On the support of the free Lie algebra: the Schützenberger problems

Ioannis C. Michos

Department of Mathematics, University of Ioannina, GR-451 10, Ioannina, Greece. E-mail: `imichos@uoi.gr`

received 20 July 2008, *accepted 5 April 2010*.

M.-P. Schützenberger asked to determine the support of the free Lie algebra $\mathcal{L}_{\mathbb{Z}_m}(A)$ on a finite alphabet A over the ring $\mathbb{Z}_m$ of integers $\bmod m$ and all pairs of *twin* and *anti-twin* words, i.e., words that appear with equal (resp. opposite) coefficients in each Lie polynomial. We characterize the complement of the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$ in A^* as the set of all words w such that m divides all the coefficients appearing in the monomials of $l^*(w)$, where l^* is the adjoint endomorphism of the left normed Lie bracketing l of the free Lie ring. Calculating $l^*(w)$ via the *shuffle product*, we recover the well known result of Duchamp and Thibon (Discrete Math. 76 (1989) 123-132) for the support of the free Lie ring in a much more natural way. We conjecture that two words u and v of common length n, which lie in the support of the free Lie ring, are twin (resp. anti-twin) if and only if either $u = v$ or n is odd and $u = \tilde{v}$ (resp. if n is even and $u = \tilde{v}$), where $\tilde{v}$ denotes the reversal of v and we prove that it suffices to show this for a two-lettered alphabet. These problems can be rephrased, for words of length n, in terms of the action of the Dynkin operator l_n on λ-tabloids, where λ is a *partition* of n. Representing a word w in two letters by the subset I of $[n] = \{1, 2, \dots, n\}$ that consists of all positions that one of the letters occurs in w, the computation of $l^*(w)$ leads us to the notion of the *Pascal descent polynomial* $p_n(I)$, a particular commutative multi-linear polynomial which is equal to the signed binomial coefficient when $|I| = 1$. We provide a recursion formula for $p_n(I)$ and show that if $m \nmid \sum_{i \in I} (-1)^{i-1} \binom{n-1}{i-1}$, then w lies in the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$.

Keywords: Free Lie algebras; Pascal triangle $\bmod m$; shuffle product; set partitions; λ-tabloids.

1 Introduction

Let A be a finite alphabet, A^* be the *free monoid* on A and $A^+ = A^* \setminus \{\epsilon\}$ be the *free semigroup* on A, with ϵ denoting the empty word. For a word $w \in A^*$ let $|w|$ denote its length, $|w|_a$ denote the number of occurrences of the letter $a \in A$ in w and let $alph(w)$ be the set of all letters actually occurring in w.

Let K be a commutative ring with unity. For most of our purposes $K = \mathbb{Z}_m$, the ring $\mathbb{Z}/(m)$ of integers $\bmod m$ for a non-negative integer m. Let $K\langle A\rangle$ be the *free associative algebra* on A over K. Its elements are polynomials on non-commuting variables from A and coefficients from K. Each polynomial $P \in K\langle A\rangle$ is written in the form $P = \sum_{w \in A^*} (P, w)\, w$, where (P, w) denotes the coefficient of the word w in P. Given two polynomials $P, Q \in K\langle A\rangle$, their Lie product is the Lie bracket $[P, Q] = PQ - QP$.

1365–8050 © 2010 Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

In this way $K\langle A\rangle$ is given a Lie structure. It can be proved (see e.g., [14, Theorem 0.5]) that the *free Lie algebra* $\mathcal{L}_K(A)$ on A over K is equal to the Lie subalgebra of $K\langle A\rangle$ generated by A. When K is the ring $\mathbb{Z}$ of rational integers, $\mathcal{L}_K(A)$ is also known as the *free Lie ring*. A *Lie monomial* is an element of $\mathcal{L}_K(A)$ formed by Lie products of the elements $a \in A$. A *Lie polynomial* is a linear combination of Lie monomials, i.e., an arbitrary element of $\mathcal{L}_K(A)$. The *support* of $\mathcal{L}_K(A)$ is the subset of A^* consisting of those words that appear (with a non-zero coefficient) in some Lie polynomial. A pair of words u, v is called *twin* (respectively *anti-twin*) if both words appear with equal (respectively opposite) coefficients in each Lie polynomial over K.

M.-P. Schützenberger had posed the following problems (pointed to us in a private communication with G. Duchamp):

Problem 1.1 *Determine the support of the free Lie ring* $\mathcal{L}_{\mathbb{Z}}(A)$.

Problem 1.2 *Determine the support of* $\mathcal{L}_{\mathbb{Z}_m}(A)$, *for* $m > 1$.

Problem 1.3 *Determine all twin and anti-twin pairs of words with respect to* $\mathcal{L}_{\mathbb{Z}}(A)$.

Problem 1.4 *Determine all twin and anti-twin pairs of words with respect to* $\mathcal{L}_{\mathbb{Z}_m}(A)$, *for* $m > 1$.

In view of these problems Schützenberger considered, for each word $w \in A^*$, the smallest non-negative integer - which we denote by $c(w)$ - that appears as a coefficient of w in some Lie polynomial over $\mathbb{Z}$. For each non-negative integer m he also defined and tried to characterize the language L_m of all words with $c(w) = m$; considering, in particular, the cases $m = 0$ and $m = 1$ (see [14, §1.6.1]).

For $m = 0$ the language L_0 is clearly equal to the complement of the support of the free Lie ring $\mathcal{L}_{\mathbb{Z}}(A)$ in A^*, since a word w does not appear in any Lie polynomial over $\mathbb{Z}$ if and only if $c(w) = 0$. Duchamp and Thibon gave a complete answer to Problem 1.1 in [4] and proved that L_0 consists of all words w which are either a power a^n of a letter a, with exponent $n > 1$, or a *palindrome* (i.e., a word u equal to its *reversal*, denoted by $\tilde{u}$) of even length. The non-trivial part of their work was to show that each word not of the previous form lies in the support of $\mathcal{L}_{\mathbb{Z}}(A)$ and this was achieved by a construction of an ad hoc family of Lie polynomials. This result was extended in [3] - under certain conditions - to *traces*, i.e., partially commutative words (see [1] for an exposition of trace theory) instead of non-commutative ones, and the corresponding free partially commutative Lie algebra (also known as *graph Lie algebra*).

For $m = 1$ all *Lyndon words* on A (for more on this subject see e.g., [9, §5.1 and §5.3]) lie in L_1 since the element P_w of the *Lyndon basis* of $\mathcal{L}_{\mathbb{Z}}(A)$ that corresponds to the *standard factorization* of a given Lyndon word w is equal to w plus a linear combination of greater words - with respect to the *lexicographic ordering* in A^+ - of the same length as w [9, Lemma 5.3.2]. On the other hand, there exist non Lyndon words which also lie in L_1. For example, one can check that the word a^2b^2a - which is clearly non Lyndon as it starts and ends with the same letter - appears with coefficient equal to -1 in the Lie monomial $P_{a^3b^2} = [a, [a, [[a, b], b]]]$ and therefore $(-P_{a^3b^2}, a^2b^2a) = 1$.

In Section 2 we relate Problems 1.1 up to 1.4 with the notion of the *adjoint endomorphism* l^* of the left-normed Lie bracketing l of the free Lie algebra $\mathcal{L}_K(A)$ with respect to the *canonical scalar product* on $K\langle A\rangle$. Our starting point is the simple idea that a word w does not lie in the support of $\mathcal{L}_K(A)$ if and only if $l^*(w) = 0$ and a pair (u, v) of words is twin (respectively anti-twin) if and only if $l^*(u) = l^*(v)$ (respectively $l^*(u) = -\,l^*(v)$). We also show that $c(w)$ is either zero or the greatest common divisor of the coefficients of the monomials appearing in $l^*(w)$, for the left-normed Lie bracketing l of the free Lie ring. It turns out that it is also equal to the greatest common divisor of the coefficients in the expression of $l^*(w)$ as a linear combination of the images of the Lyndon words of length $|w|$ under l^*.

Considering the natural projection from $\mathbb{Z}$ onto $\mathbb{Z}_m$ for $m \neq 1$, we show that the complement of the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$ in A^* is identified with the language $\overline{L}_m$ of all words w with $m \mid c(w)$. For Problem 1.3 we conjecture that two words u, v of common length n that do not lie in the support of the free Lie ring, i.e., they are not n-th powers of a letter with $n > 1$ or palindromes of even length, are twin if and only if either $u = v$ or n is odd and $u = \tilde{v}$ and are anti-twin if and only if n is even and $u = \tilde{v}$. We also show that it suffices to prove this over an alphabet of two letters.

In Section 3 we calculate the polynomial $l^*(w)$ recursively in terms of all factors u of fixed length $r \geq 1$ of w and the *shuffle product* of words (see [14, §1.4] for a definition) as

$$l^*(w) \;=\; \sum_{\substack{w=sut \\ |u|=r}} l^*(u)\,(-1)^{|s|}\,\{\tilde{s} \sqcup\!\sqcup\; t\}$$

and use this to recover naturally the result of Duchamp and Thibon in [4]. Furthermore, if w lies in the kernel of l^* over K we show that $|alph(w)| \leq \lceil |w|/2 \rceil$. Applying this for $K = \mathbb{Z}_m$ for all $m > 1$ we obtain, as a corollary, the fact that all words w with $|alph(w)| > \lceil |w|/2 \rceil$ have $c(w) = 1$ and therefore lie in L_1, just as Lyndon words do.

In Section 4 Problems 1.1 up to 1.4 boil down to particular combinatorial questions on the group ring $K\mathfrak{S}_n$ of the symmetric group $\mathfrak{S}_n$ on n letters. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$ and fix a sub-alphabet $B = \{a_1, a_2, \ldots a_r\}$ of A. The main idea is to view a word w of length n on B as an *ordered set partition* of $[n]$ denoted by $\{w\} = (I_1(w), I_2(w), \ldots, I_r(w))$, where for each $k \in [r]$ the set $I_k(w)$ consists of the positions of $[n]$ in which the letter a_k occurs in w. If $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ is the multi-degree of w then $\{w\}$ is just a λ-*tabloid*, where λ may be, without loss of generality, assumed an integer partition of n. The role of the reversal $\tilde{w}$ of a word w is then played by the tabloid $\tau_n \cdot \{w\}$, where τ_n is the involution $\prod_{i=1}^{k}(i,\, n-i+1)$ of $\mathfrak{S}_n$ with $k = \lfloor n/2 \rfloor$. Viewing each permutation as a word in n distinct letters, the left-normed multi-linear Lie bracketing $l_n = l(x_1 x_2 \cdots x_n)$ and its adjoint $l_n^* = l^*(x_1 x_2 \cdots x_n)$ can be viewed as elements of the group ring $K\mathfrak{S}_n$; the first one is known as the *Dynkin operator*. The right permutation action of l_n^* on words is then equivalent to the left natural action of l_n on tabloids; in particular $w \cdot l_n^* = 0$ if and only if $l_n \cdot \{w\} = 0$. In this way all previous results and problems translate to corresponding problems on tabloids. In particular, Problem 1.2 boils down to the problem of finding all λ-tabloids t that satisfy the equation $l_n \cdot t = 0$ in the group ring $\mathbb{Z}_m\mathfrak{S}_n$.

One can say more for words where only two letters occur since an ordered partition with two parts is determined by the subset $I = \{i_1, i_2, \ldots, i_s\}$ of $[n]$ that appears in its second row, and is denoted accordingly by $\overline{I}$. We map $\overline{I}$ to the monomial $x_I = x_{i_1} x_{i_2} \cdots x_{i_s}$ in n commuting variables $x_1, x_2, \ldots, x_n$ and extending this by linearity the element $l_n \cdot \overline{I}$ can be viewed as a multi-linear polynomial $h_n(I)$ of total degree s. In this way we can view all Schützenberger problems in a commutative algebra setting. We show that $h_n(I)$ is a multiple of the binomial $x_1 - x_2$. The corresponding quotient $p_n(I)$ is called *Pascal descent polynomial* and is in many aspects a generalization of the notion of the signed binomial coefficient. We study the polynomials $p_n(I)$ in Section 5 and give a recursion formula for their calculation. Problem 1.2 is then equivalent to determining all subsets I of $[n]$ such that $p_n(I) \equiv 0 \pmod{m}$. The latter leads us to an explicitly stated sufficient condition for a word w to lie in the support of the free Lie algebra $\mathcal{L}_{\mathbb{Z}_m}(A)$: namely $m \nmid N_n(I)$, where $n = |w|$, $I = I(w)$ is the subset of $[n]$ consisting of the positions that one of the two letters occurs in w and $N_n(I) = \sum_{i \in I} (-1)^{i-1} \binom{n-1}{i-1}$. This actually means that the signed sum of the entries appearing at the positions corresponding to the subset I in the n-th row (starting to count from $n = 0$) of the *Pascal triangle* $\bmod m$ has to be different from zero $\bmod m$. Similar necessary conditions are obtained for twin and anti-twin words with respect to $\mathcal{L}_{\mathbb{Z}_m}(A)$. Finally our conjecture for twin and anti-twin pairs in the free Lie ring is equivalent to showing that when $p_n(I) \neq 0$ and $p_n(J) \neq 0$, then $p_n(I) = p_n(J)$ if and only if $I = J$ or $I = \tau_n(J)$ and n is odd and $p_n(I) = -p_n(J)$ if and only if $I = \tau_n(J)$ and n is even.

2 Preliminary results

The set $K\langle A\rangle$ becomes a non-commutative associative algebra with the usual *concatenation* product defined as

$$(PQ,\, w) \;=\; \sum_{w=uv} (P,u)(Q,v)\,, \tag{2.1}$$

and a commutative associative algebra with the *shuffle product* that is initially defined for words as $\epsilon \sqcup\!\sqcup w = w \sqcup\!\sqcup \epsilon = w$, if at least one of them is the empty word ϵ, and recursively as

$$(au') \sqcup\!\sqcup (bv') \;=\; a(u' \sqcup\!\sqcup (bv')) \,+\, b((au') \sqcup\!\sqcup v')\,, \tag{2.2}$$

if $u = au'$ and $v = bv'$ with $a, b \in A$ and $u', v' \in A^*$ (see [14, (1.4.2)] or [2, §4.1] for a q-deformation). Elements of the form $u \sqcup\!\sqcup v$ with $u, v \in A^+$ are called *proper shuffles*. The definition of the shuffle product is extended linearly to the whole of $K\langle A\rangle$.

The *left-normed Lie bracketing* of a word is the Lie polynomial l defined recursively as

$$l(\epsilon) \,=\, 0\,, \qquad l(a) \,=\, a\,, \qquad \text{and} \qquad l(ua) \,=\, [l(u),\, a]\,, \tag{2.3}$$

for each $a \in A$ and $u \in A^+$. One can extend l linearly to $K\langle A\rangle$ and construct a linear map, denoted also by l, which maps $K\langle A\rangle$ onto the free Lie algebra $\mathcal{L}_K(A)$, since the set $\{l(u) \,:\, u \in A^*\}$ is a well known K-linear generating set of $\mathcal{L}_K(A)$ (see e.g. [14, §0.4.1]).

