ for $1 \le i \le N$, is the ring of all translation invariant members of $k[e_1, \ldots, e_N]$. Furthermore, we have $k[y_1, \ldots, y_{N-1}] = k[e_1, \ldots, e_N] \cap k[z_1 - z_2, \ldots, z_1 - z_N]$ (*e.g.*, see Ch. 2, Theorem 1 of [10]). A polynomial $h \in k[e_1, \ldots, e_N]$ is said to be homogeneous of *weight* w provided as a polynomial in $z_1, \ldots, z_N$, h is homogeneous of degree w. Note that y_i is homogeneous of weight $i+1$ for $1 \le i \le N$. Next, consider the (generic) binary form $F := \sum a_iX^iY^{N-i}$ of degree N where a_0 is an indeterminate and $a_i := a_0e_i$ for $1 \le i \le N$. A *semi-invariant of F of degree d and weight w* is a polynomial $Q \in k[a_0, a_1, \ldots, a_N]$ such that $Q = a_0^dP(e_1, \ldots, e_N)$ where $P(e_1, \ldots, e_N)$ is translation invariant, homogeneous of weight w and has total degree $\le d$ in $e_1, \ldots, e_N$. For $0 \le i \le N$, the weight of a_i is defined to be i. Then, note that Q is homogeneous of degree d and weight w in $a_0, \ldots, a_N$. An *invariant* of F of degree d is a semi-invariant of F of degree d and weight $Nd/2$. For a fixed N, the set of semi-invariants (of the binary N-ic F) of degree d and weight w form a finite dimensional k-linear subspace of $k[a_0, a_1, \ldots, a_N]$. This subspace is known to be trivial unless $2w \le Nd$. Provided $\operatorname{char} k = 0$ and $2w \le Nd$, a theorem of Cayley-Sylvester proves that the dimension of the aforementioned space of semi-invariants of degree d and weight w is the coefficient of q^w in $(1-q)\binom{N+d}{d}_q$ where $\binom{N+d}{d}_q$ is the q-binomial coefficient (see [6], [18] or Theorem 5 of [10]). Let $p_w(N,d)$ denote the coefficient of q^w in $\binom{N+d}{d}_q$. Then, $p_w(N,d)$ is the number of integer-partitions of w in at most N parts with each part $\le d$. As a corollary of the Cayley-Sylvester theorem, we then have $p_w(N,d) \ge p_{w-1}(N,d)$ for $2 \le w \le Nd/2$; this establishes the *unimodality* of the coefficients of $\binom{N+d}{d}_q$. For the first purely combinatorial proof of this result, see [11]. Since $p_w(N,d) - p_{w-1}(N,d)$ are the dimensions of spaces of semi-invariants, it is natural to investigate explicit (lower, upper) bounds on them. Recently, some interesting lower bounds on $p_w(N,d) - p_{w-1}(N,d)$ have come to light (see [4], [12], [19] and their references). This article has two objectives: provide explicit methods of constructing a class of k-linearly independent semi-invariants and obtain a new lower bound on $p_w(N,d) - p_{w-1}(N,d)$ for certain pairs (w,d).

The non-trivial lower bounds of [4], [12] and [19] are valid for $\min\{N, d\} \geq 8$ but for all sufficiently large values of d and w, they do not depend on (w, d). In contrast, our lower bounds (see Theorem 3.1) are polynomials in w for all (N, d); Example 3.1-3.2 and Remark 3.1 appearing at the end of the article present a more detailed comparison. In the rest of the introduction, we describe our motivation for, and our method of, constructing semi-invariants of a binary N-ic form.

Ever since the theory of invariants of binary forms was founded, invariant-theorists have explored and devised methods for writing down concrete invariants; however, each of these methods has its own shortcomings. The 'symbolic method' of classical invariant theory (see [3], [6], [7]) provides an easy recipe for formulating symbolic expressions that yield invariants and semi-invariants. But, without full expansion (or un-symbolization) one does not know whether a given symbolic expression yields a *nonzero* semi-invariant. Here we prefer the other method, *i.e.*, the method of symmetrized graph-monomials. This too was known to classical invariant theorists (see [13], [14], [17]). It poses the problem of finding a useful criterion to determine the nonzero-ness of the symmetrization. Historically, Sylvester and Petersen considered this problem; in fact, Petersen formulated a sufficient (but not necessary) condition that ensures zero-ness of the symmetrization. For a detailed historical sketch of this topic, we refer the reader to [16]. In [16], nonzero-ness of the symmetrization of a graph-monomial is shown to be equivalent to certain properties of the orientations and the orientation preserving graph-automorphisms of the underlying graph; but as matters stand, verification of these properties is as forbidding as is a brute force computation of the desired symmetrization. Our interest in *construction*, as opposed to *existence*, of invariants and semi-invariants stems primarily from the need to obtain explicitly described *trial wave functions* for systems of N strongly correlated Fermions in a fractional quantum Hall state. Such a trial wave function is essentially determined by a so-called *correlation function.* The intuitive approach of physics presents such a correlation function as a symmetrization of a *monomial* obtained from the graph of correlations representing allowed strong interactions between N Fermions. It so happens that this correlation function turns out to be a semi-invariant (an invariant in certain cases), of a binary N-ic form. In this article, we establish an easy-to-use yet broadly applicable sufficient criterion (see Theorem 2.1) for non-triviality of a symmetrized graph-monomial. Besides enabling explicit constructions of the desired trial wave functions, Theorem 2.1 is also interesting from a purely invariant theoretic point of view. Following Theorem 2.1, we exhibit a sample of its applications (see Theorem 2.2, Theorem 3.1).

A *multigraph* is a graph in which multiple edges are allowed between the same two vertices of the graph. Consider a loopless undirected multigraph Γ on finitely many (at least two) vertices labeled $1, 2, \ldots, N$; multigraph Γ is said to be *d-regular* provided each vertex of Γ has the same degree d. In the figures below, Γ_1 is seen to be a 2-regular multigraph and the multigraphs Γ_2, Γ_3 both are 3-regular.

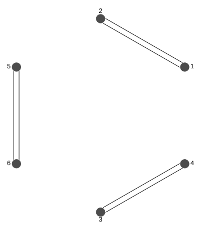

Figure 1: Γ_1

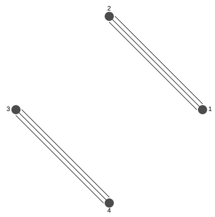

Figure 2: Γ_2

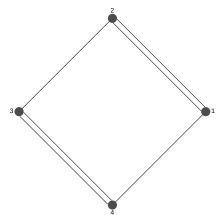

Figure 3: Γ_3

Let $\varepsilon(\Gamma, i, j)$ be the number of edges in Γ connecting vertex i to vertex j. The *graph-monomial* of Γ, denoted by $\mu(\Gamma)$, is the polynomial in $z_1, \ldots, z_N$ defined by

$$\mu(\Gamma) := \prod_{1 \leq i < j \leq N} (z_i - z_j)^{\varepsilon(\Gamma, i, j)}.$$

Let $g(\Gamma)$ denote the *symmetrization* of $\mu(\Gamma)$, *i.e.*, $g(\Gamma) := \sum \mu_\sigma(\Gamma)$, where the sum ranges over the permutations σ of $\{1, 2, \ldots, N\}$ and $\mu_\sigma(\Gamma)$ stands for the product of $(z_{\sigma(i)} - z_{\sigma(j)})^{\varepsilon(\Gamma, i, j)}$ for $1 \leq i < j \leq N$. In the classical invariant theory of binary forms (where $k = \mathbb{C}$), it is well known that if Γ is d-regular on N vertices, then $g(\Gamma)$ is a (relative) invariant of degree d (and weight $Nd/2$) of the binary N-ic form F. Moreover, the vector space of invariants of F of degree d is spanned by the set of symmetrized graph monomials corresponding to the d-regular multigraphs on N vertices (for a proof see [6] or its modern treatment: Ch. 2, Theorem 4 of [10]). If Γ is not d-regular for any d, then $g(\Gamma)$ is a semi-invariant (as defined in [6], [7]) of F irrespective of the characteristic of k. For example, $g(\Gamma_1)$ is a quadratic invariant of a binary sextic (investigated in [5]) and each of $g(\Gamma_2)$, $g(\Gamma_3)$ is a cubic invariant of a binary quartic. It can be easily verified that $g(\Gamma_2)$ is identically 0 whereas $g(\Gamma_3)$ is essentially the only nonzero cubic invariant of a binary quartic. In general, given a nonzero semi-invariant of F, there is no known method to determine whether the invariant is $g(\Gamma)$ for some multigraph Γ. Also, for non-isomorphic multigraphs Γ, Γ', their corresponding semi-invariants $g(\Gamma)$, $g(\Gamma')$ may be numerical multiples of each other. Clearly, it is desirable to understand the types of multigraph Γ for which $g(\Gamma)$ is nonzero. For then, we get a natural method of constructing nonzero semi-invariants of F.

In the physics of Fermion-correlations, vertices of Γ correspond to Fermions and the edges in Γ represent correlations (a repulsive interaction) between the Fermions; here, it suffices to work over $\mathbb{C}$. A multigraph Γ is called a *configuration* of Fermions provided $g(\Gamma)$ is nonzero, and then $g(\Gamma)$ is called the correlation-function of this configuration. A configuration Γ need not be d-regular for any d. In physics, a configuration Γ is as important as its associated correlation function $g(\Gamma)$. This leads to some interesting new problems that do not seem to have any parallels in the theory of invariants. For example, let $p(\Gamma)$ and $L(\Gamma)$ denote the maximum of and the sum of all $\varepsilon(\Gamma, i, j)$ respectively. For fixed integers N, L and d, consider the set $C(N, L, d)$ of multigraphs Γ with the maximum vertex-degree d, $L(\Gamma) = L$ and $g(\Gamma) \neq 0$. Let $p(N, L, d)$ denote the minimum of $p(\Gamma)$ as Γ ranges over $C(N, L, d)$. A configuration $\Gamma \in C(N, L, d)$ is *minimal* if $p(\Gamma) = p(N, L, d)$. It is known (see [11], [15]) that the lowest energy configurations (or states) Γ are those with the least $p(\Gamma)$. Thus one needs to estimate $p(N, L, d)$ for a given triple (N, L, D). Likewise, given Γ, $\Gamma' \in C(N, L, d)$, it is of interest to know when $g(\Gamma)$ is (or is not) a constant multiple of $g(\Gamma')$. Without digressing into deeper physics, we simply refer the reader to [2], [9], [10] and [15]. Using a weak corollary of Theorem 2.1 of this article, we have explicitly constructed trial wave functions for the *minimal IQL configurations* of N Fermions in a Jain state with filling factor $< 1/2$ (see [10]); it is not possible to give a full account of our recent results here. The central result of this article (Theorem 2.1), presents a useful sufficient condition on a multigraph Γ that ensures non-triviality of $g(\Gamma)$. There is nothing akin to Theorem 2.1 in the existing literature. Whenever Theorem 2.1 is applicable to even a single member of $C(N, L, d)$, it readily yields an upper bound on $p(N, L, d)$. Our proof of Theorem 2.1 is purely algebraic in nature; so, the edge-function (or the edge-matrix) of a multigraph is of key importance in the proof. In Theorem 2.1 we consider only those multigraphs Γ that can be partitioned into two or more sub-multigraphs $\Gamma_1, \ldots, \Gamma_m$ such that each $g(\Gamma_i)$ is nonzero (in particular, if Γ_i has no edges) and the *inter-edges* between pairs Γ_i, Γ_j are more 'dominating' (in a specific way) than the *intra-edges* within each Γ_i. Using Theorem 2.1, we are able to construct several infinite families of invariants (including skew-invariants, see Theorem 2.2) as well as families of k-linearly independent semi-invariants of a binary N-ic form over k (see Theorem 3.1). Philosophically, our approach has its source in [1] where the linear independence of standard monomials is proved by counting the corresponding standard Young bitableaux; this yields formulae for Hilbert functions of ladder determinantal ideals. In a similar spirit, we count multigraphs of a certain 'degree' and 'weight' to produce linearly independent semi-invariants of the corresponding degree and weight; this yields the aforementioned lower bound. In closing, we share our optimism that there is a generalization of Theorem 2.1 yet to be discovered, that will allow construction of all semi-invariants as symmetrized-graph-monomials.

