Graded alphabets, circular codes, free Lie algebras and comma-free codes

Dominique Perrin, Christophe Reutenauer

Graded alphabets, circular codes, free Lie algebras and comma-free codes

Dominique Perrin[1] and Christophe Reutenauer[2]
[1] Université Paris Est, LIGM, [2] Université du Québec à Montréal, LaCIM

August 24, 2020

Contents

Abstract

We show how the use of graded alphabets allows one to provide simpler proofs of some results on free monoids and free Lie algebras. We first generalize to graded alphabets the characterization of the length distributions of circular codes. We also show that the existence of a circular code with a given distribution of degrees is equivalent to the existence of an embedding of Lie algebras. We finally give a generalization to graded alphabets of the famous result of Eastman on comma free codes of odd degree.

1 Introduction

The notion of code with bounded synchronization delay was introduced by Golomb and Gordon [4]. For a finite code, the property of having finite synchronization delay is equivalent to the notion of circular code (see [2] Theorem 10.2.7) .

The characterization of the length distributions of circular codes was conjectured by Gilbert and Moore and proved by Schützenberger [10].

Graded alphabets are alphabets where to every letter is assigned a positive integer, its degree (also called a weight or a cost). This degree extends to words by additivity. These more general alphabets are used to take into account the possibility that letters have different properties, for example a length, a cost, or a duration (see [1] or [2, Section 3.9] for an exposition of algorithms on alphabets with costs).

In this note, we give a new presentation of the characterization of length distributions of circular codes, using graded alphabets (Theorem 4.1). This gives both a more general statement and a substantial simplification of the proof (although the construction remains essentially the same). Additionnally, we prove that the existence of a circular code on a graded alphabet A with degree distribution (u_n) is equivalent to the existence of a degree preserving embedding of the free Lie algebra L on an alphabet B with degree distribution (u_n) into the free Lie algebra $L(A)$ (Theorem 5.1).

We also extend to graded alphabets the result of Eastman proving the existence for every odd integer n of a comma-free code with the maximal possible number of elements, that is the number of conjugacy classes of primitive words of length n (Theorem 6.2).

Ackowledgements The authors are very grateful to the referees, who have carefully read the paper, and have provided substantial hints for an improvement of its readability.

2 Circular codes

A *code* is a set $X \subset A^*$ which is the basis of a free submonoid of A^*. In equivalent terms, X is a code if any equality

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m$$

for $n, m \geq 0$ and $x_i, y_j \in X$ implies $n = m$ and $x_i = y_i$ for $1 \leq i \leq n$.

As a stronger notion, a *circular code* X on an alphabet A is a set $X \subset A^+$ such that for all $n, m \geq 1$ and $x_1, x_2, \ldots, x_n \in X$, $y_1, y_2, \ldots, y_m \in X$ and $p \in A^*$, $s \in A^+$, the equalities

$$sx_2 \cdots x_n p = y_1 y_2 \cdots y_m, \tag{2.1}$$

$$x_1 = ps \tag{2.2}$$

imply $n = m$, $p = 1$ and $x_i = y_i$ for $1 \leq i \leq n$.

A submonoid M of A^* is generated by a circular code if and only if for every $u, v \in A^*$, one has

$$uv, vu \in M \Rightarrow u, v \in M \tag{2.3}$$

(see [2] Proposition 7.1.1) and in particular for $u \in A^*$ and $n \geq 1$,

$$u^n \in M \Rightarrow u \in M. \tag{2.4}$$

A *circular morphism* $\varphi : B^* \to A^*$ is a monoid morphism such that φ maps bijectively B onto a circular code $X \subset A^+$. Note that such a morphism is necessarily injective, since $\varphi(B)$ is a code.

The composition of two circular morphisms is circular [2, Proposition 7.1.11].

Two words x, y are *conjugate* if $x = uv$ and $y = vu$ for some words u, v. Conjugacy is an equivalence relation. A word w is called *primitive* if it is not a power of another one, that is, $w = x^n$ implies $n = 1$. A primitive word of length n has n distinct conjugates.

It follows from the definition of circular codes that a circular morphism φ sends primitive words to primitive words and that $\varphi(x), \varphi(y)$ are conjugate if and only if x, y are conjugate.

We begin with the following elementary and well-known result concerning generating series (see e.g. [2, Proposition 7.3.1]).

Proposition 2.1 *Let (u_n) be a sequence of integers and $u(z) = \sum_{n\geq 1} u_n z^n$. Define integers ℓ_n by*

$$1 - u(z) = \prod_{n\geq 1} (1 - z^n)^{\ell_n}. \tag{2.5}$$

Set

$$p_n = \sum_{d|n} d\ell_d \tag{2.6}$$

and let $p(z) = \sum_{n\geq 1} p_n z^n$. Then

$$p(z) = \frac{zu'(z)}{1 - u(z)} \tag{2.7}$$

$$\frac{1}{1 - u(z)} = \exp\Big(\sum_{n\geq 1} \frac{p_n}{n} z^n\Big). \tag{2.8}$$

$$p_n = nu_n + \sum_{i=1}^{n-1} p_i u_{n-i} \tag{2.9}$$

Proof. We have

$$\frac{1}{1 - u(z)} = \prod_{n\geq 1} \frac{1}{(1 - z^n)^{\ell_n}}.$$

Take the logarithmic derivative of each side, and multiply by z:

$$\begin{aligned} \frac{zu'(z)}{1 - u(z)} &= \sum_{n\geq 1} \frac{n\ell_n z^n}{1 - z^n} = \sum_{n\geq 1} n\ell_n \sum_{m\geq 1} z^{nm} \\ &= \sum_{N\geq 1} \sum_{N=nm} n\ell_n z^N = \sum_{N\geq 1} p_N z^N = p(z). \end{aligned}$$

This proves the first equality. The second one follows since both sides have the same constant term and the same logarithmic derivative. The first equality implies $zu'(z) = p(z) - u(z)p(z)$, whence the last equality. ∎

The following result is well known, although usually formulated for a finite alphabet.