Given two polynomials $P, Q \in K\langle A\rangle$ there is a *canonical scalar product* defined as

$$(P,Q) \;=\; \sum_{w\in A^*} (P,w)(Q,w) \tag{2.4}$$

in the sense that it is the unique scalar product on $K\langle A\rangle$ for which A^* is an orthonormal basis. The adjoint endomorphism l^* of the left-normed Lie bracketing l is then defined by the relation

$$(l^*(u),v) \;=\; (l(v),u) \tag{2.5}$$

for any words u, v. The image of l^* on a word of A^* can also be effectively defined recursively by the relations

$$l^*(\epsilon) \,=\, 0\,, \qquad l^*(a) \,=\, a\,, \qquad \text{and} \qquad l^*(aub) \,=\, l^*(au)\,b - l^*(ub)\,a\,, \tag{2.6}$$

where $a, b \in A$ and $u \in A^*$ (cf. [9, Problem 5.3.2]). The proof goes by induction on the length of the given word, just as in the case of the adjoint endomorphism of the right-normed Lie bracketing (discussed in detail in [14, pp. 32 - 33]). The reason we choose to work with the left-normed one is that its multi-linear version corresponds to the Dynkin operator which has been thoroughly studied; this will be discussed later on in Section 4.

Lemma 2.1 *Let $\tilde{w}$ denote the reversal of the word w. Then*

$$l^*(\tilde{w}) \,=\, (-1)^{|w|+1} l^*(w)\,.$$

Proof: By the recursive formula (2.6) and an easy induction on $|w|$. $\square$

One can also extend l^* linearly to the whole of $K\langle A\rangle$ and construct a linear endomorphism of $K\langle A\rangle$, denoted also by l^*. What is of crucial importance for the Schützenberger problems is the kernel $\ker l^*$ of l^*. Let $\mathcal{L}_K(A)^\perp$ denote the orthogonal complement of $\mathcal{L}_K(A)$ with respect to the scalar product (2.4) in $K\langle A\rangle$. Then, for an arbitrary commutative ring K with unity, the following two results hold.

Lemma 2.2 $\ker l^* = \mathcal{L}_K(A)^\perp$.

Proof: A polynomial $P \in \ker l^*$ if and only if $\Big(\sum_{w\in A^*} (P,w)\, l^*(w),\ u\Big) \,=\, \sum_{w\in A^*} (P,w)(l^*(w),u) \,=\, 0$, for each $u \in A^*$. By (2.5) and (2.4) the latter means that $(P,\, l(u)) \,=\, 0$, for each $u \in A^*$. Since $\{l(u)\,:\, u\in A^*\}$ is a K-linear generating set for $\mathcal{L}_K(A)$, this is equivalent to having $(P,Q) = 0$ for each $Q \in \mathcal{L}_K(A)$, which means precisely that $P \in \mathcal{L}_K(A)^\perp$. $\square$

Lemma 2.3 *Let $u, v, w \in A^*$. Then*

(i) *A word w does not lie in the support of $\mathcal{L}_K(A)$ if and only if $w \in \ker l^*$.*

(ii) *A pair of words $u,\ v$ is twin (respectively anti-twin) with respect to $\mathcal{L}_K(A)$ if and only if the binomial $u - v$ (respectively $u + v$) $\in \ker l^*$.*

Proof: (i) It follows from Lemma 2.2 and the fact that a word w does not lie in the support of $\mathcal{L}_K(A)$ if and only if $(Q,w) = 0$, for each Lie polynomial Q.

(ii) Suppose that u and v are twin words. By definition this means that $(Q,u) \,=\, (Q,v)$, for every $Q \in \mathcal{L}_K(A)$, i.e., the binomial $u - v \in \mathcal{L}_K(A)^\perp$ and the result follows from Lemma 2.2. An analogous argument is used for anti-twin pairs and the binomial $u + v$. $\square$

Remark 2.4 By a result of Ree [13] (cf. [14, Theorem 3.1]) it is known that if K is assumed to be a commutative $\mathbb{Q}$-algebra, where $\mathbb{Q}$ denotes the field of rational numbers, a polynomial with zero constant term lies in $\mathcal{L}_K(A)^\perp$ - and hence not in the support of $\mathcal{L}_K(A)$ in view of Lemma 2.2 and Lemma 2.3 - if and only if it is a K-linear combination of proper shuffles.

Proposition 2.5 *Let K be a commutative ring with unity and $l_1, l_2, \ldots, l_r$ be the Lyndon words of length n on the alphabet A. Then the set $\{l^*(l_1), l^*(l_2), \ldots, l^*(l_r)\}$ is a K-basis of the image under l^* of the n-th homogeneous component of $K\langle A\rangle$.*

Proof: Suppose that, without loss of generality, $l_1 \,<\, l_2 \,<\, \cdots \,<\, l_r$ with respect to the lexicographic ordering in A^+. Consider also the corresponding Lyndon basis $\{P_{l_1}, P_{l_2}, \ldots, P_{l_r}\}$ of the n-th homogeneous component $\mathcal{L}^n_{\mathbb{Z}}(A)$ of $\mathcal{L}_{\mathbb{Z}}(A)$, where each P_{l_i} is written in the form $P_{l_i} = l_i + \sum_{t>l_i} c_t t$, for suitable $c_t \in K$ (see [9, Lemma 5.3.2]). Let w now be a given word of length n; we have to show that there exist unique coefficients $\xi_1, \xi_2, \ldots, \xi_r \in K$ such that $\sum_{i=1}^{r} \xi_i \, l^*(l_i) \;=\; l^*(w)$. This means that for all $u \in A^n$ we must have $\sum_{i=1}^{r} (l^*(l_i), u)\, \xi_i \;=\; (l^*(w), u)$, which by (2.5) is equivalent to $\sum_{i=1}^{r} (l(u), l_i)\, \xi_i \;=\; (l(u), w)$. Since $\{l(u) \;:\; u \in A^n\}$ and $\{P_{l_1}, P_{l_2}, \ldots, P_{l_r}\}$ are respectively a K-generating set and a K-basis of $\mathcal{L}^n_K(A)$, the latter is equivalent to the $r \times r$ linear system $\sum_{i=1}^{r} (P_{l_i}, l_i)\, \xi_i \;=\; (P_{l_i}, w)$, with $i \in [r]$ in the unknowns $\xi_1, \xi_2, \ldots, \xi_r$. Since $(P_{l_i}, l_i) = 1$ and $(P_{l_i}, l_j) = 0$ for $j < i$ this boils down to

$$\xi_i \,+\, \sum_{j=i+1}^{r} (P_{l_i}, l_j)\, \xi_j \;=\; (P_{l_i}, w), \quad i \in [r]. \tag{2.7}$$

By triangularity, the linear system (2.7) has a unique solution $(\xi_1, \xi_2, \ldots, \xi_r) \in K^r$, as required. □

For a given word w of length n Schützenberger considered the unique non-negative generator $c(w)$ of the ideal $\{(P, w) \;:\; P \in \mathcal{L}_{\mathbb{Z}}(A)\}$ of $\mathbb{Z}$ (see [14, §1.6.1]). It is natural to ask how to calculate the number $c(w)$ and try to find a homogeneous Lie polynomial Q_w of degree n such that $(Q_w, w) = c(w)$. One would a priori search amongst all Lie polynomials of some basis of $\mathcal{L}^n_{\mathbb{Z}}(A)$. It turns out that this can be done in terms of just one polynomial, which is not a Lie polynomial in general, namely the element $l^*(w) \in \mathbb{Z}\langle A\rangle$.

Theorem 2.6 *Let w be a word of length n and l^* be the adjoint endomorphism of the left-normed Lie bracketing l of the free Lie ring on A. Then $c(w)$ is either zero or is equal to the greatest common divisor of the non-zero coefficients that appear either in the monomials of the polynomial $l^*(w)$ or in its representation as a linear combination of the images of the Lyndon words of length n under l^*.*

Proof: Clearly $c(w) = 0$ if and only if $l^*(w) = 0$. Suppose that $l^*(w) \neq 0$. Then we obtain

$$\{(P, w) : P \in \mathcal{L}_{\mathbb{Z}}(A)\} = \{(P, w) : P \in \mathcal{L}^n_{\mathbb{Z}}(A)\} = \langle\, \{(P, w) : P \in \mathcal{X}, \mathcal{X} \text{a generating set for} \, \mathcal{L}^n_{\mathbb{Z}}(A)\}\,\rangle\,.$$

For $s \in \mathbb{N}$ the ideal $\langle\, n_1, n_2, \ldots, n_s \,\rangle$ generated by $n_1, n_2, \ldots, n_s \in \mathbb{Z}$ is equal to $\langle\, \gcd(n_1, n_2, \ldots, n_s)\,\rangle$. Thus if we choose $\mathcal{X} = \{l(u) \;:\; u \in A^{\,n}\}$ then by (2.5) and the definition of $c(w)$ we obtain $c(w) = \gcd\big((l(u), w) \;:\; u \in A^{\,n}\big) = \gcd\big((l^*(w), u) \;:\; u \in A^{\,n}\big)$, as required. If, on the other hand, we choose $\mathcal{X} = \{P_{l_1}, P_{l_2}, \ldots, P_{l_r}\}$, where r is the number of all Lyndon words of length n, then again $c(w) = \gcd\big((P_{l_1}, w), (P_{l_2}, w), \ldots, (P_{l_r}, w)\big)$. Now the triangular form of the linear system (2.7) for $K = \mathbb{Z}$ implies that $\langle (P_{l_1}, w), (P_{l_2}, w), \ldots, (P_{l_r}, w)\rangle \;=\; \langle \xi_1, \xi_2, \ldots, \xi_r\rangle$, so that we also get $c(w) = \gcd(\xi_1, \xi_2, \ldots, \xi_r)$. □

Suppose that $l^*(w) = d_1u_1 + d_2u_2 + \cdots + d_su_s$, where $d_1, d_2, \ldots, d_s \in \mathbb{Z}^*$ and $u_1, u_2, \ldots, u_s \in A^n$. Then by Theorem 2.6 $c(w) = \gcd\,(d_1, d_2, \ldots, d_s)$ and by an extension of *Bezout's identity* to more than two integers there exist $k_1, k_2, \ldots, k_s \in \mathbb{Z}$ such that $c(w) = k_1d_1 \,+\, k_2d_2 \,+\, \cdots \,+\, k_sd_s$. Therefore if we set $Q_w = k_1\, l(u_1) \,+\, k_2\, l(u_2) \,+\, \cdots \,+\, k_s\, l(u_s)$ by (2.5) we easily obtain $(Q_w, w) = c(w)$, as required.

Let m be a positive integer with $m > 1$. The natural projection $k \mapsto \overline{k} = k \,(\mathrm{mod}\, m)$ from $\mathbb{Z}$ onto $\mathbb{Z}_m$ induces a surjective map $\theta \;:\; \mathbb{Z}\langle A\rangle \;\twoheadrightarrow\; \mathbb{Z}_m\langle A\rangle$ that sends a polynomial $P = \sum_{u \in A^*} (P, u)\, u \in \mathbb{Z}\langle A\rangle$

to the polynomial $\theta(P) = \sum_{u\in A^*} \overline{(P,u)}\, u \in \mathbb{Z}_m\langle A\rangle$. Clearly $\ker\theta = (m)\,\mathbb{Z}\langle A\rangle$. The restriction ψ of θ to $\mathcal{L}_{\mathbb{Z}}(A)$ is also surjective onto $\mathcal{L}_{\mathbb{Z}_m}(A)$ with $\ker\psi = (m)\,\mathcal{L}_{\mathbb{Z}}(A)$. If we denote the left-normed Lie bracketing over $\mathbb{Z}_m$ and its adjoint by $\bar{l}$ and $\overline{l^*}$, respectively, it is easy to see that for each word u in A^* we have $\psi(l(u)) = \bar{l}(u)$. From this we can show that $\theta(l^*(w)) = \overline{l^*}(w)$, for each word w in A^*. Indeed, $\theta(l^*(w)) = \theta\big(\sum_{u\in A^*} (l^*(w),u)\, u\big) = \sum_{u\in A^*} \overline{(l^*(w),u)}\, u = \sum_{u\in A^*} \overline{(l(u),w)}\, u = \sum_{u\in A^*} (\bar{l}(u),w)\, u = \overline{l^*}(w)$. Then extending linearly we get $\theta\circ l^* = \overline{l^*}$.

Theorem 2.7 ***(i)*** *The complement, in A^*, of the support of the free Lie algebra $\mathcal{L}_{\mathbb{Z}_m}(A)$ over the ring $\mathbb{Z}_m$ of integers $\bmod m$ consists of all words w such that $m \mid c(w)$, or equivalently those words with the property that the polynomial $l^*(w)$ lies in $(m)\,\mathbb{Z}\langle A\rangle$.*

(ii) *A pair of words u, v is twin (respectively anti-twin) with respect to $\mathcal{L}_{\mathbb{Z}_m}(A)$ if and only if the polynomial $l^*(u) - l^*(v)$ (respectively $l^*(u) + l^*(v)$) lies in $(m)\,\mathbb{Z}\langle A\rangle$.*

Proof: (i) By Lemma 2.3 (i) applied for $K = \mathbb{Z}_m$, the complement of the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$ in A^* is equal to $\{w \in A^* : \overline{l^*}(w) = \bar{0}\}$. Since $\ker\theta = (m)\,\mathbb{Z}\langle A\rangle$ and $\theta\circ l^* = \overline{l^*}$, the latter is equal to $\{w \in A^* : l^*(w) \in (m)\,\mathbb{Z}\langle A\rangle\}$. If $l^*(w) = d_1u_1 + d_2u_2 + \cdots + d_su_s$, for $d_1, d_2, \ldots, d_s \in \mathbb{Z}^*$ (that depend on the word w) then $m \mid d_i$ for all $i \in [s]$ if and only if $m \mid \gcd(d_1, d_2, \ldots, d_s)$ which, by Theorem 2.6, is equal to $c(w)$. On the other hand, it is clear that $l^*(w) = 0$ is equivalent to $c(w) = 0$. In any case $l^*(w) \in (m)\,\mathbb{Z}\langle A\rangle$ if and only if $m \mid c(w)$ and the result follows.

(ii) It follows similarly from Lemma 2.3 (ii). □

Let us see now the way the Schützenberger problems relate to the *Pascal triangle* $\bmod m$. When $m = p$, a prime number, an old result due to E. Lucas [10] known as the *Lucas correspondence theorem* (for a nice exposition of this see [5]) asserts that if n and r have expansions in base p respectively given by $n = \sum_{q\geq 0} n_q p^q$ and $r = \sum_{q\geq 0} r_q p^q$ with $n_q, r_q \in \{0, 1, \ldots, p-1\}$, then

$$\binom{n}{r} \equiv \prod_{q\geq 0} \binom{n_q}{r_q} \pmod p. \tag{2.8}$$

By another old result of E. Kummer [8] known as *Kummer's lemma*, the highest power of a prime p dividing $\binom{k+l}{k}$ is equal to the number of carries in the p-ary addition of k and l. This enables us to solve directly the Schützenberger problems for words w of the form $w = a^kba^l$.

Lemma 2.8 *Let k and l be non-negative integers which are not both equal to zero and m be a positive integer with primary decomposition $m = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$. Then*

(i) $$l^*(a^kba^l) = (-1)^k\binom{k+l}{k} l^*(ba^{k+l}) = (-1)^k\binom{k+l}{k}\{ba^{k+l} - aba^{k+l-1}\}.$$

(ii) *The word a^kba^l does not lie in the support of the free Lie algebra $\mathcal{L}_{\mathbb{Z}_m}(A)$ if and only if for each $i \in [s]$ the number of carries in the p_i-ary addition of k and l is at least e_i.*

Proof: (i) It is easy to show that $l^*(ba^m) = ba^m - aba^{m-1}$, by induction on m. Assuming, without loss of generality, that $k \geq 1$ (2.6) yields $l^*(a^k ba^l) = \{l^*(a^k ba^{l-1}) - l^*(a^{k-1} ba^l)\}\, a$. The proof is completed by induction on $k + l$ and the recursive definition of binomial coefficients.