2. Symmetrization of graph-monomials

In what follows, N is tacitly assumed to be an integer ≥ 2, k denotes a field and $z_1, \ldots, z_N$ are indeterminates. We let z stand either for $(z_1, \ldots, z_N)$ or the set $\{z_1, \ldots, z_N\}$. It is tacitly assumed that either k has characteristic 0 or the characteristic of k is $> N$. As usual, given a positive integer n, S_n denotes the group of all permutations of the set $\{1, \ldots, n\}$.

Definition 2.1. *Let m and n be positive integers.*

1. *Let $Symm_N : k[z] \to k[z]$ be the Symmetrization operator defined by*

$$Symm_N(f) := \sum_{\sigma \in S_N} f(z_{\sigma(1)}, \ldots, z_{\sigma(N)}).$$

   $f \in k[z]$ is said to be symmetric provided

$$f(z_{\sigma(1)}, \ldots, z_{\sigma(N)}) \;=\; f(z_1, \ldots, z_N) \quad \text{for all } \sigma \in S_N.$$

2. *For an $m \times n$ matrix $A := [a_{ij}]$, let $r_i(A) := a_{i1} + \cdots + a_{in}$ (the sum of the entries in the i-th row of A) for $1 \leq i \leq m$ and let*

$$\|A\| \;:=\; r_1(A) + \cdots + r_m(A) \;=\; \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}.$$

3. *Let $E(N)$ denote the set of all $N \times N$ symmetric matrices $A := [a_{ij}]$ such that each a_{ij} is a nonnegative integer and $a_{ii} = 0$ for $1 \leq i \leq N$.*

4. *Given an integer d, by $E(N, d)$ we denote the subset of $A \in E(N)$ such that $r_i(A) = d$ for $1 \leq i \leq N$, i.e., each row-sum of A is exactly d.*

5. *For an $N \times N$ matrix $A := [a_{ij}]$, let*

$$\delta(z, A) \;:=\; \prod_{1 \leq i < j \leq N} (z_i - z_j)^{a_{ij}}.$$

6. *Let $D_{(m,n)} := [(c_{ij}]$ be the $m \times n$ matrix such that*

$$c_{ii} := \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } i \neq j. \end{cases}$$

By D_n, we mean $D_{(n,n)}$. In particular, $D_1 = 0$.

Lemma 2.1. *Let n be a positive integer. For $1 \leq i \leq n$, let $g_i \in \mathbb{Q}(z)$. Then $g_1^2 + g_2^2 + \cdots + g_n^2 = 0$ if and only if $g_i = 0$ for $1 \leq i \leq n$. In particular, given a $0 \neq g \in \mathbb{Q}(z_1, \ldots, z_N)$ and a nonempty subset $S \subseteq S_N$, we have*

$$\sum_{\sigma \in S} g(z_{\sigma(1)}, \ldots, z_{\sigma(N)})^2 \neq 0.$$

Proof. With the above notation, assume that $g_1 \neq 0$. Let $h := g_1^2 + g_2^2 + \cdots + g_n^2$. For $1 \leq i \leq n$, let $p_i, q_i \in \mathbb{Q}[z_1, \ldots, z_N]$ be polynomials such that $g_i q_i = p_i$ and $q_i \neq 0$. Note that, $g_1 \neq 0$ implies $p_1 \neq 0$. Now since $f := p_1 q_1 q_2 \cdots q_n$ is a nonzero polynomial with coefficients in $\mathbb{Q}$, there exists $(a_1, \ldots, a_N) \in \mathbb{Q}^N$ such that $f(a_1, \ldots, a_N) \neq 0$. Fix such an N-tuple $(a_1, \ldots, a_N)$ and let $c_i := g_i(a_1, \ldots, a_N)$ for $1 \leq i \leq n$. Then, $c_1 \neq 0$ and $c_i \in \mathbb{Q}$ for $1 \leq i \leq n$. Since $c_1^2 > 0$ and $(c_2^2 + \cdots + c_n^2) \geq 0$, we have $h(a_1, \ldots, a_N) > 0$. This proves the first claim. The remaining assertions now easily follow. □

Definition 2.2.

1. *For $B \subseteq \{1, 2, \ldots, N\}$, let*

$$\pi(B) := \{(i, j) \in B \times B \mid i < j\}.$$

By abuse of notation, $\pi(B)$ is also identified as the set of all 2-element subsets of B. The set $\pi(\{1, \ldots, N\})$ is denoted by $\pi[N]$.

2. *Given $C \subseteq \pi[N]$ and a function $\varepsilon : C \to \mathbb{N}$, the image of $(i, j) \in C$ via ε is denoted by $\varepsilon(i, j)$. An integer $w \in \mathbb{N}$ is identified with the constant function $C \to \mathbb{N}$ such that $(i, j) \to w$ for all $(i, j) \in C$.*

3. *Given $C \subseteq \pi[N]$ and a function $\varepsilon : C \to \mathbb{N}$, define*

$$v(z, C, \varepsilon) := \prod_{(i,j) \in C} (z_i - z_j)^{\varepsilon(i,j)}$$

with the understanding that $v(z, \emptyset, \varepsilon) = 1$.

Remark 2.1. *There is an obvious bijective correspondence $\varepsilon \leftrightarrow [a_{ij}]$ given by*

$$a_{ij} = \varepsilon(i, j) \quad \text{for } 1 \leq i < j \leq N$$

between the set of functions $\varepsilon : \pi[N] \to \mathbb{N}$ and the set $E(N)$.

Suppose $m_1 \leq m_2 \leq \cdots \leq m_q$ is a partition of N and $M \in E(N)$. Consider M as a $q \times q$ block-matrix $[M_{rs}]$, where M_{rs} has size $m_r \times m_s$ for $1 \leq r, s \leq q$. View M as the sum $M^* + M^{**}$, where M^* is the $q \times q$ block-diagonal matrix having M_{rr} as its r-th diagonal block and where M^{**} is the $q \times q$ block-matrix whose diagonal blocks are zero-matrices. Clearly, M^* and M^{**} both are in $E(N)$ and $M_{rr} \in E(m_r)$ for $1 \leq r \leq q$.

Definition 2.3. *Let the notation be as above.*

1. *For $1 \leq r \leq q$, define*

$$A_r := \{i + m_0 + \cdots + m_{r-1} \mid 1 \leq i \leq m_r\}.$$

2. *For $1 \leq r \leq q$, let G_r denote the group of permutations of the set A_r.*

3. *Define*

$$\pi := \bigcup_{1 \leq r < s \leq q} A_r \times A_s.$$

4. *For $1 \leq r \leq q$ and $(i, j) \in \pi(A_r)$, let $\varepsilon_r(i, j)$ denote the ij-th entry of M^*.*

5. *For $1 \leq r \leq q$, define*

$$\delta_r(M^*) := Symm_{m_r}(v(z, \pi(A_r), \varepsilon_r)).$$

6. *For $(i,j) \in \pi[N]$, let $\varepsilon(i,j)$ denote the ij-th entry of M^{**}.*

Remark 2.2. 1. *Observe that*

$$\pi \;=\; \pi[N] \setminus \bigcup_{i=1}^{q} \pi(A_i).$$

2. *For each r, the $\varepsilon_r(i,j)$ are the entries in the strict upper-triangle of the symmetric matrix M_{rr}.*

3. *We have $\delta(z, M^{**}) \;=\; v(z, \pi[N], \varepsilon)$ and*

$$\delta(Z, M^*) \;=\; \prod_{r=1}^{q} v(z, \pi(A_r), \varepsilon_r).$$

4. *We have $\delta(z, M) = \delta(z, M^*) \cdot \delta(z, M^{**})$.*

5. *For each r, we have*

$$\delta_r(M^*) \;=\; \sum_{\sigma \in G_r} \sigma(v(z, \pi(A_r), \varepsilon_r)).$$

6. *The $\varepsilon(i,j)$ are the entries in the strict upper-triangle of the symmetric matrix M^{**}.*

Theorem 2.1. *Let the notation be as above. Assume $q \geq 2$ and of the following properties (1) - (3), either (1) and (2) hold or (1) and (3) hold.*

(1) *For $1 \leq r < s \leq q$, the matrix M_{rs} has only positive entries.*

(2) *For $1 \leq r < s \leq q$, the positive integer $b(m_r, m_s) := \|M_{rs}\|$ depends only on the ordered pair $(m_r,\, m_s)$ and furthermore, if $m_r = m_s$, then $b(m_r, m_s)$ is an even integer.*

(3) *Characteristic of k is 0 and for $1 \leq r < s \leq q$, $\|M_{rs}\|$ is even.*

Also, assume that the properties (i) - (iv) listed below are satisfied.

(i) *Either $m_i < m_j$ for $1 \leq i < j \leq q$ or $M^* = 0$.*

(ii) *If properties (1) and (2) hold, then $\prod_{r=1}^{q} \delta_r(M^*) \neq 0$.*

(iii) *If property (2) does not hold but properties (1) and (3) hold, then each entry of M^* is an even integer.*

(iv) *The least nonzero entry of the matrix M^{**} is strictly greater than the greatest entry of the matrix M^*.*

Then $Symm_N\,(\delta(z, M)) \;\neq\; 0$.

Proof. Define $m_0 \;=\; 0$. At the outset, observe that a permutation $\sigma \in S_N$ can be naturally viewed as a permutation of $\pi[N]$ by letting $\sigma(i,j) \;:=\; \{\sigma(i), \sigma(j)\}$, *i.e.*, for $(i,j) \in \pi[N]$,

$$\sigma(i,j) \;:=\; \begin{cases} (\sigma(i), \sigma(j)) & \text{if } \sigma(i) < \sigma(j), \\ (\sigma(j), \sigma(i)) & \text{if } \sigma(j) < \sigma(i). \end{cases}$$

Thus S_N is regarded as a subgroup of the group of permutations of $\pi[N]$.

