Journal of Algebra **242,** 109–145 (2001)
doi:10.1006/jabr.2000.8700, available online at http://www.idealibrary.com on IDEAL®

Asymptotic Cyclic Expansion and Bridge Groups of Formal Proofs

A. Carbone

Mathématique/Informatique, Université de Paris XII,
61 Avenue du Général de Gaulle, 94010, Créteil Cedex, France
E-mail: carbone@ihes.fr, ale@univ_paris12.fr

Communicated by J. Tits

Received February 9, 2000

Formal proofs, even simple ones, may hide an unexpected intricate combinatorics. We define a new combinatorial invariant, the *bridge group* of a proof, which encodes the cyclic structure of proofs in the sequent calculus. We compute the bridge groups of two infinite families of proofs and identify them with the Baumslag–Solitar and Gersten groups. We observe that the *distortion* of cyclic subgroups in these groups equals the asymptotic growth of the procedure of elimination of lemmas from the proofs.

Key Words: formal proofs; logical flow graphs; cut elimination; bridge groups; Baumslag–Solitar groups; Gersten groups.

1. INTRODUCTION

There is a clear sense that the process used by a human brain to generate proofs is not a one dimensional path. Unraveling the intrinsic logic of the brain seems unsurmountably difficult because language has a "sequential" nature and representations in our brain have apparently more dimensions and a different geometry. Thus, we shall be bound to *formal* proofs which are closer in spirit to what a machine can do.

We usually think of formal proofs as constructing formulas from axioms, by means of rules which combine previously proved formulas into more complicated ones, and which allow for the use of lemmas. The latter is accomplished by the use of modus ponens: if you know A and you know that A implies B then you know B. The formula A plays the role of the lemma.

0021-8693/01 $35.00

Different combinations of rules for proving the same theorem might correspond to different "arguments," and in the space of all formal proofs, we would like to have a measure to express how far apart two proofs of the same statement are. This aim seems to be currently out of reach: the traditional analytical approach to proofs attempts to reduce the study of global properties to those of the building blocks of the proof, with little regard for how these building blocks fit together. This strategy does not lead to the desired "understanding" of a proof. The reason lies in the *computational* content of proofs that is hidden in their formal representation and that cannot be captured by a purely reductionistic analysis. This point will be clear soon.

In 1934, Gentzen proved a seminal result (the Gentzen Cut Elimination Theorem [Gen34]) to the effect that the rule of modus ponens is not needed in some logical systems; that is, one can make proofs without using lemmas. The strength of this result was forcefully manifested by Girard who, by applying Gentzen's Cut Elimination Theorem, showed [Gir87a] that one can recover the elementary combinatorial argument used by van der Waerden to prove his theorem on arithmetic progressions[1] [VdW27] from the transcendental methods in dynamical systems used by Furstenberg and Weiss [FW78]. In other words, the convoluted combinatorial proof of van der Waerden and the more transparent proof expressed in the language of dynamical systems turn out to be recoverable one from the other by a purely local combinatorial manipulation of their formal rules (together with some finitarisation of compactness). Thus the proof based on dynamical systems contains, in some codified form, all information needed for the combinatorial proof. How is this codification possible?

It turns out that the use of lemmas allows the coding: the dynamical proof (with lemmas) of Furstenberg and Weiss represents an *implicit* computation, and cut-elimination unravels this computation to an *explicit* form, which is represented by the combinatorial cut-free proof. This transformation is possible at the cost of a large expansion in the size of the proof. Already for propositional tautologies, there are proofs without lemmas with a number of lines which is exponentially larger than the number of lines of proofs with lemmas [Sta78, Hak85, Bus87], and in predicate logic this expansion can be multi-exponential [Ore79, Ore93, Sta78, Sta79, Tse68].

The fact that lemmas allow dynamics within the implicit computations occurring in proofs was emphasized by Girard who, in 1987, introduced a graphical tool called *proof nets*, to study proofs as *global* entities

[1]The van der Waerden Theorem, the first and still the most inspiring result of the Ramsey theory, can be formulated geometrically as follows: given a finite set of points in a finitely colored (partitioned) plane, there is a parallel translation followed by a dilation which moves the set into a monochromatic position.

where formulas interact in a proof through logical connectives. The fundamental ideas of Girard's "geometry of interaction" are explained in [Gir89a, Gir89b, Gir95]. In 1991, another notion of graph associated to proofs has been introduced by Buss [Bus91]. This notion, called *logical flow graph*, traces the flow of formula occurrences in a proof. It captures geometries of interaction formed by duplicating formulas or by identifying several copies of them. Paths of formula occurrences might be cyclic; they might turn around in a small space, meet, and split again. This dynamical view of proofs was presented in [Car98] where it was shown that cycles are responsible for making certain proofs *short*.

In this paper, we look at a formal system with *no induction* and we present two constructions whose main point is to illustrate that an exponential and a multi-exponential speed-up in the number of lines of proofs can be obtained if quantifiers are used in the lemmas of the proofs. In [Car98] it has been shown that these two speed-ups force the presence of cycles in the underlying graphs of short proofs. Here we analyze these cycles and interpret them as *group relations*. The resulting finitely presented group is called the *bridge group* associated to the proof.

We compute the bridge groups of the families of proofs relative to the two constructions mentioned above and we show that the first family corresponds to the family of groups

$$BS_*^{(i)} = \{b, c | b^2 = b^{w_i}\},$$

where $w_1 = c, w_2 = cbc, w_3 = cbcbc$, and so on, which turn out to contain the Baumslag–Solitar group $BS_{1,2} = \{b, c \mid b^2 = cbc^{-1}\}$ [BS62] as a subgroup and to have the same kind of exponential distortion as $BS_{1,2}$. In the second case, we find the family of groups

$$Gerst_*^{(i)} = \{b, c \mid b^2 = b^{w_i^*}\},$$

where $w_1^* = b^d, w_2^* = b^{b^d}, w_3^* = b^{b^{bd}}$, and so on, $d = (b^{a^{-1}})^{-1}$ and $a = b^c$. These groups have the same multi-exponential distortion as the Gersten's groups $Gerst^{(i)}\{b, c \mid b^2 = b^{w_i}\}$, where $w_1 = b^c, w_2 = b^{b^c}, w_3 = b^{b^{bc}}$ [Ger90, Ger93]. Our basic observation is that *the asymptotic expansion induced by the elimination of lemmas in the two families of proofs coincides with the distortion in the corresponding families of groups.*

The above is reminiscent of the algorithmic study of the group theoretic problems starting from the work of Novikov [Nov54] and Boone [Boo54] who have shown that for any Turing machine M there is a finitely presented group $G(M)$ that simulates M, in the sense that there is an injective map k

from the set of input words of M into the words in the group such that a word u is accepted by M if and only if $k(u)$ is equivalent to the trivial word in $G(M)$.

Recently this work was refined by Sapir et al. [SBR99] and by Ol'shanskii and Sapir [OS99]. These authors prove that this implementation can be made with control of the Dehn function of the group by the computational complexity of the Turing machine. This construction can be thought of as an exact (injective) "functor" from the "category" of Turing machines to groups, where this functor is by no means unique or canonical. In contrast, our operation is relatively natural and not at all injective: two different proofs might give the same bridge group. There is a definite simplification when going from proofs to bridge groups and these groups may serve as invariants of proofs which are more refined than numerical complexity parameters but still transparent enough to be useful.

The introduction of bridge groups, rather concrete and elementary objects compared to proofs, is motivated by our attempt to re-think the notion of *logical deduction*. We do not expect bridge groups to be ultimate invariants but rather a step-stone towards a structural theory of *growth* of proofs (where the notion of growth might concern the size of terms in proofs, the computation time of cut elimination, or the size of proofs after cut elimination).

This paper may be of specific interest to proof theorists and group theorists. A proof theorist wonders whether the structural properties of the proof of a given theorem are language dependent or not. In this sense, bridge groups turn out to be not only interesting as combinatorial invariants but also as a kind of homotopy invariants of proofs. The group theorist might find that our approach provides a natural way to generate groups where, for example, different uses of induction in arithmetic might lead to the construction of new groups with various geometric and combinatorial properties.

In the following we think of proofs as formalized in the sequent calculus where the cut rule plays the role of modus ponens. We shall introduce these notions and give some insights in Section 2. (For a full presentation of the sequent calculus and the Gentzen's Cut Elimination theorem, see [Gir87a, Tak87].) In Subsection 2.1 we present some logical construction of large numbers in arithmetic and in Section 3 we recall the notion of distortion in groups. The notions of logical graph and cycles in proofs will be recalled in Section 4 and in Subsection 4.1 we describe how cycles are formed in the two constructions presented in subsection 2.1. Section 5 contains a presentation of various notions concerning logical graphs associated to proofs. In Section 6 we introduce the concept of a bridge group and prove our main results (Theorems 12 and 13). We conclude with some open questions.

2. FORMAL PROOFS

To construct a formal proof one starts from several sequences of formulas, combines the formulas through rules, and ends up with only one sequence. This last sequence is the theorem. This process could be, in principle, handled by a machine since rules merely provide a syntactical manipulation of the formulas.

We describe now a set of rules, called *sequent calculus*, that allows for the construction of any formal proof. It has been proposed by Gentzen in 1934 [Gen34]. The sequent calculus permits us to build *sequents*. A sequent is something of the form

$$A_1, \ldots, A_n \to B_1, \ldots, B_m,$$

where the A_i's and the B_j's are formulas. It is interpreted as "from A_1 and A_2 and ... and A_n follows B_1 or B_2 or ... or B_m." Notice that the arrow $\to$ is not a connective, nor is the sequent a formula, and that we shall use the symbol $\supset$ to represent the logical implication. One could ask: Why do we not simply use the formula $A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$ instead of the above sequent? The point is that the two representations are combinatorially different: the commas in a sequent permit us to treat the formulas A_i, B_j as individuals which can each be used separately. This feature allows a certain flexibility in formal deductions and induces some monotonicity properties on the way that formulas are constructed. An introduction to these combinatorial aspects of the sequent calculus is found in [CS97].

The detailed description of axioms and rules is not very important for our discussion and we shall only emphasize some relevant point. The *axioms* are sequents of the form $A, \Gamma \to \Delta, A$, where A is any formula and Γ, Δ are any collections of formulas. The formula A appears both on the left and on the right of the sequent arrow.

There are rules for the introduction of all logical connectives $\wedge, \vee, \supset, \neg$ and quantifiers $\forall, \exists$, both on the left and on the right of the sequent arrow. We shall display, as an example, the rules introducing the connective $\wedge$ on the right and on the left

$$\frac{\Gamma, \to \Delta, A \;\; \Pi \to \Lambda, B}{\Gamma, \Pi \to \Delta, \Lambda, A \wedge B} \qquad \frac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta},$$

where the letters A, B stand for any formula, and where $\Gamma, \Pi, \Delta, \Lambda$ are arbitrary collections of formulas. In our notation, a rule is always denoted by a bar. The sequents above the bar are called *antecedents* of the rule and the sequent below the bar is called the *consequent*. We say that a rule is *binary* if it has two antecedents, and *unary* if it has only one.

Two more rules belong to the sequent calculus

$$\textit{Cut}\ \frac{\Gamma \to \Delta, A \quad A, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}$$

$$\textit{Contraction}\ \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A} \qquad \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}.$$

The cut rule can be thought as a "generalization" of the more familiar rule of *modus ponens*

$$\frac{A \quad A \supset B}{B}$$

saying that if "A implies B" then by proving the lemma A one can derive B. Once the lemma A is applied, we forget about it and we only need to use its consequence B. This is an important difference between the cut rule and the rules introducing logical symbols. The formula A disappears from the consequent of the cut rule, while for the other rules, the formulas in the antecedent(s) appear as subformulas in the consequent.

The contraction rule says that if a formula has been deduced twice then we can identify its two occurrences. This rule seems completely innocuous, but in cooperation with the cut rule allows formal proofs with cuts to be much smaller in size than cut-free proofs.

A *proof*, in this formal language, is viewed as a *binary tree* of sequents, where each occurrence of a sequent in a proof can be used at most once as antecedent of a rule. The root of the tree is labelled by the theorem, its leaves are labelled by axioms, and its internal nodes are labelled by sequents derived from one or two sequents (which label the antecedents of the node in the tree) through the rules. We shall say that a proof has k *lines*, if the number of nodes in its tree structure is k.