Proposition 2.2 *Let $X \subset A^+$ be a code such that $u_n = \mathrm{Card}(X \cap A^n)$ is finite for every $n \geq 1$. Then $u_n^* = \mathrm{Card}(X^* \cap A^n)$ is finite for every $n \geq 0$ and*

$$\frac{1}{1 - u(z)} = \sum_{n \geq 0} u_n^* z^n. \tag{2.10}$$

Proof. For $1 \leq k \leq n$, let $u_n^{(k)}$ be defined by $u(z)^k = \sum_{n \geq 0} u_n^{(k)} z^n$. Since every word of length n has a unique decomposition in k words of X, $u_n^{(k)}$ is the number of words of length n in X^k. Since $u_n^{(k)} = 0$ if $k > n$, we obtain $u_n^* = \sum_{k \geq 0} u_n^{(k)}$, and therefore $\sum_{n \geq 0} u_n^* z^n = \sum_{n \geq 0} \sum_{k \geq 0} u_n^{(k)} z^n = \sum_{k \geq 0} u(z)^k = \frac{1}{1-u(z)}$. ∎

3 Graded alphabets

Let A be a *graded alphabet*, given by a map $d : A \to \mathbb{N} \setminus \{0\}$ assigning to every letter a nonzero integer called its *degree*. We assume that A is *locally finite*, that is, for each integer $n \geq 1$, there is only a finite number of letters of degree n. Set $u_n(A) = \mathrm{Card}(\{a \in A \mid d(a) = n\})$.

The *degree* of a word $w = a_1 a_2 \dots a_n$ on A ($n \geq 0, a_i \in A$) is then defined by $d(w) = d(a_1) + \dots + d(a_n)$. In this way the free monoid A^* on A becomes a *graded monoid*, that is a monoid such that $d(x) = 0$ if and only if $x = \varepsilon$ and such that $d(xy) = d(x) + d(y)$ for every $x, y \in A^*$.

Given graded alphabets A, B, a morphism $\varphi : A^* \to B^*$ is *degree preserving* if $d(\varphi(b)) = d(b)$ for every $b \in B$.

When A is a graded alphabet, we denote by $\ell_n(A)$ and $p_n(A)$ the integers associated with the numbers $u_n(A)$ as in Proposition 2.1.

Thus the integers $p_n(A)$ are defined by

$$p_n(A) = \sum_{d|n} d\ell_d(A) \tag{3.1}$$

and conversely, by Möbius inversion, the integers $\ell_n(A)$ are defined by

$$\ell_n(A) = \frac{1}{n} \sum_{d|n} \mu(n/d) p_d(A) \tag{3.2}$$

where μ is the Möbius function.

Let A be an ordinary alphabet with k letters. We can consider A as a graded alphabet where each letter has degree 1. We then denote $\ell_n(k)$ instead of $\ell_n(A)$ since it only depends on k.

On the other hand, for every sequence $u = (u_n)_{n \geq 1}$ of natural integers, we can consider a graded alphabet B such that $u_n(B) = u_n$. We denote $\ell_n(u)$ instead of $\ell_n(B)$.

The following result is well known (see [2, Exercise 7.3.3]). We shall give a direct simple proof below using an argument of [11, Proposition 4.7.13].

Proposition 3.1 *Let A be a graded alphabet. The number of conjugacy classes of primitive words of degree n is $\ell_n(A)$.*

Proof.

Let $A' = \{(i, a) \mid a \in A, 1 \leq i \leq d(a)\}$ and let $\varphi : A^* \to A'^*$ be the morphism defined by $\varphi(a) = (1, a)(2, a) \cdots (d(a), a)$. Set $X = \varphi(A)$. Clearly, φ is a circular morphism.

Set $u(z) = \sum_{n\geq 1} u_n(A)z^n$. Let $u_n^*(A)$ be defined by

$$\frac{1}{1 - u(z)} = \sum_{n\geq 0} u_n^*(A)z^n.$$

Then, by Proposition 2.2, $u_n^*(A)$ is the number of words of length n in X^*.

Let π_n be the number of words of length n in A'^* having a conjugate in X^*. For every $a \in A$, let $g_{n,a}$ be the number of words w of length n in A'^* of the form $w = syp$ with $y \in X^*$, $\varphi(a) = ps$ and p nonempty. The triple (s, y, p) is uniquely determined by w and thus

$$g_{n,a} = d(a)u_{n-d(a)}^*(A) \tag{3.3}$$

Conversely, every word of A'^* of length n having a conjugate in X^* is of this form for some $a \in A$ and thus $\pi_n = \sum_{a\in A} g_{n,a}$.

We obtain as consequence

$$\begin{aligned} \pi_n &= \sum_{a\in A} g_{n,a} = \sum_{a\in A, d(a)\leq n} d(a)u_{n-d(a)}^*(A) \\ &= \sum_{i=0}^{n} iu_i(A)u_{n-i}^*(A). \end{aligned}$$

By Formula (2.7), we have $p(z) = \frac{zu'(z)}{1-u(z)} = (\sum_{i\geq 0} iu_i(A)z^i)(\sum_{n\geq 0} u_n^*(A)z^n)$. Thus $p_n(A) = \pi_n$.

Let now λ_n be the number of conjugacy classes of primitive words of degree n in A^*. The morphism φ sends primitive words to primitive words and $\varphi(u), \varphi(v)$ are conjugate if and only if u, v are conjugate. Thus, λ_n is equal to the number of conjugacy classes of primitive words of length n in A'^* which meet X^*. Therefore $\pi_n = \sum_{d|n} d\lambda_d$. But we have by Equation (2.6), $p_n(A) = \sum_{d|n} d\ell_d(A)$. Since we have shown that $p_n(A) = \pi_n$, it follows by Möbius inversion that $\lambda_n = \ell_n(A)$. ∎

An alternative proof is as follows: it uses Lyndon words, which are by definition the primitive words minimal for the lexicographic oreder in their conjugacy

class (see [2]). As is well known, each word in A^* is uniquely a decreasing product of Lyndon words. It follows that in the algebra of formal power series on A over Z, one has

$$(1-A)^{-1} = A^* = \prod_w w^* = \prod_w (1-w)^{-1},$$

where the products are decreasing and over the set of Lyndon words w, and where subsets of A^* are indentified with their sum in the previous algebra. By sending each word u onto $z^{deg(u)}$ in $\mathbb{Z}[[z]]$, it follows that

$$(1-u(z))^{-1} = \prod_{n\geq 1} (1-z^n)^{-\lambda_n},$$

where λ_n is the number of primitive conjugacy classes in A^*. Comparing with Formula (2.5), we obtain that $\lambda_n = l_n(A)$, since the exponents are unique.

Example 3.2 Consider the graded alphabet $A = \{a, b\}$ with $d(a) = 1$ and $d(b) = 2$. The values of $p_n(A)$ and $\ell_n(A)$ for $1 \leq n \leq 11$ are given in Table 3.2. The sequence (p_n) is the *Lucas sequence*: it is defined by the same recursion

n	1	2	3	4	5	6	7	8	9	10	11
$p_n(A)$	1	3	4	7	11	18	29	47	76	123	199
$\ell_n(A)$	1	1	1	1	2	2	4	5	8	11	18

as the Fibonacci numbers, with initial values $1, 3$ for $n = 1, 2$; we leave this verification to the reader, using Equation (2.6).