For $\sigma \in S_N$ and $1 \leq r \leq q$, define

$$B_r(\sigma) \;:=\; \sigma^{-1}(A_r) \;=\; \{i \mid 1 \leq i \leq N \;\text{ and }\; \sigma(i) \in A_r\}.$$

Clearly, sets $B_1(\sigma), \ldots, B_q(\sigma)$ partition $\{1, \ldots, N\}$ and B_i has cardinality m_i for all $1 \leq i \leq q$.

Define

$$G \;:=\; \{\sigma \in S_N \mid \sigma(i,j) \in \pi \;\text{ for all } (i,j) \in \pi\}.$$

For $1 \leq r \leq q$, a permutation $\sigma \in G_r$ is to be regarded as an element of S_N by declaring $\sigma(i) = i$ if $i \in \{1, \ldots, N\} \setminus A_r$. This way each G_r is identified as a subgroup of S_N.

Given $\sigma \in G$ and $(i,j) \in \pi(A_r)$ with $1 \leq r \leq q$, clearly there is a unique s with $1 \leq s \leq q$ such that $\sigma(i,j) \in \pi(A_s)$. Fix a $\sigma \in G$. Consider $i \in B_r(\sigma) \cap A_s$ with $1 \leq s \leq q$. Then for $i \neq j \in A_s$, we must have $\{\sigma(i), \sigma(j)\}$ in $\pi(A_r)$ and hence $j \in B_r(\sigma)$. It follows that $A_s \subseteq B_r(\sigma)$. If $1 \leq s < p \leq q$ are such that $A_s \cup A_p \subseteq B_r(\sigma)$, then an $(i,j) \in A_s \times A_p$ is in π whereas $\sigma(i,j)$ is in $\pi(A_r)$. This is impossible since $\sigma \in G$. Thus we have established the following: given r with $1 \leq r \leq q$ and $\sigma \in G$, there is a unique integer $r(\sigma)$ such that $1 \le r(\sigma) \le q$ and $B_r(\sigma) = A_{r(\sigma)}$. In other words, the image sets $\sigma(A_1), \ldots, \sigma(A_q)$ form a permutation of the sets $A_1, \ldots, A_q$. If $1 \le r < s \le q$ and $\sigma \in G$, then since $r(\sigma) \ne s(\sigma)$, we infer that

$$\pi \cap \left(A_{r(\sigma)} \times A_{s(\sigma)}\right) \ne \emptyset \quad \text{if and only if } r(\sigma) < s(\sigma).$$

Moreover,

$$m_{r(\sigma)} \;=\; m_r \quad \text{for all } 1 \le r \le q \text{ and } \sigma \in G.$$

If the first case of (i) holds, *i.e.*, the integers m_i are mutually unequal, then we must have $r(\sigma) = r$ for all $1 \le r \le q$ and $\sigma \in G$. Hence, in this case G is the direct product of (the mutually commuting) subgroups $G_1, G_2, \ldots, G_q$.

Hypothesis (1) implies $v(z, \pi[N], \varepsilon) = v(z, \pi, \varepsilon)$. If $G = G_1 \times G_2 \times \cdots \times G_q$, then we have

$$\sum_{\sigma \in G} \left(\prod_{r=1}^{q} \sigma(v(z, \pi(A_r), \varepsilon_r)) \right) \;=\; \prod_{r=1}^{q} \left(\sum_{\theta \in G_r} \theta(v(z, \pi(A_r), \varepsilon_r)) \right).$$

For $1 \le r \le q$, define

$$w_r \;:=\; \sum_{(i,j) \in \pi(A_r)} \varepsilon_r(i,j) \quad \text{and} \quad w \;:=\; \sum_{i=1}^{q} w_i.$$

Our hypothesis (i) ensures that if $m_i = m_j$ for some $i \ne j$, then $w = 0$.

Now let $t, t_1, \ldots, t_q, x_1, \ldots, x_N$ be indeterminates and let

$$\alpha : k[z_1, \ldots, z_N] \to k[t, t_1, \ldots, t_q, x_1, \ldots, x_N]$$

be the injective k-homomorphism of rings defined by

$$\alpha(z_i) \;:=\; tx_i + t_r \quad \text{if } i \in A_r \text{ with } 1 \le r \le q.$$

Then given $\sigma \in S_N$, $(i,j) \in \pi[N]$ and $1 \le r, s \le q$, we have

$$\alpha(z_{\sigma(i)} - z_{\sigma(j)}) \;=\; t(x_{\sigma(i)} - x_{\sigma(j)}) + (t_r - t_s)$$

if and only if $(\sigma(i), \sigma(j)) \in A_r \times A_s$.

Let x stand for $(x_1, \ldots, x_N)$ and T stand for $(t_1, \ldots, t_q)$. Given $f \in k[t, T, X]$, by the x-*degree* (resp. T-*degree*) of f, we mean the total degree of f in the indeterminates $x_1, \ldots, x_N$ (resp. $t_1, \ldots, t_q$). Now fix a $\sigma \in G$ and consider

$$V_\sigma(x, t, T) \;:=\; \alpha(\sigma(v(z, \pi, \varepsilon))).$$

For an ordered pair (i,j) with $1 \le i, j \le q$, set

$$A(\sigma, i, j) \;:=\; \pi \cap (A_{i(\sigma)} \times A_{j(\sigma)}).$$

It is straightforward to verify that $V_\sigma(x, 0, T)$ is

$$\prod_{1 \le r < s \le q} \left(\prod_{(i,j) \in A(\sigma,r,s)} (t_r - t_s)^{\varepsilon(i,j)} \cdot \prod_{(i,j) \in A(\sigma,s,r)} (t_s - t_r)^{\varepsilon(i,j)} \right).$$

Suppose condition (2) of the theorem holds. Then for $1 \le r < s \le q$, we have

$$\sum_{(i,j) \in A(\sigma,r,s)} \varepsilon(i,j) \;=\; \begin{cases} 0 & \text{if } s(\sigma) < r(\sigma), \\ b(m_r, m_s) & \text{if } r(\sigma) < s(\sigma). \end{cases}$$

Further, if $1 \le r < s \le q$ are such that $s(\sigma) < r(\sigma)$, then

$$m_s = m_{s(\sigma)} \le m_{r(\sigma)} = m_r \quad \text{implies } m_s = m_{s(\sigma)} = m_{r(\sigma)} = m_r$$

and so, (2) ensures that $b(m_r, m_s)$ is an even integer. Hence, if property (2) holds, then

$$V_\sigma(x, 0, T) \;:=\; \prod_{1 \le r < s \le q} (t_r - t_s)^{b(m_r, m_s)}.$$

On the other hand, if condition (3) holds, then we merely observe that there is a nonzero homogeneous $g_\sigma \in \mathbb{Q}[t_1, \ldots, t_q]$ such that $V_\sigma(x, 0, T) = g_\sigma^2$. In any case, the t-order of $V_\sigma(x, 0, T)$ is 0 (*i.e.*, $V_\sigma(x, t, T)$ is not a multiple of t) and the T-degree of $V_\sigma(x, 0, T)$ is

$$d := \sum_{(i,j)\in\pi} \varepsilon(i, j).$$

Define

$$\gamma := \sum_{\sigma\in G} \sigma(v(z, \pi, \varepsilon)) \quad \text{and} \quad V(x, t, T) := \sum_{\sigma\in G} V_\sigma(x, t, T).$$

Then $\alpha(\gamma) = V(x, t, T)$. If (2) holds, then letting $|G|$ denote the cardinality of G, we have $|G| \neq 0$ in k and

$$(\#) \qquad V(x, 0, T) = |G| \prod_{1\le r<s\le q} (t_r - t_s)^{b(m_r,m_s)}$$

and hence $V(x, 0, T) \neq 0$. On the other hand, if (3) holds, then we have

$$V(x, 0, T) = \sum_{\sigma\in G} g_\sigma^2,$$

which is necessarily nonzero in view of Lemma 2.1. Now it is clear that $\alpha(\gamma) \neq 0$, the t-order of $\alpha(\gamma)$ is 0 and the T-degree of $\alpha(\gamma)$ is d.

For $\sigma \in S_N$, define

$$F_\sigma(z) := \prod_{r=1}^{q} \sigma(v(z, \pi(A_r), \varepsilon_r)) \quad \text{and} \quad W_\sigma(x, t, T) := \prod_{r=1}^{q} \alpha(\sigma(v(z, \pi(A_r), \varepsilon_r))).$$

Then $W_\sigma(x, t, T) = \alpha(F_\sigma(z))$. If $\varepsilon_r = 0$ for all r, then $F_\sigma(z) = 1$ and hence

$$\sum_{\sigma\in G} F_\sigma(x) = |G| \neq 0.$$

If $G = G_1 \times \cdots \times G_q$, then we have

$$\sum_{\sigma\in G} F_\sigma(x) = \prod_{r=1}^{q} \left(\sum_{\theta\in G_r} \theta(v(z, \pi(A_r), \varepsilon_r)) \right).$$

Now suppose $G = G_1 \times \cdots \times G_q$. Given $\sigma \in G$, write $\sigma =: \theta_1\theta_2 \cdots \theta_q$, where $\theta_r \in G_r$ for $1 \le r \le q$. Then

$$\alpha(\sigma(v(z, \pi(A_r), \varepsilon_r))) = t^{w_r}\, \theta_r(v(x, \pi(A_r), \varepsilon_r)) = t^{w_r}\, \sigma(v(x, \pi(A_r), \varepsilon_r))$$

and hence

$$W_\sigma(x, t, T) = t^w \prod_{r=1}^{q} \sigma(v(x, \pi(A_r), \varepsilon_r)) = t^w F_\sigma(x).$$

Consequently,

$$\alpha(\sigma(v(z, \pi, \varepsilon))) \prod_{r=1}^{q} \alpha(\sigma(v(z, \pi(A_r), \varepsilon_r))) = t^w V_\sigma(x, t, T) F_\sigma(x).$$

Case I: hypothesis (ii) holds. Then as proved above $V_\sigma(x, 0, T)$ is independent of the choice of $\sigma \in G$ and $V_\sigma(x, 0, T)$ is a nonzero polynomial depending only on T. In particular, letting $\iota \in S_N$ denote the identity permutation, we have $V_\iota(x, 0, T) \neq 0$ and

$$\sum_{\sigma\in G} V_\sigma(x, 0, T) F_\sigma(x) = V_\iota(x, 0, T) \sum_{\sigma\in G} F_\sigma(x).$$

The sum appearing on the right of the above equation is obviously independent of t; moreover, hypothesis (ii) ensures that it is nonzero and thus has t-order 0. Case II: hypothesis (iii) holds. Then $V_\sigma(x, 0, T) = g_\sigma^2$ as well as $F_\sigma(x) = f_\sigma^2$, where $g_\sigma \in k[T]$ and $f_\sigma \in k[x]$ are nonzero polynomials. In this case, Lemma 2.1 ensures that

$$\sum_{\sigma\in G} V_\sigma(x, 0, T) F_\sigma(x) = \sum_{\sigma\in G} (f_\sigma g_\sigma)^2 \neq 0.$$

In either case, the sum
$$\sum_{\sigma\in G} V_\sigma(x,t,T)W_\sigma(x,t,T) \;=\; \sum_{\sigma\in G} t^w V_\sigma(x,t,T)F_\sigma(x)$$
has t-order exactly w.

