Discrete Mathematics and Theoretical Computer Science **3**, 1999, 33–42

The Number of Sides of a Parallelogram

Elisha Falbel and Pierre-Vincent Koseleff

Institut de Mathématiques, Université Paris 6, Case 82
4 place Jussieu, F-75252 Paris Cedex 05.
email: {falbel,koseleff}@math.jussieu.fr

received 13 Oct 97, *revised 3 Nov 1998*, *accepted 10 Jan 1999*.

We define parallelograms of base a and b in a group. They appear as minimal relators in a presentation of a subgroup with generators a and b. In a Lie group they are realized as closed polygonal lines, with sides being orbits of left-invariant vector fields. We estimate the number of sides of parallelograms in a free nilpotent group and point out a relation to the rank of rational series.

Keywords: Lie algebras, free group, Magnus group, lower central series, Lyndon basis

1 Introduction

In $\mathbb{R}^2$ a parallelogram of base a and b can be defined as a closed polygon with the minimum number of sides parallel to a and b. In that paper we also consider parallelograms defined in more general groups.

In section **1.** we first give some definitions and examples of parallelograms in Lie groups. These examples show the various complex situations occurring in the general case. In this paper we concentrate our attention on free nilpotent groups. This analysis will give universal properties for parallelograms. We obtain

Theorem. The number of sides of a parallelogram on a free nilpotent group on two generators of order n is between n and n^2.

We do not know what is the exact number of sides of parallelograms in a free nilpotent group neither how many *non-equivalent* parallelograms exist. We hope that an investigation of parallelograms might help understand general nilpotent groups. In particular it will be interesting to find presentations with relators of minimal size.

We have chosen in this paper to recall the basic properties and constructions of free Lie algebras in order to make it self-contained. That is done in section **2.** In the last section we then introduce mth-order parallelograms and prove our result. A connection with rational series is pointed out at the end of the paper.

Our initial motivation to study parallelograms was the notion of curvature and holonomy of a connection for Riemannian manifolds and the generalization of those notions to sub-Riemannian geometry (see [FGR] and [BeR]). In classical differential geometry, curvature appears as the quadratic term in the asymptotic expansion of holonomy around short (four-sided) parallelograms, holonomy being the measure of the difference of the vector field by parallel translation around a closed loop. In the case of sub-Riemannian manifolds, the tangent space is naturally a nilpotent group ([BeR]) and the holonomy associated to it will be calculated using *parallelograms* with many sides. The analog of sectional curvatures should be the holonomy associated to different parallelograms.

Another motivation is the approximation of a given element of the group by elements of a given subgroup. This occur for example in the search of symplectic integrators (see [K, Su]) that give numerical schemes for long-time integration of hamiltonian systems. Namely we try to approximate $\exp(x+y)$ by a product of $\exp(x)$ and $\exp(y)$. In this frame, minimal length of mth-order approximants are bounded by approximately 2^m.

Acknowledgements

Authors would like to thank G. Duchamp for fruitful discussions and many helpful comments. He did focus our attention to the theory of noncommutative series. The first author would like to thank FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) for financial support and the *Institut de Mathématiques (UMR 7586)* for its kind support.

2 Definitions and examples

Definition 2.1 *A* segment *in a Lie group is a curve obtained by following the orbit of left-invariant vector field. It has initial and end points. Two segments are parallel if they are orbits of two dependent left-invariant vector fields.*

Definition 2.2 *A* polygonal line *in a Lie group is a curve obtained by concatenation of segments, two consecutive segments being not parallel. This is a sequence of segments where the end point of one of them coincides with the initial point of its successor. Each segment is called a* side.

Observe that once we have fixed a left invariant vector field X, a side is of the form $\gamma(t) = x_0 \exp(t\lambda X)$, where $0 \leq t \leq 1$. In that case we call $|\lambda|$ the *length* of the side. $\gamma(0)$ is its initial point and $\gamma(1)$ its end point.

