Graph-monomials and invariants of binary forms

Shashikant Mulay
Department of Mathematics
University of Tennessee, Knoxville, TN 37996 U. S. A.

Abstract: Associated with a loopless undirected multigraph on \( N \) vertices, is its graph-monomial. Symmetrization of such a graph-monomial yields a semi-invariant (which is an invariant if the multigraph is regular) of a binary form of degree \( N \). The main theorem of this article (which, somewhat amazingly, escaped detection by Cayley, Sylvester and Petersen) establishes a practical and broadly applicable sufficient condition for ensuring nontriviality of the symmetrization of a graph-monomial in characteristics 0 and \( p > N \). To demonstrate the use of the main theorem, a sample of infinite families of invariants (especially, skew-invariants) are constructed.

Keywords: Symmetrized graph-monomials, Invariants of binary forms.

MSC Classifications: 05E05, 13A50.

Ever since the theory of (relative) 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 [5], [6]) provides an easy recipe for formulating symbolic expressions that yield (relative) invariants and semi-invariants of binary forms of arbitrary degrees. But, without full expansion (or un-symbolization) one does not know whether a given symbolic expression yields a nonzero (semi-) invariant. The method of symmetrized graph-monomials which is the focus of our attention here, was also known to classical invariant theorists (see [10], [11], [14]). It poses the problem of finding a useful criterion to determine nonzero-ness of the symmetrization of graph-monomials. Historically, Sylvester and Petersen did consider this problem; in fact, Petersen formulated a sufficient (but not necessary) condition on a graph that ensures zero-ness of the symmetrization of the associated graph-monomial. For a detailed historical sketch of this topic, we refer the reader to [13]. In [13], nonzero-ness of the symmetrization of a graph-monomial is translated to certain properties of the orientations and the orientation preserving graph-automorphisms of the underlying graph; but, verification of these properties is as forbidding as is a brute force computation of the desired symmetrization.

Most modern investigations in invariant theory are focused on finding a finite set of generators for the ring of invariants (with coefficients in \( \mathbb{C} \)) of the binary form of degree \( N \) for small \( N \) (e.g., see [2], [7]). Concrete construction of invariants plays a naturally important role in such an endeavor. Invariants form a special subset of semi-invariants. Semi-invariants too play an important role in various considerations (e.g., see [3]); constructions of specific types of
semi-invariants is also of express interest to us here. Semi-invariants provide a
good example to illustrate the fact that knowing a set of generators for the ring
they form, does not enable us to construct a prescribed semi-invariant. In fact,
for each positive integer \(N\), the ring of semi-invariants of the binary form of
degree \(N\) is a polynomial ring in \(N - 1\) variables with a well understood set of
generators. Yet, the problem of constructing nonzero semi-invariants of given
degree as well as of given weight remains as challenging as before (here degree
means the total degree as a polynomial in the coefficients of the binary form
and likewise for the weight).

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 fractional quantum
Hall state. Such a function is essentially a product of an alternating function
called the Fermi factor and a so called correlation function, where the correlation
function is a semi-invariant (which is an invariant in certain cases), of the binary
form of degree \(N\). In an intuitive approach, the correlation function is realized
as a symmetrized graph-monomial. Thus arises the need to have a practical non-
triviality criterion for the symmetrization of at least those graph-monomials that
are associated with a general class of correlation functions. In this article, we
establish an easy to use yet broadly applicable sufficient criterion (see Theorem
1) for non-triviality of a symmetrized graph-monomial. Besides enabling explicit
 constructions of the desired trial wave functions, Theorem 1 is interesting from
a purely invariant theoretic point of view. The graph-monomial-symmetrization
method of constructing semi-invariants is plainly more advantageous in positive
characteristic since it does not employ differential operators or transvections.
Following the proof of Theorem 1 below, we exhibit a sample of its applications;
the reader can easily find several more. Also, our results are potentially useful
in the invariant theory of binary forms over the fields of positive characteristic.
This is still a largely open area of research (see [7] and the references within).
In particular, very little is known about the dimension of the space of semi-
invariants of given weight and degree (associated with the binary form of general
degree \(N\)); especially, if the weight is divisible by the characteristic. The classical
count of the aforementioned dimension relies on describing kernels of certain
differential operators: this approach does not work in positive characteristic.
In contrast, the symmetrized graph-monomial approach allows construction of
linearly independent semi-invariants of given weight and degree (see the remarks
following the proof of Theorem 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 \(\Gamma\)
on finitely many (at least two) vertices labeled \(1, 2, \ldots, N\); multigraph \(\Gamma\) is said
to be \(d\)-regular provided each vertex of \(\Gamma\) has the same degree \(d\). In the figures
below, \(\Gamma_1\) is seen to be a 2-regular multigraph and the multigraphs \(\Gamma_2, \Gamma_3\) both
are 3-regular.