Next, for $\sigma \in S_N$, let
$$R(\sigma) \;:=\; \bigcup_{1\le r\le q} \pi(B_r(\sigma)).$$
Observe that $\pi \cap R(\sigma) = \emptyset$ if and only if $\sigma \in G$. Also, observe that
$$\alpha(z_{\sigma(i)} - z_{\sigma(j)}) \;=\; t(x_{\sigma(i)} - x_{\sigma(j)}) + (t_r - t_s),$$
where $r = s$ if and only if $(i,j) \in R(\sigma)$.

Fix a $\sigma \in S_N \setminus G$. Then clearly
$$v(z,\pi,\varepsilon) \;=\; v(z,\pi[N],\varepsilon) \;=\; v(z,R(\sigma),\varepsilon)v(z,\pi[N]\setminus R(\sigma),\varepsilon).$$
Moreover, note that
$$v(z,R(\sigma),\varepsilon) \;=\; v(z,\pi\cap R(\sigma),\varepsilon) \quad \text{and} \quad v(z,\pi[N]\setminus R(\sigma),\varepsilon) \;=\; v(z,\pi\setminus R(\sigma),\varepsilon).$$
Define
$$\lambda(\sigma) \;:=\; \sum_{(i,j)\in\pi\cap R(\sigma)} \varepsilon(i,j) \quad \text{and} \quad d(\sigma) \;:=\; \sum_{(i,j)\in\pi\setminus R(\sigma)} \varepsilon(i,j).$$
Then $d(\sigma) = d - \lambda(\sigma)$. From our choice of σ and hypothesis (1), it follows that $\lambda(\sigma) \ge 1$ and hence $d(\sigma) < d$. Let
$$P_\sigma(x,t,T) \;:=\; \alpha(\sigma(v(z,\pi\cap R(\sigma),\varepsilon))), \quad Q_\sigma(x,t,T) \;:=\; \alpha(\sigma(v(z,\pi\setminus R(\sigma),\varepsilon))).$$
Observe that $V_\sigma(x,t,T) = P_\sigma(x,t,T)\cdot Q_\sigma(x,t,T)$,
$$P_\sigma(x,t,T) \;=\; t^{\lambda(\sigma)} \cdot \prod_{(i,j)\in\pi\cap R(\sigma)} (x_{\sigma(i)} - x_{\sigma(j)})^{\varepsilon(i,j)}$$
and $Q_\sigma(x,0,T)$ is a nonzero T-homogeneous polynomial of T-degree $d(\sigma)$. Hence the t-order of $V_\sigma(x,t,T)$ is exactly $\lambda(\sigma)$. For $1 \le r \le q$, let
$$\begin{aligned} P_\sigma^{(r)}(x,t,T) &:= \alpha(\sigma(v(z,\pi(A_r)\cap R(\sigma),\varepsilon_r))),\\ Q_\sigma^{(r)}(x,t,T) &:= \alpha(\sigma(v(z,\pi(A_r)\setminus R(\sigma),\varepsilon_r))). \end{aligned}$$
Now for $1 \le r \le q$, we do have
$$\sigma(v(z,\pi(A_r),\varepsilon_r)) \;=\; \sigma(v(z,\pi(A_r)\cap R(\sigma),\varepsilon_r))\cdot\sigma(v(z,\pi(A_r)\setminus R(\sigma),\varepsilon_r))$$
and hence
$$\alpha(\sigma(v(z,\pi(A_r),\varepsilon_r))) \;=\; P_\sigma^{(r)}(x,t,T)\cdot Q_\sigma^{(r)}(x,t,T).$$
Since $\pi(B_s(\sigma)) \cap \pi(B_r(\sigma) = \emptyset = \pi(A_r) \cap \pi(A_s)$ for $1 \le r < s \le q$, we have
$$\pi\cap R(\sigma) \;=\; \{(i,j)\in\pi \mid \sigma(i,j)\in\pi[N]\setminus\pi\} \;=\; \bigsqcup_{r=1}^{q} (\pi\cap\pi(B_r(\sigma)))$$
and
$$J \;:=\; \bigsqcup_{r=1}^{q} (\pi(A_r)\setminus R(\sigma)) \;=\; \{(i,j)\in\pi[N]\setminus\pi \mid \sigma(i,j)\in\pi\}.$$
Recall that σ is also viewed as a permutation of $\pi[N]$. Hence J and $\pi\cap R(\sigma)$ have the same cardinality. Partition $\pi\cap R(\sigma)$ into q subsets $I_1(\sigma),\ldots,I_q(\sigma)$ such that $|I_r(\sigma)| = |\pi(A_r)\setminus R(\sigma)|$ for $1 \le r \le q$. For $1 \le r \le q$, define
$$\lambda_r(\sigma) \;:=\; \sum_{(i,j)\in I_r(\sigma)} \varepsilon(i,j) \quad \text{and} \quad e_r(\sigma) \;:=\; \sum_{(i,j)\in\pi(A_r)\cap R(\sigma)} \varepsilon_r(i,j).$$
Then $\lambda(\sigma) = \lambda_1(\sigma) + \cdots + \lambda_q(\sigma)$, the t-order of $P_\sigma^{(r)}(x,t,T)$ is $e_r(\sigma)$ and the t-order of $Q_\sigma^{(r)}(x,t,T)$ is 0 for $1 \le r \le q$. Consequently, the t-order of $V_\sigma(x,t,T)W_\sigma(x,t,T)$ is
$$\lambda(\sigma) + \sum_{r=1}^{q} e_r(\sigma) \;=\; \sum_{r=1}^{q} e_r(\sigma) + \lambda_r(\sigma).$$

Our hypothesis (iv) guarantees that firstly $e_r(\sigma) + \lambda_r(\sigma) \geq w_r$ for $1 \leq r \leq q$ and secondly, since σ is not in G, there is at least one r with $e_r(\sigma) + \lambda_r(\sigma) \geq w_r + 1$. It follows that for each $\sigma \in S_N \setminus G$, the t-order of $V_\sigma(x,t,T)W_\sigma(x,t,T)$ is at least $w+1$.

Let $\Upsilon := Symm_N(\delta(z,M))$. Then we have

$$\Upsilon \;=\; Symm_N\left(v(z,\pi,\varepsilon)\prod_{r=1}^{q} v(z,\pi(A_r),\varepsilon_r)\right)$$

and hence

$$\alpha(\Upsilon) \;=\; \sum_{\sigma\in G} V_\sigma(x,t,T)W_\sigma(x,t,T) + \sum_{\sigma\in G\setminus S_N} V_\sigma(x,t,T)W_\sigma(x,t,T).$$

Since G is nonempty, the first sum on the right of the above equality is nonzero. From what has been shown above the first sum on the right has t-order w whereas the second sum on the right has t-order at least $w+1$. Hence $\alpha(\Upsilon)$ has t-order w. Since w is a nonnegative integer, $\alpha(\Upsilon) \neq 0$. In particular, $\Upsilon \neq 0$. □

Remark 2.3. *We continue to use the above notation.*

1. *Suppose M satisfies the hypotheses of Theorem 2.1 and λ is a positive integer such that*

$$Symm_{m_r}(\delta(z,\lambda M_{rr})) \neq 0$$

for $1 \leq r \leq q$. Then λM also satisfies the hypotheses of Theorem 2.1. In general, the polynomials $Symm_N(\delta(z,M))$ and $Symm_N(\delta(z,\lambda M))$ do not seem to be related in any obvious manner (see the last of the Example 2.1 below).

2. *Suppose for $1 \leq i \leq s$, there is a partition $m^{(i)}$ of N with respect to which $M_i \in E(N)$ satisfies the hypotheses of Theorem 2.1 and let $\Upsilon_i := Symm_N(\delta(z,M_i))$. If $\alpha(\Upsilon_1),\ldots,\alpha(\Upsilon_s)$ are k-linearly independent, then $\Upsilon_1,\ldots,\Upsilon_s$ are also k-linearly independent. Now to ensure k-linear independence of $\alpha(\Upsilon_1),\ldots,\alpha(\Upsilon_s)$, it suffices to ensure the k-linear independence of their respective t-initial forms. For simplicity, assume that property (2) is satisfied by the M_i and $M_i^* = 0$ for $1 \leq i \leq s$. Then from the equality (#) in the proof of Theorem 2.1, it follows that the t-initial coefficient,i.e., the coefficient of the lowest power of t present, of each $\alpha(\Upsilon_i)$ is of the type $c\prod_{1\leq r<s\leq q}(t_r - t_s)^{b(m_r,m_s)}$ for some $0 \neq c \in k$. The k-linear independence of such products is completely determined by the exponents $b(m_r,m_s)$.*

Example 2.1. 1. *Consider the following $E_1, E_2, E_3 \in E(6)$ presented as 2×2 block-matrices.*

$$E_i \;:=\; \begin{bmatrix} 0 & C_i \\ C_i^T & 0 \end{bmatrix},$$

where

$$C_1 \;:=\; \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 4 \end{bmatrix}, \quad C_2 \;:=\; \begin{bmatrix} 3 & 3 & 3 \\ 3 & 4 & 3 \\ 3 & 3 & 4 \end{bmatrix}, \quad C_3 \;:=\; \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 4 \\ 3 & 3 & 4 \end{bmatrix}.$$

A direct computation using MAPLE shows that

$$Symm_6(\delta(z,E_1)) \neq 0, \quad Symm_6(\delta(z,E_2)) = 0 \text{ and } Symm_6(\delta(z,E_3)) \neq 0.$$

Of course, in the case of E_1, Theorem 2.1 does apply. Since $\|C_2\| = 29 = \|C_3\|$ is an odd integer, Theorem 2.1 can not be applied in the case of E_2, E_3.

2. *For $j = 1,2$, let $E_j \in E(5,18)$ be presented in 2×2 block-format as*

$$E_j \;:=\; \begin{bmatrix} 0 & A_j \\ A_j^T & B \end{bmatrix}, \quad \text{where} \quad B \;:=\; \begin{bmatrix} 0 & 1 & 7 \\ 1 & 0 & 1 \\ 7 & 1 & 0 \end{bmatrix},$$

$$A_1 \;:=\; \begin{bmatrix} 5 & 13 & 0 \\ 5 & 3 & 10 \end{bmatrix} \quad \text{and} \quad A_2 \;:=\; \begin{bmatrix} 8 & 10 & 0 \\ 2 & 6 & 10 \end{bmatrix}.$$

Then a MAPLE computation shows that $h_j := Symm_5(\delta(z,E_j)) \neq 0$ for $j = 1,2$. Up to a nonzero integer multiple, h_1 and h_2 are the same; either one can be identified as the Hermite's invariant of a quintic binary form (see [2] or [3]). Since this invariant has weight 45, it is a skew invariant. Let $M \in E(9,90)$ be the 2×2 block-matrix $[M_{ij}]$ such that $M_{11} = 0$, M_{12} is the 4×5 matrix having each entry 18 and $M_{22} \in \{E_1, E_2\}$. Note that Theorem 2.1 is applicable and thus $g := Symm_9(\delta(z,M))$ is a nonzero invariant of a binary nonic. Also, since g has weight 405, g is a skew invariant.

