RULES OF THREE FOR COMMUTATION RELATIONS

JONAH BLASIAK AND SERGEY FOMIN

Dedicated to Efim Zelmanov on his 60th birthday

Abstract. We study the phenomenon in which commutation relations for sequences of elements in a ring are implied by similar relations for subsequences involving at most three indices at a time.

What I tell you three times is true.

The Hunting of the Snark, by Lewis Carroll

Introduction

In this paper, we investigate the following surprisingly widespread phenomenon which we call *The Rule of Three*: in order for a particular kind of commutation relation to hold for subsequences of elements of a ring labeled by any subset of indices, it is enough that these relations hold for subsets of size one, two, and three.

Here is a typical "Rule of Three" statement. Let $g_1, \ldots, g_N, h_1, \ldots, h_N$ be invertible elements in an associative ring. Then the following are equivalent (cf. Theorem 3.4):

- for any subsequence of indices $1 \leq s_1 < \cdots < s_m \leq N$, the element $g_{s_m} \cdots g_{s_1}$ commutes with both $h_{s_m} \cdots h_{s_1}$ and $h_{s_m} + \cdots + h_{s_1}$;
- the above condition holds for all subsequences of length $m \leq 3$.

We establish many results of this form, including

- Rules of Three for noncommutative elementary symmetric functions (Section 1);
- Rules of Three for generating functions over rings (Section 2);
- Rules of Three for sums and products (Section 3).

Proofs are given in Sections 4–8. For reference, Theorems 2.5 and 2.12 are proved in Section 5; Theorem 3.2 is proved in Section 6; Theorems 1.1, 3.4, 3.5, 3.10, and 3.11 are proved in Section 7; and Theorem 1.6 is proved in Section 8.

Date: August 16, 2016.

2010 *Mathematics Subject Classification.* Primary 16S99. Secondary 05E05.

Key words and phrases. Noncommutative symmetric function, commutation relations, elementary symmetric function, Rule of Three, Dehn diagram.

Partially supported by NSF grants DMS-14071174 (J. B.) and DMS-1361789 (S. F.).

1. Rules of Three for noncommutative symmetric functions

Let $\mathbf{u} = (u_1, \ldots, u_N)$ be an ordered N-tuple of elements in a ring R. (We informally view $u_1, \ldots, u_N$ as "noncommuting variables.") For an integer k, the *noncommutative elementary symmetric function* $e_k(\mathbf{u}) \in R$ is defined by

$$e_k(\mathbf{u}) = \sum_{N \ge i_1 > i_2 > \cdots > i_k \ge 1} u_{i_1} u_{i_2} \cdots u_{i_k} \,. \tag{1.1}$$

(By convention, $e_0(\mathbf{u})=1$ and $e_k(\mathbf{u})=0$ if $k < 0$ or $k > N$.) More generally, for a subset $S \subset \{1, \ldots, N\}$, we denote

$$e_k(\mathbf{u}_S) = \sum_{\substack{i_1 > i_2 > \cdots > i_k \\ i_1, \ldots, i_k \in S}} u_{i_1} u_{i_2} \cdots u_{i_k} \,. \tag{1.2}$$

Again, $e_0(\mathbf{u}_S)=1$, and $e_k(\mathbf{u}_S)=0$ unless $0 \le k \le |S|$. (Here $|S|$ is the cardinality of S.)

Theorem 1.1 (The Rule of Three for noncommutative elementary symmetric functions)**.** *Let $\mathbf{u} = (u_1, \ldots, u_N)$ and $\mathbf{v} = (v_1, \ldots, v_N)$ be ordered N-tuples of elements in a ring R. Then the following conditions are equivalent:*

- *the noncommutative elementary symmetric functions $e_k(\mathbf{u}_S)$ and $e_\ell(\mathbf{v}_S)$ commute with each other, for any integers k and ℓ and any subset $S \subset \{1, \ldots, N\}$:*
$$e_k(\mathbf{u}_S)\, e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S)\, e_k(\mathbf{u}_S); \tag{1.3}$$
- *the commutation relation* (1.3) *holds for $|S| \le 3$ and any k, ℓ;*
- *the commutation relation* (1.3) *holds for $|S| \le 3$ and $k\ell \le 3$.*

Remark 1.2. Explicitly, Theorem 1.1 asserts that the commutation relations (1.3) hold for all k and ℓ and all subsets $S \subset \{1, \ldots, N\}$ if and only if the following relations hold:

$$e_1(\mathbf{u}_S)e_1(\mathbf{v}_S) = e_1(\mathbf{v}_S)e_1(\mathbf{u}_S) \qquad \text{for } 1 \le |S| \le 3, \tag{1.4}$$
$$e_2(\mathbf{u}_S)e_1(\mathbf{v}_S) = e_1(\mathbf{v}_S)e_2(\mathbf{u}_S) \qquad \text{for } 2 \le |S| \le 3, \tag{1.5}$$
$$e_1(\mathbf{u}_S)e_2(\mathbf{v}_S) = e_2(\mathbf{v}_S)e_1(\mathbf{u}_S) \qquad \text{for } 2 \le |S| \le 3, \tag{1.6}$$
$$e_3(\mathbf{u}_S)e_1(\mathbf{v}_S) = e_1(\mathbf{v}_S)e_3(\mathbf{u}_S) \qquad \text{for } |S| = 3, \tag{1.7}$$
$$e_1(\mathbf{u}_S)e_3(\mathbf{v}_S) = e_3(\mathbf{v}_S)e_1(\mathbf{u}_S) \qquad \text{for } |S| = 3. \tag{1.8}$$

(Actually, it suffices to require (1.4) for $|S| \le 2$, but this is not so important.) It is rather miraculous that (1.4)–(1.8) imply the relations

$$e_2(\mathbf{u}_S)e_2(\mathbf{v}_S) = e_2(\mathbf{v}_S)e_2(\mathbf{u}_S) \qquad \text{for } 2 \le |S| \le 3, \tag{1.9}$$
$$e_2(\mathbf{u}_S)e_3(\mathbf{v}_S) = e_3(\mathbf{v}_S)e_2(\mathbf{u}_S) \qquad \text{for } |S| = 3, \tag{1.10}$$
$$e_3(\mathbf{u}_S)e_2(\mathbf{v}_S) = e_2(\mathbf{v}_S)e_3(\mathbf{u}_S) \qquad \text{for } |S| = 3, \tag{1.11}$$
$$e_3(\mathbf{u}_S)e_3(\mathbf{v}_S) = e_3(\mathbf{v}_S)e_3(\mathbf{u}_S) \qquad \text{for } |S| = 3, \tag{1.12}$$

in addition to all relations (1.3) for $|S| \ge 4$.

In the case of a single N-tuple of "noncommuting variables" $u_1 = v_1, \ldots, u_N = v_N$, we obtain the following corollary.

Corollary 1.3 ([11], [6]). *Let R be a ring, and let $\mathbf{u}=(u_1,\ldots,u_N)$ be an ordered N-tuple of elements of R. Then the following are equivalent:*

- *the noncommutative elementary symmetric functions $e_k(\mathbf{u}_S)$ and $e_\ell(\mathbf{u}_S)$ commute with each other, for any integers k and ℓ and any subset $S \subset \{1,\ldots,N\}$:*
$$e_k(\mathbf{u}_S)e_\ell(\mathbf{u}_S) = e_\ell(\mathbf{u}_S)e_k(\mathbf{u}_S); \tag{1.13}$$
- *the following special cases of* (1.13) *hold:*
$$e_1(\mathbf{u}_S)e_2(\mathbf{u}_S) = e_2(\mathbf{u}_S)e_1(\mathbf{u}_S) \qquad \text{for } 2 \le |S| \le 3, \tag{1.14}$$
$$e_1(\mathbf{u}_S)e_3(\mathbf{u}_S) = e_3(\mathbf{u}_S)e_1(\mathbf{u}_S) \qquad \text{for } |S| = 3. \tag{1.15}$$

Proof. This is a special case of Theorem 1.1. Note that when $\mathbf{u} = \mathbf{v}$, the condition (1.4) is trivial, whereas (1.5)–(1.8) become (1.14)–(1.15). □

Remark 1.4. Corollary 1.3 is equivalent to a result by A. N. Kirillov [11, Theorem 2.24]; the above version appeared in our previous paper [6, Theorem 2.3]. It generalizes similar results obtained in [4, 10, 13, 15, 19]. See [6, Remark 2.2] for additional discussion.

Remark 1.5. Corollary 1.3 and similar results serve as the starting point for the theory of *noncommutative Schur functions*, which aims to produce positive combinatorial formulae for Schur expansions of various classes of symmetric functions. This theory originated in [10], building off the work of Lascoux and Schützenberger on the plactic algebra [15, 21]. It was later adapted to study LLT polynomials [13] and k-Schur functions [12]; other variations appeared in [2, 11, 19]. Further recent work includes the papers [4, 5, 6], which advance the theory to encompass Lam's work [13] and incorporate ideas of Assaf [1]. One of the main outcomes of this approach is a proof of Haglund's conjecture on 3-column Macdonald polynomials [5].

Theorem 1.1 can be generalized to the setting of "noncommutative supersymmetric polynomials." Let us fix an arbitrary partition of the ordered alphabet $\{1 < \cdots < N\}$ into *unbarred* and *barred indices*. The *noncommutative super elementary symmetric function* $\overline{e}_k(\mathbf{u})$ is defined by the following variation of (1.1):
$$\overline{e}_k(\mathbf{u}) = \sum_{\substack{N \ge i_1 \ge i_2 \ge \cdots \ge i_k \ge 1 \\ i_j \text{ unbarred} \Rightarrow i_j > i_{j+1}}} u_{i_1} \cdots u_{i_k}\,. \tag{1.16}$$
We similarly define the elements $\overline{e}_k(\mathbf{u}_S)$ associated to sub-alphabets $S \subset \{1 < \cdots < N\}$.

Theorem 1.6. *Let R be a ring, and let $\mathbf{u}=(u_1,\ldots,u_N)$ and $\mathbf{v}=(v_1,\ldots,v_N)$ be ordered N-tuples of elements of R. Then the following are equivalent:*

- *$\overline{e}_k(\mathbf{u}_S)$ and $\overline{e}_\ell(\mathbf{v}_S)$ commute, for any k and ℓ and any subset $S \subset \{1,\ldots,N\}$:*
$$\overline{e}_k(\mathbf{u}_S)\overline{e}_\ell(\mathbf{v}_S) = \overline{e}_\ell(\mathbf{u}_S)\overline{e}_k(\mathbf{v}_S); \tag{1.17}$$
- *the following special cases of* (1.17) *hold:*
$$\overline{e}_k(\mathbf{u}_S)\overline{e}_1(\mathbf{v}_S) = \overline{e}_1(\mathbf{u}_S)\overline{e}_k(\mathbf{v}_S) \qquad \text{for } |S| \le 3 \text{ and } k \ge 1; \tag{1.18}$$
$$\overline{e}_1(\mathbf{u}_S)\overline{e}_\ell(\mathbf{v}_S) = \overline{e}_\ell(\mathbf{u}_S)\overline{e}_1(\mathbf{v}_S) \qquad \text{for } |S| \le 3 \text{ and } \ell \ge 1. \tag{1.19}$$

We discuss the broader context for Theorem 1.6 in Remark 2.7 below.