Let \(\varepsilon(\Gamma, i, j)\) be the number of edges in \(\Gamma\) connecting vertex \(i\) to vertex \(j\).
The graph-monomial of \(\Gamma\), denoted by \(\mu(\Gamma)\), is the polynomial in indeterminates
$z_1, \ldots, z_N$ 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 $\sigma$ of $\{1, 2, \ldots, N\}$ and $\mu_\sigma(\Gamma)$ stands for the product of $(z_{\sigma(i)} - z_{\sigma(j)})^{\varepsilon(\Gamma, i, j)}$: $1 \leq i < j \leq N$. Given any field $k$, $g(\Gamma)$ can be regarded as having coefficients in $k$. In the classical invariant theory of binary forms, where $k = \mathbb{C}$, it is well known that if $\Gamma$ is $d$-regular on $N$ vertices, then $g(\Gamma)$ is a (relative) invariant of degree $d$ (and weight $Nd/2$) of the binary form $F := (X - z_1 Y)(X - z_2 Y) \cdots (X - z_N Y)$. 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 [5]; note that this proof remains valid over fields $k$ of characteristics $> N$). If $\Gamma$ is not $d$-regular for any $d$, then $g(\Gamma)$ is a (relative) semi-invariant (as defined in [5]) of $F$ irrespective of the characteristic of $k$. For example, $g(\Gamma_1)$ is a quadratic invariant of a binary sextic (investigated in [4]) and each of $g(\Gamma_2)$, $g(\Gamma_3)$ is a cubic invariant of a binary quartic. It can be 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 of the form $g(\Gamma)$. Also, for non-isomorphic multigraphs $\Gamma$ and $\Gamma'$, their corresponding $g(\Gamma)$ and $g(\Gamma')$ may be numerical multiples of each other. Clearly, it is desirable to understand the types of multigraph $\Gamma$ for which $g(\Gamma)$ is nonzero. For then, we get a natural method of constructing nonzero semi-invariants of $F$. Use of symmetrized graph-monomials can also be seen in a somewhat different context in [1].

In the physics of Fermion-correlations, vertices of $\Gamma$ correspond to Fermions and the edges in $\Gamma$ represent correlations (a repulsive interaction) between the Fermions; here, it suffices to work over $\mathbb{C}$. A multigraph $\Gamma$ 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 $\Gamma$ need not be $d$-regular for any $d$. In physics a configuration $\Gamma$ 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 existing 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 \( \Gamma \) 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 \( \Gamma \) ranges over \( C(N, L, d) \). A configuration \( \Gamma \in C(N, L, d) \) is minimal if \( p(\Gamma) = p(N, L, d) \). Since it is known (see [12]) that the lowest energy configurations (or states) \( \Gamma \) are those with the least \( p(\Gamma) \), it is of interest to understand \( p(N, L, d) \) for a given triple \((N, L, D)\).

Likewise, given \( \Gamma, \Gamma' \in C(N, L, d) \), it is of interest to know when \( g(\Gamma) \) is (or is not) a constant multiple of \( g(\Gamma') \). We refer the reader to [8] for a glimpse of our investigation in this matter. Recently, using a weak corollary of Theorem 1, 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 [9]). It is not possible to give a full account of our recent results here.

The central result of this article (Theorem 1), presents a useful sufficient condition on a multigraph \( \Gamma \) that ensures nontriviality of \( g(\Gamma) \). There is nothing akin to Theorem 1 in the existing literature. Since Theorem 1 is constructive, if it 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 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 1 we consider only those multigraphs \( \Gamma \) 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 \( \Gamma_i \) has no edges) and the inter-edges between pairs \( \Gamma_i, \Gamma_j \) are more ‘dominating’ (in a specific way) than the intra-edges within each \( \Gamma_i \). For such \( \Gamma \), the proof of Theorem 1 consists of finding an appropriate evaluation-homomorphism \( h \) of \( k[z_1, \ldots, z_N] \) such that \( h(g(\Gamma)) \neq 0 \) (and thus proving non-triviality of \( g(\Gamma) \)). Using Theorem 1, we are able to construct several infinite families of invariants (including skew-invariants) of binary forms of unrestricted degrees \( N \) over the ground fields of characteristic 0 or characteristics \( p > N \). Optimistically, there is an appropriate generalization of Theorem 1, yet to be discovered, that will allow construction of all semi-invariants via the symmetrized-graph-monomial approach.