3. *Let $M \in E(4,2)$ be the 2×2 block matrix $[M_{ij}]$, where $M_{11} = 2D_2 = M_{22}$ and $M_{12} = 0 = M_{21}$. Let $g := Symm_4(\delta(z,M))$ and $h := Symm_4(\delta(z,2M))$. Then $2M \in E(4,4)$ and by Lemma 2.1, $gh \neq 0$. Clearly, g and h both are invariants of a binary quartic. A computation employing MAPLE shows that g and h are algebraically independent over k.*

Lemma 2.2. *Suppose d is a positive integer such that Nd is an integer multiple of 4. Then there is an explicitly described $E \in E(N,d)$ such that each entry of E is an even integer. Moreover, if k has characteristic 0, then $g := Symm_N(\delta(z,E))$ is a nonzero invariant (of degree d) of a binary form of degree N.*

Proof. First, suppose $N = 2m$ for some positive integer m and d is an even positive integer. Let $E \in E(N)$ be the $m \times m$ block matrix $[M_{ij}]$ such that $M_{rr} := dD_2$ for $1 \leq r \leq m$ and $M_{ij} = 0$ for $1 \leq i < j \leq m$. Then clearly $E \in E(N,d)$ and since d is even, each entry of E is an even integer. Secondly, suppose N is odd and $d = 4e$ for some positive integer e. Our construction proceeds by induction on N. If $N = 3$, then let $E := (2e)D_3$. Henceforth, assume $N \geq 5$. If $N-3$ is odd, then by induction hypothesis, we have an $M \in E(N-3,d)$ such that each entry of M is an even integer. If $N-3$ is even, then by the first part of our proof we have an $M \in E(N-3,d)$ such that each entry of M is an even integer. Now let E be the 2×2 block matrix $[C_{ij}]$ with $C_{11} := (2e)D_3$, $C_{22} := M$ and $C_{12} = 0 = C_{21}$. Then clearly $E \in E(N,d)$ and each entry of E is an even integer. In either case, provided $char\, k = 0$, Lemma 2.1 ensures that $g \neq 0$. □

Theorem 2.2. *Assume that $N \geq 3$.*

(i) *Suppose m, n are positive integers such that $n \geq 2$ and $N = mn$. Let a, b be positive integers and let $d := 2a(n-1) + (m-1)(n-1)b$. Then there is an explicitly described $E \in E(N,d)$ such that $g := Symm_N(\delta(z,E))$ is a (degree d) nonzero invariant of a binary form of degree N.*

(ii) *Suppose m, n, r are positive integers such that $n \geq 2$, $1 \leq r \leq mn-1$ and $N = 2mn - r$. Given positive integers a, b such that*

$$c := \frac{2(n-1)a + (m-1)(n-1)b}{r} \quad \text{is an integer,}$$

there is an explicitly described $E \in E(N,mnc)$ yielding a (degree mnc) nonzero invariant $g := Symm_N(\delta(z,E))$ of a binary form of degree N.

(iii) *Suppose l, m, n are positive integers such that $l < m < n < l+m$ and $N = l+m+n$. Given a positive integer d such that each of*

$$a := \frac{(m+l-n)d}{2lm}, \quad b := \frac{(l+n-m)d}{2ln}, \quad c := \frac{(m+n-l)d}{2mn}$$

is an integer, there is an explicitly described $E \in E(N,d)$ yielding a (degree d) nonzero invariant $g := Symm_N(\delta(z,E))$ of a binary form of degree N.

(iv) *Suppose s is a nonnegative integer and t, u, v are positive integers such that $t \leq 2u \leq 2t-1$. Then letting*

$$N := 2(2tv+1) \quad \text{and} \quad d := (2s+1)(2u+1)(4uv+2v+1),$$

there is an explicitly described $E \in E(N,d)$ such that $g := Symm_N(\delta(z,E))$ is a nonzero invariant of a binary form of degree N. Moreover, g is a skew invariant of weight $w := (2s+1)(2tv+1)(2u+1)(4uv+2v+1)$.

(v) *Given $E \in E(N,d)$ such that each entry of E is strictly less than d and $Symm_N(\delta(z,E)) \neq 0$, a matrix $E^* \in E(2N-1,dN)$ can be so constructed that $g := Symm_N(\delta(z,E^*))$ is a nonzero invariant of a binary form of degree $2N-1$.*

Proof. To prove (i), let $E \in E(N)$ be the $n \times n$ block matrix $[M_{ij}]$, where $M_{ii} = 0$ for $1 \leq i \leq n$ and $M_{ij} = 2aI + bD_m$ for $1 \leq i < j \leq n$. It is straightforward to verify that $E \in E(N,d)$ and Theorem 2.1 can be applied to deduce $g \neq 0$.

To prove (ii), first note that $mn - r \geq 1$. Let $E \in E(N)$ be the $(n+1) \times (n+1)$ block matrix $[M_{ij}]$ defined as follows. For $1 \leq i \leq n+1$, $M_{ii} = 0$. If $mn - r \leq m$, then for $1 \leq i < j \leq n+1$, M_{1j} is the $(mn-r) \times m$ matrix having each entry equal to c and $M_{ij} = 2aI + bD_m$. If $m < mn - r$, then for $1 \leq i < j \leq n+1$, $M_{ij} = 2aI + bD_m$ and $M_{i(n+1)}$ is the $m \times (mn-r)$ matrix having each entry equal to c. Then clearly $E \in E(N,d)$. If $mn - r = m$, then $m(mn-r)c = 2ma + m(m-1)b$ is necessarily an even integer. Now it is straightforward to verify that Theorem 2.1 can be employed to infer $g \neq 0$.

To prove (iii), let $E \in E(N)$ be the 3×3 block matrix $[M_{ij}]$ such that $M_{rr} = 0$ for $1 \leq r \leq 3$, $M_{12} = M_{21}^T$ is the $l \times m$ matrix having each entry equal to a, $M_{13} = M_{31}^T$ is the $l \times n$ matrix having each entry equal to b and $M_{23} = M_{32}^T$ is the $m \times n$ matrix having each entry equal to c. By hypothesis, each of a, b, c is a positive integer. Since $d = ma + nb = la + nc = lb + mc$, we have $E \in E(N, d)$. As before, it is easily verified that Theorem 2.1 is indeed applicable in this case and hence $g \neq 0$.

To prove (iv), let $m := 1$, $n := 4uv + 2v + 1$ and $r := 8uv - 4tv + 4v$. Clearly, $n \geq 7$ and $N = 2mn - r$. Since $t \leq 2u \leq 2t - 1$, we have $1 \leq r \leq n - 1$. Define $a := (2s + 1)(2u - t + 1)$ and say $b := 1$. Then letting $c := (2s+1)(2u+1)$, we have $c \geq 3$ and $cr = (n-1)[2a+(m-1)b]$. Observe that the positive integers a, b, c, m, n, r satisfy all the requirements of (ii). Thus, by taking $E \in E(N, d)$ as described in the proof of (ii), we infer that $g \neq 0$. If w denotes the weight of g, then $2w = Nd$ and hence $w = (2s + 1)(2tv + 1)(2u + 1)(4uv + 2v + 1)$. Since w is an odd integer, g is a skew invariant.

Lastly, to prove (v), suppose $E \in E(N, d)$ is such that each entry of E is strictly less than d and $Symm_N(\delta(z, E)) \neq 0$. Let E^* be the 2×2 block matrix $[C_{ij}]$, where $C_{11} := 0$, $C_{22} := E$ and $C_{12} = C_{21}^T$ is the $(N - 1) \times N$ matrix with each entry equal to d. Clearly, $E^* \in E(2N - 1, dN)$ and Theorem 2.1 can be applied to infer $g \neq 0$. □

Example 2.2. *We continue assuming $N \geq 3$.*

1. $N = 4e$. *Using (i) of Theorem 2.2 with $n := 2$ and $m := 2e$, we obtain nonzero invariants of degree d for $d = 2e + 1$ and all $d \geq N - 1$. If $char\, k = 0$ and $d \leq N - 2$ is even, then Lemma 2.2 yields a nonzero invariant of degree d.*

2. *With the notation of (iii), let $Y := \{1 \leq d \in \mathbb{Z} \mid a, b, c \in \mathbb{Z}\}$ and*

$$y := \frac{2lmn}{gcd(N - 2l, N - 2m, N - 2n, 2lmn)}.$$

Then it is straightforward to verify that $d \in Y$ if and only if $d = sy$ for some positive integer s. Of course, $2lmn \in Y$; but y can be strictly less than $2lmn$ (e.g., consider $(l, m, n) := (2, 5, 6)$ or $(l, m, n) := (9, 15, 21)$). If $l + m + n$ is odd and $d = 2 \bmod 4$, then the resulting g is a nonzero skew invariant. So, (iii) produces skew invariants for binary forms of odd degrees (in contrast to (iv)). The least value of N for which (iii) may be used to obtain skew invariants is $N = 3 + 5 + 7 = 15$; whereas for the ones that can be obtained by using (iv), it is $N = 2(2 \cdot 2 \cdot 1 + 1) = 10$. For 3-part partitions $N = l + m + n$ with $l \leq m \leq n < l + m$, by imposing additional requirements such as: $(l + m - n)d$ is divisible by 4 if $l = m$ and so on, hypotheses of Theorem 2.1 can be satisfied. Assertion (iii) can be generalized for certain types of partitions of N into 4 or more parts; the task of formulating such generalizations is left to the reader.

3. *Let $E \in \{E_1, E_2\} \subset E(5, 18)$, where E_1, E_2 are as in the second example above Theorem 2.2. For $2 \leq n \in \mathbb{Z}$, let d_n, $M_n \in E(2^n + 1, d_n)$ be inductively defined by setting $d_2 := 18$, $M_2 := E$, $d_{n+1} := (2^n + 1)d_n$ and where $M_{n+1} := M_n^*$, is derived from M_n as in (iv) of Theorem 2.2. Then by (v) of Theorem 2.2, $g_n := Symm_{2^n+1}(\delta(z, M_n))$ is a nonzero skew invariant of a binary form of degree $2^n + 1$ for $2 \leq n \in \mathbb{Z}$.*

Remark 2.4. *Theorem 2.2 exhibits the simplest applications of Theorem 2.1. At present, there does not exist a characterization of pairs (N, d) for which Theorem 2.1 can be used to obtain a nonzero invariant. Interestingly, it is impossible to use Theorem 2.1 to construct invariants corresponding to certain pairs (N, d), e.g, consider $(N, d) = (5, 18)$: an elementary computation verifies that Hermite's invariant of a binary quintic can not be constructed via Theorem 2.1. A 'good' generalization of Theorem 2.1, if it exists, should repair this failing.*

3. Enumeration of a class of Semi-invariants

In what follows, we use the results of the previous section to build a family of linearly independent semi-invariants of certain weights and degrees. Our construction allows explicit enumeration of these semi-invariants.