4 Length distributions of circular codes

The following statement is closely related to the main result of [10] (see also [2, Theorem 7.3.7]). Indeed, the result of Schützenberger states that there exists a circular code on A with length distribution $u = (u_n)$ if and only if $\ell_n(u) \leq \ell_n(k)$. The statement on graded alphabets is, as we shall see, more general. Moreover, it allows us to give a substantially simpler proof, using induction by change of alphabets.

Theorem 4.1 *Let A, B be two graded alphabets. The following conditions are equivalent.*

1. *There exists a degree preserving circular morphism $\varphi : B^* \to A^*$.*
2. *$\ell_i(B) \leq \ell_i(A)$ for all $i \geq 1$.*

Let us show how this statement implies the result of Schützenberger. Let A be an ordinary alphabet with k letters and let $u = (u_n)$ be a sequence of integers such that $\ell_n(u) \leq \ell_n(k)$ for all $n \geq 1$. Consider a graded alphabet B such that

$u_n(B) = u_n$ for all $n \geq 1$. Then $\ell_n(u) = \ell_n(B)$ and thus Condition 2 above is satisfied. Hence, by Theorem 4.1, there exists a degree preserving circular morphism $\varphi : B^* \to A^*$. Set $X = \varphi(B)$. Since φ is circular, X is a circular code and since it is degree preserving, we have $\mathrm{Card}(X \cap A^n) = u_n(B) = u_n$ for all $n \geq 1$.

For the reverse implication, one notes that $l_n(k)$ is the number of conjugacy classes of primitive words A^*, $|A| = k$. A circular code on A cannot contain more than $l_n(k)$ words of length n, otherwise two of them are conjugate, a contradiction.

We first prove the following elementary lemmas.

Lemma 4.2 *Let A, B be graded alphabets and let $\alpha : B^* \to A^*$ be a degree preserving circular morphism. Then α induces for every $n \geq 1$ an injective map from the set of conjugacy classes of primitive words of degree n on B into the set of conjugacy classes of primitive words of degree n on A.*

Proof. Since α is circular, the image by α of a primitive word is primitive by (2.4), and $\alpha(u), \alpha(v)$ are conjugate if and only if u, v are conjugate by (2.3). ∎

Lemma 4.3 *Let A be a graded alphabet and let $a \in A$ be a letter of degree n. Let A' be a graded alphabet in bijection with $X = a^*(A \setminus \{a\})$ by some degree preserving map α. Then*

$$\ell_i(A') = \begin{cases} \ell_i(A) - 1 & \text{if } i = n \\ \ell_i(A) & \text{otherwise} \end{cases}$$

Proof. Since X is a circular code, the map α extends to a degree preserving circular morphism $\alpha : A'^* \to A^*$. Since α is circular, it induces by Lemma 4.2, an injective map from the set of conjugacy classes of primitive words of degree i on A' into the set of conjugacy classes of primitive words of degree i on A. For $i < n$, it is a bijection and thus $\ell_i(A') = \ell_i(A)$. If $x \in A^*$ contains a letter x distinct of a, it has a conjugate ending by x, which is therefore in $X^* = \alpha(A'^*)$. Thus, for $i = n$ there is one less conjugacy class of primitive words of degree i on A' than on A and for $i > n$ the same number. ∎

Note that Lemma 4.3 can also be proved using generating series. Denote in fact $u(z) = \sum_{n \geq 1} u_n(A) z^n$ and $v(z) = \sum_{n \geq 1} u_n(A') z^n$. Since $X = a^*(A \setminus \{a\})$, we have $v(z) = \frac{1}{1-z^n}(u(z) - z^n)$ and consequently $1 - u(z) = (1 - z^n)(1 - v(z))$. Thus Lemma 4.3 follows directly from Equation (2.5).

Lemma 4.4 *Let A, B be graded alphabets with B finite, such that $\ell_i(A) = \ell_i(B)$ for $1 \leq i < k$. Then $u_i(A) = u_i(B)$ for $1 \leq i < k$. If, additionnally, $\ell_k(A) > \ell_k(B)$, then $u_k(A) > u_k(B)$.*

Proof. Equation (2.5) taken modulo z^k shows that $u_1, \ldots, u_{k-1}$ depend only on $\ell_1, \ldots, \ell_{k-1}$. This implies the first assertion.

By Equation (2.9), $p_k(A) - p_k(B) = k(u_k(A) - u_k(B))$, and by Equation (2.6), $p_k(A) - p_k(B) = k(\ell_k(A) - \ell_k(B))$. Thus $u_k(A) - u_k(B) = \ell_k(A) - \ell_k(B)$, which implies the last assertion. ∎

We now establish, the following statement (which is Theorem 4.1 in the case of a finite alphabet B, with a weaker second condition).

Proposition 4.5 *Let A, B be graded alphabets with B finite. The following conditions are equivalent.*

1. *There exists a degree preserving circular morphism $\varphi : B^* \to A^*$.*
2. *$\ell_i(B) \leq \ell_i(A)$ for $1 \leq i \leq \max\{d(b) \mid b \in B\}$.*

Proof. 1 implies 2 is clear by Lemma 4.2.

2 implies 1. Set $N = \max\{d(b) \mid b \in B\}$. We use induction on $\delta(A, B)$ defined by

$$\delta(A, B) = \sum_{i=1}^{N} (\ell_i(A) - \ell_i(B)). \tag{4.1}$$

If $\delta(A, B) = 0$, then $u_i(A) = u_i(B)$ for $i = 1, \ldots, N$ by Lemma 4.4. Let $\varphi : B \to A$ be a degree preserving injection from B onto A. This bijection defines a degree preserving circular morphism from B^* into A^*.