Definition 2.3 *A* polygon *in a Lie group is a closed polygonal line. Its* length *is the sum of its sides lengths.*

Definition 2.4 *A* parallelogram *of* base *X and Y in a Lie group is a polygon with sides of integer length, obtained from the two given left-invariant vector fields X and Y, with minimum length. Two parallelograms are* equivalent *if there exists a group isomorphism which maps one parallelogram onto the other.*

In order to describe explicitly a polygonal line with n sides, let $\mathcal{F} = \{X_\alpha\}$ be a family of linearly independent vectors in the Lie algebra $\mathbf{g}$ of the Lie group G. Fix $x_0 = 1 \in G$. We write $\gamma_j(t) = x_{j-1} \exp(t\lambda_j X_{\alpha_j})$ for $x_j = x_{j-1} \exp(\lambda_j X_{\alpha_j})$, $0 \leq t \leq 1$ and $1 \leq j \leq n$. Here we require that X_{α_j} and $X_{\alpha_{j+1}}$ are independent. Denote by $P(\lambda_1 X_{\alpha_1}, \ldots, \lambda X_{\alpha_n})$ the polygonal line defined in this way.

Example 2.1 *Consider the abelian Lie group $\mathbb{R}^n$. A parallelogram in that group is clearly a* parallelogram.

Example 2.2 *Consider the Heisenberg group H^3 with Lie algebra generated by X,Y,Z, with $[X,Y]=Z$, all other brackets being null. One can verify, using the Campbell-Hausdorff formula that both*

$$P_8(X,Y) = P(X,Y,-X,-2Y,-X,Y,X) \text{ and } P_8'(X,Y) = P(X,Y,-X,-Y,-X,Y,X,Y)$$

are parallelograms. They are not equivalent as P_8 has at least one side of length two. On the other hand starting with X,Z we get a parallelogram of 4 sides.

Example 2.3 *Let L^4 be a free nilpotent group of order 4, generated by X and Y. We can verify that $P(X,Y,-2X,-Y,X,Y,X,-Y,-2X,Y,X,-Y)$ is a parallelogram. It has length 14. An interesting question would be to know all non-equivalent parallelograms.*

Example 2.4 *If the group generated by* $\exp(X)$ *and* $\exp(Y)$ *is free, then there is no parallelogram of base X and Y.*

We thank the referee for pointing out the two following examples.

Example 2.5 *As a result of a theorem by* SANOV *([Sa]), for $X^+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $X^- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, the group $G = < \exp(2X^+), \exp(2X^-) >$ is free (see also [LS]), so there exist no parallelogram of base $2X^+$ and $2X^-$. Moreover it is straightforward that $P = (\exp(X^+)\exp(-X^-))^6 = 1$ is a parallelogram of length 12 with base X^+ and X^-.*

We could have given a more general definition of a parallelogram in an arbitrary group. Let a and b be two elements on a group G and $G<a,b>$ be the subgroup generated by a,b. Consider the set of all relators, i. e., the set of words in a,b,a^{-1},b^{-1} which are the identity in G. One should consider only reduced words in the sense that if a is of order n and a^n appears in a word, one should substitute the identity for a^n. The same for b. A *parallelogram* of base a,b is a reduced relator (in the above sense) of minimal length with letters a,b,a^{-1},b^{-1}. Of course if $G<a,b>$ is free in a,b there is no parallelogram.

Example 2.6 *In the case of the symmetric group*

$$\mathbf{S}_3 = < \sigma_1, \sigma_2;\ \sigma_i^2 = 1, \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 >$$

one can verify that a minimal relator with base σ_1, σ_2 is $(\sigma_1\sigma_2)^3$ of length 6. On the other hand we have also

$$\mathbf{S}_3 = < \sigma_1, \sigma_3 = \sigma_2\sigma_1;\ \sigma_1^2 = 1, \sigma_3^3 = 1, \sigma_1\sigma_3 = \sigma_3\sigma_1 >$$

that has a minimal relator of length 4.

In the case of Lie groups we would like to define *infinitesimal parallelograms*, that is parallelograms which remain the same in form when their sides are changed by a conformal factor. They will not exist in general but in the case of graded nilpotent groups their existence is assured.