Definition 3.1. *Let n, s be a positive integers.*

1. *Let $\preceq$ denote the lexicographic order on $\mathbb{Z}^{s+1}$.*

2. *For $\alpha := (a_1, \ldots, a_{s+1}) \in \mathbb{Z}^{s+1}$, let $|\alpha| := \sum_{i=1}^{s+1} a_i$ and*

$$wt(n, \alpha) := \frac{1}{2}\left[n^2 - \left(\sum_{i=1}^{s+1} a_i^2\right)\right].$$

3. *Define $\wp(s, n) := (\wp_1(s, n), \ldots, \wp_{s+1}(s, n)) \in \mathbb{Z}^{s+1}$, where*

$$\wp_j(s, n) := \left\lfloor \frac{n - \sum_{1 \leq i \leq j-1} \wp_i}{s + 2 - j} - \frac{(s + 1 - j)}{2} \right\rfloor \qquad \text{for } 1 \leq j \leq s + 1.$$

4. *Let* $\varpi(s,n) := wt(n,\wp(s,n))$.

5. *By* $\Im(s,n)$ *we denote the set of all* $\alpha := (a_1,\dots,a_{s+1}) \in \mathbb{Z}^{s+1}$ *such that* $a_1 < a_2 < \cdots < a_{s+1}$ *and* $|\alpha| = n$. *Let* $\mathbb{P}(s,n)$ *be the subset of* $\Im(s,n)$ *consisting of* $(a_1,\dots,a_{s+1}) \in \Im(s,n)$ *with* $a_1 \geq 1$.

6. *For* $(i,j) \in \mathbb{Z}^2$ *with* $1 \leq i < j \leq s+1$, *let* $\eta(i,j) := (\eta_1,\dots,\eta_{s+1})$ *where* $\eta_r = 0$ *if* $r \neq i,j$, $\eta_i = 1$ *and* $\eta_j = -1$. *An* $(s+1)$*-tuple* β *is said to be an elementary modification of* $\alpha \in \mathbb{Z}^{s+1}$ *provided* $\beta = \alpha + \eta(i,j)$ *for some* $1 \leq i < j \leq s+1$. *An* $(s+1)$*-tuple* β *is said to be a modification of* $\alpha \in \mathbb{Z}^{s+1}$ *if there is a finite sequence* $\alpha = \alpha_1,\dots,\alpha_r = \beta$ *such that* α_i *is an elementary modification of* α_{i-1} *for* $2 \leq i \leq r$.

Lemma 3.1. *Fix positive integers* n, s *and let* e *be the integer such that*

$$n - \frac{s(s+1)}{2} \;=\; \left\lfloor \frac{n}{s+1} - \frac{s}{2} \right\rfloor (s+1) + e.$$

Let $\wp(s,n) = (p_1,\dots,p_{s+1})$. *Then, the following holds.*

(i) *We have*

$$p_j \;=\; \begin{cases} p_1 + j - 1 & \text{if } 1 \leq j \leq s+1-e, \text{ and} \\ p_1 + j & \text{if } s+2-e \leq j \leq s+1. \end{cases}$$

In particular, $\wp(s,n) \in \Im(s,n)$. *Moreover, if* $(s+1)(s+2) \leq 2n$, *then* $\wp(s,n) \in \mathbb{P}(s,n)$.

(ii) *We have*

$$\begin{aligned} \varpi(s,n) \;=\; & \frac{(s+1)(s+2)}{2}\left\lfloor \frac{n}{s+1} - \frac{s}{2} \right\rfloor^2 \\ & + \frac{(s+1)^2(s+2) - 2n(s+2)}{2}\left\lfloor \frac{n}{s+1} - \frac{s}{2} \right\rfloor \\ & + \frac{3(s+1)^4 + 2(s+1)^3 - 3(1+4n)(s+1)^2 - 2(1+6n)(s+1) + 24n^2}{24}. \end{aligned}$$

(iii) *Let* $\alpha := (a_1,\dots,a_{s+1}) \in \Im(s,n)$. *Then,* $\alpha \preceq \wp(s,n)$, $\wp(s,n)$ *is a modification of* α *and*

$$\sum_{1 \leq i < j \leq s+1} a_i a_j \;=\; wt(n,\alpha) \;\leq\; \varpi(s,n).$$

(iv) $\mathbb{P}(s,n) \neq \emptyset$ *if and only if*

$$s \;\leq\; \left\lfloor \frac{\sqrt{8n+1} - 1}{2} \right\rfloor - 1.$$

(v) *Suppose* $s \geq 2$, $(s+1)(s+2) \leq 2n$ *and* $p_1 + e = bs + d$ *where* b, d *are nonnegative integers with* $d \leq s-1$. *Then, letting* $\wp(s-1,n) := (q_1,\dots,q_s)$, *we have* $q_1 = p_1 + b + 1$ *and*

$$\varpi(s,n) - \varpi(s-1,n) \;=\; p_1(s+1-e) + bd(s+1) + \frac{1}{2}b(b-1)s(s+1).$$

In particular, $q_1 > p_1$ *and* $\varpi(s,n) - \varpi(s-1,n) \geq 2p_1$. *If* $p_1 = 1$, *then* $2 \leq q_1 \leq 3$ *and* $2 \leq \varpi(s,n) - \varpi(s-1,n) \leq s+2$.

(vi) *Suppose* $s \geq 2$, $(s+1)(s+2) \leq 2n$ *and let* $v(s,n) := (v_1,\dots,v_s)$ *where* $v_i := i$ *for* $1 \leq i \leq s$ *and* $v_s = n - (1/2)s(s+1)$. *Then,* $v(s,n) \preceq \alpha$ *and* $wt(n,v(s,n)) \leq wt(n,\alpha)$ *for* $\alpha \in \mathbb{P}(s,n)$.

Proof. Note that $0 \leq e \leq s$ and hence $s+1-e \geq 1$. Suppose $1 \leq j \leq s+1-e$ is such that $p_i = p_1 + i - 1$ for $1 \leq i \leq j$. Then,

$$\begin{aligned} p_{j+1} \;&=\; \left\lfloor p_1 - \frac{j(j-1) - s(s+1) - 2e + (s-j)(s+1-j)}{2(s+1-j)} \right\rfloor \\ &=\; \left\lfloor p_1 + j + \frac{e}{s+1-j} \right\rfloor. \end{aligned}$$

If $j < s+1-e$, then $e < s+1-j$ and hence $p_{j+1} = p_1 + j$. If $j = s+1-e$, then $p_{j+1} = p_1 + j + 1$. Next suppose (i) holds for some j with $s+2-e \leq j \leq s$. Then,

$$p_{j+1} \;=\; \left\lfloor p_1 - \frac{j(j-1) - s(s+1) + 2(j+e-s-1) - 2e + (s-j)(s+1-j)}{2(s+1-j)} \right\rfloor$$

$$= \quad p_1 + j + 1.$$

Clearly, $p_1 < p_2 < \cdots < p_{s+1}$ and if $(s+1)(s+2) \leq 2n$, then $p_1 \geq 1$. Also, $|\wp(s,n)| = p_1(s+1)+[s(s+1)/2]+e = n$. Thus (i) holds.

Let $u(X), v(X) \in \mathbb{Z}[X]$ be defined by

$$v(X) \; = \; \prod_{j=0}^{s+1}(X + p_1 + j) \; = \; (X + p_1 + s + 1 - e)u(X).$$

Then, $\varpi(s,n)$ is the coefficient of X^{s-1} in $u(X)$. The coefficient of X^s in $v(X - p_1)$ is

$$\frac{1}{2}\left(\sum_{i=0}^{s+1} i\right)^2 - \frac{1}{2}\sum_{i=0}^{s+1} i^2 \; = \; \frac{(3s+5)(s+2)(s+1)s}{24}.$$

Now a straightforward computation verifies (ii).

Obviously, $wt(n,\alpha) < n^2$ for all $\alpha \in \Im(s,n)$. If $\beta \in \Im(s,n)$ is an elementary modification of $\alpha = (a_1,\ldots,a_{s+1}) \in \Im(s,n)$, then note that $wt(n,\beta) > wt(n,\alpha)$. Hence α has a modification $v \in \Im(s,n)$ that is 'final' in the sense that no member of $\Im(s,n)$ is an elementary modification of v. Fix such $v := (v_1,\ldots,v_{s+1})$. If $1 \leq i \leq s+1$ is such that $v_{i+1} > v_i + 2$, then $v + \eta(i,i+1) \in \Im(s,n)$; this contradicts our assumption about v. So, $v_i + 1 \leq v_{i+1} \leq v_i + 2$ for all $1 \leq i \leq s$. If there are $1 \leq i < j \leq s+1$ such that $v_{i+1} = v_i + 2$ as well as $v_{j+1} = v_j + 2$, then $v + \eta(i,j) \in \Im(s,n)$; an impossibility. Hence $a_{i+1} = a_i + 2$ for at most one i with $1 \leq i \leq s$. Consequently, $n = |v| = (s+1)v_1 + (s+1-j) + [s(s+1)/2]$ for some j with $1 \leq j \leq s+1$. Clearly, $j = s+1-e$ and in view of (ii), we have $v = \wp(s,n)$. Thus $\wp(s,n)$ is a modification of α. In particular, $wt(n,\alpha) \leq \varpi(s,n)$ and $\alpha \preceq \wp(s,n)$. The equality displayed on the left in (iii) readily follows from the definition of $wt(n,\alpha)$. Thus (iii) holds.