If $\delta(A, B) > 0$, let $n \geq 1$ be the largest integer such that $\ell_i(A) = \ell_i(B)$ for $1 \leq i < n$. By Lemma 4.4 we have $u_n(A) > u_n(B)$. Thus there exists a letter $a \in A$ of degree n. Set $X = a^*(A \setminus a)$ and let α be a degree preserving bijection from a graded alphabet A' onto X. By Lemma 4.3, we have $\ell_i(A') = \ell_i(A)$ for $i \neq n$ and $\ell_n(A') = \ell_n(A) - 1$. Thus $\ell_i(B) \leq \ell_i(A')$ for $1 \leq i \leq N$ and, by Lemma 4.3,

$$\begin{aligned} \delta(A, B) - \delta(A', B) &= \sum_{i=1}^{N} (\ell_i(A) - \ell_i(B)) - \sum_{i=1}^{N} (\ell_i(A') - \ell_i(B)) \\ &= \sum_{i=1}^{N} (\ell_i(A) - \ell_i(A')) = \ell_n(A) - \ell_n(A') = 1 \end{aligned}$$

The induction hypothesis applied to the pair A', B gives a degree preserving circular morphism φ' from B^* into A'^*. Now since the code X is circular, the morphism α is circular. Therefore $\varphi = \alpha \circ \varphi'$ is a degree preserving circular morphism from B^* into A^*. ∎

We will additionally use the following compacity lemma.

Lemma 4.6 *Let A, B be graded alphabets. For $n \geq 1$, set $B_n = \{b \in B \mid d(b) \leq n\}$. Suppose that for each n there exists a degree preserving circular morphism $B_n^* \to A^*$. Then there exists a degree preserving circular morphism $B^* \to A^*$.*

The proof is left to the reader.

Proof of Theorem 4.1.

1 implies 2 is clear by Lemma 4.2.

2 implies 1. If B is finite, the statement results from Proposition 4.5. If B is infinite, the result follows from Lemma 4.6. ∎

Example 4.7 As an example, consider $B = \{u, v, w\}$ with $d(u) = 1$ and $d(v) = d(w) = 3$ and $A = \{a, b\}$ with $d(a) = d(b) = 1$. Since $1 = \ell_1(B) < \ell_1(A) = 2$, we change A to A' in bijection with $X = a^*b = \{b, ab, aab, aaab, \ldots\}$. Again, since $0 = \ell_2(B) < \ell_2(A') = 1$, we change A' to A'' in bijection with $Y = (ab)^*(X \setminus \{ab\}) = \{b, aab, abb, aaab, \ldots\}$. The required circular morphism is $\varphi : u \mapsto b, v \mapsto aab, w \mapsto abb$.

Note an interesting consequence of the proof of Theorem 4.1 using Proposition 4.5. It shows that condition 2 in Theorem 4.1 is decidable for a finite alphabet B.

Proposition 4.8 *Let A, B be graded alphabets with B finite and $\ell_i(B) \leq \ell_i(A)$ for $i = 1, \ldots, max\{d(b) \mid b \in B\}$. Then this inequlity holds for any $i \geq 1$.*

Proof. Proposition 4.5 shows that there exists a degree preserving circular morphism from B^* into A^*. Thus one concludes with Theorem 4.1. ∎

5 Free Lie algebras

A *Lie algebra* L over $\mathbb{Z}$ is an algebra over $\mathbb{Z}$ whose product $(x, y) \mapsto [x, y]$ satisfies $[x, x] = 0$ for all $x \in L$ and the *Jacobi identity*

$$[[x, y]z] + [[y, z]x] + [[z, x]y] = 0 \tag{5.1}$$

for all $x, y, z \in L$.

We consider the free Lie algebra $L(A)$ on A with coefficients in $\mathbb{Z}$ as embedded in the free associative algebra $\mathbb{Z}\langle A\rangle$ (see [7]). It is formed of the $\mathbb{Z}$-linear combinations of *Lie monomials*, which are recursively defined as follows: a Lie monomial is either a letter, or a Lie product $[x, y]$ of two Lie monomials x, y.

The degree $d(x)$ of a noncommutative polynomial $x \in \mathbb{Z}\langle A\rangle$ is the maximum of the degrees of the words w such that the coefficient of w in x is nonzero. This defines in particular the degree of a Lie element $x \in L(A)$.

Given two graded alphabets A, B, a Lie algebra morphism $\varphi : L(B) \to L(A)$ is *monomial* if the image of a Lie monomial in $L(B)$ is a Lie monomial in $L(A)$. It is *degree preserving* if $d(\varphi(b)) = d(b)$ for every $b \in B$. An *embedding* of $L(B)$ into $L(A)$ is an injective Lie morphism from $L(B)$ into $L(A)$.

It is well known that, if A is finite, then $\ell_n(A)$ is the dimension of the homogeneous component of degree n of the free Lie algebra $L(A)$.

We prove the following result which gives a natural complement to Theorem 4.1. We state it for a finite alphabet B although it can extend to the case where B is infinite as we shall see below (Corollary 5.4).

Theorem 5.1 *Let A, B be two graded alphabets with B finite. The following conditions are equivalent.*

1. *There is a degree preserving monomial embedding of $L(B)$ into $L(A)$.*
2. *$\ell_i(B) \leq \ell_i(A)$ for all $1 \leq i \leq \max\{d(B) \mid b \in B\}$.*

A *derivation* of a Lie algebra L over $\mathbb{Z}$ is a $\mathbb{Z}$-linear map $D : L \to L$ satisfying the Leibniz rule

$$D([x, y]) = [D(x), y] + [x, D(y)].$$

It follows from the Jacobi identity that for any Lie algebra L, the map $\operatorname{Ad} x : y \mapsto [x, y]$ is a derivation for every $x \in L$.

The set of derivations of L forms a Lie algebra with respect to the usual commutator; indeed, a linear combination of derivations is a derivation, and the commutator $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$ is a derivation, as is easily verified. Let L_1, L_2 be two Lie algebras. Given a Lie algebra morphism π from L_1 to the Lie algebra of derivations of L_2, the *semidirect product* of L_1 and L_2 is the unique Lie algebra denoted $L_1 \times_\pi L_2$ which is, as $\mathbb{Z}$-module, the direct sum $L_1 \oplus L_2$ with the product extending those of L_1, L_2 and such that, for $x \in L_1$ and $y \in L_2$, one has $[x, y] = \pi(x)(y)$.

It is known by a theorem of Sirshov (see [7], Theorem 2.5) that any Lie subalgebra of a free Lie algebra is free. Let X be a subset of $L(A)$ and let J be the subalgebra of $L(A)$ generated by X. Let $\varphi : B \to X$ be a bijection from a set B onto X. There is a unique extension of φ to a Lie algebra morphism from $L(B)$ into $L(A)$. If this extension is an isomorphism, the set X is called a *Lie algebra basis* of the subalgebra J.

The next lemma is [12, Proposition 1.1]. We reproduce the proof for convenience.