(ii) By Theorem 2.7 (i) a word w lies in the complement of the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$ in A^* if and only if $p_i^{e_i} \mid c(w)$ for each $i \in [s]$. Theorem 2.6 (i) and part (i) of this lemma yield $c(a^k ba^l) = \binom{k+l}{k}$ and the result follows by Kummer's lemma. □

Note that in the binary case the condition of Lemma 2.8 (ii) simply means that if k and l are written in base 2 as $k = \sum_{q \geq 0} k_q 2^q$ and $l = \sum_{q \geq 0} \lambda_q 2^q$ with $k_q, l_q \in \{0, 1\}$, there exists at least one position q where $k_q = l_q = 1$.

Let us now discuss Problem 1.3. In view of Lemma 2.3 (ii), given a pair of words $u,\ v$ one has to check whether $l^*(u) = l^*(v)$ (respectively $l^*(u) = -l^*(v)$) for the pair to be twin (respectively anti-twin). There are some trivial solutions of this problem, namely when $l^*(u) = l^*(v) = 0$, i.e., when both u and v are either powers of a letter with exponent larger than one or palindromes of even length. So let us suppose that both words do lie in the support of the free Lie ring. In view of Lemma 2.1 we propose the following conjecture.

Conjecture 2.9 *Let l^* be the adjoint endomorphism of the left-normed Lie bracketing l of the free Lie ring and let u and v be words of common length n such that both $l^*(u)$ and $l^*(v)$ are non-zero. Then*

(i) *$l^*(u) = l^*(v)$ if and only if $u = v$ or n is odd and $u = \tilde{v}$.*

(ii) *$l^*(u) = -\, l^*(v)$ if and only if n is even and $u = \tilde{v}$.*

Reduction Theorem 2.10 *It suffices to prove Conjecture 2.9 for an alphabet of two letters.*

The proof of this result will occupy the remaining of this section. Let us first see how l^* is affected by alphabetic substitutions. Consider two finite alphabets A and Σ with $|A| \geq |\Sigma| \geq 2$ and a mapping ϕ from A onto Σ. This induces a surjective *literal* morphism (i.e., a morphism such that $\phi(a) \in \Sigma$, for each $a \in A$), also denoted by ϕ, from A^* onto Σ^* which in turn can be extended linearly to an algebra surjective homomorphism - still denoted by ϕ - from $K\langle A\rangle$ onto $K\langle\Sigma\rangle$. Let l_A^* and l_Σ^* denote the adjoint endomorphism of the left-normed Lie bracketing of the free Lie algebras $\mathcal{L}_K(A)$ and $\mathcal{L}_K(\Sigma)$, respectively.

Lemma 2.11 *Let A and Σ be two finite alphabets with $|A| \geq |\Sigma| \geq 2$ and ϕ be a fixed literal morphism from A^* onto Σ^*.*

(i) *The algebra homomorphisms $\phi \circ l_A^*$ and $l_\Sigma^* \circ \phi$ from $K\langle A\rangle$ to $K\langle\Sigma\rangle$ are identical and $\phi(\ker l_A^*) \subseteq \ker l_\Sigma^*$.*

(ii) *If $|A| = |\Sigma|$ then $\ker l_A^*$ is mapped bijectively onto $\ker l_\Sigma^*$ under ϕ.*

(iii) *$\phi(\ker l_A^*) = \ker l_\Sigma^*$ but $\ker l_A^*$ is a proper subset of $\phi^{-1}(\ker l_\Sigma^*)$ if $|A| > |\Sigma|$.*

Proof: (i) It suffices to show that $l_\Sigma^*(\phi(w)) = \phi(l_A^*(w))$ for each word $w \in A^*$. This follows by an easy induction on $|w|$ using the recursive definition (2.6) of l^*. The inclusion $\phi(\ker l_A^*) \subseteq \ker l_\Sigma^*$ follows easily.

(ii) We apply the result of part (i) for the literal morphisms $\phi : A \twoheadrightarrow \Sigma$ and $\phi^{-1} : \Sigma \twoheadrightarrow A$ and obtain $\phi(\ker l_A^*) \subseteq \ker l_\Sigma^*$ and $\phi^{-1}(\ker l_\Sigma^*) \subseteq \ker l_A^*$ which clearly implies the required result.

(iii) It remains to show that $\phi(\ker l_A^*) \supseteq \ker l_\Sigma^*$. Let $Q = \sum_i \lambda_i v_i$ be a polynomial in $\ker l_\Sigma^*$ and $\Sigma_Q = \bigcup_i alph(v_i)$. For each letter $b \in \Sigma_Q$ choose a unique letter $a \in A$ such that $\phi(a) = b$ and let A_Q be the subset of A consisting of all those chosen letters. Clearly the restriction $\widehat{\phi}$ of ϕ to A_Q is a bijection from A_Q onto Σ_Q. Consider the extension of $\widehat{\phi}$ - denoted by the same symbol - to A_Q^* which is a bijective homomorphism to Σ_Q^*. Let $P = \sum_i \lambda_i \widehat{\phi}^{-1}(v_i)$. Then clearly $\widehat{\phi}(P) = Q$, so that $\phi(P) = Q$. Furthermore, since $Q \in \ker l_{\Sigma_Q}^*$ and $|A_Q| = |\Sigma_Q|$ part (ii) applied for the bijection $\widehat{\phi}$ implies that P also lies in $\ker l_{A_Q}^*$ and hence in $\ker l_A^*$.

Suppose now that $|A| > |\Sigma|$. We can consider three distinct letters $a, b, c \in A$ and two distinct letters $e, f \in \Sigma$ in such a way that, without loss of generality, $\phi(a) = e$ and $\phi(b) = \phi(c) = f$. Consider the word $w = abca$. Then $w \in \phi^{-1}(\ker l_\Sigma^*)$ since clearly $\phi(w) = ef^2e$ is a palindrome of length 4, but $w \notin \ker l_A^*$ since $l_A^*(w) = abca - baca - 2bca^2 + 2cba^2 + caba - acba \neq 0$. □

Consider a two-lettered alphabet $\Sigma = \{0, 1\}$. For each subset B of A let ϕ_B be the literal morphism from A^* onto Σ^* defined as $\phi_B(a) = 1$, when $a \in B$ and $\phi_B(a) = 0$, otherwise. For brevity when $B = \{b\}$ we write ϕ_b instead of $\phi_{\{b\}}$. Let us also denote the set of palindromes of length n in A^* and Σ^* by $Pal_n(A)$ and $Pal_n(\Sigma)$, respectively.

Lemma 2.12 *Let $u, v \in A^*$ of common length and a, b be distinct elements of A.*

(i) $\phi_a(u) = \phi_a(v)$, *for each $a \in A$, if and only if $u = v$.*

(ii) *If $\phi_a(u) \in Pal_n(\Sigma)$ for each $a \in A$, then $u \in Pal_n(A)$.*

(iii) *If $\phi_{\{a,b\}}(u) = \phi_{\{a,b\}}(v)$ and $\phi_a(u) = \phi_a(v)$ then $\phi_b(u) = \phi_b(v)$.*

(iv) *If $\phi_{\{a,b\}}(u)$ and $\phi_a(u)$ lie in $Pal_n(\Sigma)$ then $\phi_b(u)$ does also.*

Proof: For (i) and (iii) it suffices to check the case where $u, v \in A$. Then (i) follows directly from the definition of the morphism ϕ_a. For (iii) if $u, v \notin \{a, b\}$ the result is clear, whereas if $u, v \in \{a, b\}$ we necessarily obtain $u = v = a$ or $u = v = b$ and the result follows. Parts (ii) and (iv) follow respectively from (i) and (iii) for $v = \tilde{u}$ and the fact that $\widetilde{\phi(w)} = \phi(\tilde{w})$ for each literal morphism ϕ and each word $w \in A^*$ which is easily proved by induction on $|w|$. □

Proof of Reduction Theorem 2.10.: Suppose that Conjecture 2.9 is true for a two lettered alphabet $\Sigma = \{0, 1\}$. We will show that it also holds for any finite alphabet A with $|A| > 2$. Suppose that $u, v \in A^*$ with $|u| = |v| = n > 1$ and that both polynomials $l^*(u)$ and $l^*(v)$ are non-zero.

(1) $\mathbf{l^*(u) = l^*(v)}$. It means that $u - v \in \ker l_A^*$. Then by by Lemma 2.11 (i), for any subset B of A we get $\phi_B(u - v) \in \ker l_\Sigma^*$, obtaining $l^*(\phi_B(u)) = l^*(\phi_B(v))$. We consider two cases.

(i) n is even. Our aim is to show that $u = v$. If $l^*(\phi_B(u)) = l^*(\phi_B(v)) \neq 0$, then Conjecture 2.9 yields $\phi_B(u) = \phi_B(v) \notin Pal_n(\Sigma)$. If, on the other hand, $l^*(\phi_B(u)) = l^*(\phi_B(v)) = 0$ both $\phi_B(u)$ and $\phi_B(v)$ lie in $Pal_n(\Sigma)$. Restricting ourselves initially to singleton subsets $B = \{a\}$ we define, for our fixed words u and v, the sub-alphabets C and D of A as

$$C = \{a \in A \;:\; \phi_a(u), \phi_a(v) \in Pal_n(\Sigma)\} \quad \text{and} \quad D = \{a \in A \;:\; \phi_a(u) = \phi_a(v) \notin Pal_n(\Sigma)\}. \quad (2.9)$$

By construction $A = C \cup D$ and $C \cap D = \emptyset$. Suppose that $C = \emptyset$. Then $A = D$ and the result follows immediately by Lemma 2.12 (i). If $C \neq \emptyset$ then also $D \neq \emptyset$, since otherwise $A = C$ and by Lemma 2.12 (ii) it would follow that $u, v \in Pal_n(A)$, contradicting our original assumption that both $l^*(u)$ and $l^*(v)$ are non-zero. Let c be an arbitrary element of C. In view of Lemma 2.12 (i) it suffices to show that $\phi_c(u) = \phi_c(v)$. Let $d \in D$ and set $B = \{c, d\}$. Then either $\phi_B(u)$ and $\phi_B(v)$ lie in $Pal_n(\Sigma)$ or $\phi_B(u) = \phi_B(v) \notin Pal_n(\Sigma)$. In the former case the fact that $\phi_c(u), \phi_c(v) \in Pal_n(\Sigma)$ and Lemma 2.12 (iv) yield $\phi_d(u), \phi_d(v) \in Pal_n(\Sigma)$, which contradicts the assumption that $d \in D$. In the latter case Lemma 2.12 (iii) finally yields $\phi_c(u) = \phi_c(v)$, as required.

(ii) n is odd. Our aim is to show that either $u = v$ or $u = \tilde{v}$. First we show that either $\phi_B(u) = \phi_B(v)$ or $\phi_B(u) = \phi_B(\tilde{v})$. If $l^*(\phi_B(u)) = l^*(\phi_B(v)) \neq 0$ this follows immediately by Conjecture 2.9 which is assumed to hold for Σ. If, on the other hand, $l^*(\phi_B(u)) = l^*(\phi_B(v)) = 0$ then both $\phi_B(u)$ and $\phi_B(v)$ lie in $\{0^n, 1^n\}$. We claim that $\phi_B(u) = \phi_B(v)$. If this is not the case, without loss of generality, $\phi_B(u) = 1^n$ and $\phi_B(v) = 0^n$. By the definition of ϕ_B it follows that $alph(u) \subseteq B$ and $alph(v) \subseteq A \setminus B$. On the other hand having assumed that $l^*(u) = l^*(v) \neq 0$ we also get $alph(u) = alph(v)$ and we reach a contradiction. For our fixed pair (u, v) define the sub-alphabets E and F of A as

$$E = \{a \in A \,:\, \phi_a(u) = \phi_a(v)\} \quad \text{and} \quad F = \{a \in A \,:\, \phi_a(u) = \phi_a(\tilde{v})\}. \tag{2.10}$$

It follows that $A = E \cup F$. It remains to show that either $E = A$ or $F = A$. Suppose, for the sake of contradiction, that $e \in E \setminus F$ and $f \in F \setminus E$. Then if we let $B = \{e, f\}$ we either get $\phi_B(u) = \phi_B(v)$ or $\phi_B(u) = \phi_B(\tilde{v})$. By Lemma 2.12 (iii) the former equality together with the fact that $e \in E$ yields $\phi_f(u) = \phi_f(v)$, so that f will also lie in E, which is a contradiction since we took $f \in F \setminus E$. We get a similar contradiction starting from the latter equality.

(2) $\mathbf{l^*(u) = -\,l^*(v)}$. It means that $u + v \in \ker l^*_A$ so by Lemma 2.11 (i) $\phi_B(u + v) \in \ker l^*_\Sigma$ and therefore $l^*(\phi_B(u)) = -\,l^*(\phi_B(v))$, for each subset B of A. The case where n is even is dealt in an analogous way as in case 1(i) before; we leave the details to the reader.

If n is odd, by Conjecture 2.9, we can not have $l^*(\phi_B(u)) = -\,l^*(\phi_B(v)) \neq 0$. Thus for each $B \subseteq A$ both $\phi_B(u)$ and $\phi_B(v)$ lie in $\{0^n, 1^n\}$. This will hold in particular, for each singleton $B = \{a\}$, with $a \in A$. Then if $\phi_a(u) = 1^n$ for some $a \in A$ we obtain $u = a^n$, a contradiction. Therefore $\phi_a(u) = \phi_a(v) = 0^n$ for each $a \in A$. Then $alph(u) \cap A = \emptyset$, which also clearly can not hold. □

3 Calculation of l^*

We will now generalize the effective definition (2.6) of l^* using the shuffle product of words and calculate the polynomial $l^*(w)$ recursively in terms of all factors u of fixed length $r \geq 1$ of w. By a *factor* of a word w we mean a word u such that there exist $s, t \in A^*$ with $w = sut$.

Proposition 3.1 *Let w be a word and r be a positive integer with $r \leq |w|$. Consider the set of all factors u of length r of w. Then*

$$l^*(w) \;=\; \sum_{\substack{w = sut \\ |u| = r}} l^*(u)\,(-1)^{|s|}\,\{\tilde{s} \sqcup\!\sqcup\; t\}\,.$$

Proof: Let $|w| = n$. We argue by induction on $k = n - r$. Clearly $0 \leq k \leq n - 1$. Note that for $k = 0$ the result is trivial since $s = t = \epsilon$. Also for $k = 1$ it follows from the recursive definition (2.6) of l^* since the factors of length $n - 1$ of $w = aub$ are just the words au and ub.

Let $\{u_i\,:\,0\le i\le n-r\}$ be the set of all $n-r+1$ consecutive factors of length $r\ge 2$ of w. We let $u_i=a_iv_ib_i$ with $a_i,\,b_i\in A$ and $v_i\in A^*$. Note that $v_ib_i=a_{i+1}v_{i+1}$, for $0\le i\le n-r-1$.