The sequent calculus is a system of pure logic, where axioms and rules are not concerned with any specific mathematical structure, but they constitute a flexible framework for the manipulation of formulas. One could add mathematical axioms to the system as well as new rules. For instance, for any formula A which we want to be an axiom, we could augment the system with the sequent $\Gamma \to \Delta, A$ and say that the leaves of a proof are allowed to be labelled by this sequent as well as by the usual axioms. Rules could be handled similarly.

In 1934 Gentzen ([Gen34]; see also [Gir87a, Tak87]) proved the following

CUT ELIMINATION THEOREM. *Any proof in the sequent calculus can be effectively transformed into a proof which never uses the cut rule. This works for both propositional and predicate logic.*

This is a fundamental result in logic and we will refer to it several times in the paper. The "price" of cut elimination is that the cut-free proof may have to be much larger than proofs without cuts. There are propositional tautologies for which cut-free proofs must be exponentially larger than proofs with cuts, and in predicate logic the expansion can be multi-exponential. See [Ore79, Ore93, Sta78, Tse68]. Gentzen's result can be extended to mathematical theories, like arithmetic for instance. But in this case, the cut-free proof might be infinite. (For an introduction to the combinatorics and complexity of cut elimination the reader can consult [CS97].)

To conclude this brief account, let us add a word on automatic deduction. If a machine wants to build a proof of a given theorem, it needs to choose among the formulas that it already knows how to prove, which formulas have to be combined at different moments of the proof. We all know how hard this is. Alternatively, the machine could start from the theorem and try to build the labelled binary tree corresponding to the formal proof from the root to the leaves. Then, at a given step, it decides either to use a rule introducing a logical symbol, or to apply the cut rule and "guess" the lemma. Again, we know how difficult this second choice can be. Proofs without lemmas are usually too large to be constructed by a machine, but they are the only object that a machine can presently build. This is why automatic deduction remains in a prokaryotic state.

In the next section we present two proofs which might look very simple in the eye of a mathematician but their analysis reveals an unexpectedly intricate combinatorics.

2.1. *Two Short Proofs*

How can we "build" large numbers in an efficient way? Suppose that small numbers as $0, 1, 2$ are constructible, and that if x and y are constructible numbers then also the successor of x and the product of x and y are constructible. It is clear that after some number of steps we can derive that any number is constructible. Could we use some logical reasoning to prove in a *small* number of lines that certain large numbers are constructible? The answers we present here are well known in logic and we recall them because they provide examples of formal proofs that are both sufficiently simple and representative for our further discussion.

Let us consider the language of arithmetic $2, *, s$ (along with the constant 2, the operations of multiplication $*$, and successor s we could admit the operation of addition $+$ as well but it will not be necessary for our discussion; also, the constant 2 has been chosen instead of the usual constant 0, because it simplifies the exposition) extended by a unary predicate symbol F (denoting the property "being constructible") whose

behavior is described by the following axiom and rules

(1) $\Gamma \to \Delta, F(2)$ — *2 is constructible*

(2) $\dfrac{\Gamma \to \Delta, F(r) \;\; \Pi \to \Lambda, F(t)}{\Gamma, \Pi \to \Delta, \Lambda, F(r * t)}$ — *if r and t are constructible then their product is constructible*

(3) $\dfrac{\Gamma \to \Delta, F(t)}{\Gamma \to \Delta, F(s(t))}$ — *if t is constructible then its successor is constructible*,

where r, t are arbitrary arithmetical terms. To simplify the writing of the arithmetical terms $t * t * \ldots t$, where t occurs n times, we use the shorthand notation $t^{\underline{n}}$. (We shall not be careful here on the insertion of parentheses in arithmetical terms, but the reader can control that our constructions respect the usual restrictions.)

We shall add the exponential function x^y to our language, together with the following substitution rules

$$\frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A|_r^t} \qquad \frac{A, \Gamma \to \Delta}{A|_r^t, \Gamma \to \Delta},$$

where A is an arbitrary formula, and where $A|_r^t$ denotes that the term r occurring in A is substituted by the term t, for t, r having the syntactical form of the pair of terms in the equation $(u^p)^q = u^{p*q}$, $u^2 = u * u$, $2^{\underline{2_{k+1}}} = 2^{2^{\underline{2_k}}}$ or $2^{\underline{2_1}} = 2^2$, where 2_k is the numeral defined inductively as $2_1 = 2$, $2_{n+1} = 2^{2_n}$. The exponential function will be used merely as a notational symbol. In fact, the formula $\forall x \forall y (F(x) \wedge F(y) \supset F(x^y))$ cannot be derived from the calculus. (The reader can verify that the formula is derivable in arithmetic using induction.)

How fast can we assert that a number is constructible without the help of induction? If one wants to show $\to F(s^n(2))$ (where s^n denotes n iterations of the successor function) in $\mathcal{O}(n)$ steps, it is enough to apply rule (3) n times. The sequent $\to F(2^{\underline{n}})$ can also be derived in $\mathcal{O}(n)$ steps by combining n suitable instances of the provable sequent $F(x) \to F(2 * x)$, and the sequent $\to F(2^{\underline{2^n}})$ can be obtained through n combinations of suitable instances of the provable sequent $F(x) \to F(x^{\underline{2}})$. Can we do any better than this? The answer is positive when we allow our lemmas to contain *quantifiers*. A proof of $\to F(2^{\underline{2^{2^n}}})$ needs n combinations of the provable sequent

$$\forall x.\big(F(x) \supset F(x^{\underline{k}})\big) \to \forall x.\Big(F(x) \supset F\Big(x^{\underline{k^2}}\Big)\Big),$$

where k is an arbitrary integer and $x^{\underline{k^2}}$ denotes $(x^{\underline{k}})^{\underline{k}}$. We should observe that a proof of this latter sequent will not depend on k and can be obtained

by a constant number of steps (in Subsection 4.1 we show how this is possible). By combining n times the above implication one derives

$$\forall x.\big(F(x) \supset F(x^{\underline{2}})\big) \to \forall x.\Big(F(x) \supset F\Big(x^{\underline{2^{2^n}}}\Big)\Big)$$

and since $\forall x.(F(x) \supset F(x^{\underline{2}}))$ is provable one infers $\forall x.(F(x) \supset F(x^{\underline{2^{2^n}}}))$, and then $F(2) \supset F(2^{\underline{2^{2^n}}})$ and in particular $\to F(2^{\underline{2^{2^n}}})$.

Can we obtain a proof of $\to F(e(n,2))$ in $\mathcal{O}(n)$ steps, where $e(n,2)$ is $2^{\underline{2^{n-1}}}$ for $n > 1$? The answer is again positive and to do this one need *not* use induction but simply formulas with n nested quantifiers, i.e., a sequence of alternating existential and universal quantifiers.

The idea goes like this. Let us define n new predicates $F_0, \ldots, F_n$ as

$$F_0(x) \equiv F(x)$$
$$F_i(x) \equiv \forall z.F_{i-1}(z) \supset F_{i-1}(z^x).$$

The formulas $F_i(x)$ describe sets of numbers F_i where $F_{i+1} \subset F_i$ and each F_i is closed under exponentiation for powers $x \in F_{i+1}$. It is easy to show that the following properties are provable for each $i = 0 \ldots n$:

(1) $F_i(x), F_i(y) \to F_i(x * y)$
(2) $\to F_i(2)$.

Notice that for each $i > 1$, the sequent $\to F_i(2)$ can be proved with no use of axiom (1) or rules (2), (3). It is only for the provability of $\to F_0(2)$ (i.e., $\to F(2)$) that one needs axiom (1), and for the provability of $\to F_1(2)$ (i.e., $\to \forall z.F(z) \supset F(z^2)$) that one needs rule (2).

Since the sequent

$$F_0(2), F_1(2), \ldots, F_n(2) \to F_0(e(n,2))$$

is provable in $\mathcal{O}(n)$ steps (using the first property above; in Subsection 4.1, we give the details of the proof), we can use the second property to derive $\to F_0(e(n,2))$.

Notice that the whole proof contains just one application of rule (2), and that each lemma $F_i(2)$ contains i nested quantifiers (take for instance $F_2(x)$, rewrite it as $\forall z((\exists w F_0(w) \wedge \neg F_0(w^z)) \vee (\forall w F_0(w^z) \supset F_0(w^{z^x})))$, and notice that it contains 2 nested quantifiers, i.e., a universal quantifiers followed by an existential one).

These examples illustrate how "simple parts" in a proof work together. We used some simple building blocks to show that certain large numbers are constructible and we might wonder whether the interaction of different building blocks generates an interesting extra-structure. In Section 4 we shall show that the logical flow graphs of the proofs of $\to F(2^{\underline{2^{2^n}}})$ and of $\to F(e(n,2))$ contain *cycles*.

Remark 1. The Gentzen Cut Elimination Theorem does not give any information on the way that terms evolve in a proof during the elimination of cuts [Gir87a]. Gentzen's proof relies on a non-obvious induction argument based on the notion of *degree* of a formula (i.e., $d(P) = 0$ if P is atomic; $d(A \wedge B) = d(A \vee B) = d(A \supset B) = sup\{d(A) + 1, d(B) + 1\}$; $d(\neg A) = d(\forall x A) = d(\exists x A) = d(A) + 1$) which does not take care of the terms involved in a proof. On the other hand, the extension of the sequent calculus (with axiom (1) and rules (2) and (3)) that we use in this section traces an explicit link between the operation of elimination of cuts and the construction of terms in a proof. The cut-free proofs of $\rightarrow F(2^{\underline{2^{2^n}}})$ and $\rightarrow F(e(n, 2))$ have roughly 2^{2^n} and 2_n lines, respectively.

Remark 2. In [Gen34] (see also [Gir87a]) it is shown that there is a multi-exponential upper bound on the number of lines of cut-free proofs obtained after cut elimination of proofs in predicate logic. This means that if one defines $f_\alpha : N \rightarrow N$ for ordinals $\alpha \leq \omega$ (where ω is the first infinite ordinal) inductively by $f_1(s) = 2 * s$, $f_{n+1} = f_n^{(s)}(s)$ (where $f_n^{(s)}$ denotes the s-fold iterate of f_n) and $f_\omega(s) = f_s(s)$, then the upper bound is f_3. As a consequence we have that even if we had considered a base function which is different than *multiplication* in our constructions, say a function g growing as fast as f_i, we would nevertheless be able to build in $\mathcal{O}(n)$ steps only terms whose value would be at most $f_{i+2}(n)$.

Remark 3. Can we give an estimate of how many numbers m can be proved to be constructible in n lines? An upper bound to this number of m's can be derived from the upper-bound on the number of lines of cut-free proofs which we discussed in Remark 2: any proof of n lines can be transformed into a cut-free proof of at most $c \cdot 2_n$ lines, for some $c > 0$. We claim that the number of m's is roughly bounded by 2_{n+1}.

First, let us observe that a number m might have several representations in the language of arithmetic (i.e., in terms of the symbols $2, s, *$). Take for instance the number 90 which can be represented as $s^{90}(0)$ (i.e., the successor function is applied 90 times) but also as $s^2(0) * s^5(0) * s^3(0) * s^3(0)$. All terms representing m or values larger than m in the language of arithmetic should have at least $b \log m$ symbols, for some constant $b > 0$. This is not hard to check since multiplication is the most efficient operation making large numbers.

Second, notice that the number of lines of a cut-free proof of $\rightarrow F(m)$ will depend on the syntactical form of the arithmetical term representing m and it will correspond to the number of symbols of the term. In fact, each occurrence of the constant 2 in the term will correspond to the presence of axiom (1) in the proof, each operation of successor will correspond to an application of rule (3), and each operation of multiplication will correspond to the application of rule (2). Since we can always transform a proof of n

lines into a cut-free proof of at most 2_n lines (roughly), it is clear that we cannot possibly construct in n lines a term which contains more than 2_n symbols. By combining the two observations we derive the claim.