2. Rules of Three for generating functions over rings

Commutation relations for noncommutative elementary symmetric functions can be reformulated as multiplicative identities for certain elements of a polynomial ring in two (central) variables with coefficients in R. This leads to an alternative perspective on The Rules of Three, which we discuss next.

In the rest of this paper, we repeatedly make use of the following convenient notation. Let $g_1, \dots, g_N$ be elements of a ring (or a monoid), and let $S = \{s_1 < \cdots < s_m\} \subset \{1, \dots, N\}$ be a subset of indices. We then denote

$$g_S = g_{s_m} \cdots g_{s_1}. \tag{2.1}$$

We similarly use the shorthand $h_S = h_{s_m} \cdots h_{s_1}$, etc.

Corollary 2.1. *Let $R[x, y]$ be the ring of polynomials in the formal variables x and y with coefficients in a ring R. (Here x and y commute with each other and with any $z \in R$.) Let $u_1, \dots, u_N, v_1, \dots, v_N \in R$. For $i = 1, \dots, N$, set*

$$g_i = 1 + xu_i \in R[x, y], \tag{2.2}$$

$$h_i = 1 + yv_i \in R[x, y]. \tag{2.3}$$

Then the following are equivalent:

- $g_S h_S = h_S g_S$ *for all subsets* $S \subset \{1, \dots, N\}$;
- $g_S h_S = h_S g_S$ *for all subsets S of cardinality* 1, 2, *and* 3.

Proof. We observe that (2.2)–(2.3) imply

$$g_S = (1 + xu_{s_m}) \cdots (1 + xu_{s_1}) = \textstyle\sum_k x^k \, e_k(\mathbf{u}_S), \tag{2.4}$$

$$h_S = (1 + yv_{s_m}) \cdots (1 + yv_{s_1}) = \textstyle\sum_\ell y^\ell \, e_\ell(\mathbf{v}_S). \tag{2.5}$$

Thus the property (1.3) (that is, each $e_k(\mathbf{u}_S)$ commutes with each $e_\ell(\mathbf{v}_S)$) is equivalent to saying that g_S commutes with h_S. The corollary is now immediate from Theorem 1.1. □

Given the multiplicative form of the conditions $g_S h_S = h_S g_S$ in Corollary 2.1, it is tempting to seek group-theoretic generalizations of the latter, with the factors g_i and h_i drawn from some (reasonably general) group. Unfortunately, the purely group-theoretic extension of Corollary 2.1 is false: the relation $g_4 g_3 g_2 g_1 h_4 h_3 h_2 h_1 = h_4 h_3 h_2 h_1 g_4 g_3 g_2 g_1$ does not hold in the group with presentation given by generators $g_1, \dots, g_4, h_1, \dots, h_4$ and relations $g_S h_S = h_S g_S$ for $|S| \le 3$. (This follows from the fact that replacing (2.3) with $h_i = 1 + xv_i$ transforms Corollary 2.1 into a false statement, cf. Example 2.11.)

Consequently one has to introduce some (likely nontrivial) assumptions on the group G and/or the elements g_i, h_i. Two results of this kind are stated in Section 4. A fundamental question remains (see also Problem 2.9):

Problem 2.2. *Find a group-theoretic Rule of Three strong enough to directly imply Corollary 2.1 (or better yet, Conjecture 2.3 below).*

From the standpoint of potential applications, the most important setting for "multiplicative rules of three" *à la* Corollary 2.1 is the one where the factors g_i, h_i are formal power series in xu_i and yv_i, respectively. Extensive computational evidence suggests that in this setting, the Rule of Three always holds:

Conjecture 2.3. *Let $R[[x,y]]$ be the ring of formal power series in the variables x and y with coefficients in a $\mathbb{Q}$-algebra R. Let $u_1,\dots,u_N,v_1,\dots,v_N \in R$, and assume that $g_1,\dots,g_N$, $h_1,\dots,h_N \in R[[x,y]]$ are power series of the form*

$$g_i = 1 + \alpha_{i1}xu_i + \alpha_{i2}(xu_i)^2 + \alpha_{i3}(xu_i)^3 + \cdots \qquad (\alpha_{ik} \in \mathbb{Q}), \tag{2.6}$$

$$h_i = 1 + \beta_{i1}yv_i + \beta_{i2}(yv_i)^2 + \beta_{i3}(yv_i)^3 + \cdots \qquad (\beta_{ik} \in \mathbb{Q}), \tag{2.7}$$

where for every i, either α_{i1} or β_{i1} is nonzero. Then the following are equivalent:

- *$g_S h_S = h_S g_S$ for all subsets $S \subset \{1,\dots,N\}$;*
- *$g_S h_S = h_S g_S$ for all subsets S of cardinality 1, 2, and 3.*

While Conjecture 2.3 remains open, we were able to prove it in several important cases. Three such results appear below and two more appear in Corollaries 7.6 and 7.7.

First, we obtain the following generalization of Corollary 2.1.

Theorem 2.4. *Conjecture 2.3 holds for $h_i = 1 + yv_i$ (and any g_i as in (2.6)).*

Theorem 2.4 is a special case of a more general result, see Corollary 7.6.

We also settle Conjecture 2.3 in the case of a single set of noncommuting variables:

Theorem 2.5. *Let $R[[x,y]]$ be the ring of formal power series in x and y with coefficients in a $\mathbb{Q}$-algebra R. Let $u_1,\dots,u_N \in R$. Let $g_1,\dots,g_N,h_1,\dots,h_N \in R[[x,y]]$ be of the form*

$$g_i = 1 + \alpha_{i1}xu_i + \alpha_{i2}(xu_i)^2 + \alpha_{i3}(xu_i)^3 + \cdots \qquad (\alpha_{ik} \in \mathbb{Q}), \tag{2.8}$$

$$h_i = 1 + \beta_{i1}yu_i + \beta_{i2}(yu_i)^2 + \beta_{i3}(yu_i)^3 + \cdots \qquad (\beta_{ik} \in \mathbb{Q}), \tag{2.9}$$

where for every i, either α_{i1} or β_{i1} is nonzero. Then the following are equivalent:

- *$g_S h_S = h_S g_S$ for all subsets $S \subset \{1,\dots,N\}$;*
- *$g_S h_S = h_S g_S$ for all subsets S of cardinality 2 and 3.*

Yet another case of Conjecture 2.3 follows from Theorem 1.6:

Corollary 2.6. *Conjecture 2.3 holds provided for each i, one of the following two options is chosen:*

- *$g_i = 1 + xu_i$ and $h_i = 1 + yv_i$; or*
- *$g_i = (1 - xu_i)^{-1}$ and $h_i = (1 - yv_i)^{-1}$.*

Theorem 1.6 is stronger than Corollary 2.6 since the latter requires the relations (1.17) for $|S| \le 3$ and any k, ℓ whereas the former only needs the instances with $k = 1$ or $\ell = 1$.

Remark 2.7. Theorem 2.5 is a far-reaching generalization of Corollary 1.3, which already demonstrated its importance in initiating new developments in the theory of noncommutative Schur functions (cf. Remark 1.5). It remains to be seen whether Theorem 2.5 for general power series (2.8)–(2.9) can spawn new versions of this theory.

One case (beyond the basic choice (2.2)–(2.3)) where some progress has been made is the setting of noncommutative super symmetric functions (cf. Theorem 1.6). The ring defined by the relations (1.14)–(1.15) has many quotients with rich combinatorial structure (the plactic algebra, nilCoxeter algebra, and more, see [4, 6, 10, 13]); the ring defined by the relations (1.18)–(1.19) has many interesting quotients as well, some of them similar to the plactic algebra. The recent paper [7] studies some of these quotients and develops an accompanying theory of noncommutative super Schur functions. The main application (recovering results of [3, 16]) is a positive combinatorial rule for the Kronecker coefficients where one of the shapes is a hook.

We next discuss some of the subtleties involved in generalizing the above results. To facilitate this discussion, we introduce the following concept.

Definition 2.8. Let $\mathcal{A} = \mathbb{Q}\langle u_1, \ldots, u_M, v_1, \ldots, v_M\rangle$ be the free associative $\mathbb{Q}$-algebra with generators $u_1, \ldots, u_M, v_1, \ldots, v_M$. Let $g_1, \ldots, g_N, h_1, \ldots, h_N$ be elements of $\mathcal{A}[[x, y]]$, i.e., some formal power series in x and y with coefficients in $\mathcal{A}$. We say that the *Multiplicative Rule of Three holds* for $g_1, \ldots, g_N, h_1, \ldots, h_N$ if for any quotient ring $R = \mathcal{A}/I$, the following are equivalent:

- $g_S h_S \equiv h_S g_S \bmod I$ for all subsets $S \subset \{1, \ldots, N\}$;
- $g_S h_S \equiv h_S g_S \bmod I$ for all subsets S of cardinality ≤ 3.

For example, the Multiplicative Rule of Three holds in the following cases:

- $h_i = 1 + yv_i$ and any g_i as in (2.6) (by Theorem 2.4);
- g_i, h_i are given by (2.8)–(2.9), with α_{i1}, β_{i1} not both 0 (by Theorem 2.5).

Conjecture 2.3 asserts that the Multiplicative Rule of Three holds for g_i, h_i given by (2.6)–(2.7), with α_{i1}, β_{i1} not both 0.

Problem 2.9. *Find the most general setting (i.e., the weakest restrictions on the expressions g_i, h_i) for which the Multiplicative Rule of Three holds.*

Example 2.10. The Multiplicative Rule of Three fails for

$$g_4 = (1 + xu_8)(1 + xu_7), \qquad h_4 = (1 + yu_8)(1 + yu_7), \tag{2.10}$$

$$g_3 = (1 + xu_6)(1 + xu_5), \qquad h_3 = (1 + yu_6)(1 + yu_5), \tag{2.11}$$

$$g_2 = (1 + xu_4)(1 + xu_3), \qquad h_2 = (1 + yu_4)(1 + yu_3), \tag{2.12}$$

$$g_1 = (1 + xu_2)(1 + xu_1), \qquad h_1 = (1 + yu_2)(1 + yu_1). \tag{2.13}$$

In other words, the relations on 8 elements $u_1, \ldots, u_8$ of a ring R resulting from the conditions $g_S h_S = h_S g_S$ for all subsets S of cardinality ≤ 3, with the g_i and the h_i given by (2.10)–(2.13), do not imply the relation $g_S h_S = h_S g_S$ for $S = \{1, 2, 3, 4\}$. This was shown using a noncommutative Gröbner basis calculation in `Magma` [8].

Example 2.11. For an 8-letter word $\mathbf{z} = z_1z_2z_3z_4\, z_1'z_2'z_3'z_4'$ in the alphabet $\{x, y\}$, let

$$g_i = 1 + z_iu_i, \quad h_i = 1 + z_i'v_i.$$

In this setting, the Multiplicative Rule of Three (with $N = 4$) holds for 222 of the $2^8 = 256$ choices of $\mathbf{z}$, and fails for the remaining 34. Specifically, the rule holds unless

- $z_1 = z_1', \ z_2 = z_2', \ z_3 = z_3', \ z_4 = z_4'$, or
- $z_1 < z_1', \ z_2 \geq z_2', \ z_3 \geq z_3', \ z_4 < z_4'$, or
- $z_1 > z_1', \ z_2 \leq z_2', \ z_3 \leq z_3', \ z_4 > z_4'$,

where we use the order relation $x < y$ on the symbols x and y. This was shown using a noncommutative Gröbner basis calculation in `Magma` [8].