Example 2.7 *Consider the Lie group with Lie algebra generated by X,Y with $[X,Y]=X$. Then we can construct a parallelogram which is not infinitesimal. Observe that*

$$\exp(tY)\exp(uX)\exp(-tY) = \exp(u\exp(-t)X)).$$

So if $t = -\ln 2$ *and* $u = 1$*, we have* $\exp(tY)\exp(uX)\exp(-tY)\exp(-u\exp(-t)X) = 1$*. That is a parallelogram of length 5 with base* $\ln 2\ Y$ *and* X*. It is clear that if we change the sides by a conformal factor this will no longer be a parallelogram. More generally, a polygon is a product*

$$\exp(c_1 Y)\exp(d_1 X)\cdots\exp(c_n X)\exp(d_n Y)$$

such that $\sum_i(\sum_{j\leq i} c_j)\exp(-d_i) = 0$*. The previous equation has clearly no integer solutions.*

Example 2.8 *Let us consider in* $\mathbb{R}^2$*,* $X = \partial_x$ *and* $Y = f(x)\partial_y$ *for a given analytic function* f*. The Lie algebra* $L(X,Y)$ *is in general infinite dimensional as* $(\mathrm{ad}\ X)^n Y = f^{(n)}(x)\partial_y$ *and is spanned, as vector space by* X *and* $\{(\mathrm{ad}\ X)^n Y\}$*. By noticing that* $\exp(\lambda \mathrm{ad}\ X)Y = f(x+\lambda)\partial_y$*, we deduce that*

$$\exp(tX)\exp(uY)\exp(-tX) = \exp(uf(x+t)\partial_y)$$

so

$$\begin{aligned}\exp(X)\exp(Y)\exp(-X)\exp(Y)\exp(X)\exp(-Y)\exp(-X)\exp(-Y) &= \\ \exp(f(x+1)\partial_y)\exp(f(x)\partial_y)\exp(-f(x+1)\partial_y)\exp(-f(x)\partial_y) &= 1.\end{aligned}$$

This gives a parallelogram of length 8.

3 Magnus Groups and Algebras

Let us first introduce some notations and recall some results about free groups, free associative algebras and free Lie algebras. All these results can be found in ([B, La, R]).

Let X be a set (alphabet). We denote by X^* the free monoid generated by X, that is, the set of words including the empty word denoted by 1, with concatenation as a product. X^* is totally ordered by the lexicographic order. The free magma $M(X)$ is the set of words with parentheses, generated by X and $A(X)$ denotes the free associative algebra, that is to say the $\mathbb{Q}$-algebra of X^*. An element P in $A(X)$ will be written $\sum_{w\in X^*}(P,w)w$.

We denote by $L(X)$ the free Lie algebra on A. It is the quotient of the $\mathbb{Q}$-algebra of $M(X)$ by the ideal generated by the elements (u,u) and $(u,(v,w)) + (v,(w,u)) + (w,(u,v))$. The associative algebra $A(X)$ may be identified to the enveloping algebra of $L(X)$ by considering $[v,w] = vw - wv$. We denote by ad x the map $y \mapsto [x,y]$.

The free group generated by X is denoted by $F(X)$.

3.1 Gradations

The sets $L(X), F(X)$ so as $A(X)$ are graded by
— the length (the unique homomorphism that extends the function $x \mapsto 1$ on X). For $x \in X^*$ (resp. $F(X), M(X)$) $|x|$ denotes the length. $L_n(X)$ (resp. $A_n(X)$) is the submodule generated by monomials of length n.
— the multi-degree which is the unique homomorphism from X^* (resp. $F(X), M(X)$) onto $\mathbb{N}^{(X)}$ that extends $x \mapsto \mathbb{1}_x$. For a given α in $\mathbb{N}^{(X)}$, $L^\alpha(X)$ (resp. $A^\alpha(X)$) denotes the submodule generated by monomials of degree α.

Definition 3.1 *Let A,B be subgroups of a group C. We denote by (A,B) the set of all commutators $(a,b)=aba^{-1}b^{-1}$. Starting with $F_{\geq 1}(X)=F(X)$ and defining $F_{\geq n}(X)=(F_{\geq 1}(X),F_{\geq n-1}(X))$, we get the so-called* lower central series.