Lemma 5.2 *Let A be a nonempty alphabet, let $a_1 \in A$ and let $A_2 = A \setminus \{a_1\}$. The $\mathbb{Z}$-module $L(A)$ is a direct sum of the module $\mathbb{Z}a_1$ and the Lie ideal J of $L(A)$ generated by A_2. Moreover, the set of elements $(\operatorname{Ad} a_1)^n(a)$ for $a \in A_2$ is a Lie algebra basis of the Lie subalgebra J.*

Proof. Let $A' = \{(n, a) \mid n \in \mathbb{N}, a \in A_2\}$. Let $L_1 = L(a_1)$ and $L_2 = L(A')$. There is a unique derivation D on L_2 defined by $D(n, a) = (n + 1, a)$ for every $a \in A_2$. We consider the semidirect product L of L_1 and L_2 relative to the map π defined by $\pi(a_1) = D$. Thus in L (which contains naturally L_1 and L_2), one has $[a_1, (n, a)] = D(n, a) = (n + 1, a)$ for every $a \in A_2$.

The map $\psi : A \to L$ defined by $\psi(a_1) = a_1$ and $\psi(a) = (0, a)$ for $a \in A_2$ extends in a unique way to a Lie algebra morphism form $L(A)$ into L.

We also have Lie morphisms $\varphi_1 : L_1 \to L(A)$ and $\varphi_2 : L_2 \to L(A)$ defined by $\varphi_1(a_1) = a_1$ and $\varphi_2(n, a) = (\operatorname{Ad} a_1)^n(a)$. They extend in a unique way to a morphism $\varphi : L \to L(A)$: indeed, this follows from the fact that in L one has $[a_1, (n, a)] = (n + 1, a)$, and in $L(A)$, one has $[a_1, \operatorname{Ad}(a_1)^n(a)] = \operatorname{Ad}(a_1)^{n+1}(a)$.

We have $\psi \circ \varphi(a) = a$ for every $a \in A$. Next $\varphi \circ \psi(a_1) = a_1$ and an easy induction on n shows that $\varphi \circ \psi(n, a) = (n, a)$. Thus, φ, ψ are mutually inverse isomorphisms between $L(A)$ and L, exchanging J and L_2. ∎

Proof of Theorem 5.1.

1 implies 2. Indeed, if there is a degree preserving monomial embedding of $L(B)$ into $L(A)$, it maps the homogeneous component of degree n of $L(B)$ into the homogeneous component of degree n of $L(A)$ and thus $\ell_n(B) \leq \ell_n(A)$.

2 implies 1. We use an induction on the integer $\delta(A, B)$ defined by Equation (4.1). If $\delta(A, B) = 0$, then $u_n(A) = u_n(B)$ for all $n = 1, \ldots, max(d(B))$, by Lemma 4.4 (with k replaced by $n + 1$). Let $\varphi : B \to A$ be a degree preserving injection from B onto A. This injection extends to a monomial degree preserving injection from $L(B)$ onto $L(A)$.

If $\delta(A, B) > 0$, let $n \geq 1$ be the largest integer such that $\ell_i(A) = \ell_i(B)$ for $1 \leq i < n$. By Lemma 4.4 we have $u_n(A) > u_n(B)$. Thus there exists a letter $a_1 \in A$ of degree n. Let α be a degree preserving bijection from an alphabet A' onto $X = a_1^*(A \setminus a_1)$. By Lemma 4.3, we have $\ell_i(A') = \ell_i(A)$ for $i \neq n$ and $\ell_n(A') = \ell_n(A) - 1$. Thus $\ell_i(B) \leq \ell_i(A')$ for all $i \geq 1$ and moreover,

$$\delta(A, B) - \delta(A', B) = \ell_n(A) - \ell_n(A') = 1$$

The induction hypothesis applied to the pair A', B gives a monomial degree preserving embedding φ' of $L(B)$ into $L(A')$. Consider the map $\beta : X \to L(A), a_1^i a \mapsto (\mathrm{Ad}\, a_1)^i(a)$ for $a \in A \setminus \{a_1\}$. By Lemma 5.2, the map $\beta \circ \alpha : A' \to L(A)$ extends to a monomial degree preserving embedding of $L(A')$ into $L(A)$. Therefore $\varphi = \beta \circ \alpha \circ \varphi'$ is a monomial degree preserving embedding of $L(B)$ into $L(A)$. ∎

Example 5.3 As an example, consider again $B = \{u, v, w\}$ with $d(u) = 1$ and $d(v) = d(w) = 3$ and $A = \{a, b\}$ with $d(a) = d(b) = 1$. The result is the monomial degree preserving morphism $\varphi : u \mapsto b, v \mapsto [a[a, b]], w \mapsto [[a, b]b]$.

Corollary 5.4 *Let A, B be two graded alphabets. The following conditions are equivalent.*

1. *There is a degree preserving monomial embedding of $L(B)$ into $L(A)$.*
2. *$\ell_i(B) \leq \ell_i(A)$ for all i.*

This follows from the theorem by considering the finite subalphabets of B: the sequence of embeddings constructed in such a way allows to construct an embedding of $L(B)$ into $L(A)$, since Lie monomials of degree $\leq m$ are finitely many.

6 Comma-free codes

A code $X \subset A^+$ is called *comma-free* if no word of X can overlap nontrivially a product of two words of X. Formally, a code X is comma-free if for every $x \in X$ and $u, v \in A^*$, one has

$$uxv \in X^* \Rightarrow u, v \in X^*. \tag{6.1}$$

The following is [2, Proposition 7.2.14]. We give a proof for the convenience of the reader.

Proposition 6.1 *Comma free codes are circular.*

Proof. Let $X \subset A^+$ be a comma-free code. Assume that for $n \geq 1$, $m \geq 1$, $x_i, y_j \in X$ and $p \in A^*$, $s \in A^+$, we have

$$sx_2 \cdots x_n p = y_1 y_2 \cdots y_m, \tag{6.2}$$

$$x_1 = ps. \tag{6.3}$$

Since X is a code, it is enough to prove that $p = 1$.

If $n \geq 2$, then an iterated use of (6.1) implies $p, s \in X^*$ which in turn implies $p = 1$ since X is a code.

If $n = 1$, we replace (6.2) by $sx_1p = (y_1 \cdots y_m)^2$. The conclusion follows by the previous case. ∎

The converse is not true. For example, $\{aab, abb, bbc\}$ is circular but not comma-free because $(aab)(bbc) = a(abb)bc$.

A morphism $\varphi : B^* \to A^*$ is comma-free if it maps bijectively B to a comma-free code. The composition of two comma-free morphisms is comma-free [2, Proposition 7.2.15].