The Multiplicative Rule of Three always holds in the simplified version of Example 2.11 wherein the factors g_i, h_i depend on a single set of noncommuting variables:

Theorem 2.12. *The Multiplicative Rule of Three holds when* $g_i = 1 + (\alpha_i x + \alpha_i' y)u_i$ *and* $h_i = 1 + (\beta_i x + \beta_i' y)u_i$ *for any* $\alpha_i, \alpha_i', \beta_i, \beta_i' \in \mathbb{Q}$. *(Here we use the notational conventions of Definition 2.8.)*

Theorem 2.12 is a special case of a more general result, see Theorem 5.3.

Since the Multiplicative Rule of Three does not always hold, it is natural to consider Rules of Four and beyond (though this has not been the main focus of our investigation). For example, we can generalize Definition 2.8 as follows: for any $k \geq 0$, we say that the *Multiplicative Rule of k holds* for $g_1, \dots, g_N, h_1, \dots, h_N$ if for any quotient ring $R = \mathcal{A}/I$, the following are equivalent:

- $g_Sh_S \equiv h_Sg_S \bmod I$ for all subsets $S \subset \{1, \dots, N\}$;
- $g_Sh_S \equiv h_Sg_S \bmod I$ for all subsets S of cardinality $\leq k$.

Conjecture 2.13. *For any* $k \geq 0$ *and* $N > k$, *the Multiplicative Rule of* k *fails for* $g_i = 1 + xu_i$, $h_i = 1 + xv_i$, $i = 1, 2, \dots, N$.

Conjecture 2.13 would imply the failure of the "group-theoretic Rule of k," for any k:

Conjecture 2.14. *Fix integers* $k \geq 0$ *and* $N > k$, *and consider the group whose presentation is given by generators* $g_1, \dots, g_N, h_1, \dots, h_N$ *and relations* $g_Sh_S = h_Sg_S$ *for* $|S| \leq k$. *Then* $g_Sh_S \neq h_Sg_S$ *for any* $|S| > k$.

We verified Conjecture 2.13 (hence Conjecture 2.14) in the cases $k \leq 5$ via a noncommutative Gröbner basis calculation.

3. Rules of Three for sums and products

Definition 3.1. Let M be a monoid. A subset $M' \subset M$ is called *potentially invertible* if M can be embedded into a larger monoid in which all elements of M' have left and right inverses (necessarily equal to each other); see [9, Section VII.3]. Similarly, a subset R' of a ring R is potentially invertible if R can be embedded into a larger ring in which all elements of R' are invertible.

By abuse of terminology, we say that elements $g_1, \dots, g_N$ of a monoid (or ring) are potentially invertible if $\{g_1, \dots, g_N\}$ is a potentially invertible subset.

Let $R[x]$ be the ring of polynomials in one formal (central) variable x, with coefficients in a ring R. Then any subset of $R[x]$ consisting of polynomials with constant term 1 is potentially invertible. Indeed, $R[x]$ can be embedded into the ring $R[[x]]$ of formal power series over R, and each polynomial with constant term 1 is invertible in $R[[x]]$.

Throughout this paper, we use the notation $[g, h] = gh - hg$ for the commutator of elements g, h of an associative ring.

Theorem 3.2 (The Rule of Three for sums *vs.* products). *Let R be a ring, and let $v_1, \dots, v_N \in R$ and $g_1, \dots, g_N \in R$, with $g_1, \dots, g_N$ potentially invertible. Then the following are equivalent:*

- $\big[\sum_{i\in S} v_i, g_S\big] = 0$ *for all subsets $S \subset \{1, \dots, N\}$;*
- $\big[\sum_{i\in S} v_i, g_S\big] = 0$ *for all subsets S of cardinality ≤ 3.*

Theorem 3.2 can be generalized to a setting of algebras with derivations. Recall that a *derivation* on a $\mathbb{Q}$-algebra R is a $\mathbb{Q}$-linear map $\partial : R \to R$ satisfying Leibniz's law

$$\partial(fg) = \partial(f)g + f\partial(g).$$

Theorem 3.3 (The Rule of Three for derivations). *Let R be a $\mathbb{Q}$-algebra. Let $\partial_1, \dots, \partial_N$ be derivations on R, and let $g_1, \dots, g_N$ be potentially invertible elements of R satisfying*

$$\partial_a(g_a) = 0 \qquad \text{for all } 1 \le a \le N; \tag{3.1}$$

$$(\partial_b + \partial_a)(g_b g_a) = 0 \qquad \text{for all } 1 \le a < b \le N; \tag{3.2}$$

$$(\partial_c + \partial_b + \partial_a)(g_c g_b g_a) = 0 \qquad \text{for all } 1 \le a < b < c \le N. \tag{3.3}$$

Then $(\partial_N + \partial_{N-1} + \cdots + \partial_1)(g_N g_{N-1} \cdots g_1) = 0$.

Theorem 3.4 (The Rule of Three for products *vs.* products and sums). *Let R be a ring, and let $g_1, \dots, g_N, h_1, \dots, h_N \in R$ be potentially invertible. Then the following are equivalent:*

- $[g_S, h_S] = [g_S, \sum_{i\in S} h_i] = 0$ *for all subsets $S \subset \{1, \dots, N\}$;*
- $[g_S, h_S] = [g_S, \sum_{i\in S} h_i] = 0$ *for all subsets S of cardinality ≤ 3.*

Theorem 3.5. *Let R be a ring, and let $g_1, \dots, g_N, h_1, \dots, h_N \in R$ be potentially invertible elements satisfying the relations*

$$[h_a, g_a] = 0 \qquad \text{for all } 1 \le a \le N; \tag{3.4}$$

$$[h_b + h_a, g_b + g_a] = 0 \qquad \text{for all } 1 \le a < b \le N; \tag{3.5}$$

$$[h_b + h_a, g_b g_a] = 0 \qquad \text{for all } 1 \le a < b \le N; \tag{3.6}$$

$$[h_c + h_b + h_a, g_c g_b g_a] = 0 \qquad \text{for all } 1 \le a < b < c \le N; \tag{3.7}$$

$$[g_b + g_a, h_b h_a] = 0 \qquad \text{for all } 1 \le a < b \le N; \tag{3.8}$$

$$[g_c + g_b + g_a, h_c h_b h_a] = 0 \qquad \text{for all } 1 \le a < b < c \le N. \tag{3.9}$$

Then $\big[\sum_{i\in S} g_i, \sum_{i\in S} h_i\big] = \big[\sum_{i\in S} g_i, h_S\big] = \big[g_S, \sum_{i\in S} h_i\big] = [g_S, h_S] = 0$ for all subsets S.

Remark 3.6. It is easy to see that the relations (3.4)–(3.5) alone imply

$$\left[\sum_{i\in S} g_i, \sum_{i\in S} h_i\right] = 0$$

for all $S \subset \{1, \ldots, N\}$; this implication can be regarded as an "Additive Rule of Two."

Theorem 3.5 implies (and so can be regarded as a strengthening of) the following rule.

Corollary 3.7 (The Rule of Three for products and sums *vs.* products and sums)**.** *Let R be a ring, and let $g_1, \ldots, g_N, h_1, \ldots, h_N \in R$ be potentially invertible. Then the following are equivalent:*

- $\left[\sum_{i\in S} g_i, \sum_{i\in S} h_i\right] = \left[\sum_{i\in S} g_i, h_S\right] = \left[g_S, \sum_{i\in S} h_i\right] = [g_S, h_S] = 0$ *for all S;*
- $\left[\sum_{i\in S} g_i, \sum_{i\in S} h_i\right] = \left[\sum_{i\in S} g_i, h_S\right] = \left[g_S, \sum_{i\in S} h_i\right] = [g_S, h_S] = 0$ *for all $|S| \leq 3$.*

We note that Corollary 3.7 is also immediate from Theorem 3.4 and Remark 3.6.

Remark 3.8. The cases $|S| \leq 3$ of Theorem 3.5 hold without the requirement of potential invertibility; this can be verified by a noncommutative Gröbner basis calculation. However, for $|S| \geq 4$, this requirement cannot be dropped. More precisely, in the free associative algebra $\mathbb{Q}\langle g_1, g_2, g_3, g_4, h_1, h_2, h_3, h_4\rangle$, the two-sided ideal generated by the left-hand sides of (3.4)–(3.9) does not contain the element $[g_4g_3g_2g_1, h_4h_3h_2h_1]$ (nor does it contain $[h_4 + h_3 + h_2 + h_1, g_4g_3g_2g_1]$). This was checked using a noncommutative Gröbner basis calculation in `Magma` [8].

Remark 3.9. As explained in Section 7, Theorem 3.5 directly implies Theorem 1.1 via the substitutions $g_i = 1 + xu_i$, $h_i = 1 + yv_i$. On the other hand, if we think of g_i and h_i in Theorem 3.5 as u_i and v_i, then Theorems 3.5 and 1.1 are "incomparable": in Theorem 3.5, we do not need the relations

$$[h_c + h_b + h_a, g_cg_b + g_cg_a + g_bg_a] = 0, \tag{3.10}$$

but we do require g_i and h_i to be potentially invertible (cf. Remark 3.8), while Theorem 1.1 requires $[e_1(\mathbf{v}_S), e_2(\mathbf{u}_S)] = 0$ for $|S| = 3$ but not invertibility.

To further clarify matters, we note that the assumptions of Theorem 3.5 (including invertibility) do not imply (3.10). To see this, take $N = 3$, $g_i = 1 + x^3u_i^3 + x^4u_i^4 + x^5u_i^5$, and $h_i = 1 + yv_i$ for $i = 1, 2, 3$. Impose relations on the u_i, v_i derived from the conditions $g_Sh_S = h_Sg_S$ for all S of cardinality ≤ 3. Then relations (3.4)–(3.9) hold but (3.10) (with $(a, b, c) = (1, 2, 3)$) does not. This was checked via a noncommutative Gröbner basis computation.

Theorem 3.2 and Theorems 3.10–3.11 below form a natural progression.

Theorem 3.10 (The Rule of Three for products *vs.* sums and quadratic forms)**.** *Let R be a ring. Let $v_1, \ldots, v_N \in R$ and $g_1, \ldots, g_N \in R$, with $g_1, \ldots, g_N$ potentially invertible. Then the following are equivalent:*

- $g_S\, e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S)\, g_S$ *for all subsets $S \subset \{1, \ldots, N\}$ and $\ell \leq 2$;*
- $g_S\, e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S)\, g_S$ *for all subsets S of cardinality ≤ 3 and $\ell \leq 2$.*

Theorem 3.11 (The Rule of Three for products *vs.* elementary symmetric functions)**.** *Let R be a ring. Let $v_1, \dots, v_N \in R$ and $g_1, \dots, g_N \in R$, with $g_1, \dots, g_N$ potentially invertible. Then the following are equivalent:*

- $g_S\, e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S)\, g_S$ *for all subsets $S \subset \{1, \dots, N\}$ and all ℓ;*
- $g_S\, e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S)\, g_S$ *for all subsets S of cardinality ≤ 3 and all ℓ.*

Remark 3.12. Theorem 3.11 implies a variant of the Multiplicative Rule of Three (see Corollary 7.6) which generalizes Theorem 2.4 (which in turn generalizes Corollary 2.1).