As a consequence, we have $(F_{\geq n}(X),F_{\geq m}(X))\subset F_{\geq n+m}(X)$ and $F(X)/F_{\geq n}(X)$ is an abelian group.

3.2 Formal series

We define $\hat{L}(X)$ and $\hat{A}(X)$ as $\hat{L}(X)=\prod_{n\geq 0}L_n(X)$ $\hat{A}(X)=\prod_{n\geq 0}A_n(X)$. We will write $x\in\hat{L}(X)$ (resp. $\hat{A}(X)$) as a series $\sum_{n\geq 0}x_n$. $\hat{L}(X)$ so as $\hat{A}(X)$ are algebras with multiplications law

$$(xy)_n=\sum_{p+q=n}x_py_q,\ ([x,y])_n=\sum_{p+q=n}[x_p,y_q]. \tag{1}$$

We will also use $\hat{L}_{\geq p}(X)=\prod_{n\geq p}L_n(X)$ $\hat{A}_{\geq p}(X)=\prod_{n\geq p}A_n(X)$. The set $\Gamma(X)=1+\hat{A}_{\geq 1}(X)$ is called the *Magnus group*. It is a subgroup of the invertible elements of $\hat{A}(X)$. One defines the exponential and the logarithm as

$$\begin{array}{rcl} \exp:\hat{A}_{\geq 1}(X) & \to & \Gamma(X) \\ x & \mapsto & \sum_{n\geq 0}\dfrac{x^n}{n!}, \end{array} \qquad \begin{array}{rcl} \log:\Gamma(X) & \to & \hat{A}_{\geq 1}(X) \\ x & \mapsto & -\sum_{n\geq 1}\dfrac{(1-x)^n}{n}. \end{array}$$

They are mutually reciprocal functions and we have (see [B, Ch. II, §5]) the

Theorem 3.1 (Campbell-Hausdorff) *For $x,y\in\hat{L}_{\geq 1}(X)$,*

$$H(x,y)=\log[\exp(x)\exp(y)]\in\hat{L}_{\geq 1}(X). \tag{2}$$

Denoting by $\hat{E}_{\geq n}(X)=\exp(\hat{L}_{\geq n}(X))$, we get

Corollary 3.1 *The set $\hat{E}_{\geq 1}(X)=\exp(\hat{L}_{\geq 1}(X))\subset\Gamma(X)$ is a group.*

$\hat{E}_{\geq 1}(X)$ acts on itself by conjugacy and we have $\exp(x)\exp(y)\exp(-x)=\exp(\exp(\mathrm{ad}\,x)y)$.

Definition 3.2 *Let us consider the Magnus map $\mu:F(X)\to\Gamma(X)$ as the unique group homomorphism that extends $x\mapsto 1+x$, for $x\in X$. We set $D_{\geq n}(X)=\mu^{-1}(1+\hat{A}_{\geq n}(X))$. This is Magnus' n-th dimension subgroup of F.*

Definition 3.3 *Let us consider the map $\mu':F(X)\to\Gamma(X)$ as the unique group homomorphism that extends $x\mapsto\exp(x)$, for $x\in X$. We set $D'_{\geq n}(X)=\mu'^{-1}(1+\hat{A}_{\geq n}(X))$.*

This defines central filtrations of $F(X)$. We have clearly that $F_{\geq n}(X)\subset D_{\geq n}(X)$ and $F_{\geq n}(X)\subset D'_{\geq n}(X)$. In fact Magnus proved a stronger result (see [B])

Proposition 3.1 $D_{\geq n}(X)=D'_{\geq n}(X)=F_{\geq n}(X)$

Let $N_n(X)$ be the free nilpotent group of class n (or order $n+1$) on X. That is

$$1\to F_{\geq n+1}(X)\to F(X)\to N_n(X)\to 1 \tag{3}$$

We will use the following corollary to establish the lower bound to the number of sides of parallelogram on the free nilpotent group.