A set $X \subset A^+$ formed of words all of the same degree $n \geq 1$ is a comma-free code if and only if for every $x, y, z \in X$, the word z cannot be a factor of xy unless $x = z$ or $y = z$.

The following result is the generalization to graded alphabets of a result due to Eastman [3]. Another proof was given by Scholtz [8] and is reproduced as [2, Theorem 7.3.11]. As for Theorem 4.1, the statement for graded alphabets is more general, but this time the proof will be very similar to the proof in [2].

Theorem 6.2 *Let A be a graded alphabet. For every odd integer n, there exists a comma-free code formed of $\ell_n(A)$ words of degree n.*

We will follow the proof of Scholtz, who constructs, by iterated bisections, a subset of what is called a Lazard set. Another proof, following [9] and given in [7] (Theorem 5.17), is based on the construction of what is called a Hall set, where each word of even length is smaller than each word of odd length. Note that Hall sets and Lazard sets coincide, as shown by Viennot (see [12] or [7, Theorem 4.18]).

We may assume that A contains letters of odd degree, since otherwise there are no words of odd degree and, by Proposition 3.1, $\ell_n(A) = 0$ for n odd. Thus there is nothing to prove in this case. We may also assume that $\mathrm{Card}(A) \geq 2$.

To prove Theorem 6.2, we build a sequence $(x_k)_{k\geq 0}$ of words of odd degree and a sequence $(X_k)_{k\geq 0}$ of maximal prefix codes such that

$$X_0^* \supset X_1^* \supset X_2^* \supset \cdots \tag{6.4}$$

and that, for $k \geq 1$, X_k contains an infinity of words of odd degree.

We start with $X_0 = A$, which contains by hypothesis a letter x_0 of odd degree and is, by hypothesis, not reduced to x_0; we choose x_0 of minimum degree. Thus $X_1 = x_0^*(X_0 \setminus x_0)$ is a maximal prefix code. It contains an infinity of words of odd degree because, for $x \in X_0 \setminus x_0$ and $i \geq 0$, $d(x_0^i x) = i\ d(x_0) + d(x) \equiv i + d(x) \bmod 2$.

In general, for each $k \geq 1$, let x_k be a word of minimal odd degree in X_k (such a word exists since X_k contains words of odd degree). The set

$$X_{k+1} = x_k^*(X_k \setminus x_k)$$

is clearly a maximal prefix code such that $X_{k+1} \subset X_k^*$ (and thus $X_{k+1}^* \subset X_k^*$). It contains again an infinity of words of odd degree because $X_k \setminus x_k$ has this property. Such a sequence $(x_k, X_k)_{k\geq 0}$ is called a *Scholtz sequence* on A.

Note that the x_k are all distinct. Indeed, if $k < l$, then $x_k \in X_k$, $x_l \in X_l$, $x_k \notin X_{k+1}^*$, hence $x_k \notin X_l$ by (6.4).

Note also that $X_k \setminus X_{k+1} = \{x_k\}$.

Set $U = \bigcup X_k$. Let U_0 (resp. U_1) be the set of elements of even (resp. odd) degree in U.

Lemma 6.3 *We have*

$$U_1 = \{x_\ell \mid \ell \geq 0\}. \tag{6.5}$$

Proof. Indeed, every x_ℓ is of odd degree and in U, and thus in U_1. Conversely, consider $z \in U_1$ and set $d = d(z)$. Let k be such that $z \in X_k$. For $\ell > k$ such that $z \in X_\ell$, we have $d(x_k), \ldots, d(x_\ell) \leq d$. But the set S_d of words of odd degree $\leq d$ is finite since A is locally finite. Thus $\ell - k \leq \mathrm{Card}(S_d)$. This implies that there is an $\ell > k$ such that $z \notin X_\ell$. We conclude that $z = x_\ell$ where ℓ is the largest integer $\geq k$ such that $z \in X_\ell$. This proves Equation (6.5). ∎

We now make a series of remarks which will be used in the sequel.

For $u \in U$, set

$$\nu(u) = \min\{i \geq 0 \mid u \in X_i\} - 1.$$

Note first that for $u \in U_0$ and $h \geq 0$,

$$u \in X_h \Leftrightarrow \nu(u) < h. \tag{6.6}$$

Indeed, if $u \in X_h$, then $\nu(u) < h$ by definition of ν. The converse follows from the fact that $u \in X_h$ for $h = \nu(u) + 1$ by definition of ν and that a word of even length which is in X_h is also in X_{h+1}.

Next, consider $u \in U_1$. Then $u = x_\ell$ for some $\ell \geq 0$ by (6.5). We have for every $h \geq 0$,

$$u \in X_h \Leftrightarrow \nu(u) < h \leq \ell. \tag{6.7}$$

Indeed, if $u \in X_h$ then $\nu(u) < h$ by definition of ν. Next, because $x_\ell \notin X^*_{\ell+1}$ and $X_h \subset X^*_{\ell+1}$ for $\ell < h$ by (6.4), we have $x_\ell \notin X_h$ for $\ell < h$. This proves the left to right implication. Conversely, we use induction on h. The implication is true for $h = \nu(u) + 1$. Assuming that the implication is true for $h < \ell$, we have $u \neq x_h$ (since $u = x_l$) and thus, since $u \in X_h$, we have $u \in X_{h+1}$. This proves (6.7).

Combining (6.6) and (6.7), we note that for every $u \in X_k$,

$$\nu(u) < h \leq k \Rightarrow u \in X_h. \tag{6.8}$$

Indeed, if $u \in U_0$, this results from (6.6). Otherwise, set $u = x_\ell$. By (6.7), since $u \in X_k$, we have $\nu(u) < k \leq \ell$. Now $\nu(u) < h \leq k \leq \ell$ implies $u \in X_h$ by (6.7) again.

Furthermore, for every $u \in X_\ell$,

$$\nu(u) \leq k < \ell \Rightarrow x_k u \in U. \tag{6.9}$$

Indeed, if $k = \nu(u)$, we have $u \in X_{k+1}$ and $x_k u \in x_k X_{k+1} \subset X_{k+1}$. Otherwise, u is in all X_h for $\nu(u) + 1 \leq h \leq \ell$ by (6.8) and thus u is in X_k. But $u \neq x_k$. Indeed, if $u = x_k$ then, since $u \in X_\ell$, we have, by (6.7), $\nu(u) < \ell \leq k$ in contradiction with the hypothesis $k < \ell$. Therefore $x_k u \in x_k(X_k \setminus x_k) \subset X_{k+1}$.

The two next remarks are stated as the following lemmas.