Suppose that the result holds for the factors u_i. We have to show that it also holds for factors of length $r-1$ of w. We let $w=s_iu_it_i$ for $0\le i\le n-r$, where $s_0=t_{n-r}=\epsilon$, $s_1=a_0$ and $t_{n-r-1}=b_{n-r}$. Then $|\widetilde{s_i}|=|s_i|=i$, for each $0\le i\le n-r$ and our induction hypothesis for factors of length r yields

$$l^*(w)=l^*(u_0)t_0\,+\,\sum_{i=1}^{n-r-1}\,l^*(u_i)\,(-1)^i\,\{\widetilde{s_i}\,\sqcup\!\sqcup\,\,t_i\}\,+\,l^*(u_{n-r})\,(-1)^{n-r}\,\widetilde{s_{n-r}}\,.$$

We apply the recursive formula (2.6) on factors $u_i=a_iv_ib_i$ and obtain

$$\begin{aligned} l^*(w) \;\;=\;\; & \Big[l^*(a_0v_0)b_0\,-\,l^*(v_0b_0)a_0\Big]\,t_0\,+\,\sum_{i=1}^{n-r-1}\,\Big[l^*(a_iv_i)b_i\,-\,l^*(v_ib_i)a_i\Big]\,(-1)^i\,\{\widetilde{s_i}\,\sqcup\!\sqcup\,\,t_i\} \\ & +\Big[l^*(a_{n-r}v_{n-r})b_{n-r}\,-\,l^*(v_{n-r}b_{n-r})a_{n-r}\Big]\,(-1)^{n-r}\,\widetilde{s_{n-r}}\,. \end{aligned}$$

Since $v_ib_i=a_{i+1}v_{i+1}$ for $0\le i\le n-r-1$, grouping all elements of the form a_iv_i for $0\le i\le n-r$ we obtain

$$\begin{aligned} l^*(w) \;\;=\;\; & l^*(a_0v_0)\,(-1)^0b_0t_0\,+\,l^*(a_1v_1)\,(-1)^1\,\{a_0t_0\,+\,b_1\,(a_0\sqcup\!\sqcup\,t_1)\}\,+ \\ & \sum_{i=2}^{n-r-1}\,l^*(a_iv_i)\,(-1)^i\,\{b_i\,(\widetilde{s_i}\sqcup\!\sqcup\,t_i)\,+\,a_{i-1}\,(\widetilde{s_{i-1}}\sqcup\!\sqcup\,t_{i-1})\}\,+ \\ & l^*(a_{n-r}v_{n-r})\,(-1)^{n-r}\,\{b_{n-r}\widetilde{s_{n-r}}\,+\,a_{n-r-1}\,(\widetilde{s_{n-r-1}}\sqcup\!\sqcup\,t_{n-r-1})\}\,+ \\ & l^*(v_{n-r}b_{n-r})\,(-1)^{n-r+1}\,a_{n-r}\widetilde{s_{n-r}}\,. \end{aligned}$$

Since $s_i=s_{i-1}a_{i-1}$ and $t_{i-1}=b_it_i$ for $1\le i\le n-r$ (note the extreme cases $s_1=a_0$ for $i=1$ and $t_{n-r-1}=b_{n-r}$ for $i=n-r$), from the recursive definition (2.2) of the shuffle product we get

$$b_i\,(\widetilde{s_i}\sqcup\!\sqcup\,t_i)\,+\,a_{i-1}\,(\widetilde{s_{i-1}}\sqcup\!\sqcup\,t_{i-1})\;=\;a_{i-1}\widetilde{s_{i-1}}\sqcup\!\sqcup\,b_it_i\;=\;\widetilde{s_i}\sqcup\!\sqcup\,b_it_i,$$

for all $i\in[n-r]$. Then we immediately obtain

$$\begin{aligned} l^*(w) \;\;=\;\; & l^*(a_0v_0)\,(-1)^0\{\epsilon\sqcup\!\sqcup\,b_0t_0\}\,+\,\sum_{i=1}^{n-r}\,l^*(a_iv_i)\,(-1)^i\,\{\widetilde{s_i}\sqcup\!\sqcup\,b_it_i\}\,+ \\ & l^*(v_{n-r}b_{n-r})\,(-1)^{n-r+1}\,\{\widetilde{s_{n-r}a_{n-r}}\sqcup\!\sqcup\,\epsilon\}\,, \end{aligned}$$

which is precisely the required summation for factors of length $r-1$ we had aimed for. $\square$

Remarks. The case where the factors u of the word w are letters (i.e., we are at the bottom level $r=1$) seems to be known in a different setting in the literature (see [7, Lemma 2.1], cf. [1, Ex. 4.6.5 (2), p.126]) even for the broader class of free partially commutative Lie algebras. On the other hand, Proposition 3.1 clearly does not hold if we consider trivial factors of w, i.e., factors of length $r=0$. In this case the identity $0\;=\;\sum_{w=st}\,(-1)^{|s|}\,\{\tilde{s}\,\sqcup\!\sqcup\,\,t\}$, due to W. Schmidt, holds; see [14, §1.6.4].

We will now use Proposition 3.1 to reobtain - in a non ad hoc way - the result by Duchamp and Thibon [4, §3, p.124] for the calculation of the support of the free Lie ring.

Theorem 3.2 *The words that vanish under the adjoint endomorphism l^* of the left-normed Lie bracketing l of the free Lie ring are either powers of a single letter with exponent greater than one or palindromes of even length.*

Proof: If $w = a^n$, where $n \geq 2$, then $l^*(w) = 0$, since $l^*(w) = l^*(a^{n-1})\,a - l^*(a^{n-1})\,a$. For a palindrome w of even length Lemma 2.1 yields $2\,l^*(w) = 0$, hence $l^*(w) = 0$ since we are in characteristic zero.

For the other direction of the theorem consider a word w such that $l^*(w) = 0$. We will argue by induction on the length $|w| = n$. For $n = 2$ we necessarily get $w = a^2$ because if $w = ab$ with $a \neq b$ then $l^*(ab) = ab - ba \neq 0$, so the result follows trivially. Let $n > 2$. We consider two cases.

(1) $\mathbf{w = aub}$, $(\mathbf{a, b \in A},\ \mathbf{a \neq b})$. Then $0 = l^*(w) = l^*(au)\,b - l^*(ub)\,a$. Since $a \neq b$ we get $l^*(au) = l^*(ub) = 0$. By our induction hypothesis we have to consider two subcases.

(i) If at least one of the words au and ub (without loss of generality say au) is a power of a single letter we obtain $au = a^{n-1}$. It follows that $ub = a^{n-2}b$, which contradicts $l^*(ub) = 0$, as the word $a^{n-2}b$ is neither a power of a single letter nor a palindrome of even length.

(ii) If both au and ub are palindromes of even length and not powers of a single letter we must have $au = s\tilde{s}$, for some $s \in A^+$, so that there exists a $t \in A^*$ with $s = at$ and $u = t\tilde{t}a$. But then the word $ub = t\tilde{t}ab$ can not be a palindrome of even length since $|ub|_a = |u|_a = 2|t|_a + 1$ which is an odd positive integer and we obtain another contradiction.

(2) $\mathbf{w = a^k\, bvc\, a^l}$, $(\mathbf{a, b, c \in A},\ \mathbf{b, c \neq a})$. We consider all factors x of length $|v| + 2$ of w. Then Proposition 3.1 yields

$$\begin{aligned} l^*(w) &= l^*(bvc)\,(-1)^k\,\{a^k \sqcup\!\sqcup\ a^l\} + \sum_{\substack{w=sxt \\ (s,t)\neq(a^k,a^l)}} l^*(x)\,(-1)^{|s|}\,\{\tilde{s} \sqcup\!\sqcup\ t\} \\ &= (-1)^k \binom{k+l}{k}\, l^*(bvc)\,a^{k+l} + \sum_{\substack{w=sxt \\ (s,t)\neq(a^k,a^l)}} l^*(x)\,(-1)^{|s|}\,\{\tilde{s} \sqcup\!\sqcup\ t\}. \end{aligned}$$

For any factorization $w = sxt$ other than the one where $(s, x, t) = (a^k, bvc, a^l)$, each shuffle of $\tilde{s}$ and t contains other letters except a so it will be different from a^{k+l}, which will appear only as a shuffle of a^k and a^l. From this we deduce that the monomials of $l^*(w)$ such that a power of the letter a appears as a right factor with maximum possible exponent are precisely the monomials in $\binom{k+l}{k}\, l^*(bvc)\,a^{k+l}$. Now, the assumption $l^*(w) = 0$ yields $\binom{k+l}{l}\, l^*(bvc) = 0$ and since we are in characteristic zero we immediately obtain $l^*(bvc) = 0$. Then by our induction hypothesis we get $b = c$ and v is a power of b or a palindrome of even length. Two subcases have to be considered.

(i) If $k \neq l$ (without loss of generality say $k < l$) we consider factors y of length $|v| + l + 1$ of w and apply again Proposition 3.1. We obtain

$$l^*(w) = \sum_{\substack{w=syt \\ (s,t)\neq(a^k b,\epsilon)}} l^*(y)\,(-1)^{|s|}\,\{\tilde{s} \sqcup\!\sqcup\ t\} \quad + \quad l^*(vba^l)\,(-1)^{k+1}\,b\,a^k. \tag{3.1}$$

In this case every shuffle of the words $\tilde{s}$ and t from each term of the first summand of (3.1) will be equal to a^{k+1}. Assuming that $l^*(w) = 0$ yields $(-1)^{k+1}l^*(vba^l)ba^k + Pa^{k+1} = 0$, for some polynomial $P \in \mathbb{Z}\langle A\rangle$. But then $l^*(vba^l) = P = 0$, so by our induction hypothesis the word vba^l has to be a palindrome of even length. When v is a power of b this clearly can not happen. It remains to check the case where both bvb and vba^l are palindromes of even length. Then $|v|_b$ would be an even positive integer in the former case, whereas $|v|_b = |vba^l|_b - 1$ would be odd in the latter case, a clear contradiction.

(ii) Suppose that $k = l$. If $bvb = b^q$ with q an odd positive integer then $l^*(w) = l^*(a^k\, b^q a^k) = 2\, l^*(a^k\, b^q\, a^{k-1})\, a = 0$, so that $l^*(a^k b^q a^{k-1}) = 0$ which is a contradiction since the word $a^k b^q a^{k-1}$ can not be a palindrome of even length. So we are finally left with the case where bvb is a palindrome of even length which is what we had originally aimed for. □

Theorem 3.3 *Let K be a commutative ring with unity and suppose that $l^*(w) = 0$ for a word $w \in A^*$. Then $|alph(w)| \leq \lceil |w|/2 \rceil$.*

Proof: Consider a word w such that $l^*(w) = 0$. We will argue by induction on the length $|w| = n$. For $n = 2$ we clearly get $w = a^2$ and the result follows trivially. Let $n > 2$. We consider two cases.

(1) $\mathbf{w = aub}$, $(\mathbf{a, b \in A},\ \mathbf{a \neq b})$. Then $0 = l^*(w) = l^*(au)\, b - l^*(ub)\, a$. Since $a \neq b$ we get $l^*(au) = l^*(ub) = 0$. Our first claim is that both letters a and b have to lie in $alph(u)$. Indeed, suppose for the sake of contradiction, that - without loss of generality - $a \notin alph(u)$. Let us consider all factors of length 1 of $w = aub$ and apply Proposition 3.1. We obtain

$$l^*(w) = a\,ub \quad + \sum_{\substack{w=sct \\ c\,\in\, alph(ub)}} (-1)^{|s|}\, c\,\{\tilde{s} \sqcup\!\sqcup\ t\}\,.$$

Since $a \notin alph(u)$ and $a \neq b$, we have $c \neq a$, hence the only monomial of $l^*(w)$ that starts with the letter a is the word aub which cannot be canceled and therefore $l^*(w) \neq 0$, a contradiction.

Having obtained that $a, b \in alph(u)$, we get $alph(w) = alph(u)$. Our result then follows since, by our induction hypothesis, $|alph(u)| \leq \lceil (n-2)/2 \rceil \leq \lceil n/2 \rceil$.

(2) $\mathbf{w = aua}$, $(\mathbf{a \in A})$. We set $r(w) = \max\{\, |s| \ :\ w = sut\,,\ |s| = |t|\,,\ alph(s) = alph(t)\,\}$. Since w starts and ends with the same letter, $r(w)$ is a well defined positive integer. Let p and q be respectively the left and the right factor of w of length equal to $r(w)$. There are three cases to consider: either $w = pq$; $w = pbq$ with $b \in A$; or finally $w = pbucq$, where $u \in A^*$, b, c are distinct letters and at least one of them, without loss of generality say b, does not lie in $alph(p)$. In the first case our result follows immediately since clearly $|alph(w)| = |alph(p)| \leq |p| = |w|/2 = \lceil |w|/2 \rceil$. Similarly in the second one $|alph(w)| \leq |alph(p)| + 1 \leq |p| + 1 = \lceil |w|/2 \rceil$. Finally in the third one we have $alph(w) = alph(pbuc) = alph(p) \cup alph(buc)$, hence $|alph(w)| \leq |alph(p)| + |alph(buc)|$. Since $b \neq c$, Case (1) yields $|alph(buc)| \leq \lceil |buc|/2 \rceil$, so that $|alph(w)| \leq |p| + \lceil |buc|/2 \rceil = \lceil (2|p| + |buc|)/2 \rceil = \lceil |w|/2 \rceil$. □

Corollary 3.4 *If w is a word of A^* with $|alph(w)| > \lceil |w|/2 \rceil$ then $c(w) = 1$.*

Proof: Suppose that $c(w) = m$ where m is a non-negative integer with $m \neq 1$. If $m = 0$ then $l^*(w) = 0$ over $\mathbb{Z}$, hence by Theorem 3.3 for $K = \mathbb{Z}$ we get $|alph(w)| \leq \lceil |w|/2 \rceil$, a contradiction. If $m > 1$ then $l^*(w) \in (m)\mathbb{Z}\langle A\rangle$ by Theorem 2.7 (i). Thus if $\overline{l^*}$ is the adjoint of the left-normed Lie bracketing $\overline{l}$ over

$\mathbb{Z}_m$, we get $\overline{l^*}(w) = \overline{0}$. Once more Theorem 3.3, this time for $K = \mathbb{Z}_m$, yields $|alph(w)| \le \lceil |w|/2 \rceil$, the same contradiction. □

Recall that by Lemma 2.11 (iii) if A and Σ are finite alphabets with $|A| > |\Sigma| \geq 2$ and ϕ is a literal morphism from A^* onto Σ^* then $\phi(\ker l^*_A) = \ker l^*_\Sigma$ and $\ker l^*_A$ is a proper subset of $\phi^{-1}(\ker l^*_\Sigma)$. It is worth asking the following: *is it possible to have a solution w of the equation $l^*_\Sigma(w) = 0$ with $alph(w) = \Sigma$ that can not be the image, under* any *literal surjective morphism $\phi : A^* \twoheadrightarrow \Sigma^*$, of a corresponding solution u of the equation $l^*_A(u) = 0$ with $alph(u) = A$?* If $|w| = n$ Theorem 3.3 implies that our question makes sense when in fact $\lceil n/2 \rceil \geq |A| > |\Sigma|$.

The following example demonstrates that this is indeed possible.