Corollary 3.2 *The projection of g in $F(X)$ onto $N_n(X)$ is the identity if and only if $\mu'(g)\in\hat{E}_{\geq n}(X)$.*

In fact we need only the if part of the corollary for the lower bound, that is not dependent on Magnus result but on the inclusion $F_{\geq n}(X)\subset D_{\geq n}(X)$.

4 mth-order parallelograms

Definition 4.1 *The* order *of g in $F(X)$ is the biggest integer k such that $g \in F_{\geq k}(X)$. An element of order k will be called* kth-order polygon.

Using proposition (3.1), a mth-order polygon g satisfies

$$\begin{aligned} g &= x^{a_1}y^{b_1}\cdots x^{a_n}y^{b_n} \in F_{\geq m}(X), & (4)\\ \mu'(g) &= \exp(a_1x)\exp(b_1y)\cdots\exp(a_nx)\exp(b_ny) \in 1+\hat{A}_{\geq m}(X), & (5)\\ \mu(g) &= (1+x)^{a_1}(1+y)^{b_1}\cdots(1+x)^{a_n}(1+y)^{b_n} \in 1+\hat{A}_{\geq m}(X). & (6)\end{aligned}$$

Here none of $a_i's$ nor $b_i's$ is 0.

Definition 4.2 *The* length $l : F(X) \to \mathbb{N}$ *is the unique homomorphism that extends $x \mapsto 1, x^{-1} \mapsto 1$, for x in X. If $g = x_1^{i_1}\cdots x_p^{i_p} \in F(X)$, we sill say that it is a* p-sided *polygon. For example $xyx^{-1}y^{-1}$ is a 4-sided second-order parallelogram of length 4. In formula (4), we have $l(g) = \sum_{i=1}^n(|a_i|+|b_i|)$.*

We thus deduce that for any g_1, g_2 in $F(X)$, we have $l(g_1g_2) \leq l(g_1)+l(g_2)$. The inequality is strict only if terms of g_1 cancel terms of g_2.

Definition 4.3 *For $m \in \mathbb{N}$, we define l_m as the lowest length of mth-order polygons. A* mth-order parallelogram *will be a mth-order polygon of minimal length.*

Before discussing the lower and upper bounds for the length and the number of factors of mth-order parallelograms, let us show some transformations that preserve polygons.

Proposition 4.1 *Let $\alpha\beta$ be a mth-order polygon then so is $\beta\alpha$.*

Corollary 4.1 *If g is a $(2p+1)$-sided mth-order polygon then there exists a $2p$-sided mth-order polygon.*

Proof. — The proposition comes from the fact that $F/F_{\geq m}(X)$ is abelian.
Let us suppose that $g = x^{a_1}y^{b_1}\cdots y^{b_p}x^{a_{p+1}}$ is a mth-order polygon. Then

$$x^{(a_1+a_{p+1})}y^{b_1}\cdots y^{b_p} \tag{7}$$

has smaller length as $|a_1+a_{p+1}| \leq |a_1|+|a_{p+1}|$ and is also a mth-order polygon. □

We can now suppose that for any integer m, an mth-order parallelogram has an even number of factors. We will now discuss lower and upper bound of l_m.

4.1 Lower bound

Proposition 4.2 *For any $m \in \mathbb{N}$ we have $m \leq l_m$.*

Proof. — Let us consider the following equality

$$\exp(a_1x)\exp(b_1y)\cdots\exp(a_nx)\exp(b_ny) = \exp(z). \tag{8}$$

where $z \in \hat{L}_{\geq m}(X)$ and none of the $a_i's$ nor b_i's is 0. Considering the word $w = (xy)^n$, we have

$$(\exp(z), w) = \prod_{i=1}^n a_ib_i \neq 0$$

and so $m \leq 2n \leq l_m$. In fact the number of sides itself is bigger than m. □

4.2 Upper bound

First of all, let us show some small-order parallelograms.