Lemma 6.4 *For every element u of U which is not a letter, we have $u = x_k v$ with $k = \nu(u)$ and $v \in X_{k+1}$. If $u \in U_0$ (or equivalently $v \in U_1$) then $v = x_\ell$ with $k < \ell$.*

Proof. Since u is not a letter, it is not in X_0. Then, u is in X_{k+1} but not in X_k. Then, by definition of X_{k+1}, we have $u = x_k v$ for some $v \in X_{k+1}$. If moreover $v \in U_1$, then $v = x_\ell$ for some $\ell \geq 0$ by Equation (6.5). We have $k < \ell$ since $x_\ell \in X_{k+1}$ implies $k + 1 \leq \ell$ by Equation (6.7). ∎

Lemma 6.5 *For every odd integer n and every Scholtz sequence $(x_k, X_k)_{k\geq 0}$, the number of words of $U = \cup X_k$ of degree n is $\ell_n(A)$.*

Proof. Let (x_k, X_k) be a Scholtz sequence on A. We use an induction on the integer $\beta_n(A) = \sum_{k \text{ odd}, k<n} \ell_k(A)$.

If $\beta_n(A) = 0$, then, by Proposition 3.1, there are no letters of odd degree $< n$, hence the words of degree n are all letters, which are all primitive words. Thus the set of words in U of degree n is the set of letters of degree n. Thus the property holds trivially.

Next, if $\beta_n(A) > 0$, there is a letter of odd degree $< n$. Thus we have $d(x_0) < n$. Let $\alpha : A' \to X_1$ be a degree preserving bijection from a graded

alphabet A' onto X_1 and extend it to a monoid morphism $\alpha : A'^* \to A^*$. Then $X_k \subset X_1^*$ for all $k \geq 1$ by (6.4). We can thus define a sequence $(x'_k)_{k\geq 0}$ of words in A'^* by $x'_k = \alpha^{-1}(x_{k+1})$ and a sequence $(X'_k)_{k\geq 0}$ of prefix codes by $X'_k = \alpha^{-1}(X_{k+1})$. Then $X'_0 = A'$ and for each $k \geq 0$, x'_k is of minimal odd degree in X'_k. Moreover $X'_{k+1} = {x'_k}^*(X'_k \setminus x'_k)$. Thus $(x'_k, X'_k)_{k\geq 0}$ is a Scholtz sequence on A'. Set $U' = \cup X'_k$. Then $U' = \alpha^{-1}(U \setminus x_0)$. Since $d(x_0) < n$, the number of words of degree n in U and U' is the same.

By Lemma 4.3, we have $\beta_n(A') = \beta_n(A) - 1$. Thus by induction hypothesis, the number of words in U' of degree n is $\ell_n(A')$. Since $\ell_n(A) = \ell_n(A')$ by Lemma 4.3 again, we obtain the conclusion. ∎

We define a total order on U_1 by $u < v$ if $u = x_k$ and $v = x_\ell$ with $k < \ell$.

Lemma 6.6 *Every word $w \in A^*$ admits a unique factorization*

$$w = yz_{\ell-1} \cdots z_1 z_0 \tag{6.10}$$

with $y \in U_0^*$, $z_i \in U_1$, $\ell \geq 0$ and $z_{\ell-1} \geq \ldots \geq z_1 \geq z_0$.

Proof. We have for every $k \geq 1$ an unambiguous factorization

$$A^* = X_k^* x_{k-1}^* \cdots x_0^*. \tag{6.11}$$

The word unambiguous factorization used here means that for every word w in A^*, there is a unique decomposition $w = x x_{k-1}^{n_{k-1}} \cdots x_0^{n_0}$ with $x \in X_k^*$ and $n_i \geq 0$.

Choosing k large enough so that X_k does not contain words of odd degree $\leq d(w)$, we obtain a factorization (6.10). This proves the existence. To prove the uniqueness, observe that given a factorization (6.10), we have $y \in X_k^*$ for all large enough k. If w has two distinct factorizations (6.10), then it has multiplicity more than one in the factorization (6.11), a contradiction. Thus the factorization is unique. ∎

Lemma 6.7 *Every proper prefix of a word of U has a factorization (6.10) with $y = \varepsilon$.*

Proof. Let P_k be the set of proper prefixes of X_k. Since X_k is a maximal prefix code, we have an unambiguous factorization

$$A^* = X_k^* P_k.$$

Comparing with the unambiguous factorization given by Equation (6.11), we obtain $P_k = x_{k-1}^* \cdots x_0^*$. This proves the statement. ∎

Lemma 6.8 *For $0 \leq k < \ell$, we have $x_k x_\ell \in U_0^*$. Further $U_1 U_0 \subset U_0^* U_1$.*

Proof. We prove the first statement by induction on $\ell - k$. Set $p = \nu(x_\ell)$. Observe that $\ell = k+1$ implies $p \leq k$. Indeed, $x_\ell \in X_{p+1}$ implies $p+1 \leq \ell$ by (6.7) so that $\ell = k+1 \Rightarrow p+1 \leq k+1$.

If $\ell - k = 1$ or, more generally, if $p \leq k$, then $x_k x_\ell \in U_0$ by (6.9).

Assume now $k < p$ (and thus $\ell - k \geq 2$). Note that since $x_\ell \in X_{p+1}$, we have $p < \ell$ by (6.7). Since $p > 0$, we have $x_\ell \in U \setminus A$ and $x_\ell = x_p v$ with $v \in X_{p+1}$ by Lemma 6.4. Since x_ℓ, x_p have odd degree, v has even degree, and thus it it is in U_0. Since $p < \ell$, we have by induction hypothesis, $x_k x_p \in U_0^*$ and thus $x_k x_\ell = (x_k x_p)v \in U_0^*$.

We now prove the second statement. Let us consider $z \in U_1$ and $y \in U_0$. Set $z = x_k$ for some $k \geq 0$. If $y \in A$, then y is in all X_i and in particular in X_k. Thus zy is in X_{k+1} (since $y \in X_k \setminus x_k$) and actually $zy \in U_1$ because it has odd degree. If $y \notin A$, then $y = x_q x_t$ with $q = \nu(y)$ and $q < t$ by Lemma 6.4.

If $k < q$, then $x_k x_q$ is in U_0^* by what we have just seen before and thus $(x_k x_q)x_t \in U_0^* U_1$ since $x_t \in U_1$.

Otherwise $q \leq k$. Since $q = \nu(y)$, we have $y \in X_\ell$ for all $\ell \geq k+1 \geq q+1$ by (6.6). By (6.9), we have $zy \in U$ and thus $zy \in U_1$ since zy has odd degree. ∎

Lemma 6.9 *Any suffix of a word u in U admits a factorization (6.10) with $\ell = 0$ or $\ell = 1$.*

Proof.