4. Dehn diagrams. Group-theoretic lemmas

For the purposes of this paper, a Dehn diagram (a simplified version of the notion of van Kampen diagram, see, e.g., [20, Section 4]) is a planar oriented graph whose edges are labeled by elements of a group, so that each cycle corresponds to a relation in the group. A more precise formulation is given in Definition 4.1 below.

Definition 4.1. Let D be a finite oriented graph properly embedded in the real plane; that is, it is drawn so that its edges only meet at common endpoints. We require each vertex of D to have at least two incident edges. The complement of D in the plane is a disjoint union of *faces*: some *bounded faces* homeomorphic to disks, and a single *outer face*.

Assume that every edge of D has been labeled by an element of a group G. Such an edge-labeled oriented graph is called a *Dehn diagram* if the product along the boundary ∂F of each bounded face F is equal to 1. More precisely, starting with an arbitrary vertex on ∂F and moving either clockwise or counterclockwise, we multiply the elements of G associated with the edges, inverting them when moving against the orientation of an edge. It is easy to see that this condition does not depend on the starting location on ∂F.

The following simple but useful observation goes back to M. Dehn.

Lemma 4.2. *In a Dehn diagram, the product of labels along the boundary of the outer face is equal to* 1*.*

Below we present several group-theoretic results in the spirit of (multiplicative) Rules of Three, cf. Problem 2.2. All the proofs utilize Dehn diagrams.

Proposition 4.3. *Let G be a group, and let $a, b, c, A, B, C \in G$ satisfy*

$$aC = Ca, \quad bB = Bb, \quad cA = Ac, \quad baBA = BAba, \quad cbCB = CBcb. \tag{4.1}$$

Then $cba\,CBA = CBA\,cba$.

Proof. In the Dehn diagram shown in Figure 1, each bounded face commutes. Hence so does the outer face, and the claim follows. □

Proposition 4.3 is a special case of the following result.

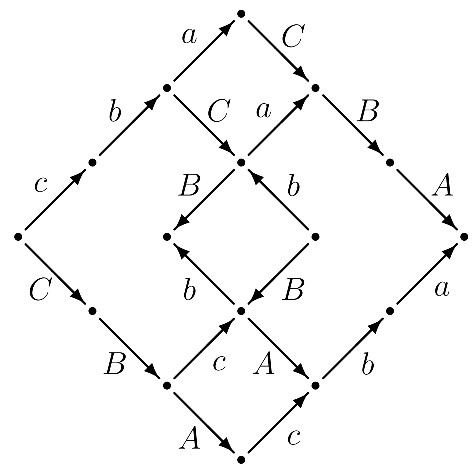

FIGURE 1. The proof of Proposition 4.3.

Theorem 4.4. *Let G be a group, and let the elements $g_1, \ldots, g_N, h_1, \ldots, h_N \in G$ satisfy*

$$g_a h_c = h_c g_a \qquad \text{for all } a, c \in \{1, \ldots, N\} \text{ with } |a-c| \geq 2; \tag{4.2}$$

$$g_a h_a = h_a g_a \qquad \text{for all } 1 < a < N; \tag{4.3}$$

$$g_{a+1} g_a h_{a+1} h_a = h_{a+1} h_a g_{a+1} g_a \qquad \text{for all } 1 \leq a < N. \tag{4.4}$$

Then

$$g_N g_{N-1} \cdots g_1 \, h_N h_{N-1} \cdots h_1 = h_N h_{N-1} \cdots h_1 \, g_N g_{N-1} \cdots g_1. \tag{4.5}$$

Proof. The proof is a direct generalization of the above proof of Proposition 4.3. It relies on the Dehn diagram shown in Figure 2, which illustrates the case $N = 6$. The quadrilateral and octagonal faces of the diagram correspond to relations (4.3) and (4.4), respectively. The bounded faces at the bottom and the top can be tiled by rhombi corresponding to the relations (4.2); to avoid clutter, these tiles are not shown. The outer boundary corresponds to (4.5). □

Remark 4.5. The statement of Proposition 4.3 (or its generalization, Theorem 4.4) does not involve inverses. As such, it readily extends to potentially invertible elements a, b, c, A, B, C in a monoid M. Note however that the assumption of potential invertibility cannot be dropped: in an arbitrary monoid M, elements a, b, c, A, B, C satisfying relations (4.1) do not have to satisfy $cbaCBA = CBAcba$. On the other hand, the latter identity is implied by (4.1) under the additional assumption that B is potentially invertible. (There is no need to require anything else.)

Remark 4.6. A. I. Malcev [17, 18] gave an infinite list of conditions (more precisely, *quasi-identities*) that a monoid M must satisfy in order to be embeddable into a group. (Note that embeddability of M into a group is equivalent to the set of all elements of M being potentially invertible. Malcev's argument is reproduced in [9, Section VII.3]; see also [14] for an alternative perspective.) Apart from left and right cancellativity, the simplest of those conditions is the following (cf. Figure 3):

$$\forall\, p, q, r, s, P, Q, R, S \in M \quad ((PQ = pq \;\&\; RQ = rq \;\&\; RS = rs) \Rightarrow PS = ps). \tag{4.6}$$

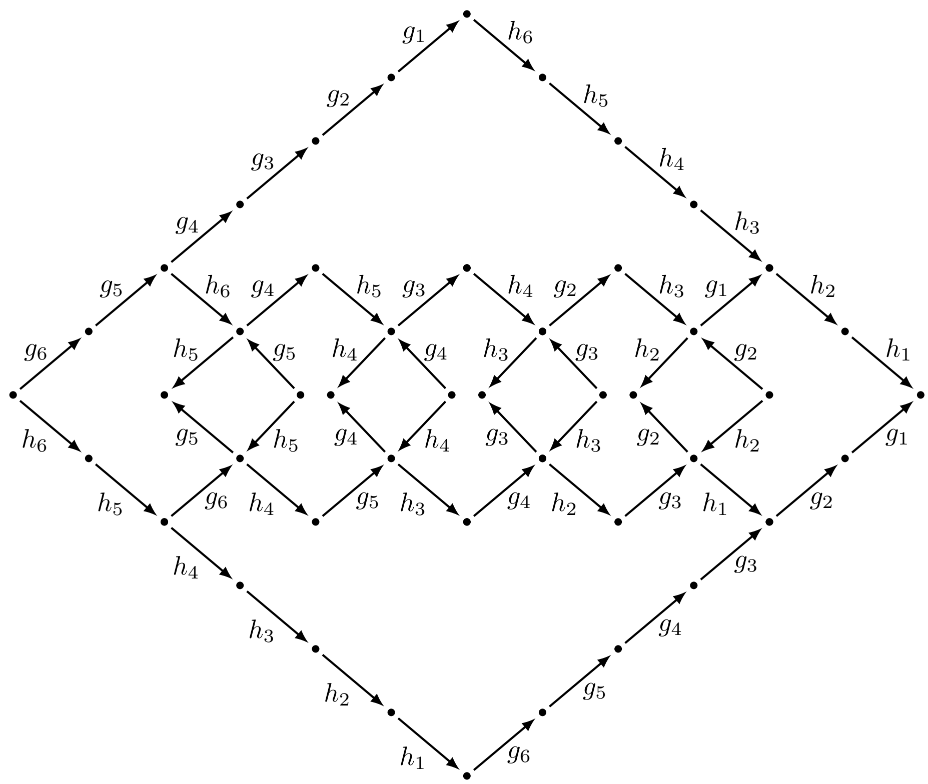

FIGURE 2. Proof of Theorem 4.4.

It turns out that Theorem 4.4 holds for any monoid satisfying condition (4.6). Curiously, neither cancellativity nor other Malcev's conditions are required.

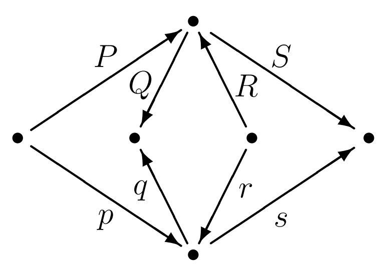

FIGURE 3. Dehn diagram illustrating Malcev's condition (4.6).

Theorem 4.7. *Let G be a group, and let $g_1, \ldots, g_N, h_1, \ldots, h_N \in G$ be such that for $1 < b < N$, we have:*

$$\text{if } z \in G \text{ commutes with } h_b^{-1} g_b, \text{ then } z \text{ commutes with both } g_b \text{ and } h_b. \tag{4.7}$$

Then the following are equivalent:

- $g_S h_S = h_S g_S$ *for all subsets* $S \subset \{1, \ldots, N\}$;
- $g_S h_S = h_S g_S$ *for all subsets* S *of cardinality* ≤ 3.

In Section 5, we show that condition (4.7) is satisfied in the setting of Theorem 2.5. This enables us to deduce the latter from Theorem 4.7.

The proof of Theorem 4.7 relies on two group-theoretic lemmas.

Lemma 4.8. *Let G be a group, and let $g_a, g_b, g_c, h_a, h_b, h_c \in G$ satisfy*

$$g_a h_a = h_a g_a, \qquad g_b h_b = h_b g_b, \qquad g_c h_c = h_c g_c, \tag{4.8}$$

$$g_b g_a h_b h_a = h_b h_a g_b g_a, \quad g_c g_a h_c h_a = h_c h_a g_c g_a, \quad g_c g_b h_c h_b = h_c h_b g_c g_b. \tag{4.9}$$

Then, if one of the following two relations holds in G, so does the other:

$$h_b^{-1} g_b (g_c^{-1} h_a g_c h_a^{-1}) = (g_c^{-1} h_a g_c h_a^{-1}) h_b^{-1} g_b; \tag{4.10}$$

$$g_c g_b g_a h_c h_b h_a = h_c h_b h_a g_c g_b g_a. \tag{4.11}$$

Proof. It suffices to observe that in the Dehn diagram in Figure 4,

- the outer face corresponds to the relation (4.11);
- the 12-gon in the middle corresponds to the relation (4.10);
- the other bounded faces correspond to relations (4.8)–(4.9). □

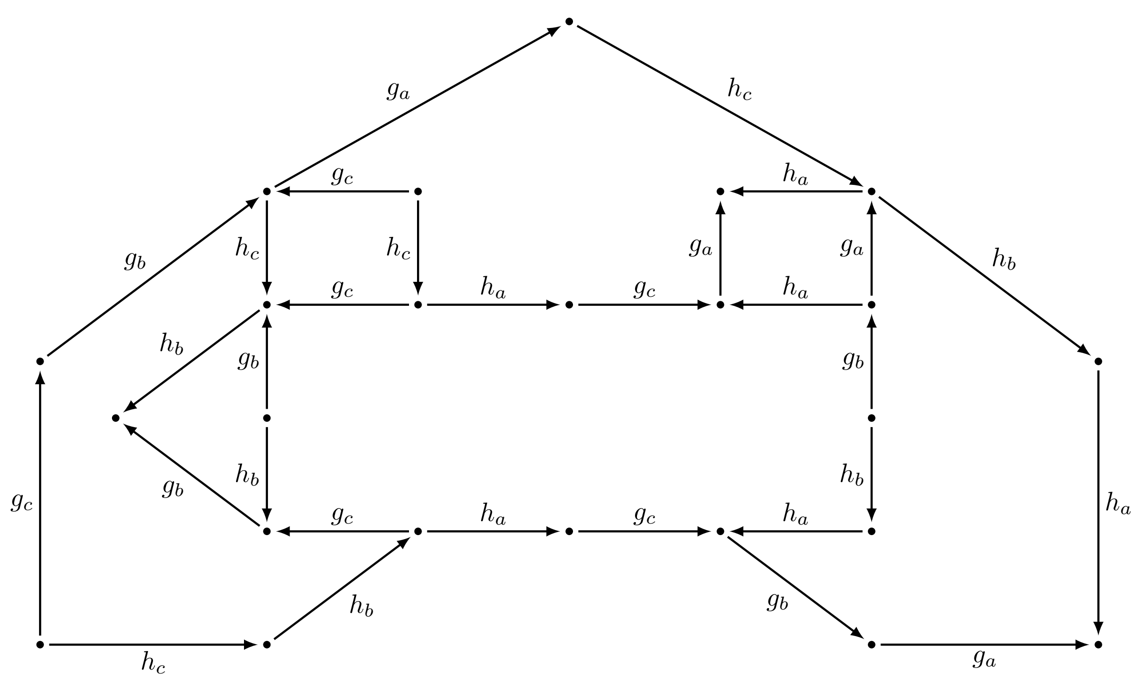

Figure 4. The proof of Lemma 4.8.