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

**Definitions:** Let \( m \) and \( n \) be positive integers.

1. Let \( \text{Symm}_N : k[z] \to k[z] \) be the Symmetrization operator defined by
   \[
   \text{Symm}_N(f) := \sum_{\sigma \in S_N} f(z_{\sigma(1)}, \ldots, z_{\sigma(N)}).
   \]
   \( f \in k[z] \) 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 1:** Let \( n \) be a positive integer. For \( 1 \leq i \leq n \), let \( g_i \in \mathbb{Q}(z) \). Then \( g_1^2 + g_2^2 + \cdots + g_n^2 \) is 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 notation of (i), 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 of (i); the second claim of (i) easily follows. Assertion (ii) readily follows from (i). \( \square \)

**Definitions:**

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 $\varepsilon$ is denoted by $\varepsilon(i, j)$. An integer $w \in \mathbb{N}$ is identified with the constant function $C \to \mathbb{N}$ such that $(i, j) \mapsto w$ 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 1**: There is an obvious bijective correspondence $\varepsilon \leftrightarrow [a_{ij}]$ between the set of functions $\varepsilon : \pi[N] \to \mathbb{N}$ and the set $E(\mathbb{N})$, given by
\[a_{ij} = \varepsilon(i, j) \quad \text{for } 1 \leq i < j \leq N.\]

Suppose $m_1 \leq m_2 \leq \cdots \leq m_q$ is a partition of $N$ and $M \in E(\mathbb{N})$. 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 $E(\mathbb{N})$ and $M_{rr} \in E(m_r)$ for $1 \leq r \leq q$.

**Definitions**: 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 $M^{**}$.

**Remarks 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 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 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 \( \text{Symm}_N(\delta(z, M)) \neq 0 \).
**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 $\pi$ 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 $1 \leq r(\sigma) \leq q$ 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 $1 \leq r < s \leq q$ and $\sigma \in G$, then since $r(\sigma) \neq s(\sigma)$, we infer that

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

Moreover,

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

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 $1 \leq r \leq q$ 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 $1 \leq r \leq q$, define

$$w_r := \sum_{(i, j) \in \pi(A_r)} \varepsilon_r(i, j) \text{ and } w := \sum_{i=1}^q w_i.$$
Our hypothesis (i) assures that if \( m_i = m_j \) for some \( i \neq j \), 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

\[
\alpha(z_i) := tx_i + t_r \quad \text{if} \quad i \in A_r \quad \text{with} \quad 1 \leq r \leq q.
\]

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

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

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

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

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

\[
m_s = m_{s(\sigma)} \leq m_r = m_{r(\sigma)} \implies m_s = m_{s(\sigma)} = m_{r(\sigma)} = m_r
\]

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

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

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
\[
V(x, 0, T) = |G| \prod_{1 \leq r < s \leq q} (t_r - t_s)^{b(m_r, m_s)}
\]
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 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 \(1 \leq r \leq q\). Then
\[
\alpha(\sigma(v(z, \pi(A_r), \varepsilon_r))) = t^{wr} \theta_r(v(x, \pi(A_r), \varepsilon_r)) = t^{wr} \sigma(v(x, \pi(A_r), \varepsilon_r))
\]
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) assures 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 1 assures 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

$$\sum_{\sigma \in G} V_{\sigma}(x, t, T)W_{\sigma}(x, t, T) = \sum_{\sigma \in G} t^wV_{\sigma}(x, t, T)F_{\sigma}(x)$$

has $t$-order exactly $w$.