Nevertheless, one would expect the number of m's to be bounded by a function which grows much slower than 2_{n+1}. Unfortunately, a satisfactory answer coming from proof theory is not straightforward. The reason is twofold: the size of logical terms in proofs (with cuts) cannot be bounded by the number of lines n of the proof, and the problem of substitution of terms in proofs can be reduced to the second-order unification problem which is known to be undecidable [Gol81]. (References related to undecidability questions on the number of lines in proofs are [Bus91, KP88].)

3. DISTORTION IN GROUPS

We present a few examples with the aim to illustrate the notion of distortion for finitely presented groups. We take them from [Gro93] where the notion and its Riemannian counterpart are amply discussed and many examples are given. The examples we have chosen will be used later in our discussion.

Let G be a finitely generated group and E be its finite generating set. Define the *length function* $l(g)$ of $g \in G$ as the minimum length of a representation of g as a product of elements in $E \cup E^{-1}$ (this notion appears in the geometric framework in [Schw55, Mil68]). We define the *distance* between two elements $g_1, g_2 \in G$ to be $l(g_1^{-1} g_2)$.

Consider an embedding between finitely generated groups $G_0 \subset G$, such that the generating set of G_0 includes into that of G. Then clearly

$$l_{G_0}(w) \geq l_G(w) \qquad \text{for all } w \in G_0$$

and we want to understand by how much l_{G_0} is greater than $l_G|G_0$. If there is a constant C such that

$$l_{G_0}(w_1^{-1} w_2) \leq C \cdot l_G(w_1^{-1} w_2)$$

for any pair of words w_1, w_2 in G_0, then the distortion is *linear* (the constant C is the *Lipschitz* constant). (Reference [Gro93] calls it *bounded* distortion.) For example, if G is a free group or a free abelian group, then the distortion is linear for every $G_0 \subset G$.

In the sequel we will be interested in studying the distortion of cyclic subgroups G_0 generated by a single element $g \in G$. We will say that the subgroup $\{g^i\}$ has *linear* distortion in G if

$$l(g^i) \geq C \cdot i$$

for some constant $C > 0$. We say that the subgroup $\{g^i\}$ has (at most) *polynomial* distortion if

$$l(g^i) \geq C \cdot i^\alpha$$

for some constants $C > 0, 0 < \alpha \leq 1$. It has *exponential* distortion if

$$C \cdot \log(i) \leq l(g^i) \leq D \cdot \log(i) \qquad \text{for all } i$$

for some positive constants C, D.

The definition of *double exponential* distortion is a bit more delicate. This is because the relation $l(g^i) \leq C \cdot loglog(i)$, for some constant $C > 0$, cannot hold for all i as this would give more than an exponential number k^i of words of length i on an alphabet of k letters. We say that the distortion is double exponential when

$$l(g^i) \leq D \cdot \log\log(i) \qquad \text{for infinitely many } i$$

and

$$C \cdot \log\log(i) \leq l(g^i) \qquad \text{for all } i$$

for some positive constants C, D.

Analogously, we speak about *multi-exponential* distortion once we replace the logarithm by the iterated logarithmic function. Again, we shall be able to observe the distortion with respect to *some* value i, for the same reasons we discussed above. When the distortion is multi-exponential, we will also say that the subgroup $\{g^i\}$ is *strongly distorted*.

Let us now introduce the examples we anticipated at the beginning of the section.

Let $G = \{a, b | a^b = a^2\}$ where the symbol a^b denotes the word bab^{-1}. The minimal word length of a^{2^n} (in the letters a, b) satisfies the inequality $l(a^{2^n}) \leq 2n + 1$. In particular, since $(a^m)^b = a^{2m}$ for all $m = 1, 2, \ldots$ the length function satisfies $l(a^{2m}) \leq l(a^m) + 2$, which implies $l(a^m) \leq C \cdot log(m)$ for all m (where C is some constant value). This relation makes the distortion *exponential*. The group G belongs to the family of Baumslag–Solitar groups $BS_{l,m} = \{b, c \mid cb^l c^{-1} = b^m\}$, where l, m are positive integers [BS62]. All groups $BS_{l,m}$ are seen to have exponential distortion with a similar argument.

Let us consider another distorted group G defined as $\{a, b, c | a^b = a^2, b^c = b^2\}$. The length function here satisfies the inequality

$$l\left(a^{2^{2^n}}\right) \leq 4n + 3$$

which makes the distortion *double exponential*. Notice that the relation $l(a^m) \leq \log\log(m)$ does not hold for all m because there are only 3^m words of length m on an alphabet of 3 letters.

Let G be the group $\{a, b, c | a^b = a^2, a^c = b\}$. Since $a^{(a^n)^c} = a^{2^n}$, the length function satisfies the inequality

$$l\left(a^{2^n}\right) \leq 2 \cdot l(a^n) + 5$$

which makes the distortion of the cyclic subgroup $\{a^i\} \subset G$ to be multi-exponential. It is important to notice here that the whole action takes place in the subgroup $G' = \{a, c | a^{a^c} = a^2\}$ which was considered by Gersten along with the groups $Gerst^{(i)} = \{a, c | a^{w_i} = a^2\}$ for $w_1 = a^c$, $w_2 = a^{a^c}$, and so on [Ger93]. All these groups have multi-exponential distortion and they form the only known examples of 1-relator groups with such a property. It is an open question whether one might have stronger forms of distortion for 1-relator groups. (In Section 7 we shall come back to this point.)

To conclude, let us mention that there are finitely presented groups with a cyclic subgroup $\{g^i\}$ that presents a distortion which grows faster than any recursive function. Once more, the distortion appears on *some* of the values i. Examples can be found in [Gro93].

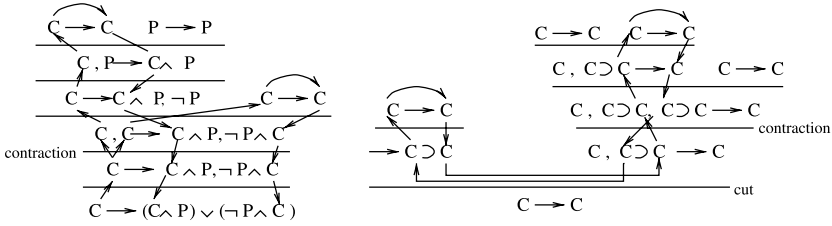
The phenomena described in this section are reminiscent of the ones discussed in Subsection 2.1. We will show that this is more than an analogy. In fact, in Section 6 we will find group relations in the structure of proofs of large numbers and we will be able to associate finitely presented groups with distortion to these proofs.

4. LOGICAL GRAPHS AND CYCLES

The *analytical* approach to the study of formal proofs, which divides a proof into building blocks and analyses the blocks separately with little regard on how these blocks fit together, has failed: by "cutting up" it destroys the dynamics within proofs. This important point has been emphasized by Girard who, in 1987, introduced *proof nets* to study proofs as *global* entities [Gir87] where formulas interact in a proof through logical connectives [Gir89a, Gir89b, Gir95]. In 1991, another notion of graph associated to proofs was introduced by Buss [Bus91] for different purposes (namely, to prove that given a positive integer k, one cannot decide whether a formula has a proof of length at most k or not). This graph, called *logical flow graph*, traces the flow of occurrences of formulas in a proof. It was employed in [Car97, Car98, Car97b, Car97c] to study the dynamics within proofs which arises from the duplication and the identification of formulas in a proof.

We illustrate the notion of a logical flow graph through an example. A formal definition together with an informal discussion of some of its properties follow (see also Bus91, Car97]). We consider two formal proofs

(formalized in the language of propositional logic) and the sequences of edges that one can trace through them



The arrows indicated in the figures represent only *some* of the links between formulas: for each application of a rule, there is an edge between an occurrence of C in the upper sequent(s) and the corresponding occurrence of C in the lower sequent of the rule. (The correspondence between formula occurrences is induced by the rule in the obvious way.) There is a horizontal edge from the antecedent to the consequent of the axioms $C \to C$, and there are horizontal edges between occurrences of C lying in cut-formulas. Similar links are present for the occurrences P and also for formulas which are logically more complicated, as $C \wedge P$, $\neg P$, $\neg P \wedge C$, and $(C \wedge P) \vee (\neg P \wedge C)$. For instance, we will say that there is a path from the occurrence $C \wedge P$ in the second line of the proof on the left, which goes down until the end-sequent. As a result of these links, different occurrences of a formula in a proof might be logically linked even if their position in the proof is apparently very far apart. The graph that we obtain is in general disconnected and each connected component corresponds to a different formula in the proof.

While it is not so satisfactory to prove the tautologies above, the structure of the proof on the left is interesting because it shows that paths in a proof can get together through contraction of formulas (in fact, this is the only rule of the sequent calculus that allows the branching), and the structure on the right shows that cyclic paths might be formed.

Let us now describe in detail the formal definition of a *logical flow graph*. We recall first that, given two formulas A and B, by counting 1 for each time B occurs in the scope of a negation in A and 1 for each time B occurs on the left side of an implication in A, the formula B is said to occur *positively (negatively) in the formula* A if the sum is even (odd). A formula B occurs *positively (negatively) in a sequent* $\Gamma \to \Delta$ if B occurs negatively (positively) in a formula of Γ or positively (negatively) in a formula of Δ. From now on, we shall intend a positive or negative occurrence of a formula to be defined relatively to sequents.

For each axiom $A, \Gamma \to \Delta, A$, we trace an edge, called the *axiom-edge*, from any negative occurrence of B in one of the A's to the corresponding positive occurrence of B in the other A.

For each rule, we trace an edge between any positive occurrence of a formula B in the upper sequent(s) of the rule and the corresponding occurrence of B in the lower sequent of the rule. Similarly, we trace an edge between any negative occurrence of a formula B in the lower sequent of the rule and the corresponding occurrence of B in the upper sequent(s) of the rule.

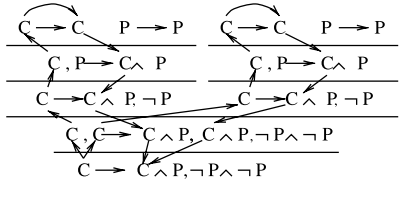
If the rule is a contraction, then there are two edges going to (coming from) the negative (positive) occurrences of B in the contraction formulas and coming from (going to) the relative occurrence of B in the main formula.

In the case of a cut rule applied to sequents $\Gamma_1 \to \Delta_1, A$ and $A, \Gamma_2 \to \Delta_2$, edges, called *cut-edges*, are traced between the two cut-formulas A as follows: for any subformula B of A occurring positively (negatively) in $\Gamma_1 \to \Delta_1, A$, there is an edge going from (coming to) it to (from) the correspondent occurrence of B in A of $A, \Gamma_2 \to \Delta_2$.

This concludes the definition of the edges of the graph. We say that the *logical flow graph* of a proof Π is the directed graph which we can read off the proof, whose nodes are labelled by the occurrences of formulas in Π, and whose edges are the links induced by the axioms and the rules of Π, as defined above.

The logical flow graph carries a natural orientation [Car97]: negative occurrences in a sequent have edges going up in the proof and positive occurrences have edges going down; negative occurrences are linked to positive ones through axioms, and positive occurrences are linked to negative through cuts.

The logical flow graph of a proof might contain both *oriented* and *non-oriented* cycles. The first are defined as sequences of directed edges starting and ending in the same point. An example is illustrated in the proof on the right hand side given above. More complicated cyclic structures arise in the proofs of constructibility of large numbers presented in Subsection 2.1. We shall describe these structures in Subsection 4.1. Non-oriented cycles arise by combinations of oriented paths which have the same initial and ending points. Here is a concrete example



where two paths depart from the negative occurrence of C in the end-sequent, to recombine in a positive occurrence of C and to form a non-oriented cycle. In the sequel we call a *bridge* any maximal oriented path

that starts from a negative occurrence, ends in a positive occurrence, and does not traverse cut-edges. The maximality condition implies that both the starting and ending occurrences of a bridge should lie either in a cut-formula or in the end-sequent of the proof. A nice example of non-oriented cycles in proofs is given by the cut-free proofs of the pigeon hole principle PHP_n. These proofs are exponentially large [Hak85] and contain an exponential number of bridges between some pair of formula occurrences in the end-sequent of the proof. The combinations of these paths give rise to an exponential number of non-oriented cycles.