Lemma 4.9. *Let G be a group, and let $g_1, \ldots, g_N, h_1, \ldots, h_N \in G$ satisfy*

$$g_a h_a = h_a g_a \qquad \text{for all } 1 \le a \le N, \tag{4.12}$$

$$g_b g_a h_b h_a = h_b h_a g_b g_a \qquad \text{for all } 1 \le a < b \le N, \tag{4.13}$$

$$g_b (g_c^{-1} h_a g_c h_a^{-1}) = (g_c^{-1} h_a g_c h_a^{-1}) g_b \qquad \text{for all } 1 \le a < b < c \le N, \tag{4.14}$$

$$h_b^{-1} (g_c^{-1} h_a g_c h_a^{-1}) = (g_c^{-1} h_a g_c h_a^{-1}) h_b^{-1} \qquad \text{for all } 1 \le a < b < c \le N. \tag{4.15}$$

Then

$$g_N g_{N-1} \cdots g_1 h_N h_{N-1} \cdots h_1 = h_N h_{N-1} \cdots h_1 g_N g_{N-1} \cdots g_1. \tag{4.16}$$

Proof. Induction on N. The cases $N = 1$ and $N = 2$ are immediate from (4.12)–(4.13). The case $N = 3$ follows from Lemma 4.8 since the relations (4.14)–(4.15) imply (4.10).

Now assume $N \geq 4$. By the inductive hypothesis, the following relations hold:

$$g_{N-1}g_{N-2}\cdots g_2 h_{N-1}h_{N-2}\cdots h_2 = h_{N-1}h_{N-2}\cdots h_2 g_{N-1}g_{N-2}\cdots g_2. \tag{4.17}$$

$$g_{N-1}g_{N-2}\cdots g_1 h_{N-1}h_{N-2}\cdots h_1 = h_{N-1}h_{N-2}\cdots h_1 g_{N-1}g_{N-2}\cdots g_1. \tag{4.18}$$

$$g_N g_{N-1}\cdots g_2 h_N h_{N-1}\cdots h_2 = h_N h_{N-1}\cdots h_2 g_N g_{N-1}\cdots g_2. \tag{4.19}$$

It remains to verify that the relations (4.12)–(4.15) and (4.17)–(4.19) imply (4.16). The Dehn diagram in Figure 5 illustrates the argument in the case $N = 4$. In the diagram,

- the leftmost bounded face corresponds to the relation (4.19);
- the rightmost bounded face corresponds to the relation (4.18);
- the octagonal face on the left corresponds to the relation (4.17);
- the octagonal face at the top corresponds to the relation (4.13);
- the two quadrilateral faces correspond to the relation (4.12);
- the four inner rectangles correspond to the relations (4.14)–(4.15);
- and the outer face corresponds to (4.16).

The general case is similar, with N rectangles in the center. □

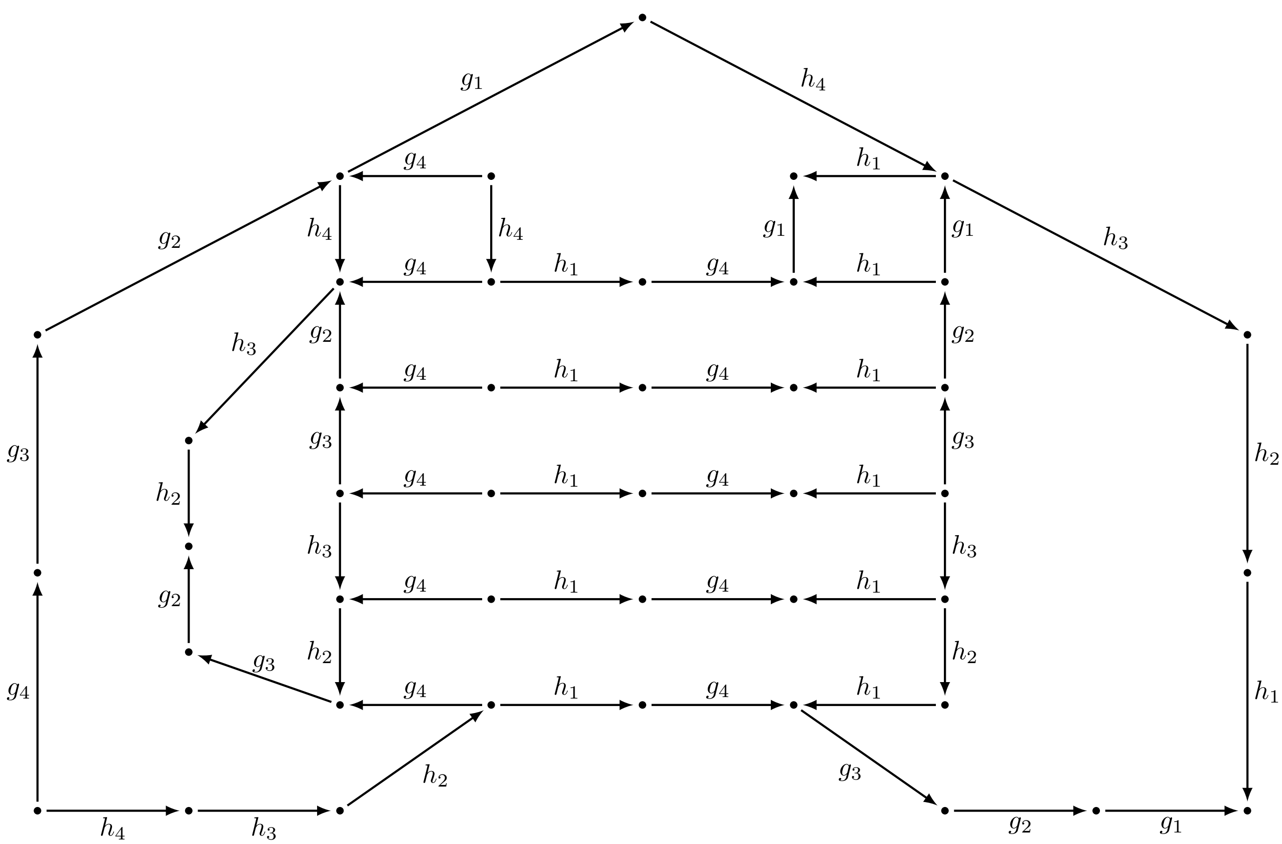

FIGURE 5. The proof of Lemma 4.9.

Proof of Theorem 4.7. For $1 \le a < b < c \le N$, conditions of Theorem 4.7 include (4.8), (4.9), and (4.11). By Lemma 4.8, relation (4.10) follows. In view of condition (4.7), we then obtain (4.14)–(4.15). Hence Lemma 4.9 applies, yielding (4.16), as desired. □

We conclude this section by slightly strengthening Theorem 4.7, see Corollary 4.11 below. This will require the following immediate consequence of Lemma 4.8.

Lemma 4.10. *Let G be a group, and let $g_a, g_b, g_c, h_a, h_b, h_c \in G$ satisfy*

$$g_a h_a = h_a g_a, \qquad g_b = h_b, \qquad g_c h_c = h_c g_c,$$
$$g_b g_a h_b h_a = h_b h_a g_b g_a, \quad g_c g_a h_c h_a = h_c h_a g_c g_a, \quad g_c g_b h_c h_b = h_c h_b g_c g_b.$$

Then $g_c g_b g_a h_c h_b h_a = h_c h_b h_a g_c g_b g_a$.

Corollary 4.11. *Let G be a group. Let $g_1, \dots, g_N, h_1, \dots, h_N \in G$ be such that for each $1 < b < N$, either $g_b = h_b$ or condition (4.7) holds. Then the following are equivalent:*

- *$g_S h_S = h_S g_S$ for all subsets $S \subset \{1, \dots, N\}$;*
- *$g_S h_S = h_S g_S$ for all subsets S of cardinality ≤ 3.*

Proof. Induction on N. For $N \le 3$, the result is clear. Now assume $N \ge 4$. If $g_b = h_b$ for some $b \in \{2, \dots, N-1\}$, then the claim

$$g_N \cdots g_1 h_N \cdots h_1 = h_N \cdots h_1 g_N \cdots g_1$$

follows by combining the induction assumption with Lemma 4.10, for $g_a = g_{b-1} \cdots g_1$, $g_c = g_N \cdots g_{b+1}$, $h_a = h_{b-1} \cdots h_1$, $h_c = h_N \cdots h_{b+1}$. In the only remaining case, condition (4.7) holds for all $b \in \{2, \dots, N-1\}$, and the claim follows from Theorem 4.7. □

5. Proofs of Theorems 2.5 and 2.12

We obtain Theorem 2.5 by combining Theorem 4.7 with Lemma 5.2 below. While Theorem 4.7 is purely group-theoretic, the proof of Lemma 5.2 implicitly relies on a Lagrange inversion argument for formal power series.

As before, we denote by $R[[x,y]]$ the ring of formal power series in x and y, with coefficients in the (unital) $\mathbb{Q}$-algebra R. We use the notation $R[[x,y]]^*$ for the multiplicative subgroup of $R[[x,y]]$ formed by power series with constant term 1. Thus the elements of $R[[x,y]]$ are formal expressions $z = \sum_{k=0}^{\infty} z_k$, with each $z_k \in R[x,y]$ a homogeneous polynomial of degree k in x and y, with coefficients in R. (From now on, we adopt the convention $\deg(x) = \deg(y) = 1$.) We have $z \in R[[x,y]]^*$ if and only if $z_0 = 1 \in R$.