If $m=1$ $g_1=x$ or $g_1=y$ is convenient. If $m=2$, we find $g_2=xyx^{-1}y^{-1}$ thus $l_2\leq 4$. In fact $l_2=4$ which is a consequence of the following

Lemma 4.1 *For any $m\geq 2$, l_m is even.*

Proof. — This is a consequence of

$$\mu(g)=(1+x)^{a_1}(1+y)^{b_1}\cdots(1+x)^{a_1}(1+y)^{b_1}=1+(a_1+\cdots+a_n)x+(b_1+\cdots+b_n)y\ (\hat{A}_{\geq 2}(X)).$$

So if $\mu(g)$ belongs to $\hat{A}_{\geq m}(X)$ we have $\sum_{i=1}^n a_i=\sum_{i=1}^n b_i=0$ thus $\sum|a_i|$ and $\sum|b_i|$ are even. □

We have seen g_2 as the commutator of two first-order polygons. We will now build a sequence g_m of mth-order polygons, each g_m being constructed as commutator of g_p and g_{m-p} for some p. We first use the following lemma

Lemma 4.2 *Let g_p and g_q be two polygons of order p and q respectively, then (g_p,g_q) has order at least $p+q$ and has length at most $2(l(g_p)+l(g_q))$.*

Remark. — This is also a consequence of the fact that $(F_{\geq n}(X))_n$ is a central filtration but we will show it by using the Hausdorff series.

Proof. — Let us write

$$P_p=\mu'(g_p)=\exp(x)=\exp(\textstyle\sum_{k\geq p}x_k),P_q=\mu'(g_q)=\exp(y)=\exp(\sum_{k\geq q}y_k). \tag{9}$$

then we have

$$P_pP_qP_p^{-1}P_q^{-1}=\exp(\exp(\operatorname{ad}x)y)\exp(-y)=\exp(H(\exp(\operatorname{ad}x)y,-y)). \tag{10}$$

But

$$\begin{aligned} H(\exp(\operatorname{ad}x)y,-y) &= H_1(\exp(\operatorname{ad}x)y,-y)+\sum_{k\geq 2}H_k(\exp(\operatorname{ad}x)y,-y) &(11)\\ &= \exp(\operatorname{ad}x))y-y+\textstyle\sum_{k\geq 2}H_k(\exp(\operatorname{ad}x)y,-y) &(12)\\ &= [x,y]+\sum_{k\geq 2}\frac{1}{k!}(\operatorname{ad}x)^k y+\sum_{k\geq 2}H_k(\exp(\operatorname{ad}x)y,-y). &(13)\end{aligned}$$

But $(\operatorname{ad}x)^k y\in\hat{L}_{\geq kp+q}(X)\in\hat{L}_{\geq 2p+q}(X)$ and $H_k(\exp(\operatorname{ad}x)y,-y)=H_k(\exp(\operatorname{ad}x)y-y,-y)\in\hat{L}_{\geq p+2q}(X)$. In conclusion, if $[x_p,y_q]\neq 0$, then $g_{p+q}=(g_p,g_q)$ is a $p+q$-th order polygon and has length $2(l(g_p)+l(g_q))$. In order to be sure to obtain a $(p+q)$-th order polygon let us show that

Lemma 4.3 *Let $\alpha\in F_{\geq p}(X)$ and $\beta\in F_{\geq q}(X)$ such that*

$$\mu'(\alpha)=\exp(x)=\exp(\textstyle\sum_{k\geq p}x_k),\mu'(\beta)=\exp(y)=\exp(\sum_{k\geq q}y_k). \tag{14}$$

If x_p and y_q are not proportional, then (α,β) has order exactly $p+q$.

Proof. — This is a consequence of the following lemma.