Assertion (iv) is simple to verify. To prove (v), assume $s \geq 2$ and let $p_1 + e = bs + d$ where b, d are nonnegative integers with $d \leq s-1$. Consequently, $q_1 = p_1 + b + 1 > p_1$. Using (ii) $\varpi(s,n) - \varpi(s-1,n)$ can be computed in a straightforward manner. If $e \leq s-1$, then $\varpi(s,n) - \varpi(s-1,n)$ is clearly $\geq 2p_1$. If $e = s$, then we have $b \geq 1$ and since $(b-1)s = p_1 - d$,

$$\varpi(s,n) - \varpi(s-1,n) \; \geq \; p_1\left(1 + \frac{1}{2}b(s+1)\right) \; \geq \; 2p_1.$$

If $p_1 = 1$, then since $0 \leq e \leq s$ and $s \geq 2$, we have $0 \leq b \leq 1$. If $e \leq s-2$, then $b = 0$ and hence $q_1 = 2$, $\varpi(s,n) - \varpi(s-1,n) = s+1-e \leq s+1$. If $e = s-1$, then $b = 1$, $d = 0$ and hence $q_1 = 3$, $\varpi(s,n) - \varpi(s-1,n) = 2$. Lastly, if $e = s$, then $b = 1 = d$ and hence $q_1 = 3$, $\varpi(s,n) - \varpi(s-1,n) = s+2$. This establishes (v). The proof of (vi) is left to the reader. ☐

Lemma 3.2. *Let $m, n, t \in \mathbb{Z}$ and $(b_1,\ldots,b_m) \in \mathbb{Z}^m$ be such that $m \geq 1$, $n \geq 1$, $b_1 + \cdots + b_m = t$ and $b_i \geq 0$ for $1 \leq i \leq m$. Let $t = qn + r$, where q, r are integers with $q \geq 0$ and $0 \leq r < n$. Then, there exists an $m \times n$ matrix $A := [a_{ij}]$ satisfying the following.*

(i) *$0 \leq a_{ij} \in \mathbb{Z}$ for $1 \leq i \leq m$, $1 \leq j \leq n$ and $\|A\| = t$.*

(ii)

$$c_j(A) \; := \; r_j\left(A^T\right) \; = \; \begin{cases} q+1 & \text{if } 1 \leq j \leq r \text{ and} \\ q & \text{if } r+1 \leq j \leq n. \end{cases}$$

(iii) *$r_i(A) = b_i$ for $1 \leq i \leq m$.*

Proof. Let $t = qn + r$, where q, r are integers with $q \geq 0$ and $0 \leq r < n$. Our proof proceeds by induction on m. If $m = 1$, then let $a_{1j} := q+1$ if $1 \leq j \leq r$ and $a_{1j} := q$ if $r+1 \leq j \leq n$. Henceforth suppose $m \geq 2$ and $b_m = \ell n + \rho$ where ℓ, ρ are integers with $\ell \geq 0$ and $0 \leq \rho < n$.
Case 1: $\rho \leq r$. By our induction hypothesis there is an $(m-1) \times n$ matrix $[a_{ij}]$ such that $0 \leq a_{ij} \in \mathbb{Z}$ for $1 \leq i \leq m-1$ and $1 \leq j \leq n$, $\|A\| = t - b_m$, $a_{1j} + \cdots + a_{(m-1)j} = q - \ell + 1$ for $1 \leq j \leq r - \rho$, $a_{1j} + \cdots + a_{(m-1)j} = q - \ell$ for $r - \rho + 1 \leq j \leq n$ and $a_{i1} + \cdots + a_{in} = b_i$ for $1 \leq i \leq m-1$. Define $a_{mj} := \ell$ for $1 \leq j \leq r - \rho$, $a_{mj} := \ell + 1$ for $r - \rho + 1 \leq j \leq r$ and $a_{mj} := \ell$ for $r+1 \leq j \leq n$. Then, the resulting $m \times n$ matrix $[a_{ij}]$ is clearly the desired matrix A.
Case 2: $\rho > r$. At the outset observe that $r < n + r - \rho < n$. As before, our induction hypothesis ensures the existence of an $(m-1) \times n$ matrix $[a_{ij}]$ such that $0 \leq a_{ij} \in \mathbb{Z}$ for $1 \leq i \leq m-1$ and $1 \leq j \leq n$, $\|A\| = t - b_m$, $a_{1j} + \cdots + a_{(m-1)j} = q - \ell$ for $1 \leq j \leq n + r - \rho$, $a_{1j} + \cdots + a_{(m-1)j} = q - \ell - 1$ for $n + r - \rho + 1 \leq j \leq n$ and $a_{i1} + \cdots + a_{in} = b_i$ for $1 \leq i \leq m-1$. Define $a_{mj} := \ell + 1$ for $1 \leq j \leq r$, $a_{mj} := \ell$ for $r+1 \leq j \leq n + r - \rho$ and $a_{mj} := \ell + 1$ for $n + r - \rho + 1 \leq j \leq n$. Then, the resulting $m \times n$ matrix $[a_{ij}]$ is the desired matrix A. ☐

Definition 3.2. *Let n and w be positive integers.*

1. *Define*

$$\beta(n) \;:=\; \left\lfloor \frac{\sqrt{8n+1}-1}{2} \right\rfloor.$$

2. *For an integer s with $1 \leq s \leq \beta(n)-1$ and an $\mathfrak{a} := (m_1, \ldots, m_{s+1}) \in \mathbb{P}(s,n)$, define*

$$\nu(w,\mathfrak{a}) \;:=\; \binom{s-1+w-wt(n,\mathfrak{a})}{s-1}$$

and

$$d(w,\mathfrak{a}) \;:=\; \begin{cases} n-1+w-wt(n,\mathfrak{a}) & \text{if } m_1 = 1, \\ n-1+w-wt(n,\mathfrak{a}) & \text{if } w = 1+wt(n,\mathfrak{a}), \\ n-m_1+1+\left\lceil \frac{w-wt(n,\mathfrak{a})}{m_1} \right\rceil & \text{otherwise.} \end{cases}$$

3. *Let $\nu(w,s,n) := \nu(w,\wp(s,n))$ and $d(w,s,n) := d(w,\wp(s,n))$.*

Theorem 3.1. *Assume that N is an integer ≥ 3 and k is a field of characteristic either 0 or strictly greater than N. Let F be the generic binary form of degree N (as in the introduction). Let s be an integer with $1 \leq s \leq \beta(N)-1$ and let $\mathfrak{a} := (m_1, \ldots, m_{s+1}) \in \mathbb{P}(s,N)$. Let $m := m_1$ and let w be an integer such that $\theta := w - wt(N,\mathfrak{a}) \geq 1$. Then, for a positive integer $d \geq d(w,\mathfrak{a})$, there exist $\nu(w,\mathfrak{a})$ k-linearly independent semi-invariants of F of weight w and degree d.*

Proof. Fix an ordered s-tuple $(\theta_1, \ldots, \theta_s)$ of nonnegative integers with

$$\theta_1 + \cdots + \theta_s \;=\; \theta.$$

Since $\theta \geq 1$, using Lemma 3.2 we obtain an $s \times m$ matrix $B^* := [b^*_{ij}]$ having nonnegative integer entries such that $r_i(B^*) = \theta_i$ for $1 \leq i \leq s$ and

$$\lfloor \theta/m \rfloor \;\leq\; c_m(B^*) \;\leq\; \cdots \;\leq\; c_1(B^*) \;=\; \lceil \theta/m \rceil.$$

Let u be the greatest positive integer such that $c_u(B^*) \geq 1$ and let v be the least positive integer with $b^*_{vu} \geq 1$. Define an $s \times m$ matrix $B := [b_{ij}]$ as follows. If $u = 1$ (in particular, if $m = 1$), let $B = B^*$. If $u \geq 2$, then let $b_{ij} := b^*_{ij}$ for $(i,j) \neq (v,1), (v,u)$, let $b_{vu} := b^*_{vu} - 1$ and let $b_{v1} := b^*_{v1} + 1$. Then, B has nonnegative integer entries, $r_i(B) = \theta_i$ for $1 \leq i \leq s$,

$$\begin{aligned} c_1(B) \;&=\; \min\{1 + \lceil \theta/m \rceil, \theta\}, \quad \text{and} \\ \lfloor \theta/m \rfloor - 1 \;\leq\; c_j(B) \;&\leq\; \lceil \theta/m \rceil, \quad \text{for } 2 \leq j \leq m. \end{aligned}$$

Using Lemma 3.2 again, we obtain matrices $A_1, \ldots, A_s$ with nonnegative integer entries such that

(1) A_l has size $m \times m_{l+1}$ for $1 \leq l \leq s$,
(2) $r_i(A_l) = b_{li}$ for $1 \leq l \leq s$, $1 \leq i \leq m$ and
(3) $\lfloor \theta_l/m \rfloor \leq c_j(A_l) \leq c_{j-1}(A_l) \leq \lceil \theta_l/m \rceil$ for $2 \leq j \leq m_{l+1}$.

Clearly, $\|A_l\| = \theta_l$ for $1 \leq l \leq s$. Furthermore, we have

(4) $r_1(A_1) + \cdots + r_1(A_s) = \min\{1 + \lceil \theta/m \rceil, \theta\}$, and
(5) $r_i(A_1) + \cdots + r_i(A_s) \leq \lceil \theta/m \rceil$ for $2 \leq i \leq m$.

Let $\mathbb{I}$ denote a matrix (of any chosen size) having each entry 1. Let $M := [M_{ij}]$ be an $(s+1) \times (s+1)$ block-matrix such that M_{ji} is the transpose of M_{ij} for $1 \leq i \leq j \leq s+1$, and the block M_{ij} is a $m_i \times m_j$ matrix defined by

$$M_{ij} \;:=\; \begin{cases} 0 & i = j, \\ \mathbb{I} + A_{j-1} & \text{if } i = 1 < j \leq s+1, \\ \mathbb{I} & \text{if } 2 \leq i < j \leq s+1. \end{cases}$$

Let M' denote the $(N-1) \times (N-1)$ matrix obtained from M by deleting the first row as well as the first column of M. Then, $M \in E(N)$ and $M' \in E(N-1)$. Also, in view of properties (1) - (5), it is straightforward to verify that

$$r_1(M) \;=\; d(w,\mathfrak{a}) \;>\; r_i(M) \quad \text{for } 2 \leq i \leq N,$$

and each of M, M' satisfies requirements (1), (2), (i) - (iv) of Theorem 2.1. Hence letting $\phi(\theta_1,\ldots,\theta_s) := Symm_N\,(\delta(z,M))$, we have $\phi(\theta_1,\ldots,\theta_s) \neq 0$ as well as $Symm_{N-1}\,(\delta(z,M')) \neq 0$. Observe that the coefficient of $z_1^{d(w,\alpha)}$ in $\phi(\theta_1,\ldots,\theta_s)$ is the symmetrization of $\delta(z',M')$ where $z' := (z_2,\ldots,z_N)$. Since $Symm_{N-1}$ $(\delta(z,M')) \neq 0$, we conclude that the z_1-degree (and hence also each z_i-degree) of $\phi(\theta_1,\ldots,\theta_s)$ is exactly $d(w,\mathfrak{a})$. Let α be the k-monomorphism employed in Theorem 2.1. Then, as noted in no. 2 of Remark 2.3, the t-initial coefficient of $\alpha\,(\phi(\theta_1,\ldots,\theta_s))$ is a nonzero constant (*i.e.*, element of k) multiple of

$$\eta(\theta_1,\ldots,\theta_s) \;:=\; \prod_{1\le j\le s}(t_1-t_{j+1})^{\theta_j}\prod_{1\le i<j\le s+1}(t_i-t_j)^{m_im_j}.$$

The set of all $\eta(\theta_1,\ldots,\theta_s)$ ranging over the allowed choices of s-tuples $(\theta_1,\ldots,\theta_s)$, is clearly a k-linearly independent subset of $k[t_1,\ldots,t_{s+1}]$. Hence the corresponding set $S(\theta)$ of $\phi(\theta_1,\ldots,\theta_s)$ is also a k-linearly independent subset of $k[z_1,\ldots,z_N]$. Of course $S(\theta)\subset k[y_1,\ldots,y_{N-1}]\subset k[e_1,\ldots,e_N]$ (where $y_1,\ldots,y_{N-1}$ and $e_1,\ldots,e_N$ are as in the introduction). Given $\phi\in S(\theta)$, we homogenize ϕ to get a homogeneous polynomial of degree $d(w,\mathfrak{a})$ in $a_0,\ldots,a_N$ as in the introduction. In this manner we obtain a k-linearly independent set $\mathbb{S}(\theta)$ of semi-invariants of F of degree $d(w,\mathfrak{a})$ and weight w. Obviously, $|\mathbb{S}(\theta)| = |S(\theta)| = \nu(w,\mathfrak{a})$. Letting $v := d-d(w,\mathfrak{a})$, it follows that the set $\{a_0^v\sigma \mid \sigma\in\mathbb{S}(\theta)\}$ is also k-linearly independent. □