Lemma 5.1. *Let $q \in \mathbb{Q}[[x,y]]$ and $r \in R[[x,y]]$, with $q \neq 0$ and $r \neq 0$. Then $qr \neq 0$.*

Proof. Define the lexicographic order $\prec$ on the monomials $x^i y^j$ by setting

$$x^i y^j \prec x^{i'} y^{j'} \overset{\text{def}}{\Longleftrightarrow} (i < i' \text{ or } (i = i' \text{ and } j < j')).$$

The statement of the lemma is true for $q \in \mathbb{Q}$ and $r \in R$. Consequently the leading term of the power series qr, with respect to the lexicographic order, is the product of the leading terms of q and r, respectively. The lemma follows. □

Lemma 5.2. *Let $\varphi_1, \varphi_2, \dots \in \mathbb{Q}[x,y]$ be homogeneous polynomials of degrees $\deg(\varphi_k) = k$. Assume that $\varphi_1 \neq 0$. Let $u \in R$, and let $f = 1+\varphi_1 u+\varphi_2 u^2+\cdots \in R[[x,y]]^*$. If f commutes with $z \in R[[x,y]]$, then u commutes with z.*

Proof. Let $z = z_0 + z_1 + z_2 + \cdots$, with $z_k \in R[x,y]$ a homogeneous polynomial of degree k. Then $[f,z] = [f-1,z] = \sum_{j\geq 1}\sum_{k\geq 0}\varphi_j[u^j,z_k]$. In order for this commutator to vanish, it must vanish in each degree. Since $\deg(\varphi_j[u^j,z_k]) = j+k$, we conclude that $\sum_{1\leq j\leq m}\varphi_j[u^j,z_{m-j}] = 0$ for every $m \geq 1$. So we have:

- $\varphi_1[u,z_0] = 0$ and $\varphi_1 \neq 0$, hence $[u,z_0] = 0$ (by Lemma 5.1);
- $\varphi_1[u,z_1] + \varphi_2[u^2,z_0] = \varphi_1[u,z_1] = 0$, hence $[u,z_1] = 0$;
- $\varphi_1[u,z_2] + \varphi_2[u^2,z_1] + \varphi_3[u^3,z_0] = \varphi_1[u,z_2] = 0$, hence $[u,z_2] = 0$;

and so on. We conclude that $[u,z] = [u, z_0 + z_1 + z_2 + \cdots] = 0$, as desired. ☐

Proof of Theorem 2.5. Let us denote

$$f_b = h_b^{-1}g_b = (1 - \beta_{b1}yu_b + \cdots)(1 + \alpha_{b1}xu_b + \cdots) = 1 + (\alpha_{b1}x - \beta_{b1}y)u_b + \cdots .$$

By Theorem 4.7, it suffices to verify that if f_b commutes with $z \in R[[x,y]]^*$, then so do both g_b and h_b. Indeed, we have $\alpha_{b1}x - \beta_{b1}y \neq 0$, so Lemma 5.2 applies; hence u_b commutes with z, and therefore so do g_b and h_b. ☐

Replacing Theorem 4.7 by Corollary 4.11 in the above argument, we obtain a stronger version of the Multiplicative Rule of Three:

Theorem 5.3. *Let R be a $\mathbb{Q}$-algebra, and let $u_1, \dots, u_N \in R$. Let $g_1, \dots, g_N, h_1, \dots, h_N \in R[[x,y]]^*$ be of the form*

$$g_i = 1 + \alpha_{i1}u_i + \alpha_{i2}u_i^2 + \alpha_{i3}u_i^3 + \cdots , \tag{5.1}$$

$$h_i = 1 + \beta_{i1}u_i + \beta_{i2}u_i^2 + \beta_{i3}u_i^3 + \cdots , \tag{5.2}$$

where $\alpha_{ik}, \beta_{ik} \in \mathbb{Q}[x,y]$ are homogeneous polynomials of degree k. Assume that for every $b \in \{2, \dots, N-1\}$, either $g_b = h_b$ or $\alpha_{b1} \neq \beta_{b1}$. Then the following are equivalent:

- *$g_S h_S = h_S g_S$ for all subsets $S \subset \{1, \dots, N\}$;*
- *$g_S h_S = h_S g_S$ for all subsets S of cardinality 2 and 3.*

Proof of Theorem 2.12. It suffices to note that the assumptions in Theorem 5.3 are satisfied when $g_i = 1+\alpha_{i1}u_i$ and $h_i = 1+\beta_{i1}u_i$, for any linear polynomials $\alpha_{i1}, \beta_{i1} \in \mathbb{Q}[x,y]$. ☐

6. Proof of Theorem 3.2

Lemma 6.1. *Let R be a ring, and let $g_a, g_b, v_a, v_b \in R$ satisfy*

$$[v_a, g_a] = [v_b, g_b] = 0,$$
$$[v_b + v_a, g_b g_a] = 0.$$

Then $[v_a, g_b]g_a = g_b[g_a, v_b]$.

Proof. This follows from the identity

$$[v_a, g_b]g_a - g_b[g_a, v_b] = [v_b + v_a, g_bg_a] - g_b[v_a, g_a] - [v_b, g_b]g_a\,. \qquad \square$$

Lemma 6.2. *Let R be a ring, and let $g_a, g_b, g_c, v_a, v_b, v_c \in R$ satisfy*

$$\begin{aligned}[v_b, g_b] &= 0,\\ [v_b + v_a, g_bg_a] = [v_c + v_b, g_cg_b] &= 0,\\ [v_c + v_b + v_a, g_cg_bg_a] &= 0.\end{aligned}$$

Then $[v_a, g_c]g_bg_a = g_cg_b[g_a, v_c]$.

Proof. This follows from the identity

$$\begin{aligned}&[v_a, g_c]g_bg_a - g_cg_b[g_a, v_c]\\ &= [v_c + v_b + v_a, g_cg_bg_a] - g_c[v_b + v_a, g_bg_a] - [v_c + v_b, g_cg_b]g_a + g_c[v_b, g_b]g_a\,. \qquad \square\end{aligned}$$

Lemma 6.3. *Let R be a monoid (or a ring), and let $g_1, \dots, g_m, z, z' \in R$ satisfy*

$$zg_1 = g_mz', \tag{6.1}$$

$$zg_bg_1 = g_mg_bz' \qquad \text{for all } 1 < b < m. \tag{6.2}$$

If g_1 and g_m are potentially invertible, then

$$zg_{m-1}g_{m-2}\cdots g_1 = g_mg_{m-1}\cdots g_2z'. \tag{6.3}$$

Proof. Passing to an extension of R wherein g_1 and g_m have inverses, let us denote $r = g_m^{-1}z = z'g_1^{-1}$ (cf. (6.1)). Condition (6.2) means that r commutes with g_b for $1<b<m$. Hence r commutes with $g_{m-1}\cdots g_2$, which is nothing but (6.3). $\square$

Corollary 6.4. *Let R be a ring and let $v_1, \dots, v_N, g_1, \dots, g_N \in R$ with $g_1, \dots, g_N$ potentially invertible. Suppose*

$$[\textstyle\sum_{i\in S} v_i, g_S] = 0 \text{ for all } S \subset \{1, \dots, N\} \text{ of cardinality} \le 3.$$

Then for each subset $S = \{s_1 < \cdots < s_m\} \subset \{1, \dots, N\}$,

$$[v_{s_1}, g_{s_m}]g_{s_{m-1}}g_{s_{m-2}}\cdots g_{s_1} = g_{s_m}g_{s_{m-1}}\cdots g_{s_2}[g_{s_1}, v_{s_m}].$$

Proof. Apply Lemmas 6.1, 6.2, and 6.3, with $z = [v_{s_1}, g_{s_m}]$ and $z' = [g_{s_1}, v_{s_m}]$. $\square$

Proof of Theorem 3.2. We need to show that relations

$$[v_a, g_a] = 0 \qquad \text{for all } 1 \le a \le N; \tag{6.4}$$

$$[v_b + v_a, g_bg_a] = 0 \qquad \text{for all } 1 \le a < b \le N; \tag{6.5}$$

$$[v_c + v_b + v_a, g_cg_bg_a] = 0 \qquad \text{for all } 1 \le a < b < c \le N \tag{6.6}$$

imply $[v_{s_m} + v_{s_{m-1}} + \cdots + v_{s_1}, g_S] = 0$ for any subset $S = \{s_1 < \cdots < s_m\} \subset \{1, \ldots, N\}$. We establish this claim by induction on $m = |S|$. The cases $m \leq 3$ are covered by (6.4)–(6.6). Using the induction assumption and the Leibniz rule for commutators, we get:

$$\begin{aligned}
&[v_{s_m} + v_{s_{m-1}} + \cdots + v_{s_1}, g_{s_m} \cdots g_{s_1}] \\
&= [(v_{s_m} + \cdots + v_{s_2}) + (v_{s_{m-1}} + \cdots + v_{s_1}) - (v_{s_{m-1}} + \cdots + v_{s_2}), g_{s_m} \cdots g_{s_1}] \\
&= [v_{s_m} + \cdots + v_{s_2}, g_{s_m} \cdots g_{s_2}] g_{s_1} + g_{s_m} \cdots g_{s_2} [v_{s_m} + \cdots + v_{s_2}, g_{s_1}] \\
&+ [v_{s_{m-1}} + \cdots + v_{s_1}, g_{s_m}] g_{s_{m-1}} \cdots g_{s_1} + g_{s_m} [v_{s_{m-1}} + \cdots + v_{s_1}, g_{s_{m-1}} \cdots g_{s_1}] \\
&- [v_{s_{m-1}} + \cdots + v_{s_2}, g_{s_m}] g_{s_{m-1}} \cdots g_{s_1} - g_{s_m} [v_{s_{m-1}} + \cdots + v_{s_2}, g_{s_{m-1}} \cdots g_{s_2}] g_{s_1} \\
&\qquad - g_{s_m} \cdots g_{s_2} [v_{s_{m-1}} + \cdots + v_{s_2}, g_{s_1}] \\
&= [v_{s_1}, g_{s_m}] g_{s_{m-1}} \cdots g_{s_1} - g_{s_m} \cdots g_{s_2} [g_{s_1}, v_{s_m}] \\
&= 0,
\end{aligned}$$

where the last equality is by Corollary 6.4. □

Proof of Theorem 3.3. This theorem is proved by exactly the same argument as the one used for Theorem 3.2. □

7. Proofs of Theorems 1.1, 3.4, 3.5, 3.10, and 3.11

Lemma 7.1. *Let R be a ring, and let $g_a, g_b, g_c, h_a, h_b, h_c \in R$, with h_b potentially invertible, satisfy the relations*

$$g_b h_b = h_b g_b, \tag{7.1}$$

$$g_b g_a h_b h_a = h_b h_a g_b g_a, \tag{7.2}$$

$$g_c g_b h_c h_b = h_c h_b g_c g_b. \tag{7.3}$$

Then the following are equivalent:

$$g_c g_b g_a h_c h_b h_a = h_c h_b h_a g_c g_b g_a,$$

$$g_c g_b [g_a, h_c] h_b h_a = h_c h_b [h_a, g_c] g_b g_a.$$

Proof. The statement follows from the identity (in the appropriate extension of R):

$$\begin{aligned}
[g_c g_b g_a, h_c h_b h_a] &= g_c g_b [g_a, h_c] h_b h_a - h_c h_b [h_a, g_c] g_b g_a \\
&\quad + [g_c g_b, h_c h_b] h_b^{-1} g_a h_b h_a + h_c h_b g_c h_b^{-1} ([g_b g_a, h_b h_a] - [g_b, h_b] h_b^{-1} g_a h_b h_a).
\end{aligned} \tag{7.4}$$