Example 3.5 *Set $K = \mathbb{Z}_2$, $A = \{a, b, c, d\}$, $\Sigma = \{e, f, g\}$ and $w = efegfef$. Then $w \in \ker l^*_\Sigma$ but for each literal morphism ϕ from A^* onto Σ^* no word u with $alph(u) = A$ and $\phi(u) = w$ lies in $\ker l^*_A$.*

Proof: All calculations are made over $\mathbb{Z}_2$. We apply Proposition 3.1 for all factors of length 3 in w. Since $l^*(efe) = l^*(fef) = 0$ and $e \sqcup\!\sqcup fef = fe \sqcup\!\sqcup ef = efe \sqcup\!\sqcup f = efef + fefe,$ we get

$$\begin{aligned} l^*_\Sigma(w) &= l^*_\Sigma(feg)\{e \sqcup\!\sqcup fef\} + l^*_\Sigma(egf)\{fe \sqcup\!\sqcup ef\} + l^*_\Sigma(gfe)\{efe \sqcup\!\sqcup f\} \\ &= \{l^*_\Sigma(feg) + l^*_\Sigma(egf) + l^*_\Sigma(gfe)\}\{efef + fefe\}. \end{aligned}$$

All terms in $l^*_\Sigma(feg) + l^*_\Sigma(egf) + l^*_\Sigma(gfe)$ cancel out, and therefore we obtain $l^*_\Sigma(w) = 0$.

Now consider an arbitrary surjective map ϕ from A onto Σ and an arbitrary word $u \in \phi^{-1}(\{w\})$ with $alph(u) = A$. Without loss of generality we may assume that $\phi(a) = e$, $\phi(b) = f$, $\phi(d) = g$ and $\phi(c) \in \{e, f\}$. Indeed if $\phi(c) = g$ then $alph(u)$ is either equal to $\{a, b, c\}$ or to $\{a, b, d\}$ which in both cases is a proper subset of A. We may also assume that $\phi(c) = f$; the case $\phi(c) = e$ is handled in a similar manner. Then $u = apadqar$, where p, q and r are either equal to b or c. We will show that $l^*_A(u) \neq 0$. Suppose the contrary. Since $r \neq a$ we get $l^*_A(padqar) = 0$, so by Theorem 3.3 $|alph(padqar)| \leq 3$. On the other hand, clearly $alph(padqar) = alph(u) = A$, so that $|alph(padqar)| = 4$ and we reach a contradiction. □

4 Combinatorial interpretation of $\mathbf{l}^*$

It is customary for many problems on free Lie algebras to boil down to particular combinatorial questions on the group algebra of the symmetric group. This will also be the case for the Schützenberger problems.

We start from the *place permutation action* of the symmetric group $\mathfrak{S}_n$ on n letters, on the set of words of length n, where if $w = x_1x_2 \ldots x_n$ and $\sigma \in \mathfrak{S}_n$ we have $(x_1x_2 \ldots x_n) \cdot \sigma = x_{\sigma(1)}x_{\sigma(2)} \ldots x_{\sigma(n)}$. This is a right action of $\mathfrak{S}_n$ that extends by linearity to a right action of the group ring $K\mathfrak{S}_n$ on the n-th homogeneous component of the free associative algebra $K\langle A\rangle$ (e.g., see [14, §8.1]). Viewing each permutation in $\mathfrak{S}_n$ as a word in n distinct letters, the left-normed multi-linear Lie bracketing of the free Lie algebra, denoted by l_n, is known as the *Dynkin operator* and can be viewed as an element of $K\mathfrak{S}_n$ defined by

$$(x_1x_2 \ldots x_n) \cdot l_n \;=\; l(x_1x_2 \ldots x_n). \tag{4.1}$$

For a non-negative integer k let $[k]$ denote the set $\{1, 2, \ldots, k\}$, when $k \geq 1$, or the empty set, when $k = 0$. A *descent* of a permutation $\sigma \in \mathfrak{S}_n$ is a position $i \in [n-1]$ for which $\sigma(i) > \sigma(i+1)$. Let

$D(\sigma)$ be the set of all descents of σ and for $X \subseteq [n-1]$ let $D_X = \sum_{D(\sigma)=X} \sigma \in K\mathfrak{S}_n$. Then the following formulae for l_n are well known (see [14, Theorem 8.16]):

$$\begin{aligned} l_n &= (\mathbf{1}-\zeta_2)(\mathbf{1}-\zeta_3)\cdots(\mathbf{1}-\zeta_n) && (4.2)\\ &= \sum_{k=1}^{n}(-1)^{k-1}D_{[k-1]}\,, && (4.3)\end{aligned}$$

where $\mathbf{1}$ denotes the identity permutation and ζ_k the descending k-cycle $(k\ \ldots\ 2\,1)$. Note that in (4.2) the products $\sigma\tau$ of permutations $\sigma, \tau \in \mathfrak{S}_n$ are to be read from right to left: first τ and then σ. It is well known that the elements D_X span a subalgebra of rank 2^{n-1} of the group algebra $\mathbb{Q}\mathfrak{S}_n$, called the *Solomon descent algebra* and denoted by $\mathcal{D}_n$ (e.g., see [16] and cf. [14, Chapter 9]). By (4.3) it follows that l_n lies in $\mathcal{D}_n$.

We also define l_n^* to be the element of $K\mathfrak{S}_n$ such that

$$(x_1x_2\ldots x_n)\cdot l_n^* \;=\; l^*(x_1x_2\ldots x_n)\,, \tag{4.4}$$

where $x_1x_2\ldots x_n$ is a word in n distinct letters and obtain the following result.

Lemma 4.1 ***(i)*** *Suppose that* $l_n = \sum_{\sigma\in\mathfrak{S}_n}\alpha_\sigma\sigma$ *and* $l_n^* = \sum_{\sigma\in\mathfrak{S}_n}\beta_\sigma\sigma$*. Then* $\beta_\sigma = \alpha_{\sigma^{-1}}$*.*

(ii) $\quad l_n^* \;=\; (\mathbf{1}-\zeta_n^{-1})\cdots(\mathbf{1}-\zeta_3^{-1})(\mathbf{1}-\zeta_2^{-1})\,.$

Proof: (i) The coefficients β_σ and $\alpha_{\sigma^{-1}}$ are related via the canonical scalar product in $K\langle A\rangle$ defined by (2.4) in the following way:

$$\begin{aligned}\beta_\sigma &= \big((x_1x_2\ldots x_n)\cdot l_n^*,\quad x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)}\big) && \text{[by definition]}\\ &= \big(l^*(x_1x_2\ldots x_n),\quad x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)}\big) && \text{[by (4.4)]}\\ &= \big(l(x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)}),\quad x_1x_2\ldots x_n\big) && \text{[by (2.5)].}\end{aligned}$$

Setting new variables $y_i = x_{\sigma(i)}$ for $i\in[n]$ we have $y_{\sigma^{-1}(i)} = x_i$, so we obtain

$$\begin{aligned}\beta_\sigma &= \big(l(y_1y_2\ldots y_n),\quad y_{\sigma^{-1}(1)}y_{\sigma^{-1}(2)}\cdots y_{\sigma^{-1}(n)}\big)\\ &= \big((y_1y_2\ldots y_n)\cdot l_n,\quad y_{\sigma^{-1}(1)}y_{\sigma^{-1}(2)}\cdots y_{\sigma^{-1}(n)}\big) && \text{[by (4.1)]}\\ &= \alpha_{\sigma^{-1}} \qquad \text{[by definition].}\end{aligned}$$

(ii) Let $\sigma_1, \sigma_2, \ldots, \sigma_k$ be arbitrary elements of $\mathfrak{S}_n$. By induction on k it is straightforward to check that if $(\mathbf{1}-\sigma_1)(\mathbf{1}-\sigma_2)\cdots(\mathbf{1}-\sigma_k) = \sum_{\sigma\in\mathfrak{S}_n}\gamma_\sigma\sigma$ then $(\mathbf{1}-\sigma_k^{-1})(\mathbf{1}-\sigma_{k-1}^{-1})\cdots(\mathbf{1}-\sigma_1^{-1}) = \sum_{\sigma\in\mathfrak{S}_n}\gamma_\sigma\,\sigma^{-1}$. Our result then follows from this property and part (i). □

We carry on with some preliminaries on set partitions and tabloids. A *composition* λ of a positive integer n into r positive parts, written $\lambda \models n$, is an ordered sequence $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ of positive integers such that $\sum_{j=1}^{r} \lambda_j = n$. If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$ then λ is called an *(integer) partition* of n, written $\lambda \vdash n$. An *ordered set partition* (or *set composition*) P of $[n]$ into r parts is an ordered r-tuple $P = (I_1, I_2, \ldots, I_r)$ of r pairwise disjoint non empty subsets I_k of $[n]$ (called *blocks*) whose union is $[n]$. If we forget the ordering of the blocks and consider just the collection $\pi = \{I_1, I_2, \ldots, I_r\}$ we obtain an *(unordered) set partition* π of $[n]$ into r parts. The *type* of P is the composition $\lambda(P) = (|I_1|, |I_2|, \ldots, |I_r|)$ of n and its length $l(P)$ is the number of blocks r. Let Π_n^r (respectively Δ_n^r) denote the set of ordered (respectively unordered) partitions of $[n]$ with r blocks and Π_n (respectively Δ_n) be the set of all ordered (respectively unordered) set partitions of $[n]$. Let also $\mathcal{T}_n^\lambda$ be the set of ordered partitions of given type $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$, where $\lambda \models n$. This is nothing but the set of λ-*tabloids*. (Note that λ-tabloids are usually defined for $\lambda \vdash n$ as row equivalence classes of *Young tableaux of shape* λ (see [15, Def. 2.1.4]), but the same can be done in general for $\lambda \models n$ since the definition of a tableau is extended to compositions in the obvious way (cf. [15, p. 67]).)

It is well known (see [6, §6.1]) that $|\Delta_n^r|$ is equal to the *Stirling number of the second kind*, denoted by $\left\{ {n \atop r} \right\}$, which can be computed by the sum $\frac{1}{r!} \sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^n$ and $|\Delta_n|$ is equal to the n-th *Bell number* B_n which can recursively be defined as $B_0 = 1$ and $B_n = \sum_{i=0}^{n-1} \binom{n-1}{i} B_i$. Then $|\Pi_n^r|$ is equal to $r! \left\{ {n \atop r} \right\}$, since each element in Δ_n^r yields $r!$ distinct elements in Π_n^r by permuting its blocks. On the other hand, clearly $|\mathcal{T}_n^\lambda|$ is equal to the multinomial coefficient $\binom{n}{\lambda} := \binom{n}{\lambda_1,\, \lambda_2,\, \ldots,\, \lambda_r} = \frac{n!}{\lambda_1! \lambda_2! \cdots \lambda_r!}$.

Following Sagan in [15, Def. 5.5.7] each $\pi \in \Delta_n^r$ may be written uniquely in the form of a special ordered partition, called the *tabloid form* of π, which is defined as

$$\mathcal{P} \;=\; I_1/I_2/\ldots/I_r\,, \tag{4.5}$$

where numbers in each block are written in the natural increasing order; blocks are listed in weakly decreasing order of size and furthermore blocks of equal size are arranged in increasing order of their minimal elements. The *type* of π is then the integer partition $\lambda(\pi) = (|I_1|, |I_2|, \ldots, |I_r|)$ of n. For example the partition $\pi = \{\{1,2\}, \{4,7,8\}, \{3,5,6\}\}$ of [8] is written in tabloid form as $\mathcal{P} = 3,5,6\,/\,4,7,8\,/\,1,2$ and is of type $(3,3,2)$.

Let $P, Q \in \Pi_n$. We say that P *refines* Q and write $P \preceq Q$ if each block of P is a subset of some block of Q. The relation $\preceq$ on Π_n is reflexive and transitive. We have $P \preceq Q$ and $Q \preceq P$ if and only if Q may be obtained by rearranging the blocks of P. In this case we write $P \simeq Q$ and obtain an equivalence relation $\simeq$ in Π_n. The set of its equivalence classes is then clearly identified with the set Δ_n of unordered set partitions of $[n]$ which inherits the refinement order $\preceq$ from Π_n. The n-block partition $1\,/2\,/\,\ldots\,/\,n$ and the 1-block partition $1, 2, \ldots, n\,/$ appear respectively at the bottom and at the top of the *Hasse diagram* of the partially ordered set $(\Delta_n, \preceq)$.

The symmetric group $\mathfrak{S}_n$ acts naturally from the left on the sets Δ_n^r, Π_n^r and $\mathcal{T}_n^\lambda$ defined above, simply by permuting the entries in the blocks of a set partition or a tabloid. For a commutative ring K with unity let D_n^r, P_n^r and T_n^λ be the K-modules freely generated by the sets Δ_n^r, Π_n^r and $\mathcal{T}_n^\lambda$, respectively. Extending the permutation action of $\mathfrak{S}_n$ linearly to D_n^r, P_n^r and T_n^λ these become left permutation $K\mathfrak{S}_n$-modules.

In Problem 1.2 we search for words w with $|w| = n$ and $|alph(w)| = r$ that vanish under l^*. By Lemma 2.11 (ii) if B_1 and B_2 are sub-alphabets of cardinality r of A then $\ker l^*_{B_1}$ is identified with $\ker l^*_{B_2}$. Therefore, without loss of generality, we may fix a sub-alphabet $B = \{a_1, a_2, \dots a_r\}$ of A with the natural total order $a_1 < a_2 < \cdots < a_r$ and consider the set $\mathcal{W}^r_n$ of all words w with $|w| = n$ and $alph(w) = B$. The mapping $w \mapsto \{w\}$ from $\mathcal{W}^r_n$ to Π^r_n that sends a word $w = x_1x_2\dots x_n \in \mathcal{W}^r_n$ to the ordered partition $\{w\} = (I_1(w), I_2(w), \dots, I_r(w))$, where for each $k \in [r]$ the set $I_k(w)$ consists of the positions in $[n]$ where the letter a_k occurs in w, is clearly a bijection. Moreover, if $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r) \models n$ we can also consider the set $\mathcal{W}^\lambda_n$ of all words w of multi-degree $(\lambda_1, \lambda_2, \dots, \lambda_r)$ in B, i.e., $|w|_{a_k} = \lambda_k$ for each $k \in [r]$. The ordered partition $\{w\}$ is then a λ-tabloid, hence the restriction of the map $w \mapsto \{w\}$ to $\mathcal{W}^\lambda_n$ is a bijection between the set of words $\mathcal{W}^\lambda_n$ and the set $\mathcal{T}^\lambda_n$ of λ-tabloids. For example, for $\lambda = (3, 3, 1, 1)$ and $B = \{a, b, c, d\}$, the word $w = aacbdbba$ is represented by the tabloid $1, 2, 8 \,/\, 4, 6, 7 \,/\, 3 \,/\, 5$. By changing our initial order on B to another one which makes $\lambda = (|w|_{a_1}, |w|_{a_2}, \dots, |w|_{a_r})$ an integer partition of n, we may, without loss of generality, assume that $\lambda \vdash n$ and consider only the sets $\mathcal{W}^\lambda_n$ and $\mathcal{T}^\lambda_n$ for $\lambda \vdash n$.

Let W^r_n be the K-span of $\mathcal{W}^r_n$ in $K\langle B\rangle$ and W^λ_n be the set of all polynomials on B over K of multi-degree $(\lambda_1, \lambda_2, \dots, \lambda_r)$. The symmetric group $\mathfrak{S}_n$ acts on the sets $\mathcal{W}^r_n$ and $\mathcal{W}^\lambda_n$ from the right by place permutations. Extending these actions naturally to W^r_n and W^λ_n the latter become right permutation modules for $\mathfrak{S}_n$. We compare the left action of $\mathfrak{S}_n$ on P^r_n and T^λ_n with the right action of $\mathfrak{S}_n$ on W^r_n and W^λ_n, respectively by the following results.