Next, for $\sigma \in S_N$, let

$$R(\sigma) := \bigcup_{1 \leq r \leq q} \pi(B_r(\sigma)).$$

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 $\sigma$ and hypothesis (1), it follows that $\lambda(\sigma) \geq 1$ 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 $V_\sigma(x,t,T) = P_\sigma(x,t,T) \cdot Q_\sigma(x,t,T)$,
$$P_\sigma(x,t,T) = t^{\lambda(\sigma)} \prod_{(i,j) \in \pi \cap R(\sigma)} (x_{\sigma(i)} - x_{\sigma(j)})$$
and $Q_\sigma(x,0,T)$ is a nonzero $T$-homogeneous polynomial of $T$-degree $d(\pi)$. Hence the $t$-order of $V_\sigma(x,t,T)$ is exactly $\lambda(\sigma)$. For $1 \leq r \leq q$, let
$$P^{(r)}_\sigma(x,t,T) := \alpha(\sigma(v(z, \pi(A_r) \cap R(\sigma), \varepsilon_r))),$$
$$Q^{(r)}_\sigma(x,t,T) := \alpha(\sigma(v(z, \pi(A_r) \setminus R(\sigma), \varepsilon_r))).$$
Now for $1 \leq r \leq q$, 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
$$\alpha(\sigma(v(z, \pi(A_r), \varepsilon_r))) = P^{(r)}_\sigma(x,t,T) \cdot Q^{(r)}_\sigma(x,t,T).$$
Since $\pi(B_s(\sigma)) \cap \pi(B_r(\sigma)) = \emptyset = \pi(A_r) \cap \pi(A_s)$ for $1 \leq r < s \leq q$, 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
$$J := \bigsqcup_{r=1}^{q} (\pi(A_r) \setminus R(\sigma)) = \{(i,j) \in \pi[N] \setminus \pi \mid \sigma(i,j) \in \pi\}.$$
Let $\Upsilon := \text{Symm}_N(\delta(z, M))$. Then we have

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

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, $\Upsilon \neq 0$. □

Remarks 3: We continue to use the above notation.

1. Suppose $M$ satisfies the hypotheses of Theorem 1 and $\lambda$ is a positive integer such that $\text{Symm}_{m_r}(\delta(z, \lambda M_{rr})) \neq 0$ for $1 \leq r \leq q$. Then $\lambda M$ also satisfies the hypotheses of Theorem 1. In general, the polynomials $\text{Symm}_N(\delta(z, M))$ and $\text{Symm}_N(\delta(z, \lambda M))$ do not seem to be related in any obvious manner (see the last of the Examples 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 1 and let $\Upsilon_i := \text{Symm}_N(\delta(z, M_i))$. 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 proof of Theorem 1 it follows that the $t$-initial form of each $\alpha(\Upsilon_i)$ is essentially of the type $\prod_{1 \leq r < s \leq q} (t_r - t_s)^{b(m_r, m_s)}$. The $k$-linear independence of such products is completely determined by the exponents $b(m_r, m_s)$.

Examples 1:

1. Consider the following $E_1, E_2, E_3 \in E(6)$ presented as $2 \times 2$ 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 $\text{Symm}_6(\delta(z, E_1)) \neq 0$, $\text{Symm}_6(\delta(z, E_2)) = 0$ and $\text{Symm}_6(\delta(z, E_3)) \neq 0$. Of course, in the case of $E_1$, Theorem 1 does apply. Since $\|C_2\| = 29 = \|C_3\|$ is an odd integer, Theorem 1 can not be applied in the case of $E_2, E_3$. 

13
2. For \( j = 1, 2 \), let \( E_j \in E(5, 18) \) be presented in \( 2 \times 2 \) 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 \( h_j := \text{Symm}_5(\delta(z, E_j)) \neq 0 \) 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 \( 2 \times 2 \) block-matrix \( [M_{ij}] \) such that \( M_{11} = 0 \), \( M_{12} = 0 = M_{21} \). Note that Theorem 1 is applicable and thus \( g := \text{Symm}_9(\delta(z, M)) \) 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 \( 2 \times 2 \) block matrix \( [M_{ij}] \), where \( M_{11} = 2D_2 = M_{22} \) and \( M_{12} = 0 = M_{21} \). Let \( g := \text{Symm}_4(\delta(z, M)) \) and \( h := \text{Symm}_4(\delta(z, 2M)) \). Then \( 2M \in E(4, 4) \) and by Lemma 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:** 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 \( g := \text{Symm}_N(\delta(z, E)) \) 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 \( M_{rr} := dD_r \) 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 \( 2 \times 2 \) 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 \( \text{char} k = 0 \), Lemma 1 assures that \( g \neq 0 \). □