Example 3.1. *Here we consider the case of $3\le N\le 7$. It is essential to point out that the lower bounds proved in [4], [12], [19] assume $N\ge 8$. To the best of our knowledge, there is nothing in the existing literature with which we can compare the bounds in examples below.*

1. *If $N=3$, then $s=1$ and $\varpi(1,3)=2$. In this case, Theorem 3.1 implies that for $0\le n\in\mathbb{Z}$, there exists a nonzero semi-invariant (of a binary cubic form F) of weight $2+n$ and degree at least $2+n$.*

2. *If $N=4$, then $s=1$ and $\varpi(1,4)=3$. In this case, Theorem 3.1 implies that for $0\le n\in\mathbb{Z}$, there exists a nonzero semi-invariant (of a binary quartic form F) of weight $3+n$ and degree at least $3+n$.*

3. *If $N=5$, then $s=1$ and $\varpi(1,5)=6$. In this case, Theorem 3.1 implies that for $0\le n\in\mathbb{Z}$, there exists a nonzero semi-invariant (of a binary quintic form F) of weight $6+n$ and degree at least $4+\lceil n/2\rceil$. Note that for the partition $1<4$, we can use Theorem 2.1 to verify the existence of a nonzero semi-invariant of weight $4+n$ and degree at least $4+n$. So, we obtain two k-linearly independent semi-invariants of weight $6+n$ and degree at least $6+n$.*

4. *Assume $N=6$. Then $1\le s\le 2$, $\varpi(1,6)=8$ and $\varpi(2,6)=11$. Taking $s=1$ in Theorem 3.1, we infer the existence of a nonzero semi-invariant (of a binary sextic form F) of weight $8+n$ and degree at least $8+n$ for all $0\le n\in\mathbb{Z}$. Next, taking $s=2$, Theorem 3.1 ensures the existence of $5+n$ k-linearly independent semi-invariants of weight $16+n$ and degree at least $10+n$ for all $0\le n\in\mathbb{Z}$.*

5. *Assume $N=7$. Then $1\le s\le 2$, $\varpi(1,7)=12$ and $\varpi(2,7)=14$. Letting $s=1$ in Theorem 3.1, we obtain a nonzero semi-invariant (of a binary heptic form F) of weight $12+n$ and degree at least $5+\lceil n/3\rceil$ for $0\le n\in\mathbb{Z}$. Using Theorem 2.1 for the partition $2<5$, we infer the existence of a nonzero semi-invariant of weight $10+n$ and degree at least $6+\lceil n/2\rceil$ for all $0\le n\in\mathbb{Z}$. Letting $s=2$ in Theorem 3.1, we deduce the existence of $5+n$ k-linearly independent semi-invariants of weight $18+n$ and degree at least $5+\lceil (n+4)/3\rceil$ for all $0\le n\in\mathbb{Z}$.*

Remark 3.1. *Let N, w and d are positive integers. Let*

$$PP(N,w,d) \;:=\; \left\lceil \frac{4}{1000}\cdot(\min\{2w,\,d^2,\,N^2\})^{\frac{-9}{4}}\cdot 2^{\sqrt{\min\{2w,\,d^2,\,N^2\}}}\right\rceil.$$

If $\min\{N,d\}\ge 8$ and $w\le Nd/2$, then by Theorem 1.2 of [12], there are at least $PP(N,w,d)$ k-linearly independent semi-invariants (of a binary N-ic form F) of degree d and weight w. Observe that for (w,d) with $w\ge N^2/2$ and $d\ge N$, the bound $PP(N,w,d)$ is independent of (w,d) (i.e., depends only on N). In contrast, the lower bound $\nu(w,\mathfrak{a})$ is a polynomial of degree $s-1$ in w. The reader may wish to make similar comparison with results of [4].

Example 3.2. *Let $\nu(w,N) := \nu(w,\beta(N)-1,N)$. Consider the case of $N=15$. Note that $\beta(N)=5$ and $\mathbb{P}(4,15)=\{\wp(4,15)\}$. We have $\varpi(4,15)=85$ and $\wp_1(4,15)=1$. Let $\nu(w):=\nu(w,4,15)$. Then, Theorem 3.1 ensures that for $0\le n\in\mathbb{Z}$, we have at least $\nu(85+n)$ k-linearly independent semi-invariants of weight $85+n$ and degree $d\ge 14+n$. Observe that $2(85+n)<(14+n)^2$ for $n\ge 0$, $N^2=225<2(85+n)$ for $n\ge 28$ and*

$$\nu(85+n) \;=\; \binom{3+n}{3} \;=\; \frac{1}{6}n^3+n^2+\frac{11}{6}n+1 \quad \textit{for } n\ge 0.$$

A straightforward computation verifies that $PP(15, 85+n, d) = 1 < \nu(85+n)$ *for all* $n \geq 0$ *and* $d \geq 14+n$. *Let* $semdim(w, d, N)$ *denote the dimension of the* k*-vector space of semi-invariants (of our* N*-ic form* F*) of weight* w *and degree* d. *Assume* k *has characteristic* 0. *Then, in the notation of the introduction,* $semdim(w, d, N)$ *is*

$$p_w(N, d) - p_{w-1}(N, d) \;:=\; \text{the coefficient of } q^w \text{ in } (1-q)\binom{N+d}{d}_q.$$

The table below presents a MAPLE computation of $\nu(85+n)$ *and* $semdim(85+n, 14+n, 15)$ *(denoted by semdim) for a small sample of values of* w.

w	$\nu(w)$	*semdim*
95	286	1020697
105	1771	4232793
115	5456	11374824

w	$\nu(w)$	*semdim*
125	12341	25995316
135	23426	54621331
145	39711	108639772

Let $s = 3$ *and* $\mathfrak{a} := v(3, 15) = (1, 2, 3, 9)$. *Then, for integers* $n \geq 0$, *we have* $\nu(65+n, \mathfrak{a}) = (1/2)(n+2)(n+1)$ *and* $d(65+n, \mathfrak{a}) = 14+n$. *At the other extreme, if* $\mathfrak{a} = \wp(3, 15)$, *then* $\varpi(3, 15) = 80$ *and* $\wp_1(3, 15) = 2$. *So,* $\nu(80+n, 3, 15) = (1/2)(n+2)(n+1)$ *and* $d(80+n, 3, 15) = 14 + \lceil n/2 \rceil$ *for all* $n \geq 0$. *Thus for weights* $65 \leq w < 80$, *our lower bound is for degrees* $\geq w-1$; *whereas, for weights* $w \geq 80$ *our lower bound is for degrees* $\geq 14 + \lceil (w-80)/2 \rceil$. *If* $s = 2$, *then* $\varpi(2, 15) = 74$ *and* $\wp_1(2, 15) = 4$. *Hence* $\nu(74+n, 2, 15) = n+1$ *and* $d(74+n, 2, 15) = 12 + \lceil n/4 \rceil$ *for all* $n \geq 0$. *For* $s = 1$, *we have* $\varpi(1, 15) = 56$ *and* $\wp_1(1, 15) = 7$. *Consequently,* $\nu(56+n, 1, 15) = 1$ *and* $d(56+n, 1, 15) = 9 + \lceil n/7 \rceil$.

References

[1] S. S. Abhyankar, *Enumerative combinatorics of Young tableaux*, Monographs and Textbooks in Pure and Applied Mathematics 115. Marcel Dekker, Inc., New York, 1988.

[2] A. T. Benjamin, J. J. Quinn, J. J. Quinn and A. Wójs, *Composite fermions and integer partitions*, J. Combin. Theory Ser. A 95:2 (2001), 390–397.

[3] J. P. Brennan, *Invariant theory in characteristic p: Hazlett's symbolic method for binary quantics*, Factorization in integral domains (Iowa City, IA, 1996), 257–269, Lecture Notes in Pure and Appl. Math. 189, Dekker, New York, 1997.

[4] V. Dhand, *A combinatorial proof of strict unimodality for q-binomial coefficients*, Discrete Math. 335 (2014), 20–24.

[5] M. Dunajski and R. Penrose *On the quadratic invariant of binary sextics*, Math. Proc. Cambridge Philos. Soc. 162:3 (2017), 435–445.

[6] E. B. Elliot, *An Introduction to the Algebra of Quantics*, Chelsea Publishing Company, New York, 1964, Second edition, reprint, 1913.

[7] J. H. Grace and A. Young, *The Algebra of Invariants*, Chelsea Publishing Company, New York, 1964, reprint, 1903.

[8] J. P. S. Kung and G.-C. Rota, *The invariant theory of binary forms*, Bull. Amer. Math. Soc. 10 (1984), 27–85.

[9] S. Mulay, J. J. Quinn, and M. Shattuck, *Correlation diagrams: an intuitive approach to correlations in quantum Hall systems*, Journal of Physics: Series C 702 (2016), (012007-1)–(012007-9).

[10] S. Mulay, J. J. Quinn, and M. Shattuck, *Strong Fermion Interactions in Fractional Quantum Hall States, Correlation Functions*, Springer Series in Solid-State Sciences 193, 2018.

[11] K. M. O'Hara, *Unimodality of Gaussian coefficients: a constructive proof*, J. Combin. Theory Ser. A 53:1 (1990), 29–52.

[12] I. Pak and G. Panova, *Bounds on certain classes of Kronecker and q-binomial coefficients*, J. Combin. Theory Ser. A 147 (2017), 1–17.

[13] J. Petersen, *Die Theorie der regularen Graphs*, Acta Math. 15 (1891), 193–220.

[14] J. Petersen, *Theorie des equations Algébrique*, Gauthier-Villars, Paris, 1897.

[15] J. J. Quinn and A. Wójs, *Composite fermions in fractional quantum Hall systems*, Journal of Physics: Condensed Matter 12 (2000), R265–R298.

[16] G. Sabidussi, *Binary invariants and orientations of graphs*, Discrete Math. 101 (1992), 251-277.

[17] J. J. Sylvester, *On an application of the New Atomic Theory to the graphical representation of invariants and covariants of binary quantics, with three appendices*, Amer. J. Math. 1 (1878), 64–125.

[18] J. J. Sylvester, *Proof of the hitherto undemonstrated fundamental theorem of invariants*, Phi-los. Mag. 5 (1878), 178–188 (reprinted in: Coll. Math. Papers, vol. 3, Chelsea, New York, 1973).

[19] F. Zanello, *Zeilberger's KOH theorem and the strict unimodality of q-binomial coefficients*, Proc. Amer. Math. Soc. 143:7 (2015), 2795–2799.