□

Lemma 7.2. *Let R be a ring, and let $g_a, g_b, g_c, h_a, h_b, h_c$ be potentially invertible elements of R satisfying* (7.1)–(7.3)*. Then any two of the following conditions imply the third:*

$$g_c g_b g_a h_c h_b h_a = h_c h_b h_a g_c g_b g_a,$$

$$g_c g_b [g_a, h_c] = [h_a, g_c] g_b g_a,$$

$$h_c h_b [h_a, g_c] = [h_a, g_c] h_b h_a.$$

Proof. Adding the trivial identity

$$0 = -[h_a, g_c]g_b g_a h_b h_a + [h_a, g_c]h_b h_a g_b g_a + [h_a, g_c][g_b g_a, h_b h_a]$$

to (7.4), we obtain

$$[g_c g_b g_a, h_c h_b h_a] = (g_c g_b[g_a, h_c] - [h_a, g_c]g_b g_a)h_b h_a - (h_c h_b[h_a, g_c] - [h_a, g_c]h_b h_a)g_b g_a$$
$$+[h_a, g_c][g_b g_a, h_b h_a]+[g_c g_b, h_c h_b]h_b^{-1}g_a h_b h_a+h_c h_b g_c h_b^{-1}([g_b g_a, h_b h_a]-[g_b, h_b]h_b^{-1}g_a h_b h_a),$$

and the claim follows. □

Lemma 7.3. *Let R be a (unital) ring, and let g_a, g_b, h_a, h_b be potentially invertible elements of R satisfying $g_a h_a = h_a g_a$ and $g_b h_b = h_b g_b$. Then any two of the following conditions imply the third:*

$$g_b g_a h_b h_a = h_b h_a g_b g_a,$$
$$g_b[g_a, h_b] = [h_a, g_b]g_a,$$
$$h_b[h_a, g_b] = [h_a, g_b]h_a.$$

Proof. This is the $g_b = h_b = 1$ case of Lemma 7.2, with a suitable change of notation. □

Theorem 7.4 below, although not a "Rule of Three," is a powerful result which will be used to prove Theorems 3.4 and 3.5.

Theorem 7.4. *Let $g_1, \dots, g_N, h_1, \dots, h_N$ be potentially invertible elements of a ring R satisfying the relations*

$$g_a h_a = h_a g_a \qquad \text{for all } 1 \le a \le N; \tag{7.5}$$
$$g_b[g_a, h_b] = [h_a, g_b]g_a \qquad \text{for all } 1 \le a < b \le N; \tag{7.6}$$
$$g_c g_b[g_a, h_c] = [h_a, g_c]g_b g_a \qquad \text{for all } 1 \le a < b < c \le N; \tag{7.7}$$
$$h_b[h_a, g_b] = [h_a, g_b]h_a \qquad \text{for all } 1 \le a < b \le N; \tag{7.8}$$
$$h_c h_b[h_a, g_c] = [h_a, g_c]h_b h_a \qquad \text{for all } 1 \le a < b < c \le N. \tag{7.9}$$

Then $g_S h_S = h_S g_S$ for any $S \subset \{1, \dots, N\}$.

Proof. First, we claim that for any subset $S=\{s_1 < \cdots < s_m\} \subset \{1, \dots, N\}$, one has

$$[h_{s_1}, g_{s_m}]g_{s_{m-1}}g_{s_{m-2}} \cdots g_{s_1} = g_{s_m}g_{s_{m-1}} \cdots g_{s_2}[g_{s_1}, h_{s_m}]. \tag{7.10}$$

This follows by applying Lemma 6.3 with $z = [h_{s_1}, g_{s_m}]$ and $z' = [g_{s_1}, h_{s_m}]$. (Conditions (6.1)–(6.2) hold by (7.6)–(7.7).) Again applying Lemma 6.3, this time with $z = z' = [h_{s_1}, g_{s_m}]$ (and relying on (7.8)–(7.9)), we get

$$[h_{s_1}, g_{s_m}]h_{s_{m-1}}h_{s_{m-2}} \cdots h_{s_1} = h_{s_m}h_{s_{m-1}} \cdots h_{s_2}[h_{s_1}, g_{s_m}]. \tag{7.11}$$

We now prove $g_S h_S = h_S g_S$ by induction on $m = |S|$. The base case $m = 1$ is given in (7.5). It remains to invoke Lemma 7.2 with

$$g_a = g_{s_1}, \quad g_b = g_{s_{m-1}} \cdots g_{s_2}, \quad g_c = g_{s_m},$$
$$h_a = h_{s_1}, \quad h_b = h_{s_{m-1}} \cdots h_{s_2}, \quad h_c = h_{s_m},$$

making use of (7.10) and (7.11). □

Proof of Theorem 3.4. We need to show that relations

$$g_a h_a = h_a g_a \qquad \text{for all } 1 \le a \le N; \tag{7.12}$$
$$g_b g_a h_b h_a = h_b h_a g_b g_a \qquad \text{for all } 1 \le a < b \le N; \tag{7.13}$$
$$g_c g_b g_a h_c h_b h_a = h_c h_b h_a g_c g_b g_a \qquad \text{for all } 1 \le a < b < c \le N; \tag{7.14}$$
$$g_b g_a (h_b + h_a) = (h_b + h_a) g_b g_a \qquad \text{for all } 1 \le a < b \le N; \tag{7.15}$$
$$g_c g_b g_a (h_c + h_b + h_a) = (h_c + h_b + h_a) g_c g_b g_a \qquad \text{for all } 1 \le a < b < c \le N \tag{7.16}$$

imply $g_S h_S = h_S g_S$ for all subsets S. (The other conclusion is by Theorem 3.2.) By Theorem 7.4, the claim will follow once we have checked conditions (7.5)–(7.9).

Relation (7.12) is the same as (7.5). By Lemma 6.1, relations (7.12) and (7.15) imply (7.6). By Lemma 6.2, relations (7.12) and (7.15)–(7.16) imply (7.7). Finally, by Lemmas 7.2–7.3, relations (7.6)–(7.7) and (7.12)–(7.14) imply (7.8)–(7.9). □

Corollary 7.5. *Let $g_1, \dots, g_N, h_1, \dots, h_N$ be potentially invertible elements of a ring R satisfying*

$$[g_a, h_b] = [h_a, g_b] \qquad \textit{for all } 1 \le a < b \le N; \tag{7.17}$$
$$[g_a, h_a] = 0 \qquad \textit{for all } 1 \le a \le N; \tag{7.18}$$
$$g_b [g_a, h_b] = [h_a, g_b] g_a \qquad \textit{for all } 1 \le a < b \le N; \tag{7.19}$$
$$g_c g_b [g_a, h_c] = [h_a, g_c] g_b g_a \qquad \textit{for all } 1 \le a < b < c \le N; \tag{7.20}$$
$$h_b [h_a, g_b] = [g_a, h_b] h_a \qquad \textit{for all } 1 \le a < b \le N; \tag{7.21}$$
$$h_c h_b [h_a, g_c] = [g_a, h_c] h_b h_a \qquad \textit{for all } 1 \le a < b < c \le N. \tag{7.22}$$

Then $g_S h_S = h_S g_S$ for any $S \subset \{1, \dots, N\}$.

Proof. Substitute (7.17) into (7.21)–(7.22) to get (7.8)–(7.9); then apply Theorem 7.4. □

Proof of Theorem 3.5. We will use Corollary 7.5 to show that (3.4)–(3.9) imply $g_S h_S = h_S g_S$ for all subsets S. (The other conclusions are by Theorem 3.2 and Remark 3.6.) Relations (7.17)–(7.18) are equivalent to (3.4)–(3.5). Relations (7.19)–(7.20) (which are identical to (7.6)–(7.7)) are checked precisely as in the proof of Theorem 3.4, using (3.6)–(3.7) and Lemmas 6.1–6.2. In the same way, we use (3.8)–(3.9) to obtain (7.21)–(7.22). □

Proof of Theorem 1.1. Set $g_i = 1 + x u_i$ and $h_i = 1 + y v_i$ for $i = 1, \dots, N$. (Here, as before, we are operating in the ring of formal power series in two variables x and y.) Then the g_i and the h_i are invertible. Furthermore, the relations (1.4)–(1.8) imply the relations (3.4)–(3.9). Applying Theorem 3.5, we conclude that $g_S h_S = h_S g_S$ for any $S \subset \{1, \dots, N\}$. Equivalently, $e_k(\mathbf{u}_S) e_\ell(\mathbf{v}_S) = e_\ell(\mathbf{v}_S) e_k(\mathbf{u}_S)$ for all k, ℓ, as desired. □

Proof of Theorem 3.11. Set $h_i = 1 + y f_i \in R[y]$; here, as before, y is a formal variable commuting with all elements of R. One then checks that the two statements in Theorem 3.4 translate into the respective statements in Theorem 3.11. The claim follows. □

Proof of Theorem 3.10. Same argument as above, this time with $h_i = 1 + y f_i \in R[y]/(y^3)$. □

We conclude this section with additional results on the Multiplicative Rule of Three, cf. Definition 2.8.

Corollary 7.6. *The Multiplicative Rule of Three holds for* $g_i = 1 + \alpha_{i1}x + \alpha_{i2}x^2 + \cdots$ *and* $h_i = 1 + yv_i$*, for any* $\alpha_{ik} \in \mathcal{A} = \mathbb{Q}\langle u_1, \ldots, u_M, v_1, \ldots, v_M\rangle$.

Proof. Let I be an ideal in $\mathcal{A}$, and let $I[[x, y]]$ be the ideal generated by I inside $\mathcal{A}[[x, y]]$. Suppose $[g_S, h_S] \equiv 0 \bmod I[[x, y]]$ for all $|S| \leq 3$. Taking the coefficient of y, we get $[g_S, \sum_{i\in S} v_i] \equiv 0 \bmod I[[x, y]]$ and consequently $[g_S, \sum_{i\in S} h_i] \equiv 0 \bmod I[[x, y]]$. It remains to apply Theorem 3.4 (with $R = \mathcal{A}[[x, y]]/I[[x, y]]$). □

One can more generally identify specific conditions on the β_{ij} in Conjecture 2.3 which ensure that $g_S(\sum_{i\in S} h_i) = (\sum_{i\in S} h_i)g_S$ for all $|S| \leq 3$. Here is one example.

Corollary 7.7. *The Multiplicative Rule of Three holds for* $g_i = 1 + \alpha_{i1}x + \alpha_{i2}x^2 + \cdots$ *and* $h_i = 1 + \beta_{i1}yv_i + \beta_{i4}y^4v_i^4$*, for any* $\alpha_{ik} \in \mathcal{A}$ *and* $\beta_{i1}, \beta_{i4} \in \mathbb{Q}$.

Proof. Same argument as above, this time noting that for $d = 1, 4$ and $|S| \leq 3$, taking the coefficient of y^d in $[g_S, h_S] \equiv 0$ yields $[g_S, \sum_{i\in S} \beta_{id}v_i^d] \equiv 0$. □

8. Proof of Theorem 1.6

We will need the following slight generalization of Lemma 7.2.