We use an induction on the degree of u. We have to prove that each suffix w of u is in $U_0^* \cup U_0^* U_1$. Note that $U = U_0 \cup U_1 \subset U_0^* \cup U_0^* U_1$, so that the conclusion is clear if $w = u$ or $w = 1$. In particular, we may conclude if u is a letter. If u is not a letter, then by Lemma 6.4, we have $u = x_p v$ with $p \geq 0$ and $v \in X_{p+1}$. Moreover, if $v \in U_1$, then $v = x_q$ with $p < q$. If w is a suffix of v, the conclusion holds by induction hypothesis since $v \in U$ and $d(v) < d(u)$.

Assume now that $w = w'v$ with w' a proper suffix of x_p. By induction hypothesis, we have $w' \in U_0^* \cup U_0^* U_1$. If $w' \in U_0^*$, then $w = w'v$ is in $U_0^* \cup U_0^* U_1$ since $v \in U = U_0 \cup U_1$, and the property is satisfied. Assume next that $w' \in U_0^* U_1$. Set $w' = y x_k$ with $y \in U_0^*$ and $k \geq 0$. Since $d(x_k) \leq d(w') < d(x_p)$ (because w' is a proper suffix of x_p), we have $k < p$. We distinguish two cases.

First, suppose that $v \in U_0$. Then $x_k v$ is in $U_1 U_0$ and thus in $U_0^* U_1$ by Lemma 6.8. We conclude in this case that $w = y x_k v$ is in $U_0^* U_1$ as required.

In the second case, we suppose that $v \in U_1$. Then $v = x_q$ with $p < q$ as noted previously. Then $k < p < q$ implies that $x_k x_q \in U_0^*$ by Lemma 6.8 again. We obtain $w = w'v = y(x_k x_q) \in U_0^*$ concluding the proof. ∎

Proof of Theorem 6.2. By Lemma 6.5, it is enough to prove that the set X of words of degree n of U is comma-free. Assume that X is not comma-free. Then there are $x, y, z \in X$ such that $xy = pzs$ with p, s nonempty. Set $x = pu$, $y = vs$ and $z = uv$. Since z has odd degree, either u or v has even degree. Assume that u has even degree. Note that u is a suffix of x and a prefix of z. By Lemmas 6.7 and 6.9, it is empty or in U_1. Since it is of even degree, it is

empty. This implies $y = zs$ and thus, since y and z have the same degree, that s is empty, a contradiction. ∎

For example, let $A = \{a, b\}$ with $d(a) = 1$ and $d(b) = 2$. Then $X = \{a^3b, ab^2\}$ is a comma-free code formed of words of degree 5 with $\ell_5(A) = 2$ elements. It is obtained by the algorithm underlying the proof above by successively considering

$$\begin{aligned} X_0 &= \{a, b\},\ x_0 = a \\ X_1 &= \{b, ab, aab, aaab, \ldots\},\ x_1 = ab \\ X_2 &= \{b, aab, aaab, abb, \ldots\} \end{aligned}$$

7 Eastman algorithm

We have presented in [6] an analysis of Eastman original proof, following the recent exposition in [5]. It seems that it cannot be adapted to graded alphabets, as we will see now.

Let A be a graded ordered alphabet with at least two elements. Consider the set

$$D(A) = \{a_1a_2 \cdots a_n \mid a_i \in A, n \geq 2, a_1 \geq a_2 \geq \ldots \geq a_{n-1} < a_n\}.$$

The elements of $D(A)$ are called *dips*.

In the case of ordinary alphabets, the set of dips of odd length $m \geq 3$ is a comma-free code [6, Proposition 17]. It is part of a comma-free code formed for every odd integer m of $\ell_m(A)$ words of length m.

This property does not hold for the set of dips of odd degree $m = 7$, as shown by the following example.

Example 7.1 Let $A = \{a_1, a_2, a_3, a_4\}$ with $a_1 < a_2 < a_3 < a_4$ and $d(a_i) = i$ for $1 \leq i \leq 4$. Then $a_3a_1a_3, a_3a_4, a_4a_1a_2 \in D(A)$ are dips of degree 7. They do not form a comma-free code since $(a_3a_1a_3)(a_4a_1a_2) = a_3a_1(a_3a_4)a_1a_2$.

References

[1] Marie-Pierre Béal, Jean Berstel, Brian H. Marcus, Dominique Perrin, Christophe Reutenauer, and Paul H. Siegel. Variable length-codes and finite automata. In Isaac Woungang, editor, *Selected Topics in Information and Coding Theory*. World Scientific, 2009. 2

[2] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. *Codes and automata*, volume 129 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2010. 1, 2, 3, 5, 6, 12

[3] Williard L. Eastman. On the construction of comma-free codes. *IEEE Trans. Inform. Theory*, IT-11:263–267, 1965. 12

[4] Solomon W. Golomb and Basil Gordon. Codes with bounded synchronization delay. *Inform. and Control*, 8:355–372, 1965. 1

[5] Donald E. Knuth. *The Art of Computer Programming*, volume 4. Addison-Wesley, 2015. pre-fascicule 5B, Introduction to backtracking. 17

[6] Dominique Perrin and Christophe Reutenauer. Hall sets, Lazard sets and comma-free codes. *Discrete Mathematics*, 341(1):232–243, 2018. 17

[7] Christophe Reutenauer. *Free Lie Algebras*. Oxford University Press, 1993. 9, 10, 12

[8] Robert A. Scholtz. Maximal and variable length comma-free codes. *IEEE Trans. Inform. Theory*, IT-15:300–306, 1969. 12

[9] Marcel-Paul Schützenberger. Sur une propriété combinatoire des monoïdes libres pouvant être utilisée dans un problème de mathématiques appliquées. *Séminaire Dubreil. Algèbre et théorie des nombres*, pages 1–23, 1958. 12

[10] Marcel-Paul Schützenberger. Sur une question concernant certains sous-monoïdes libres. *C. R. Acad. Sci. Paris*, 261:2419–2420, 1965. 2, 6

[11] Richard P. Stanley. *Enumerative combinatorics. Vol. 1.* Cambridge University Press, Cambridge, 1997. 5

[12] Gérard Viennot. *Algèbres de Lie libres et monoïdes libres*, volume 691 of *Lecture Notes in Mathematics*. Springer, Berlin, 1978. Bases des algèbres de Lie libres et factorisations des monoïdes libres. 10, 12