**Theorem 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 $g := \text{Symm}_N(\delta(z, E))$ 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
\[
c := \frac{2(n - 1)a + (m - 1)(n - 1)b}{r}
\]
is an integer, there is an explicitly described $E \in E(N, mnc)$ yielding a (degree $mnc$) nonzero invariant $g := \text{Symm}_N(\delta(z, E))$ 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 $g := \text{Symm}_N(\delta(z, E))$ 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 $g := \text{Symm}_N(\delta(z, E))$ 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 $\text{Symm}_N(\delta(z, E^*)) \neq 0$, a matrix $E^* \in E(2N - 1, dN)$ can be so constructed that $g := \text{Symm}_N(\delta(z, E^*))$ 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 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 $1 \leq i < j \leq n + 1$, $M_{ij}$ 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 1 can be employed to infer $g \neq 0$. 

15
To prove (iii), let $E \in E(N)$ be the $3 \times 3$ block matrix $[M_{ij}]$ such that $M_{rr} = 0$ for $1 \leq r \leq 3$, $M_{12} = M_{13}^T$ is the $l \times m$ matrix having each entry equal to $a$, $M_{13} = M_{23}^T$ 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 1 is indeed applicable in this case and hence $g \neq 0$.

To prove (iv), let $m := 1$, $n := 4u + 2v + 1$ and $r := 8wu - 4tv - 4v$. 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 $w = (2s + 1)(2t - 1)(2u + 1)(4wu - 4v + 1)$. 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 $2 \times 2$ 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 1 can be applied to infer $g \neq 0$. □

**Examples 2:** We continue assuming $N \geq 3$.

1. $N = 4e$. Using (i) of Theorem 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 $\text{char} \, k = 0$ and $d \leq N - 2$ is even, then Lemma 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 $d = 2 \mod 4$, 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) 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 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. 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. Then by (v) of Theorem 2, $g_n := \text{Symm}_{2^n+1}(\delta(z, M_n))$ is a nonzero skew invariant of a binary form of degree $2^n + 1$ for $2 \leq n \in \mathbb{Z}$.

Remarks 4: Theorem 2 exhibits the simplest applications of Theorem 1. At present, there does not exist a characterization of pairs $(N,d)$ for which Theorem 1 can be used to obtain a nonzero invariant. Interestingly, it is impossible to use Theorem 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 1. A ‘good’ generalization of Theorem 1, if it exists, should repair this failing.

References

1. Alexandersson, Per; Shapiro, Boris (2012) Discriminants, symmetrized graph monomials, and sums of squares, Exp. Math. 21, no. 4, 353–361.

2. Bedratyuk, Leonid (2007) On complete system of invariants for the binary form of degree 7, J. Symbolic Comput. 42, no. 10, 935–947.

3. Bedratyuk, Leonid (2012) Semi-invariants of binary forms and identities for Bernoulli, Euler and Hermite polynomials, Acta Arith. 151, no. 4, 361–376.

4. Dunajski, M.; Penrose, R. (2017) On the quadratic invariant of binary sexstics, Math. Proc. Cambridge Philos. Soc., 162, no. 3, 435-445.

5. Elliot, E. B. (1913) An Introduction to the Algebra of Quantics, Chelsea Publishing Company, New York, 1964, Second edition, reprint.

6. Grace J. H.; Young, A. (1903) The Algebra of Invariants, Chelsea Publishing Company, New York, 1964, reprint.

7. Krishnamoorthy, V.; Shaska, T.; Völklein, H. (2005) Invariants of binary forms, Progress in Galois theory, 101122, Dev. Math., 12, Springer, New York.

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

9. Mulay, S.; Quinn, John J.; Shattuck, M. (2018) Strong Fermion Interactions in Fractional Quantum Hall States, Correlation Functions, Springer Series in Solid-State Sciences, in press.
10. Petersen, J. (1891) *Die Theorie der regulären Graphs*, Acta Math., 15, 193-220.

11. Petersen, J. (1897) *Theorie des equations Algèbriques*, Gauthier-Villars, Paris.

12. Quinn, John J.; Wójs, A. (2000) *Composite fermions in fractional quantum Hall systems*, Journal of Physics: Condensed Matter 12, R265 - R298.

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

14. Sylvester, J. J., (1878) *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, 64-125.