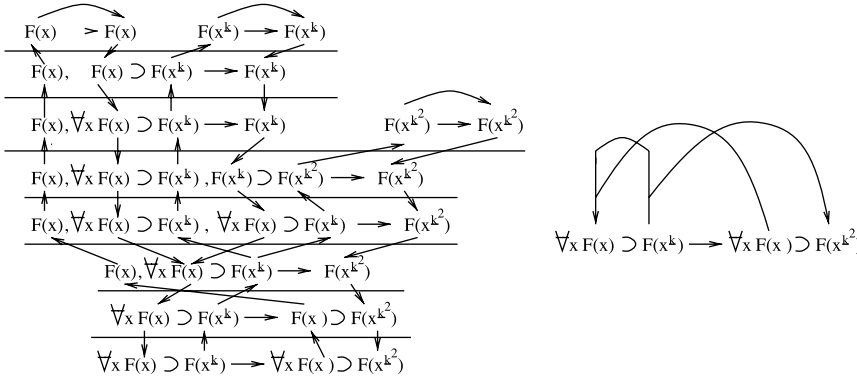
4.1. *Cycles in Short Proofs*

The two constructions proposed in Subsection 2.1 for proving $\rightarrow F(2^{\underline{2^{2^n}}})$ and $\rightarrow F(e(n,2))$ in $\mathcal{O}(n)$ lines present oriented cycles in their logical flow graph. In fact, *all* proofs of these sequents which have a number of lines that is *linear* in n display oriented cycles [Car98]. In this section we shall describe how these cycles arise.

The first construction, which proves $\rightarrow F(2^{\underline{2^{2^n}}})$, glues together proofs of the sequent

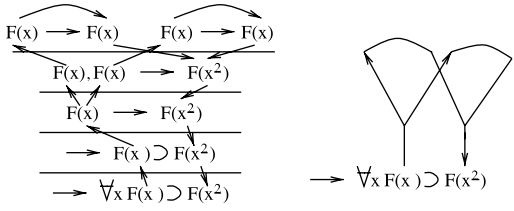
$$\forall x.\left(F(x) \supset F\left(x^{\underline{k}}\right)\right) \rightarrow \forall x.\left(F(x) \supset F\left(x^{\underline{k^2}}\right)\right) \tag{1}$$

for $k = 2, 2^2, 2^{2^2}, 2^{2^3}, \ldots, 2^{2^{n-1}}$. This sequent is provable in a constant number of lines, independent by k. In the left diagram below, we display the formal proof together with the logical paths associated to the proof, and on the right, we display a schema of the paths linking the formulas in the end-sequent of the proof

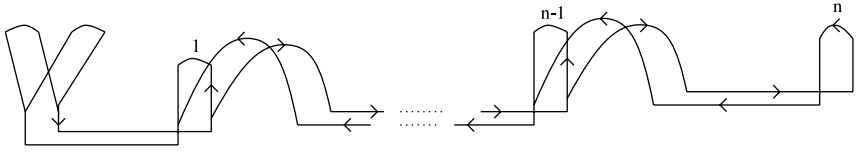


By gluing together (through cuts) a chain of these proofs (for different values of k), together with a proof of the sequent $\forall x.(F(x) \supset F(x^{\underline{2^{2^{n-1}}}})) \rightarrow F(2) \supset F(2^{\underline{2^{2^n}}})$ (which can be obtained as above, with x

replaced by 2, $x^{\underline{k}}$ by $2^{\underline{2^{n-1}}}$ and $x^{\underline{k^2}}$ by $2^{\underline{2^n}}$), and the following proof of $\rightarrow \forall x.F(x) \supset F(x^{\underline{2}})$

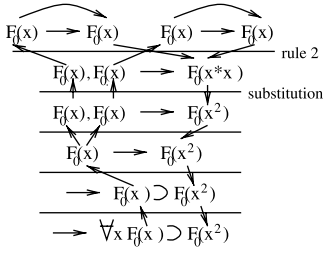


we obtain a proof of the sequent $\rightarrow F(2) \supset F(2^{\underline{2^n}})$ whose logical flow graph contains a linear cascade of cycles that looks as

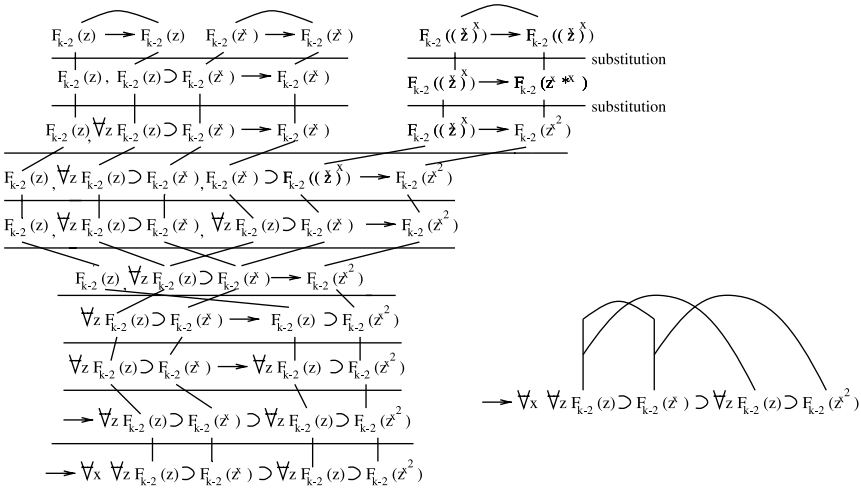


To conclude the proof, one needs to combine $\rightarrow F(2) \supset F(2^{\underline{2^n}})$ with the provable sequent $\rightarrow F(2)$ and to derive $\rightarrow F(2^{\underline{2^n}})$ as wished.

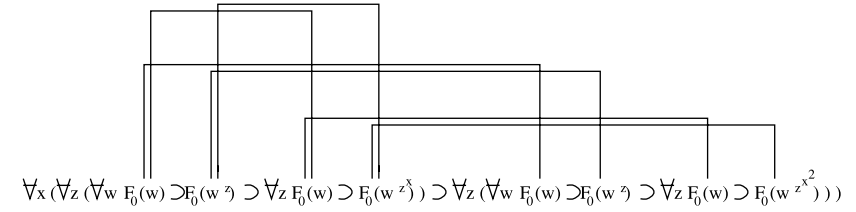
The second construction, relative to the proof of the sequent $\rightarrow F(e(n,2))$, presents a cyclic structure which is much more intriguing. The idea is to glue together a proof of $F_0(2), F_1(2), \ldots, F_n(0) \rightarrow F_0(e(n,2))$ with the proofs of $\rightarrow F_k(2)$ for $k = 0, \ldots n$. (We remind the reader that the notation $F_k(t)$ is used here to shorten the writing of formulas which contain 2^k occurrences of the atomic formula $F_0(s)$, for some term s; the expanded form would take too much space to be written.) The sequent $\rightarrow F_0(2)$ is axiom (1), the sequent $\rightarrow F_1(2)$ is provable as



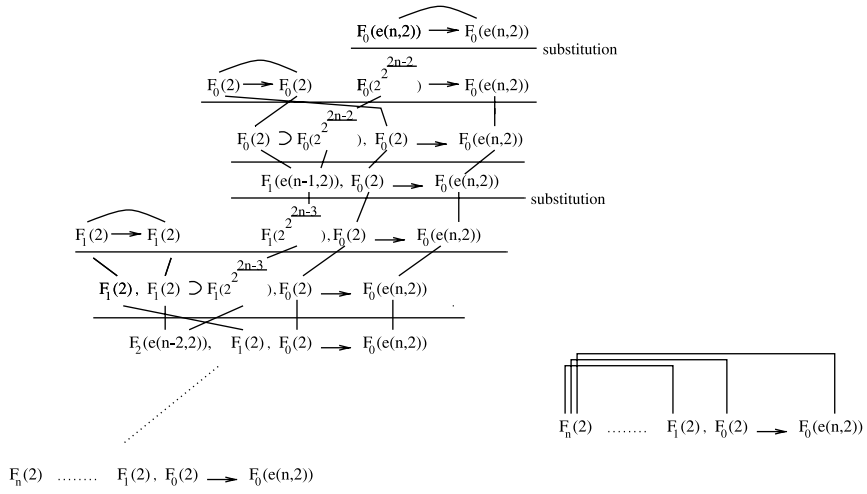
and the sequents $\rightarrow F_k(2)$ for $k = 2, \ldots, n$ are provable in a constant number of lines as



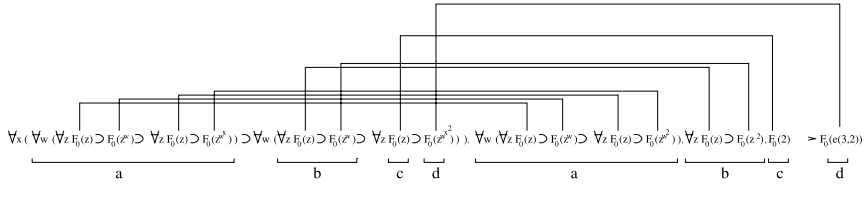
where $\forall x(\forall z F_{k-2}(z) \supset F_{k-2}(z^x)) \supset (\forall z F_{k-2}(z) \supset F_{k-2}(z^{x^2}))$ is $F_k(2)$ (since we can rewrite it as $\forall x F_{k-1}(x) \supset F_{k-1}(x^2)$, that by definition is $F_k(2)$). Also, notice that the logical paths indicated in the figure correspond to *bundles* of logical paths passing through atomic formulas of the form $F_0(s)$ (for some term s) by definition of F_k. In the case $k = 3$ for instance, the bundle of paths is illustrated below



The formal proof of $F_0(2), F_1(2), \ldots, F_n(0) \to F(e(n,2))$ has the structure



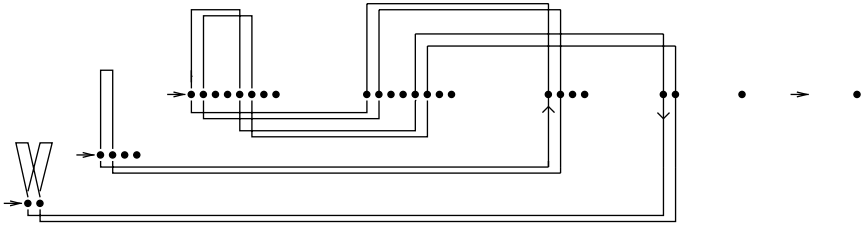
where $F_0(e(n,2))$ and the formulas $F_k(2)$, for $k = 0, \ldots, n-1$, of the end-sequent are linked through a bundle of logical paths to some subformula of $F_n(2)$ (as illustrated on the right hand side in the schema above). The reader can check that the formula $F_n(2)$ which denotes $\forall z F_{n-1}(z) \supset F_{n-1}(z^2)$ has a bundle of paths linking the atomic subformulas of $F_{n-1}(z)$ to the occurrence $F_{n-1}(2)$, and a bundle of paths linking $F_{n-1}(z^2)$ to $F_{n-2}(2), \ldots, F_0(2)$ and $F_0(e(n,2))$. More precisely, the formula $F_{n-1}(z^2)$ which denotes the formula $\forall w F_{n-1}(w) \supset F_{n-1}(w^{z^2})$ has a bundle of paths linking the atomic subformulas of $F_{n-1}(w)$ to the occurrence $F_{n-2}(2)$, and a bundle of paths linking $F_{n-1}(w^{z^2})$ to $F_{n-3}(2), \ldots F_0(2), F_0(e(n,2))$. This recursive pattern holds for all $k < n$. Let us see this fact in the case $n = 3$,



where we denote a, b, c, d as the bundles of paths formed by the proof.