Lemma 4.2 *Let w be a word of length n and σ be an arbitrary permutation in the symmetric group $\mathfrak{S}_n$ on n letters. Then*

$$\sigma \cdot \{w\} \;=\; \{w \cdot \sigma^{-1}\}\,.$$

Proof: Since $\{w\} = (I_1(w), I_2(w), \dots, I_r(w))$ it suffices to show that $I_k(w \cdot \sigma^{-1}) = \sigma \cdot I_k(w)$, for each $k \in [r]$. By definition $I_k(w) = \{i \in [n] \,:\, x_i = a_k\}$, hence clearly $\sigma \cdot I_k(w) = \{\sigma(i) \in [n] \,:\, x_i = a_k\} = \{j \in [n] \,:\, x_{\sigma^{-1}(j)} = a_k\} = I_k(w \cdot \sigma^{-1})$. $\square$

We extend by linearity the bijective mapping $w \mapsto \{w\}$ from $\mathcal{W}^r_n$ to Π^r_n to a K-module isomorphism f from W^r_n to P^r_n defined as $f(\sum_w k_w w) = \sum_w k_w \{w\}$, for a typical element $\sum_w k_w w \in W^r_n$.

Theorem 4.3 *The right action of the symmetric group $\mathfrak{S}_n$ on the polynomials W^r_n (respectively W^λ_n, where $\lambda \vdash n$) is equivalent to the left action of $\mathfrak{S}_n$ on the K-space of ordered partitions P^r_n of $[n]$ into r parts (respectively on λ-tabloids T^λ_n). Moreover,*

$$f(w \cdot l^*_n) \;=\; l_n \cdot \{w\}\,.$$

Proof: If we define $\sigma \circ w = w \cdot \sigma^{-1}$ for $\sigma \in \mathfrak{S}_n$ and $w \in \mathcal{W}^r_n$, we have also a left action of $\mathfrak{S}_n$ on $\mathcal{W}^r_n$ and consequently on W^r_n. In view of Lemma 4.2 one can show that $f(\sigma \circ P) = \sigma \cdot f(P)$, for a polynomial $P \in W^\lambda_n$. As a result the corresponding left $K\mathfrak{S}_n$-modules W^r_n and P^r_n are isomorphic. The restriction of f to W^λ_n is an isomorphism of W^λ_n onto T^λ_n. The second part of the theorem follows directly from Lemma 4.2 and Lemma 4.1 (i). $\square$

Consider the involution τ_n of the symmetric group $\mathfrak{S}_n$ written as

$$\tau_n \;=\; \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (i,\, n - i + 1)\,. \tag{4.6}$$

Lemma 4.4 *The right action of l_n^* on $\tilde{w}$ is equivalent to the left action of l_n to the tabloid $\tau_n \cdot \{w\}$, i.e.,*

$$f(\tilde{w} \cdot l_n^*) \;=\; l_n \cdot (\tau_n \cdot \{w\})\,.$$

Proof: Clearly $w \cdot \tau_n = \tilde{w}$ so if we apply Lemma 4.2 for $\sigma = \tau_n$ we obtain $\tau_n \cdot \{w\} = \{\tilde{w}\}$. The result then follows from Theorem 4.3. □

A major implication of the isomorphism established in Theorem 4.3 is the equivalence

$$\boxed{w \cdot l_n^* \;=\; 0 \quad \Longleftrightarrow \quad l_n \cdot \{w\} \;=\; 0}\,, \tag{4.7}$$

so Problem 1.2 takes the following form.

Problem 4.5 *Let m be a positive integer with $m \neq 1$. Find all unordered set partitions of $[n]$, written in tabloid form $\mathcal{P} = I_1/I_2/\ldots/I_r$, with the property that $\mathcal{P}$ satisfies*

$$l_n \,\cdot\, \mathcal{P} \;=\; 0\,, \tag{4.8}$$

where l_n is the left-normed multi-linear Lie bracketing viewed as an element of the group ring $\mathbb{Z}_m\mathfrak{S}_n$.

A few points need to be clarified here.

1. Theorem 3.3 imposes the restriction $r = l(\mathcal{P}) \leq \lceil n/2 \rceil$ in (4.8). Fix such a length r. If a specific ordered partition $P = (I_1, I_2, \ldots, I_r)$ satisfies (4.8) then by Lemma 2.11 (ii) and the equivalence (4.7) all $r!$ ordered partitions formed by permutations of its blocks will also be solutions of (4.8). Hence it suffices to consider only ordered partitions in tabloid form, i.e., unordered partitions, of length r where $2 \leq r \leq \lceil n/2 \rceil$, since the 1-block partition is always a trivial solution of (4.8).

2. If B_1 and B_2 are sub-alphabets of A with $B_1 \supset B_2$, ϕ is a literal surjective morphism from B_1^* onto B_2^* and there exists a word $w \in B_1^*$ such that $l_n \cdot \{w\} = 0$ then Lemma 2.11 (i) and the equivalence (4.7) imply that also $l_n \cdot \{\phi(w)\} = 0$. Consequently, if $P, Q \in \Pi_n$, P is a solution of (4.8) and $P \preceq Q$ then Q will also satisfy (4.8).

3. In view of the two previous remarks to solve Problem 4.5 we must determine the smallest set of unordered partitions $\mathcal{P}$ in tabloid form (4.5) with r parts that satisfy (4.8) and generate all solutions of (4.8) in the sense that every other solution will be a partition $\mathcal{Q}$ refined by $\mathcal{P}$ and moreover $\mathcal{P}$ can not itself be refined by some other solution $\mathcal{R}$ of (4.8) with more than r parts. We search for such a set of minimal solutions starting from partitions of length $\lceil n/2 \rceil$ and moving up on in the Hasse diagram of the partially ordered set $(\Delta_n, \preceq)$.

   For example, when $n = 5$ and $m = 2$ one can show that the solutions with 3 parts are the tabloids of the form $1, 3, 5 \,/\, 2 \,/\, 4$ and $1, 5 \,/\, 2, 4 \,/\, 3$ and every solution with 2 parts is generated from those. On the other hand, for $n = 7$ and $m = 2$ we have the solution $1, 3, 6 \,/\, 2, 5, 7 \,/\, 4$ with 3 parts which can not be refined by any solution with 4 parts; the latter follows directly from Example 3.5.

In characteristic zero Theorem 3.2 and the equivalence (4.7) yield the following result, which - according to our knowledge - has not been traced in the literature.

Proposition 4.6 *Let $\lambda \vdash n$. The λ-tabloids that satisfy the equation*

$$l_n \cdot t = 0 ,$$

where l_n is the Dynkin operator of the free Lie ring, are either the 1-block partition $1, 2, \ldots, n \,/$ or the tabloids t which, when viewed as partitions of $[n]$, are refined by the tabloid

$$1, n \,/\, 2, n-1 \,/\, 3, n-2 \,/ \ldots /\, k, k+1 , \tag{4.9}$$

for $n = 2k$.

We also present the equivalent of Conjecture 2.9 stated in λ-tabloid form.

Conjecture 4.7 *Let $\lambda \vdash n$, l_n be the Dynkin operator of the free Lie ring and t_1 and t_2 be λ-tabloids with both $l_n \cdot t_1$ and $l_n \cdot t_2$ different from zero. Then*

(i) $l_n \cdot t_1 = l_n \cdot t_2$ *if and only if* $t_1 = t_2$ *or n is odd and* $t_1 = \tau_n \cdot t_2$.

(ii) $l_n \cdot t_1 = - l_n \cdot t_2$ *if and only if* n *is even and* $t_1 = \tau_n \cdot t_2$.

We conclude this section with a few remarks on the case $m = 2$. It is easy to show by induction that palindromes of length $n > 1$, where n might be even or odd, lie in the kernel of l^*. The latter correspond of course to tabloids of the form

$$t = 1, n \,/\, 2, n-1 \,/\, 3, n-2 \,/ \ldots /\, r, r+2 \,/\, r+1 , \tag{4.10}$$

where $n = 2r + 1$. By an easy induction on r we also get the hook-shaped solution

$$1, 3, 5, \ldots, 2r+1 \,/\, 2 \,/\, 4 \,/\, 6 \,/ \ldots /\, 2r . \tag{4.11}$$

We conjecture that (4.10) and (4.11) are the only solutions of (4.8) with $r + 1$ parts when $n = 2r + 1$. For $n = 2r$, except from tabloids of the form (4.9) that correspond to palindromes of even length, there exist other solutions with r parts. For example for $n = 6$ we have also the solutions $1, 3, 5 \,/\, 2, 6 \,/\, 4$; $1, 3, 6 \,/\, 2, 5 \,/\, 4$; $1, 4, 6 \,/\, 2, 5 \,/\, 3$ and $2, 4, 6 \,/\, 1, 5 \,/\, 3$. Nevertheless, we conjecture that the only solution of type $(2, 2, \ldots, 2)$ with r parts is of the form (4.9).

5 Pascal descent polynomials

In this section we restrict ourselves to words of length n where only two letters occur and consider the corresponding set Δ_n^2 of all unordered set partitions of $[n]$ with 2 parts. It is known [6, p. 258] that $|\Delta_n^2| = \left\{ {n \atop 2} \right\} = 2^{n-1} - 1$. Such a partition is written in tabloid form $J \,/\, I$, so it is uniquely determined by the subset $I = \{i_1, i_2, \ldots, i_s\}$ of $[n]$ appearing in its second block and will be denoted accordingly by $\overline{I}$; when $I = \{i\}$ for brevity we will write $\overline{i}$.

We define a mapping ψ from the set Π_n^2 of ordered partitions with 2 parts to the polynomial algebra $K[x_1, x_2, \ldots, x_n]$ in n commuting variables that sends $\overline{I}$ - viewed as an ordered partition - to the monomial $x_I = x_{i_1} x_{i_2} \cdots x_{i_s}$. In the extreme case where $I = \emptyset$ we set $x_I = 1$. The mapping ψ is extended by linearity to a $K\mathfrak{S}_n$-module isomorphism, also denoted by ψ, from P_n^2 to $K[x_1, x_2, \ldots, x_n]$, under the natural place permutation actions of the symmetric group $\mathfrak{S}_n$ in each case.

Let $h_n(I)$ be the image under ψ of the element $l_n \cdot \overline{I}$; for simplicity we write $h_n(i)$ instead of $h_n(\{i\})$. Let us clarify this definition a bit more. Suppose that $l_n = \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma \sigma$. Then we obtain

$$h_n(I) \;=\; \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma \psi(\sigma\cdot\overline{I}) \;=\; \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma \psi\overline{(\sigma(I))} \;=\; \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma x_{\sigma(I)}. \tag{5.1}$$

The polynomial $h_n(I)$ is multi-linear and homogeneous of total degree s.

Let now N be a positive integer with $N > n$ and set $[n+1, N] = [N] \setminus [n]$. It will be useful for us to extend the definition of $h_n(I)$ to subsets of $[N]$. We do this by using the last equality of (5.1), i.e., $h_n(I) = \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma x_{\sigma(I)}$, and by identifying $\mathfrak{S}_n$ with the set of permutations $\sigma \in \mathfrak{S}_N$ that leave the subset $[n+1, N]$ of $[N]$ point-wise invariant. We obtain the following technical result.

Lemma 5.1 *Let n, N be positive integers with $n < N$ and $I \subseteq [N]$ such that $J = I \cap [n+1, N] \neq \emptyset$. Then*

$$h_n(I) \;=\; h_n(I\setminus J)\, x_J\,.$$

Proof: In view of the aforementioned identification let $\sigma \in \mathfrak{S}_n$. Then $\sigma(I)$ is the disjoint union of $\sigma(I \setminus J)$ and J since $\sigma(J) = J$, so that (5.1) yields

$$h_n(I) \;=\; \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma x_{\sigma(I)} \;=\; \sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma x_{\sigma(I\setminus J)} x_J \;=\; \Big[\sum_{\sigma\in\mathfrak{S}_n} \alpha_\sigma x_{\sigma(I\setminus J)}\Big]\, x_J \;=\; h_n(I\setminus J)\, x_J,$$

as required. $\square$

Lemma 5.2 *Let $I \subseteq [n]$. Then the polynomial $h_n(I)$ is recursively defined as*

$$h_n(I) = \begin{cases} (-1)^{i-1}\dbinom{n-1}{i-1}\{x_1 - x_2\}, & \textit{if } \; I = \{i\}; \\ h_{n-1}(I) \;-\; h_{n-1}(\zeta_n I), & \textit{otherwise,} \end{cases}$$

where ζ_n denotes the descending cycle $(n\ \ldots\ 2\,1)$.

Proof: For $I = \{i\}$ Theorem 4.3 and Lemma 2.8 (i) yield

$$\begin{aligned} h_n(i) \;=\; \psi(l_n\cdot\overline{i}\,) \;&=\; \psi\Big(f\big((a^{i-1}ba^{n-i})\cdot l_n^*\big)\Big) \;=\; \psi\Big(f\big(l^*(a^{i-1}ba^{n-i})\big)\Big) \\ &=\; (\psi\circ f)\big((-1)^{i-1}\binom{n-1}{i-1}\{ba^{n-1} - aba^{n-2}\}\big) \\ &=\; (-1)^{i-1}\binom{n-1}{i-1}\{(\psi\circ f)(ba^{n-1}) - (\psi\circ f)(aba^{n-2})\} \\ &=\; (-1)^{i-1}\binom{n-1}{i-1}\{(\psi(\overline{1}) - \psi(\overline{2})\} \;=\; (-1)^{i-1}\binom{n-1}{i-1}\{x_1 - x_2\}. \end{aligned}$$

When $|I| > 1$ we argue by induction on n, where $n \geq 2$. The case $n = 2$ follows trivially. Using the multiplicative formula (4.2) for l_n the induction step yields

$$\begin{aligned} h_n(I) = \psi(l_n \cdot \overline{I}) &= \psi\big[l_{n-1}(\mathbf{1} - \zeta_n) \cdot \overline{I}\big] \\ &= \psi\big[l_{n-1} \cdot \overline{I} \ - \ l_{n-1} \cdot (\zeta_n \overline{I})\big] \\ &= h_{n-1}(I) - h_{n-1}\big(\zeta_n I\big)\,. \end{aligned}$$

Note that if $n \in I$ or $1 \in I$ we obtain $h_{n-1}(I) = h_{n-1}(I \backslash \{n\})\, x_n$ and $h_{n-1}(\zeta_n I) = h_{n-1}(\zeta_n I \backslash \{n\})\, x_n$, respectively, by Lemma 5.1. □

Proposition 5.3 *Let I be a subset of $[n]$ of cardinality s. The binomial $x_1 - x_2$ divides $h_n(I)$. The corresponding quotient, which we denote by $p_n(I)$, is a multi-linear polynomial of total degree $s - 1$ given by the recursive formula*

$$p_n(I) = \begin{cases} (-1)^{i-1} \dbinom{n-1}{i-1}, & \textit{if } \ I = \{i\}; \\ p_{n-1}(I) \ - \ p_{n-1}(\zeta_n I), & \textit{otherwise,} \end{cases}$$

where whenever I' is a subset of $[n]$ with $n \in I'$ we set $p_{n-1}(I') = p_{n-1}(I' \setminus \{n\})\, x_n$.