Lemma 4.4 *Let $x_p \in L_p(X)$ and $y \in L_q(X)$. If x_p and y_q are not proportional then $[x_p, y_q] \neq 0$.*

Proof. — Let us write

$$x_p = \sum_{w \in X_p^*} (x_p, w) = \sum_{i=1}^{n} \lambda_i w_i, y_q = \sum_{w \in X_q^*} (y_q, w) = \sum_{i=1}^{n'} \lambda'_i w'_i. \tag{15}$$

Here we have $w_i < w_j$ if $i < j$. As $[x_p, y_q] = [x_p, y_q - \lambda x_p]$ for some λ, one can suppose that $w_1 < w'_1$. In fact w_1 and w'_1 are so-called Lyndon words (see [R]), that is to say satisfy $w_1 w'_1 < w'_1 w_1$. In

$$\begin{aligned}[x_p, y_q] &= \lambda_1 \lambda'_1 (w_1 w'_1 - w'_1 w_1) \\ &+ \lambda_1 \sum_j \lambda'_j (w_1 w'_j - w'_j w_j) + \lambda'_1 \sum_i \lambda_i (w_i w'_1 - w'_1 w_i) + \sum_{i,j>1} \lambda_i \lambda'_j (w_i w'_j - w'_j w_i)\end{aligned} \tag{16}$$

As $w_1 < w'_1 < w'_j$ we deduce that $w_1 w'_1 < w_i w'_1 < w_i w'_j$ for each $i, j > 1$. We have also $w_1 w'_1 < w'_1 w_1 < w'_1 w_i < w'_j w_i$ so $w_1 w'_1$ is the smallest word in formula (16). This proves that $([x_p, y_q], w_1 w'_1) \neq 0$ and so $[x_p, y_q] \neq 0$. □

Remark. — Lemma 4.4 shows that for any not null Lie polynomial P the kernel of ad P is spanned by P.

We will show that

Proposition 4.3 *There exists a sequence of mth-order polygons g_m with even length $l_m \leq m^2$.*

Proof. — We will prove by induction on m the following $P(m)$: "there exists a sequence g_m or order exactly m with even length $l_m \leq m^2$."

If $m = 1$, then $g_1 = x$ or $g_1 = y$ is convenient. If $m = 2$ then $g_2 = (x, y) = xyx^{-1}y^{-1}$ is convenient and has length 4. If $m = 3$ then $g_3 = (g_1, g_2) = x^2 yx^{-1}y^{-1}x^{-1}yxy^{-1} \cdot x^{-1}$ is a third-order polygon so as $xyx^{-1}y^{-1}x^{-1}yxy^{-1}$ that has length 8.

Suppose now $P(m)$.

- If $m + 1 = 2p + 1$ is odd, let us consider $g = (g_p, g_{p+1})$. p and $p + 1$ have not same parity so

  $$l(g) \leq 2(l_p + l_{p+1}) \leq 2(p^2 + (p+1)^2 - 1) = (2p+1)^2 - 1.$$

  We thus deduce that g is a $(2p+1)$th-order polygon and so $l_{2p+1} \leq (2p+1)^2 - 1$.

- If $m + 1 = 4p$, let us consider $g = (g_{2p-1}, g_{2p+1})$.

  $$l(g) \leq 2(l_{2p-1} + l_{2p+1}) \leq 2((2p+1)^2 + (2p-1)^2 - 2) = (4p)^2$$

- If $m + 1 = 4p + 2$, let us consider $g = (g_{2p+1}, \varphi(g_{2p+1}))$. Here φ is the involution $x \mapsto y, y \mapsto x$. If $\mu'(g_{2p+1}) = \exp(\sum_{k \leq 2p+1} x_k)$, we will have

  $$\mu'(g) = \exp([x_{2p+1}, \varphi(x_{2p+1})] + \textstyle\sum_{k \geq 2p+2} y_k). \tag{17}$$

  The degree of x_{2p+1} in x is not the degree in y so x_{2p+1} as $2p + 1$ is odd and $\varphi(x_{2p+1})$ have not same multi-degree thus are not proportional. It follows that $g \in F_{\geq m+1}(X)$. We have

  $$l(g) \leq 4 l_{2p+1} \leq (4p+2)^2 - 4 \leq (4p+2)^2. \tag{18}$$

We thus deduce that $l_{m+1} \leq (m+1)^2$. Proposition 4.3 is then proved. □

4.3 Rational series

In fact there is a strong connection with the rank of rational series. The set $\hat{A}(X)$ is usually denoted by $\mathbb{Q}<<X>>$ and is called the set of formal series.