By gluing together (through cuts) the proofs that we have described above, several cycles might arise. In particular, there is a cycle that visits the whole proof. It goes back and forth from the proofs of $\to F_k(2)$ for $k = 1, \ldots n$, and the proof of $F_0(2), F_1(2), \ldots, F_n(2) \to F(e(n,2))$. We can

see this for the case $n = 3$

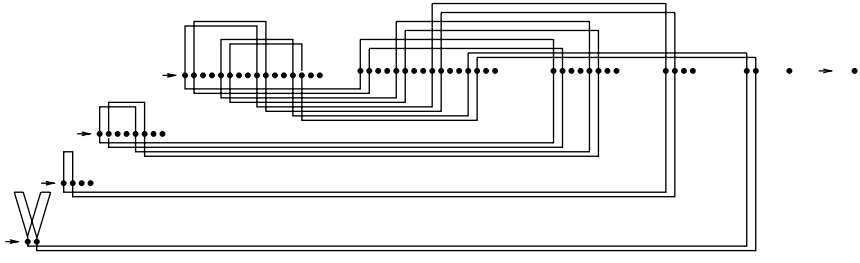


where the dots represent atomic formulas in the end-sequents of the proofs. The list of dots on the right represents all atomic occurrences in the sequent

$$F_3(2), F_2(2), F_1(2), F_0(2) \to F_0(e_2(3, 2))$$

and the three lists of dots on the left represent the atomic occurrences in the sequents $\to F_3(2), \to F_2(2), \to F_1(2)$ when one reads them from top to bottom.

For the case $n = 4$, the cyclic structure is already more complicated



For $n > 4$, the reader can figure out how this cycle looks like. In the following we shall try to make sense of these complicated structures of logical flow graphs.

5. LOGICAL GRAPHS EMBEDDED IN THE PLANE

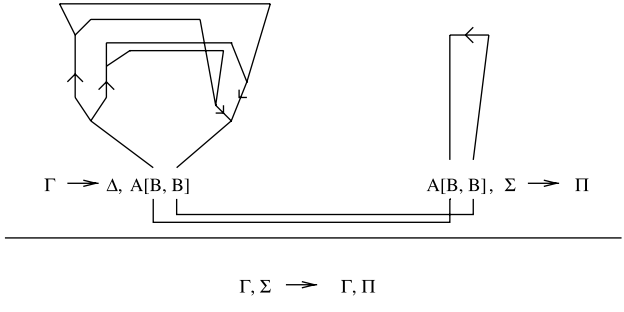
In purely combinatorial terms, the graphs of proofs that we consider are oriented graphs *embedded* in the plane with possible crossing of edges and they are equipped with some extra information: we shall think at the cut-edges and at the branching nodes corresponding to the applications of rule (2) as carrying *special* information. The information coming from logical rules will not play any role. (In topology an *embedding* does not allow double points while our graphs are similar to knot diagrams as it was pointed out by the referee.)

The embedding of the graph in the plane associates a *direction* to the paths which go either "up" or "down" by means of vertical edges, and turn either "from left to right" or "from right to left" by means of horizontal edges. It also associates a *height* to each one of the nodes in the obvious way: the height of a node in the graph corresponds to the height of the sequent in the proof to which the node belongs. (We recall that $h(S) = 1$ if S is an axiom; $h(S) = max\{h(S_1), h(S_2)\} + 1$, if S is a sequent obtained by applying a binary rule to the sequents S_1, S_2; $h(S) = h(S_1) + 1$ if S is a sequent obtained by applying a unary rule to the sequent S_1.)

This is the only information coming from a proof that we need to consider in the analysis of Section 6. Strictly speaking, the embedding of the graph in the plane allows us to distinguish cut-edges from bridges, to determine the "degree of multiplicity" of a bridge (this notion will be formally introduced in Definition 4), to determine whether a path is a bridge or not, which are its starting and ending points, and whether the starting point lies on the left or on the right of its ending point.

5.1. *Oriented Cycles*

We are interested in *oriented* cycles and from now on we refer to them simply as "cycles." We describe them as sequences of *bridges* and *cut-edges*. For instance the cycle given at the beginning of Section 4 will be regarded as being composed by a bridge followed by a cut-edge followed by a bridge which is followed by a cut-edge. This is an easy example but the structure of proofs might be more complicated and cycles might be nested. Suppose that several bridges start and end at the same pair of formula occurrences in a proof and that this pair of formulas belongs to a cyclic path in the proof.



This means that each one of the bridges helps to form a distinct cycle in the proof. In the illustration above, four different bridges are nested on the left hand side of the proof; they start and end in the same pair of formula occurrences B lying in the cut-formula A (the B's are sub-formulas of A) of

the sequent $\Gamma \to \Delta, A[B, B]$. They help to form four distinct cycles which pass through the bridge on the right hand side of the proof.

The nesting of bridges takes place by means of the contraction rule (applied to *positive* as well as to *negative* occurrences of formulas) and rule (2) (applied to *positive* formula occurrences). (These are the only rules that can bring together and split apart distinct paths.)

DEFINITION 4. A *bridge of multiplicity k* is a nesting of k distinct bridges which is formed by means of the contraction rule applied to *negative* occurrences and rule (2) applied to *positive* occurrences.

Suppose that the three branching points on the left of the above picture correspond to contraction rules and the three branching points on the right correspond to the application of rule (2). Then we say that there is "a bridge of multiplicity 4" passing through the two occurrences of B in A.

The notion of multiplicity takes into account only those bridges whose nesting is obtained by applying rule (2) to *positive* occurrences and ignores nesting realized by *contractions* on positive occurrences. Technically speaking we will consider only cycles passing through bridges with multiplicity k strictly greater than 1 and this choice enables us to study the effect of multiplication in the construction of terms in proofs.

DEFINITION 5. A *simple cycle* is a graph which is formed by an oriented sequence of consecutive cut-edges and bridges (possibly with non-trivial multiplicity) that starts from a point and comes back to it without passing twice through the same bridge or the same cut-edge.

If all the bridges forming a simple cycle have multiplicity 1, then the notion coincides with the usual notion of "loop" in graph theory. The cyclic structure illustrated in the picture above shows a simple cycle formed by a bridge of multiplicity 4.

Notice that simple cycles might be *nested*, i.e. they might share a bridge or a cut-edge. Examples of these structures are easy to build through the use of contractions on *positive* occurrences (as we observed above these contractions are *not* considered in Definition 4). A concrete example is presented in Subsection 4.1 where the first construction generates a cascade of nested cycles sharing a bridge of multiplicity 2.

Given a proof, we are interested in *families* of simple cycles which *share* a bridge. It is clear that a proof might contain several families of nested simple cycles and that these families are uniquely defined. In particular, the same simple cycle might belong to different families.

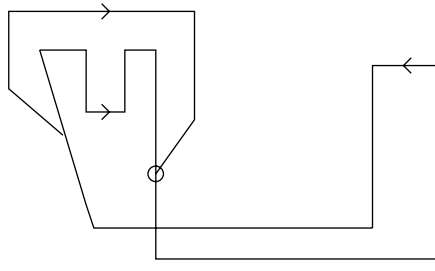
Given one of these families, one can define a *partition* by asking that two simple cycles S_1, S_2 belong to the same partition class if and only if the number of bridges with multiplicity k lying in S_1 is the same as the number of bridges with multiplicity k lying in S_2, for all $k > 1$. We say that a

representative of a partition class is a simple cycle in the class with the largest number of cut-edges. Since there might be more than one representative for a given partition class, we assume that exactly one is chosen for each class.

DEFINITION 6. A simple cycle is called *special* in the proof Π if it is the representative of the partition of some family of nested simple cycles in Π and if it contains a bridge of non-trivial multiplicity.

In Section 6 we shall be interested only in special cycles.

Remark 7. The notions of bridge with non-trivial multiplicity and special cycle fulfill the purposes of this paper but they are not sufficient to capture the rich structure of paths in the whole space of formal proofs. Namely, one needs to consider *all* possible forms of nesting of paths and cycles. Our definitions achieve their goal in Section 6 and remain sufficiently transparent, but a general theory of *growth* for proofs ("growth" here refers to the size of the proof, to the computation time of cut elimination, or to the size of the terms in a proof) requires more flexible notions: the definition of "non-trivial multiplicity," for instance, should not apply only to bridges but to more complicated structures of paths. Consider the following cycle

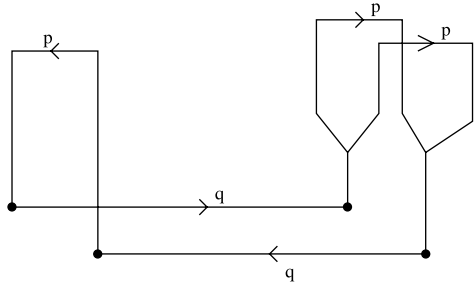


where the branching node marked in the figure corresponds to the application of rule (2). One would like to capture the "multiplicity" of the *pair* of paths on the left, where one of them is a bridge but the other is not.

Remark 8. A cycle in a propositional proof can be eliminated with at most a quadratic expansion in the number of lines of the original proof. In particular, if a proof contains n cycles then there is an acyclic proof of the same statement where the number of lines is polynomially bounded by the number of lines of the original proof, where the polynomial is of degree $n + 1$. This was proved in [Car97c]. Taking into account this fact, the machinery developed in this article is mostly useful in the analysis of growth in proofs *with quantifiers*. A combinatorial model explaining the exponential growth of the cut elimination procedure for propositional proofs is presented in [CS97a, Car97b].

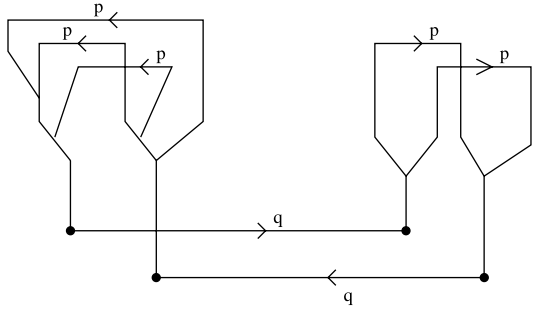
5.2. *Signs and Words*

The geometry of simple cycles can be described through *words*. We illustrate this idea with an example. Let us assign a "label" to bridges, say p, and a different "label" to cut-edges, say q, and let us consider the following simple cycle which might appear as a substructure of some proof



We can read the above cycle, by following the clockwise orientation, as the word p^2qpq, where p^2 corresponds to the fact that the label p appears with *multiplicity* 2 on the right-hand side of the picture.

While going along a cycle, we might pass through *several* bridges of non-trivial multiplicity (for an example of a formal proof where this situation occurs, see Remark 19). Each time this happens, we register the multiplicity of the bridge in our word through an appropriate composition of labels. For instance the following simple cycle



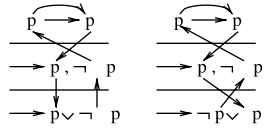
gives rise to the word p^2qp^3q.

A careful labelling of bridges and cut-edges allows us to describe the geometry of cyclic paths in an unambiguous way. Let b, c, b^{-1}, c^{-1} be four labels. Bridges are associated to either b or b^{-1}, and cut-edges are associated to either c or c^{-1}. The choice will depend on the geometry of the cycles.

First let us define the *sign of a bridge*. It is important to think of the logical graph as lying in the plane. Bridges might start and end in occurrences of

formulas with different height, say h_s, h_e. To assign the sign to a bridge we look at the pair of nodes in the bridge which have height $\min\{h_s, h_e\}$. (It is clear that at least one of the nodes in the pair is either the starting point or the ending point of the bridge. If $h_s = h_e$ then the points in the pair are exactly the starting and ending points of the bridge.) If $\min\{h_s, h_e\} = h_s$ (h_e) then we call *negative* (*positive*) the starting (ending) point of the bridge and *positive* (*negative*) the second node of the pair. Notice that the position of the pair of nodes is uniquely determined by the embedding of the graph in the plane.

We define the *sign of a bridge* with respect to the position of the pair of nodes as follows: whenever the negative point of the pair lies to the left of the positive point we assign to the bridge a *positive* sign. Similarly, if the negative point lies on the right of the positive point then we assign a *negative* sign. Take for instance the following example



where the proof on the left has a bridge of *negative* sign while the one on the right has a bridge of *positive* sign.

We are now ready to assign labellings to bridges and cut-edges. We assign the label b to bridges with positive sign and the label b^{-1} to bridges with negative sign. We assign c to cut-edges going from left to right, and c^{-1} to those going from right to left. A *word*, made out of labels b, c, b^{-1}, c^{-1}, is read by going around a simple cycle *clockwise*. As illustrated at the beginning of this section, one reads one after the other the edges that are encountered.