Proof: For $s = 1$ the result follows immediately immediately by Lemma 5.2. For $s > 1$ we argue by induction on n. Set $J = I \cap \{n\}$ and $K = \zeta_n\, I \cap \{n\}$. Then clearly $x_J = 1$ when $n \notin I$ and $x_K = 1$ when $1 \notin I$. By Lemma 5.2 we have $h_n(I) = h_{n-1}(I) - h_{n-1}(\zeta_n I)$, so by Lemma 5.1 we obtain $h_n(I) = h_{n-1}(I \setminus J)\, x_J \ - \ h_{n-1}(\zeta_n I \setminus K)\, x_K$. By our induction hypothesis we get $h_{n-1}(I \setminus J) = (x_1 - x_2) \cdot p_{n-1}(I \setminus J)$ and $h_{n-1}(\zeta_n I \setminus K) = (x_1 - x_2) \cdot p_{n-1}(\zeta_n I \setminus K)$. Our result then follows if we set $p_n(I) = p_{n-1}(I \setminus J)\, x_J \ - \ p_{n-1}(\zeta_n I \setminus K)\, x_K$. □

We give the name *Pascal descent polynomial* to $p_n(I)$ since it yields a signed binomial coefficient when $|I| = 1$ and it originates from the additive formula (4.3) which relates to the descent sums $D_{[k-1]}$, for $k \in [n]$.

By Lemma 4.4, the analogue of Lemma 2.1 for Pascal descent polynomials is given by the equation

$$p_n(\tau_n(I)) \ = \ (-1)^{n+1}\, p_n(I), \tag{5.2}$$

where τ_n is the involution of $\mathfrak{S}_n$ defined in (4.6). In particular, if n is even and $\tau_n(I) = I$ then $p_n(I) = 0$.

The following result yields a recursive decomposition of the polynomial $p_n(I)$.

Proposition 5.4 *Let $I = \{a_1, a_2, \ldots, a_d\}$ be a proper subset of $[n]$ of cardinality $d \geq 2$. Set $k = a_1 - 1$ and $l = n - a_d$. Then*

$$p_n(I) \ = \ (-1)^{k+1} \sum_{i=0}^{l} \binom{k+i}{i} p_{n-k-1-i}(D) \cdot x_{n-k-i} \ + \ \sum_{j=0}^{k} (-1)^j \binom{l+j}{j} p_{n-l-1-j}(D_j) \cdot x_{n-l-j},$$

where $D = \{a_2 - a_1,\, a_3 - a_1,\, \ldots,\, a_d - a_1\}$ and $D_j = \{a_1 - j,\, a_2 - j,\, \ldots,\, a_{d-1} - j\}$, for each $j = 0, \ldots, k$.

Proof: We apply Proposition 5.3. The case where $a_1 = 1$ and $a_d = n$ follows trivially. The cases $a_1 = 1,\ a_d < n$ and $a_1 > 1,\ a_d = n$ follow by an immediate induction on n. If $1 < a_1$ and $a_d < n$ the induction on n is a bit more tedious. For $n = 3$ the result is true; one can check it easily for $I = \{1, 2\}$ and $I = \{2, 3\}$. Suppose that it holds for $n = m$. We will show that it also holds for $n = m + 1$. Setting $k = a_1 - 1$ and $l = m + 1 - a_d$, Proposition 5.3 and our induction hypothesis yield

$$
\begin{aligned}
&p_{m+1}(I) \;=\; p_m(I) \;-\; p_m(\{a_1-1, a_2-1, \ldots, a_d-1\})\\
&= (-1)^{k+1}\sum_{i=0}^{l-1}\binom{k+i}{i}p_{m-k-1-i}(D)\cdot x_{m-k-i} \;+\; \sum_{j=0}^{k}(-1)^j\binom{l-1+j}{j}p_{m-l-j}(D_j)\cdot x_{m-l-j+1}\\
&+\;(-1)^{k+1}\sum_{i=0}^{l}\binom{k-1+i}{i}p_{m-k-i}(D)\cdot x_{m-k-i+1} \;+\; \sum_{j=0}^{k-1}(-1)^{j+1}\binom{l+j}{j}p_{m-l-1-j}(D_{j+1})\cdot x_{m-l-j}\\
&= (-1)^{k+1}\Big\{\sum_{i=1}^{l}\binom{k+i-1}{i-1}p_{m-k-i}(D)\cdot x_{m-k-i+1} + \sum_{i=0}^{l}\binom{k+i-1}{i}p_{m-k-i}(D)\cdot x_{m-k-i+1}\Big\}\\
&+\;\Big\{\sum_{j=0}^{k}(-1)^j\binom{l-1+j}{j}p_{m-l-j}(D_j)\cdot x_{m-l-j+1} \;+\; \sum_{j=1}^{k}(-1)^j\binom{l-1+j}{j-1}p_{m-l-j}(D_j)\cdot x_{m-l-j+1}\Big\}\\
&= (-1)^{k+1}\Big\{\sum_{i=1}^{l}\Big[\binom{k+i-1}{i-1}+\binom{k+i-1}{i}\Big]p_{m-k-i}(D)\cdot x_{m-k-i+1} \;+\; p_{m-k}(D)\cdot x_{m-k+1}\Big\}\\
&+\;\Big\{\sum_{j=1}^{k}(-1)^j\Big[\binom{l-1+j}{j}+\binom{l-1+j}{j-1}\Big]p_{m-l-j}(D_j)\cdot x_{m-l-j+1} \;+\; p_{m-l}(D_0)\cdot x_{m-l+1}\Big\}\\
&= (-1)^{k+1}\Big\{\sum_{i=1}^{l}\binom{k+i}{i}p_{m-k-i}(D)\cdot x_{m-k-i+1} \;+\; \binom{k+0}{0}p_{m-k}(D)\cdot x_{m-k+1}\Big\}\\
&+\;\Big\{\sum_{j=1}^{k}(-1)^j\binom{l+j}{j}p_{m-l-j}(D_j)\cdot x_{m-l-j+1} \;+\; (-1)^0\binom{l+0}{0}p_{m-l}(D_0)\cdot x_{m-l+1}\Big\}\\
&= (-1)^{k+1}\sum_{i=0}^{l}\binom{k+i}{i}p_{m-k-i}(D)\cdot x_{m-k-i+1} \;+\; \sum_{j=0}^{k}(-1)^j\binom{l+j}{j}p_{m-l-j}(D_j)\cdot x_{m-l-j+1},
\end{aligned}
$$

as required. □

By way of example let us calculate $p_6(I)$ for the subset $I = \{2, 3, 5\}$ of [6]. We write $p_6(2, 3, 5)$ for brevity and by Proposition 5.4 we obtain

$$
p_6(2,3,5) = \binom{1+0}{0}p_4(1,3)\cdot x_5 + \binom{1+1}{1}p_3(1,3)\cdot x_4 + \binom{1+0}{0}p_4(2,3)\cdot x_5 - \binom{1+1}{1}p_3(1,2)\cdot x_4\,.
$$

Clearly $p_4(2, 3) = 0$ since the subset $\{2, 3\}$ of [4] corresponds to the even palindrome ab^2a. For $p_3(1, 2)$ we obtain $p_3(1, 2) = p_2(1, 2) - p_2(1)\cdot x_3$. Again $\{1, 2\} = [2]$ corresponds to the word b^2 so we have $p_2(1,2) = 0$, hence $p_3(1,2) = -(-1)^{1-1}\binom{2-1}{1-1}x_3 = -x_3$. For the remaining terms we have $p_3(1,3) = p_2(1)\cdot x_3 - p_2(2)\cdot x_3 = (-1)^{1-1}\binom{2-1}{1-1}x_3 - (-1)^{2-1}\binom{2-1}{2-1}x_3 = 2x_3$ and consequently $p_4(1,3) = p_3(1,3) - p_3(2)\cdot x_4 = 2x_3 - (-1)^{2-1}\binom{3-1}{2-1}x_4 = 2x_3 + 2x_4$. Summing up we finally obtain

$$p_6(2,3,5) = 1\cdot(2x_3+2x_4)\cdot x_5 + 2\cdot(2x_3)\cdot x_4 - 2\cdot(-x_3)\cdot x_4 = 6x_3x_4 + 2x_3x_5 + 2x_4x_5.$$

Observe that the greatest common divisor of the coefficients of $p_6(2,3,5)$ is equal to 2, hence the word ab^2aba of length 6, that corresponds to I, has $c(w) = 2$ and therefore does not lie in the support of the free Lie algebra over a field of characteristic 2.

By Theorem 2.7 (i) and the equivalence (4.7) established by Theorem 4.3, if we consider words on a two-lettered alphabet Problem 1.2 will be equivalent to the following.

Problem 5.5 *Let m be a non-negative integer with $m \neq 1$. Find all set partitions J / I of $[n]$ with the property that*

$$p_n(I) \equiv 0 \pmod{m}.$$

For $m = 0$ Proposition 4.6 implies that the only solutions to Problem 5.5 are - except from the trivial solution where $I = \emptyset$, for each n - all the subsets I of $[n]$ fixed by the involution τ_n defined by (4.6), when n is even.

For $m > 1$ our next result provides a necessary condition - stated explicitly on n, m and I - for $p_n(I) \equiv 0 \pmod{m}$ to hold.

Proposition 5.6 *Let m and n be positive integers with $m > 1$, I be a subset of $[n]$ and $N_n(I)$ be the integer defined as*

$$N_n(I) = \sum_{i\in I}(-1)^{i-1}\binom{n-1}{i-1}.$$

(i) *If $p_n(I) \equiv 0 \pmod{m}$ then $m \mid N_n(I)$.*

(ii) *In particular if m is a prime number p, $n = p^e$ and $p \nmid |I|$ then $p_n(I) \not\equiv 0 \pmod{m}$.*

Proof: (i) We need to relate the polynomial $h_n(I) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ with the integer $N_n(I)$. Let $|I| = s$. We claim that if we set $x_1 = 1$ and $x_2 = x_3 = \cdots = x_n = t$ in $h_n(I)$ we obtain the polynomial specialization

$$h_n(I)(1,t,t,\ldots,t) = N_n(I)\,t^{s-1} - N_n(I)\,t^s. \tag{5.3}$$

If (5.3) is true then it is evident that $m \mid N_n(I)$. Since $h_n(I) = (x_1 - x_2)\,p_n(I)$ by Proposition 5.3, equation (5.3) yields

$$p_n(I)(1,t,t,\ldots,t) = N_n(I)\,t^{s-1}. \tag{5.4}$$

Thus $N_n(I)$ may be given a combinatorial interpretation as the sum of the coefficients appearing in all the monomials of $p_n(I)$.

To prove our claim we use the additive formula (4.3) for l_n. Since $h_n(I) = \psi(l_n \cdot \overline{I})$ we obtain

$$h_n(I) = \sum_{k=1}^{n}(-1)^{k-1}\psi(D_{[k-1]}\cdot\overline{I}\,). \tag{5.5}$$

A typical element of $D_{[k-1]}$ is a permutation π which, when viewed as word in n distinct letters from $[n]$, is written as

$$\pi \;=\; j_1\, j_2\, \ldots\, j_{k-1} \boxed{j_k}\, j_{k+1}\, \ldots\, j_{n-1}\, j_n\,, \tag{5.6}$$

where $j_1 > j_2 > \cdots > j_{k-1} > j_k = 1 < j_{k+1} < \cdots < j_{n-1} < j_n$. Clearly $|D_{[k-1]}| = \binom{n-1}{k-1}$ and $\psi(\pi \cdot \overline{I}) = x_{j_{i_1}} x_{j_{i_2}} \cdots x_{j_{i_s}}$, when $I = \{i_1, i_2, \ldots, i_s\}$. Setting $x_1 = 1$ and $x_2 = x_3 = \cdots = x_n = t$ we obtain

$$\psi(D_{[k-1]} \cdot \overline{I})(1, t, t, \ldots, t) = \begin{cases} \binom{n-1}{k-1} t^{s-1}, & \text{if } k \in I; \\ \\ \binom{n-1}{k-1} t^{s}, & \text{otherwise.} \end{cases} \tag{5.7}$$

Summing up all these elements by (5.5) we obtain

$$h_n(I)(1, t, t, \ldots, t) = \sum_{i \in I} (-1)^{i-1} \binom{n-1}{i-1} t^{s-1} + \sum_{i \notin I} (-1)^{i-1} \binom{n-1}{i-1} t^{s}$$

and our claim follows since $\displaystyle\sum_{i \in I} (-1)^{i-1} \binom{n-1}{i-1} + \sum_{i \notin I} (-1)^{i-1} \binom{n-1}{i-1} = \sum_{i=1}^{n} (-1)^{i-1} \binom{n-1}{i-1} = 0$, by the binomial theorem.

(ii) We claim that $N_n(I) = s$. If this is true the result will follow immediately by part (i) and the assumption $p \nmid s$. To prove the claim it suffices to show that for each $k \in \{0, \ldots, p^e - 1\}$

$$(-1)^k \binom{p^e - 1}{k} \equiv 1 \pmod{p}. \tag{5.8}$$

We write $p^e - 1$ and k in base p respectively as $p^e - 1 = \displaystyle\sum_{t=0}^{e-1} (p-1)\, p^t$ and $k = \displaystyle\sum_{t=0}^{e-1} k_t\, p^t$, where $k_t \in \{0, 1, \ldots, p-1\}$. By Lucas correspondence theorem it is enough to show that $(-1)^l \binom{p-1}{l} \equiv 1 (\mathrm{mod}\, p)$, for each $l \in \{0, \ldots, p-1\}$. The latter follows from the fact that $p \,\Big|\, \binom{p}{l} = \binom{p-1}{l} + \binom{p-1}{l-1}$, which yields $\binom{p-1}{l} \equiv -\binom{p-1}{l-1} \pmod{p}$, and a straightforward induction on l. $\square$

Corollary 5.7 *Let u, v and w be words of length n with $alph(w) = \{a, b\}$; I, J and K be the subsets of $[n]$ consisting of the positions that b occurs in u, v and w, respectively and $N_n(I)$, $N_n(J)$ and $N_n(K)$ be defined as in Proposition 5.6. If m is a non-negative integer with $m \neq 1$ then*

(i) *If $m \nmid N_n(K)$ the word w lies in the support of the free Lie algebra $\mathcal{L}_{\mathbb{Z}_m}(A)$. In particular, if $m = p$, a prime number and $n = p^e$ every word w with $|K| = s$ and $p \nmid s$ lies in the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$.*

(ii) *If u, v is a twin pair of words with respect to $\mathcal{L}_{\mathbb{Z}_m}(A)$ then $N_n(I) \equiv N_n(J) \pmod{m}$.*

(iii) *If u, v is an anti-twin pair of words with respect to $\mathcal{L}_{\mathbb{Z}_m}(A)$ then $N_n(I) \equiv -N_n(J) \pmod m$.*

Proof: Part (i) is a direct consequence of Proposition 5.6. For parts (ii) and (iii) we use Theorem 2.7 (ii). For a twin pair we obtain $l^*(u) - l^*(v) \in (m)\,\mathbb{Z}\langle A\rangle$ which yields $p_n(I) - p_n(J) \equiv 0 \pmod m$ by Theorem 4.3 and our result follows by (5.4). For an anti-twin pair we argue similarly for the polynomial $l^*(u) + l^*(v)$ and its commutative analogue $p_n(I) + p_n(J)$. □

Remarks. The invariant $N_n(I)$ is a partial sum of signed binomial coefficients from the n-th row of the Pascal triangle (starting to count from $n = 0$). Considering this row $\bmod m$, Corollary 5.7 (i) poses the requirement that the signed sum of the entries in the positions appearing in I has to be different from zero $\bmod m$ in order that the word w corresponding to I lies in the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$. In the binary case this simply means that the digit 1 is allowed to appear an odd number of times in these positions; note that the number of appearances of 1's in each row of the Pascal triangle $\bmod 2$ is equal to $2^{b(n)}$, where $b(n)$ is the number of occurrences of 1 in the binary representation of n (e.g., see [17]).