Consider the following operation of X^* on $\hat{A}(X)$; for $u \in X^*$, let

$$u^{-1}S = \sum_{w \in X^*} (S, uw)w \tag{19}$$

We extend it by linearity to obtain $\hat{A}(X)$ as a right module over $A(X)$.

A combinatorial interpretation of that operation in the case where $S = v$ is a single word says that $u^{-1}v$ vanishes , unless v starts with u, that is, $v = uv'$, and in that case $u^{-1}v = v'$.

Definition 4.4 *A formal series is rational if it is an element of the closure of* $A(X)$

A fundamental theorem due to M.-P. Schützenberger assures that the orbits of the action of $A(X)$ are finite dimensional over $\mathbb{Q}$ on rational series. We may then state the following

Definition 4.5 *The rank of a rational series S is the dimension of the space* $S \circ A(X)$.

We state now corollary 3.6 of [BR].

Proposition 4.4 *If* $S \in 1 + \hat{A}_{\geq m}(X)$ *is a rational series, then* $\operatorname{rank} S \geq m$

To obtain a lower bound on the length of a polygon we will compute the rank of the rational series $\mu(g) = (1+x)^{a_1}(1+y)^{b_1} \cdots (1+x)^{a_n}(1+y)^{b_n}$.

Proposition 4.5 $\operatorname{rank}\left[(1+x)^{a_1}(1+y)^{b_1} \cdots (1+x)^{a_n}(1+y)^{b_n}\right] \leq \sum_i |a_i| + |b_i|$.

Proof. — We first observe that the following properties are easily established [BR]

$$x^{-1}(ST) = (x^{-1}S)T + (S,1)(x^{-1}T) \tag{20}$$

$$x^{-1}(S^*) = x^{-1}S^* \quad \text{where} \quad S^* = (1-S)^{-1} \tag{21}$$

Observe that $x^{-1}(1+x) = 1, x^{-1}(1+y) = 0, y^{-1}(1+x) = 0, y^{-1}(1+y) = 1$.

An easy computation then gives that $\operatorname{rank}[(1+x)^a] = |a|$, and this implies that

$$\operatorname{rank}\left[(1+x)^a(1+y)^b\right] = |a| + |b| .$$

From equation 20 we deduce that $\operatorname{rank}(ST) \leq \operatorname{rank}(S) + \operatorname{rank}(T)$ and that implies that the rank of a product $(1+x)^{a_1}(1+y)^{b_1} \cdots (1+x)^{a_n}(1+y)^{b_n}$ can be at most $\sum_{i=1}^n |a_i| + |b_i|$. □

References

[BeR] A. BELLAÏCHE, J.-J. RISLER (EDITORS), Sub-Riemannian Geometry. Progress in Mathematics 144. Birkhäuser 1996.

[BR] J. BERSTEL, C. REUTENAUER, Rational series and their languages EATCS Monographs on Theoretical Computer Science. Springer (1988).

[B] N. BOURBAKI, *Groupes et algèbres de Lie*. Hermann, Paris (1972).

[FGR] E. FALBEL, C. GORODSKI, M. RUMIN, *Holonomy of sub-Riemannian manifolds*. International Journal of Mathematics, **8**, No. 3, pp. 317-344, 1997.

[K] P.-V. KOSELEFF, *About approximations of exponentials*, Lecture Notes in Computer Science, **948** pp. 323-333, 1995.

[La] J. P. LABUTE, *Groups and Lie algebras: the Magnus theory* in mathematical legacy of Wilhelm Magnus: groups, geometry and special functions, Contemp. Math. **169**, A.M.S., 1992.

[LS] R.C. LYNDON R.C., P.E. SHUPP, *Combinatorial group theory*, Springer (1977).

[R] C. REUTENAUER, *Free Lie algebras*, Oxford Science Publications (1993).

[Sa] I. N. SANOV, *A property of a representation of a free group.* Dokl. Akad. Nauk. SSSR **57**, 657-659, 1947.

[Su] M. SUZUKI, *General nonsymetric higher-order decompositions of exponential operators and symplectic integrators*, Physics Letters A, **165**, pp. 387-395, 1993