Remark 9. It is clear from the definition of sign that any bridge of multiplicity k is formed by k nested bridges with the same sign (this is because the sign of the bridge depends only on the position of the pair of nodes associated to it, and at least one of these nodes is an extreme of the bridge). Denoting such a bridge as the kth "power" of some "label" (i.e., either b or b^{-1}) is therefore consistent with our previous assumption: a bridge of multiplicity k is denoted b^k if its sign is positive, and b^{-k} if its sign is negative.

6. BRIDGE GROUPS AND ASYMPTOTIC EXPANSION

In this section, families of finitely presented groups on two generators b, c are associated to families of proofs. Here, as in Section 4, the labels b, b^{-1} are assigned to bridges and the labels c, c^{-1} to cut-edges. Both b, c

are thought of as generators of some group and the labels b^{-1}, c^{-1} to be their respective inverses.

DEFINITION 10. Let Π be a proof and A be an atomic formula in Π. The *bridge group* $G(\Pi, A)$ associated to Π, A is the finitely presented group of the form

$$\{b, c \mid w_1 = 1, \dots w_m = 1\},$$

where $w_1, \dots w_m$ are the words read out from the special cycles (see Definition 6) of Π that correspond to the atomic formula A.

If Π does not contain special cycles and A corresponds to a connected component of the logical graph formed by cut-edges, then the bridge group $G(\Pi, A)$ is the *free* group in *two* generators $F(b, c)$. If A corresponds to a connected component which is not formed by cut-edges, then $G(\Pi, A)$ is the *free* group in *one* generator $F(b)$. If the logical graph of Π is connected then there is only one bridge group associated to Π and we denote it $G(\Pi)$.

DEFINITION 11. A family $\{G_n\}_{n=1}^{\infty}$ of finitely presented groups is called *uniform* if the following conditions are satisfied

(1) all G_n's have a common set of generators $\{a_1, \dots, a_m\}$;

(2) the number of relations $R_1^n, \dots, R_{k_n}^n$ representing the G_n's grows linearly;

(3) there is a positive constant C such that for all n, the group G_{n+1} is represented by relations R_p^{n+1} of the form

$$z_1^{\epsilon_1} \dots z_r^{\epsilon_r} = 1,$$

where $r \leq C, \epsilon_i = \pm 1$, and z_i is either one of the generators a_l, or one of the words $w_{n+1,j}$ in the set S_{n+1}. The set S_{n+1} is defined inductively as follows: S_1 is the set of generators $\{a_1, \dots, a_m\}$, and S_{n+1} consists of the words of the form

$$s_1^{\delta_1} \dots s_k^{\delta_k},$$

where $k \leq C, \delta_i = \pm 1$, and s_i is either one of the generators a_l, or one of the words $w_{n,j} \in S_n$. The set S_{n+1} is minimal in the sense that all words in it must be used to define the relations representing G_{n+1}.

An example of uniform family of groups is Gersten's family [Ger93]

$$Gerst^{(n)} = \{a, b | a^{w_n} = a^2\} \qquad \text{with } w_n = a^{a^{a^{\cdot^{\cdot^{\cdot^{a^b}}}}}},$$

where w_n is defined by n iterations of a. We have already encountered this family in Section 3. To see that this family is uniform we simply need to

observe that the relation defining $Gerst^{(n+1)}$ is of the form $a^{w_{n+1}}a^{-1}a^{-1} = 1$ where $w_{n+1} = a^{w_n}$ and notice that for $C = 5$ the conditions of Definition 11 are satisfied. In fact, for all n and $C = 5$, we have $w_n \in S_n$. This is easily seen by induction. If $n = 1$, then w_1 is bab^{-1} and with 2 multiplications we have $bab^{-1} \in S_1$; if $n > 1$ then observe that w_{n+1} is equal to $w_n a(w_n)^{-1}$ and that by induction $w_n \in S_n$. Again we see that 2 multiplications are sufficient to build w_{n+1} out of the words in S_n and this establishes the uniformity of Gersten's family.

We are now ready to *compute* the bridge groups of the two families of proofs introduced in Subsection 2.1.

THEOREM 12. *Let* $\{\Pi_n :\rightarrow F(2^{\underline{2^{2^n}}})\}_{n=1}^{\infty}$ *be the family of proofs of* $\mathcal{O}(n)$ *lines introduced in Subsection* 2.1. *Then the bridge group* $G(\Pi_n)$ *is*

$$BS_*^{(n)} = \{b, c | b^2 = b^{w_n}\},$$

where $w_1 = c, w_2 = cbc, w_3 = cbcbc$, *and so on. The family* $\{G(\Pi_n)\}_{i=1}^{\infty}$ *is uniform, and moreover, there is a monomorphism*

$$BS_{1,2} \rightarrow G(\Pi_n)$$

from the Baumslag–Solitar group $BS_{1,2}$ *into every bridge group* $G(\Pi_n)$.

THEOREM 13. *Let* $\{\Pi_n :\rightarrow F(e(n, 2))\}_{n=1}^{\infty}$ *be the family of proofs of* $\mathcal{O}(n)$ *lines introduced in Subsection* 2.1. *Then the bridge group* $G(\Pi_n)$, *for* $n \geq 4$, *is*

$$Gerst_*^{(n-3)} = \{b, c \mid b^2 = b^{w^*_{n-3}}\},$$

where $w_1^* = b^d, w_2^* = b^{b^d}, w_3^* = b^{b^{b^d}}$ *and so on,* $d = (b^{a^{-1}})^{-1}$ *and* $a = b^c$. *The family* $\{G(\Pi_n)\}_{i=4}^{\infty}$ *is uniform.*

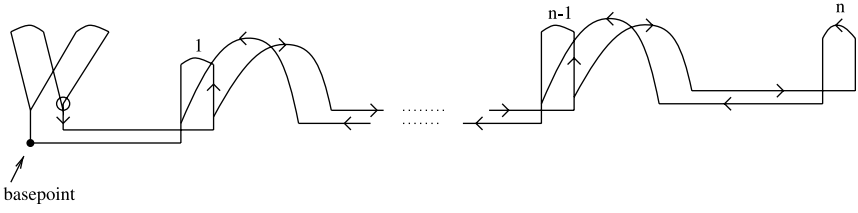
The proofs of Theorems 12 and 13 will be based on a careful analysis of the geometrical structure of the families of proofs of $\rightarrow F(2^{\underline{2^{2^n}}})$ and of $\rightarrow F(e(n, 2))$. These proofs contain simple cycles formed by bridges of multiplicity 2. More precisely, these cycles pass through the intermediate sequents $\rightarrow \forall x.(F(x) \supset F(x^{\underline{2}}))$ and $\rightarrow \forall x.(F(x) \supset F(x^2))$ (that is, $\rightarrow \forall x.(F_0(x) \supset F_0(x^2))$), respectively. These sequents are proved by combining (through rule 2) two identical axioms of the form $F(a) \rightarrow F(a)$ to obtain the sequent $F(a), F(a) \rightarrow F(a^2)$. A contraction on the left applied to this sequent will then give the sequent $F(a) \rightarrow F(a^{\underline{2}})$ from which $\rightarrow \forall x.(F(x) \supset F(x^{\underline{2}}))$ and $\rightarrow \forall x.(F(x) \supset F(x^2))$ are easily derived. The important point here is to observe that a path starting at the negative occurrence $F(x)$ in $\rightarrow \forall x.(F(x) \supset F(x^{\underline{2}}))$ splits into two distinguished paths at the contraction point. These paths, after passing through the pair of distinguished axioms, will join again with rule (2) to

end-up into the positive occurrence $F(x^{\underline{2}})$. (A similar consideration holds for $\rightarrow \forall x.(F(x) \supset F(x^2))$.) This is the only place in the two constructions where rule (2) is applied and hence it is the only place where a bridge with non-trivial multiplicity is formed. It is through the presence of simple cycles passing through this bridge that the effect of multiplication is propagated in both proofs and the phenomenon of "compression" takes place.

Proof (Theorem 12). The proof Π_n of $\rightarrow F(2^{\underline{2^{2^n}}})$ described in Subsection 2.1 contains n cycles, each of them passing through a copy of the building block proving

$$\forall x.(F(x) \rightarrow F(x^{\underline{k}})) \rightarrow \forall x.(F(x) \rightarrow F(x^{\underline{k^2}})).$$

As described in Subsection 4.1, the logical graph of this proof contains the subgraph



where the circle around one of the splitting points corresponds to the application of rule (2). Note the presence of a bridge of multiplicity 2 associated to it. All the other splitting points in the graph correspond to the application of contraction rules. It is easy to verify through a direct checking on the logical flow graph of Π_n that these are the only simple cycles in Π_n. They form a family with a trivial partition whose representative is the simple cycle passing through the bridge denoted by n in the picture.

We can write down the relation R_n describing the special cycle in proof Π_n, for all $n = 1, 2, 3, \ldots$ as

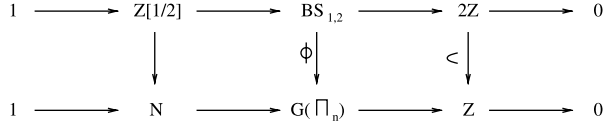
$$\begin{array}{lll} R_1 & b^2 = cbc^{-1} = b^{w_1} & \text{where } w_1 = c \\ R_2 & b^2 = cbcbc^{-1}b^{-1}c^{-1} = b^{w_2} & \text{where } w_2 = cbc \\ R_3 & b^2 = cbcbcbc^{-1}b^{-1}c^{-1}b^{-1}c^{-1} = b^{w_3} & \text{where } w_3 = cbcbc. \\ \vdots & & \end{array}$$

The bridge groups $G(\Pi_n) = \{b, c \mid R_n\}$ (where $n \geq 1$) form a *uniform* family (for $C = 5$ in Definition 11). In fact the relation R_n can be written on the form $b^{w_n}b^{-1}b^{-1} = 1$ and the set S_n can be forced to contain the words w_n (notice that w_1 is the generator c and that $w_{n+1} \in S_{n+1}$ because w_{n+1} is of the form w_nbc, where $w_n \in S_n$ by induction).

The group $BS_{1,2} = \{b, a \mid b^2 = b^a\}$ is an isomorphic subgroup of $G(\Pi_n) = \{b, c \mid b^2 = b^{w_n}\}$ and this is proved as follows. (The argument was suggested by Steve Gersten.) Define a map from the free group in two generators $F(a, b)$ to $F(b, c)$ by $b \mapsto b$, $a \mapsto w_n$, so the relator $b^a b^{-2}$ maps to the relator $b^{w_n} b^{-2}$. This induces a homomorphism ϕ of 1-relator groups $BS_{1,2} \to G(\Pi_n)$ which we claim to be injective. (For $n = 1$, the map is the identity.)

The proof makes use of the Freiheitssatz and the structure of the group $BS_{1,2}$; this is an extension of Z (the cokernel) by the dyadic rationals $Z[1/2]$ (the kernel) where the monodromy is multiplication by 2. The fraction $r/2^i$ with r odd corresponds to the element $(b^r)^{a^{-i}}$.

One has the commutative diagram with rows short exact sequences



The horizontal arrow $BS_{1,2} \to 2Z$ is given by $a \mapsto 2, b \mapsto 0$. The horizontal arrow $G(\Pi_n) \mapsto Z$ is given by $b \mapsto 0, c \mapsto 1$. N is the kernel of the last map. Hence to prove ϕ is injective it suffices to show that its restriction to $Z[1/2]$ is injective.