Lemma 8.1. *Let R be a ring, and let $g_a, g_b, g_c, h_a, h_b, h_c$ be potentially invertible elements of R satisfying* (7.1)–(7.3)*. Let $z \in R$. Then any two of the following conditions imply the third:*

$$\begin{aligned} g_cg_bg_ah_ch_bh_a &= h_ch_bh_ag_cg_bg_a, \\ g_cg_b[g_a, h_c] &= zg_bg_a, \\ h_ch_b[h_a, g_c] &= zh_bh_a. \end{aligned}$$

Proof. This follows from a modified version of the identity in the proof of Lemma 7.2:

$$\begin{aligned} &[g_cg_bg_a, h_ch_bh_a] = (g_cg_b[g_a, h_c] - zg_bg_a)h_bh_a - (h_ch_b[h_a, g_c] - zh_bh_a)g_bg_a \\ &+ z[g_bg_a, h_bh_a] + [g_cg_b, h_ch_b]h_b^{-1}g_ah_bh_a + h_ch_bg_ch_b^{-1}([g_bg_a, h_bh_a] - [g_b, h_b]h_b^{-1}g_ah_bh_a). \end{aligned}$$ □

Lemma 8.2. *Let A be a ring, and let $u_1, \ldots, u_N, v_1, \ldots, v_N \in A$ satisfy*

$$[u_a, v_b] = [v_a, u_b] \quad \text{for all } 1 \leq a < b \leq N. \tag{8.1}$$

For every $i \in \{1, \ldots, N\}$, let α_i, β_i be central elements of A such that $1+\alpha_iu_i$ and $1+\beta_iv_i$ are invertible, and define $g_i, h_i \in A$ by making one of the following two choices:

$$\text{either} \quad \begin{cases} g_i = 1 + \alpha_iu_i\,, \\ h_i = 1 + \beta_iv_i\,, \end{cases} \quad \text{or} \quad \begin{cases} g_i = (1 + \alpha_iu_i)^{-1}\,, \\ h_i = (1 + \beta_iv_i)^{-1}\,. \end{cases} \tag{8.2}$$

Suppose that the following relations are satisfied:

$$[v_a, g_a] = 0 \qquad \textit{for all } 1 \le a \le N; \tag{8.3}$$

$$[v_b + v_a, g_b g_a] = 0 \qquad \textit{for all } 1 \le a < b \le N; \tag{8.4}$$

$$[v_c + v_b + v_a, g_c g_b g_a] = 0 \qquad \textit{for all } 1 \le a < b < c \le N; \tag{8.5}$$

$$[u_a, h_a] = 0 \qquad \textit{for all } 1 \le a \le N; \tag{8.6}$$

$$[u_b + u_a, h_b h_a] = 0 \qquad \textit{for all } 1 \le a < b \le N; \tag{8.7}$$

$$[u_c + u_b + u_a, h_c h_b h_a] = 0 \qquad \textit{for all } 1 \le a < b < c \le N. \tag{8.8}$$

Then $g_N g_{N-1} \cdots g_1 \, h_N h_{N-1} \cdots h_1 = h_N h_{N-1} \cdots h_1 \, g_N g_{N-1} \cdots g_1$.

Lemma 8.2 can be thought of as a fancy version of Theorem 3.5.

Proof. Let $P(m, n)$ be the statement of the lemma with 1 and N replaced by m and n, respectively. We will prove $P(m, n)$ by induction on $n-m$. The case $n = m$ is the relation

$$[g_a, h_a] = 0 \quad \text{for all } 1 \le a \le N, \tag{8.9}$$

which is immediate from (8.2) and (8.3) (or (8.6)). Now assume $m < n$.

First notice that $P(m, n)$ is equivalent to $P(m, n)$ with g^{-1}_{m+n-i} in place of g_i, h^{-1}_{m+n-i} in place of h_i, and u_{m+n-i} (resp., v_{m+n-i}, α_{m+n-i}, β_{m+n-i}) in place of u_i (resp., v_i, α_i, β_i). For instance, $[v_c + v_b + v_a, g_c g_b g_a] = 0$ is equivalent to $[v_c + v_b + v_a, g_a^{-1} g_b^{-1} g_c^{-1}] = 0$; the set of these relations over all $m \le a < b < c \le n$ is identical to the relations $[v_{n+m-c} + v_{n+m-b} + v_{n+m-a}, g^{-1}_{n+m-c} g^{-1}_{n+m-b} g^{-1}_{n+m-a}] = 0$ over all $m \le a < b < c \le n$.

By the previous paragraph, we may assume that at least one of the following holds:

$$g_m = 1 + \alpha_m u_m \text{ and } h_m = 1 + \beta_m v_m; \tag{8.10}$$

$$g_n = 1 + \alpha_n u_n \text{ and } h_n = 1 + \beta_n v_n. \tag{8.11}$$

Let us assume (8.11), as the case of (8.10) is handled similarly. By (8.1) and (8.11), we have

$$\alpha_n [u_m, h_n] = \alpha_n \beta_n [u_m, v_n] = \alpha_n \beta_n [v_m, u_n] = \beta_n [v_m, g_n]. \tag{8.12}$$

By Corollary 6.4, the relations (8.3)–(8.8) imply

$$g_n g_{n-1} \cdots g_{m+1} [g_m, v_n] = [v_m, g_n] g_{n-1} g_{n-2} \cdots g_m, \tag{8.13}$$

$$h_n h_{n-1} \cdots h_{m+1} [h_m, u_n] = [u_m, h_n] h_{n-1} h_{n-2} \cdots h_m. \tag{8.14}$$

Next multiply (8.13), (8.14) by β_n, α_n, respectively, and apply (8.11) and (8.12) to obtain

$$g_n g_{n-1} \cdots g_{m+1} [g_m, h_n] = \beta_n [v_m, g_n] g_{n-1} g_{n-2} \cdots g_m, \tag{8.15}$$

$$h_n h_{n-1} \cdots h_{m+1} [h_m, g_n] = \beta_n [v_m, g_n] h_{n-1} h_{n-2} \cdots h_m. \tag{8.16}$$

Now $P(m, n)$ follows by applying Lemma 8.1 with $g_a = g_m$, $g_b = g_{n-1} \cdots g_{m+1}$, $g_c = g_n$, $h_a = h_m$, $h_b = h_{n-1} \cdots h_{m+1}$, $h_c = h_n$, $z = \beta_n [v_m, g_n]$, making use of (8.15)–(8.16) and the induction assumption. □

Proof of Theorem 1.6. The statement is proved by applying Lemma 8.2 with $A = R[[x,y]]$ and g_i, h_i given by

$$g_i = \begin{cases} 1 + xu_i & \text{if } i \text{ is unbarred} \\ (1 - xu_i)^{-1} & \text{if } i \text{ is barred,} \end{cases} \qquad h_i = \begin{cases} 1 + yv_i & \text{if } i \text{ is unbarred} \\ (1 - yv_i)^{-1} & \text{if } i \text{ is barred.} \end{cases} \tag{8.17}$$

(Thus $\alpha_i = x, \beta_i = y$ if i is unbarred and $\alpha_i = -x, \beta_i = -y$ if i is barred.)

We verify the relation (8.1) using the $|S| \leq 2$, $k = 1$ cases of (1.18):

$$[u_a, v_b] - [v_a, u_b] = [u_b + u_a, v_b + v_a] - [u_a, v_a] - [u_b, v_b] = 0.$$

The remaining relations (8.3)–(8.8) follow from (1.18)–(1.19), using the fact that

$$g_S = \textstyle\sum_k x^k \, \overline{e}_k(\mathbf{u}_S),$$
$$h_S = \textstyle\sum_\ell y^\ell \, \overline{e}_\ell(\mathbf{v}_S),$$

for any $S \subset \{1, \ldots, N\}$. So Lemma 8.2 applies, and Theorem 1.6 follows. □

Acknowledgments. We thank the participants of the conference *Lie and Jordan Algebras VI* (Bento Gonçalves, December 2015) for stimulating discussions. We thank Elaine So for help typing and typesetting figures and the anonymous referee for a number of helpful comments.

References

[1] S. H. Assaf, Dual equivalence graphs and a combinatorial proof of LLT and Macdonald positivity, `arXiv:1005.3759v5`, October 2013.

[2] C. Benedetti and N. Bergeron, Fomin-Greene monoids and Pieri operations, *Algebraic monoids, group embeddings, and algebraic combinatorics*, Fields Inst. Commun. **71**, 305–338, Springer, 2014.

[3] J. Blasiak, Kronecker coefficients for one hook shape, `arXiv:1209.2018`.

[4] J. Blasiak, What makes a D_0 graph Schur positive? *J. Algebraic Combin.* (2016), 1–51.

[5] J. Blasiak, Haglund's conjecture on 3-column Macdonald polynomials, *Math. Z.* **283** (2016), 601–628.

[6] J. Blasiak and S. Fomin, Noncommutative Schur functions, switchboards, and Schur positivity, `arXiv:1510.00657`, to appear in *Selecta Math.*

[7] J. Blasiak and R. I. Liu, Kronecker coefficients and noncommutative super Schur functions, `arXiv:1510.00644`.

[8] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[9] P. M. Cohn, *Universal algebra*, Dordrecht, 1981.

[10] S. Fomin and C. Greene, Noncommutative Schur functions and their applications, *Discrete Math.* **193** (1998), 179–200.

[11] A. N. Kirillov, Notes on Schubert, Grothendieck and key polynomials, *SIGMA* **12** (2016), 57 pp.

[12] T. Lam, Affine Stanley symmetric functions, *Amer. J. Math.* **128** (2006), 1553–1586.

[13] T. Lam, Ribbon Schur operators, *European J. Combin.* **29** (2008), 343–359.

[14] J. Lambek, The immersibility of a semigroup into a group, *Canadian J. Math.* **3** (1951), 34–43.

[15] A. Lascoux and M.-P. Schützenberger, Le monoïde plaxique, *Noncommutative structures in algebra and geometric combinatorics (Naples, 1978)*, 129–156, Quad. "Ricerca Sci.", 109, CNR, 1981.

[16] R. I. Liu, A simplified Kronecker rule for one hook shape. `arXiv:1412.2180`.

[17] A. Malcev, On embedding of associative systems into groups [*in Russian*], *Mat. Sbornik N.S.* **6** (48) (1939), 331–336.

[18] A. Malcev, On embedding of associative systems into groups. II [*in Russian*], *Mat. Sbornik N.S.* **8** (50) (1940), 251–264.

[19] J.-C. Novelli and A. Schilling, The forgotten monoid, *Combinatorial representation theory and related topics*, 71–83, RIMS Kôkyûroku Bessatsu, B8, Res. Inst. Math. Sci. (RIMS), Kyoto, 2008.

[20] D. Peifer, Max Dehn and the origins of topology and infinite group theory, *Amer. Math. Monthly* **122** (2015), 217–233.

[21] M.-P. Schützenberger, La correspondance de Robinson, *Combinatoire et représentation du groupe symétrique*, 59–113, Lecture Notes in Math., 579, Springer, Berlin, 1977.

[22] R. P. Stanley, *Enumerative combinatorics, vol. 2*, Cambridge University Press, Cambridge, 1999.

Department of Mathematics, Drexel University, Philadelphia, PA 19104

E-mail address: jblasiak@gmail.com

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109

E-mail address: fomin@umich.edu