The condition of Corollary 5.7 (i) is sufficient but not necessary since there exist many words w with $m \mid N_n(I)$ that also lie in the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$. For example, for $m = 2$ and $w = a^2b^2a$ we get $I = I(w) = \{2, 3\}$ and $N_5(I) = 2$, but w lies in the support of $\mathcal{L}_{\mathbb{Z}_2}(A)$ since $p_5(I) = x_3 + x_4$ and $c(w) = 1$. On the other hand, for $|I| = 1$ it is a necessary and sufficient condition identified with our theoretical characterization of the support of $\mathcal{L}_{\mathbb{Z}_m}(A)$ and is checked with Kummer's Lemma. Note also that it is even possible to have $N_n(I) = 0$ with $p_n(I) \neq 0$, e.g., for $w = a^2b^2a^2ba^2$ we get $I = \{3, 4, 7\}$ and $N_9(I) = 0$. Similar examples which demonstrate that the converse of Corollary 5.7 (ii) and (iii) does not hold, can be found. For example, consider the words $u = ab^3a^2ba^2$ and $v = a^2b^2a^2b^2a$ of length 9 with corresponding $I = I(u) = \{2, 3, 4, 7\}$ and $J = J(v) = \{3, 4, 7, 8\}$. Then clearly $N_9(I) = N_9(J) = -8$, but $p_9(I) \neq p_9(J)$, as one can check by Proposition 5.4, so that $l^*(u) \neq l^*(v)$ and hence the the words u, v are not twin.

Finally, in view of Reduction Theorem 2.10, Conjecture 4.7 for tabloids boils down to the following one for Pascal descent polynomials.

Conjecture 5.8 *Let I and J be subsets of $[n]$ of cardinality $s \leq \lfloor n/2 \rfloor$ such that $p_n(I) \neq 0$ and $p_n(J) \neq 0$. Then*

(i) *$p_n(I) = p_n(J)$ if and only if $I = J$ or n is odd and $I = \tau_n(J)$.*

(ii) *$p_n(I) = -p_n(J)$ if and only if n is even and $I = \tau_n(J)$.*

For $s = 1$, i.e., when $I = \{i\}$ and $J = \{j\}$, Conjecture 5.8 holds as a special case (for $r = n - 1$, $k = i - 1$ and $l = j - 1$) of the fact that $\binom{r}{k} = \binom{r}{l}$ if and only if $k = l$ or $k = r - l$. The "if" part, known as the *symmetry identity*, follows directly from the definition of binomial coefficients and the "only if" part follows from the inequality $\binom{r}{k} < \binom{r}{k+1}$ when $1 \leq k+1 \leq \lfloor r/2 \rfloor$. This is another indication showing that the Pascal descent polynomial $p_n(I)$ is indeed an extension of the usual notion of the binomial coefficient.

6 Further Research

Various equivalent forms of Conjecture 2.9 on twin and anti-twin words - which, in view of Reduction Theorem 2.10, is enough to prove on a two-lettered alphabet - have been presented in this article and we strongly believe that this will finally be resolved. More precisely one can use the recursive formula of Proposition 3.1 in a manner similar to the proofs of Theorem 3.2 and Theorem 3.3, but as it has turned out so far, a lot more cases in combinatorics on words appear in such a consideration.

In view of Remark 2.4, another equivalent to Conjecture 2.9 which seems to be worth investigating is the following. Suppose that K is a $\mathbb{Q}$-algebra and u and v are words of common multi-degree and length n on a two-lettered alphabet which are not powers of a single letter or palindromes of even length. Then the binomial $u - v$ (respectively $u + v$) can be expressed as a K-linear combination of proper shuffles if and only if either $u = v$ or n is odd and $u = \tilde{v}$ (respectively if n is even and $u = \tilde{v}$).

One is challenged to check this using one of the two well known bases of the shuffle algebra, namely the triangular $\mathbb{Z}$-basis $\{\mathcal{Q}_w : w \text{ not a Lyndon word}\}$, originally due to Radford [12], where $\mathcal{Q}_w = \dfrac{1}{i_1! i_2! \cdots i_k!} l_1^{\sqcup\!\sqcup\, i_1} \sqcup\!\sqcup\, l_2^{\sqcup\!\sqcup\, i_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup\, l_k^{\sqcup\!\sqcup\, i_k}$, and $w = l_1^{i_1} l_2^{i_2} \cdots l_k^{i_k}$ is the unique decreasing decreasing factorization (with respect to the lexicographical order in A^+) of w as a product of Lyndon words with $l_1 > l_2 > \cdots > l_k$ and $i_1, i_2, \ldots, i_k \in \mathbb{N}$ (see [14, §6.1]); and the Lie polynomial $\mathbb{Q}$-basis that corresponds to the decomposition $\bigoplus_{n \geq 0} V_n$, where V_n denotes the subspace of $\mathbb{Q}\langle A\rangle$ generated by the shuffle products of n Lie polynomials (see [14, §6.5.1]).

A completely different approach via Pascal descent polynomials, is to use Proposition 5.4 in order to be able to resolve Conjecture 5.8. We do not yet know how this could lead to a complete solution of Problem 5.5 (probably combined with successive applications of our condition in Proposition 5.6 involving the invariant $N_n(I)$) but we are certain that the right framework for such a search is within the geometry of the Pascal triangle $\bmod m$, which after all is needed even in the simple case where $|I| = 1$.

Finally, in the case where $m = 2$ - the smallest instance of Problem 5.5 - we have made some computations using the computer algebra system GAP 4 and have obtained all solutions up to $n = 12$. (A list of those solutions up to $n = 10$ is presented in the Appendix.)

Acknowledgements

The author wishes to thank Professor G. Duchamp for helpful discussions on this subject — in particular for pointing out Problems 1.3 and 1.4 on twin and anti-twin words - during the author's visit at LIPN (Laboratoire d' Informatique de Paris–Nord) at the University of Paris XIII. He is also indebted to professor A. Konovalov for his advice on computations using GAP 4 to implement the action of l_n on subsets of $[n]$.

Note added in proof

After the submission of this manuscript we followed the guidelines drawn up in Section 6 and quite recently we have finally managed to resolve Conjecture 2.9 in [11] using a combination of techniques from combinatorics of words (mainly the 1st and the 2nd Theorem of Lyndon and Schützenberger) and the shuffle algebra $(K\langle A\rangle, +, \sqcup\!\sqcup)$, where K is a commutative $\mathbb{Q}$-algebra (in particular, the left or right residual of shuffles by a Lie polynomial R).

References

[1] V. Diekert and G. Rozenberg (editors), *The Book of Traces*, World Scientific, 1995.

[2] G. Duchamp, A. Klyachko, D. Krob, J.-Y. Thibon, *Noncommutative symmetric functions III: Deformations of Cauchy and convolution algebras*, Discrete Math. and Theoret. Comp. Sci. 1, (1997), 159-216.

[3] G. Duchamp, É. Laugerotte, J.-G. Luque, *On the support of graph Lie algebras*, Theoret. Comput. Sci. 273 (2002) 283-294.

[4] G. Duchamp, J.-Y. Thibon, *Le support de l'algèbre de Lie libre*, Discrete Math. 76 (1989) 123-132.

[5] N. J. Fine, *Binomial coefficients modulo a prime*, The American Math. Month. 54, no. 10, part 1, (1984) 589-592.

[6] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics : a foundation for computer science*, 2nd ed., Addison-Wesley, 1994.

[7] M. Katsura, Y. Kobayashi, *The shuffle algebra and its derivations*, Theoret. Comput. Sci. 115 (1993) 359-369.

[8] E. E. Kummer, *Über die Ergänzungssätze den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math., 44 (1852) 93-146. Reprinted in his Collected Papers, Vol. 1, 485-538.

[9] M. Lothaire, *Combinatorics on Words*, Encyclopedia of Mathematics and its Applications, Vol. 17, Addison-Wesley, Reading, 1983.

[10] E. Lucas, *Sur les congruences des nombres Eulériens et des coefficients differentiels des fonctions trigonométriques, suivant un module premier*, Bull. de la Soc. Math. de France, 6 (1877) 49-54.

[11] I. Michos, *On twin and anti-twin words in the support of the free Lie algebra*, Preprint, (2010).

[12] D. E. Radford, *A natural ring basis for the shuffle algebra and an application to group schemes*, Jour. of Algebra 58 (1979) 432-454.

[13] R. Ree, *Lie elements and algebra associated with shuffles*, Ann. Math. 68 (1958) 210-220.

[14] C. Reutenauer, *Free Lie Algebras*, London Mathematical Society New Series, Vol. 7, Oxford University Press, London, 1993.

[15] B. E. Sagan, *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*, Second Edition, Graduate Texts in Mathematics, Vol. 203, Springer-Verlag, New York, 2001.

[16] M. Schocker, *The descent algebra of the symmetric group*, Representations of finite dimensional algebras and related topics in Lie theory and geometry, Fields Inst. Comm. 40 (2004) 145-161.

[17] S. Wolfram, *Geometry of binomial coefficients*, The American Mathematical Monthly, 91 (1984) 566-571.

Appendix: Solutions of Problem 5.5 for $\mathbf{m = 2}$ and $\mathbf{n \leq 10}$

For $3 \leq n \leq 10$ and $1 \leq s \leq \lfloor n/2 \rfloor$ we list all subsets I of $[n]$ with cardinality s with the property that $p_n(I) \equiv 0 \pmod 2$. By Corollary 5.7 (i) there are no solutions when n is a power of 2 and s is odd.

$\mathbf{n= 3} \quad \mathbf{s= 1} \quad : \quad \{2\}$

$\mathbf{n= 4} \quad \mathbf{s= 2} \quad : \quad \{1,3\},\ \{1,4\},\ \{2,3\},\ \{2,4\}$

n= 5	**s= 1**	:	$\{2\}$, $\{3\}$, $\{4\}$
	s= 2	:	$\{1,5\}$, $\{2,4\}$
n= 6	**s= 1**	:	$\{3\}$, $\{4\}$
	s= 2	:	$\{1,5\}$, $\{1,6\}$, $\{2,5\}$, $\{2,6\}$, $\{3,4\}$
	s= 3	:	$\{1,3,5\}$, $\{1,3,6\}$, $\{1,4,6\}$, $\{2,3,5\}$, $\{2,4,5\}$, $\{2,4,6\}$
n= 7	**s= 1**	:	$\{2\}$, $\{4\}$, $\{6\}$
	s= 2	:	$\{1,5\}$, $\{1,7\}$, $\{2,4\}$, $\{2,6\}$, $\{3,5\}$, $\{3,7\}$, $\{4,6\}$
	s= 3	:	$\{1,3,6\}$, $\{1,4,7\}$, $\{2,4,6\}$, $\{2,5,7\}$, $\{3,4,5\}$
n= 8	**s= 2**	:	$\{1,5\}$, $\{1,7\}$, $\{1,8\}$, $\{2,5\}$, $\{2,6\}$, $\{2,7\}$, $\{2,8\}$, $\{3,5\}$, $\{3,6\}$, $\{3,7\}$, $\{4,5\}$, $\{4,6\}$, $\{4,7\}$, $\{4,8\}$
	s= 4	:	$\{1,2,7,8\}$, $\{1,3,5,7\}$, $\{1,3,5,8\}$, $\{1,3,6,8\}$, $\{1,4,5,8\}$, $\{1,4,6,8\}$, $\{2,3,5,7\}$, $\{2,3,6,7\}$, $\{2,4,5,7\}$, $\{2,4,6,7\}$, $\{2,4,6,8\}$, $\{3,4,5,6\}$
n= 9	**s= 1**	:	$\{2\}$, $\{3\}$, $\{4\}$, $\{5\}$, $\{6\}$, $\{7\}$, $\{8\}$
	s= 2	:	$\{1,9\}$, $\{2,4\}$, $\{2,6\}$, $\{2,8\}$, $\{3,6\}$, $\{3,7\}$, $\{4,6\}$, $\{4,7\}$, $\{4,8\}$, $\{6,8\}$
	s= 3	:	$\{1,5,9\}$, $\{2,4,6\}$, $\{2,4,8\}$, $\{2,5,7\}$, $\{2,5,8\}$, $\{2,6,8\}$, $\{3,5,7\}$, $\{3,5,8\}$, $\{4,5,6\}$, $\{4,6,8\}$
	s= 4	:	$\{1,2,8,9\}$, $\{1,3,5,9\}$, $\{1,3,6,9\}$, $\{1,3,7,9\}$, $\{1,4,6,9\}$, $\{1,4,7,9\}$, $\{1,5,7,9\}$, $\{2,3,4,8\}$, $\{2,3,7,8\}$, $\{2,4,6,8\}$, $\{2,6,7,8\}$, $\{3,4,6,7\}$
n= 10	**s= 1**	:	$\{3\}$, $\{4\}$, $\{5\}$, $\{6\}$, $\{7\}$, $\{8\}$
	s= 2	:	$\{1,9\}$, $\{1,10\}$, $\{2,9\}$, $\{2,10\}$, $\{3,7\}$, $\{3,8\}$, $\{4,7\}$, $\{4,8\}$, $\{5,6\}$
	s= 3	:	$\{1,5,9\}$, $\{2,5,9\}$, $\{2,6,9\}$, $\{2,6,10\}$, $\{3,5,7\}$, $\{4,5,7\}$, $\{4,6,7\}$, $\{4,6,8\}$
	s= 4	:	$\{1,2,9,10\}$, $\{1,3,5,9\}$, $\{1,3,6,9\}$, $\{1,3,6,10\}$, $\{1,3,7,9\}$, $\{1,3,8,10\}$, $\{1,4,6,9\}$, $\{1,4,6,10\}$, $\{1,4,7,10\}$, $\{1,5,6,10\}$, $\{1,5,7,9\}$, $\{1,5,7,10\}$, $\{1,5,8,10\}$, $\{2,3,5,9\}$, $\{2,3,7,9\}$, $\{2,3,8,9\}$, $\{2,4,5,9\}$, $\{2,4,6,9\}$, $\{2,4,6,10\}$, $\{2,4,7,9\}$, $\{2,4,8,9\}$, $\{2,4,8,10\}$, $\{2,5,6,9\}$, $\{2,5,7,9\}$, $\{2,5,7,10\}$, $\{2,5,8,10\}$, $\{2,6,7,9\}$, $\{2,6,8,9\}$, $\{2,6,8,10\}$, $\{3,4,7,8\}$, $\{3,5,6,8\}$, $\{4,5,6,7\}$
	s= 5	:	$\{1,3,4,5,9\}$, $\{1,3,4,6,10\}$, $\{1,3,5,7,9\}$, $\{1,3,5,7,10\}$, $\{1,3,5,8,10\}$, $\{1,3,6,8,10\}$, $\{1,4,6,8,10\}$, $\{1,5,7,8,10\}$, $\{2,3,4,6,9\}$, $\{2,3,5,7,9\}$, $\{2,4,5,7,9\}$, $\{2,4,6,7,9\}$, $\{2,4,6,8,9\}$, $\{2,4,6,8,10\}$, $\{2,5,7,8,9\}$, $\{2,6,7,8,10\}$