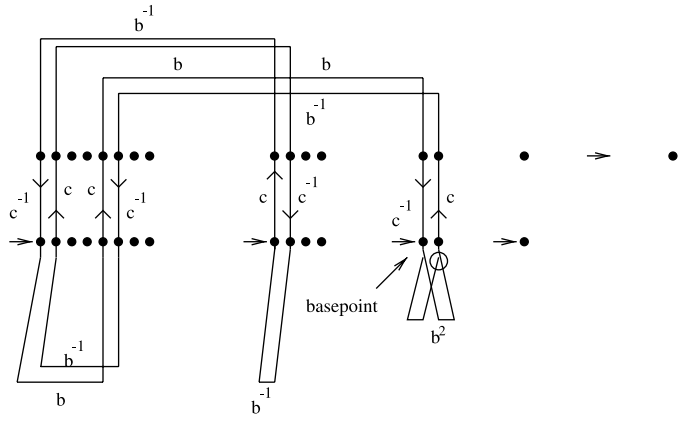
Suppose then that $r/2^i$ is in the kernel of ϕ, where r is odd. This means that $(b^r)^{a^{-i}}$ is in the kernel of ϕ, and hence b^r is in the kernel of ϕ. But by the Freiheitssatz, the subgroups of both $BS_{1,2}$ and $G(\Pi_n)$ generated by the cosets of b are infinite cyclic. Since r is odd, this gives a contradiction. ∎

Proof (Theorem 13). As explained in Subsections 2.1 and 4.1, a proof of $\mathcal{O}(n)$ lines of $\to F(e(n, 2))$ can be constructed by putting together in the obvious way the proofs of the sequents $\to F_i(2)$ (for $i = 1 \ldots n$), and

$$F_n(2), F_{n-1}(2), \ldots, F_1(2), F_0(2) \to F(e(n, 2)).$$

We start with the analysis of the cyclic structure (presented in Subsection 4.1) for $n = 3$, even if at the end we will be interested in those proofs where $n \geq 4$. The proof associated to $n = 3$ displays a simpler structure and simpler calculations are associated to its analysis. The logical flow graph of the simple cycle which passes through the bridge of

non-trivial multiplicity in the proof $\Pi_3 : \to F(e(3,2))$ looks as



where the dots represent atomic formulas in the graph. (This is the same picture presented in Subsection 4.1; here, for convenience, we depict cut-edges vertically; as a consequence, notice that also some of the bridges are pictured upside-down.) The upper list of dots represents all atomic occurrences in the sequent $F_3(2), F_2(2), F_1(2), F_0(2) \to F_0(e_2(3,2))$ and the lower lists of dots represent the atomic occurrences in the sequents $\to F_3(2)$, $\to F_2(2)$, $\to F_1(2)$, $\to F_0(2)$ when one reads them from left to right. It is routine to control that there is only one simple cycle of multiplicity 2 in the logical flow graph of Π_3, and that it passes through the sequents $\to F_3(2)$, $\to F_2(2)$, $\to F_1(2)$. This cycle is special, by definition. Its relation defines the bridge group

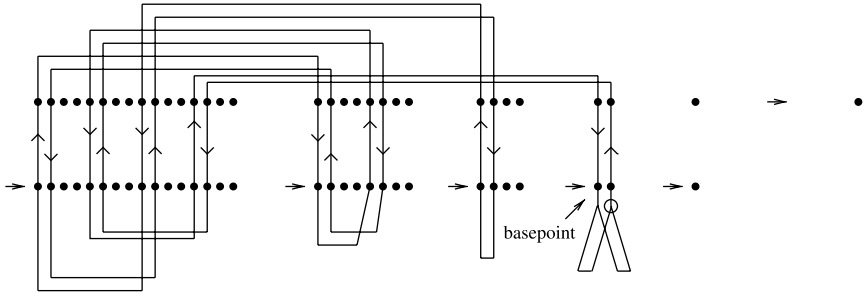
$$G(\Pi_3) = \left\{ b, c \mid b^2 = b^{(b^{a^{-1}})^{-1}} \right\}, \qquad \text{where } a = cbc^{-1}.$$

To see how the relation $b^2 = b^{(b^{a^{-1}})^{-1}}$ is obtained, one might start from the base-point indicated in the picture (the choice of this point of departure is irrelevant), and go along the path following the orientation of the edges. Specifically, this relation comes from the equivalence

$$b^2cb^{-1}c^{-1}b^{-1}cbc^{-1}b^{-1}cb^{-1}c^{-1}bcbc^{-1} = 1$$

which suitably rewritten gives $b^2a^{-1}b^{-1}ab^{-1}a^{-1}ba = 1$ and finally $b^2 = (b^{a^{-1}})^{-1}bb^{a^{-1}}$ which can be also written as $b^2 = b^{(b^{a^{-1}})^{-1}}$.

The proof structure of the simple cycle passing through rule (2) in the proof $\Pi_4 : \rightarrow F(e_2(4, 2))$ can be pictured (as described in Subsection 4.1) as



and from it one reads off the bridge group

$$G(\Pi_4) = \left\{ b, c \mid b^2 = b^{b^{(b^{a^{-1}})^{-1}}} \right\}.$$

Let us make explicit the calculation of the relation. Starting from the base-point indicated in the figure and reading the cycle one writes the equation

$$b^2cb^{-1}c^{-1}b^{-1}cbc^{-1}b^{-1}cb^{-1}c^{-1}bcbc^{-1}b^{-1} \times cb^{-1}c^{-1}b^{-1}cbc^{-1}bcb^{-1}c^{-1}bcbc^{-1} = 1$$

which once rewritten looks as

$$b^2a^{-1}b^{-1}ab^{-1}a^{-1}bab^{-1}a^{-1}b^{-1}aba^{-1}ba = 1$$

and then as

$$b^2 = (b^{a^{-1}})^{-1}b^{-1}(b^{a^{-1}})b(b^{a^{-1}})^{-1}b(b^{a^{-1}}).$$

The family of bridge groups $\{G(\Pi_i)\}_{i=4}^{\infty}$ is uniform, and to show this one can follow the same argument used after Definition 11 to prove that Gersten's family is uniform. ∎

THEOREM 14. *The groups* $BS_*^{(n)} = \{b, c | b^2 = b^{w_n}\}$, *where* $w_1 = c, w_2 = cbc, w_3 = cbcbc$ *and so on, have exponential distortion.*

Proof. We want to show that the distortion of the subgroup $\{b^i\}$ of $BS_*^{(n)}$ is *exponential*, for all $n \geq 1$. The argument is the same as the one we used to prove that $BS_{1,2}$ has exponential distortion (Section 3): for m sufficiently large compared to n, the word b^{2^m} can be reduced using the relation $b^2 = b^{w_n}$ to the word $w_n^m b(w_n^{-1})^m$ which has length $4nm + 1$. ∎

THEOREM 15. *The groups* $Gerst_*^{(n)} = \{b, c \mid b^2 = b^{w_n^*}\}$ *where* $w_1^* = b^d$, $w_2^* = b^{b^d}, w_3^* = b^{b^{b^d}}$, *and so on,* $d = (b^{a^{-1}})^{-1}$ *and* $a = b^c$, *have multi-exponential distortion*.

Proof We want to show that the distortion of the subgroup $\{b^i\}$ of $Gerst_*^{(n)}$ is *multi-exponential*, for all $n \geq 1$. The argument is the same as the one we used to prove that the group $Gerst^{(1)}$ has multi-exponential distortion (Section 3): for m sufficiently large compared to n, the length function satisfies the inequality $l(b^{2^m}) \leq 2 \cdot l(b^m) + 2 \cdot |w_{n-1}| + 1$ (where $w_0 = d$) which makes the distortion of the cyclic group $\{b^i\}$ to be multi-exponential. ∎

We want to compare the *distortion* of the bridge groups associated to proofs with the *expansion* obtained by the elimination of cuts (i.e., lemmas) from these proofs. As we mention in Section 2, there is always a way to transform a proof that uses cuts into a proof that does not contain them [Gen34]. Gentzen procedure of cut elimination is non-deterministic and in principle might not terminate [Gir87a, CS97]. On the other hand Gentzen Cut Elimination Theorem ensures that *there is* always a terminating process which outputs a proof without cuts. In our next definition we look among all cut-free proofs resulting from the effective algorithm proposed by Gentzen and define a function that computes the number of steps of cut-elimination.

DEFINITION 16. The *asymptotic expansion* for a family of proofs $\{\Pi_n\}_{n=1}^{\infty}$ is the growth rate of the function f defined as

$$f(n) = \text{the minimal number of steps used by the procedure of cut-elimination to obtain a cut-free proof from } \Pi_n.$$

In the next two statements we compute the asymptotic expansions of the families of proofs considered in Theorems 12 and 13.

OBSERVATION 17. *Let* $\{\Pi_n :\to F(2^{\underline{2^{2^n}}})\}_{i=1}^{\infty}$ *be the family of proofs of* $\mathcal{O}(n)$ *lines introduced in Subsection* 4.1. *The asymptotic expansion of* $\{\Pi_n\}_{i=1}^{\infty}$ *is exponential*.

Proof. The number of lines in the proof of $\to F(2^{\underline{2^{2^m}}})$ is $\mathcal{O}(m)$. On the other hand one needs $2^m - 1$ duplications (of the proof) to eliminate cuts from the proof. The idea is to start by eliminating the quantified cut-formula at the bottom of the proof. After its elimination one remains with $2 \cdot (m-1)$ quantified formulas to eliminate. Each of them induces a duplication for its elimination. By induction after *at most* 2^m steps we end-up with a cut-free proof. Notice that this process will induce a double-exponential enlargement of the size of the proof. This expansion matches with what we require: any cut-free proof of $\to F(2^{\underline{2^{2^m}}})$ needs to

contain 2^{2^m} applications of rule (2) and with *at least* 2^m duplications we reach the desired number of multiplications. ∎

OBSERVATION 18. *Let* $\{\Pi_n :\to F(e(2,n))\}_{i=1}^{\infty}$ *be the family of proofs of* $\mathcal{O}(n)$ *lines introduced in Subsection* 2.1. *The asymptotic expansion of* $\{\Pi_n\}_{i=1}^{\infty}$ *is multi-exponential.*

Proof. The cut elimination process for proofs of $\to F(e_2(i,2))$ (for $i \geq 4$) is multi-exponential. To see this notice that any cut-free proof of $\to F(e_2(i,2))$ must contain $e_2(i-1,2)$ multiplications and by duplicating (through cut-elimination) one needs as many steps to obtain a proof-tree with $\mathcal{O}(e_2(n-1,2))$ lines. ∎

The last two observations suggest that the distortion of bridge groups associated to proofs may capture the compression induced by the presence of cuts for a sufficiently large class of examples. In Theorem 12 and Observation 17 we provide a family of proofs where the asymptotic expansion is exponential as well as the distortion of the bridge groups associated to it. Theorem 13 and Observation 18 provide an instance of multi-exponential asymptotic expansion and multi-exponential distortion.

The paradigm remains valid for the family of proofs $\{\Pi_n :\to F(2^{2^n})\}_{n=1}^{\infty}$ of $\mathcal{O}(n)$ lines described in Subsection 2.1. The bridge groups associated to this family of proofs are the *free* group $F(b,c)$. Hence, it is straightforward to check that $\{G(\Pi_n)\}_{n=1}^{\infty}$ is a uniform family and that the distortion of these groups is linear. Moreover, by eliminating cuts from (the top of) the proofs Π_n one easily obtains, after $\mathcal{O}(n)$ steps of reduction, cut-free proofs of $\to F(2^{\underline{2^n}})$. (Notice that any cut-free proof has about 2^n steps, which correspond to the 2^n multiplications necessary to construct the arithmetical term representing 2^{2^n}.) Hence, the asymptotic expansion of $\{\Pi_n\}_{n=1}^{\infty}$ is linear.

Remark 19. A family of proofs whose associated bridge groups contain subgroups which are isomorphic to the Baumslag–Solitar group $G_{l,m} = \{b, c \mid c^{-1}b^l c = b^m\}$ (where l, m are positive integers) is easily obtained by simulating the construction of the family proving $\to F(2^{\underline{2^{2^n}}})$. Fixing l, m, the sequent $\forall x.F(x) \supset F(x^{\underline{k}}) \to \forall x.F(x) \supset F(x^{\underline{l\cdot k^2}})$ is provable in a constant number of lines independent by k, and the same is true for the sequent $\to \forall x.F(x) \supset F(x^{\underline{m}})$. (The first sequent can be proved by suitably combining the axioms $F(x) \to F(x), F(x^{\underline{l\cdot k^2}}) \to F(x^{\underline{l\cdot k^2}})$ and the sequent $F(x^k) \to F(x^{\underline{l\cdot k}})$ which can be derived using l applications of rule (2) and l contractions. The second sequent is provable using m applications of rule (2) and l contractions.) One should notice that a bridge of multiplicity l linking the two occurrences $F(x), F(x^{\underline{k}})$ in the antecedent of the first sequent appears in the proof of it, and that a bridge of multiplicity m linking the two occurrences $F(x), F(x^{\underline{m}})$ appears in the proof of the second

sequent. By combining repeatedly suitable instances of the two sequents above one can build short proofs of much weirder powers of 2 than the ones we have been analyzing until now. Just to give an example, if l divides m, say $m = r \cdot l$, then one can build proofs of $\to F(2^{\frac{l^{3^n} \cdot r^{2^n}}{}})$ with $\mathcal{O}(n)$ lines. The bridge groups of these proofs have exponential distortion and their asymptotic expansion is exponential. The structure of the cycles occurring in these proofs is more complicated than the one described for the family of proofs in Theorem 12. Here, the cycles are made out of *two* bridges of non-trivial multiplicities m and l. On the other hand, their geometry remains the same.

Remark 20. If one is interested in the construction of a family of proofs containing groups with polynomial distortion, the first natural step would be to look at *nilpotent* groups which are known [Gro93] to have polynomial distortion and try to describe their relations inside a proof.

7. DISCUSSION

We computed the bridge groups of certain families of proofs and observed that their distortion is comparable to the asymptotic expansion of the cut elimination procedure applied to the proofs of the family. We considered exponential and multi-exponential growth and one might wonder whether proofs with such asymptotic expansion would always contain cycles. Strictly speaking, the answer is no. In fact, there is a purely *syntactic* manipulation of proofs which is based on the elimination of the logical symbol of *negation* from cut-formulas [BL98] and that allows the construction of acyclic[2] proofs with multi-exponential cut elimination. (The symbol of negation is eliminated from a proof by redefining it using new predicates, and this redefinition appears in the statement of the end-sequent of the acyclic proof.) This "elimination of negations" leaves essentially unaltered the proof, and in particular the geometry of the paths in the proof. Hence, apart from syntactical details, the issue remains and one could reformulate our result by asking whether proofs with certain complexity of cut elimination must display a certain geometry of *paths*.

We would like to pose here a question on "reduced" proofs, i.e., proofs where all redundancies are eliminated. (Technically speaking this means that weak occurrences which are "unnecessary" to the proof are forbidden. The precise notion of "unnecessary weak occurrence" has been

[2]It is fairly easy to show that any cycle in a proof must be formed by a bridge passing through both a positive and a negative occurrence in a cut-formula [Car97c]. For this to happen, such a cut-formula has to contain negations.

introduced in [Car97b] and we refer the interested reader there. This hypothesis is not mysterious and it is assumed to avoid trivial counterexamples to the question.)

QUESTION 21. *Let* $\{\Pi_i\}_{i=0}^{\infty}$ *be a family of reduced proofs and* A *be a formula occurring in the proofs* Π_i*'s. If* $\{G(\Pi_i, A)\}_{i=0}^{\infty}$ *is a uniform family of bridge groups with linear distortion* (*respectively polynomial*, *exponential*, *or multi-exponential*) *then is it true that the asymptotic expansion of* $\{\Pi_i\}_{i=0}^{\infty}$ *is linear* (*respectively polynomial*, *exponential*, *multi-exponential*)?

The bridge groups that we consider in Section 6 are very special since they all have two generators and a 1-relator presentation where the subwords c^2, c^{-2} do not occur in the relation (for an introduction to the theory of 1-relator presentations see [LSc77, Bau86]). This leads to a second question

QUESTION 22. *Given a uniform family of finitely presented groups* $\{H_n\}_{n=1}^{\infty}$ *with* 1*-relator presentation, does there exist a uniform family of finitely presented groups* $\{G_n\}_{n=1}^{\infty}$ *with two generators* b, c, *and* 1*-relator presentation such that*

(1) *the relators defining the* G_n*'s do not contain the subwords* c^2, c^{-2};

(2) *if* $\{h^i\}$ *is the cyclic subgroup of* H_n *with maximal distortion then*

$$l_{H_n}(h^i) \approx l_{G_n}(b^i) \qquad \text{for all } i \to \infty;$$

(3) *there is a family of proofs* $\{\Pi_n\}_{n=1}^{\infty}$ *whose bridge group* $G(\Pi_n, A)$ (*for some* A) *has the same distortion of* G_n*, for all* n*, and whose asymptotic expansion corresponds to the distortion of* $\{G(\Pi_n, A)\}_{n=1}^{\infty}$.

In [Ger93], Gersten remarks that the distortion induced by the relation $b^2 = b^{b^a}$ is the fastest that he could prove to be realized by a 1-relator presentation. If our question had a positive answer then by Remark 2 we would have that multi-exponential distortion is indeed the strongest distortion coded in 1-relator presentations.

ACKNOWLEDGMENTS

The idea of a connection between distortion in groups and complexity of cut elimination occurred to me during a talk of Misha Gromov in 1996. Udi Hrushovski and Rohit Parikh made some remarks on an earlier version of this manuscript and Steve Gersten suggested an argument used in the proof of Theorem 12. The exposition took the present form under the suggestion from Misha Gromov to write a text accessible to a wide audience (logicians may smile at the naivety of some of my remarks). I express my sincere thanks to all of them.

REFERENCES

[BL98] M. Baaz and A. Leitsch, Cut normal forms and proof complexity. *Ann. Pure Appl. Logic* **94** (1998).

[BS62] G. Baumslag and D. Solitar, Some two-generators one-relator non-Hopfian groups, *Bull. Amer. Math. Soc.* **68** (1962), 199–201.

[Bau86] G. Baumslag, A survey on groups with a single defining relation, *in* "Proceedings of Groups—St. Andrews, 1985" (E. F. Robertson and C. M. Campbell, Eds.), London Math. Soc. Lecture Note Ser., Vol. 121, pp. 30–58, Cambridge Univ. Press, Cambridge, UK, 1986.

[Boo54] W. W. Boone, Certain simple unsolvable problems of group theory I, *Nederl. Akad. Wetensch. Indag. Math.* **6** (1954), 231–237.

[Bus87] S. R. Buss, The propositional pigeonhole principle has polynomial size frege proofs, *J. Symbolic Logic* **52** (1987), 916–927.

[Bus91] S. R. Buss, The undecidability of k-provability, *Ann. Pure Appl. Logic* **53** (1991), 72–102.

[Car97] A. Carbone, Interpolants, cut elimination and flow graphs for the propositional calculus, *Ann. Pure Appl. Logic* **83** (1997), 249–299.

[Car98] A. Carbone, Cycling in proofs and feasibility, *Trans. Amer. Math. Soc.* **5** (2000), 2049–2075.

[Car97b] A. Carbone, Duplication of directed graphs and exponential blow up of proofs, *Ann. Pure Appl. Logic* **100** (1999), 1–76.

[Car97c] A. Carbone, The cost of a cycle is a square, *J. Symbolic Logic*, in press.

[CS96a] A. Carbone and S. Semmes, Looking from the inside and the outside, *Synthèse*, **125** (2000), 385–412.

[CS97] A. Carbone and S. Semmes, Making proofs without modus ponens: An introduction to the combinatorics and complexity of cut elimination, *Bull. Amer. Math. Soc.* **34** (1997), 131–159.

[CS97a] A. Carbone and S. Semmes, "A Graphic Apology for Symmetry and Implicitness," Mathematical Monographs, Oxford Univ. Press, London, 2000.

[Eps92] D. B. A. Epstein with J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, "Word Processing in Groups," Jones & Bartlett, Boston/London, 1992.

[FW78] H. Furstenberg and B. Weiss, Topological dynamics and combinatorial number theory, *J. Anal. Math.* **34** (1978), 61–85.

[Gen34] G. Gentzen, Untersuchungen über das logische Schließen, I, II, *Math. Z.* **39** (1934), 176–210, 405–431.

[Ger90] S. Gersten, Dehn functions and ℓ_1-norms of finite representations, *in* "Algorithmic and Classification Problems" (Baumslag and Miller, Eds.), MSRI Series, Vol. 23, Springer-Verlag, New York/Berlin, 1990.

[Ger93] S. Gersten, Isoperimetric and isodiametric functions of finite presentations, *in* Geometric Group Theory, Vol. 1" (Niblo and Roller, Eds.), London Math. Soc. Lecture Note Ser., Vol. 181, Cambridge Univ. Press, Cambridge, UK, 1993.

[Gir87] J. Y. Girard, Linear logic, *Theoret. Comput. Sci.* **50** (1987), 1–102.

[Gir87a] J. Y. Girard, "Proof Theory and Logical Complexity," Studies in Proof Theory, Monographs, Vol. 1, Bibliopolis, Napoli, Italy, 1987.

[Gir89a] J.-Y. Girard, Geometry of interaction. I. Interpretation of system F, *in* "Logic Colloquium 1988" (Ferro *et al.*, Eds.), North-Holland, Amsterdam, 1989.

[Gir89b] J.-Y. Girard, Geometry of interaction. II. Deadlockfree algorithms, *in* "Proceedings of COLOG '88" (P. M. Löf and G. Mints, Eds.), Lecture Notes Comput. Sci., Vol. 417, pp. 76–93, Springer-verlag, Berlin, 1989.

[Gir95] J.-Y. Girard, Geometry of interaction. III. The general case, *in* "Proceedings, Workshop on Linear Logic, Cornell 1993, Advances in Linear Logic" (J. Girard, Y. Lafont, and L. Regnier, Eds.), London Math. Soc. Lecture Note Ser., Vol. 222, Cambridge Univ. Press, Cambridge, UK, 1995.

[Gol81] W. D. Goldfarb, The undecidability of the second-order unification problem, *Theoret. Comput. Sci.* **13** (1981), 225–230.

[Gro93] M. Gromov, Asymptotic invariants of infinite groups, *in* "Geometric Group Theory, Vol. 2" (Niblo and Roller, Eds.), London Math. Soc. Lecture Note Ser., Vol. 182, Cambridge Univ. Press, Cambridge, UK, 1993.

[Hak85] A. Haken, The intractability of resolution, *Theoret. Comput. Sci.* **39** (1985), 297–308.

[KP88] J. Krajiček and P. Pudlák, The number of proof lines and the size of proofs in first order logic, *Arch. Math. Logic* **27** (1988), 69–84.

[LSc77] R. C. Lyndon and P. E. Schupp, "Combinatorial Group Theory," Springer-Verlag, New York/Berlin, 1977.

[Mil68] J. Milnor, A note on curvature and fundamental group, *J. Differential Geom.* **2** (1968), 1–7.

[Nov54] P. S. Novikov, Unsolvability for the conjugacy problem in the theory of groups, *Izv. Akad. Nauk SSSR Ser. Mat.* **18** (1954), 485–525.

[OS99] A.Yu. Ol'shanskii and M.V. Sapir, Length and area functions on groups and quasi-isometric Higman embeddings, preprint, `http://atlas.math.vanderbilt.edu/~msapir`, 1999.

[Ore79] V. P. Orevkov, Lower bounds for increasing complexity of derivations after cut elimination, *J. Soviet Math.* **20**, No. 4 (1982).

[Ore93] V. P. Orevkov, "Complexity of Proofs and Their Transformations in Axiomatic Theories," Translations of Mathematical Monographs, Vol. 128, Amer. Math. Soc., Providence, 1993.

[Par71] R. Parikh, Existence and feasibility in arithmetic, *J. Symbolic Logic* **36** (1971), 494–508.

[SBR99] M. V. Sapir, J. C. Birget, and E. Rips, Isoperimetric and isodiametric functions of groups, *Internat. J. Algebra Comput.* (1999).

[Schw55] A. Schwartz, A volume invariant of coverings, *Dokl. Akad. Nauk SSSR* **105** (1995), 32–34.

[Sta78] R. Statman, Bounds for proof-search and speed-up in predicate calculus, *Ann. Math. Logic* **15** (1978), 225–287.

[Sta79] R. Statman, Lower bounds on Herbrand's Theorem, *Proc. Amer. Math. Soc.* **75** (1979), 104–107.

[Tak87] G. Takeuti, "Proof Theory," 2nd ed., Studies in Logic 81, North-Holland, Amsterdam, 1987.

[Tse68] G. S. Tseitin, Complexity of a derivation in the propositional calculus, *Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Akad. Nauk SSSR* **8** (1968), 234–259.

[VdW27] B. L. Van der Waerden, Beweis einer baudetschen vermutung, *Nieuw Arch. Wisk.* (1927), 212–216.